

Wszystko, co chcesz wiedzieć o sieciach komputerowych!

**Barrie Sosinsky**

# Sieci komputerowe

**Jak zaprojektować**  
sieć komputerową?

**Jak zapewnić**  
bezpieczeństwo  
sieci komputerowej

**Jak zestawić**  
bezpieczne  
połączenie VPN?

A collection of network cables with RJ45 connectors, some plugged into a network switch or patch panel, all resting on a large, textured rock. The background is a solid red color.

# Biblia

**Wiedza obiecana**

Tytuł oryginału: Networking Bible

Tłumaczenie: Marek Pałczyński, (wstęp, rozdz. 1 – 11)  
Robert Górczyński, (rozdz. 15 – 28, 30 – 32)  
Tomasz Bienkiewicz (rozdz. 12 – 14, 29)

ISBN: 978-83-246-8346-8

Copyright © 2009 by Wiley Publishing, Inc., Indianapolis, Indiana.  
All Rights Reserved. This translation published under license.

Translation copyright © 2011 by Helion S.A.

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 the Publisher.

Wiley, the Wiley logo and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission.

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](mailto: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?siekb\\_ebook](http://helion.pl/user/opinie?siekb_ebook)

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

- [Poleć książkę na Facebook.com](#)
- [Kup w wersji papierowej](#)
- [Oceń książkę](#)

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

*Książkę tę z całego serca dedykuję mojej żonie Carol Westheimer.*

# Podziękowania

Ta książka jest wynikiem wielu miesięcy intensywnej pracy, w czasie której spotkałem się z dużym wsparciem mojej rodziny i wydawcy. Przez wiele lat przeglądałem i czytałem niezliczone publikacje na temat technologii sieciowych — niektóre ściśle techniczne, inne poświęcone określonej platformie — i wszystkie wymagały pewnego stopnia znajomości zagadnienia. Ta książka ma odgrywać rolę ogólnego wprowadzenia, które pozwoli poszerzyć podstawową wiedzę użytkownika komputera do poziomu eksperckiego w dziedzinie sieci komputerowych. Dołożyłem wszelkich starań, aby uwzględnić nie tylko różnorodne platformy sprzętowe i programowe, ale także informacje na temat projektów będących w początkowej fazie wdrażania.

Chciałbym podziękować mojemu agentowi Mattowi Wagnerowi z Fresh Books za zarekomendowanie mnie jako autora tej pozycji. Jego wieloletnie wsparcie i przyjaźń są dla mnie bardzo ważne.

Możliwość napisania dla wydawnictwa Wiley książki *Sieci komputerowe. Biblia* była dla mnie czymś bardzo ekscytującym. Seria „Biblia”, która została zapoczątkowana w wydawnictwie IDG Books i przejęta przez Wiley, obejmuje liczne renomowane pozycje, które przez lata pomogły wielu osobom w zdobyciu wiedzy na temat różnych technologii. Doskonale pamiętam założycieli IDG i wiem, że choć większość z nich nie jest już związana z książkami z tej serii, ich praca na rzecz wydawania publikacji poświęconych tematyce komputerowej nie ustała.

Chciałbym podziękować zespołowi wydawnictwa Wiley za wsparcie w czasie realizowania projektu. Współpraca z nim była bardzo profesjonalna, a jednocześnie przyjemna. Szczególnie dziękuję trzem osobom, które w największym stopniu zaangażowały się w to przedsięwzięcie: redaktorowi zamawiającemu Courtneyowi Allenowi, redaktorowi projektu Sarah Cisco oraz redaktorowi technicznemu Steve’owi Wrightowi. Steve wykonał znakomitą pracę w czasie korekty technicznej, podobnie jak Sarah i inne osoby uczestniczące w realizacji tego projektu. Wszystkim im szczerze dziękuję.

Przedsięwzięcia związane z publikacją książki wymagają zaangażowania ze strony autora i wydawcy. To wspólne ryzyko. Jednak przygotowanie tej książki wymagało również poświęcenia ze strony mojej rodziny, która musiała się pogodzić z moją częstą nieobecnością wynikającą z toku prac. W trakcie wielu dni i nocy spędzonych nad książką byłem odwiedzany przez sporą liczbę małych, szarych stworzeń, które towarzyszyły mi w pisaniu. Z chwilą zakończenia projektu zaczynam wyczekiwać, kiedy będę mógł spędzić z nimi więcej czasu.

# Rzut oka na książkę

<b>O autorze .....</b>	<b>19</b>
<b>Wprowadzenie .....</b>	<b>21</b>
<b>Część I Podstawy sieci .....</b>	<b>25</b>
Rozdział 1. <b>Wprowadzenie do sieci .....</b>	<b>27</b>
Rozdział 2. <b>Stos protokołów sieciowych .....</b>	<b>43</b>
Rozdział 3. <b>Architektura i projektowanie sieci .....</b>	<b>59</b>
Rozdział 4. <b>Zbieranie informacji o sieci i sporządzanie map sieci .....</b>	<b>85</b>
Rozdział 5. <b>Szerokość pasma i przepustowość .....</b>	<b>105</b>
<b>Część II Sprzęt .....</b>	<b>127</b>
Rozdział 6. <b>Serwery i systemy sieciowe .....</b>	<b>129</b>
Rozdział 7. <b>Interfejsy sieciowe .....</b>	<b>157</b>
Rozdział 8. <b>Media transmisyjne .....</b>	<b>177</b>
Rozdział 9. <b>Routing, przełączanie i mostkowanie .....</b>	<b>205</b>
<b>Część III Rodzaje sieci .....</b>	<b>249</b>
Rozdział 10. <b>Sieci domowe .....</b>	<b>251</b>
Rozdział 11. <b>Sieci peer-to-peer i osobiste sieci LAN .....</b>	<b>271</b>
Rozdział 12. <b>Tworzenie sieci lokalnych .....</b>	<b>293</b>
Rozdział 13. <b>Sieci szkieletowe i rozległe WAN .....</b>	<b>335</b>
Rozdział 14. <b>Sieci bezprzewodowe .....</b>	<b>365</b>
Rozdział 15. <b>Sieć pamięci masowej .....</b>	<b>407</b>
Rozdział 16. <b>Łączy o dużej szybkości .....</b>	<b>441</b>

<b>Część IV Sieci TCP/IP .....</b>	<b>461</b>
Rozdział 17. Internetowy protokół transportowy .....	463
Rozdział 18. Protokoły internetowe .....	485
Rozdział 19. Usługi określania nazw .....	527
<b>Część V Aplikacje i usługi .....</b>	<b>547</b>
Rozdział 20. Sieciowe systemy operacyjne .....	549
Rozdział 21. Usługi domen i katalogowe .....	567
Rozdział 22. Usługi plików i buforowanie .....	593
Rozdział 23. Usługi sieciowe .....	611
Rozdział 24. Protokoły poczty elektronicznej .....	625
Rozdział 25. Strumieniowanie multimediiów .....	643
Rozdział 26. Telefonía cyfrowa i VoIP .....	665
<b>Część VI Bezpieczeństwo w sieci .....</b>	<b>685</b>
Rozdział 27. Usługi i protokoły bezpieczeństwa .....	687
Rozdział 28. Zapory sieciowe, bramy i serwery proxy .....	717
Rozdział 29. Sieci VPN .....	741
<b>Część VII Diagnostyka i zarządzanie siecią .....</b>	<b>759</b>
Rozdział 30. Zarządzanie siecią .....	761
Rozdział 31. Polecenia diagnostyczne sieci .....	789
Rozdział 32. Dostęp zdalny .....	827
Dodatek A Przypisania portów TCP — UDP .....	841
<b>Skorowidz .....</b>	<b>863</b>

# Spis treści

<b>O autorze .....</b>	<b>19</b>
<b>Wprowadzenie .....</b>	<b>21</b>
<b>Część I Podstawy sieci .....</b>	<b>25</b>
<b>Rozdział 1. Wprowadzenie do sieci .....</b>	<b>27</b>
Definiowanie sieci komputerowej .....	28
Rodzaje sieci .....	30
Rodzaje transmisji danych .....	31
Komunikacja punkt-punkt .....	31
Komunikacja rozgłoszeniowa .....	32
Topologie .....	33
Topologie fizyczne .....	33
Topologie hybrydowe .....	39
Topologie logiczne .....	40
Podsumowanie .....	42
<b>Rozdział 2. Stos protokołów sieciowych .....</b>	<b>43</b>
Organizacje opracowujące standardy .....	44
Model odniesienia OSI .....	45
Komunikacja między warstwami .....	46
Warstwa fizyczna .....	50
Warstwa łącza danych .....	51
Warstwa sieciowa .....	52
Warstwa transportowa .....	53
Warstwa sesji .....	53
Warstwa prezentacji .....	54
Warstwa aplikacji .....	54
Model odniesienia TCP/IP .....	55
Porównanie modeli odniesienia OSI i TCP/IP .....	56
Podsumowanie .....	57
<b>Rozdział 3. Architektura i projektowanie sieci .....</b>	<b>59</b>
Architektura sieci i topologia .....	60
Komunikacja punkt-punkt .....	61
Sieci przełączane i pakietowe .....	69

Magistrale .....	70
Segmenty sieci .....	71
Domeny kolizyjne .....	72
Wytłumianie sygnału .....	74
Punkty przyłączeniowe .....	74
Sieci jednostek równorzędnych (peer-to-peer) .....	77
Sieci klient-serwer .....	79
Sieci wielowarstwowe .....	80
Uproszczony klient-serwer .....	82
Serwer terminali .....	82
Sieci X Window .....	83
Podsumowanie .....	84
<b>Rozdział 4. Zbieranie informacji o sieci i sporządzanie map sieci .....</b>	<b>85</b>
Zbieranie informacji o sieci .....	86
Publikowanie informacji o węźle .....	90
Przeglądanie .....	91
Odpytywanie .....	93
Połączenia .....	94
Prosty protokół zarządzania siecią .....	96
Oprzysięganie do zarządzania systemem Windows .....	101
Sporządzanie mapy sieci .....	102
Podsumowanie .....	104
<b>Rozdział 5. Szerokość pasma i przepustowość .....</b>	<b>105</b>
Szerokość pasma i pojemność systemu .....	106
Koraliki w rurze z syropem .....	106
Teoria sygnałów .....	107
Szerokość pasma .....	111
Teoria próbkowania .....	112
Multipleksacja .....	115
Multipleksacja z podziałem czasu .....	115
Multipleksacja z podziałem częstotliwości .....	117
Inne techniki multipleksacji .....	118
Sterowanie przepływem .....	119
Inżynieria ruchu .....	121
Kształtowanie ruchu .....	121
Algorytm ciekącego wiadra .....	122
Algorytm wiadra z żetonami .....	123
Jakość usługi .....	124
Podsumowanie .....	126
<b>Część II Sprzęt .....</b>	<b>127</b>
<b>Rozdział 6. Serwery i systemy sieciowe .....</b>	<b>129</b>
Rodzaje serwerów sieciowych .....	130
Pojemność i obciążenie .....	133
Trzy metody działania .....	133
Metodologia prac projektowych .....	134

Skalowanie serwerów i systemów sieciowych .....	139
Definiowanie poziomów usług .....	139
Szacowanie wydajności .....	143
Rozbudowa serwerów .....	153
Podsumowanie .....	155
<b>Rozdział 7. Interfejsy sieciowe .....</b>	<b>157</b>
Czym jest interfejs sieciowy? .....	157
Fizyczne interfejsy sieciowe .....	158
Logiczne interfejsy sieciowe .....	159
Adresy sieciowe .....	161
Adresy fizyczne .....	161
Konfiguracja interfejsów sieciowych .....	162
Powiązania i dostawcy .....	165
Izolacja i routing .....	168
Izolacja fizyczna .....	168
Izolacja protokołów .....	170
Magistrale komunikacyjne kart sieciowych .....	170
Przykładowa karta sieciowa .....	172
Sterowniki sieciowe .....	173
Podsumowanie .....	174
<b>Rozdział 8. Media transmisyjne .....</b>	<b>177</b>
Media kablowe .....	177
Przygotowanie okablowania .....	178
Skrętka .....	180
Kable współosiowe .....	182
Okablowanie sieci Ethernet .....	184
Kable optyczne .....	187
Łączność bezprzewodowa .....	196
Promieniowanie elektromagnetyczne .....	196
Informacja i transmisja .....	199
Połączenia bezprzewodowe .....	201
Podsumowanie .....	203
<b>Rozdział 9. Routing, przełączanie i mostkowanie .....</b>	<b>205</b>
Przełączanie obwodów i pakietów .....	205
Urządzenia warstw 1. i 2. ....	209
Koncentratory pasywne .....	209
Regeneratory .....	210
Przełączniki .....	211
Mosty .....	212
Routery .....	215
Warstwa sterująca .....	217
Warstwa przełączania .....	217
Topologie routingu .....	219
Metody optymalizacji .....	221
Algorytm wektora odległości .....	221
Algorytm stanu łącza .....	226
Algorytm wektora ścieżki .....	229
Protokół drzewa rozpinającego .....	232

Routery cebulowe .....	242
Sieci Tor .....	244
Jednostki klienckie Tor .....	244
Ukryte usługi .....	245
Bramy .....	247
Podsumowanie .....	247

## Część III Rodzaje sieci ..... 249

### Rozdział 10. Sieci domowe ..... 251

Elementy sieci domowej .....	252
Połączenia szerokopasmowe .....	253
Połączenia bezprzewodowe .....	257
Połączenia stałe .....	258
Ethernet .....	258
Linie telefoniczne .....	259
Zasilanie przez Ethernet .....	262
Technologia HomePlug .....	262
Serwery sieci domowych .....	268
Podsumowanie .....	269

### Rozdział 11. Sieci peer-to-peer i osobiste sieci LAN ..... 271

Sieci peer-to-peer .....	272
Czyste sieci P2P .....	273
Systemy hybrydowe .....	276
Sieci przyjacielskie .....	280
Magistrale .....	281
Uniwersalna magistrala szeregową .....	282
FireWire .....	285
Bluetooth .....	287
Połączenia .....	288
Profile .....	290
Podsumowanie .....	290

### Rozdział 12. Tworzenie sieci lokalnych ..... 293

Wprowadzenie .....	294
Standardy sieci LAN .....	295
Kanały rozgłoszeniowe .....	298
Ethernet .....	300
Ramki protokołu Ethernet .....	303
Protokół CSMA/CD .....	307
Transmisja w trybie pełnoduplexowym (dwukierunkowym) .....	310
Sieci Token Ring .....	310
Sieci FDDI .....	314
Sieci wykorzystywane w automatyce .....	318
Standard X10 i automatyka domowa .....	319
Systemy sterowania procesami .....	324
Podsumowanie .....	333

<b>Rozdział 13. Sieci szkieletowe i rozległe WAN .....</b>	<b>335</b>
Sieci rozległe WAN .....	336
Sieci z komutacją obwodów .....	337
Sieć telekomunikacyjna PSTN .....	339
ISDN .....	341
DSL .....	342
Sieć telewizji kablowej .....	346
Łacza T i E .....	346
Sieci SONET/SDH .....	348
Architektura SONET/SDH .....	349
Ramkowanie .....	350
Protokół PoS (Packet over SONET/SDH) .....	353
Sieci pakietowe .....	354
Sieci X.25 .....	355
Technologia SMDS .....	356
Technologia ATM .....	357
Frame Relay .....	359
Protokół MPLS .....	360
Sieci Internet i Internet2 .....	361
Punkty wymiany ruchu internetowego .....	361
Internet2 .....	363
Podsumowanie .....	364
<b>Rozdział 14. Sieci bezprzewodowe .....</b>	<b>365</b>
Sieci bezprzewodowe .....	366
Sieci Wi-Fi .....	367
Standardy grupy IEEE 802.11x .....	368
Standard 802.11 .....	370
Standard 802.11y .....	372
Modulacja .....	373
Protokół 802.11 .....	380
Punkty dostępu i bramy .....	385
Regeneratory i mosty .....	386
Tryb Wireless Distribution System .....	388
Routery i bramy bezprzewodowe .....	390
Konfiguracja routera .....	391
Aktualizacja routera .....	392
Sieć bezprzewodowa laptopów XO .....	393
Anteny .....	395
Charakterystyka anteny .....	396
Anteny inteligentne .....	398
Oprogramowanie wspierające sieci bezprzewodowe .....	399
Bezpieczeństwo .....	402
Szyfrowanie WEP .....	402
Szyfrowanie WPA .....	404
Podsumowanie .....	406

<b>Rozdział 15. Sieć pamięci masowej .....</b>	<b>407</b>
Potrzeba utworzenia sieci pamięci masowej .....	408
Różne typy sieci pamięci masowej .....	409
SAN kontra NAS .....	410
Koncepcja Business Continuance Volumes .....	411
Wirtualizacja pamięci masowej .....	412
Model współdzielonej sieci pamięci masowej .....	414
Współdzielone taśmy .....	415
Domena pamięci masowej .....	420
Agregacja .....	421
Modele urządzeń .....	422
Sieci Fibre Channel .....	425
Standardy sieci Fibre Channel .....	426
Oznaczenia portów .....	427
Protokół Fibre Channel Protocol .....	428
Fibre Channel z pętlą arbitrażową .....	430
Sieć Fibre Channel Switched fabrics .....	431
Technologie pamięci masowej z zastosowaniem IP .....	433
Protokół iSCSI .....	435
Fibre Channel over IP .....	436
Protokół Internet Fibre Channel Protocol .....	438
Zarządzanie siecią Storage Area Network .....	438
Protokół Internet Storage Name Service .....	439
Podsumowanie .....	440
<b>Rozdział 16. Łącza o dużej szybkości .....</b>	<b>441</b>
Wydajne systemy obliczeniowe .....	442
Poza gigabitowy Ethernet .....	443
10GBase-T .....	445
Przetwarzanie stosu TCP bez użycia procesora .....	445
Sieci Zero Copy Network .....	448
Virtual Interface Architecture .....	449
InfiniBand .....	451
Klastry sieciowe .....	453
Równoważenie obciążenia .....	455
Systemy przetwarzania sieciowego .....	457
Podsumowanie .....	459
<b>Część IV Sieci TCP/IP .....</b>	<b>461</b>
<b>Rozdział 17. Internetowy protokół transportowy .....</b>	<b>463</b>
Transmission Control Protocol .....	464
Struktura pakietu .....	465
Pola nagłówka .....	466
Flagi .....	466
Pole sumy kontrolnej .....	467
Pola kontrolne .....	468
Pole danych .....	468
Operacje protokołu .....	469
Połączenia .....	472

Kontrola przepływu .....	473
Przesuwające się okna .....	473
Kontrola przeciążenia sieci .....	473
Multipleksowanie .....	474
Protokół User Datagram Protocol .....	475
Porty .....	477
Problemy z TCP .....	481
Podsumowanie .....	482
<b>Rozdział 18. Protokoły internetowe .....</b>	<b>485</b>
Ogólny opis protokołu IP .....	486
Protokół Internet Protocol Version 4 (IPv4) .....	487
Adresowanie IPv4 .....	488
Tworzenie podsieci .....	504
Ustawianie adresu IP .....	505
Adresowanie statyczne .....	507
Adresowanie dynamiczne .....	508
Dynamic Host Configuration Protocol .....	508
Konfiguracja .....	509
Zabezpieczanie DHCP .....	510
Protokół Bootstrap .....	510
Protokół Internet Control Message Protocol .....	511
IPv6 (Internet Protocol Version 6) .....	514
Adresowanie IPv6 .....	516
Datagramy IPv6 .....	523
Protokół IPv6 Neighbor Discovery .....	524
ICMPv6 .....	525
Podsumowanie .....	526
<b>Rozdział 19. Usługi określania nazw .....</b>	<b>527</b>
Plik HOSTS .....	528
Protokół Address Resolution Protocol (ARP) .....	531
Żądania ARP .....	531
Protokół Reverse Address Resolution Protocol .....	532
Przeglądanie bufora ARP .....	533
Podstawowy system wejścia-wyjścia sieci .....	534
Windows Internet Name Service .....	535
Domain Name System .....	536
Żądania DNS .....	537
Topologia DNS .....	539
Rekordy zasobów .....	540
Określanie nazw kontra usługi katalogowe .....	544
Podsumowanie .....	545
<b>Część V Aplikacje i usługi .....</b>	<b>547</b>
<b>Rozdział 20. Sieciowe systemy operacyjne .....</b>	<b>549</b>
Co to jest sieciowy system operacyjny? .....	550
Protokoły i usługi .....	551
Sieciowy system operacyjny — ogólny kontra specjalnego przeznaczenia .....	551

Sieciowe systemy operacyjne i oprogramowanie .....	552
Unix .....	554
POSIX .....	556
Architektura STREAMS i gniazda .....	557
Single UNIX specification .....	558
Linux .....	559
Dystrybucje .....	560
Solaris .....	561
Novell NetWare oraz Open Enterprise Server .....	563
Windows Server .....	564
Podsumowanie .....	566
<b>Rozdział 21. Usługi domen i katalogowe .....</b>	<b>567</b>
Usługi katalogowe i domeny .....	568
Banyan VINES .....	569
Typy domen .....	570
Wzajemna współpraca .....	571
Serwery domen .....	571
Usługi katalogowe .....	572
Synchronizacja i replikacja .....	573
Jednokrotne logowanie .....	574
Przestrzenie nazw .....	575
Zarządzanie polityką .....	576
Kontrola dostępu bazująca na roli .....	580
Zarządzanie tożsamością .....	581
X.500 oraz LDAP .....	582
Network Information Service .....	583
Serwery LDAP .....	584
LDAP Data Interchange Format .....	584
Novell eDirectory .....	585
Nazwa wyróżniająca .....	586
Microsoft Active Directory .....	587
Replikacja .....	590
Podsumowanie .....	591
<b>Rozdział 22. Usługi plików i buforowanie .....</b>	<b>593</b>
Network Attached Storage .....	594
Funkcje NAS .....	595
NAS kontra SAN .....	597
Sieciowe bufor plików .....	597
Protokoły sieciowych systemów plików .....	598
Network File System .....	599
Server Message Block/Common Internet File System .....	600
Samba .....	602
Bezpieczeństwo Samby .....	603
Określanie nazw w serwerze Samba i przeglądanie udziałów .....	603
Samba w Ubuntu .....	604
Distributed File System .....	606
Podsumowanie .....	609

<b>Rozdział 23. Usługi sieciowe .....</b>	<b>611</b>
Protokół HyperText Transfer Protocol .....	612
Żądania HTTP .....	613
Kody stanów HTTP .....	615
Statyczne kontra dynamiczne strony internetowe .....	619
Usługi sieciowe .....	620
Architektura oparta na usługach .....	622
Podsumowanie .....	624
<b>Rozdział 24. Protokoły poczty elektronicznej .....</b>	<b>625</b>
Trzy główne protokoły .....	626
Przegląd poczty elektronicznej .....	626
Technologia push e-mail .....	628
Wiadomości w częściach .....	628
Simple Mail Transfer Protocol .....	630
Typy MIME .....	631
Protokół Post Office Protocol .....	636
Klienty poczty Webmail .....	637
Protokół Internet Message Access Protocol .....	637
Serwery poczty .....	638
Konfiguracja klienta poczty .....	639
Podsumowanie .....	642
<b>Rozdział 25. Strumieniowanie multimedialnych .....</b>	<b>643</b>
W jaki sposób działa strumieniowanie? .....	644
Strumieniowanie kontra pobieranie progresywne .....	644
Emisja pojedyncza kontra multiemisja .....	648
Protokoły strumieniowania .....	650
Protokół Real-Time Streaming Protocol .....	650
Protokół Real-Time Transport Protocol .....	651
Protokół Real-Time Control Protocol .....	653
Język Synchronized Markup Integration Language .....	654
Kodowanie .....	655
Serwery strumieniowania .....	658
Formaty strumieniowanych plików .....	659
Odtwarzacze .....	661
Flash .....	662
Silverlight .....	663
Podsumowanie .....	664
<b>Rozdział 26. Telefonia cyfrowa i VoIP .....</b>	<b>665</b>
Telefonia cyfrowa .....	666
Systemy PBX .....	667
Asterisk .....	668
Oprogramowanie Cisco Unified Communications Manager .....	669
Microsoft Response Point .....	669
Technologia VoIP .....	671
Adaptery ATA .....	672
Telefony VoIP .....	674
Protokoły VoIP .....	675
System integracji telefonu z komputerem .....	678

Wideotelefonia .....	679
Mobile VoIP .....	680
Kamery internetowe .....	681
Podsumowanie .....	682

## **Część VI Bezpieczeństwo w sieci ..... 685**

### **Rozdział 27. Usługi i protokoły bezpieczeństwa ..... 687**

Ogólny opis bezpieczeństwa sieci .....	688
Luki w zabezpieczeniach sieci .....	688
Baza danych National Vulnerability Database .....	690
Miejsca ataku .....	691
Reguły tworzenia bezpiecznej sieci .....	694
Technologie NLA oraz NAP .....	696
Bezpieczne protokoły w internecie .....	698
IPsec .....	699
Zestaw protokołów Transport Layer Security .....	702
Protokół HTTPS .....	703
Szyfrowanie i kryptografia .....	705
Atak siłowy i ignorancja .....	706
Algorytmy klucza symetrycznego .....	708
Algorytmy asymetryczne, czyli algorytmy klucza publicznego .....	711
Kerberos .....	712
Podsumowanie .....	715

### **Rozdział 28. Zapory sieciowe, bramy i serwery proxy ..... 717**

Zapory sieciowe .....	718
Funkcje zapory sieciowej .....	718
Strefy sieciowe .....	725
Filtry bezstanowe .....	727
Filtry stanu .....	727
Filtry aplikacji .....	730
Domyślnie odmawiaj .....	731
Mechanizm NAT .....	732
Serwery proxy .....	735
Przezroczyste serwery proxy i przynęty .....	738
Serwery odwrotnego proxy .....	738
Podsumowanie .....	740

### **Rozdział 29. Sieci VPN ..... 741**

Technologie VPN .....	742
Rodzaje VPN .....	742
Łączy VPN .....	743
Topologie połączeń między lokacjami .....	745
Urządzenia w sieci VPN .....	746
Oprogramowanie VPN .....	747
Szyfrowanie .....	752
Tunelowanie .....	753
Protokoły tunelowania .....	754
Protokół Generic Routing Encapsulation .....	754
Tunel IPsec .....	754

TLS/SSL .....	755
Tunelowanie punkt-punkt .....	755
Podsumowanie .....	756

## **Część VII Diagnostyka i zarządzanie siecią ..... 759**

### **Rozdział 30. Zarządzanie siecią ..... 761**

Znaczenie zarządzania siecią .....	762
FCAPS .....	762
Zarządzanie usterkami .....	764
Zarządzanie konfiguracją .....	769
Zarządzanie rozliczeniami i administracją .....	778
Zarządzanie wydajnością .....	779
Zarządzanie bezpieczeństwem .....	782
Kategorie oprogramowania do zarządzania siecią .....	783
Platformy sieciowe .....	784
Podsumowanie .....	787

### **Rozdział 31. Polecenia diagnostyczne sieci ..... 789**

Diagnostyka sieci .....	790
Polecenia sieciowe .....	790
Narzędzia wiersza poleceń .....	790
Powłoki sieciowe .....	807
Powłoka Windows NetShell .....	807
Sesje Telnet .....	814
PowerShell .....	815
Podsumowanie .....	826

### **Rozdział 32. Dostęp zdalny ..... 827**

Dostęp zdalny .....	828
Protokoły połączenia zdalnego .....	829
Usługi dostępu zdalnego .....	830
Pulpit zdalny .....	831
Serwery RADIUS .....	834
Sesje RADIUS .....	836
Roaming RADIUS .....	837
Protokół Diameter .....	838
Podsumowanie .....	840

### **Dodatek A Przypisania portów TCP — UDP ..... 841**

### **Skorowidz ..... 863**



# O autorze

**Barrie Sosinsky** od ponad 25 lat publikuje prace na temat komputerów i technologii informatycznej. Rozpoczął tę działalność na początku lat 80. ubiegłego wieku od pisanie artykułów o komputerach osobistych dla „Boston Computer Society”. Wydał książki na temat systemów operacyjnych, aplikacji, baz danych, składu komputerowego oraz sieci. Współpracuje między innymi z wydawnictwami Que, Sybex, Ventana, IDG, Wiley. Był świadkiem wielu przełomowych zmian w przemyśle informatycznym i sam wielokrotnie zmieniał zainteresowania technologią.

Barrie jest prawdziwym entuzjastą komputerów PC. Uwielbia je budować, a także wyszukiwać i poznawać nowe aplikacje, pozwalające mu na zajmowanie się wciąż nowymi zagadnieniami i na nadążanie za zmianami w technologii komputerowej, która jego zdaniem jest jeszcze w okresie niemowlęctwa. Barrie żyje dostatecznie długo, żeby widzieć, jak Boston Red Sox zdobywają nie jedno, ale dwa trofea World Series. Ma zamiar pożyć tak długo, żeby zobaczyć swoje wnuki i sklonowanego mamuta włochatego. Do tej listy dodaje również nowy kamień milowy w dziejach — uniwersalny translator. Urządzenie, które pojawi się, jak sądzi Barrie, w następnej dekadzie.

Autor mieszka w Medfiels, w stanie Massachusetts, około 25 mil na południowy zachód od Bostonu, z sześcioma kotami — są to Stormy, Shadow, Smokey, Scamper, Slate i Spat — swoim synem Josephem, córką Allie, żoną Carol i żółwiem Brittany, w domu otoczonym przez sosny, w którego pobliżu żyją jelenie i dzikie indyki.

Wszelkie komentarze i sugestie Barrie przyjmuje drogą elektroniczną pod adresem

*[bsosinsky@mindspring.org](mailto:bsosinsky@mindspring.org).*



# Wprowadzenie

Sieć jest bardzo rozległym tematem, który obejmuje wszystkie aspekty technologii komputerowej. Niektóre osoby twierdzą nawet, że komputer niepodłączony do sieci nie jest wcale komputerem. Można również nieco wyolbrzymić tę zależność i stwierdzić, jak kilka lat temu tygodnik „Sun”, że „sieć jest komputerem”. Wiadomo bowiem, że każda licząca się technologia komputerowa uwzględnia pewne metody wysyłania danych do innych komputerów i odbierania ich z innych jednostek. Pierwsze komercyjnie konstruowane komputery były projektowane w taki sposób, aby ich koszt amortyzował się dzięki współdzieleniu czasu dostępu do jednostek przez wielu użytkowników. Komputerowe systemy rezerwacyjne, takie jak SABRE, łączyły terminale na całym świecie, a gdy komputer osobisty stał się niemal tak tani jak zwykły terminal, w rozproszonych po całym świecie węzłach zaczęły funkcjonować komputery PC.

Rozwój komputerów osobistych w latach 80. i 90. stał się przyczyną szybkiego rozwoju technologii sieciowych, które ułatwiły ustanawianie połączeń, uczyniły je tańszymi, a co najważniejsze, zestandaryzowały działania producentów. Powstanie sieci TCP/IP charakterystycznych dla internetu było możliwe dzięki pracom nad wieloma różnymi rozwiązaniami firmowymi. Choć w książce zostały opisane niektóre starsze technologie, w większości jej tematyka odnosi się do standardów sieciowych bazujących na protokołach TCP/IP. Trzeba jednak pamiętać, że w sieciach o szczególnie dużej szybkości transmisji danych, bardzo szerokim paśmie i wysokim poziomie niezawodności stosowane są inne rozwiązania.

Wiele ze wspomnianych technologii alternatywnych zostało krótko scharakteryzowanych przy okazji wymieniania różnych ich możliwości. Dlatego wraz z omówieniem poszczególnych rodzajów sieci lokalnych wzmiankowane są sieci rozległe, włókna światłowodowe, sieci pamięci masowej, chmury obliczeniowe, systemy przetwarzania sieciowego i inne zaawansowane technologie. W różnych częściach książki rozproszone zostały również informacje na temat nowych produktów, takich jak laptop XO-1 zaprojektowany przez organizację One Laptop Per Child (laptop dla każdego dziecka), system przetwarzania rozproszonego SETI @ Home, sieci SNET, transmisja solitonowa i wiele innych rozwiązań, o których z pewnością część osób słyszała, a które będzie można bliżej poznać dzięki temu opracowaniu.

Pisząc książkę, chciałem przygotować ogólną monografię na temat sieci, a nie publikację faworyzującą określoną platformę komputerową. Nie jestem zagorzałym zwolennikiem żadnej konkretnej platformy. Moim pierwszym komputerem był Macintosh, a z biegiem lat zacząłem korzystać z systemów Windows. Ostatnio pracuję w systemie Ubuntu, a wcześniej wielokrotnie zdarzało mi się pracować z różnymi dystrybucjami Linuksa i systemem

Solaris. Obecnie korzystam z niewielkiej sieci. Jednak w czasie wielu lat pracy miałem do czynienia zarówno z małymi, jak i dużymi sieciami, homogenicznymi i heterogenicznymi. Każdy sieciowy system operacyjny ma swoje wady i zalety, ale niemal każdy z nich umożliwia wykonywanie najważniejszych operacji sieciowych.

Prezentowane przykłady odnoszą się do technologii sieciowych obecnych w różnych platformach systemowych. Niestety (z mojego punktu widzenia), liczba przykładów odnoszących się do systemu Windows jest większa, niżbym chciał. Przyczyną takiego stanu rzeczy jest przede wszystkim brak czasu i łatwość przeprowadzenia testów, a nie szczególna natura zagadnienia.

Starałem się znaleźć złoty środek między teoretyzowaniem zapewniającym solidne podstawy z dziedziny sieci komputerowych a omawianiem zagadnień praktycznych, które pozwalają na stosowanie nowych technologii i produktów w codziennej pracy. W książce znajduje się wiele informacji na temat określonych produktów. Bardzo się starałem, aby były one precyzyjne i aktualne. Niestety, dane tego typu szybko ulegają przedawnieniu. Wielokrotnie jeszcze przed wydaniem książki dowiadywałem się, że określone produkty stały się niedostępne, a firmy zamknęto. Z wieloma z tych produktów związane były osoby, które spotkałem lub znałem, więc pisanie o nich często przywodziło mi na myśl minione czasy.

Książka składa się z siedmiu części:

- ◆ Część I. W pierwszej części zostały przedstawione ogólne teorie i zasady pracy sieci komputerowej. Zagadnienia te w większości odnoszą się do różnych modeli sieciowych, które zostały powszechnie zaakceptowane przez przemysł.
- ◆ Część II. W drugiej części znajduje się omówienie komponentów sprzętowych, w tym systemów komputerowych, interfejsów sieciowych, fizycznych mediów transmisyjnych oraz metod tworzenia i utrzymywania obwodów ze szczególnym wyróżnieniem routingu.
- ◆ Część III. Trzecia część książki jest poświęcona różnym rodzajom sieci — sieciom o niewielkim rozmiarze i domowym, technologii peer-to-peer, rozwiązaniom LAN i WAN, sieciom pamięci masowych (SAN), a także technologiom zapewniającym wysoką wydajność i dużą szybkość transmisji.
- ◆ Część IV. W części czwartej znajduje się omówienie poszczególnych elementów stosu TCP/IP. Tematyka rozdziałów nie koncentruje się jedynie na sposobie wykorzystania protokołów TCP/IP, ale obejmuje również adresowanie, odwzorowanie nazw i inne operacje, które trapią i zajmują administratorów sieci.
- ◆ Część V. Piąta część odnosi się do różnych aplikacji i usług działających w sieciach komputerowych. Opisane tutaj zostały ogólne zasady funkcjonowania systemów operacyjnych oraz usług sieciowych, takich jak usługi katalogowe, plikowe, pocztowe, strumieniowanie multimedialnych oraz telefonia internetowa.
- ◆ Część VI. Tematyka trzech rozdziałów części szóstej koncentruje się wokół bezpieczeństwa pracy sieciowej. Wśród omawianych zagadnień znajdują się protokoły i usługi związane z zabezpieczeniem danych, firewalle, bramy, serwery pośredniczące, wirtualne sieci prywatne oraz inne technologie zapewniające izolację ruchu sieciowego.

- ♦ Część VII. W ostatniej części książki zostały zamieszczone informacje na temat technik zarządzania siecią i diagnozowania stanu sieci. Są w niej opisane klasy aplikacji przeznaczonych do zarządzania siecią, z których część to rozbudowane platformy, nieznane większości Czytelników. Dwa kończące książkę rozdziały zawierają omówienia sposobów diagnozowania stanu sieci oraz technologii zdalnego dostępu.

Mam nadzieję, że czytanie książki sprawi Ci tyle samo radości, ile mi sprawiło jej pisanie.

Barrie Sosinsky  
Medfield, Massachusetts  
18 marca 2009



# Część I

# Podstawy sieci

## **W tej części:**

**Rozdział 1.** Wprowadzenie do sieci

**Rozdział 2.** Stos protokołów sieciowych

**Rozdział 3.** Architektura i projektowanie sieci

**Rozdział 4.** Zbieranie informacji o sieci i sporządzanie map sieci

**Rozdział 5.** Szerokość pasma i przepustowość



# Rozdział 1.

## Wprowadzenie do sieci

### W tym rozdziale:

- ♦ Rodzaje sieci i transmisji sieciowych
- ♦ Topologie sieci
- ♦ Sieci pLAN, LAN, MAN, CAN i WAN

Sieć komputerowa to połączenie lub zbiór połączeń między dwoma komputerami lub większą ich liczbą, ustanowione w celu wymiany danych. Sieć składa się z wielu różnych elementów: komputerów, przełączników, kabli itp. Chcąc właściwie sklasyfikować konkretną sieć, należy uwzględnić kilka czynników, takich jak liczba jej komponentów, rozmieszczenie jej składników oraz sposób łączenia poszczególnych jednostek. W dalszej części rozdziału zostały opisane różne rodzaje sieci komputerowych oraz związane z nimi założenia projektowe.

Najmniejszą sieć stanowią dwa komputery połączone bezpośrednio ze sobą za pomocą kabla. W konfiguracjach złożonych z niewielkiej liczby systemów, w których nie jest stosowany jeden centralny serwer, wykorzystuje się model grup roboczych bazujących na połączeniach równorzędnych (ang. *peer-to-peer*). Część magistrali komputerowych jest konfigurowalna, przez co zalicza się je do sieci o małym zasięgu, zwanych osobistymi sieciami LAN lub sieciami pLAN (ang. *personal LAN*). Typowym przykładem wspomnianego rozwiązania są połączenia Bluetooth. Z kolei technologia USB nie umożliwia konfigurowania połączeń, przez co nie jest uznawana za technologię sieciową.

Sieć obejmująca swoim zasięgiem biuro, piętro budynku lub cały budynek jest nazywana siecią lokalną, czyli siecią LAN. W sieciach LAN można korzystać z różnych protokołów komunikacyjnych i łączyć ze sobą stacje klienckie różnego typu. Sieć LAN wydzielona za pomocą odpowiedniego urządzenia separującego stanowi niezależną sieć LAN. Jeśli urządzenie to wydziela wiele sieci LAN odległych od siebie geograficznie, tworzy sieć rozległą, czyli sieć WAN.

Do analizy i kategoryzacji topologii sieciowych można zastosować teorię grafów. Rozmieszczane na różne sposoby urządzenia sieci formują zazwyczaj linie (łańcuchy), gwiazdy, pierścienie lub tworzą siatkę połączeń typu „każdy z każdym”. Różne topologie mają różne zastosowania i różne wymagania sprzętowe. Sam proces wyznaczania topologii odnosi się do fizycznego lub logicznego rozmieszczenia elementów bądź do sposobu propagowania sygnału w sieci.

## Definiowanie sieci komputerowej

Aby zbiór elementów został uznany za sieć komputerową, musi obejmować: oprogramowanie komunikacyjne, systemy operacyjne oraz komponenty sieciowe (takie jak przełączniki, media transmisyjne czy system adresacji). W każdej sieci komputerowej można wyróżnić następujące elementy składowe:

- ♦ połączone ze sobą systemy,
- ♦ oprogramowanie komunikacyjne,
- ♦ urządzenia sieciowe,
- ♦ fizyczne medium transmisyjne,
- ♦ system adresacji uwzględniający wszystkie z wymienionych komponentów.

Powyższa definicja jest dostatecznie ogólna, aby można było objąć nią systemy, w których skład wchodzi nie tylko komputery, ale również telefony komórkowe (a także telefonia komórkowa z różnymi jej funkcjami), urządzenia przeznaczone do przechowywania danych, komponenty Wi-Fi, systemy strumieniowania danych, łącza szerokopasmowe oraz wiele innych rozwiązań, które w jakiś sposób są uwzględniane w sieci komputerowej.

Oprogramowanie komunikacyjne jest powszechnie stosowane w każdym urządzeniu, które zapewnia łączność z innymi jednostkami. Jest zatem instalowane w systemach operacyjnych komputerów, w jednostkach sieciowych (takich jak routery i firewalle), w układach ASIC, również w pamięci flash kart sieciowych i koncentratorów, a nawet w fizycznych mediach transmisyjnych, jeśli zapewniają one przełączanie danych lub regenerację sygnału.

Termin „fizyczne medium transmisyjne” odnosi się do każdego medium, które może przetransmitować sygnały elektromagnetyczne. Sygnał transmisyjny jest opisywany przez zmieniającą się w czasie amplitudę, poziom lub częstotliwość sygnału nośnego, które odpowiadają danym przenoszonym na pewnej odległości i są zrozumiałe dla urządzenia odbiorczego. Zmiany stanu sygnału mogą mieć charakter ciągły (sygnał analogowy) lub impulsowy i ograniczony do znanej liczby stanów (sygnał cyfrowy). Choć istnieją komputery analogowe, niemal wszystkie wykorzystywane obecnie urządzenia są rozwiązaniami cyfrowymi, a dokładniej binarnymi. Systemy binarne przekazują informację w jednym z dwóch stanów: włączonym lub wyłączonym, 1 lub 0, TAK lub NIE, o napięciu 1 lub 2. Komputery cyfrowe wykorzystują sygnały binarne i logikę boolowską z uwagi na łatwość do realizacji i szybkość w działaniu sygnalizację oraz możliwość wykorzystania ich do reprezentowania dowolnych znaków i rozwiązania niemal każdego równania matematycznego.

Transmisja binarnego sygnału podczas strumieniowania danych między dwoma systemami nie ogranicza się jedynie do wykorzystania materialnego medium, jakim są kable i przewody, ale znajduje zastosowanie w przekazywaniu informacji w każdym zakresie widma elektromagnetycznego. Uruchamiając przeglądarkę w telefonie komórkowym, łączymy się z siecią za pomocą fal radiowych. Z kolei operatorzy sieci komórkowych do przesyłania danych na dużych odległościach wykorzystują nadajniki mikrofalowe. Komunikacja za pośrednictwem urządzeń zgodnych ze standardem 802.11 (Wi-Fi) również wymaga transmisji na falach radiowych. Dlatego też niekiedy doświadczamy nakładania się transmisji z telefonów

bezprzewodowych i bezprzewodowych sieci komputerowych lub zakłócania połączeń realizowanych na częstotliwości 2,4 GHz w standardzie 802.11g (Wi-Fi) podczas pracy kuchenki mikrofalowej. Większość rozwiązań opisanych w dalszej części książki odnosi się do stałych połączeń między komputerami (bazujących na kablach). Należy pamiętać, że połączenia radiowe nie wykorzystują fizycznego medium transmisyjnego.



Połączenia radiowe zostały opisane w rozdziałach 5., 8. i 14.

Żadna operacja, w której dane nie są przekazywane w sposób automatyczny, nie może zostać uznana za operację sieciową. Na przykład transmisją sieciową z pewnością nie można określić zadania skopiowania danych z jednego komputera do pamięci USB, przejścia między urządzeniami i zapisania informacji w drugiej jednostce. Taki sposób działania jest określany mianem *sneakernetu*<sup>1</sup>. Nie ma żadnego związku z pracą sieci komputerowej, gdyż informacje nie są przesyłane między systemami z wykorzystaniem mechanizmu adresacji lub identyfikacji — dane zapisane w pamięci USB nie są skojarzone z żadnym adresem.

Z drugiej strony nie można być również zbyt skrupulatnym w narzucaniu rygoru adresacji. Transmisja rozgłoszeniowa jest przecież uważana za formę komunikacji sieciowej, mimo że system docelowy nie jest w niej wskazywany za pomocą konkretnego adresu. Każdy system odpowiadający definicji odbiorcy może bowiem skorzystać z transmisji rozgłoszeniowej. Poza tym sama transmisja rozgłoszeniowa jest istotnym elementem komunikacji w ramach większości sieci. Poszczególne systemy wysyłają rozgłoszenia, aby poinformować inne jednostki, że są gotowe do działania, czyli że pracują i mogą realizować żądania. Transmisja rozgłoszeniowa pozwala na identyfikowanie systemów sieciowych oraz na przeszukiwanie sieci. Z definicji komunikacji rozgłoszeniowej wynika, że każdy system zdolny do jej prowadzenia musi spełniać poniższe warunki.

- ♦ Funkcjonuje w tej samej sieci co inne urządzenia, z którymi wymienia dane, lub korzysta z tego samego protokołu identyfikacji (np. Windows NetBEUI lub WINS).
- ♦ Ma zainstalowane oprogramowanie, które umożliwia odbieranie strumienia danych, zarządzanie nim oraz pozwala na udział w komunikacji rozgłoszeniowej.

Zamieszczona w książce definicja sieci komputerowej stanowi, że za sieć uznawane jest każde połączenie lub zbiór połączeń przeznaczonych do wymiany danych. Stwierdzenie to będzie wykorzystywane wielokrotnie podczas omawiania najważniejszych problemów, z jakimi mają do czynienia administratorzy sieci korporacyjnych, użytkownicy łączący się z różnorodnymi usługami (np. z pocztą elektroniczną) bądź osoby, które muszą zdobyć podstawowe umiejętności, aby zarządzać urządzeniami sieciowymi występującymi zazwyczaj w każdym domu. W tej książce zamieszczone zostały podstawowe informacje na temat sieci komputerowych, odnoszące się do większości problemów, z którymi spotykamy się w codziennej pracy lub podczas zabawy.

<sup>1</sup> Nazwa pochodzi od angielskich słów *sneak* i *net*. Pierwsze z nich oznacza tenisówkę. Natomiast drugie jest określeniem sieci — *przyp. tłum.*

## Rodzaje sieci

Kategoryzacja sieci jest wykonywana na podstawie stopnia rozproszenia jednostek, rozmiaru sieci oraz jej architektury. Niekiedy siecią jest zwykłe połączenie dwóch komputerów za pomocą kabla szeregowego, równoległego lub USB, prowadzące do powstania równorzędnej zależności między urządzeniami. Na przykład połączenie komputerów kablem szeregowym w celu przesłania zainstalowanego oprogramowania jest w praktyce operacją utworzenia sieci typu peer-to-peer. Relacja między jednostkami jest wówczas tworzona *ad hoc*, czyli na żądanie. Choć większość osób nie uznałaby takiej konfiguracji za sieć, z pewnością za takową uważane byłoby przyłączenie kilku systemów do koncentratora i utworzenie w ten sposób grupy roboczej równorzędnych stacji. *Grupa robocza* jest zbiorem komputerów, które nie współdzielą jednej bazy danych systemu zabezpieczeń i w której każda jednostka może dowolnie udostępniać swoje usługi innym stacjom.

Pod względem dystrybucyjnym najmniejszymi sieciami są sieci pLAN (nazywane również sieciami PAN). Termin pLAN odnosi się zazwyczaj do kilku urządzeń peryferyjnych połączonych z pojedynczym systemem komputerowym. Dobrym przykładem tego typu rozwiązania są połączenia Bluetooth. Urządzenia Bluetooth ustanawiają połączenia na częstotliwościach radiowych, wykorzystując technikę rozpraszania widma ze „skakaniem” po częstotliwościach (częstotliwość kanału komunikacyjnego jest nieustannie zmieniana). Strumień danych po segmentacji jest przekazywany na ponad 75 częstotliwościach na odległość około 10 metrów. Choć zasięg tego rozwiązania nie jest imponujący, połączenia pLAN można uznać za bardzo wyrafinowane technologicznie. Sieci Bluetooth mają wbudowane mechanizmy autokonfiguracji, mogą transmitować dane w sposób bezpieczny, a każde z urządzeń może informować inne jednostki o swoich funkcjach i usługach. Technologię Bluetooth wykorzystuje wiele telefonów, słuchawek, myszy, klawiatur, drukarek, urządzeń GPS, konsol do gier i urządzeń PDA.

Bluetooth z pewnością spełnia przedstawione w książce kryteria sieci, ponieważ obejmuje wszystkie elementy charakterystyczne dla sieci. Technologia ta została uwzględniona w opracowaniu, gdyż użytkownik musi ją odpowiednio skonfigurować. Z drugiej strony technologia USB umożliwia przyłączenie do jednego kontrolera nawet 127 urządzeń, ale ponieważ połączenia są automatycznie konfigurowane, jest uznawana za rodzaj magistrali komputerowej. Wszystkie wymienione wcześniej urządzenia Bluetooth można przyłączyć do komputera również za pośrednictwem portu USB. Dlatego mimo że są urządzeniami sieci pLAN w technologii Bluetooth, są jednocześnie określane jako urządzenia peryferyjne. Choć rozwiązania USB doskonale sprawdzają się w przekazywaniu danych, nie będą szczegółowo opisywane w dalszej części książki.



Więcej informacji na temat technologii USB znajduje się w rozdziale 11.

Znaczna część niniejszej książki została poświęcona sieciom lokalnym (LAN). Określenie *lokalne* jest jednak względne. Sieć LAN wyznaczają komputery połączone ze sobą na obszarze pojedynczego pokoju, piętra lub budynku. Niekiedy może się ona ograniczać do zaledwie kilku jednostek połączonych za pomocą koncentratora. Sieci LAN są wydzielane na podstawie określonego schematu adresacji oraz w odniesieniu do zbioru reguł (czyli protokołów), które rządzą komunikacją między stacjami. Dlatego AppleTalk i NetWare są uznawane za niezależne sieci LAN. Konfiguracje heterogeniczne nie są niczym szczególnym. Często w jednej sieci LAN funkcjonuje domena Windows z klienckimi systemami Macin-

tosh i serwerami NetWare. Wspomniane systemy Macintosh i NetWare mogą również działać w sieci AppleTalk lub NetWare, ale oprogramowanie oraz system adresacji są niezależne w ramach każdej z tych sieci.

Sieć przestaje być pojedynczą siecią LAN, gdy nie występuje w niej jednolita adresacja lub gdy dwie sieci (lub większa ich liczba) są połączone za pomocą routera. Na przykład jeśli pewnej grupie komputerów przypiszemy adresy pochodzące z jednej puli, a kolejnej grupie komputerów nadamy adresy z innej puli, otrzymamy konfigurację, którą można nazwać siecią LAN. Praktyczny sposób realizacji tego zadania polegałby na wykorzystaniu różnych zakresów adresów IP (np. 192.168.1.x i 192.168.3.x) lub wydzieleniu podsieci w ramach jednego z zakresów (np. od 192.168.1.x do 192.168.1.99 oraz od 192.168.1.100 do 192.168.1.199). W obydwu opisanych przypadkach wynikiem będzie sieć LAN. Jeśli jednak między tymi dwoma sieciami zostałyby umieszczone routery (czyli bardziej „inteligentne” przełączniki), uzyskalibyśmy zbiór odrębnych sieci. Zależność ta wydaje się jeszcze bardziej oczywista, gdy odległość między dwoma routerami jest znaczna lub gdy na wejściu do każdej sieci znajdują się dodatkowe routery.

Do opisanego długodystansowych połączeń sieciowych lub połączeń obejmujących wiele sieci wykorzystuje się kilka różnych terminów. Najpopularniejszym jest „sieć rozległa” (WAN — *Wide Area Network*). Odnosi się on do każdego przypadku, w którym mamy do czynienia z siecią sieci. Doskonałym przykładem sieci WAN jest internet, niekiedy określany mianem intersieci. Często wykorzystuje się również określenia „sieć kampusowa” (CAN — *Campus Area Network*) czy sieć metropolitarna (MAN — *Metropolitan Area Network*). Sieć CAN obejmuje pewną grupę budynków. Natomiast sieć MAN rozciąga się na obszarze miasta.

Sieci rozległe geograficznie bazują zazwyczaj na łączach o dużej przepustowości, takich jak kable światłowodowe, które przyłączane do regeneratorów umożliwiają pokonywanie dużych dystansów. Łącze o dużej przepustowości jest nazywane *łączem szkieletowym*. Gdyby na przykład system banku z Wall Street w Nowym Jorku przekazywał dane przez łącze optyczne ułożone na dnie rzeki Hudson do centrum danych w New Jersey, taką konfigurację można by uznać za sieć MAN.

## Rodzaje transmisji danych

W sieciach stosuje się dwa rodzaje transmisji danych — transmisję punkt-punkt oraz transmisję rozgłoszeniową.

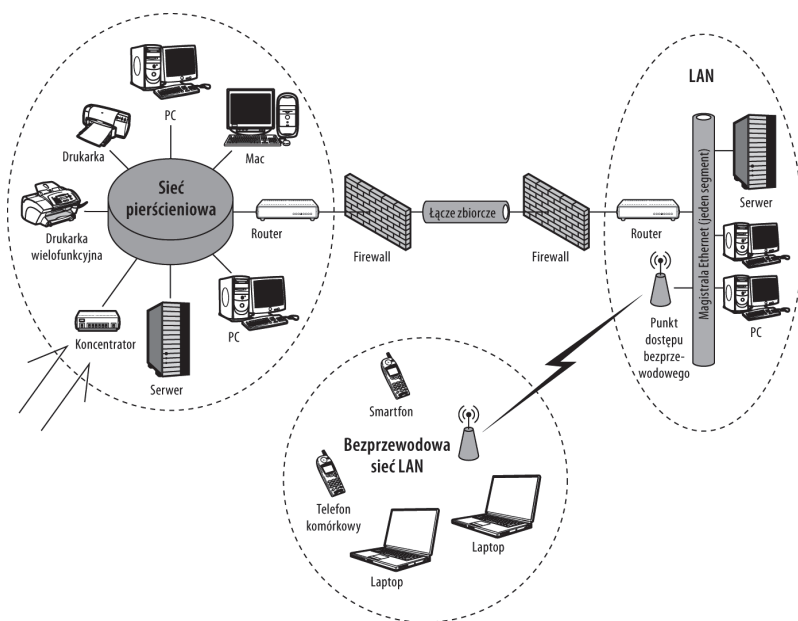
### Komunikacja punkt-punkt

W komunikacji punkt-punkt tworzone jest połączenie między dwoma systemami sieciowymi, które pełnią funkcję nadajnika i odbiornika danych. Przekazywane dane mogą być przetwarzane przez urządzenia pośrednie umieszczone na trasie pomiędzy jednostkami końcowymi. Wiele z rozwiązań komunikacji punkt-punkt zakłada ustanawianie nadmiarowych ścieżek transmisyjnych, często o różnej długości. Dlatego też rola routerów w sieciach punkt-punkt jest jednym z kluczowych czynników, uwzględnianych podczas szacowania wydajności tej sieci.

Aby zagwarantować poprawność połączenia w komunikacji punkt-punkt, często trzeba stosować wiele różnych technologii, właściwych dla różnych podsieci objętych połączeniem. Problem ten jest charakterystyczny dla sieci WAN, co ilustruje rysunek 1.1. Przedstawiona na nim sieć WAN składa się z trzech podsieci — z sieci pierścieniowej, magistralnej oraz bezprzewodowej. Jedną z technik przekazywania informacji (nazywana „przechowaj i przekazaj” (ang. *store-and-forward*)) polega na zapisywaniu pakietów dostarczanych z jednego z routerów i przetrzymaniu ich w urządzeniu do czasu, aż zwolni się wybrane łącze punkt-punkt do urządzenia docelowego. Mechanizm ten jest często nazywany *przełączaniem pakietów*. Sieci pakietowe bazujące na przekazywaniu niewielkich pakietów o określonym rozmiarze — nazywanych *komórkami* — są podstawą funkcjonowania telefonii bezprzewodowej i znajdują zastosowanie w powszechnie wykorzystywanych obecnie sieciach komórkowych.

**Rysunek 1.1.**

Sieć pakietowa WAN



## Komunikacja rozgłoszeniowa

W komunikacji rozgłoszeniowej wiadomość wygenerowana przez jeden system jest dostarczana do wszystkich pozostałych systemów w sieci. Przykładem rozwiązania tego typu jest sieć satelitarna. Jeżeli komunikacja rozgłoszeniowa zostanie skonfigurowana w taki sposób, aby dane wysyłane przez jeden system były dostarczane do podzbioru wszystkich systemów końcowych, przesyłanie informacji ma charakter transmisji wielopunktowej i jest nazywane *multiemisją* (ang. *multicasting*). Multiemisja jest często stosowana podczas strumieniowania danych multimedialnych, gdy te same informacje muszą zostać dostarczone do wielu systemów jednocześnie.

Pakiety rozgłoszeniowe zawierają pole adresowe, które wskazuje system lub systemy docelowe. Urządzeniem odbiorczym może być pojedynczy komputer lub grupa komputerów. Niemniej każdy węzeł sieci rozgłoszeniowej musi zweryfikować pakiet. Jeśli zawarty w nim adres docelowy zgadza się z adresem urządzenia, pakiet jest przetwarzany. W przeciwnym razie zostaje zignorowany.



Można przyjąć, że im większa jest sieć (w sensie geograficznym), tym bardziej prawdopodobne jest to, że wykorzystuje ona połączenia punkt-punkt. Sieci o mniejszych rozmiarach funkcjonują wydajniej z zastosowaniem technologii rozgłoszeniowych.

## Topologie

Inny sposób klasyfikowania sieci polega na określeniu ich topologii. Topologia sieci opisuje rozmieszczenie i wzajemne powiązania elementów sieci, uwzględniając zarówno same urządzenia końcowe, jak i połączenia między nimi. Ponieważ każdy komponent, któremu można przypisać adres, jest uznawany za element sieci, w opracowywaniu topologii trzeba również uwzględnić elementy logiczne (wirtualne), utworzone za pomocą oprogramowania.

Do opisu sieci stosuje się definicje topologii fizycznej (charakteryzujące zależności między urządzeniami), topologii logicznej (odnoszące się do zależności i hierarchii między jednostkami sieci) lub topologii hybrydowej (stanowiącej połączenie dwóch wcześniej wymienionych topologii). W bardzo rzadkich przypadkach sieć można również opisać za pomocą topologii sygnału. Topologia logiczna odwzorowuje zależności między węzłami w sieci. Wyznacza ich wzajemne umiejscowienie oraz zasady komunikacji między nimi. Topologia fizyczna odnosi się natomiast do fizycznych połączeń oraz fizycznej struktury sieci. Topologię sygnału określa się niekiedy w celu zobrazowania tego, w jaki sposób określone rodzaje sygnałów są propagowane w sieci. Choć topologie fizyczne i logiczne mogą być identyczne, zazwyczaj znacznie się od siebie różnią.

Matematyczne opisanie połączonych ze sobą systemów wymaga zastosowania teorii grafów. Na jej podstawie z kolei możliwe jest wyznaczenie liczby węzłów niezbędnych w każdej z topologii, liczby połączeń itp. Określona topologia sieciowa nie zależy od szybkości łączy, zastosowanych protokołów komunikacyjnych czy rodzaju węzłów lub łączy. Topologia wyznacza jedynie wzajemne rozmieszczenie poszczególnych elementów.

## Topologie fizyczne

Topologia fizyczna określa rozmieszczenie urządzeń wchodzących w skład sieci. Komponentami w schemacie topologicznym mogą być węzły pośrednie, urządzenia końcowe, a także połączenia między nimi. Oto kilka rodzajów topologii fizycznych:

- ♦ **Magistrala.** Każdy z węzłów jest przyłączony do wspólnego łącza.
- ♦ **Gwiazda.** Poszczególne węzły komunikują się ze sobą za pośrednictwem jednego z węzłów.
- ♦ **Pierścień.** Poszczególne węzły są połączone ze sobą za pomocą pojedynczych łączy tworzących zamknięty pierścień.
- ♦ **Siatka.** Poszczególne węzły są łączone bezpośrednio ze sobą.
- ♦ **Drzewo.** Poszczególne węzły są dołączane do węzłów wewnętrznych, tworząc rozgałęzienia podobne do drzewa.

W praktyce wiele topologii sieciowych jest połączeniem kilku wymienionych rodzajów.

Wyznaczenie liczby połączeń między wszystkimi węzłami w przypadku zastosowania topologii siatki nie stanowi większego problemu. Stałe pojedyncze połączenie punkt-punkt w tego typu konfiguracji jest jednocześnie najłatwiejsze do zrealizowania oraz najbardziej niepraktyczne. Aby obsłużyć  $n$  węzłów końcowych, potrzebne jest bowiem  $2(n + 1)$  połączeń, co w przypadku sieci o dużym rozmiarze oznaczałoby wykorzystanie niemożliwej do zaimplementowania liczby stałych połączeń. Z tego względu większość komunikacji punkt-punkt, na przykład w telefonii, wykorzystuje technikę przełączania, która eliminuje konieczność utrzymywania stałych połączeń punkt-punkt między węzłami sieci. Przełączanie można zrealizować w urządzeniach (*przełączanie obwodów*) lub poprzez zmianę adresów w strumieniu danych (*przełączanie pakietów*).

Rober Metcalfe — jeden z twórców technologii Ethernet — wyraził wartość użytkową sieci przełączanej za pomocą liczby jej użytkowników. Zgodnie z prawem Metcalfa wartość użytkowa sieci telekomunikacyjnej jest proporcjonalna do kwadratu liczby użytkowników tej sieci, a liczba połączeń punkt-punkt między systemami przyłączonymi do sieci ( $N$ ) jest wyrażana wzorem:

$$N = n(n-1)/2$$

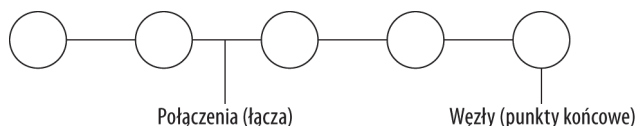
gdzie  $n$  odpowiada liczbie węzłów. Gdy liczba węzłów rośnie, przebieg funkcji zbliża się asymptotycznie do krzywej  $n^2$ . Asymptota jest krzywą, do której zbliżają się wyniki funkcji podczas zwiększania wartości zmiennej tej funkcji. Gdy w opisanym przypadku  $n$  otrzymuje duże wartości, równanie  $(n^2 - n)/2$  jest zdominowane przez element  $n^2$ , a wartość funkcji będzie zbliżona do  $1/2$  wartości  $n^2$ .

## Topologia magistrali

Magistrala jest wspólnym medium transmisyjnym, łączącym ze sobą dwa węzły sieciowe zwane punktami końcowymi lub większą ich liczbę. Punkt końcowy jest odpowiednikiem węzła, a jego najważniejszą cechą jest to, że ma własny adres. Karta sieciowa komputera jest węzłem lub punktem końcowym, podobnie jak router. Punktem końcowym może być również port przełącznika lub routera.

Łąca szkieletowe lub zbiorcze (trunkowe) są doskonałymi przykładami magistrali liniowej (rysunek 1.2), ponieważ wszystkie dane są przekazywane między punktami końcowymi w ramach wspólnej magistrali. Na rysunku 1.2 magistrala została przedstawiona jako zbiór łączy; każde kółko odpowiada węzłowi sieci lub punktowi końcowemu. Przekazywanie informacji z jednego węzła do innego rozpoczyna się od dostarczenia danych do najbliższego węzła, w którym sprawdzany jest adres odbiorcy. Jeśli określony węzeł nie jest odbiorcą informacji, następuje przekazanie danych do kolejnego węzła, aż do dostarczenia ich do ostatecznego odbiorcy. Mechanizm ten wprowadza pewne opóźnienia propagacyjne, które jednak w nowoczesnych sieciach można uznać za niewielkie.

**Rysunek 1.2.**  
System magistrali  
liniowej

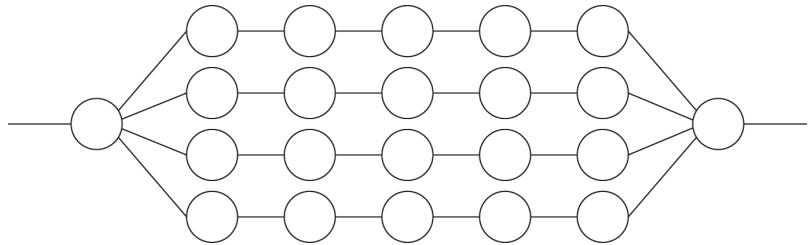


Każdy z punktów końcowych magistrali (rysunek 1.2) musi być logicznie odróżnialny od innych punktów końcowych. Ponadto każde urządzenie wykonuje funkcję *terminatora*. Polega ona na absorbowaniu sygnału tak, aby nie był on przekazywany w dalszej części magistrali. Terminatory są projektowane w taki sposób, aby ich impedancja odpowiadała impedancji linii transmisyjnej. Często są to zwykłe rezystory, choć część terminatorów to urządzenia aktywne, które za pomocą obwodu elektronicznego eliminują odbicie sygnału.

Magistrale liniowe, wykorzystujące szkieletowe linie transmisyjne, są wydajnymi rozwiązaniami, ale nie dość elastycznymi. Brak elastyczności należy rozumieć jako trudność w dostosowywaniu magistrali liniowej do zmiany liczby jednostek, zmiany położenia jednostek lub innych modyfikacji struktury. W celu zwiększenia elastyczności sieci magistralnych opracowana została technologia magistrali rozproszonych. Magistrala rozproszona obejmuje kilka gałęzi, z których każda działa podobnie jak magistrala liniowa. Również w tym przypadku węzły zawierają komponent terminatora. Natomiast sam system rozproszonej magistrali często jest mylony z systemem o topologii drzewa, charakterystycznym dla systemów plików. W rozproszonych magistralach nie występuje jednak centralny węzeł, który skupiałby połączenia do wszystkich pozostałych węzłów. Nie istnieje również określona hierarchia węzłów. Strukturę rozproszonej magistrali przedstawiono na rysunku 1.3.

**Rysunek 1.3.**

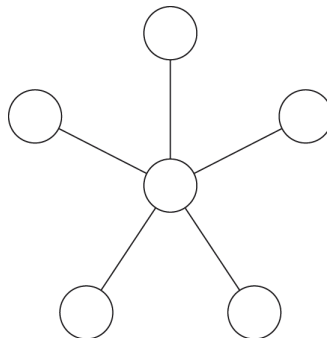
Struktura  
rozproszonej  
magistrali

**Topologia gwiazdy**

Topologia gwiazdy jest powszechnie stosowaną topologią sieciową. Zgodnie z jej założeniami połączenia punkt-punkt rozchodzą się gwieźdzście od węzła centralnego, co zostało pokazane na rysunku 1.4. W topologii gwiazdy wszystkie dane przesyłane przez sieć muszą zostać przekazane przez węzeł centralny. W najprostszej konfiguracji elementem centralnym jest pojedyncza krosownica. Choć może nim być również komponent aktywny, który retransmituje dane, wykonując jednoczesną korekcję błędów i wzmacniając sygnał. Krosownica to matryca połączeń elektrycznych, z których każde jest otwarte na końcu, dzięki czemu wybierając odpowiednie gniazda, można połączyć dowolne obwody.

**Rysunek 1.4.**

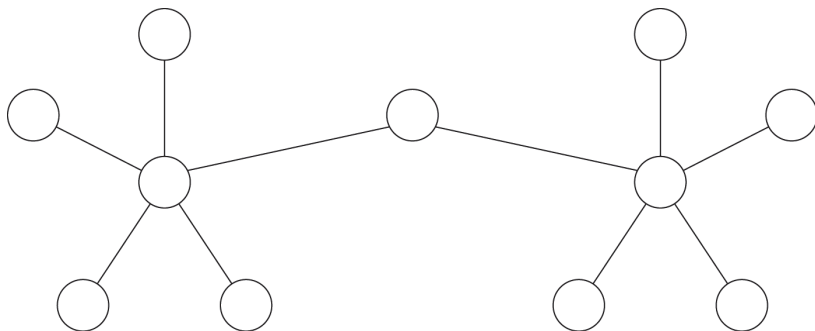
Sieć gwieżdzista



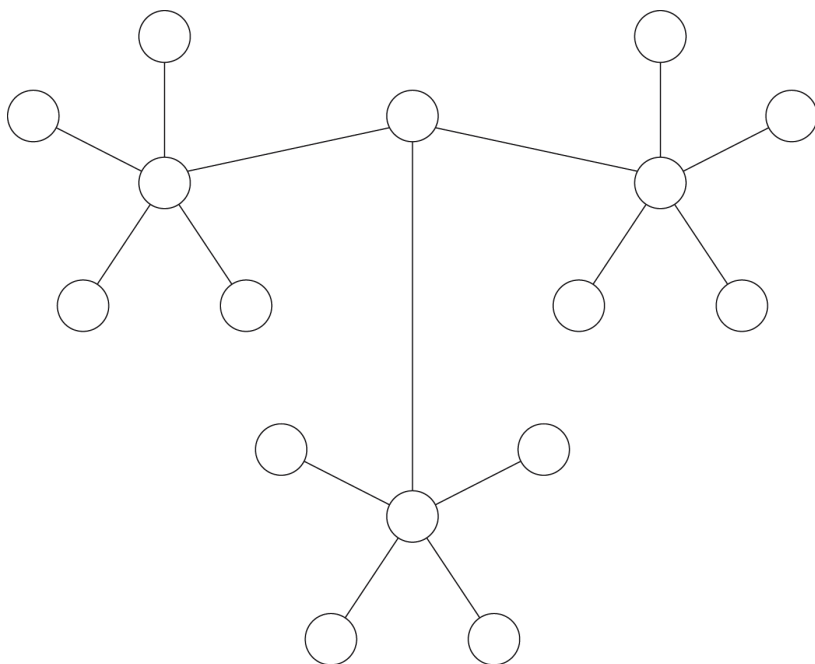
Sieci gwieździste można zaprojektować w taki sposób, aby jeden z elementów łączył dwie lub większą liczbę sieci. Rozwiązanie to stosuje się w topologiach rozszerzonej gwiazdy i rozproszonej gwiazdy. W topologii rozszerzonej gwiazdy wykorzystywane są regeneratory, które wydłużają odległość między elementem centralnym a węzłem dołączonym. Zastąpienie regeneratora przełącznikiem powoduje przekształcenie topologii rozszerzonej gwiazdy w topologię hybrydową, nazywaną niekiedy fizyczną gwiazdą. Topologie rozszerzonej gwiazdy oraz rozproszonej gwiazdy zostały przedstawione odpowiednio na rysunkach 1.5 i 1.6.

**Rysunek 1.5.**

*Topologia  
rozszerzonej gwiazdy*

**Rysunek 1.6.**

*Topologia  
rozproszonej gwiazdy*



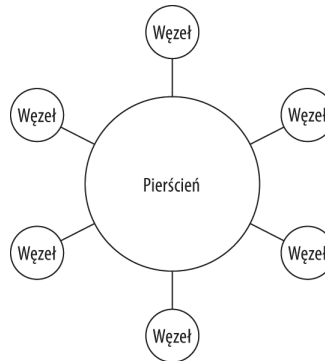
W topologii rozproszonej gwiazdy kilka sieci gwieździstych jest łączonych ze sobą liniowo w łańcuch. W rozproszonej gwieździe nie istnieje hierarchia i nie ma punktu centralnego, z którego można by wyznaczyć połączenia do zdalnych węzłów. Wszystkie sieci gwieździste skupione w ogólnej gwieździe są względem siebie równorzędne.

Gdy sieci gwiazdowe wykorzystują komunikację rozgłoszeniową, są nazywane *rozgłoszeniowymi sieciami wielodostępnymi*. W takich przypadkach sygnał jest dostarczany do wszystkich rozgałęzień sieci. Niektóre sieci gwiazdowe przekazują dane do poszczególnych węzłów na podstawie adresów jednostek. Takie sieci są nazywane *nierozgłoszeniowymi sieciami wielodostępnymi* (NBMA — *non-broadcast multi-access*).

## Topologia pierścienia

Sieć pierścieniowa (pokazana na rysunku 1.7) stanowi zamkniętą pętlę, w której każdy węzeł jest elementem inicjującym i kończącym transmisję danych. W sieci pierścieniowej dane są przekazywane w jednym kierunku, od jednego węzła do następnego, do chwili, gdy jeden z węzłów okaże się urządzeniem docelowym. Jednokierunkowa transmisja danych zabezpiecza sieć przed przeciążeniem i nakładaniem sygnałów. Nakładanie się sygnałów prowadzi bowiem do występowania błędów. Topologie podwójnego pierścienia zapewniają przekazywanie informacji w obydwu kierunkach (w jednym kierunku w każdym z pierścieni) lub umożliwiają wykorzystanie drugiego pierścienia jako łącza zapasowego, zwiększając odporność konfiguracji na awarie.

**Rysunek 1.7.**  
*Sieć pierścieniowa*



Do typowych przykładów implementacji topologii pierścieniowej zaliczają się sieci Token Ring (IBM), ARCNET oraz FDDI. W rozwiązaniu Token Ring pomiędzy węzłami stanowiącymi elementy pierścienia przekazywany jest specjalny znacznik (ang. *token*). Węzeł dysponujący znacznikiem może przetwarzać dane krążące w pierścieniu. Okablowanie w sieci Token Ring odpowiada strukturze gwiazdowej, jednak każdy koncentrator ma dwa połączenia do innego koncentratora, dzięki czemu tworzy pierścień. Węzeł centralny (koncentrator) został w standardzie 802.5 Token Ring nazwany *wielostanowiskową jednostką dostępową* (ang. *multistation access unit*).

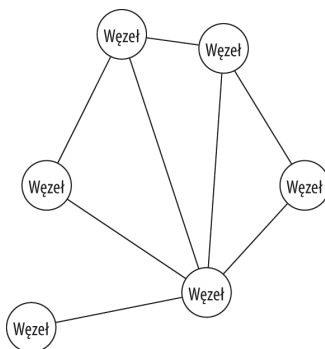
## Topologia siatki

Topologia siatki to rozwiązanie, w którym każdy węzeł sieci może mieć ustanowione połączenie punkt-punkt z dowolnym innym węzłem. Struktura takiej sieci została przedstawiona na rysunku 1.8. Topologia siatki stanowi więc rozwinięcie opisaną wcześniej topologii magistralnej. Zgodnie z prawem Reeda sieci o topologii siatki mają wartość użytkową wykładniczo proporcjonalną do liczby węzłów:

$$2^n - n - 1$$

**Rysunek 1.8.**

*Częściowo połączona  
sieć siatkowa*

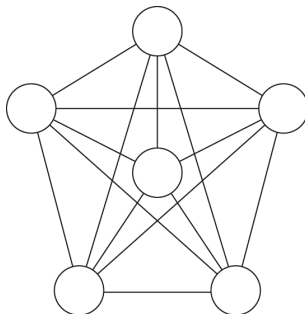


gdzie  $n$  odpowiada liczbie węzłów. Sieci siatkowe charakteryzują się dużą liczbą połączeń wychodzących z każdego węzła. Liczba połączeń dwustronnych przy  $n$  węzłach wynika z prawa Metcalfe'a i wynosi  $n(n-1)/2$ .

Sieć siatkowa może być połączona częściowo (zgodnie z rysunkiem 1.8) lub w pełni (zgodnie z rysunkiem 1.9) w zależności od tego, czy każdy z węzłów jest połączony z każdym innym węzłem w sieci za pomocą łącza typu punkt-punkt. W praktyce w pełni połączone sieci siatkowe nie są stosowane (oprócz instalacji o niewielkich rozmiarach), ponieważ liczba potrzebnych łączy istotnie zwiększa koszty wdrożenia systemu. W sieci częściowo połączonej niektóre węzły (a często większość) są połączone z kilkoma innymi węzłami za pomocą łączy typu punkt-punkt. Brak jednorodnych połączeń wprowadza do sieci pewne opóźnienia. Jednak można ten problem eliminować przez stosowanie „inteligentnego” routingu, który zapewni wybór innej trasy, gdy jedno z łączy jest zajęte. Doskonałym przykładem częściowo połączonej sieci siatkowej jest internet.

**Rysunek 1.9.**

*W pełni połączona  
sieć siatkowa*



## Topologie drzewiaste lub hierarchiczne

W sieciach drzewiastych pojedynczy węzeł najwyższego poziomu jest połączony z węzłami znajdującymi się na drugim poziomie hierarchii. Każdy z węzłów drugiego poziomu jest z kolei połączony z dowolną liczbą węzłów trzeciego poziomu itd. W rozwiązaniu tym muszą istnieć co najmniej trzy poziomy, gdyż dwa poziomy są właściwe dla topologii gwiazdy.

Liczba połączeń w topologii drzewiastej jest określona za pomocą równania:

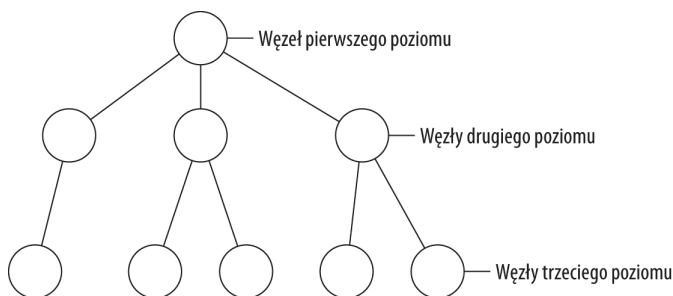
$$L = n - 1$$

gdzie  $L$  odpowiada liczbie połączeń punkt-punkt, a  $n$  wyznacza liczbę węzłów.

Liczba węzłów przyłączonych do węzła nadrzędnego jest nazywana *współczynnikiem rozgałęzienia* ( $f$ ). W niektórych sieciach zakłada się symetryczne rozgałęzianie. Wówczas współczynnik rozgałęzienia musi mieć wartość 2, gdyż wartość 1 oznaczałaby topologię liniową. Choć opisywana konfiguracja nazywa się drzewiastą, zazwyczaj jest prezentowana z węzłem początkowym umieszczonym na górze schematu. Przedstawia więc drzewo obrócone korzeniem do góry, co można zauważyć na rysunku 1.10.

### Rysunek 1.10.

## Sieć o topologii drzewiastej



Topologia ta jest stosowana w większości systemów plików, baz danych oraz usług katalogowych. Wynika to z faktu, że algorytmy wyszukiwania danych mogą znacznie efektywniej przeszukiwać tego typu strukturę niż struktury liniowe lub siatkowe.

Rozwiązanie to ma również pewną wadę. Narzut związany z transmisją danych między poziomami jest wzmacniany podczas podążania w górę hierarchii. Węzły na każdym niższym poziomie mają swój wkład w narzut związany z przetwarzaniem przesyłanych danych.

## Topologie hybrydowe

Wszystkie opisane powyżej topologie mogą być łączone ze sobą, co prowadzi do powstania topologii hybrydowych, charakteryzujących się większą złożonością, ale jednocześnie większą elastycznością niż rozwiązania bazujące na pojedynczej topologii. W rezultacie mogą powstać następujące topologie:

- ♦ **Gwiazda — magistrala.** Sieć tego typu łączy dwie sieci fizycznej gwiazdy lub większą ich liczbę za pomocą wspólnej magistrali. W praktyce oznacza to, że łącza sieciowe są zakończone dwoma lub większą liczbą koncentratorów, a port uplink każdego z koncentratorów jest połączony z kolejnym koncentrატorem w celu utworzenia fizycznej gwiazdy. Każdy z portów uplink jest wówczas połączony z punktem centralnym gwiazdy za pomocą kabla odgałęziającego (ang. *drop cable*).
- ♦ **Hierarchiczna gwiazda.** W sieci tego typu każdy z węzłów w drzewie stanowi koncentrator, od którego wyprowadzane są gwieździste rozgałęzienia. Na każdym kolejnym poziomie hierarchii znajduje się koncentrator gwiazdy. Nie istnieje wspólna magistrala łącząca poszczególne gwiazdy z wykorzystaniem połączeń punkt-punkt. Niekiedy węzeł nadrzędny jest przyłączony do wysokowydajnego połączenia szkieletowego (łącza trunkowego), który jest kolejnym elementem hybrydowym w tej konfiguracji.

- ♦ **Gwiazda — pierścień.** W sieci tego typu występuje centralny koncentrator, który przekazuje informacje kolejno do wszystkich rozgałęzień wychodzących z punktu wspólnego, symulując pierścieniowy fragment sieci. Połączenia między elementem centralnym a poszczególnymi węzłami mają charakter komunikacji punkt-punkt.
- ♦ **Hybrydowa siatka.** Sieci tego typu stanowią połączenie topologii siatkowej z węzłami pracującymi w innych topologiach. Rozwiązanie to charakteryzuje się dużą nadmiarowością i odpornością na błędy, dlatego jest często stosowane w praktyce. W internecie wykorzystuje się właśnie częściowo połączoną hybrydową siatkę.

## Topologie logiczne

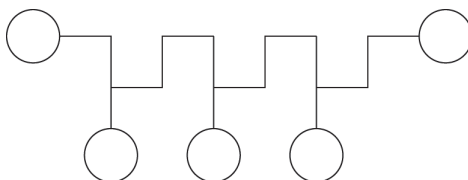
Topologie logiczne stanowią odwzorowanie tras, którymi dane są przekazywane między poszczególnymi węzłami. W topologii logicznej każdy węzeł musi być osiągalny z użyciem protokołu stosowanego do wymiany danych. Z kolei aby urządzenie było osiągalne musi mieć przypisany niepowtarzalny numer, nazywany *adresem MAC*. Termin „adres MAC” pochodzi od angielskich słów opisujących mechanizm kontroli dostępu do medium (ang. *Media Access Control*), który jest stosowany w celu wyróżniania węzłów w sieci.

Adresy MAC mogą być przypisywane także wirtualnym interfejsom sieciowym. Stosowanie inteligentnych routerów i przełączników pozwala na przykład na dynamiczną zmianę logicznej topologii sieci w zależności od różnych czynników zewnętrznych. Do typowych topologii logicznych zalicza się logiczny łańcuch, logiczną gwiazdę oraz logiczną siatkę. Każde z tych rozwiązań zostało opisane w kolejnych punktach.

### Topologia logicznego łańcucha

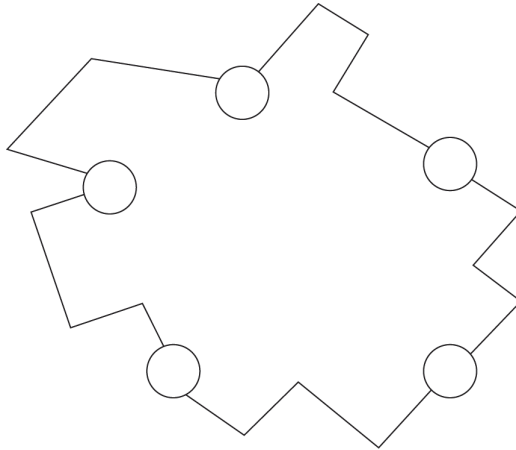
Topologia logicznego łańcucha jest konfiguracją, która może zostać zaimplementowana w formie liniowej lub pierścieniowej topologii fizycznej, jak zostało pokazane na rysunkach 1.11 i 1.12. Przy dodawaniu nowego systemu do łańcucha konieczne jest utworzenie dwukierunkowych połączeń między wstawianym systemem a jego sąsiadami. System znajdujący się pomiędzy innymi węzłami musi dysponować jednym odbiornikiem i jednym nadajnikiem w ramach każdego połączenia z systemem sąsiednim. Jednostka znajdująca się na końcu łańcucha powinna być wyposażona w tylko jeden odbiornik i jeden nadajnik. W przypadku łańcucha połączonych w pierścień dane są przekazywane w jednym kierunku dookoła pierścienia. Zatem każde z urządzeń musi być wyposażone tylko w jeden nadajnik i jeden odbiornik. Topologie pierścieniowe charakteryzują się większymi opóźnieniami, ponieważ dostarczenie danych może zająć dwa razy więcej czasu w porównaniu z topologią liniową. Ich zaletą jest jednak niższy koszt implementacji.

**Rysunek 1.11.**  
Sieć o topologii  
liniowego łańcucha



**Rysunek 1.12.**

*Sieć o topologii łańcucha połączona w pierścień. Dane mogą być przekazywane zgodnie z kierunkiem ruchu wskazówek zegara lub przeciwnie, a łącza pracują jednokierunkowo (w trybie simpleksu)*

**Topologia logicznej gwiazdy**

Sieci gwiazdowe są rozważane zarówno jako topologie fizyczne, jak i topologie logiczne. W logicznej sieci gwiazdowej, jaką jest Ethernet, węzeł centralny rozsyła rozgłoszeniowo sygnał otrzymany z dowolnego z węzłów do wszystkich pozostałych węzłów sieci. Gdy odbiór sygnału zostanie potwierdzony, rozpoczyna się transmisja danych. Sieci o logicznej topologii gwiazdy ulegają awarii, gdy przestanie działać węzeł centralny. Jednak uszkodzenie któregośkolwiek z połączeń punkt-punkt wpływa jedynie na działanie węzła podłączonego do punktu wspólnego.

Sieci gwiazdowe można podzielić na pasywne i aktywne. W pasywnej sieci gwiazdowej węzeł nadawczy musi mieć możliwość rozpoznania własnego sygnału zwracanego z węzła centralnego. W sieciach aktywnych węzeł centralny jest wyposażony w obwód elektroniczny, który uniemożliwia retransmisję sygnału do systemu nadawczego. Typowymi urządzeniami funkcjonującymi w sieciach gwiazdowych są przełączniki, które budują tabelę powiązań między systemami docelowymi i portami, które są wykorzystywane w przekazywaniu danych. Gdy tabela zostanie zapełniona, odgrywa rolę tablicy tras, na których podstawie przełącznik może dostarczać dane bezpośrednio do jednostek docelowych.

Połączenie kilku logicznych gwiazd w sposób hierarchiczny prowadzi do powstania topologii drzewiastej. Koncentratory w logicznej gwiazdzie zazwyczaj powielają lub regenerują przesyłane przez sieć dane. W sieciach tego typu często obciążenie jest rozkładane między różne koncentratory. Każdy węzeł gwiazdy ustanawia pojedyncze połączenie typu punkt-punkt z innym węzłem. Dlatego w razie uszkodzenia koncentratora cały liść drzewa staje się niedostępny. Jednak w przypadku awarii pojedynczego połączenia punkt-punkt niedostępny staje się tylko jeden węzeł.

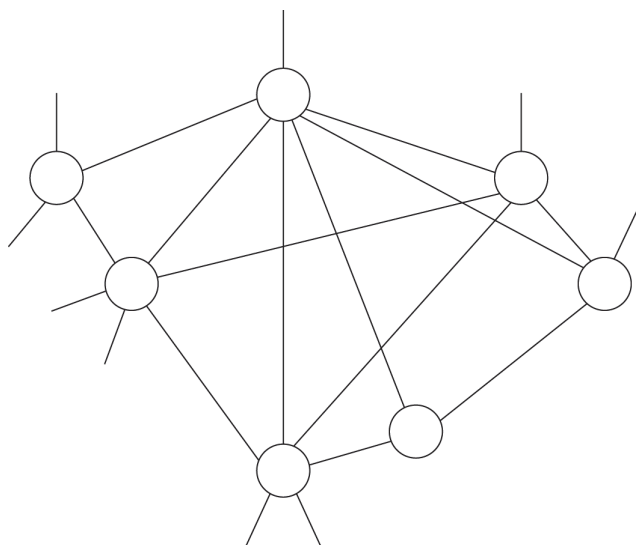
Logiczne topologie gwiazdy mogą przyjmować również formy hybrydowe. Dwie typowe konfiguracje hybrydowe tego typu to gwiazda-pierścień oraz gwiazda-magistrala.

## Topologia logicznej siatki

Topologia logicznej siatki jest jedyną, w której występują dodatkowe trasy między parami węzłów. Jej przykład został przedstawiony na rysunku 1.13. Istnieje wiele rozwiązań bazujących na logicznej siatce. Jednym z nich jest sieć siatkowa o znacznym rozproszeniu utworzona na podstawie topologii liniowej lub pierścieniowej, nazywana siecią kratową (ang. *grid network*). Sieci siatkowe można również konstruować na bazie topologii toroidalnej lub wielokrotnego pierścienia, a także z wykorzystaniem hipersześcianów.

### Rysunek 1.13.

*Sieć kratowa jako przykład topologii logicznej siatki*



Podobnie jak topologia fizyczna siatki, topologia logicznej siatki może być w pełni połączona lub częściowo połączona. Częściowo połączona sieć siatkowa w praktyce jest znacznie częściej stosowana niż sieć w pełni połączona z uwagi na wysoki koszt utworzenia wszystkich połączeń. Sieci w pełni połączone są wykorzystywane wówczas, gdy niezbędna jest wysoka niezawodność i konieczne jest utworzenie nadmiarowych połączeń. Niemniej istnieje jedna często wykorzystywana w pełni połączona sieć *ad hoc*. Jest to system wymiany plików BitTorrent. Połączenia w tej sieci są ustanawiane tylko na czas przesyłania części pliku.

## Podsumowanie

W tym rozdziale zostały opisane różne rodzaje sieci oraz zasady ich klasyfikowania. Z przedstawionych informacji wynika, że na podstawie obejmowanego obszaru geograficznego można podzielić sieci na osobiste, lokalne, rozległe, kampusowe oraz metropolitarne. W każdej z nich wykorzystywane są specjalnie zaprojektowane przemysłowe protokoły, które są dostosowane do określonego rodzaju sieci oraz urządzeń w niej funkcjonujących.

Sieci można również opisać na podstawie ich kształtu, czyli topologii. Typowe topologie sieciowe to: magistrała lub łańcuch, gwiazda, pierścień i siatka. Ponadto wyróżnia się kilka topologii hybrydowych, które są połączeniem innych rozwiązań. Analizując sieć, można wyznaczyć jej topologię na podstawie fizycznych elementów, logicznych elementów lub sposobu przekazywania sygnału przez sieć.

# Rozdział 2.

# Stos protokołów sieciowych

## W tym rozdziale:

- ♦ Jak powstają standardy
- ♦ Omówienie organizacji standaryzujących
- ♦ Model odniesienia OSI
- ♦ Wykorzystanie stosu protokołów w analizie produktów i usług
- ♦ Omówienie każdej warstwy modelu OSI i jej aplikacji
- ♦ Interfejsy, usługi i protokoły
- ♦ Gdzie model OSI nie znajduje zastosowania
- ♦ Model odniesienia TCP/IP
- ♦ Porównanie modeli OSI i TPC/IP

Stos protokołów sieciowych jest odwzorowaniem architektonicznego modelu, który jest wykorzystywany do opisywania transakcji sieciowych zainicjowanych w jednym komputerze i kończących się w innym. Modele zostały opracowane w celu standaryzacji urządzeń i usług oraz aby umożliwić rozwój standardów przemysłowych zapewniających komunikację między różnymi warstwami sieci.

W tym rozdziale zostały opisane dwa najważniejsze modele sieciowe wykorzystywane obecnie — opracowany w ramach organizacji ISO model połączeń systemów otwartych (OSI — *Open System Interconnection*) oraz model internetowy, nazywany również modelem TCP/IP. Każdy z wymienionych modeli wprowadza do urządzeń, usług i oprogramowania podział na kilka warstw architektonicznych. Związane z nimi definicje i zależności umożliwiają kategoryzowanie i analizowanie nowoczesnych technologii sieciowych. Stosowana w tym rozdziale terminologia jest wykorzystywana w dalszej części książki.

## Organizacje opracowujące standardy

Po opracowaniu standardów komunikacji sieciowej w latach 70. i 80. ubiegłego stulecia producenci rozwiązań komputerowych stanęli w obliczu problemu zapewnienia zgodności produktów przygotowywanych przez różnych dostawców. Twórcy systemów operacyjnych, tacy jak Microsoft, zdołali utworzyć tzw. de facto standardy, czego przykładem jest system Windows. Jednak wśród producentów sprzętu i oprogramowania sieciowego nie było jednego dominującego podmiotu. Standardy mogły powstawać jedynie dzięki porozumieniu przedstawicieli przemysłu i nauki. Gdy pojawiła się nowa technologia — Ethernet — różne grupy dostawców przygotowały niezależne zestawy standardów, które umożliwiały komunikację z użyciem sieci pakietowych.

Zespoły standaryzujące są zazwyczaj powoływane przez organizacje standaryzacyjne, które zarządzają pracą nad wieloma różnymi grupami standardów. Niekiedy są one również wyłaniane spośród przedstawicieli przemysłu i mają wówczas tylko jeden cel — opracowanie standardu dla jednej technologii lub zbioru powiązanych ze sobą technologii. Przykładem organizacji standaryzacyjnej może być ANSI (American National Standards Institute).

Niezależnie od sposobu powołania zespołu ds. standaryzacji prace nad standardem są pewnym procesem, im bardziej otwartym, tym lepiej. Proces standaryzowania technologii składa się z kilku etapów. Oto one:

1. **Powołanie grupy** reprezentantów przemysłu.
2. **Prośba o propozycje** (RFP — *Request For Proposal*) standardu, zarys proponowanego standardu lub przegląd zaproponowanego standardu.
3. **Prośba o komentarze** (RFC — *Request For Comments*) do standardu zaproponowanego przez zespół.
4. **Testowanie i modyfikacje.** W celu sprawdzenia zgodności z innymi technologiami organizowane są sesje plugfest. Plugfest jest spotkaniem przedstawicieli przemysłu, na którym dostawcy produktu testują sprzęt lub oprogramowanie z producentami innych komponentów w celu zapewnienia współdziałania rozwiązań i zaakceptowania nowych standardów.
5. **Opracowanie wstępnej wersji standardu**, który nie został jeszcze całkowicie dopracowany.
6. **Akceptacja standardu**, czyli wydanie ostatecznej wersji określonego standardu. Każdy standard może być rozbudowywany w czasie przez dodawanie kolejnych wersji. Doskonałym przykładem są tutaj standardy 802.11x (WiFi), które obejmują wersje a, b, g i n.

Biorąc pod uwagę czas i nakład pracy włożony w opracowanie standardu, a także środki finansowe wymagane do jego wdrożenia, nie należy się dziwić, że opracowywanie standardów bywa źródłem wielu kontrowersji. Wiele z propozycji nigdy nie przeszło etapu wstępnej prezentacji. Nietrudno sobie wyobrazić, ile wysiłku wymagało opracowanie standardów zapisu video Betamax i VHS albo niedawno HD DVD i Blu-ray, z których przetrwał tylko jeden z pary. Nie bez znaczenia jest więc siła przebicia określonej organizacji, która niekiedy może nawet zaważyć na odrzuceniu lepszej technologii.

W branży sieci komputerowych najważniejsze są następujące organizacje standaryzacyjne:

- ♦ **American National Standard Institute (ANSI, [www.ansi.org](http://www.ansi.org))**. ANSI jest organizacją non profit, która opracowuje standardy produktów i usług.
- ♦ **Międzynarodowa Organizacja Normalizacyjna (ISO, [www.iso.org](http://www.iso.org))**. Standardy ISO są wykorzystywane w różnych aspektach transmisji danych, włączając w to standardy i model opisywane w niniejszym rozdziale.
- ♦ **Międzynarodowa Unia Telekomunikacyjna — Grupa ds. Telekomunikacji (ITU-T, [www.itu.int](http://www.itu.int)), Grupa ds. Radiokomunikacji (ITU-R), Grupa Rozwoju Telefonii (ITU-T)**. Członkiem ITU jest między innymi organizacja ISO. Każda z grup opracowuje standardy komunikacyjne.
- ♦ **Internet Engineering Task Force (IETF, [www.ietf.org](http://www.ietf.org))**. IETF opracowuje standardy internetowe i wchodzi w skład grupy odpowiedzialnej za definiowanie protokołów internetowych, w tym TCP/IP.
- ♦ **Institute of Electrical and Electronics Engineers (IEEE, [www.ieee.org](http://www.ieee.org))**. IEEE (czytaj „aj tripyl i”) jest jednym z głównych organów standaryzujących komunikację przewodową i radiową.
- ♦ **Storage Networking Industry Association (SNIA, [www.snia.org](http://www.snia.org))**. SNIA definiuje standardy związane z sieciami pamięci masowych, na przykład Fiber Channel, Ethernet dużych prędkości czy iSCSI.
- ♦ **World Wide Web Consortium (W3C, [www.w3.org](http://www.w3.org))**. W3C jest najważniejszym organem standaryzacji technologii WWW. Definiuje format HTML oraz związane z nim rozwiązania, a także protokoły wykorzystywane przez serwery WWW.



Więcej informacji na temat pracy organizacji standaryzacyjnych oraz bogatsza ich lista znajduje się pod adresem [http://en.wikipedia.org/wiki/Standards\\_organizations](http://en.wikipedia.org/wiki/Standards_organizations).

## Model odniesienia OSI

Najpowszechniej wykorzystywanym obecnie sieciowym modelem odniesienia jest bez wątpienia model łączenia systemów otwartych (OSI — *Open System Interconnection*). Wprowadza on podział komunikacji sieciowej na siedem niezależnych warstw i opisuje sposób działania każdej warstwy w procesie przekazywania danych. Każda z warstw dodaje pewne informacje do danych użytkowych podczas wysyłania tych danych oraz usuwa określone informacje podczas odbierania danych. Dokumentacja modelu OSI jest dostępna na stronie ITU-T w sekcji X.200 pod adresem <http://www.itu.int/rec/T-REC-X/en>.

W modelu OSI wyróżniono siedem warstw o numerach od 1 do 7 w następującej kolejności: fizyczna, łącza danych, sieciowa, transportowa, sesji, prezentacji i aplikacji. Pierwsze cztery warstwy odnoszą się do sprzętu. Natomiast trzy ostatnie są związane z oprogramowaniem.

Definicje wszystkich siedmiu warstw zostały zamieszczone w tabeli 2.1.

**Tabela 2.1.** *Warstwy modelu OSI*

Warstwa	Rodzaj ruchu	Funkcja
Aplikacji	Dane	Warstwa aplikacji zarządza połączeniem sieciowym na styku aplikacji i sieci.
Prezentacji	Dane	W warstwie prezentacji dane są przekształcane na format właściwy do przetwarzania w systemie odbiorczym.
Sesji	Dane	Warstwa sesji tworzy dedykowane połączenie między systemem nadawczym i odbiorczym oraz zapewnia poprawne przekazanie informacji.
Transportowa	Segmenty lub datagramy	Warstwa transportowa zarządza przepływem danych między systemem nadawczym i odbiorczym.
Sieciowa	Pakiety	Warstwa sieciowa zarządza adresowaniem w transmisji danych.
Łączy danych	Ramki	Warstwa łączy danych obsługuje adresy sprzętowe.
Fizyczna	Bity	W warstwie fizycznej definiowane jest medium transmisyjne — kabel, fale radiowe, fale świetlne lub inne metody przekazywania sygnału.

Bardzo rzadko jakakolwiek sieć wykorzystuje wszystkie siedem warstw jako swoją zasadniczą architekturę. Jednak model ten jest najczęściej stosowanym sposobem opisu różnych urządzeń oraz technologii sieciowych.

Do analizy sieci TCP/IP używa się również innego modelu, w którym wydzielono cztery warstwy odnoszące się do operacji realizowanych w sieciach pakietowych (jest to model TCP/IP). Większość nowoczesnych sieci składa się z urządzeń, które mogą być opisywane na podstawie modelu TCP/IP. Jednak model ten nie jest dostatecznie elastyczny, by można go stosować w odniesieniu do innych typów sieci. Jego szczegółowe omówienie znajduje się w dalszej części rozdziału.

## Komunikacja między warstwami

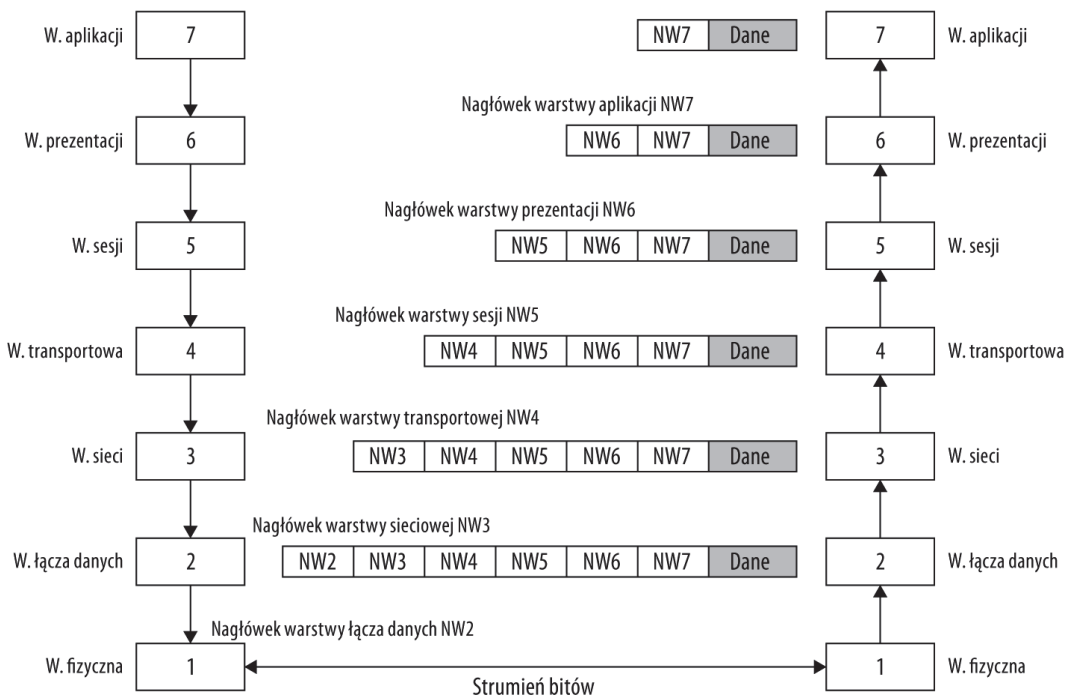
Każda wymiana danych między dwoma systemami wymaga przekazania informacji od warstwy aplikacji do warstwy fizycznej systemu nadawczego oraz od warstwy fizycznej do warstwy aplikacji systemu odbiorczego. O ile protokoły zastosowane na poziomie danej warstwy muszą być identyczne w obydwu urządzeniach końcowych, protokoły komunikacji międzywarstwowej nie są już definiowane i mogą być zmieniane.

Przekazywanie danych rozpoczyna się w warstwie aplikacji systemu nadawczego po wprowadzeniu przez użytkownika odpowiedniego polecenia lub po wystąpieniu określonego zdarzenia. Zdarzenie to jest interpretowane jako operacja wejścia-wyjścia (która ma za zadanie odczytać dane lub dostarczyć je do odległego urządzenia) i powoduje wygenerowanie danych, które zostają przekazane przez poszczególne warstwy stosu do warstwy fizycznej. Następnie informacje są przesyłane w warstwie fizycznej w ramach określonego połączenia i docierają do stosu protokołów systemu docelowego. Są wówczas przekazywane między kolejnymi warstwami w górę stosu i w końcu trafiają do warstwy aplikacji, gdzie podlegają przetwarzaniu.

Aby dane zostały dostarczone do odpowiedniego systemu lub kilku systemów, muszą być opatrzone dodatkowymi informacjami, opisującymi zasady postępowania z nimi. Informacje tego typu często określa się mianem *metadanych*, czyli „danych o danych”. Proces dołączania metadanych nazywa się *enkapsulacją*, natomiast usuwanie metadanych to *dekapsulacja*. Podczas przenoszenia informacji w dół stosu metadane są dodawane. Z kolei w trakcie propagowania informacji w górę są usuwane.

Na rysunku 2.1 można zauważyć, że proces enkapsulacji rozpoczyna się od formatowania i segmentacji danych, aby optymalnie dostosować ich rozmiar do transmisji. W każdej warstwie modelu OSI do bloku danych dołączany jest nagłówek określonej warstwy, który zawiera informacje niezbędne do prawidłowego funkcjonowania protokołu związanego z tą warstwą. Zatem kolejno dodawane są nagłówki warstw: aplikacji (NW7), prezentacji (NW6), sesji (NW5), transportowej (NW4), sieciowej (NW3), łącza danych (NW2). Każdy z nagłówków zawiera adresy, parametry i instrukcje opisujące sposób przetwarzania przekazywanych informacji. Do pakietu przekazanego do warstwy łącza danych dodawana jest stopka wyznaczająca koniec bloku danych. W stopce znajduje się również wartość kontrolna, która umożliwia sprawdzenie poprawności dostarczenia informacji za pośrednictwem warstwy fizycznej. W systemie docelowym blok danych jest odczytywany i na poziomie każdej warstwy modelu OSI usuwane są z niego nagłówki wraz z informacjami przeznaczonymi dla określonej warstwy.

### Enkapsulacja danych



**Rysunek 2.1.** Transport danych w ramach modelu OSI

Wszystkie odbierane dane są przetwarzane z wykorzystaniem algorytmów takich jak CRC. Algorytm CRC jest uruchamiany po odebraniu informacji (również w urządzeniach pośredniczących w przesyłaniu danych) w celu sprawdzenia, czy pakiet nie zawiera przekłamań. Jeśli wartość CRC wyliczona dla odebranych informacji zgadza się z wartością pola CRC w ramce, dane są uznawane za poprawne. CRC jest funkcją skrótu, generującą niepowtarzające się 32-bitowe wartości całkowitoliczbowe. Wykorzystuje się ją jako mechanizm walidacji danych poprzez porównanie jej wyników z wartościami zawartymi w samym bloku danych. Zmiana choćby jednego bitu wystarczy, aby zmieniła się również wartość kontrolna i by rozpoczęta została procedura retransmisji. Przekazywane dane mają charakter binarny, więc algorytm CRC działa bardzo wydajnie i nie wnosi istotnego narzutu do procedury przekazywania informacji. Obecnie w sieciach Ethernet stosowany jest standard CRC-32, bez którego jakakolwiek komunikacja nie byłaby wystarczająco wiarygodna.

Jak wiadomo, model OSI składa się z siedmiu warstw; każda ma określoną funkcję i odpowiada innej technologii sieciowej. Jednak w praktyce bardzo rzadko zdarza się, że ktoś korzysta z sieci złożonej z siedmiu różnych warstw — odpowiadających różnym technologiom (choć takie sieci rzeczywiście istnieją). Efekt skali oraz czynniki takie jak koszt sprawiły, że produkowane urządzenia obejmują dwie warstwy lub większą ich liczbę. Poza tym należy pamiętać, że istnieją również inne sieciowe modele odniesienia, w którym wyróżniono mniejszą liczbę warstw w stosie protokołów. Jednym z alternatywnych jest stos czterowarstwowy.



W tabeli na stronie [http://en.wikipedia.org/wiki/Internet\\_Protocol\\_Suite](http://en.wikipedia.org/wiki/Internet_Protocol_Suite) zostały przedstawione różne sposoby podziału stosu protokołów sieciowych.

W praktyce urządzenia sieciowe i protokoły funkcjonują w różnych warstwach w różnych modelach sieciowych. Doskonałym przykładem jest tutaj router Cisco, który obejmuje kilka warstw modelu OSI. Pierwsze routery miały charakter programowy i były tworzone na bazie systemów operacyjnych takich jak Unix lub Solaris. Jednak firma Cisco przekształciła routery w niezależne urządzenia, zwiększając ich wydajność, dzięki czemu zdominowała rynek tych urządzeń. Routery Cisco obejmują zarówno warstwę sieciową, jak i transportową. Nie zmienia to faktu, że model odniesienia można traktować jako sposób na opisanie komunikacji sieciowej i wyróżnienie urządzeń pełniących poszczególne funkcje. Stanowi on również podstawę do opracowywania innych modeli definiujących ruch w internecie, sieciach SAN itp.

Definicji modelu OSI nie należy brać zbyt dosłownie. Oczywiście uwzględniła ona kryteria umożliwiające sklasyfikowanie produktów poszczególnych dostawców, co zresztą czyni ten model tak użytecznym. Jednak prawdziwa wartość modelu OSI wynika z tego, że pozwala on zrozumieć zasady komunikowania się różnych komponentów sieciowych. Każda warstwa modelu opisuje protokół lub zestaw protokołów. Dlatego sam model często jest nazywany stosiem protokołów. Na granicy każdej pary warstw zdefiniowane są pewne pionowe zależności, które wymagają opracowania wspólnego interfejsu programistycznego (API — *Application Programming Interface*), zapewniającego komunikację między dwiema warstwami. Pionowa zależność między warstwami 4. i 5. będzie nazywana interfejsem warstw 4 – 5. Samo zastosowanie słowa *interfejs* oznacza bowiem konieczność wprowadzenia pewnego mechanizmu komunikacji, bazującego na kodzie API.

Z kolei poziome zależności, nazywane *protokołami warstwy n*, odnoszą się do komunikacji między dwoma równorzędnymi warstwami. Zazwyczaj nie wymagają one opracowywania wspólnego interfejsu API. Zależności te są poziome tylko wtedy, gdy dwa procesy działające

w ramach jednego systemu jednocześnie korzystają z tej samej warstwy (przykładem mogą być aplikacje pocztowe). Gdy różne urządzenia lub procesy w różnych urządzeniach korzystają z tej samej warstwy, również tworzą poziomą zależność między warstwami, ale jakakolwiek komunikacja między nimi wymaga przekazania danych przez obydwa stosy protokołów.

Gdy dane są przekazywane w stosie protokołów, ich transport odbywa się w ramach kanałów komunikacyjnych (nazwanych połączeń). W niektórych technologiach wykorzystuje się pojedyncze potoki, podobne do jednokierunkowych dróg; w potokach tych informacje przepływają tylko w jednym kierunku. Komunikację tego typu określa się mianem komunikacji *simpleksowej*. Można również zastosować pojedyncze połączenie do przekazywania informacji w jednym i w drugim kierunku naprzemiennie. Mamy wówczas do czynienia z przesyłaniem danych w trybie *półdupleksowym*. Gdy informacje są przesyłane jednocześnie w dwóch kierunkach, komunikacja jest realizowana w trybie *pełnego duplexu*. Pełny duplex wymaga zagwarantowania kanału o dostatecznej przepustowości, by dane mogły podróżować w dwóch kierunkach, lub zastosowania kilku kanałów. Sposób komunikacji jest wyznaczany przez sprzęt lub oprogramowanie i nie wynika z definicji modelu OSI.

Każda warstwa w modelu OSI zawiera jeden lub większą liczbę elementów aktywnych, które niekiedy określa się mianem *encji*. Encją może być moduł oprogramowania lub blok funkcjonalny urządzenia odpowiedzialny za określone operacje sieciowe. Encja lub zbiór encji komunikujących się z warstwą wyższą wyznacza *dostawcę usługi*. Z kolei encja, która korzysta z usługi, jest nazywana *użytkownikiem usługi*. Adres wykorzystywany do odwołania się do dostawcy usługi wskazuje na *punkt dostępu do usługi* (SAP — *Service Access Point*). Gdy dwie encje nawiążą komunikację za pośrednictwem interfejsu i z wykorzystaniem SAP, przekazują przez SAP dane, które nazywa się jednostką danych interfejsu (IDU — *Interface Data Unit*). W skład IDU wchodzi jednostka danych usługi (SDU — *Service Data Unit*), informacje sterujące oraz przekazywane dane.

Niektóre warstwy wymagają segmentowania informacji przed ich przetworzeniem. W takim przypadku każda porcja danych otrzymuje nagłówek i jest transmitowana jako niezależna jednostka, nazywana *jednostką danych protokołu* (PDU — *Protocol Data Unit*). Przykładem stosowania jednostek PDU jest wydzielanie pakietów podczas transmisji danych oraz odtwarzanie na podstawie tych pakietów pierwotnego bloku informacji podczas odbierania, weryfikowania i kolejkowania danych.

Usługi opisują mechanizm komunikacji między poszczególnymi warstwami w modelu OSI. Realizują określone zadania i często są udostępniane za pośrednictwem interfejsu API. Ich działanie może mieć charakter połączeniowy lub bezpołączeniowy. Zgodnie z założeniami modelu połączeniowego po ustanowieniu połączenia, połączenie to jest przeznaczone dla określonej usługi. Doskonałym przykładem usługi połączeniowej jest sieć telefoniczna. Usługa ustanawia połączenie, wyznaczając obwód do komunikacji. Po zakończeniu rozmowy obwód ulega rozłączeniu i staje się dostępny do ponownego użycia. Model połączeniowy ma wiele zalet, szczególnie w zakresie niezawodności połączeń i gwarantowania określonej jakości obsługi. Jednak z drugiej strony zerwanie połączenia powoduje natychmiastowe zakończenie transmisji, co stanowi wadę tego rozwiązania. Nie jest ono odporne na awarie i nie zapewnia nadmiarowości połączeń.

Alternatywny — bezpołączeniowy — model usługi został wykorzystany w warstwie fizycznej internetu oraz w modelu TCP/IP. Komunikacja bazuje na niezależnym adresowaniu każdej porcji danych. Trasa do urządzenia docelowego nie musi być z góry określona

i może przebiegać w różny sposób w zależności od bieżących uwarunkowań. Usługi bezpołączeniowe cechują się wysoką odpornością na awarie, ale jednocześnie obniżają wydajność komunikacji z uwagi na istnienie dodatkowego narzutu transmisyjnego w porównaniu z usługami połączeniowymi.

Każda forma komunikacji bazuje na wykorzystaniu pewnych podstawowych poleceń, które inicjują oraz nadzorują połączenie. Usługi połączeniowe rozpoczynają swoje działania od procedury *negocjacji*. Służy ona do ustalenia parametrów połączenia. Piski wydane przez modem w trakcie nawiązywania połączenia są właśnie sposobem na przekazanie informacji o parametrach łącza. Poniżej zostały wymienione podstawowe polecenia (prymitywy usługi), które są stosowane w procesie negocjacji.

- ♦ **Inicjacja (żądanie połączenia).** Jest to forma zachęcenia usługi do wykonania określonego zadania.
- ♦ **Raport o stanie połączenia.** Jest to zdarzenie o charakterze informacyjnym, które dostarcza danych na temat stanu modułu oprogramowania lub aktywności jednostki realizującej usługę.
- ♦ **Odpowiedź.** Dostawca usługi odsyła komunikat stanowiący odpowiedź na dostarczone żądanie.
- ♦ **Potwierdzenie.** Wynik komunikacji jest przekazywany do jednostki inicjującej wymianę danych. W niektórych rodzajach usług potwierdzenia nie są stosowane.

Trzeba pamiętać, że proces negocjacji jest realizowany w dwóch różnych systemach. Z tego względu oprócz wykorzystania interfejsu między dwoma różnymi warstwami modelu każde polecenie sterujące musi zostać przekazane w górę lub w dół między dwoma warstwami jednego systemu, a następnie musi zostać wygenerowana odpowiedź na nie w tych samych dwóch warstwach zdalnego systemu. Dlatego usługa jest wyznaczana przez operacje (prymitywy instrukcji) oraz przez dwie warstwy, które ze sobą łączy.

Usługi nie definiują sposobu praktycznej implementacji poszczególnych operacji. Jest to domena protokołów. Protokół z kolei stanowi zbiór ustalonych reguł formatowania danych, na których podstawie encje poszczególnych warstw mogą zrealizować usługę. Oddzielenie zbioru instrukcji od implementacji umożliwia stosowanie różnych protokołów (opracowywanych przez różnych dostawców sprzętu), różnych rodzajów sieci i innych rozwiązań, które wpływają na wydajność komunikacji.

## Warstwa fizyczna

Warstwa fizyczna jest najniższą warstwą modelu OSI oraz innych modeli o podobnym znaczeniu. Jej zadanie polega na przenoszeniu bitów danych z jednego urządzenia do innego. W definiowaniu parametrów warstwy fizycznej urządzeń najważniejsze jest określenie sposobu reprezentacji logicznych wartości 1 i 0 oraz czas trwania bitu (czas podtrzymania stanu przed wygenerowaniem kolejnego bitu). Opracowując urządzenie warstwy fizycznej, należy określić, w jaki sposób będzie realizowane elektryczne połączenie, jak różne urządzenia będą podłączane do siebie nawzajem, a także opracować mechaniczne aspekty przyłączy.

Najpowszechniej wykorzystywanym medium transmisyjnym warstwy fizycznej są:

- ♦ Przewody miedziane, czyli różne kategorie kabli ethernetowych (produkowanych zgodnie ze specyfikacjami CAT5 lub CAT6), pojedyncze pary skręconych przewodów stosowane w liniach telefonicznych lub w sieciach o mniejszym zasięgu, takich jak Apple Talk firmy Apple lub inne.
- ♦ Włókna światłowodowe, w których przekazywane jest światło.
- ♦ Fale radiowe o różnym zakresie częstotliwości, w tym rozwiązania WiFi 802.11, mikrofalowe i inne.

Warstwa fizyczna obejmuje również urządzenia, które zapewniają przyłączenie do medium transmisyjnego, na przykład karty komputerowe, modemy, koncentratory itp.

## Warstwa łączy danych

Warstwa łączy danych uczestniczy w przekazywaniu danych formowanych w bity na poziomie warstwy fizycznej, ale posługuje się połączeniami, które wyznaczają trasę do systemu nadawczego lub z systemu odbiorczego. Zapewnia mechanizmy kontrolne odpowiedzialne za wybór odpowiedniej trasy. Podobnie jak w przypadku warstwy fizycznej, warstwa łączy danych występuje nie tylko w modelu OSI, ale również w innych podobnych modelach, na przykład w modelu wykorzystywanym do opisu ruchu internetowego.

Sterowanie przepływem danych wymaga tego, aby w warstwie łączy danych komunikaty były formatowane w sposób umożliwiający wyznaczenie początku i końca wiadomości. W tym celu informacje są dzielone na porcje danych, nazywane ramkami. Każda z ramek przenosi fragment komunikatu lub segmentu o rozmiarze od kilkuset do kilku tysięcy bajtów, w zależności od zastosowanej technologii oraz parametrów zdefiniowanych przez użytkownika (na przykład w celu zwiększenia wydajności lub niezawodności). W łączach o dużej przepustowości zazwyczaj stosuje się ramki o dużych rozmiarach. Natomiast w łączach o niskiej przepustowości lub o dużej zawodności wykorzystywane są niewielkie ramki.

Proces segmentacji danych przeznaczonych do transmisji w ramach polega na przygotowaniu sekwencji ramek podczas nadawania, które w warstwie łączy danych urządzenia docelowego muszą zostać odtworzone w początkowy blok danych. W implementacji warstwy łączy danych musi być również uwzględniony fakt, że dane mogą zostać przekłamate podczas transmisji, a poszczególne ramki niekiedy docierają do jednostki docelowej zduplikowane. Rozwiązanie tego problemu polega na odsyłaniu potwierdzeń, dzięki którym urządzenie nadawcze uzyskuje informacje o tym, które ramki zostały poprawnie odebrane. Mechanizmy detekcji i korekty błędów są również elementami warstwy łączy danych. Dane bywają przekłamate z wielu różnych powodów. Na przykład w wyniku zakłóceń występujących w medium transmisyjnym, błędów transmisyjnych lub utraty danych. Gdy warstwa łączy danych wykryje błąd, wysyła do nadawcy komunikat o konieczności retransmisji określonego bloku. Tego typu mechanizmy nie są zaimplementowane we wszystkich protokołach tej warstwy. Dla łączy o niewielkiej liczbie błędów są one pomijane, ewentualną detekcją i korektą błędów zajmują się warstwy wyższe.

Jedną z funkcji warstwy łącza danych jest zarządzanie szybkością transmisji danych. Zbyt duża szybkość powoduje utratę danych i konieczność ich retransmitowania. Z kolei zbyt mała szybkość powoduje marnowanie cennego pasma i sprawia, że połączenie nie jest optymalne. Część protokołów warstwy drugiej ma zaimplementowane mechanizmy regulowania szybkości. Na przykład w Frame Relay system regulowania szybkości transmisji bazuje na wykorzystaniu buforów, w których przechowywane są ramki po ich odebraniu. Bufor ramek jest pewnym obszarem pamięci przeznaczonym wyłącznie do gromadzenia odbieranych ramek. Aby wprowadzanie ramek do bufora i wyprowadzanie ich z bufora było wydajne, zaimplementowano mechanizm sterowania przepływem danych i korekcji błędów. Ramki potwierżeń zawierają informację o bieżącym stanie bufora ramek. Ponieważ ramki potwierżeń są przekazywane w obrębie tego samego fizycznego połączenia, w którym podróżują ramki danych, jedną z form optymalizacji połączenia jest przesyłanie danych sterujących do systemu nadawczego „na doczepkę” do potwierżeń. W każdym rozgłoszeniowym systemie komunikacji sieciowej (takim jak transmisja TCP/IP w sieci Ethernet) warstwa łącza danych reguluje dostęp do współdzielonego medium w ramach jednej ze swoich podwarstw. Współdzielony kanał wymiany danych jest trasą przez sieć, która jest wykorzystywana jednocześnie przez dwa lub większą liczbę systemów nadawczych i odbiorczych.

## Warstwa sieciowa

Warstwa sieciowa odpowiada za routing oraz funkcje kontrolne, które zapewniają wybór trasy pakietów podczas przekazywania ich między sieciami, a także steruje przepływem danych w taki sposób, aby dana podsieć nie została zalana zbyt dużą liczbą pakietów w jednostce czasu. Komunikacja na poziomie warstwy sieciowej jest opisywana jako *sesja*, a logika zarządzania sesją wynika ze specyfiki trasy wyznaczonej przez funkcję routingu.

Routing odgrywa bardzo ważną rolę w sieciach przełączanych, ponieważ obejmuje rozwiązania, dzięki którym ruch sieciowy dostosowuje się do dynamicznych zmian w samej sieci. Jeżeli router nie odbierze żądania potwierdzenia obecności w sieci od drugiego routera, może wyznaczyć inną trasę do zdalnej sieci. Routery przechowują informacje o połączeniach i trasach w tablicy routingu, które są tworzone w sposób statyczny lub dynamiczny. W sieciach o niewielkim zasięgu, w których adresy zmieniają się rzadko, oraz w sieciach rozległych, w których istnieją połączenia o dużej przepustowości i niezmiennych adresach, korzystniejsze wydaje się stosowanie statycznych tablic routingu. Jednak w przypadku dużych sieci routing dynamiczny jest lepszym rozwiązaniem niż routing statyczny.

Sposób formatowania danych w poszczególnych sieciach lub podsieciach bywa różny. Problem ten często występuje podczas przekazywania informacji przez granice międzynarodowe. Granica może bowiem wymusić zmianę adresów, a także szybkość transmisji lub rodzaj protokołu stosowanego do przesyłania danych. Niektóre sieci wymagają dostarczania pakietów wraz z informacjami, które umożliwią śledzenie ramek przekazywanych przez urządzenia pośrednie w celu wygenerowania zestawienia bilingowego. Warstwa sieciowa uwzględnia rozwiązania, które eliminują wymienione niezgodności.

Warstwa sieciowa występuje zarówno w modelu OSI, jak i w modelu internetowym. Jednak w przypadku ruchu rozgłoszeniowego, w którym dane są przekazywane do wszystkich systemów (umożliwiających dostarczanie tego typu danych), komunikacja nie wymaga wykonywania większości funkcji oferowanych przez warstwę sieciową. Dlatego w systemach rozgłoszeniowych warstwa sieciowa ma znikome znaczenie lub jest całkowicie pomijana.

## Warstwa transportowa

Warstwa transportowa łączy warstwę sieciową znajdującą się poniżej niej z warstwą sesji zdefiniowaną powyżej. Zadanie warstwy transportowej polega na segmentowaniu danych otrzymanych z warstwy sesji i przekazywanie bloków o odpowiednim rozmiarze i formacie do warstwy sieciowej. Podczas odbierania danych z warstwy sieciowej warstwa transportowa odpowiada za kontrolowanie poprawnego dostarczania pakietów, zarządzanie danymi sesji oraz potwierdzanie (za pomocą polecenia ACK) odbioru informacji. Warstwa transportowa obsługuje komunikację w charakterze połączeniowym i bezpołączeniowym.

Warstwa transportowa zarządza połączeniem między dwoma sąsiednimi warstwami — warstwą sesji i warstwą sieci. Gdy jest to konieczne, może tworzyć i zarządzać wieloma połączeniami sieciowymi skojarzonymi z odpowiednimi połączeniami transportowymi. Ponieważ utrzymuje połączenia między warstwami sesji i sieciową (i zarządza tymi połączeniami), oddziela wyższe warstwy stosu protokołów implementowanych programowo od niższych warstw stosu, realizowanych sprzętowo. W czasie wymiany informacji warstwa transportowa odpowiada za zarządzanie multipleksowanymi strumieniami oraz za tworzenie i kończenie połączeń na żądanie. Ta funkcja jest elementem mechanizmu sterowania przepływem danych.

Połączenia warstwy transportowej stanowią jedyne bezpośrednie połączenia między dwoma stosami protokołów biorących udział w komunikacji. Pozostałe warstwy stosu protokołów działają niezależnie od ich odpowiedników w stosie jednostki zdalnej. Warstwy transportowe w systemie nadawczym i odbiorczym komunikują się bezpośrednio ze sobą za pomocą nagłówków i komunikatów sterujących. Nagłówek sterujący jest specjalnym polem pakietu, które przechowuje określony komunikat. Natomiast komunikat sterujący jest niezależnym pakietem (zazwyczaj bardzo krótkim), stanowiącym odrębną wiadomość. W praktyce warstwy sprzętowe mogą ustanawiać połączenia jedynie z warstwami sąsiednimi, ponieważ systemy uczestniczące w połączeniach między warstwami sieciowymi, warstwami łączy danych i warstwami fizycznymi nie są wstępnie znane. W zależności od stanu sieci routing może obejmować różną liczbę systemów wymaganych do ustanowienia połączenia inicjowanego przez elementy sprzętowe. Wyższe warstwy stosu protokołów — aplikacje, prezentacje i sesji — korzystają z pojedynczych kanałów, wymieniając dane na zasadzie komunikacji punkt-punkt.

## Warstwa sesji

Warstwa sesji obejmuje funkcje odpowiedzialne za tworzenie sesji i zarządzanie nimi oraz udostępnia usługi przeznaczone do inicjowania tych sesji. Nieodłącznymi elementami warstwy sesji są mechanizmy zabezpieczania danych, takie jak okna logowania i inne formy dialogu z użytkownikiem.

Dane przepływają przez warstwę sesji w jednym lub w dwóch kierunkach naraz — w trybie pełnego duplexu lub półduplexu. Gdy stosowane jest połączenie jednokierunkowe (półduplexowe), warstwa sesji dołącza do danych identyfikator nazywany znacznikiem i w odpowiednim momencie (gdy nadejdzie ich kolej) przesyła je w kanale komunikacyjnym. Znacznik jest zwalniany w czasie komunikacji w przeciwnym kierunku.

W czasie pracy warstwy sesji w strumieniu danych wyznaczane są punkty kontrolne (wstawiane są znaczniki separacji), dzięki którym ewentualne przerwanie transmisji wiąże się jedynie z odtworzeniem połączenia bez konieczności powtórznego przesyłania wszystkich danych sesji. Synchronizacja przekazywanych informacji sprawia, że warstwa sesji zapewnia nie tylko niezawodne przesyłanie informacji, ale również gwarantuje wysoką wydajność komunikacji.

## Warstwa prezentacji

Warstwa prezentacji formatuje informacje przekazane z warstwy aplikacji, a także kompresuje je lub szyfruje przed dostarczeniem do warstwy sesji. Po odebraniu danych z warstwy sesji jej zadanie polega na rozszyfrowaniu i rozpakowaniu porcji danych (jeśli jest to konieczne) i dostarczeniu ich do warstwy aplikacji we właściwej formie.

Warstwa prezentacji pobiera obiekty danych utworzone przez aplikację z zastosowaniem różnych typów (np. znakowych, całkowitoliczbowych, binarnych) i przekształca je na format, który umożliwia przesłanie ich do zdalnego systemu w standardowym kodowaniu. Protokoły sieciowe łączą systemy operacyjne i aplikacje, eliminując dzielące je różnice. Dzięki temu komputer wykorzystujący jeden zestaw kodowy (np. ASCII) może komunikować się z komputerem używającym innego zestawu znaków (np. Unicode).

## Warstwa aplikacji

Warstwa aplikacji obejmuje oprogramowanie, z którym pracuje użytkownik. Programy warstwy aplikacji to przeglądarki internetowe, aplikacje pocztowe, interpretery poleceń (interfejsy wiersza poleceń), pakiety biurowe itp. Sam system operacyjny zawiera wiele programów warstwy aplikacji. Jednak nie każdy rodzaj oprogramowania można przypisać do tej warstwy. Na przykład edytor Microsoft Word nie jest oprogramowaniem wyłącznie warstwy aplikacji. Składa się bowiem z wielu komponentów, które funkcjonują na różnych poziomach stosu protokołów, a część jego modułów nie ma żadnego związku z siecią. Niemniej gdy użytkownik zleci wykonanie wydruku przez sieć, niejawnie odwoła się do podsystemu wydruku — pracującego w warstwie aplikacji — który przekaże zadanie do sieci.

Oprogramowanie warstwy aplikacji często opisuje się w sposób właściwy dla sesji terminalowej. Sesja terminalowa jest aplikacją, która dostarcza informacji na temat stanu systemu, umożliwia wprowadzanie poleceń i stanowi interfejs pozwalający użytkownikowi na interakcje z systemem. Po uruchomieniu sesji terminalowej i zalogowaniu się w zdalnym systemie użytkownik korzysta z programu warstwy aplikacji. Aby sesja terminalowa mogła współdziałać z różnymi programami, musi istnieć zunifikowany sposób komunikowania się wspomnianych aplikacji z sesją terminalową. Wiele programów tego typu korzysta z wirtualnego terminalu sieciowego w celu ustandaryzowania interakcji między aplikacjami takimi jak edytory tekstowe a różnymi dostępnymi terminalami. Dzięki temu takie parametry jak rozdzielczość ekranu oraz kody klawiszy pozostają standardowe.

Warstwa aplikacji obejmuje wiele różnorodnych usług, a rodzaj i liczba tych usług różni się w poszczególnych systemach. Usługi warstwy aplikacji są udostępniane przez same aplikacje. Oto lista przykładowych usług:

- ♦ Wyświetlanie obrazu.
- ♦ Inicjowanie operacji wejścia-wyjścia i zarządzanie nimi.
- ♦ Transfer plików.
- ♦ Obsługa poczty elektronicznej.
- ♦ Drukowanie sieciowe.
- ♦ Przeszukiwanie usług katalogowych.

W warstwie aplikacji zdefiniowano największy zbiór protokołów sieciowych. Są wśród nich: protokół przesyłania dokumentów hipertekstowych (HTTP — *HyperText Transfer Protocol*) wykorzystywany przez przeglądarki internetowe, protokół transferu plików (FTP — *File Transfer Protocol*) stosowany do przesyłania plików do serwera i pobierania ich z serwera, protokoły wysyłania i pobierania poczty (SMTP — *Simple Mail Transfer Protocol*; POP — *Post Office Protocol*).

## Model odniesienia TCP/IP

Choć model OSI jest najlepiej znanym modelem odniesienia, nie jest jedynym wykorzystywanym warstwowym modelem sieciowym. Najchętniej stosowaną alternatywą dla niego jest model TCP/IP.



Model TCP/IP został szczegółowo opisany w rozdziale 18.

W modelu TCP/IP zdefiniowano trzy różne protokoły odpowiedzialne za transportowanie i formatowanie danych. Protokół sterowania transmisją (TCP — *Transmission Control Protocol*) opisuje zasady nawiązywania połączeń przez systemy pracujące w internecie. Protokół datagramów użytkownika (UDP — *User Datagram Protocol*) określa, w jaki sposób należy realizować transmisję bezpołączeniową. Z kolei trzeci z protokołów — protokół internetowy (IP — *Internet Protocol*) — definiuje zasady formowania pakietów danych. TCP i UDP są protokołami warstwy transportowej, natomiast IP jest protokołem warstwy internetowej.

W modelu TCP/IP wyróżniono cztery warstwy o nieco innym znaczeniu niż w modelu OSI. Warstwy 1. i 2. modelu OSI (fizyczna i łącza danych) odpowiadają warstwie dostępu do sieci w modelu TCP/IP. Warstwa 3. (sieci) w modelu OSI jest bezpośrednim odpowiednikiem warstwy internetowej w modelu TCP/IP. Warstwa transportowa występuje w obydwu modelach na tej samej pozycji. W modelu TCP/IP nie zostały uwzględnione warstwy 5. i 6. (sesji i prezentacji). Natomiast na samym szczycie obydwu stosów znajduje się warstwa aplikacji (czyli 7. warstwa modelu OSI). Zestawienie obydwu modeli zostało przedstawione na rysunku 2.2.

**Rysunek 2.2.**

*Porównanie modeli  
OSI i TCP/IP*

	OSI	TCP/IP
7	W. aplikacji	W. aplikacji
6	W. prezentacji	
5	W. sesji	
4	W. transportowa	W. transportowa
3	W. sieci	W. internetowa
2	W. łącza danych	W. dostępu do sieci
1	W. fizyczna	

## Porównanie modeli odniesienia OSI i TCP/IP

Przez wiele lat modele OSI i TCP/IP kształtowały rozwój przemysłu sieciowego. Choć w obydwu występują pewne niedoskonałości w odwzorowywaniu rzeczywistych sieci, ich poznanie okazuje się nieodzowne. Model TCP/IP w znacznym stopniu odpowiada produktom i technologiom, które bazują na protokołach stanowiących dominujące obecnie standardy. Z kolei model OSI nie odzwierciedla w dostatecznym stopniu żadnego produktu. Dlatego jest on pewnym abstrakcyjnym wzorcem, pomocnym w zrozumieniu komunikacji sieciowej.

Nawet w sieciach zaprojektowanych na bazie siedmiowarstwowego modelu OSI niektóre z warstw (szczególnie sesji i prezentacji) są implementowane w niewielkim zakresie lub w ogóle. Z drugiej strony warstwy sprzętowe, takie jak łącza danych i sieciowa, realizują tak wiele funkcji i usług, że każda wnikliwa analiza prowadzi do podziału ich na kilka podwarstw.

Z powodu dużej złożoności modelu OSI żadna kluczowa technologia nie została zaimplementowana w pojedynczej warstwie. Poszczególne polecenia i komponenty sterujące są natomiast rozproszone w kilku różnych warstwach. Ta nadmiarowość sprawia, że model OSI jest znacznie bardziej skomplikowany, niż mógłby być. W praktyce rozwiązania sieciowe obejmują kilka warstw modelu OSI w jednym urządzeniu.

Model OSI został opracowany w formie siedmiu warstw najprawdopodobniej z tego powodu, że firma IBM stosowała siedmiowarstwową architekturę systemów sieciowych (SNA — *Systems Network Architecture*). W latach 70. można było przypuszczać, że przemysł sieciowy pozostanie pod kontrolą firmy IBM. Model OSI został więc przygotowany w taki sposób, aby odpowiadał technologii SNA bez konieczności wprowadzania istotnych modyfikacji.

Choć model TCP/IP jest odwzorowywany w znacznej liczbie produktów dostępnych na rynku, wciąż jest krytykowany za to, że jest niedostatecznie ogólny, by znajdował zastosowanie w odniesieniu do innych protokołów. Rozróżnienie interfejsów, usług oraz sposób wykorzystania protokołów w ramach modelu nie są przejrzyste zdefiniowane. Na przykład warstwa dostępu do sieci wcale nie obejmuje osobnych protokołów i bardziej przypomina interfejs. Poza tym formalnie nie występują warstwy prezentacji oraz sesji. W praktyce oznacza to tworzenie ad hoc standardów protokołów.

Najlepiej nie przywiązywać zbyt dużej wagi do modeli sieciowych. Choć model OSI charakteryzuje się wyjątkową elastycznością i jest powszechnie wykorzystywany w teoretycznych rozważaniach, a model TCP/IP jest w pewnym zakresie odwzorowywany w produktach sieciowych, żaden z nich nie nadaje się do bezpośredniego zastosowania w rzeczywistych sieciach.



Być może najlepszym rozwiązaniem byłoby przyjęcie jednej z alternatywnych definicji rozważanych podczas opracowywania modelu OSI — modelu pięciowarstwowego. W odrzuconym projekcie nie występowały warstwy sesji i prezentacji właściwe dla modelu OSI, a funkcje tych warstw były rozmieszczone w warstwach aplikacji i transportowej. Warstwy sieciowa, łącza danych i fizyczna miały taki sam charakter.

## Podsumowanie

W tym rozdziale został przedstawiony model OSI stanowiący architektoniczną platformę opisu urządzeń i sieci komputerowych. Ten siedmiowarstwowy model reprezentuje stos protokołów z aplikacjami i oprogramowaniem umieszczonym na szczycie, warstwami przetwarzania danych znajdującymi się w środkowej części stosu oraz warstwami sprzętowymi na dole. Komunikacja między jednostkami polega na przesłaniu danych ze stosu protokołów urządzenia nadawczego do stosu protokołów urządzenia odbiorczego.

Granicę między każdą warstwą wyznacza interfejs, który wymaga zastosowania interfejsu API w celu utworzenia usługi łączącej obydwie warstwy. Model OSI nie definiuje samego interfejsu lub usługi, ale wskazuje potrzebę ich użycia.

Oprócz modelu OSI stosowane są również inne opisy architektury sieci, w tym model TCP/IP. Choć model TCP/IP znajduje większe odzwierciedlenie w rzeczywistych sieciach i urządzeniach, model OSI charakteryzuje się znacznie większą elastycznością i częściej jest wykorzystywany do opisywania różnych aspektów funkcjonowania sieci. Istnieją również modele hybrydowe, które uwzględniają mniejszą liczbę warstw niż model OSI i są nieco mniej skomplikowane.



# Rozdział 3.

## Architektura i projektowanie sieci

### W tym rozdziale:

- ♦ Różne topologie sieciowe
- ♦ Wpływ typów połączeń na rodzaje sieci
- ♦ Segmenty sieci i routing
- ♦ Różne architektury sieciowe

W tym rozdziale zostaną przedstawione różne zagadnienia związane z opracowywaniem topologii i architektury sieci. Topologia sieci wynika między innymi z rodzajów połączeń. Natomiast architekturę sieci definiują systemy sieciowe bazujące na wspólnym protokole. Rozróżnienie tego, czy rozważanie odnosi się do architektury, czy topologii, sprowadza się do określenia najwyższego protokołu w stosie. Topologie są wyznaczane w odniesieniu do fizycznego transportu danych. Natomiast architekturę definiuje się na podstawie protokołów warstw wyższych.

W rozważaniach trzeba uwzględnić kilka typów połączeń punkt-punkt. Wyróżnia się bowiem cztery rodzaje połączeń między punktami końcowymi — połączenia fizyczne, połączenia wirtualne, połączenia tymczasowe oraz łącza bez jednoznacznie wydzielonych połączeń. Wszystkie one stanowią podstawę funkcjonowania nowoczesnych sieci.

Zbiór węzłów współdzielących określone medium fizyczne jest nazywany *segmentem*. Segmenty są podstawowymi jednostkami sieci. Ruch w nich nie musi być przekazywany przez jednostki pośrednie. Poszczególne węzły muszą natomiast współdzielić określoną przestrzeń adresowania logicznego, mimo że posiadają własne adresy fizyczne (np. adresy MAC). Segmenty wyznaczają również domeny kolizyjne.

Aby rozdzielić segmenty, należy wstawić między nie punkty łącznikowe, takie jak przełączniki lub routery. Sieci składające się z wielu segmentów muszą zawierać routery, przez które przekazywany jest ruch. Routery z kolei mogą korzystać z dowolnych z czterech wymienionych wcześniej połączeń. Komunikacja może mieć charakter „jeden do jednego” (ang. *unicast*), „jeden do wielu” (ang. *multicast*), „jeden do wszystkich” (rozgłoszeniowy (ang. *broadcast*)) lub „jeden do dowolnego” (ang. *anycast*). Wpływ przełączania tras oraz pakietowej transmisji danych na budowę sieci zostanie omówiony w dalszej części rozdziału.

Wśród prezentowanych zagadnień przedstawione zostaną także różne architektury sieci istotne z punktu widzenia projektanta sieci, w tym rozwiązania peer-to-peer, klient-serwer, wielowarstwowe oraz uproszczone klient-serwer. Wybór jednej z architektur wyznacza sposób rozmieszczenia zasobów sieciowych, lokalizację poszczególnych systemów oraz rodzaj stosowanych protokołów.

## Architektura sieci i topologia

Metody komunikacji między systemami sieciowymi nazywa się *architekturą sieci*. Z kolei sposób przygotowania infrastruktury fizycznej w celu ustanowienia połączeń sieciowych jest nazywany *topologią sieci*. Topologia określa fizyczne aspekty transportu danych. Architektura opisuje natomiast technologie zastosowane do zarządzania danymi i ich przetwarzania.

W niektórych przypadkach architektura wymusza wdrożenie określonej topologii, a w innych określona topologia narzuca architekturę. Jednak nie zawsze architektura i topologia są tak ściśle ze sobą związane.

Najczęściej architekturę wybiera się w taki sposób, aby odpowiadała geograficznemu rozmieszczeniu stacji, strukturze organizacyjnej, obciążeniu systemów, wymogom wydajnościowym lub dostępności personelu odpowiedzialnego za zarządzanie infrastrukturą.

Oto typowe architektury sieciowe:

- ♦ Sieci peer-to-peer.
- ♦ Sieci klient-serwer (dwuwarstwowe).
- ♦ Sieci wielowarstwowe.
- ♦ Usługi katalogowe lub sieci stowarzyszone.
- ♦ Sieci kratowe lub rozproszone.
- ♦ Hybrydowe połączenia wymienionych rozwiązań.



Usługi katalogowe zostały opisane w rozdziale 21.



Sieci hybrydowe obejmują dwie spośród wymienionych architektur lub większą ich liczbę.

W celu ustalenia, czy opis technologii odnosi się do architektury sieci, czy do jej topologii, wystarczy przeanalizować najwyższą warstwę modelu OSI, do której ta technologia się odnosi. Topologia jest związana z technologiami implementowanymi na poziomie warstw fizycznej i łącza danych. Natomiast architektura wyznacza technologie stosowane na poziomie warstwy sieciowej oraz warstw wyższych.

Różnicę między topologią i architekturą można zilustrować kilkoma przykładami. Ethernet jest technologią, która definiuje przenoszenie ramek danych w medium transmisyjnym. Istnieją odmiany Ethernetu działające w skręćce oraz w kablu światłowodowym. Najwyższą

warstwą uwzględnioną w standardzie Ethernet jest warstwa łącza danych, w której wyznaczany jest wspólny format adresowania bazujący na adresach MAC. Ethernet jest więc topologią sieci. Sieci Ethernet można budować na wiele różnych sposobów — jako magistrale, hierarchiczne drzewa, pierścienie itp. Jednak wszystkie wymienione warianty wymagają zastosowania adresowania MAC w najwyższej warstwie obejmowanej przez Ethernet.



Więcej informacji na temat budowy sieci Ethernet, w tym opisy magistral, hierarchicznych drzew i pierścieni, zostało zamieszczonych w rozdziale 1.

Działanie internetu bazuje na wielu protokołach, czyli standardowych zasadach generowania danych i zarządzania nimi. Protokoły te są en bloc nazywane *zestawem protokołów internetowych* (ang. *Internet Protocol Suite*). Znaczna część niniejszej książki jest poświęcona protokołom internetowym, ponieważ zdominowały one dzisiejsze sieci i większość osób często z nich korzysta.

Dwoma najważniejszymi protokołami internetowymi są protokół sterowania transmisją (TCP — *Transmission Control Protocol*) oraz protokół internetowy (IP — *Internet Protocol*). Protokół TCP jest protokołem warstwy transportowej. Natomiast protokół IP funkcjonuje w warstwie sieciowej modelu OSI. Protokół IP jest również bardzo często odnoszony do innego sieciowego modelu — modelu TCP/IP — w którym przynależy do warstwy międzysieciowej. Warstwa międzysieciowa stosu TCP/IP pokrywa się z warstwą sieciową modelu OSI. Jednak w warstwie sieciowej modelu OSI uwzględniane są również pewne technologie odpowiadające za odwzorowanie adresów, które w modelu TCP/IP bardziej pasują do warstwy dostępu do sieci. Jednym z przykładów może być protokół odwzorowywania adresów (ARP — *Address Resolution Protocol*). Zasadniczą różnicą między obydwo ma modelami jest to, że w modelu OSI nie ma podziału na komunikację połączeniową oraz komunikację o niezdefiniowanym rodzaju połączeń. Niemniej jeśli przeanalizuje się poszczególne warstwy modelu TCP/IP, można zauważyć, że niemal wszystkie z nich odpowiadają rozwiązaniom zdefiniowanym powyżej warstwy łącza danych modelu OSI. Wiele z nich, szczególnie protokoły routingu, to protokoły warstwy aplikacji. Protokoły wyższych warstw sprawiają, że technologię IP należy uznać za architekturę.

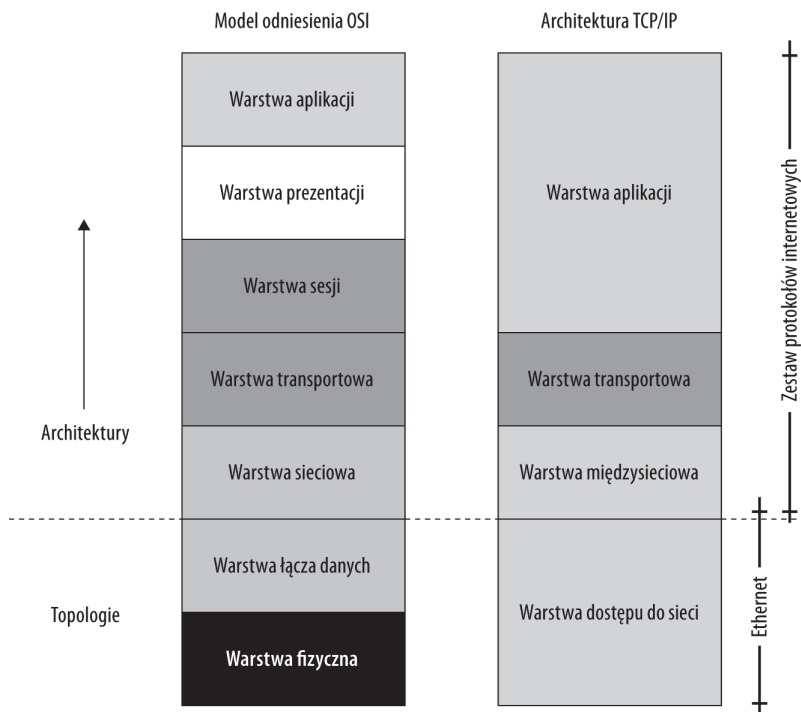
Porównanie obydwu modeli (OSI i TCP/IP) zostało przedstawione na rysunku 3.1. Model architektury TCP/IP jest opisany w dokumencie RFC 1122 (<http://tools.ietf.org/html/rfc1122>). W literaturze często w różny sposób opisywane są relacje między obydwo ma stosami. Różnie też prezentowana jest struktura modelu TCP/IP oraz nazwy warstw. Z tego względu nie należy przywiązywać zbyt dużej wagi do zależności wynikających z rysunku 3.1. Część autorów wyróżnia w modelu TCP/IP cztery lub pięć innych warstw i przypisuje im inne nazwy. W niektórych analizach warstwa dostępu do sieci jest nazywana warstwą sieciową. W innych warstwa dostępu do sieci jest podzielona na warstwę sieciową i fizyczną, warstwę łącza danych i sprzętową lub warstwę łącza danych i fizyczną. Jednak we wszystkich modelach TCP/IP warstwa aplikacji obejmuje warstwy aplikacji, prezentacji i sesji modelu OSI. Wynika to z tego, że protokoły internetowe powyżej IP funkcjonują we wszystkich tych warstwach.

## Komunikacja punkt-punkt

Połączenia punkt-punkt są najprostszą formą sieci obejmującej dwa dowolne systemy. Każde połączenie składa się z trzech komponentów: dwóch punktów końcowych oraz połączenia między nimi. Różne chwilowe ustawienia każdego z tych elementów wyznaczają określony

**Rysunek 3.1.**

Porównanie modelu  
OSI do architektury  
TCP/IP



rodzaj połączenia. Z kolei każdemu rodzajowi połączenia odpowiadają różne stany, z których wynikają właściwości połączenia. Stan połączenia jest charakteryzowany przez następujące parametry:

- ♦ **Stan fizyczny.** Każdy komponent (punkt końcowy lub połączenie) może mieć charakter fizyczny lub wirtualny.
- ♦ **Stan logiczny.** Stan logiczny opisuje nazwa lub identyfikator skojarzony z punktem końcowym lub połączeniem. Nazwą może być adres IP lub definicja trasy przez sieć (w połączeniach trwałych lub przełączonych). Adres i trasa mogą jednak być wirtualne lub zmienne.
- ♦ **Sygnal.** Różne rodzaje połączeń mogą obsługiwać jedną lub większą liczbę sesji, przysyłać dane w formie pojedynczego komunikatu lub przekształcać je w pakiety itp.
- ♦ **Wydajność.** W zależności od stanu fizycznego i logicznego oraz typu sygnału połączenia mogą pracować z różną wydajnością.

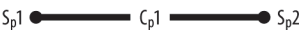
W kolejnych punktach omówiono cztery rodzaje połączeń. Towarzyszące im rysunki ułatwiają porównywanie poszczególnych połączeń, wskazując ich fizyczną i logiczną realizację oraz wpływ na formowanie sygnału przenoszonego w ramach połączenia i charakterystyki wydajnościowe wraz z ograniczeniami transmisyjnymi. Rysunek przedstawiony obok nazwy typu połączenia jest symbolem tego połączenia.

Fizyczne połączenia punkt-punkt

Najmniej skomplikowanym połączeniem jest połączenie punkt-punkt. Na rysunku 3.2 zostało przedstawione połączenie fizyczne z fizycznymi punktami końcowymi. Znajdujący się z lewej strony rysunku symbol *Sp1* reprezentuje system nadawczy. Z kolei występujący z prawej strony symbol *Sp2* odpowiada systemowi odbiorczemu. Połączenie jest ustanowione w ramach stałego medium transmisyjnego (np. przewodu lub światłowodu), a protokoły najwyższej warstwy zapewniają negocjację parametrów sesji. Szybkość transmisji jest uzależniona od mocy interfejsów sieciowych oraz ich wydajności, a także od wynegocjowanej zdolności do transmitowania danych w ramach połączenia. Dane są przekazywane z lewej strony w prawo w czasie półdupleksowej sesji. Jeśli w ramach sesji zostanie ustanowione połączenie dwukierunkowe, dane będą przesyłane w obydwu kierunkach.

Rysunek 3.2.

Połączenie punkt-punkt i jego tabela stanów



	<i>Sp1</i>	<i>Cp1</i>	<i>Sp2</i>
Stan fizyczny	Fizyczny interfejs sieciowy	Połączenie fizyczne	Fizyczny interfejs sieciowy
Stan logiczny	Adres	Wyznaczony obwód	Adres
Sygnal	Wysyłany – pojedynczy lub wielokrotna sesja	Fizyczny (ustalony)	Odbierany – pojedynczy lub wielokrotna sesja
Wydajność	Częstotliwość sygnału	Pełna szerokość pasma	Częstotliwość sygnału

Tabela znajdująca się po prawej stronie każdego rodzaju połączenia przedstawia różne charakterystyki dwóch punktów końcowych (*Sp1* i *Sp2*) oraz połączenia (*Cp1*). W przypadku połączeń typu punkt-punkt punkty końcowe są fizycznymi interfejsami sieciowymi (kartaми sieciowymi), a łączem jest kabel. Aby opisać ten rodzaj połączenia, potrzebne są adresy odpowiadające każdemu z punktów końcowych. Dzięki nim można wyróżnić obwód (czyli trasę) sygnału przekazywanego z jednego punktu do drugiego. Fizyczne i logiczne parametry trasy nie będą się zmieniały przez cały czas obowiązywania połączenia punkt-punkt.

Zaletą połączeń punkt-punkt jest to, że mogą one przenosić jednocześnie wiele sygnałów, ponieważ obwód jest ustanawiany na bazie dedykowanego połączenia. Ograniczenie wydajności wynika z ograniczeń elementów fizycznych wchodzących w skład układu. Szybkość transmisji zostanie więc wyznaczona przez najniższą wartość następujących parametrów: szybkość, z jaką punkt końcowy *Sp1* może generować sygnał, szerokość pasma połączenia *Cp1*, szybkość, z jaką punkt końcowy *Sp2* może odbierać nadchodzące sygnały.

Ograniczeniem dla szybkości transmisji może być:

- ♦ Szerokość pasma medium transmisyjnego.
- ♦ Mniej efektywny z punktów końcowych.
- ♦ Zdolność do przetwarzania danych przez określony protokół warstwy wyższej.

Jeśli dane są przesyłane w formie skompresowanej lub zaszyfrowanej, granice wydajności określone przez przepustowość (na przykład w bitach na sekundę) są opisywane jako zdolność punktu końcowego do przesyłania danych w formie zwykłego tekstu (lub innej wymaganej formie). Do pewnego stopnia w transferze danych na etapach pośrednich pomocne

jest ich buforowanie. Jednak jeśli komunikacja jest realizowana z pełną szybkością przez dłuższy czas, buforowanie może się okazać efektywne tylko w pewnym okresie, dopóki napływające informacje nie przepełnią bufora.

Całkowicie fizyczne połączenia punkt-punkt są typowe dla niewielkich sieci i przeważają w rozwiązaniach peer-to-peer. Połączenia punkt-punkt są wariantem topologii. Natomiast termin „sieci peer-to-peer” odnosi się do architektury. Jako przykład obydwu rozwiązań można sobie wyobrazić wiele połączeń punkt-punkt tworzących pajęczynę, siatkę lub kratę. Czy mamy w tym przypadku do czynienia z topologią, czy architekturą? Tak duża liczba połączeń do różnych punktów końcowych sieci oznacza, że rozwiązanie to można sklasyfikować jako architekturę siatkową lub kratową. Jeśli sieć siatkowa ma za zadanie jedynie przekazywać ruch sieciowy, jest topologią. Jeżeli jednak z działania sieci wynika rozproszenie zadań związanych z przetwarzaniem danych, tak jak ma to miejsce w przypadku aplikacji rozproszonych, to opisywane rozwiązanie jest architekturą (zgodnie z regułami opisanymi w niniejszym rozdziale).



Sieci peer-to-peer są szczegółowo opisane w rozdziale 11. Z kolei sieci siatkowe i kratowe są tematem rozdziału 17., w którym przedstawiono sieci o wysokiej wydajności.

Wirtualne połączenia punkt-punkt

W drugim przypadku połączenia punkt-punkt (przedstawionym na rysunku 3.3) wszystkie trzy komponenty są zwirtualizowane. Punkty końcowe Sv1 i Sv2 to wirtualne interfejsy sieciowe. Natomiast połączenie Cv1 jest wirtualnym obwodem. Wirtualny interfejs sieciowy jest symulowaną programowo fizyczną kartą sieciową. Aby utworzyć w systemie wirtualny interfejs sieciowy (lub większą ich liczbę), system ten musi być wyposażony w fizyczny interfejs sieciowy przenoszący ruch sieciowy. Liczba interfejsów wirtualnych nie jest w żaden sposób ograniczona, jednak wszystkie muszą mieć logiczny adres odpowiadający interfejsowi fizycznemu. Interfejsy sieciowe (włącznie z wirtualnymi) zostały opisane w rozdziale 7.

Rysunek 3.3.

Wirtualne połączenie punkt-punkt oraz jego tabela stanów



	Sv1	Cv1	Sv2
Stan fizyczny	Wirtualny interfejs sieciowy	Połączenie wirtualne	Wirtualny interfejs sieciowy
Stan logiczny	Adres	Wyznaczony obwód	Adres
Sygnał	Wysyłany – pojedynczy lub wielokrotna sesja	Tymczasowy (ustalony)	Odbierany – pojedynczy lub wielokrotna sesja
Wydajność	Częstotliwość sygnału	Przydzielona szerokość pasma	Częstotliwość sygnału

Tabela stanów wirtualnego połączenia punkt-punkt również została przedstawiona na rysunku 3.3. Aby opisać ten rodzaj połączenia, niezbędne są adresy każdego z dwóch punktów końcowych. Adresy te nie są jednak jedynymi stosowanymi na danym interfejsie fizycznym — interfejsie, do którego są przypisane punkty Sv1 lub Sv2.

Trasa (łącze) jest obwodem wirtualnym Cv1. Oznacza to, że obwód ten jest ustanawiany na początku sesji komunikacyjnej i rozłączany wraz z jej zakończeniem. Po zakończeniu sesji nie można określić dokładnej trasy przekazywania danych między punktami końcowymi, ponieważ trasa obwodu zmienia się z sesji na sesję. Niemniej w czasie trwania sesji obwód

wirtualny jest stały. Proces ustanawiania i rozłączania obwodu wirtualnego wnosi pewne opóźnienia w działaniu wirtualnego połączenia punkt-punkt, które nie występują w obwodach fizycznych.

Zaletą wirtualnych połączeń punkt-punkt jest to, że są one w stanie wykorzystać wszystkie fizyczne interfejsy sieciowe oraz wszystkie fizyczne obwody, a dzięki temu mogą korzystać z wszystkich dostępnych zasobów sieciowych. Obwód wirtualny jest kojarzony z sesją. Zatem mimo że punkty końcowe mogą realizować pojedyncze lub wielokrotne sesje w ramach wirtualnego połączenia punkt-punkt, sam obwód jest przeznaczony do komunikacji tylko między dwoma punktami końcowymi  $Sv1$  i  $Sv2$ . Wydajność wirtualnego obwodu jest ograniczona przez częstotliwość sygnału generowanego przez punkty końcowe oraz przez pasmo alokowane do połączenia  $Cv1$ .

Wirtualne połączenie punkt-punkt ma te same właściwości co połączenie fizyczne. Po ustanowieniu sesji sygnał jest przekazywany w obwodzie przypisanym określonej sesji. Wydajność jest limitowana przez te same czynniki, które ograniczają wydajność elementów fizycznych. Oznacza to, że szybkość transmisji jest determinowana przez najwolniejszy z trzech parametrów: szybkość, z jaką punkt końcowy  $Sp1$  może generować sygnał, szerokość pasma połączenia  $Cp1$ , szybkość, z jaką punkt końcowy  $Sp2$  może odbierać nadchodzące sygnały.

Połączenie wirtualne jest obwodem utworzonym w celu realizacji określonej sesji i utrzymywanym w czasie trwania sesji. Po zakończeniu sesji obwód wirtualny ulega rozłączeniu. Utrzymywanie dużej liczby połączeń fizycznych jest bowiem niepraktyczne. Aby utworzyć obwód wirtualny, urządzenia przełączające muszą zgromadzić wszystkie informacje o urządzeniach sąsiednich oraz muszą korzystać z mechanizmów optymalizacji tras. Z tego wynika pewien narzut systemowy uwidaczniający się podczas tworzenia obwodu wirtualnego i jego zrywania. Wspomniany narzut może się wiązać ze znacznym wykorzystaniem zasobów systemowych, a może być również pomijalnie mały. Wszystko zależy od zastosowanych technologii. Pod względem funkcjonalności po ustanowieniu obwodu nie ma żadnej różnicy między przesyłaniem danych w obwodach wirtualnych i obwodach fizycznych, ponieważ obwód wirtualny działa na bazie wielu połączeń fizycznych występujących na trasie. Obwody wirtualne są podstawowym elementem wirtualnych sieci prywatnych, których szczegółowy opis znajduje się w rozdziale 29.

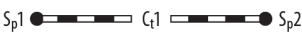
Wirtualizacja jest doskonałą techniką unifikacji rozwiązań informatycznych. Z tego powodu staje się coraz istotniejsza, gdyż umożliwia optymalizowanie wydajności systemów sieciowych. Uruchamianie maszyn wirtualnych staje się standardowym rozwiązaniem w systemach serwerowych i zaczyna wkraczać w obszar stacji roboczych. Obecnie istnieje możliwość zwirtualizowania niemal dowolnego komponentu informatycznego w ramach jednego systemu fizycznego, który jest zdolny do wydajnego działania. W tym rozumieniu wirtualizacja stanowi formę przekierowania i partycjonowania pracy.

## Przełączanie pakietów i połączenia tymczasowe

Na rysunku 3.4 został przedstawiony zupełnie inny model połączeń punkt-punkt w porównaniu z wcześniejszymi rozważaniami. Reprezentuje on połączenia pakietowe lub tymczasowe, w których połączenie w ogóle nie jest definiowane. Internet bazuje na rozwiązaniach bezpołączeniowych, czyli bezstanowych. Brak wyznaczonego obwodu całkowicie zmienia mechanizmy dostarczania danych przez sieć.

**Rysunek 3.4.**

Przełączanie pakietowe (połączenie tymczasowe) i odpowiadająca mu tabela stanów



	Sp1	Ct1	Sp2
Stan fizyczny	Fizyczny interfejs sieciowy	Przełączanie pakietów (połączenie tymczasowe)	Fizyczny interfejs sieciowy
Stan logiczny	Adres	Brak zdefiniowanego obwodu	Adres
Sygnal	Wysyłany we fragmentach	Wielodrogowy	Odbierany (odtwarzanie kolejności)
Wydajność	Zmienna częstotliwość sygnału	Zmienna szerokość pasma	Zmienna częstotliwość sygnału

Zgodnie z informacjami zawartymi na rysunku 3.4 komunikacja tego typu bazuje na modelu bezpołączeniowym. System nadawczy i system odbiorczy zostały przedstawione jako dwa fizyczne punkty końcowe *Sp1* i *Sp2*. Jednak równie dobrze mogłyby być dwoma wirtualnymi punktami końcowymi *Sv1* i *Sv2* lub dowolną kombinacją węzła fizycznego i wirtualnego, np. *Sp1* i *Sv2*. Przedstawienie jednej konkretnej konfiguracji ma na celu tylko uproszczenie analizy. Rodzaj punktu końcowego nie ma większego znaczenia w dalszych rozważaniach. Najistotniejszą cechą tej konfiguracji jest brak zdefiniowanej trasy, co zostało przedstawione na diagramie w formie przerywanej linii *Ct1*. Brak określonego obwodu oznacza, że trasa zmienia się i dane są przekazywane trasami, które w danej chwili są najkorzystniejsze. W połączeniach bezstanowych transmisja jest realizowana zgodnie z zasadą działania „najlepszego z możliwych” (ang. *best effort*).

Jest to pierwsze z połączeń punkt-punkt o charakterze bezstanowym (ang. *stateless*). Wszystkie opisane wcześniej były połączeniami stanowymi (ang. *statefull*). Z tej różnicy wynikają bardzo istotne implikacje. W połączeniu stanowym obwód jest wstępnie określony. Natomiast w połączeniu bezstanowym żadna trasa nie jest wstępnie zdefiniowana.

Połączenia stanowe mogą być trwałe, co pozwala na przesyłanie strumieni informacji w formie serii bitów, bajtów lub znaków. Przekazywane w ten sposób dane docierają do odbiorcy sekwencyjnie (w odpowiedniej kolejności) i nie wymagają odtwarzania pierwotnej kolejności segmentów. Generowany strumień może w niektórych przypadkach w ogóle nie podlegać segmentacji (jeśli rozmiar danych to umożliwi). W pewnym badaniu dotyczącym korporacyjnej poczty elektronicznej ustalono, że 90 procent wiadomości ma nieduży rozmiar (3 KB lub mniej), ale pozostałe 10 procent listów stanowi 90 procent wszystkich danych. Wyniki podobnego testu mogą się różnić w zależności od rodzaju aplikacji, ale konkluzja jest taka, że większość przekazywanych danych podlega podziałowi na fragmenty, ponieważ protokoły sieciowe ograniczają rozmiar segmentu w celu uproszczenia mechanizmów korekty błędów.

Z kolei połączenia bezstanowe wykorzystują wszystkie dostępne fizyczne trasy lub trasy wyznaczone przez algorytmy optymalizacji lub routingu. Kolejne porcje danych docierające do odbiorcy mogą być przekazywane tą samą trasą lub różnymi trasami. Oznacza to, że sieci pakietowe (bazujące na przełączaniu pakietów) znacznie lepiej wykorzystują sieć fizyczną niż jakiegokolwiek inne rodzaje połączeń. Z tego też powodu niemal wszystkie komercyjne połączenia sieciowe bazują na technologii przełączania pakietów. Jedynie połączenia sieci rdzeniowej (o bardzo dużych szybkościach transmisyjnych) nie podlegają tej zasadzie. Z przedstawionego rysunku wynika, że sieci o przełączanych obwodach przekazują dane we fragmentach różnymi drogami. Wydajność opisywanego rozwiązania może być regulowana przez zmianę częstotliwości wysyłania lub odbierania danych w punktach końcowych, a także przez dynamiczną zmianę szerokości pasma przydzielanego połączeniu.

Choć połączenia punkt-punkt bywają wstępnie przygotowane, mogą również być ustanawiane okresowo, jak wynika z rysunku 3.3. Typowym przykładem rozwiązania tego typu są sieci token ring, w których jednostka sieci otrzymuje prawo pełnego wykorzystania sieci, tylko jeśli jest stacją o wysokim priorytecie i tylko na czas sesji. Analogiczne zależności występują w wirtualnych sieciach prywatnych (VPN — *Virtual Private Network*), w których obwód jest ustanawiany na czas sesji.

Aby połączenie działało również w przypadku braku wstępnie zdefiniowanego obwodu, system nadawczy dzieli dane na fragmenty nazywane pakietami, ramkami lub datagramami. Każdy fragment sekwencji jest szyfrowany (jeśli jest to konieczne), oznaczany numerem sekwencyjnym, uzupełniany o wartość kontrolną algorytmu korekcji błędów, enkapsulowany (niemal w każdym przypadku) i wysyłany. Każdy z wprowadzonych do sieci fragmentów jest dostarczany do elementu koncentrującego ruch, a następnie przekazywany najlepszą trasą przez kolejne routery.

Uszkodzenie łącza nie stanowi problemu. Kolejne porcje danych mogą być przesyłane innymi trasami. Połączenia bezstanowe cechują się dużą odpornością na awarie. Spełnią swoje zadanie nawet w czasie lokalnej wojny nuklearnej. Dzięki możliwości przekazywania bloków danych różnymi trasami sieć jest równomiernie obciążona, a dostępne pasmo jest w pełni wykorzystane. Twierdzenie to nie jest prawdziwe w przypadku połączeń stanowych. Z tego względu połączenia pakietowe (tymczasowe obwody punkt-punkt) dominują w branży sieciowej.

Warto zwrócić uwagę na fakt, że obwody o przełączanych pakietach są klasyfikowane jako architektura, a nie topologia. Choć znane są adresy punktów końcowych, nie można zdefiniować połączenia między nimi. Oznacza to, że konieczne jest zastosowanie protokołów warstw wyższych w celu prawidłowego dostarczania danych do jednostek zdalnych. Operacje te nie należą do zadań warstw fizycznej i łącza danych.

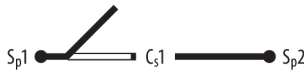
Na skutek przesyłania różnymi drogami pewne pakiety mogą docierać do stacji docelowych wcześniej od innych, a w związku z tym — w niewłaściwej kolejności. Ponadto część pakietów może utknąć w sieci po dostarczeniu do węzła, który nie ma informacji o trasie do jednostki docelowej. Inna część z pewnością dotrze do odbiorcy z błędami. Do zadań docelowego punktu końcowego należy więc sprawdzenie błędów, odtworzenie pierwotnej kolejności pakietów oraz rozszyfrowanie danych. W połączeniach bezstanowych wszystkie węzły sieciowe wraz z docelowym punktem końcowym muszą uczestniczyć w wymianie żądań i potwierdzeń dostarczenia danych. Przekazywanie związanych z tym komunikatów wnosi dodatkowy narzut transmisyjny, który w pewnych przypadkach (szczególnie gdy stopa błędów jest wysoka) może być istotnym czynnikiem spowalniającym. Wdrożenie bowiem mechanizmów gwarantowanej jakości obsługi (QoS — *Quality of Service*) jest znacznie łatwiejsze w połączeniach stanowych niż bezstanowych.

## Połączenia przełączane

Na rysunku 3.5 zostało przedstawione przełączane połączenie punkt-punkt, w którym obwód jest ustanawiany okresowo. Dostęp do obwodu regulują dwie metody — *podziału czasu* oraz *dostępu negocjowanego*. Typowym przykładem zastosowania omawianego rozwiązania jest publiczna sieć telefoniczna (PSTN — *Public Switched Telephone Network*).

**Rysunek 3.5.**

Połączenie  
przełączane  
i jego tabela  
stanów



	$S_{p1}$	$C_{s1}$	$S_{p2}$
Stan fizyczny	Fizyczny interfejs sieciowy	Przełączanie obwodów	Fizyczny interfejs sieciowy
Stan logiczny	Adres	Tymczasowy obwód	Adres
Sygnal	Wysyłany we fragmentach	Pojedyncza trasa	Odbierany i odtwarzany
Wydajność	Niepełna częstotliwość sygnału	Okresowo pełna szerokość pasma	Niepełna częstotliwość sygnału

W metodzie podziału czasu określony węzeł uzyskuje dostęp do obwodu w regularnych odstępach czasowych. Technika ta jest powszechnie stosowana w systemach mikroprocesorowych, ale niezwykle rzadko wykorzystywana w technologiach sieciowych. W przypadku okresowego odwoływania się do zasobów systemu mikroprocesorowego nie występuje żadne opóźnienie w dostępie do informacji zgromadzonych w buforach. Jednak w sieciach dostęp z podziałem czasowym do połączenia wiąże się z koniecznością jego nawiązywania i zrywania, co wprowadza opóźnienie o wartościach, które nie mogą zostać zaakceptowane. Dodatkowa zwłoka oznaczałaby nieefektywne wykorzystanie pasma sieci.

Na rysunku 3.5 zostały przedstawione fizyczne punkty końcowe  $S_{p1}$  i  $S_{p2}$ , gdyż jest to charakterystyczna konfiguracja w przypadku większości sieci przełączanych. Podobnie jak w opisanych wcześniej sieciach pakietowych, technika przełączania obwodów bazuje na założeniu, że połączenie  $C_{s1}$  jest ustanawiane w chwili inicjowania sesji komunikacyjnej. Jednak w przeciwieństwie do mechanizmu przełączania pakietów połączenie to jest podtrzymywane przez cały czas trwania sesji. Przekazywane dane mogą być dzielone na fragmenty, ale wszystkie fragmenty są przekazywane tą samą trasą. Zaletą przełączania obwodów jest więc możliwość przesyłania strumieni danych. Ponadto fizyczne łącze może zostać podzielone na kanały, a bezproblemowa obsługa zbitek danych zapewnia poprawną komunikację w przypadku obniżenia jakości sygnału.

Najpowszechniej stosowane rozwiązanie związane z przełączaniem połączeń polega na negocjowaniu dostępu do sieci. Symulowanie przełączanych połączeń jest realizowane na przykład w sieciach, w których dostęp do medium reguluje mechanizm przekazywania znacznika. Przekazanie znacznika zachodzi w regularnych interwałach, więc nawet węzeł o wysokim priorytecie nie może w nieskończoność korzystać z pasma transmisyjnego. Z punktu widzenia innych użytkowników systemu sieć kontrolowana przez pojedynczy węzeł może się jednak wydawać niedostępna lub zablokowana.

Większość połączeń sieciowych to połączenia przełączane, gwarantujące istnienie trasy między dwoma punktami końcowymi. Niektóre połączenia sieciowe (np. łącza mostkowe, sieci szkieletowe itp.) są połączeniami dedykowanymi, ale zazwyczaj obejmują one tylko niewielki podzbiór wszystkich połączeń występujących w sieci.



Więcej informacji na temat routerów, mostów i przełączników znajduje się w rozdziale 10. Natomiast szczegółowy opis sieci WAN i połączeń szkieletowych został zaprezentowany w rozdziale 13.

## Sieci przełączane i pakietowe

Wokół terminów *pakiet*, *ramka* i *datagram* jest wiele niejasności. Wynikają one przede wszystkim z podobnego znaczenia poszczególnych słów, a zastosowanie odpowiedniego zależy od rodzaju opisywanej technologii. Pakiet jest porcją odpowiednio sformatowanych danych, która jest przekazywana w sieci pakietowej (w sieci z przełączaniem pakietów). Przełączanie pakietów polega na kierowaniu ruchu poprzez operowanie pojedynczymi pakietami. Mechanizm ten ma charakter bezstanowy.

Technika przełączania pakietów została zilustrowana na rysunku 3.5. Przekazywane informacje zawsze są dzielone na pewne porcje, do których dołącza się adres. Nie są natomiast związane ze wstępnie ustanowionym połączeniem. Przełączanie zachodzi w komputerze, przełączniku, routerze lub innym urządzeniu. Trasa przesyłania pakietu jest wyznaczana na podstawie zawartych w nim informacji adresowych oraz ewentualnie danych na temat priorytetu.

Termin *przełączanie obwodów* znajduje zastosowanie w opisywaniu sieci bazujących na stałych połączeniach między punktami końcowymi wymieniającymi informacje. Typowym przykładem sieci z przełączaniem obwodów jest stara sieć telefoniczna. Z informacji zamieszczonych na rysunkach 3.2 i 3.3 wynika, że obwody te mogą być obwodami trwałymi lub wirtualnymi. Sieci wykorzystujące technikę przełączania obwodów współdziałają z największą liczbą protokołów transportowych, ponieważ informacje mogą być w nich przesyłane w formie ciągłego strumienia (stałe lub okresowo) lub w porcjach, takich jak pakiety. Dzięki temu, że punkty końcowe „zawłaszczają” obwód (przynajmniej na czas trwania sesji), dane mogą być transportowane w dowolny sposób, rozumiały dla obydwu punktów końcowych.

Aby pakiety były poprawnie wysyłane i odbierane, danym (polu ładunkowemu) muszą towarzyszyć dodatkowe informacje, takie jak adresy, sumy kontrolne i wartości wyznaczające prawidłową sekwencję pakietów. Proces dołączania wspomnianych informacji jest nazywany *ramkowaniem* lub *ramkowaniem pakietu*. Z kolei przygotowane do wysłania dane nazywają się *ramkami*. Zatem pakietyzacja polega na dzieleniu danych na porcje, a ramkowanie wiąże się z nadawaniem im odpowiedniego formatu.

Należy pamiętać, że przełączanie pakietów wymaga również komponentu przetwarzania komunikatów. Komunikaty podlegają pakietyzacji, ale mogą się składać z samych poleceń (bez danych). Niemniej ramki komunikatów zawsze będą zawierały dane w odpowiedniej otoczce.

Termin *pakiet* jest wykorzystywany w odniesieniu zarówno do stanowych, jak i bezstanowych połączeń. Opisuje bowiem tylko proces dzielenia danych (nic poza tym). Z kolei termin *datagram* znajduje zastosowanie jedynie w odniesieniu do technologii bezstanowych, czyli takich, w których usługi są uznawane za zawodne. Na potrzeby tych rozważań można przyjąć, że zawodne usługi to takie, które wymagają generowania komunikatów na każdym etapie procesu komunikacji.



W rozdziale 17. został opisany protokół kontroli transmisji (TCP) oraz protokół dostarczania datagramów użytkownika (UDP). W rozdziale 18. znajduje się omówienie protokołu internetowego (IP). W rozdziałach tych została zawarta również szczegółowa charakterystyka stanowej i bezstanowej komunikacji oraz związanych z nią mechanizmów komunikacyjnych.

Niezawodna usługa pakietowa może (ale nie musi) przysyłać zwrotne komunikaty potwierdzające poprawny odbiór danych. Jednak zawodna usługa zawsze generuje komunikaty zwrotne, dostarczane do systemu wysyłającego informacje. Co więcej, usługa tego typu może również wysyłać komunikaty do każdego węzła pośredniczącego w przekazywaniu pakietu lub ramki. W przypadku współdziałania protokołów TCP i IP świadczenie usług należy uznać za niezawodne. Stos TCP/IP został zaprojektowany w sposób dający gwarancję dokładnego odtworzenia przesyłanych danych w punkcie odbiorczym. Z założenia mechanizm TCP/IP jest wolniejszy w działaniu od technik, które nie wymuszają niezawodnego dostarczania informacji lub nie zapewniają odpowiedniej jakości obsługi.

Chcąc ocenić wpływ mechanizmu generowania komunikatów na poszczególnych etapach transmisyjnych, można użyć polecenia `TRACERT` (dla systemu Windows lub `tracert` w systemach UNIX, Linux czy Cisco IOS-ie). Tworzy ono tabelę komunikatów ICMP, zwracanych przez każdy węzeł na trasie pakietu (wysłanego przez polecenie `PING`) do jednostki docelowej.

Z kolei protokół UDP zastosowany w połączeniu z protokołem IP odpowiada za powstanie zawodnej usługi sieciowej. Zgodnie z założeniami protokołu UDP dane są przekazywane w formie pakietów, ale bez konieczności dokładnego odtworzenia ich w węźle docelowym. Protokół UDP znajduje zastosowanie w strumieniowaniu danych multimedialnych, w których utrata pewnej porcji informacji nie ma znaczenia dla całości transmisji. Podczas emisji filmu (w czasie której w ciągu sekundy generowanych jest ponad 30 obrazów) utrata jednej klatki lub wyświetlenie jednej klatki w niewłaściwej kolejności są niezauważalne. Przeznaczenie datagramu można łatwo zapamiętać, jeśli zwróci się uwagę, że litera *D* w akronimie UDP odpowiada *datagramowi* oraz że ten rodzaj technologii jest stosowany w strumieniowaniu muzyki i sekwencji wizyjnych. W przypadku każdej transmisji strumieniowej wykorzystywane są *datagramy*. Choć ewentualne omyłkowe użycie terminu *ramka* lub *pakiet* nie zostanie zauważone przez większość osób. Różnica jest nieznaczna, ale warto o niej pamiętać.

## Magistrale

Logicznym rozszerzeniem połączenia punkt-punkt jest zbiór połączeń punkt-punkt tworzących magistralę, czyli łańcuch węzłów korzystających ze wspólnego medium transmisyjnego (zagadnienie to zostało opisane w rozdziale 1.). Rozwiązania tego typu były stosowane we wczesnych wersjach sieci Ethernet, a dokładniej w wersjach 10Base5 (bazującej na odcepach od kabla magistralnego) oraz 10Base2 (wymagającej zastosowania złączy BNC).

W architekturze tej magistrala wyznacza segment sieci składający się z logicznego podzbioru węzłów sieciowych. Segmenty sieci nie tylko współdzielą jedną przestrzeń adresową, ale stanowią również granice dla komunikatów rozgłoszeniowych i reprezentują ten fragment sieci, w którym dochodzi do kolizji. Aby ograniczyć liczbę kolizji oraz zmniejszyć obciążenie łącza, projekt sieci musi zapewniać, że sygnały transmitowane w segmencie sieci będą odbijane na końcach segmentu i przesyłane ponownie wzdłuż medium transmisyjnego. Odpowiada za to mechanizm wytłumiania sygnału. W kolejnych punktach tego podrozdziału zostaną opisane same segmenty sieci, a także domeny kolizyjne oraz zasady tłumienia sygnału.

## Segmenty sieci

Magistralę można postrzegać jako segment lub zbiór segmentów sieciowych o wspólnych parametrach sieciowych, które mogą się ze sobą komunikować przy jak najmniejszym narzucie transmisyjnym. W każdym rodzaju sieci wyróżnia się przynajmniej jeden segment sieci. W najprostszym przypadku segment składa się z dwóch lub większej liczby komputerów przyłączonych do jednego medium fizycznego. Ponieważ segment sieci stanowi podstawową jednostkę sieciową, warto poświęcić chwilę na zapoznanie się z jego definicją oraz charakterystycznymi cechami.

W niektórych przypadkach segment sieci jest pojedynczym połączeniem punkt-punkt. Jednak znacznie częściej obejmuje wiele połączeń punkt-punkt. Niektóre urządzenia sieciowe, takie jak koncentratory i regeneratory, zwiększają obszar segmentu, włączając do niego wszystkie dochodzące do tego urządzenia połączenia. W sieciach magistralnych wykorzystujących technikę przekazywania znacznika segment sieci jest definiowany jako warstwa fizyczna między dwoma jednostkami dostępu do medium. Ponieważ działanie takich sieci bazuje na założeniu, że znacznik jest przekazywany między jednostkami od początku magistrali do jej końca, cała sieć jest uznawana za jeden segment.

Definicja segmentu sieci, jako obszaru, w którym poszczególne systemy współdzielą fizyczne medium, nie jest dostatecznie uniwersalna. Niekiedy segmentami sieciowymi określane są te obszary sieci, w których poszczególne systemy mogą się komunikować między sobą na poziomie warstwy łącza danych. Oznacza to, że jeden system może wymieniać informacje z innym na podstawie adresów MAC. Kolejny sposób wyznaczenia segmentu sieci sprawdza się do uznania go za zbiór systemów, które wymieniają między sobą komunikaty w sposób rozgłoszeniowy lub które należą do jednej podsieci.

Ponieważ podsieć wyznaczają wszystkie systemy o jednakowym prefiksie IP (wykorzystywanym w routingu), wszystkie systemy w podsieci należą do jednej domeny rozgłoszeniowej. Każdy system funkcjonujący w podsieci powinien mieć możliwość odwołania się (na przykład za pomocą polecenia PING) do innego systemu w tej samej podsieci. Z założenia routery rozdzielają dwa połączenia na niezależne segmenty sieciowe. Domena rozgłoszeniowa jest więc ograniczana przez każde urządzenie warstwy sieciowej (warstwy 3.), na przykład przez router.



Domena kolizyjna jest ograniczana przez dowolne urządzenie warstwy łącza danych (warstwy 2.), takie jak przełącznik. Domena rozgłoszeniowa jest natomiast wyznaczana przez urządzenia warstwy sieciowej (warstwy 3.), na przykład przez router. Szczegółowy opis modelu OSI znajduje się w rozdziale 2.

Ponieważ każda podsieć jest wydzielana na podstawie prefiksu wykorzystywanego w routingu, teoretycznie każde połączenie wychodzące z routera powinno wyznaczać niezależną trasę. Jest to oczywiście prawdą na poziomie warstwy fizycznej. Jednak podsieci definiuje się na poziomie protokołu wyższej warstwy — warstwy sieci modelu OSI lub warstwy internetowej modelu TCP/IP. Nic nie stoi na przeszkodzie, aby systemy przypisane do jednej podsieci były umiejscowione po dwóch stronach routera (przy założeniu, że adresy poszczególnych systemów są niepowtarzalne). Zatem mimo że w większości przypadków ze względów wydajnościowych każda podsieć jest skojarzona z jednym interfejsem routera, takie rozwiązanie nie zawsze musi być stosowane. Warto o tym pamiętać.

Podział podsieci na grupy jednostek i przyłączenie ich do różnych interfejsów routera powoduje wpisanie poszczególnych grup do różnych domen rozgłoszeniowych. Z tego względu stosowany w książce termin *domena rozgłoszeniowa* odnosi się do grupy systemów, które mogą odbierać komunikaty rozgłoszeniowe od innych systemów, co nie jest tożsame z wydzieleniem podsieci.

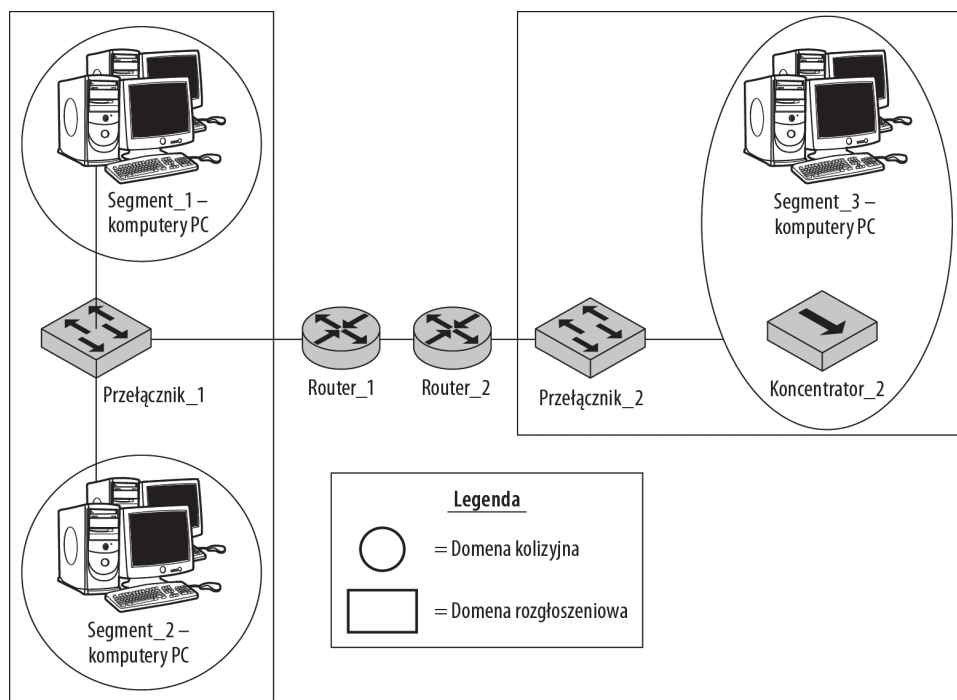
## Domeny kolizyjne

Umiejętność wyznaczania granic segmentu sieci, szczególnie w sieciach Ethernet, jest niezwykle istotna, gdyż wiąże się ona z określaniem *domeny kolizyjnej*. Domena kolizyjna obejmuje tę część fizycznej warstwy sieci, w której może wystąpić kolizja. Granicę domeny kolizyjnej wyznaczają urządzenia warstwy łącza danych (warstwy 2.), takie jak przełączniki. Projektując sieć, należy pamiętać o tym, aby obszar jednego segmentu sieci był jak najbardziej ograniczony, co spowoduje zmniejszenie ryzyka wystąpienia kolizji pakietów. W sieciach token ring oraz token bus w danym czasie tylko jeden węzeł może się komunikować z innym węzłem sieci. Prawdopodobieństwo wystąpienia kolizji jest więc znikome, a pojęcie domeny kolizyjnej nie ma zastosowania. Ogólna zasada stanowi, że domeny kolizyjne są obszarowo mniejsze od domen rozgłoszeniowych i się w nich zawierają.

Przykłady domen kolizyjnych i domen rozgłoszeniowych zostały przedstawione na rysunku 3.6. Domeny kolizyjne oznaczono za pomocą okręgów, natomiast domeny rozgłoszeniowe za pomocą prostokątów. W lewej części rysunku znajdują się dwie domeny kolizyjne opisane jako Segment\_1 i Segment\_2. Stanowią one dwie podsieci rozdzielone przełącznikiem. Każda z tych podsieci dysponuje własnym adresem logicznym (adresem podsieci) i jest ograniczona urządzeniem warstwy łącza danych (warstwy 2.) wyznaczającym domenę kolizyjną. Domena kolizyjna opisana jako Segment\_3 obejmuje również Koncentrator\_2, ponieważ koncentrator jest urządzeniem warstwy fizycznej (warstwy 1.). Domeny rozgłoszeniowe rozciągają się na obszarze podsieci, a ich granice są wyznaczane przez routery, czyli urządzenia warstwy sieciowej (warstwy 3.).

Kolizje występują w sieciach wykorzystujących wspólne medium transmisyjne. Określenie *wspólne* odnosi się do współdzielenia kabli połączeniowych oraz pasma transmisyjnego. Zgodnie z informacjami zamieszczonymi wcześniej istnieje bowiem wiele technik przekazywania znacznika, które regulują dostęp do sieci. Systemy tego rodzaju bazują na założeniu, że określony węzeł przesyła cały strumień danych do innego urządzenia docelowego. Oznacza to, że w czasie, gdy ma on dostęp do sieci, dysponuje dedykowanym mu obwodem i może realizować transakcje z dużą przepustowością. Dedykowany obwód umożliwia przekazywanie informacji tylko z jednego punktu końcowego lub węzła sieci. Dane docierają do odbiorcy w odpowiedniej kolejności i wymagają zastosowania mniej restrykcyjnych procedur weryfikacji poprawności. Jednak nie wszystkie sieci działają w opisany sposób. I nie zawsze takie działanie jest pożądane.

Kolizja występuje wtedy, gdy jeden z punktów końcowych lub węzłów przed odebraniem całego przekazu z pewnego węzła odbierze sygnał emitowany z innego źródła lub gdy sygnał emitowany z innego źródła nałoży się na transmisję z pierwszego źródła. W każdym rodzaju sieci rejestruje się pewien poziom błędów wynikających z kolizji. Z tego względu system transportu danych każdego rodzaju sieci uwzględnia pewne mechanizmy weryfikacji spójności odbieranych informacji. Wyjątkiem od tej reguły są obwody dwukierunkowe, w których



**Rysunek 3.6.** Przykład sieci z wydzielonymi domenami kolizyjnymi i domenami rozgłoszeniowymi

ruch jest przenoszony w obydwu kierunkach jednocześnie w sposób niezależny od siebie. Wraz ze wzrostem natężenia ruchu rośnie procentowa wartość kolizji, co w konsekwencji prowadzi do istotnego zmniejszenia wydajności sieci.

Aby uniknąć kolizji, w niemal wszystkich protokołach sieciowych zaimplementowano moduł obsługi komunikatów, które potwierdzają poprawne dostarczenie danych lub wymuszają wykonanie retransmisji w ramach każdej wymiany informacji. Za wykrywanie kolizji odpowiadają różne rozwiązania. Dwa najczęściej stosowane to:

- ♦ **Wielodostęp z wykrywaniem nośnej i detekcją kolizji (CSMA/CD — *Carrier Sense Multiple Access with Collision Detection*)**. Jest to mechanizm stosowany w wielu sieciach przewodowych, w tym w Ethernetie opisanym w standardzie IEEE 802.3. Zakłada on, że każdy z węzłów nasłuchuje (wykrywanie nośnej) ruchu w kanale, oczekując na chwilę ciszy przed przystąpieniem do nadawania nowych danych.
- ♦ **Wielodostęp z wykrywaniem nośnej i unikaniem kolizji (CSMA/CA — *Carrier Sense Multiple Access with Collision Avoidance*)**. W tym rozwiązaniu węzeł sygnalizuje sieci, że zamierza rozpocząć transmisję danych przed rzeczywistym przystąpieniem do nadawania. Unikanie kolizji jest mechanizmem wolniejszym niż detekcja kolizji, ponieważ uwzględnia dodatkowy etap w procedurze transmisji danych.

Obydwie wersje protokołu CSMA zostały szczegółowo omówione w rozdziałach 12. (CSMA/CD w Ethernetie) i 14. (CSMA/CA w WiFi).



## Wytłumianie sygnału

Jeżeli połączenie sieciowe nie zostało poprawnie skonfigurowane, można rejestrować wysoką stopę błędów nawet w przypadku ruchu o małym natężeniu. Wiele technologii sieciowych (np. magistrale systemowe) wymaga odpowiedniego zakończenia segmentów w punktach końcowych. Niewłaściwe przygotowanie zakończenia może skutkować odbijaniem sygnału i powstawaniem kolizji. Rozwiązanie polega na zmniejszeniu siły sygnału do poziomu, w którym amplituda odbitego impulsu będzie niższa od poziomu akceptacji sygnału, co w konsekwencji doprowadzi do zignorowania tego sygnału.

Jedną z cech dedykowanych obwodów jest to, że w czasie, gdy obwód nie jest wykorzystywany, związana z nim szerokość pasma jest marnowana. Z kolei stosowanie obwodu dedykowanego wiąże się z koniecznością zapewnienia ciągłej jego dostępności w celu zagwarantowania określonego poziomu obsługi. Rozwiązanie to nie jest więc właściwe, gdy chcemy maksymalnie wykorzystać pasmo sieci lub gdy przesyłamy dane w łączach o zmiennej jakości. Problem ten został zauważony przez twórców internetu i zmusił ich do opracowania stosu TCP/IP. W mechanizmie TCP/IP dane są transmitowane w porcjach najlepszą w danej chwili trasą i podlegają retransmisji w razie konieczności. Pakiety odbierane w urządzeniu docelowym są ustawiane w odpowiedniej kolejności i weryfikowane. Rozwiązanie to zapewnia maksymalne wykorzystanie pasma oraz odporność na błędy za cenę dodatkowego narzutu transmisyjnego.

Istnieją również technologie sieciowe, w których nie występują ani domeny rozgłoszeniowe, ani domeny kolizyjne. Ich działanie bazuje na ustanawianiu pojedynczego dedykowanego łącza, inicjowanego zazwyczaj na poziomie warstwy łącza danych (warstwy 2.). Przykładami takich technologii są sieci VPN oraz protokół PPP. Połączenia PPP uwzględniają procedurę uwierzytelniania, a przekazywane w ramach nich dane podlegają kompresowaniu i szyfrowaniu. Mogą być realizowane w ramach różnych połączeń fizycznych, od skrętki nieekranowanej, przez linie telefoniczne, kable szeregowe, łącza telefonii komórkowych, włókna światłowodowe, po sieci optyczne SDH. Nie wyróżnia się w nich domen kolizyjnych, ponieważ punkt końcowy komunikacji jest punktem końcowym łącza PPP. Brak domeny kolizyjnej wynika natomiast z tego, że łącze ma charakter dedykowany, a protokół PPP nie obsługuje rozgłoszeń. Choć informacje przenoszone w zaszyfrowanej ramce PPP mogą zawierać adres rozgłoszeniowy, jest on interpretowany przez system docelowy.

## Punkty przyłączeniowe

Topologia magistrali jest obecnie stosowana w niewielu już technologiach sieciowych. Przyczyną jest znaczne obniżenie cen przełączników i routerów. Przełączniki i router są bowiem elementami, do których może być podłączonych wiele punktów końcowych. Rozwiązania magistralne mają natomiast ograniczone możliwości rozszerzania sieci. Nie są dostatecznie elastyczne w tym względzie. W większości sieci stosowane są różne urządzenia przyłączeniowe, w tym koncentratory, regeneratory, przełączniki, routery i bramy. Każdy z wymienionych komponentów został szczegółowo opisany w rozdziale 9. Niemniej na potrzeby rozważań prowadzonych w tej części książki warto zapoznać się z informacjami na temat wnoszonej przez nie elastyczności w projektowaniu architektury sieciowej.



Koncentratory, regeneratory, przełączniki, routery i bramy zostały opisane w rozdziale 9. Z kolei sieci token ring są tematem rozdziału 12.

Koncentratory są najmniej skomplikowanymi urządzeniami sieciowymi. Ich zadanie polega na rozszerzaniu segmentu sieciowego. Wszystkie urządzenia przyłączone do koncentratora pracują w tym samym segmencie sieci. Koncentrator jako urządzenie warstwy fizycznej można traktować jako element zapewniający przedłużenie kabla sieciowego. Sygnały elektryczne są przekazywane przez złącza o niewielkiej rezystancji bez jakichkolwiek strat. Biorąc pod uwagę topologię sieci, koncentratory są elementami tworzącymi gwiazdy, lecz mogą być również łączone w strukturze drzewiastej. Regenerator jest pewną odmianą koncentratora, który zapewnia odtwarzanie sygnału. Do segmentu zawierającego koncentrator odnoszą się wszystkie informacje o domenach kolizyjnych prezentowane we wcześniejszej części rozdziału.

Przełączniki mogą być urządzeniami warstwy łącza danych (warstwy 2.) lub warstwy sieciowej (warstwy 3.). Separują fizycznie kilka segmentów sieci. Routery z kolei są przełącznikami, które zostały wyposażone w funkcje wyznaczania tras dla danych za pomocą odpowiednich protokołów i algorytmów wykonywanych w ich systemie. Dane na temat tras (dane o routingu) są generowane w routerze, przekazywane między routerami, a następnie przechowywane w pamięci operacyjnej lub trwałej. Trasa jest określoną ścieżką przekazywania danych w sieci między jednostką źródłową a docelową. W przypadku przełącznika lub routera trasa zdefiniowana w jego systemie jest trasą od tego urządzenia do punktu końcowego. Sama trasa składa się z wielu etapów (skoków), które odpowiadają poszczególnym segmentom sieci.

Przełączniki i routery są urządzeniami najpowszechniej stosowanymi w dzisiejszych sieciach komputerowych. Nadają tym sieciom niezwykłą elastyczność w konfiguracji, umożliwiają przyłączanie kolejnych węzłów, gwarantują niezawodną pracę sieci (dzięki zmianie tras w zależności od bieżącego stanu sieci). Routery dodatkowo zapewniają optymalizację i adaptację tras, którymi są przekazywane informacje. W przypadku sieci złożonych jedynie z przełączników routing można zrealizować za pomocą komputerów. Jednak w sieciach wyposażonych w routery wybór tras dla danych jest realizowany właśnie w tych urządzeniach.

Optymalizacja tras jest operacją niezbędną, gdy między dwoma punktami końcowymi występuje kilka ścieżek, których część może być niedostatecznie szybka w działaniu lub nawet chwilowo niedostępna. W zależności od zastosowanego algorytmu wykorzystywanych jest wiele metod optymalizacji routingu. Niektóre rozwiązania bazują na czasie przesyłania pakietów. Inne uwzględniają liczbę segmentów sieci, które muszą zostać pokonane przez porcję danych, bądź wyznaczają trasę o maksymalnej przepustowości. W większości przypadków wynikiem optymalizacji jest wskazanie trasy o największej szybkości przekazywania informacji lub trasy zapewniającej największą przepustowość. Administrator routera ma również możliwość osobistego wprowadzania lub modyfikowania informacji o trasach przez operowanie statycznymi tablicami routingu.

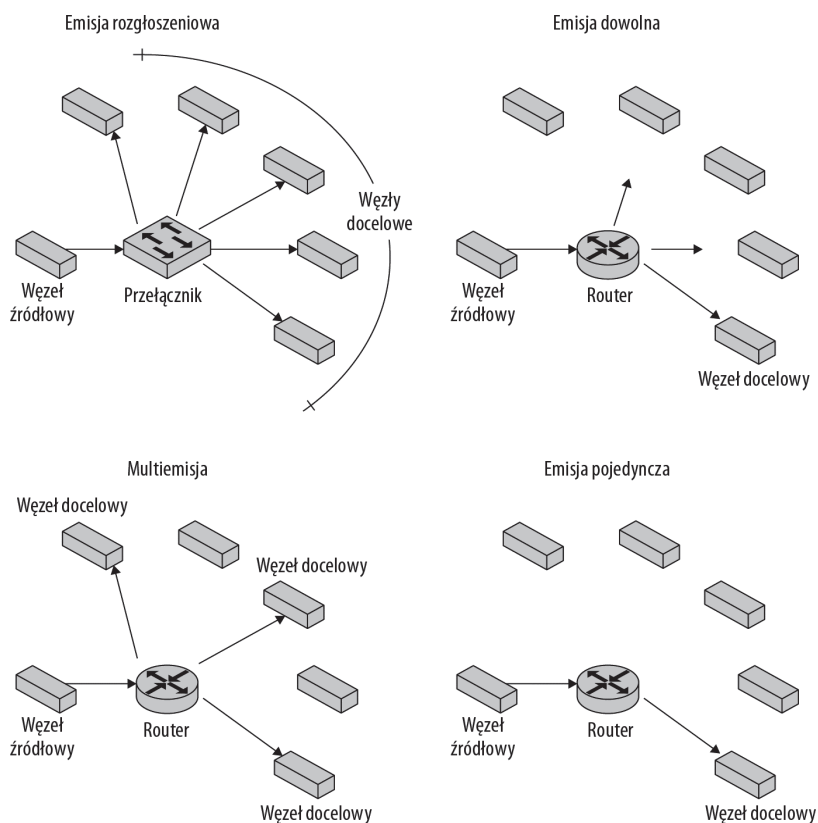


Routing statyczny został opisany w rozdziale 9.

Wyróżnia się cztery następujące topologie routingu:

- ♦ **Emisja pojedyncza (ang. *unicast*) („jeden do jednego”).** Jest to transmisja, w której jeden punkt końcowy przekazuje informację do innego punktu końcowego. W transmisji typu unicast informacje docierają do pojedynczego systemu docelowego niezależnie od tego, czy prowadzi do niego jedna trasa, czy wiele tras.
- ♦ **Emisja rozgłoszeniowa (ang. *broadcast*) („jeden do wszystkich”).** Transmisja rozgłoszeniowa jest adresowana do wszystkich systemów funkcjonujących w sieci (zazwyczaj w segmencie sieci), które mają możliwość odebrania komunikatu. Rozgłoszenia są zazwyczaj ograniczane do jednego segmentu sieci, ponieważ zajmują znaczną szerokość pasma transmisyjnego.
- ♦ **Multiemisja (ang. *multicast*) („jeden do wielu”).** Multiemisja polega na dostarczaniu komunikatu do grupy węzłów, które wcześniej przyłączyły się do wspomnianej grupy za pomocą mechanizmu rejestracji.
- ♦ **Emisja dowolna (ang. *anycast*) („jeden do dowolnego”).** Transmisja tego typu sprowadza się do przesłania komunikatu do najbliższego (najlepszego) urządzenia docelowego. Odpowiedź na komunikat jest generowana przez pojedynczy system.

Poszczególne techniki routingu zostały przedstawione na rysunku 3.7.



**Rysunek 3.7.** Cztery podstawowe techniki routingu

Bramy są urządzeniami warstwy aplikacji (warstwy 7.). Wykorzystuje się je do łączenia dwóch różnych rodzajów sieci na dowolnym poziomie modelu odniesienia. Znajdują zastosowanie na przykład w łączeniu sieci Apple Talk lub IPX z sieciami TCP/IP (choć w praktyce większość systemów Apple Macintosh i Novell Netware współdziała z protokołami TCP/IP). Bramy stanowią również element pośredniczący w działaniu aplikacji, na przykład zapewniając przekazywanie ruchu z serwera WWW do serwisu elektronicznego handlu.

Sieci magistralne są sieciami otwartymi, w których nie występują zamknięte trasy. Niemniej wciąż budowanych jest wiele sieci pierścieniowych. Do najczęściej wykorzystywanych rozwiązań tego typu należą sieci IBM token ring oraz FDDI. Gdyby nie marketing, nadal używalibyśmy sieci token ring zamiast Ethernet. Ale to już zupełnie inna historia. Pierścienie mogą być tworzone na wiele różnych sposobów. W rozwiązaniach token ring często okablowanie jest realizowane w sposób odpowiadający gwiazdzie, w której węzły (stacje) są połączone z koncentratorami. Jeden kabel doprowadzony do koncentratora wprowadza dane do pierścienia, a inny kabel wyprowadza je z pierścienia. W topologii pierścienia występuje pojedyncza domena kolizyjna i teoretycznie jeden segment sieci.

Awaria jednego połączenia powoduje przerwanie pierścienia i uszkodzenie segmentu sieci. Aby nie dopuścić do wystąpienia takiego problemu, w instalacjach pierścieniowych są wyznaczane zapasowe pierścienie oraz jednostki MAU. Wiele sieci jest budowanych z wykorzystaniem dwóch pierścieni. Drugi pierścień odgrywa wówczas rolę dodatkowej trasy lub służy jako ścieżka zapasowa na wypadek wystąpienia awarii. W rozwiązaniu token ring stosowane są urządzenia, które firma IBM nazwała jednostkami dostępowymi dla wielu stacji (MAU — *Multistation Access Unit*). Urządzenie MAU działa w warstwie łącza danych (warstwie 2.). Jego zadanie polega na utworzeniu logicznego pierścienia w sieci o fizycznej topologii gwiazdy.

Aby uniknąć kolizji, w sieci wykorzystywana jest technika regulowania dostępu do medium przez *przekazywanie znacznika* (ang. *token passing*). Podczas gdy znacznik jest przekazywany przez sieć, każdy węzeł, który odbierze znacznik, porównuje własną wartość priorytetu z wartością zapisaną w znaczniku. Po zakończeniu przesyłania informacji z jednego węzła odbiór znacznika umożliwia innemu węzłowi rozpoczęcie nowej komunikacji. Technika przekazywania znacznika zapewnia dostęp do sieci tylko jednemu węzłowi w danej chwili. Jednak gdy węzeł ten rozpocznie transmitowanie danych, może realizować swoje zadanie z pełną przepustowością sieci, wykorzystując całe dostępne pasmo.

## Sieci jednostek równorzędnych (peer-to-peer)

Sieci jednostek równorzędnych (peer-to-peer, P2P) są pierwszymi z grupy architektur sieciowych, które zostaną przeanalizowane pod względem projektowym. Rozwiązania przedstawione wcześniej (w tym sieci magistralne) mogą być postrzegane jako zbiór niezwiązanych ze sobą połączeń. Sieci P2P są natomiast opracowywane jako logiczne rozszerzenie zbioru łączy punkt-punkt. Implementacje P2P mogą obejmować dowolną liczbę różnych technologii, włącznie z mechanizmami budowania sieci „w locie”, czyli tworzenia połączeń ad hoc. Najważniejszym wyróżnikiem tego, czy dana sieć jest rozwiązaniem P2P, czy instalacją o innej architekturze, jest sposób uczestnictwa węzła w interakcjach sieciowych. W sieciach P2P poszczególne węzły są równorzędnymi partnerami w przetwarzaniu danych.

Szczegółowe informacje na ten temat zostały zamieszczone w rozdziale 11. Niemniej warto zapoznać się z podstawowymi zagadnieniami związanymi z połączeniami P2P, ponieważ posłużą one jako odniesienie do omawianych w dalszej części rozdziału architektur klient-serwer, X-Architecture oraz architektur wielowarstwowych.



Topologie sieciowe (w tym magistrale, pierścienie, siatki i połączenia hybrydowe) stosowane w różnych architekturach sieciowych zostały opisane w rozdziale 1.

Pojęcie sieci peer-to-peer ma różne znaczenie w zależności od kontekstu użycia terminu. Firma Microsoft do opisu sieci jednostek równorzędnych stosuje termin *grupy roboczej*. Do usług funkcjonujących w ramach zależności peer-to-peer zalicza się usługi zabezpieczenia sieci, współdzielenia plików i drukarek oraz udostępniania połączenia internetowego. W grupie roboczej Windows wspólne zasoby sieciowe mogą być wykorzystywane jedynie przez jednostki należące do tej grupy roboczej i posługujące się protokołem TCP/IP. Oprócz grup roboczych firma Microsoft opracowała również koncepcję domen, których działanie opiera się na usługach katalogowych.

Po dokładniejszym przeanalizowaniu sposobu działania grup roboczych Windows można dojść do wniosku, że funkcje serwerowe są rozdzielane między jednostki członkowskie grupy roboczej podczas ich przyłączania do grupy (i wykorzystywania udostępnionych zasobów, np. plików lub drukarek) bądź w czasie, gdy jednostka komunikuje się z pierwszym systemem grupy (np. w celu sprawdzenia, czy jest dostępna usługa przeglądania sieci). Firma Microsoft nakłada pewne ograniczenia na liczbę jednoczesnych połączeń z jednostkami grupy roboczej, przez co osobisty serwer WWW może obsługiwać tylko 10 połączeń w danej chwili. Systemy Windows przeznaczone dla użytkowników końcowych są zubożonymi wersjami serwerowych systemów operacyjnych i zawierają ograniczenia funkcjonalne w wielu istotnych obszarach działania.

Aby zintensyfikować wrażenie różnic między poszczególnymi wersjami systemów operacyjnych, firma Microsoft implementuje w nich różne zestawy modułów i rozszerzeń. W rzeczywistości wersje systemów nie są od siebie aż tak odmienne. Osoby, które poświęcą trochę czasu na instalowanie komponentów interfejsu użytkownika, włączanie dodatkowych funkcji i zmianę sposobu działania niektórych usług, mogą doprowadzić system Windows Server do stanu, w którym dla postronnego obserwatora nie będzie się niczym różnił od wersji desktop. Zatem mimo że grupy robocze wydają się rozwiązaniami typu peer-to-peer, w rzeczywistości stanowią rozproszony system klient-serwer. Prawdziwe aplikacje P2P wykorzystują inne systemy jako źródła danych, a następnie przetwarzają dane lokalnie.

Wiele osób nie uznaje tej definicji, twierdząc, że równorzędność węzłów sieci P2P przejawia się tym, że mogą one funkcjonować zarówno jako jednostki klienckie, jak i serwerowe. Analiza sposobu działania takich aplikacji P2P, jak BitTorrent lub Kazaa, prowadzi do wniosku, że niektóre funkcje przez nie realizowane są typowymi relacjami P2P, ale jednocześnie do wykonywania innych zadań wykorzystywany jest model klient-serwer. W sieciach P2P stosowane są modele: scentralizowany (nadzorowany przez serwer), zdecentralizowany, strukturalny, ustrukturyzowany i nieustrukturyzowany, a także hybrydowe połączenia wymienionych opcji.



Architektura niektórych powszechnie stosowanych aplikacji P2P (takich jak BitTorrent i Kazaa) została omówiona w rozdziale 11.

## Sieci klient-serwer

Sieć klient-serwer stanowi implementację dwuwarstwowej architektury, w której system serwerowy przetwarza dane wykorzystywane przez system kliencki lub wiele systemów klienckich. Rozwiązania klient-serwer są obecnie najczęściej wdrażanymi formami rozproszonego przetwarzania danych i znajdują zastosowanie w wielu aplikacjach sieciowych, takich jak bazy danych, poczta elektroniczna, serwisy WWW i inne typowe usługi internetowe. W modelu klient-serwer obowiązuje założenie, że na serwerze jest uruchomione odpowiednie oprogramowanie serwerowe, natomiast w systemie klienckim działa specjalne oprogramowanie klienckie. Ważne jest to, że obydwie wersje oprogramowania wykonują zadania na podstawie zupełnie innego kodu lub mają wspólny kod, ale realizujący odmienne funkcje.

Wzajemne rozmieszczenie jednostek klienckich i serwerów nie jest w żaden sposób ograniczane, jeśli tylko będą się one mogły komunikować. W większości przypadków aplikacje klienckie i serwerowe działają w różnych systemach. Choć niekiedy mogą pracować również w jednym systemie.

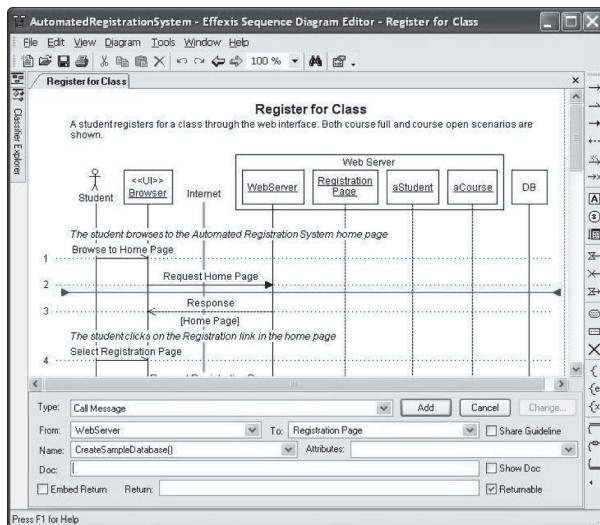
Aby aplikacja klient-serwer działała poprawnie, żądania realizacji usługi muszą być dostarczane do serwera za pośrednictwem odpowiedniego protokołu. Musi również istnieć protokół, który zapewni przekazywanie danych między serwerem i klientem. Zazwyczaj zadania te realizuje jeden zuniifikowany mechanizm, na przykład HTTP, SNMP, Java RMI, .NET Remoting, TCP, UDP, gniazda, WCF lub CORBA.

W wielu publikacjach interakcje typu klient-serwer opisuje się w formie diagramów sekwencji (z uwzględnieniem kolejności komunikatów i relacji między nimi), które są zapisywane w plikach o standardowym formacie, przeznaczonym do wymiany danych. Zamiast terminu *diagram sekwencji* często można przeczytać określenie *diagram czasowy* lub *diagram zdarzeń*. Obecnie diagramy sekwencji są najczęściej zapisywane w plikach zuniifikowanego języka modelowania (UML — *Unified Modeling Language*). Na rysunku 3.8 został przedstawiony przykładowy diagram sekwencji wygenerowany w programie Sequence Diagram Editor firmy Effexis Software (<http://www.sequencediagrameditor.com>). Zarówno to narzędzie, jak i wiele innych o podobnym zakresie działania umożliwia graficzne opracowanie sekwencji zdarzeń, a następnie zapisanie ich w formie pliku UML.

W typowej architekturze klient-serwer istnieje wyraźny podział na działania klienckie i serwerowe. Klient może zainicjować żądanie i przetworzyć odpowiedź po jej odebraniu. Aplikacja generująca żądanie musi oczekiwać na reakcję serwera. Choć jednostka kliencka może być połączona z wieloma serwerami jednocześnie, często twórcy oprogramowania narzucają ograniczenia w liczbie połączeń w celu zachowania odpowiedniej wydajności narzędzia. Na przykład przeglądarka Microsoft Internet Explorer może utworzyć cztery połączenia, którymi będzie zarządzała, a aplikacja Apple iTunes dopuszcza jedynie trzy równoległe połączenia. Ponieważ operacje realizowane po stronie klienckiej wymagają zazwyczaj interakcji użytkownika, programy klienckie często udostępniają graficzny interfejs użytkownika (GUI — *Graphical User Interface*).

Określenie „serwer” odnosi się do aplikacji, programu lub modułu oprogramowania, które na żądanie mogą dokonać pewnego przetwarzania danych. „Serwerem” nazywa się również urządzenie, w którego systemie wykonywany jest jeden z wymienionych rodzajów oprogramowania. Konfiguracja serwerów polega na wykorzystaniu specjalnych narzędzi konfiguracyjnych

**Rysunek 3.8.**  
*Program Sequence  
 Diagram Editor firmy  
 Effexis Software*



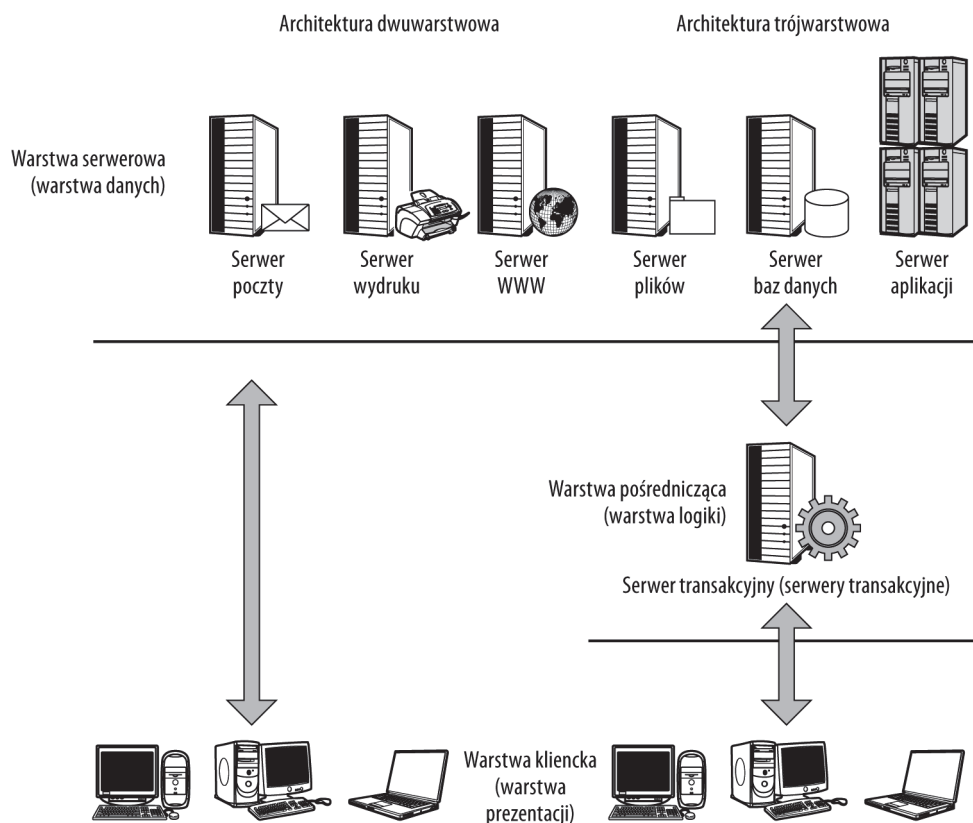
— czasami są to aplikacje GUI, a częściej programy wiersza poleceń. W czasie działania serwer powołuje proces zwany usługą. Usługi związane z funkcjonowaniem systemu operacyjnego są najczęściej zarządzane za pośrednictwem odpowiedniego narzędzia, wchodzącego w skład systemu operacyjnego serwera.

Na przykład usługi systemu Windows Server są obsługiwane za pośrednictwem konsoli MMC (po kliknięciu ikony *Usługi* w sekcji *Narzędzia administracyjne*) w późniejszych wersjach systemu lub bezpośrednio z poziomu panelu sterowania w wersjach wcześniejszych. Opcja *Usługi* jest również dostępna w programie *Zarządzaj tym serwerem* w Windows Server 2008. Gdy usługa jest elementem aplikacji (np. korporacyjnej bazy danych), dostawca oprogramowania często dołącza specjalne narzędzie lub konsolę, dzięki którym można konfigurować tę usługę, a także włączać ją i wyłączać. Usługę można ustawić w taki sposób, aby była wyłączona do czasu wylogowania użytkownika, a także by była włączana automatycznie wraz ze startem systemu lub po pewnym czasie (w Windows Server 2008) bądź była włączana osobiście przez administratora.

## Sieci wielowarstwowe

Architektura wielowarstwowa, nazywana czasami architekturą  $n$ -warstwową, jest pewną odmianą architektury klient-serwer, w której w transakcji między klientem a serwerem uczestniczą usługi pośrednie. W rozwiązaniach tego typu jednostka kliencka wymienia dane z serwerem pośredniczącym, a serwer pośredniczący komunikuje się z serwerem zasadniczym. Serwer końcowy przekazuje informacje do klienta również z wykorzystaniem serwera pośredniczącego. Przykładami oprogramowania pośredniczącego są różne serwery transakcyjne oraz platforma Java 2 Enterprise Edition.

Na rysunku 3.9 zostały przedstawione dwuwarstwowa architektura klient-serwer oraz architektura wielowarstwowa. Rozwiązanie trójwarstwowe jest najpowszechniej stosowaną implementacją architektury  $n$ -warstwowej. W modelu klient-serwer występują tylko dwie warstwy — kliencka i serwerowa. Z kolei w aplikacji trójwarstwowej podstawowe funkcje sieciowe są rozdzielone zgodnie z poniższymi założeniami.



**Rysunek 3.9.** Architektura dwuwarstwowa i trójwarstwowa

- ♦ Warstwa kliencka (warstwa prezentacji) zapewnia użytkownikowi możliwość operowania aplikacją i zarządzania systemem.
- ♦ Warstwa pośrednicząca (warstwa logiki) wymusza stosowanie określonych zasad logicznych oraz obsługuje interakcje użytkownika w formie niezależnych transakcji.
- ♦ Warstwa serwerowa (warstwa danych) składa się z serwerów aplikacji oraz usług, które zapewniają dostęp do zgromadzonych informacji.

Dodanie trzeciej warstwy do architektury klient-serwer jest źródłem wielu korzyści. Dzięki oddzieleniu jednostki klienckiej od serwera serwer pośredniczący może odgrywać rolę usługi translacji protokołów. Warstwa pośrednicząca sprawia, że jednostka kliencka i serwer są bardziej abstrakcyjnymi komponentami dla siebie nawzajem. Dzięki niej transakcje ustanowione z serwerem pośredniczącym mogą przetrwać utratę połączenia klienckiego lub serwerowego bądź wyłączenie któregośkolwiek z systemów. Same transakcje mogą być natomiast realizowane poprzez wymianę komunikatów zgodnie z modelem ACID (skrót ACID jest akronimem od słów *atomicity*, *consistency*, *isolation* i *durability*, oznaczających niepodzielność, spójność, izolację i trwałość transakcji). W przypadku awarii jakiegokolwiek komponentu w  $n$ -warstwowej architekturze takie transakcje są po prostu wycofywane. Model ACID zawiera bowiem definicje parametrów, które transakcja bazodanowa musi mieć, aby można było bezpiecznie przeprowadzić poprawnie zdefiniowaną operację logiczną.

Trójwarstwowe systemy są znacznie łatwiejsze w skalowaniu, zapewniają większą modularność projektu i dają możliwość aktualizowania systemu bez przerw w pracy. Wynika to z faktu odseparowania jednostki klienckiej od serwera. Gdy konieczne jest wprowadzenie istotnych poprawek lub zmian w sposobie funkcjonowania serwera pośredniczącego, wystarczy uruchomić nowy serwer, a następnie zmienić odwołania w programie klienckim i serwerze końcowym w taki sposób, aby odnosiły się do nowego systemu pośredniczącego. Często instalacje wielowarstwowe są uruchamiane z wykorzystaniem różnych systemów operacyjnych.

## Uproszczony klient-serwer

Ostatnim rodzajem architektury sieciowej, któremu warto poświęcić trochę uwagi, są połączenia klient-serwer i serwer-klient wykorzystujące uproszczone jednostki klienckie (ang. *thin client*). Uproszczony klient jest terminalem o obniżonym poborze mocy z podsystemami sieciowym i graficznym. Jednostki tego typu mogą być komputerami lub urządzeniami przenośnymi, w których został zainstalowany uproszczony system operacyjny, taki jak zubożony Linux, wbudowany system operacyjny czasu rzeczywistego (RTOS — *Real-Time Operating System*) lub Windows CE. Mogą to być również klasyczne komputery z oprogramowaniem klienckim. W przypadku uproszczonego klienta większość operacji związanych z przetwarzaniem danych jest wykonywana po stronie „serwera”. Zadaniem jednostki jest jedynie umożliwienie wprowadzania informacji oraz wyświetlanie danych.

Termin „serwer” został umieszczony w cudzysłowie, ponieważ obecnie stosuje się dwa różne rodzaje sieci klient-serwer. Obydwie wersje realizują zbliżone zadania. Pierwsza z nich to mechanizm X Window, który definiuje jako serwer aplikację uruchomioną w jednostce klienckiej i odwołuje się do serwera lub dostawcy danych jak do klienta. Rozwiązanie X Window służy do uruchamiania graficznych aplikacji w systemie klienckim, który odpowiada tylko za wyświetlanie informacji. Wszystkie pozostałe operacje związane z działaniem aplikacji są wykonywane po stronie serwera.

Drugi rodzaj połączeń uproszczonego klienta z serwerem pełni analogiczne zadania, ale stosuje się w nim inne konwencje nazewnictwa. Na przykład w modelu bazującym na serwerze terminali Windows jednostka kliencka jest stacją roboczą, która wyświetla obraz aplikacji na własnym monitorze. Również w tym przypadku serwer jest systemem odpowiedzialnym za całe przetwarzanie danych. Terminal Windows pobiera informacje graficzne wytworzone na serwerze i prezentuje je lokalnie. Najważniejsza różnica sprowadza się do tego, że stacja robocza jest klientem, podczas gdy w rozwiązaniu X Window stacja robocza jest uznawana za serwer (z uwagi na miejsce, z którego są generowane polecenia).

## Serwer terminali

Serwer terminali jest elementem sieci, w której występują uproszczone jednostki klienckie. Jego zadanie polega na wykonywaniu procesów inicjowanych przez poszczególne przyłączone do niego stacje. Najpowszechniej stosowane rozwiązania scentralizowanego przetwarzania danych obejmują serwer terminali Windows (usługę systemu Windows Server 2003/2008) oraz system Citrix XenApp (wcześniej Citrix MetaFrame — <http://www.citrix.com/English/ps2/products/product.asp?contentID=186>). Uruchomienie którejkolwiek z wy-

mienionych usług powoduje wydzielenie w pamięci serwera obszarów przeznaczonych dla systemów operacyjnych stacji roboczych, choć pewne moduły systemu operacyjnego — wspólne dla wszystkich egzemplarzy systemu operacyjnego stacji roboczych — są wykonywane we wspólnym obszarze pamięci. Dzięki temu serwer może obsługiwać jednocześnie wiele niezależnych sesji terminalowych.

Podczas nawiązywania połączenia między klientem a serwerem uruchamiany jest specjalny protokół transmisyjny, taki jak protokół zdalnego pulpitu (RDP — *Remote Desktop Protocol*) firmy Microsoft lub protokół niezależnej architektury obliczeniowej (ICA — *Independent Computing Architecture*) firmy Citrix. W obydwu przypadkach obraz pulpitu działającego po stronie serwera jest przesyłany w formie skompresowanej do uproszczonego klienta. Aplikacje i usługi są wykonywane w przestrzeni klienckiej na serwerze, a wyniki ich pracy są prezentowane użytkownikowi bez konieczności wymiany znacznych ilości danych.

Zgodnie z założeniami technologii bazujących na serwerach terminali, do obsługi wielu stacji roboczych wystarczy jeden dostatecznie wydajny serwer (wyposażony w odpowiednią ilość pamięci operacyjnej). To samo zadanie można jednak zlecić farmie serwerów, co pozwala na rozłożenie obciążenia na poszczególne systemy. Ponieważ serwer pozostaje pod kontrolą administratora sieci, a stacje robocze podlegają ograniczeniom zdefiniowanym przez politykę bezpieczeństwa systemu, użytkownik końcowy praktycznie nie ma możliwości wprowadzenia zmian w oprogramowaniu lub konfiguracji sprzętowej w sposób, który mógłby stanowić zagrożenie dla systemu. Wiele urządzeń uproszczonego klienta jest sprzedawanych jako stacje bezdyskowe.

## Sieci X Window

Drugie rozwiązanie uwzględniające uproszczone stacje klienckie wykorzystuje system X Window, który z kolei bazuje na protokole sieciowym X11. W rozwiązaniu X Window serwer jest aplikacją uruchomioną w stacji klienckiej (terminal X), która za pośrednictwem protokołu wyświetlania X zapewnia dostęp do systemu przetwarzającego dane. Terminal X Window odwołuje się do systemu przetwarzania danych, który w tym przypadku jest nazywany klientem. Najstarsze wersje X Window działały w systemach UNIX i DEC OpenVMS, ale bieżące wydania aplikacji można zainstalować w niemal każdym systemie operacyjnym.



Więcej informacji na temat systemu X Window znajduje się pod adresami <http://www.x.org>, <http://xwinman.org> oraz [http://pl.wikipedia.org/wiki/X\\_Window\\_System](http://pl.wikipedia.org/wiki/X_Window_System).

Serwer X Window System uruchamia graficzny interfejs użytkownika (np. GNOME lub KDE) w oknie systemu Linux. Okazuje się on szczególnie użyteczny, gdy trzeba uruchomić proces na komputerze o innym systemie operacyjnym niż zainstalowany na komputerze użytkownika wykonującego zadanie. Aplikacje X Window są niezależne od sieci. Obraz widoczny na monitorze (w serwerze wyświetlania) jest wynikiem pracy aplikacji uruchomionej po stronie klienta. System X-Window jest rozwiązaniem typu klient-serwer, podobnie jak serwer terminali. Jednak rozkazy (polecenia użytkownika) są w tym przypadku wydawane przez serwer, a aplikacja działa po stronie klienta. Aplikacja wykorzystuje bowiem usługi wyświetlania, które jednostka uproszczonego klienta udostępnia w sieci jako serwer. Mimo że nazewnictwo sugeruje odwrotną logikę działania, sama architektura sieci nie zmienia się w porównaniu z serwerami terminali.

Rozwiązania X Window mają długą historię i udostępniają wiele niestandardowych funkcji. Każdy, kto musi pracować w heterogenicznych sieciach, powinien się nimi zainteresować.

## Podsumowanie

W tym rozdziale zostały przedstawione podstawowe zasady projektowania sieci wynikające z różnorodności urządzeń sieciowych. Do najważniejszych spośród omówionych zagadnień z pewnością należy zaliczyć zależność topologii od architektury sieci, a także różnice między topologią i architekturą.

Warto zapamiętać, że połączenia punkt-punkt można rozpatrywać jako połączenia fizyczne, wirtualne, tymczasowe lub jako łącza o niezdefiniowanym rodzaju połączenia. Ponadto z zamieszczonych informacji wynika, że węzły współdzielące fizyczne medium tworzą segment. Segmenty wyznaczają domeny kolizyjne. Do rozdzielania poszczególnych segmentów służą punkty przyłączeniowe, takie jak przełączniki i routery. Omówione zostały również różne techniki routingu oraz rodzaje sieci — przełączane i pakietowe.

W niniejszym rozdziale uwzględniono także architektury peer-to-peer, klient-serwer, wielowarstwową oraz architekturę uproszczony klient-serwer.

W kolejnym rozdziale znajdują się informacje na temat metod przeszukiwania sieci oraz sposobów sporządzania mapy sieci z uwzględnieniem jej zasobów.

# Rozdział 4.

## Zbieranie informacji o sieci i sporządzanie map sieci

### **W tym rozdziale:**

- ♦ Metody zbierania informacji o sieci
- ♦ Właściwości połączeń
- ♦ Wykorzystanie protokołu SNMP do zarządzania pracą urządzeń sieciowych
- ♦ Sporządzanie mapy sieci

Zbieranie informacji o sieci jest mechanizmem, na którego podstawie ustalane jest rozmieszczenie poszczególnych systemów i urządzeń w sieci. Do wykrywania jednostek służy wiele różnych technik, w tym rozgłaszanie węzłów, tworzenie list przeglądania, odpytywanie i połączenia bezpośrednie. Często również stosuje się kilka z wymienionych metod jednocześnie. Każde z rozwiązań jest niezależne od konkretnych protokołów sieciowych. Niemniej wiele protokołów jest zaprojektowanych z myślą o wykorzystaniu określonej metody wyszukiwania stacji.

Mechanizmy zbierania informacji o sieci bazują na innych procesach i protokołach niż funkcje odwzorowania nazw. Oczywiście obydwa zadania muszą zostać zrealizowane poprawnie, aby ich wyniki były przydatne dla użytkownika. Metody odwzorowywania nazw zostały jednak opisane w dalszej części książki. Obejmują one sprawdzanie pliku *HOSTS*, odwołania do serwerów DNS, przeszukiwanie pamięci podręcznej NetBIOS, komunikację z serwerami WINS i wyszukiwanie wpisów w pliku *LMHOSTS*.

Połączenie sieciowe opisuje trasa ustanowiona między dwoma punktami końcowymi. Zgodnie z wcześniej przedstawionymi informacjami można zdefiniować wiele różnych rodzajów takich połączeń. Trasy (lub obwody) oraz punkty końcowe mogą mieć charakter fizyczny lub wirtualny. Dopuszcza się tworzenie prywatnych obwodów lub kanałów, co jest podstawą funkcjonowania wirtualnych sieci prywatnych. Wyróżnia się połączenia stanowe i bezstanowe. Połączenie stanowe przechowuje informację o nawiązanym połączeniu w czasie całej sesji, a w niektórych przypadkach również między sesjami. Połączenia bezstanowe są stosowane wówczas, gdy trasa nie jest wstępnie zdefiniowana.

Szczegółowych informacji na temat zarządzalnych urządzeń sieciowych dostarcza prosty protokół zarządzania siecią (SNMP — *Simple Network Management Protocol*), który jest przenoszony przez protokół IP. Jego działanie polega na zbieraniu danych z agentów SNMP, zainstalowanych w zarządzanych węzłach, i na przechowywaniu pozyskanych informacji w bazie danych o ustandaryzowanej strukturze. Mechanizm SNMP może posłużyć do sporządzenia mapy sieci, a także do generowania poleceń zmiany konfiguracji poszczególnych systemów i urządzeń sieciowych.

Przygotowanie mapy sieci jest procesem graficznego wyświetlenia rozpoznanych elementów sieciowych i zaprezentowania relacji między nimi. Mechanizmy przeglądania sieci zapewniają bazę danych informacjami o wykrytych obiektach (urządzeniach końcowych, łączach wyznaczających trasy itp.), a następnie ustalają sposób wzajemnego połączenia tych obiektów. Funkcje sporządzania map wykorzystują dane z przeglądania sieci w celu zobrazowania bieżącego stanu sieci. Jednak z uwagi na częste zmiany w środowisku sieciowym (włączanie i wyłączanie różnych elementów) mapy sieci nie zawsze są aktualne.

## Zbieranie informacji o sieci

Zbieranie informacji o sieci jest procesem, w którym jeden system lub jedno urządzenie wyszukuje wszystkie inne systemy i urządzenia sieciowe. Operacja ta może być realizowana za pomocą komunikatów rozgłoszeniowych, pozyskiwania i dystrybuowania list elementów sieciowych, odpytywania jednostek (z zastosowaniem mechanizmów rozgłoszeniowych zapytań i odpowiedzi) lub bezpośredniej komunikacji między różnymi węzłami i systemami. W praktyce wykorzystywane są wszystkie z wymienionych rozwiązań, a każde z nich ma inne cechy, predysponujące je do użycia w określonych warunkach.

Urządzenia sieciowe informują o swoim działaniu zaraz po przyłączeniu do sieci lub w odpowiedzi na zapytanie dostarczone z innego urządzenia. Zależności te zostały przedstawione na rysunku 4.1.

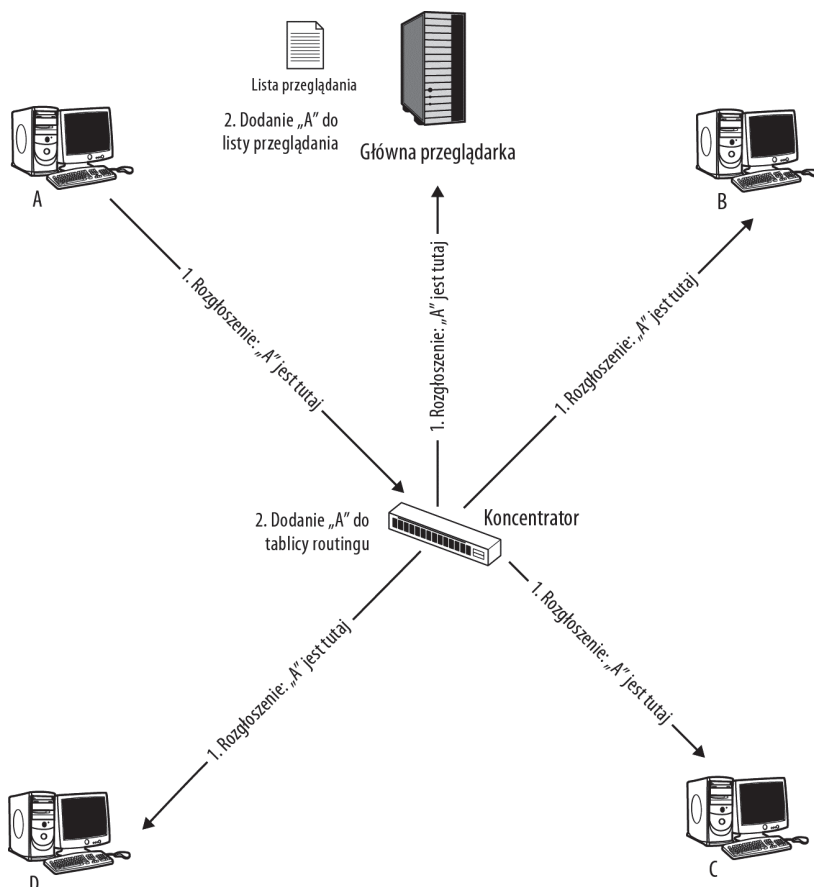
Najmniej skomplikowany sposób realizacji opisywanego zadania polega na wysłaniu komunikatu rozgłoszeniowego, który poinformuje urządzenia sieciowe o dostępności nowego elementu. Właśnie taki mechanizm został zilustrowany na rysunku 4.1. Węzeł A po uruchomieniu interfejsu sieciowego wysyła stosowny komunikat rozgłoszeniowy. W treści komunikatu wraz z informacją o poprawnym działaniu systemu zawarty jest adres interfejsu jednostki. Każdy system odbierający rozgłoszenie wygenerowane w węźle A dodaje informację o tym węźle do swojej listy urządzeń sieciowych.

Doskonałym przykładem protokołu wykorzystującego rozgłoszenia sieciowe jest protokół BOOTP, przeznaczony do dynamicznego pozyskiwania adresu IP. W sieciach o niewielkich rozmiarach rozgłoszeniowe powiadomienia są użytecznym mechanizmem pozyskiwania informacji z pojedynczego systemu (np. z serwera DHCP) lub jednostek grupy roboczej. Jednak w średnich i dużych sieciach transmisja rozgłoszeniowa okazuje się bardzo mało wydajną techniką gromadzenia informacji.

Zamiana adresów sieciowych na nazwy należy do zadań usług odwzorowania adresów. Przykładami usług odwzorowania adresów są: system nazw domenowych (DNS — *Domain Name System*), NetBEUI i inne.

**Rysunek 4.1.**

Zbieranie informacji o sieci za pomocą mechanizmu rozgłaszania dostępności urządzeń



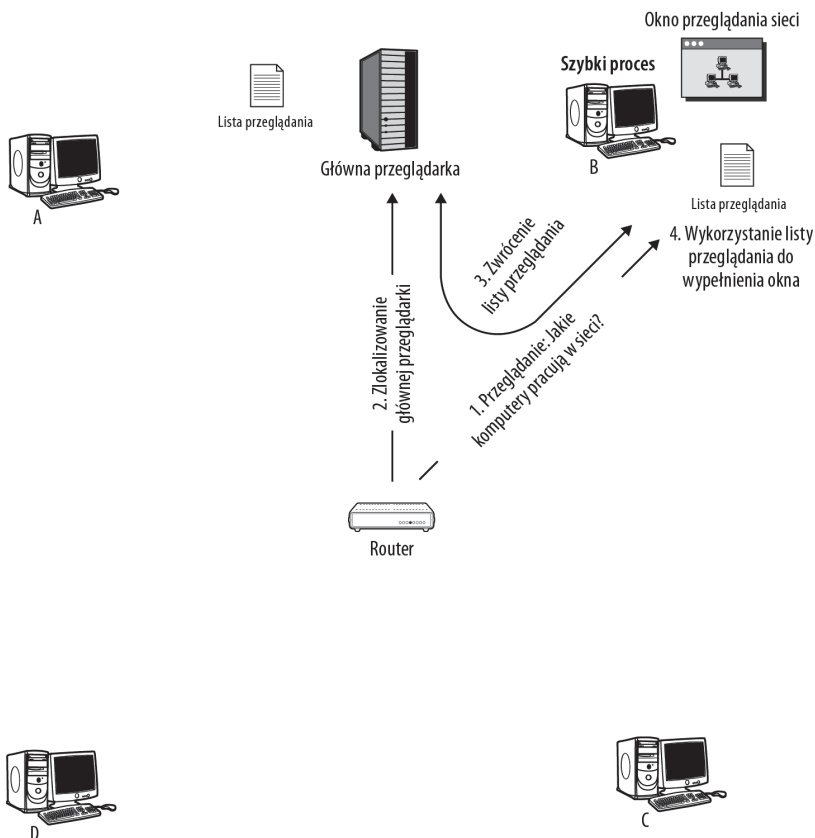
Zbieranie informacji o sieci jest najczęściej wynikiem zdarzenia wygenerowanego w warstwie aplikacji (na przykład otwarcia folderu *Sieć* lub wybrania opcji *Otwórz* lub *Zapisz* i wskazania sieciowej lokalizacji w oknie dialogowym). Dalszy tok postępowania zależy od sposobu działania określonej aplikacji, użytych protokołów oraz rodzaju systemu operacyjnego.

Efektywniejszy mechanizm gromadzenia informacji o sieci polega na utworzeniu i dynamicznym aktualizowaniu listy elementów sieciowych. Lista ta jest często nazywana *listą przeglądania*, ponieważ po zgromadzeniu informacji o stanie sieci jest ona udostępniana aplikacji jako obraz sieci. System zarządzający listą jest nazywany *główną przeglądarką*. Komunikują się z nim inne sieciowe systemy operacyjne, wykorzystując do tego celu różne protokoły. W przypadku grup roboczych główna przeglądarka jest wybierana spośród jednostek sieci. W domenach jest nią serwer domeny. W obydwu przypadkach operacja przeglądania sieci polega na odszukaniu przez dany system głównej przeglądarki i zażądaniu od niej dostarczenia listy przeglądania w celu sporządzenia lokalnej kopii tej listy. Listom przeglądania jest przypisany pewien czas ważności, po którego upływie system musi odświeżyć lokalną kopię. Z tego względu mechanizm przeglądania czasami nie obejmuje informacji o jednostkach włączonych do sieci tuż przed wyświetleniem jej stanu lub zawiera dane o komputerach, które zostały już odłączone. Ma jednak ogromną zaletę — istotnie ogranicza ruch sieciowy w porównaniu z techniką rozgłaszania powiadomień i jest szybszy w działaniu.

Przykład procedury przeglądania został przedstawiony na rysunku 4.2. Otwarcie okna sieci w komputerze B inicjuje żądanie przejrzania sieci. Jego wynikiem jest odszukanie głównej przeglądarki i zwrócenie aktualnej listy przeglądania. Dane z listy są następnie wykorzystane do wypełnienia okna sieci. Warto zwrócić uwagę na fakt, że węzły A, C i D nie biorą udziału w operacji przeglądania sieci.

### Rysunek 4.2.

*Gromadzenie informacji o sieci z wykorzystaniem mechanizmu przeglądania*

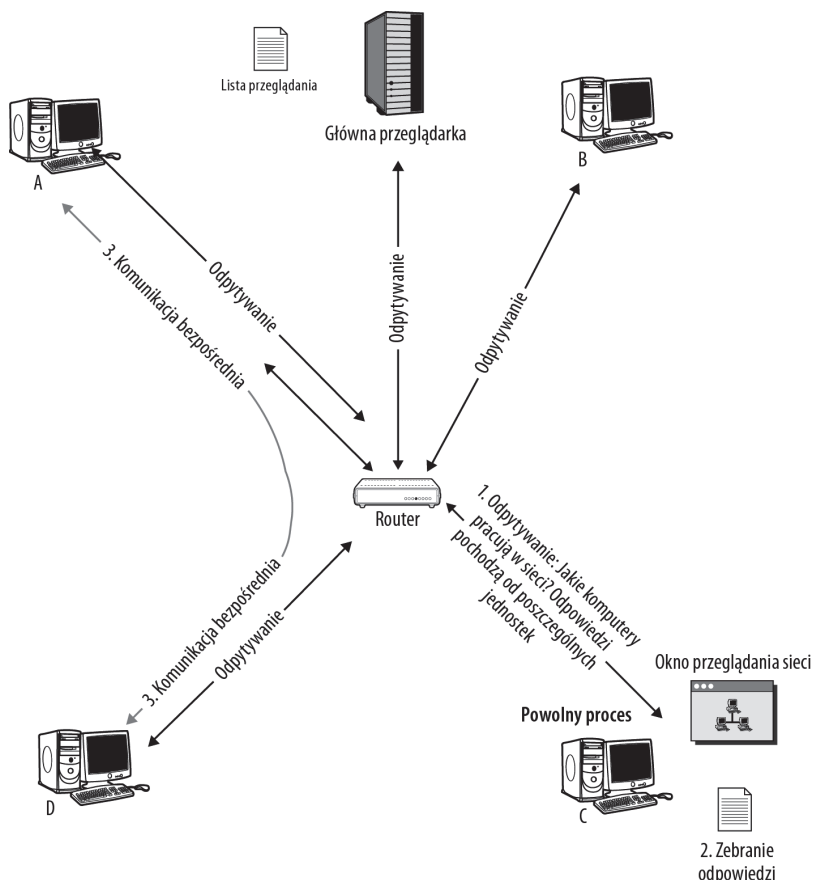


Kolejnym rozgłoszeniowym mechanizmem jest *odpytywanie*. Jego działanie zostało przedstawione na rysunku 4.3. Zgodnie z rysunkiem każdy węzeł wysyła żądanie w sposób rozgłoszeniowy, a inne elementy sieci odsyłają odpowiedź z informacjami na swój temat. Po odebraniu odpowiedzi pozyskane dane są zapisywane na liście jednostek sieciowych. Typowym zastosowaniem mechanizmu odpytywania jest wykrywanie routerów, w czasie którego router buduje tablicę routingu lub bazę danych informacji o trasach (RIB — *Routing Information Base*). Odpytywanie ma wszystkie wady mechanizmu rozgłoszeniowego powiadamiania i jest powolnym procesem.

Ostatni z mechanizmów wykrywania jednostek sieciowych działa z wykorzystaniem bezpośredniej komunikacji między systemami. Jeżeli jeden węzeł dysponuje listą elementów sieciowych, może wykorzystać bezpośrednie odwołania do komunikacji z węzłami zamieszczonymi na tej liście i zarządzać od nich dostarczenia listy węzłów w nich zarejestrowanych itd. Bezpośrednia komunikacja połączona z odpytywaniem jest obecnie najczęściej stosowaną techniką wykrywania routerów.

**Rysunek 4.3.**

Gromadzenie informacji o sieci z wykorzystaniem mechanizmu odpytywania lub komunikacji bezpośredniej



Zbieranie informacji o sieci jest jedną z podstawowych funkcji implementowanych we wszystkich urządzeniach sieciowych. Karty sieciowe, routery, przełączniki, a nawet drukarki przechowują we wbudowanym oprogramowaniu parametr nazywany adresem MAC. Adres MAC jest niepowtarzalną wartością, przypisaną do urządzenia przez producenta. Występowanie w sieci jednostek o takim samym adresie MAC prowadzi do błędnego funkcjonowania sieci.

**Ostrzeżenie**

Choć adresy MAC z założenia są niepowtarzalne, można je zmieniać. Modyfikacja adresu MAC skutkuje niewłaściwym identyfikowaniem urządzenia w czasie transmisji danych i ma na celu ukrycie rzeczywistego pochodzenia informacji. Adresy MAC można często zmieniać w sposób programowy.

W dotychczasowych rozważaniach nie została wymieniona żadna konkretna technologia realizująca w praktyce opisane zasady. W wielu publikacjach można bez trudu znaleźć informacje o tym, że za przeglądanie odpowiada protokół SMB, odwzorowanie nazw jest realizowane przez protokół NetBIOS w ramach TCP/IP (NBT — *NetBIOS over TCP/IP*), a rozgłoszenia w sieciach IP są generowane przez mechanizm ARP. Również w tej książce można znaleźć tego typu informacje. Nie są jednak istotne różne akronimy nazw, lecz ogólna zasada działania mechanizmu. Wydaje się, że w wielu publikacjach techniki zbierania

informacji o sieci są prezentowane fragmentarycznie lub w ogóle pomijane. Tymczasem rozpoznawanie sieci jest podstawową operacją sieciową i powinno być przeanalizowane na poziomie idei funkcjonowania.

Ważne jest, aby zrozumieć, że za gromadzenie informacji o sieciach odpowiedzialnych jest wiele różnych protokołów, a ich powstawanie wynika z potrzeby realizowania tej funkcji, a nie odwrotnie. Wszystkie sieciowe systemy operacyjne, oprogramowanie zarządcze oraz niemal każda aplikacja lub narzędzie korzystają z mechanizmów gromadzenia informacji o sieci, wykonując swoje zadania i udostępniając usługi. Nie można wyświetlić okna otwarcia lub zapisu pliku udostępnionego w zdalnym urządzeniu bez zainicjowania operacji pozyskania danych o sieci.

Niektóre usługi rozpoznawania sieci mogą być bardzo rozbudowane. Dostarczają informacji nie tylko o dostępności urządzeń, ale przekazują również listę parametrów konkretnego urządzenia. W przypadku rozbudowanych usług prezentowane są przynajmniej dane o statusie jednostki wraz z listą setek atrybutów, których wartości można pozyskać za pomocą odrębnego zapytania. Niekiedy udostępniają również funkcje umożliwiające rekonfigurację urządzeń. Część usług gromadzenia danych o sieciach automatycznie sporządza mapę sieci (nawet jeśli jest ona złożona z dziesiątków lub setek węzłów), która zawsze budzi zaciekawienie. Generowanie map jest wykorzystywane w zarządzaniu zasobami, optymalizacji pracy sieci i wielu innych operacjach, które zapewniają ciągłość pracy nowoczesnym sieciom.

Najczęściej stosowanym sposobem zbierania szczegółowych informacji o sieci jest uruchomienie prostego protokołu zarządzania siecią (SNMP — *Simple Network Management Protocol*), opisanego w dalszej części niniejszego rozdziału. Inną technologią przekazywania informacji o urządzeniach w sieci Windows jest system oprzyrządowania do zarządzania (WMI — *Windows Management Instrumentation*) stanowiący rozszerzenie modelu sterowników systemu Windows. Obydwa rozwiązania zapisują dane na temat urządzeń w bazie danych o ustalonej formie. W przypadku protokołu SNMP jest to plik bazy informacji z zakresu zarządzania (MIB — *Management Information Base*). Natomiast informacje pozyskane z mechanizmu WMI są zapisywane w repozytorium wspólnego modelu informacji (CIM — *Common Information Model*). Modelowi CIM towarzyszy technologia zarządzania siecią korporacyjną (WBEM — *Web-Based Enterprise Management*), stosowana również w innych operacjach związanych z zarządzaniem. Krótka charakterystyka tego rozwiązania została zamieszczona w dalszej części rozdziału.

Aby realizować swoje zadania, każdy system zarządzania siecią musi polegać na wymienionych wcześniej technologiach. Zarządzanie określonym urządzeniem jest możliwe dopiero po wykryciu, że jest ono dostępne w sieci. Z kolei niemożność wyszukania urządzenia jest podstawą działania wielu jednostek związanych z zabezpieczaniem sieci, takich jak firewalle. Narzędzia przeznaczone do zarządzania często znacznie ułatwiają pracę administratorom przez automatyczne instalowanie systemu operacyjnego na wielu komputerach lub porównywanie skomplikowanych założeń licencyjnych odnoszących się do wielu różnych urządzeń.

## Publikowanie informacji o węźle

Operacja publikowania informacji o węźle jest realizowana przez system lub urządzenie, które może świadczyć określoną usługę, i w sposób rozgłoszeniowy powiadamia inne jednostki o swojej dostępności. Proces ten został zilustrowany na rysunku 4.1. W niektórych

metodach rozgłaszania zakłada się odsyłanie odpowiedzi z każdego systemu, do którego dotrze żądanie, lub z pierwszego systemu spełniającego kryteria zawarte w rozgłoszeniu. W tym punkcie zostały opisane zasady działania niektórych protokołów rozgłoszeniowego rozpoznawania sieci.

W obecnie funkcjonujących sieciach powszechnie stosuje się cztery wymienione poniżej usługi rozgłoszeniowe:

- ♦ Protokół dynamicznej konfiguracji stacji (DHCP — *Dynamic Host Configuration Protocol*).
- ♦ Protokół uruchamiania stacji (BOOTP — *Bootstrap Protocol*).
- ♦ Aktualizacje tablic routingu.
- ♦ Prosty protokół zarządzania siecią (SNMP — *Simple Network Management Protocol*).



Routing jest tematem rozdziału 10. Natomiast w rozdziale 19. została opisana procedura ARP.

Serwery DHCP są wykorzystywane do dynamicznego przydzielania adresów IP jednostkom sieciowym. Usługi DHCP działają w sposób rozgłoszeniowy, ponieważ muszą być dostępne z każdego urządzenia, które dopiero stara się o adres. W analogiczny sposób funkcjonuje protokół BOOTP. Korzystają z niego jednostki, które nie uruchomiły jeszcze systemu operacyjnego i muszą uzyskać adres IP z puli utrzymywanej przez serwer BOOTP. Zadaniem protokołu BOOTP jest również przesłanie obrazu systemu operacyjnego do komputera pozbawionego oprogramowania lub zainicjowanie pracy uproszczonej jednostki klienckiej, która nie została wyposażona w twardy dysk i ma za zadanie udostępnić użytkownikowi oprogramowanie uruchomione w serwerze terminali.

Starsze protokoły routingu, takie jak pierwsza wersja protokołu informowania o trasach (RIP — *Routing Information Protocol*) i protokół trasowania bramy wewnętrznej (IGRP — *Interior Gateway Routing Protocol*), wykorzystują rozgłoszenia do aktualizacji tablic routingu. Protokół RIP jest rozwiązaniem z grupy protokołów wewnętrznych (IGP — *Interior Gateway Protocol*), działającym na podstawie wektora odległości. Aktualizacje wymieniane w ramach mechanizmu RIP tracą ważność po upływie ustalonej liczby sekund.



Routery są tematem rozdziału 9.

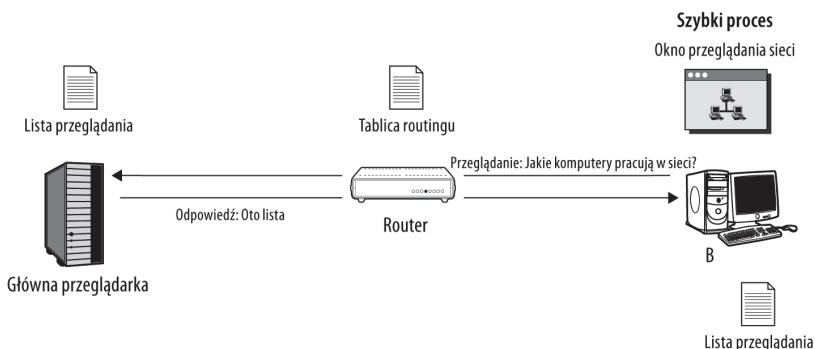
Protokół SNMP został omówiony w dalszej części tego rozdziału.

## Przeglądanie

Operacja przeglądania sieci jest wykonywana podczas każdorazowego otwarcia folderu *Sieć* w celu wyświetlenia listy dostępnych systemów. Choć wynik wydaje się tak oczywisty, a jego uzyskanie nieskomplikowane, w rzeczywistości jest efektem pracy wielu różnych procesów. Wymaga wykonania wcześniej opisanych zadań, a także pewnej aktywności systemu i sieci, zależnej od rodzaju żądania. Na rysunku 4.4 została przedstawiona sekwencja zdarzeń towarzyszących przeglądaniu sieci. Rozpoczyna ją otwarcie okna sieci w systemie B. Jeśli lista przeglądania jest zbuforowana lokalnie, okno *Sieć* jest automatycznie wypełniane

**Rysunek 4.4.**

Operacja  
przeglądania sieci



zgrupowanymi w niej danymi. W przeciwnym razie konieczne może się okazać wygenerowanie zapytania, które za pomocą protokołu takiego jak NetBEUI będzie dostarczone do głównej przeglądarki, skąd następnie zostanie przesłana lista dostępnych systemów.

Polecenie przeglądania sieci zostanie zrealizowane poprawnie w przypadku spełnienia następujących założeń dotyczących sieci:

- ♦ Systemy i urządzenia, które zarejestrowały się w sieci, są wymienione na liście przeglądania dostarczanej przez główną przeglądarkę.
- ♦ Router utrzymuje tablice routingu zawierającą informację o innych routerach i znanych adresach.
- ♦ Systemy i urządzenia zgłosiły swoją dostępność głównej przeglądarce w czasie procedury odpytywania (podczas uaktualniania listy).
- ♦ Jednostki, które wcześniej komunikowały się z główną przeglądarką mogą przechowywać listę nazw stacji w pamięci podręcznej w celu późniejszego wykorzystania.

W zależności od rodzaju systemu uzupełnienie listy przeglądania może być krótkotrwałym lub całkiem czasochłonnym procesem. Okres odświeżania jest parametrem, który podlega modyfikacji w rejestrze systemu Windows lub w ustawieniach oprogramowania głównej przeglądarki (na przykład w pliku konfiguracyjnym demona *nmbd* w serwerze Samba). Główna przeglądarka jest po prostu usługą sieciową działającą w systemie, który utrzymuje podstawową listę elementów sieciowych.

Niektóre systemy operacyjne i oprogramowanie sieciowe replikują główną listę w innych systemach w celu zwiększenia wydajności operacji, zwiększenia niezawodności i zapewnienia współdziałania z innymi protokołami. W mechanizmie przeglądania oprócz głównej przeglądarki wyróżnia się także przeglądarkę domeny, przeglądarkę lokalną, preferowaną przeglądarkę i kilka innych rodzajów serwerów udostępniających listę aktywnych systemów. Główną przeglądarką wcale nie musi być kontroler domeny. W grupie roboczej funkcję tę może pełnić dowolny komputer. Niekiedy nawet jest ona realizowana przez odpowiednie oprogramowanie. Na przykład w konfiguracji serwera plików Samba administrator może określić, czy chce, aby dany system był główną przeglądarką. Kontroler domeny jest systemem, który przechowuje bazę danych informacji potrzebnych do ograniczenia dostępu do sieci jedynie do zarejestrowanych systemów domeny.

Polecenie przeglądania sieci może zainicjować następujące czynności:

- ♦ Odwołanie do lokalnego bufora nazw w celu uruchomienia procesu przeglądania z jednoczesnym wypełnieniem listy jednostek, jeśli system został wcześniej uruchomiony (pracuje od pewnego czasu). Trzeba jednak pamiętać, że całkowite wypełnienie listy może zająć nawet godzinę.
- ♦ Odwołanie się do głównej przeglądarki w celu pozyskania listy stacji przechowywanej w tym systemie.
- ♦ Wysłanie żądania ujawnienia się innych dostępnych systemów (odpytywanie, opisane w kolejnym punkcie).

Wykrycie dostępności systemów sieciowych i usług to dopiero połowa zadania. Wiele usług i protokołów musi skojarzyć adres sieciowy rozpoznanej jednostki z przypisaną jej nazwą. Gdy dwa systemy (lub urządzenia) rozpoczynają komunikację, muszą dysponować swoimi adresami sieciowymi. Tylko kilka usług może realizować swoje zadania bezpośrednio na podstawie nazw stacji. Uzyskanie wspomnianego adresu wymaga przeszukania tabeli odwzorowań, zapisanej w usłudze, która jest odpytywana w ramach procesu odwzorowania nazwy.



Różne techniki ustalania adresów w sieciach TCP/IP zostały opisane w rozdziale 19.

Operacja odwzorowania adresu wymaga wykonania niektórych lub wszystkich wymienionych poniżej kroków (w przedstawionej kolejności):

1. Odszukanie nazwy w pliku *HOSTS*.
2. Odwołanie się do serwera DNS.
3. Sprawdzenie pamięci podręcznej NetBIOS (w systemie Windows). Choć obecnie mechanizm NetBIOS na bazie TCP/IP jest uznawany za przedawniony na rzecz DNS.
4. Odwołanie do serwera WINS (w systemie Windows), jeśli taki występuje w sieci.
5. Sprawdzenie wpisów w pliku *LMHOSTS* (w systemie Windows). Plik *LMHOSTS* jest odpowiednikiem pliku *HOSTS* odnoszącym się do nazw systemów Windows.

## Odpytywanie

Odpytywanie jest znacznie wolniejszym procesem niż operacja odszukania listy jednostek zbuforowanej w jednej ze stacji, pobrania jej i utworzenia własnej listy elementów sieci. Zmusza ono stację kliencką do wykonania czasochłonnego zadania zbudowania własnej listy. Przykład odpytywania został zaprezentowany na rysunku 4.3. Z uwagi na narzut wnoszony przez operację odpytywania jest ona stosowana tylko w protokole odwzorowania adresu (ARP — *Address Resolution Protocol*). Znajduje zastosowanie w różnych sieciach LAN, w tym w sieciach token ring, 802.11x (bezprzewodowych) oraz podczas przenoszenia ruchu IP w sieciach ATM. Jako rozwiązanie warstwy łącza danych żądanie ARP nie może być przenoszone przez router, ogranicza to jego działanie do pojedynczej podsieci.



Protokół DHCP został szczegółowo opisany w rozdziale 18.

## Połączenia

Połączenie sieciowe (*obwód*) jest ścieżką wykorzystywaną do przesyłania komunikatów między dwoma punktami końcowymi. Połączenia sieciowe mają wiele różnych cech. Część z nich ma charakter uniwersalny, a część jest zależna od rodzaju sieci.

Punkt końcowy to jednostka posiadająca adres, która może odbierać i generować ruch sieciowy. Punkty końcowe są interfejsami sieciowymi, a nie systemami lub urządzeniami, w których te interfejsy są zainstalowane. Chcąc być dokładniejszym, można stwierdzić, że karta sieciowa jest po prostu kartą rozszerzeń, a jednocześnie urządzeniem formującym ramki na potrzeby właściwego dla danej aplikacji układu scalonego (ASIC — *Application-Specific Integrated Circuit*), stanowiącego element warstwy fizycznej i warstwy łącza danych modelu OSI. Precyzyjniej rzecz ujmując, punkt końcowy połączenia sieciowego jest definiowany przez zbiór procedur programowych, umożliwiających wysyłanie i odbieranie ruchu sieciowego w ramach medium transmisyjnego, z dodatkiem fizycznego interfejsu odpowiedzialnego za cyfrowe przetwarzanie sygnału, niezbędne do przekształcania danych w transmitowane sygnały.

Idea reprezentowania punktu końcowego przez oprogramowanie stanowi podstawę do wirtualizacji — jednej z najważniejszych koncepcji w dziedzinie informatyki. Wirtualizacja polega na programowym emulowaniu pracy systemów i urządzeń. Dzięki niej użytkownik w każdej chwili może utworzyć wirtualny punkt końcowy (wirtualny interfejs). W środowiskach maszyn wirtualnych, w których emulowanych jest wiele komputerów, nie tylko systemy operacyjne podlegają wirtualizacji, ale także interfejsy sieciowe. Wirtualizacja oddziela funkcje od ich implementacji. Przykładami środowisk umożliwiających wirtualizowanie systemów są produkty Virtual Server i VMWare.

Ścieżka lub obwód jest drugą częścią definicji połączenia. Ścieżka może być specjalnym fizycznym obwodem — kablem rozciągniętym między dwoma punktami końcowymi — o wstępnie ustalonych parametrach i niezmiennym w czasie. Wiele sieci działa zgodnie z takimi założeniami. Szczególnie dotyczy to instalacji o mniejszym zasięgu, w których liczba połączeń pozwala na łatwe zarządzanie nimi. Jednak z uwagi na to, że liczba portów sieciowych przekłada się w sposób wykładniczy na liczbę możliwych połączeń, w większości sieci nie definiuje się trwałych połączeń fizycznych (byłoby to niezwykle kosztowne). Zamiast tego stosuje się różne techniki przełączania, prowadzące do tworzenia tymczasowych obwodów, zależnych od bieżącego stanu sieci. Tymczasowe połączenia są zwalniane po ich wykorzystaniu w przeciwieństwie do połączeń trwałych, w których obowiązuje ta sama ścieżka przekazywania danych przez cały czas trwania sesji komunikacyjnej (a nie tylko w czasie przesyłania porcji danych). Ruch sieciowy jest przekazywany przez tymczasowe obwody, wybierane w wyniku działania wyrafinowanych algorytmów routingu, wyznaczających trasy na podstawie ich długości, obciążenia, wydajności przełączania, przepustowości medium transmisyjnego i każdego innego czynnika uwzględnionego w określonym przełączniku lub routerze.

Nie wszystkie połączenia sieciowe zostały jednak zaprojektowane w taki sposób, by były trwałe lub tymczasowe. Projektując sieć, o której wstępnie wiadomo, że będzie zawodna, trzeba zastosować inne rozwiązania. Z problemem tym zetknęli się między innymi projektanci internetu. W jaki sposób można zaprojektować sieć, która zagwarantuje wysoką odporność na błędy podczas awarii rozległych jej obszarów? Rozwiązaniem okazało się użycie

transmisji pakietowej, wyznaczającej wirtualne obwody. Ścieżka transmisyjna nie jest wstępnie definiowana (jest wyznaczana dynamicznie) i może się zmieniać w każdej chwili w zależności od warunków środowiskowych. Jeden pakiet może być przekazywany określoną trasą, a następny zupełnie inną.

Obwody wirtualne mogą być również tworzone w ramach połączeń jako niezależne kanały, przenoszące tylko określony rodzaj informacji. Na tym założeniu bazują wirtualne sieci prywatne (VPN), przekazujące szyfrowane dane z jednego punktu końcowego do drugiego. Aby utworzyć połączenie VPN, dwie aplikacje muszą wynegocjować szereg parametrów połączenia, które zdefiniują sposób pracy obwodu wirtualnego.



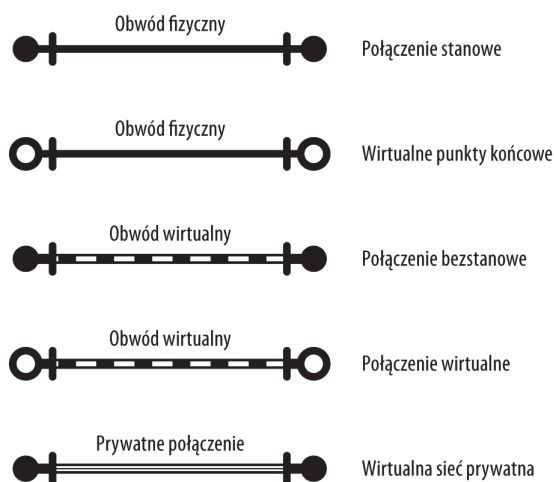
Więcej informacji na temat połączeń VPN zostało zamieszczonych w rozdziale 29.

Do opisu połączeń zostały wykorzystane terminy *trwale* i *tyczasowe*, odnoszące się do rodzaju ścieżki komunikacyjnej. Typowymi określeniami na połączenia tego typu, stosowanymi w informatyce, są jednak terminy *stanowe* i *bezstanowe*. Połączenie stanowe to takie, w którym połączenie między dwoma punktami końcowymi jest ustanawiane na cały czas trwania sesji i może zostać odtworzone po zakończeniu tej sesji. Połączenia stanowe przechowują wiele atrybutów umożliwiających ponowne ich ustanowienie. Termin „stanowy” odnosi się również do każdego procesu, który w swoim działaniu uwzględnia treść prowadzonej komunikacji. Firewall wykonujące w pełni stanową inspekcję pakietów nie tylko sprawdzają nagłówki pakietów, ale również ich zawartość.

Graficzne symbole poszczególnych rodzajów połączeń zostały przedstawione na rysunku 4.5. Punkty końcowe są w nich reprezentowane przez kółka znajdujące się na końcach każdej linii. Linie odpowiadają natomiast ścieżkom transmisyjnym. Ciągła linia lub w pełni zamalowane kółko oznaczają, że dany element ma trwały charakter. Puste kółko i linia przerywana symbolizują element tymczasowy (zmienny). W ostatnim przykładzie (połączenia prywatnego) cienka ciągła linia została otoczona grubszymi liniami, co oznacza, że połączenie jest tymczasowe i zabezpieczone.

#### Rysunek 4.5.

Pięć typów połączeń sieciowych



Na rysunku 4.5 zostało pokazanych pięć różnych rodzajów połączeń, które można ustanowić.

Połączenia bezstanowe charakteryzują się tym, że ścieżka komunikacyjna nie jest wstępnie znana. Znane są jedynie punkty końcowe, a samo połączenie jest zmienne (tymczasowe). Żadne informacje na temat połączenia nie są przechowywane lub przetwarzane. Przykładem połączenia bezstanowego jest komunikacja z wykorzystaniem protokołu HTTP w sieciach TCP/IP. Zgodnie z wcześniejszymi informacjami pakiety mogą być w niej dostarczane dowolnymi (właściwymi w danej chwili) trasami. Uzupełnienie połączeń bezstanowych o elementy „stanowości” sprowadza się do zarejestrowania tymczasowych informacji w sposób umożliwiający ich odtworzenie w późniejszym czasie. Właśnie w tym celu serwisy internetowe zapisują w komputerach klienckich pliki cookies. Przechowują informacje o użytkowniku, jego wcześniejszych sesjach i innych szczegółach komunikacji.

We wszystkich systemach operacyjnych połączenia są obiektami o odpowiednich nazwach, dostępnymi programowo z dowolnego obiektowego języka programowania. Obiekty sieciowe mają wiele parametrów opisujących ich sposób działania. Zapoznanie się z nimi jest więc kluczowe dla zrozumienia sposobu działania połączenia. Wśród wspomnianych parametrów znajdują się dane na temat stanu połączenia, wykorzystywanego protokołu itp. Innym obiektem związanym z połączeniem jest *sesja*. Sesja określa okres, w którym połączenie sieciowe jest używane do prowadzenia komunikacji konkretnego typu. W przypadku niektórych funkcji systemowych sesja może obowiązywać przez cały czas działania interfejsu generującego i odbierającego ruch sieciowy. Pojęcie sesji jest stosowane w projektowaniu aplikacji w celu grupowania pewnych reguł komunikacji, takich jak przydzielona szerokość pasma, wartość TTL pakietu itp. Atrybuty połączeń i sesji są wartościami ustalonymi przez dwa systemy lub urządzenia podczas negocjowania parametrów transmisji.

## Prosty protokół zarządzania siecią

Wraz ze wzrostem złożoności sieci coraz ważniejsze stawało się również wykrywanie urządzeń, monitorowanie ich pracy i zarządzanie nimi. W tym celu inżynierowie skupieni w ramach społeczności IETF (*Internet Engineering Task Force*) opracowali prosty protokół zarządzania siecią (SNMP — *Simple Network Management Protocol*). Protokół SNMP jest rozwiązaniem warstwy aplikacji (warstwy 7.), który stał się jednym z najczęściej wykorzystywanych systemów zarządzania siecią.

Mechanizm SNMP składa się z pięciu elementów stanowiących komponenty urządzeń sieciowych. Oto one:

- ♦ **Protokół SNMP.** Jest stosowany do komunikacji między urządzeniami a oprogramowaniem SNMP w sieciach TCP/IP.
- ♦ **Zarządzane obiekty.** Wywoływane urządzenia, takie jak karty sieciowe, routery, przełączniki, drukarki i wiele innych komponentów.
- ♦ **Agent.** Niewielki moduł programowy rezydujący w zarządzanych obiektach. Jego zadanie polega na zbieraniu informacji z obiektów oraz z sieci i udostępnianiu ich w formie właściwej dla protokołu SNMP.
- ♦ **Baza danych informacji zarządzania (MIB — *Management Information Base*).** Baza MIB zawiera informacje (w formie obiektów) na temat zarządzanych obiektów. Wiele, jeśli nie większość, obiektów danych wykorzystywanych przez urządzenia

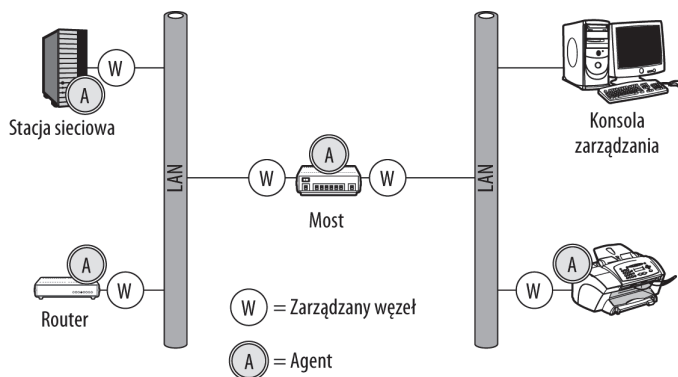
SNMP jest przeznaczonych tylko do odczytu (np. informacja o modelu urządzenia). Pozostałe obiekty danych mogą być odczytywane i zapisywane (np. nazwa urządzenia). Są więc zmiennymi, za których pomocą można zarządzać obiektami sieciowymi.

- ♦ **Konsola zarządzania.** Konsola zarządzania służy do zbierania odpowiedzi na żądania wygenerowane przez oprogramowanie SNMP.

Oprogramowanie SNMP może się komunikować z wymienionymi elementami w celu stworzenia obrazu sieci, zinventaryzowania funkcji urządzeń oraz ich stanów, rejestrowania zdarzeń i reagowania na nie. Model komunikacyjny wykorzystywany przez protokół SNMP jest stosowany przez wielu producentów w projektowanych systemach zarządzania. Jednym z przykładów niestandardowej implementacji mechanizmu SNMP może być chociażby system oprzyrządowania do zarządzania (WMI) firmy Microsoft, opisany w dalszej części rozdziału.

Zarządzanie siecią polega na generowaniu poleceń SNMP do agentów SNMP i zbieraniu danych z zarządzanych węzłów. Przebieg operacji wykrywania urządzeń i zarządzania nimi został zilustrowany na rysunku 4.6. Konsola zarządzania zbiera odpowiedzi SNMP, zapisuje je, a następnie wyświetla w formie dogodnej dla użytkownika. Konsola jest również zastosowana do wysyłania poleceń SNMP w celu zmiany ustawień urządzenia. Zarządzany węzeł (oznaczony na rysunku literą *W* w kółku) może odbierać i wykonywać polecenia SNMP. Litera *A* w kółku symbolizuje agenty SNMP, czyli moduły oprogramowania odpowiedzialne za wysyłanie i odbieranie informacji SNMP. Mechanizmy SNMP są implementowane w wielu różnych produktach.

**Rysunek 4.6.**  
Wykrywanie urządzeń  
w protokole SNMP  
i zarządzanie nimi



Na rysunku 4.6 zostały przedstawione interakcje między poszczególnymi elementami SNMP.

Konsola zarządzania jest oprogramowaniem pracującym na jednej ze stacji sieciowych, które wysyła polecenia SNMP i odbiera odpowiedzi. Do zadań tej aplikacji należy przechowywanie informacji o urządzeniach, prezentowanie ich użytkownikowi i zmiana ustawień urządzenia za pośrednictwem wprowadzanych przez użytkownika poleceń. Urządzenie, które ma możliwość inicjowania poleceń SNMP i odpowiadania na nie, jest określane *stroną* w komunikacji. Nazwa ta została formalnie zdefiniowana w wersji 2. protokołu SNMP. Strona jest pojedynczym komponentem, który ma własną lokalizację sieciową. Każda strona w komunikacji SNMP dysponuje protokołem uwierzytelniania i zachowania prywatności, dzięki któremu można ustanowić bezpieczne połączenie między stronami. Urządzenie współpracujące z protokołem SNMP może zawierać wiele elementów o charakterze stron

komunikacji pod warunkiem, że każdy z nich będzie niepowtarzalny. Na przykład każdy port routera obsługującego protokół SNMP może być stroną w komunikacji. Zarządzanie routerem można wówczas sprowadzić do poziomu pojedynczego portu.

Działanie oprogramowania do zarządzania siecią jest możliwe dzięki niewielkim modułom oprogramowania nazywanym *agentami*, zainstalowanym w zarządzanych urządzeniach. Zazwyczaj oprogramowanie to jest ściśle związane z systemem operacyjnym, przez co jego usunięcie jest bardzo trudne. Oprogramowanie agenta może być instalowane przez producentów w komponentach sprzętowych każdego urządzenia, które nadaje się do zarządzania. Jednak nie wszyscy dostawcy zadają sobie trud, aby udostępnić oprogramowanie do komunikacji z agentami SNMP. Niemniej w internecie jest dostępnych wiele aplikacji odpowiedzialnych za wykrywanie, sporządzanie mapy sieci na podstawie protokołu SNMP i zarządzanie nią. Wśród nich występują narzędzia typu shareware, udostępniane w takich serwisach, jak *download.com* lub *tucows.com*. Jednym z komercyjnych pakietów jest aplikacja WhatsUp Gold firmy Ipswitch (<http://www.whatsupgold.com>). Poza tym zadania SNMP są realizowane przez wiele komponentów rozbudowanych systemów zarządzania sieciami, takich jak LANtastic, HP OpenView, IBM Tivoli, CA NSM (wcześniej znany jako Unicenter), Altiris, ZENworks itp.

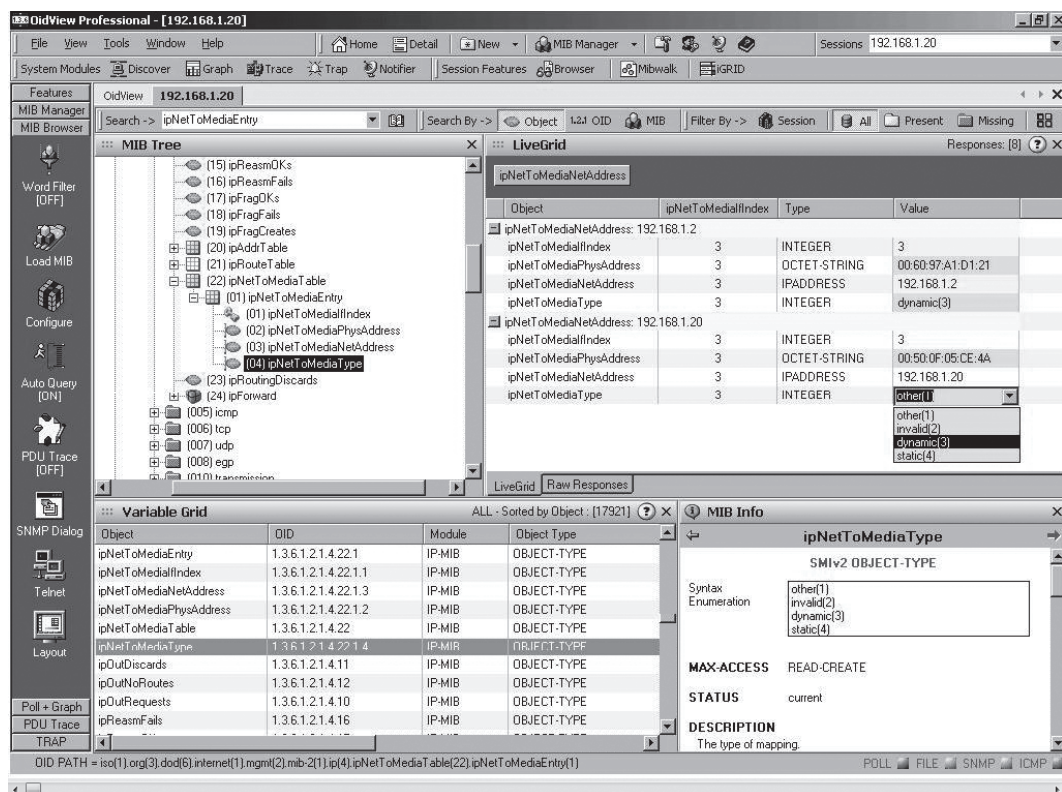
SNMP jest protokołem funkcjonującym w najwyższej warstwie modelu OSI — w warstwie aplikacji (w warstwie 7.). Oprogramowanie SNMP może wysyłać żądania (zapytania) do dowolnego komponentu, zdolnego do odpowiedzi na takie żądanie. W protokole SNMP został zdefiniowany niezbyt liczny zbiór poleceń, który powinien wydawać się znajomy każdemu, kto wie, jak działa protokół HTTP. Do komunikacji z określonymi agentami w zarządzanych urządzeniach służą polecenia SNMP, takie jak GET. Istnieją również pewne odmiany polecenia GET — GETBULK oraz GETNEXT. Pozwalają one na pobranie większej ilości informacji. Agenty zgłaszają swoją dostępność przez wysyłanie instrukcji INFORM lub TRAP, które mogą być rejestrowane przez systemy zarządzania. Zmiana dowolnego obiektu przeznaczonego do zapisu sprowadza się do wysłania polecenia SET.

Baza danych informacji zarządzania (MIB) zbiera dane o zarządzanym węźle lub systemie. Rodzaj informacji w niej zawartych wynika z typu urządzenia, choć zbiór danych można dowolnie rozszerzać. Protokół SNMP nie wyznacza precyzyjnie zakresu informacji przechowywanych w urządzeniu ani nie definiuje, który atrybut jest zmienną. SNMP określa jedynie zasady przechowywania danych w plikach MIB oraz sposób ich udostępniania.

Urządzenia SNMP mogą zmieniać swój stan w dowolnym momencie. Model zarządzania wymusza na nich poinformowanie o zmianie stanu, ale nie wymaga oczekiwania na odczytanie stanu. Moduł MIB urządzenia przechowuje obiekty zdarzeń, które są wysyłane jako tzw. pułapki SNMP (ang. *trap*). Urządzenia nasłuchujące przechwytyują wspomniane pułapki i w razie konieczności generują żądanie dostarczenia szczegółowych informacji o zdarzeniu. Dane SNMP są przekazywane w sieciach pakietowych (takich jak TCP/IP), przez co projektując konsolę zarządzania, nie można zakładać, że wszystkie wygenerowane zdarzenia zostaną przez nią odebrane. Z tego względu oprogramowanie SNMP odpytuje zarządzane urządzenia o bieżący status w konfigurowalnych odstępach czasowych. Odpytywanie wyzwalane zdarzeniami powoduje przesłanie żądań do określonego urządzenia z prośbą o aktualizację statusu danego komponentu. Ponieważ obydwie strony komunikacji są sobie znane, można uznać procedurę odbioru i uaktualnienia danych za wiarygodną. W przypadku odebrania informacji o wyjątkowo ważnym zdarzeniu częstotliwość aktualizacji statusu urządzenia wzrasta.

Pliki MIB mają hierarchiczną organizację właściwą dla przestrzeni nazw. Są więc przedstawiane w formie odwróconego drzewa, w którym każdy węzeł jest identyfikatorem obiektu (OID — *Object Identifier*). Poszczególne obiekty OID mogą być odczytywane i (lub) modyfikowane. Sposób interpretacji plików MIB jest opisany przez standard notacji ASN.1 modelu OSI organizacji ISO. Gwarantuje on niezależność operacji od rodzaju platformy systemowej. Zbiór reguł definiujących plik MIB wynika z kolei ze struktury informacji zarządzania (SMI — *Structure of Management Information*). Dzięki temu struktura i zawartość pliku MIB może być odczytywana za pomocą dowolnego narzędzia zgodnego ze standardem SNMP.

Na rysunku 4.7 został pokazany program OidView Professional (<http://www.oidview.com>) będący jednym z wielu dostępnych w internecie narzędzi do przeglądania plików MIB, ich struktury i zawartości. Aplikacja OidView analizuje zgromadzone informacje i prezentuje w przeglądarce MIB. W poszczególnych panelach wyświetlane są łatwe w przeglądaniu drzewa danych, wyniki analizy informacji, wykresy, zarejestrowane zdarzenia SNMP oraz poszczególne bazy MIB z różnych agentów SNMP działających w sieci.



Rysunek 4.7. Program do zarządzania SNMP OidView Professional

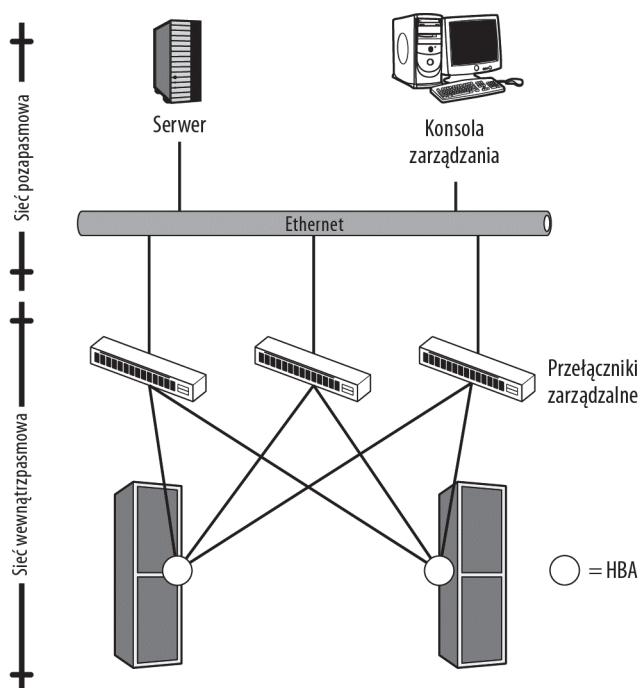
Struktury SMI wyznaczają schemat zapisu zgromadzonych informacji w plikach tekstowych. W praktyce oznacza to, że jeśli do pozyskania danych na temat urządzeń zostanie wykorzystana konsola zarządzania, to nie ma znaczenia, czy urządzenia te pracują w sieci

Ethernet, czy w sieci innego typu. Nie jest również istotne, jaki system operacyjny został uruchomiony w badanym urządzeniu. Informacje mają zwykły tekstowy format, a konsola zarządzania musi je tylko odpowiednio przeanalizować, co nie wydaje się szczególnie trudne.

Sieci pamięci masowych (SAN — *Storage Area Network*) są pewnym rodzajem sieci heterogenicznych, w których przechowywane informacje są rozdzielane między segmenty zbudowane w technologii Fibre Channel oraz sieci Ethernet z jednostkami klienckimi. Sieci heterogeniczne umożliwiają współdziałanie wielu różnych sieciowych systemów operacyjnych w ramach tej samej infrastruktury. W tym przypadku dwie sieci są połączone za pomocą jednego przełącznika lub większej liczby przełączników w taki sposób, aby urządzenia każdej sieci mogły się ze sobą komunikować i aby ruch związany ze składowaniem danych w pamięciach masowych był oddzielony od tradycyjnej wymiany danych. Sieć tego typu została przedstawiona na rysunku 4.8.

### Rysunek 4.8.

*Sieć pamięci masowej (SAN) — wykonana w technologii Fibre Channel — przyłączona do sieci Ethernet*



Szczegółowe informacje na temat sieci pamięci masowych znajdują się w rozdziale 15.

Jeżeli konsola zarządzania SNMP zostanie uruchomiona w sieci Ethernet, nie ma znaczenia, czy aplikacja SNMP działa pod kontrolą systemu Windows, czy Solaris. Nie jest istotna również wersja systemu (stacja robocza, czy serwer). Struktury SMI są niezależne od konkretnych systemów. W komunikacji z urządzeniami Fibre Channel konsola zarządzania wykorzystuje komunikację poza pasmem, podczas gdy elementy sieci Fibre Channel generują ruch wewnątrz pasma. Określenie komunikacji pozapasmowej oznacza, że ruch TCP/IP jest odmienny od strumieni danych Fibre Channel. Konsola zarządzania z oprogramowaniem takim jak StorageWorks firmy Hewlett-Packard może rozpoznawać jednocześnie urządzenia pracujące w sieci Ethernet i SAN. Wykrywane są nie tylko porty przełącznika, ale

również interfejsy HBA (*Host Bus Adapter*) oraz inteligentne twarde dyski stanowiące elementy systemu SAN. Komponenty HBA są interfejsami sieciowymi połączonymi z urządzeniami pamięci masowej. Biorąc pod uwagę to, że niektóre systemy pamięci masowej zawierają setki twarde dysków, zdolność do wykrycia i sparametryzowania (wprowadzenia zmian w czasie pracy) każdego dysku czyni z pakietów takich jak Storage Resource Management niezwykle użyteczne narzędzia. To właśnie tę wszechstronność SNMP wprowadza do inteligentnego oprogramowania sieciowego.

## Oprzysiężowanie do zarządzania systemem Windows

Oprzysiężowanie do zarządzania systemem Windows (WMI — *Windows Management Instrumentation*) jest opracowanym przez firmę Microsoft rozszerzeniem modelu CIM, który został udostępniony za pośrednictwem systemu zarządzania siecią WBEM. Mechanizm WMI tworzy repozytorium danych pozyskanych z zarządzanych obiektów i udostępnia je oprogramowaniu przeznaczonemu do zarządzania za pomocą interfejsu API, będącego rozszerzeniem modelu sterowników Windows (WDM — *Windows Driver Model*). System WMI stanowi interfejs, za którego pomocą można pobierać dane z repozytorium oraz wysyłać polecenia i ustawienia konfiguracyjne do zarządzalnych urządzeń sieciowych w sieci Windows. Instrukcje WMI można zawrzeć w skrypcie VBScript lub PowerShell. Choć nic nie stoi na przeszkodzie, żeby zostały wpisane bezpośrednio w wierszu poleceń.

Technologia WMI zapewnia dostępność rozbudowanego systemu zarządzania, który może nadzorować znaczną liczbę urządzeń i prezentować szczegółowe opisy ich bieżącego stanu. Niestety, jest to rozwiązanie współdziałające jedynie z systemem Windows.

Dodatkowo bazująca na technologii WMI platforma zarządzania siecią korporacyjną umożliwia gromadzenie danych z węzłów SNMP (agentów SNMP) oraz innych źródeł informacji współdziałających z interfejsem zarządzania stacją roboczą (DMI — *Desktop Management Interface*) i dostarczenie ich do oprogramowania zarządzczego w formie zgodnej ze zunifikowanym modelem dostępu do danych. W ten sposób do repozytorium CIM swoje dane dodaje wiele serwerów, aplikacji z pakietu Microsoft Office, a nawet przeglądarka Microsoft Internet Explorer. Repozytorium jest dostępne w formie klasy WMI o określonych właściwościach. Ma również własną przestrzeń nazw i język zapytań WQL (*WMI Query Language*). W repozytorium CIM zostały zdefiniowane przestrzenie nazw dla technologii Active Directory (RootDirectoryDAP), SNMP (RootSNMP) oraz usługi IIS (RootMicrosoftIISv2).

Oto kilka operacji, które można wykonać za pomocą WMI:

- ♦ Uruchomienie lub zatrzymanie procesu w systemie sieciowym.
- ♦ Ponowne uruchomienie zdalnego komputera.
- ♦ Utworzenie listy zainstalowanych aplikacji systemu sieciowego.
- ♦ Uruchomienie procesu o określonej godzinie.
- ♦ Sprawdzenie dziennika zdarzeń w systemie sieciowym.

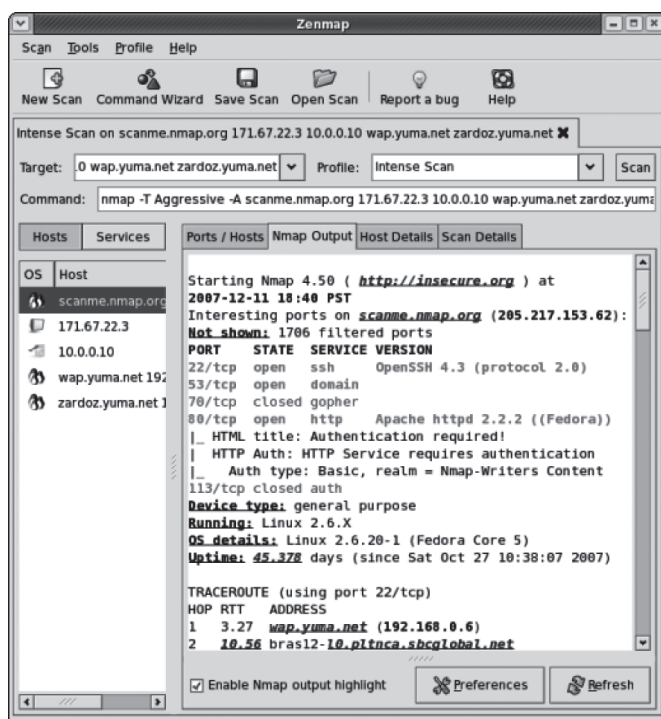
Firma Microsoft udostępniła mechanizmy WMI w formie zbioru dostawców usług (ang. *providers*). W systemie Windows Server 2008 i Windows Vista upublicznionych jest około 100 takich dostawców. Odbiorcami danych WMI poza wspomnianymi wcześniej narzędziami skryptowymi są również inne programy związane z zarządzaniem. Są to między innymi Microsoft System Center Operations Manager, HP OpenView, BMC Software Distributed Systems Management. Oprócz interfejsu do automatyzacji zadań system WMI zawiera także interfejs środowiska .NET oraz interfejs COM/DCOM przeznaczony dla starszych aplikacji. Dostęp do zdarzeń WMI jest więc możliwy za pośrednictwem mechanizmów DCOM i protokołu SOAP.

## Sporządzanie mapy sieci

Sporządzanie mapy sieci polega na zautomatyzowanym wykrywaniu systemów i połączeń między nimi. Różne programy wykonują to zadanie w różny sposób, ale początek operacji jest jednakowy we wszystkich przypadkach. Procedura rozpoczyna się od użycia instrukcji PING w odniesieniu do każdego poprawnego adresu sieciowego, właściwego dla podsieci, do której przyłączony jest komputer. W ten sposób powstaje lista wszystkich urządzeń, które aktywnie działają w sieci i pozwalają na ich wyszukanie. Do sporządzenia mapy sieci można się posłużyć takimi narzędziami jak nmap (program dostępny w wersji dla systemów Linux, Microsoft Windows, Solaris, BSD i Mac OS X). Program nmap (<http://www.nmap.org>) jest narzędziem wiersza poleceń, ale towarzyszy mu wiele graficznych nakładek, a wśród nich przedstawiony na rysunku 4.9 program Zenmap (<http://nmap.org/zenmap>).

### Rysunek 4.9.

*Skanowanie sieci  
w programie Zenmap*



Do sieci mogą być przyłączone jednostki, które są nieaktywne w czasie wykonywania testu. Oczywiście nie zostaną one wykryte przez mechanizmy aktywnego poszukiwania stacji. Analogicznie na mapie sieci nie zostaną uwzględnione systemy należące do podsieci nieznanymi programowi skanującemu. Aby wyszukać pozostałe stacje, trzeba zastosować odpowiednie techniki poszukiwania pasywnego.

Narzędzia aktywnego rozpoznawania elementów sieciowych mają jednak pewną wadę. Nie wykrywają systemów operacyjnych zabezpieczonych popularnymi obecnie osobistymi firewallami. Problematyczne jest również identyfikowanie systemów, które nie są dostępne przez cały czas w sieci (na przykład zainstalowanych na notebookach). Dlatego programy opracowujące mapy sieci korzystają z aktywnych i pasywnych metod detekcji. Pasywne badanie polega na sprawdzaniu miejsc, w których są przechowywane adresy sieciowe (na przykład tablice routingu lub listy przeglądania). Z kolei aktywne przeszukiwanie oznacza bezpośrednie ustalenie dostępności urządzenia w sieci. Zestawienia wygenerowane w ramach metod pasywnych dostarczają informacji o sposobie przeszukiwania całej sieci i przenoszą proces wykrywania urządzeń do innych podsieci (znajdujących się w odległości określonej liczby skoków od konkretnego routera).

Istnieje kilka technik sporządzania map sieci. Oto one:

- ♦ Aktywna identyfikacja różnych interfejsów przyłączeniowych, za których pomocą urządzenia komunikują się z siecią.
- ♦ Analiza routingu pakietów przez weryfikację tablic routingu.
- ♦ Przeglądanie pola ładunkowego pakietów w celu ustalenia systemu źródłowego oraz ewentualnych węzłów pośrednich, które zawarły informacje adresowe w pakiecie.
- ♦ Przeszukiwanie danych w dostępnych serwerach uwierzytelniania, autoryzacji i obsługi profilu (AAA — *Authentication, Authorization, Accounting*). Do grupy serwerów AAA zalicza się serwery dial-in, RADIUS oraz serwery dostępu zdalnego.
- ♦ Przechwytywanie danych uwierzytelniających dostęp do sieci (dane z logowania użytkowników i stacji roboczych).

Przygotowywanie obrazu sieci należy do zadań wielu pakietów oprogramowania. Warto wśród nich wymienić SNMPWalk, Cheops, SNMPutil, WhatsUp Gold oraz PacketTrap.

Celem gromadzenia informacji o sieci jest sporządzenie mapy sieci, ustalenie, jakiego rodzaju systemy, urządzenia i programy funkcjonują w sieci, oraz zwiększenie niezawodności i bezpieczeństwa sieci. Przeprowadzenie takiej operacji może wykazać obecność nieznanymi systemów, które były celowo ukrywane.

Narzędzia do obrazowania sieci gromadzą dane różnego rodzaju. Gdy system jest odpowiednio przygotowany, można pozyskać szczegółowe informacje na temat rodzaju zainstalowanego procesora (typ i identyfikator), wersji systemu operacyjnego (typ i identyfikator instalacji), czasu ostatniej aktualizacji, rodzaju dysku (typ i identyfikator) itp. Zgromadzone w ten sposób dane pozwalają administratorowi zainwentaryzować sieć. Organizacje, w których wdrożono systemy zarządzania siecią z modułami zarządzania zasobami (takie jak LANtastic lub Altiris), mogą generować szczegółowe raporty na temat przeznaczenia i lokalizacji poszczególnych zasobów, co bywa nieocenione podczas planowania, wdrażania i wykorzystywania nowych rozwiązań.

## Podsumowanie

W tym rozdziale zostały przedstawione różne metody gromadzenia informacji o sieciach oraz techniki odwzorowywania nazw jednostek. Zaprezentowane rozwiązania nie są zależne od zastosowanych protokołów, choć często determinują sposób przygotowywania protokołów.

Połączenia są wyznaczane przez ścieżki komunikacyjne ze zdefiniowanymi punktami końcowymi. Odpowiednie zestawienie fizycznych i wirtualnych ścieżek i punktów końcowych prowadzi do powstania różnych rodzajów połączeń.

W rozdziale zostały zamieszczone informacje na temat protokołu SNMP, sposobu gromadzenia danych na temat urządzeń oraz udostępniania tych danych innym aplikacjom. Systemy SNMP nie tylko zbierają informacje o urządzeniach, ale mogą również przysyłać polecenia i zmieniać parametry konfiguracyjne oraz stan urządzeń. Dodatkowo usprawniają przygotowywanie map sieci i szczegółową analizę jej zasobów.

Tematem kolejnego rozdziału jest wydajność sieci i jej związek z szerokością pasma oraz przepustowością.

# Rozdział 5.

## Szerokość pasma i przepustowość

### W tym rozdziale:

- ◆ Przetwarzanie sygnału podczas transmisji danych
- ◆ Rejestrowanie i odtwarzanie złożonych danych
- ◆ Transmisja wielu strumieni danych w jednym połączeniu
- ◆ Alokacja zasobów i metody sterowania ruchem

Informacje są przekazywane przez sieć w formie zbioru sygnałów. Sygnały z kolei reprezentują dane analogowe lub cyfrowe. Poszczególnym rodzajom danych odpowiadają różne grupy sygnałów, zdefiniowane w poszczególnych standardach. Niektóre grupy przenoszą zbiory znaków, inne grupy reprezentują nuty melodii lub słowa konwersacji. Kodowanie i dekodowanie danych należy do zadań określonego protokołu. Są jednak również protokoły, które odpowiadają za transport danych oraz za sterowanie ich przepływem. Odpowiedni zbiór danych reprezentuje przekazywaną informację. W tym rozdziale zostanie omówiona szerokość pasma segmentu sieci, jego przepustowość oraz pojemność.

Sygnały przenoszące dane są przekazywane w formie fal okresowych. Każda funkcja okresowa lub sygnał zespolony mogą zostać poddane analizie Fouriera, która jest matematyczną operacją przekształcającą złożony przebieg wejściowy w zbiór funkcji sinusoidalnych i odpowiadających im współczynników. W wyniku przeprowadzonej analizy otrzymujemy zbiór sygnałów *harmonicznych*, które po złożeniu odpowiadają przebiegowi wejściowemu. Przeprowadzenie opisanej operacji jest konieczne do zapisania informacji i odtworzenia ich w późniejszym czasie.

Aby sygnał mógł zostać odtworzony, trzeba przeprowadzić procedurę próbkowania, prowadzącego do rozbicia sygnału na pojedyncze komponenty. Teoria próbkowania precyzyjnie definiuje minimalną częstotliwość próbkowania, przy której uzyskuje się użyteczne informacje.

Technika *multipleksacji* umożliwia przekazywanie wielu strumieni danych przez jedną sieć. Rozwiązania takie jak podział czasowy, podział częstotliwościowy lub zmiana polaryzacji mają na celu odseparowanie poszczególnych strumieni danych od innych. Multipleksacja jest operacją, która musi być właściwie obsługiwana przez stosowany protokół i stanowi czynnik odróżniający jeden rodzaj sieci od innego.

Ruch w sieci podlega kształtowaniu przez protokoły wyższych warstw modelu OSI. Również w sieci IP implementowane są mechanizmy regulowania transmisji pakietów. Kształtowanie ruchu polega na monitorowaniu typów danych, adresów docelowych i innych cech transmisji, a także na modyfikowaniu priorytetów strumieni, ograniczaniu przepustowości i wykonywaniu innych operacji na pakietach. Zbiór rozwiązań zapewniający dostosowanie ruchu sieciowego do zasobów sieciowych jest określany po prostu mechanizmem zapewnienia odpowiedniej jakości usługi (QoS — *Quality of Service*).

## Szerokość pasma i pojemność systemu

Powszechnie wiadomo, że przekazywanie informacji w medium (takim jak drut miedziany w kablu ethernetowym) wymaga przepływu elektronów. Z kolei transmisja sygnału polega na okresowej zmianie w czasie prądu, napięcia, częstotliwości, fazy lub kilku tych wielkości jednocześnie. W celu przekształcenia sygnału w dane najczęściej wykorzystuje się określone zmiany amplitudy i (lub) częstotliwości tego sygnału.

Sygnały przesyłane w kablu są sygnałami analogowymi nawet wówczas, gdy reprezentują sygnał cyfrowy. Pojedynczy bit o wartości logicznej jedynki jest generowany przez dowolny system jako niemal idealny impuls fali prostokątnej. Jednak szum, zakłócenia i wiele innych czynników niszczą jego pierwotny kształt. System odbiorczy musi więc zbadać w rejestrowanym sygnale jego okresowość oraz poziom, aby zdecydować, czy odebrany impuls mieści się w zakresie wartości odpowiadających bitowi „1”.

W sieciach komputerowych do przesyłania danych z punktu do punktu stosuje się różne media transmisyjne. We włóknach światłowodowych sygnał jest przenoszony jako światło, technologie Bluetooth, WiFi i WIMAX wykorzystują fale elektromagnetyczne o częstotliwościach mikrofalowych (podzbiór fal radiowych). Charakter sygnału bywa różny, ale szerokość pasma, przepustowość, pojemność i inne parametry transmisyjne opisane w tym rozdziale są jednakowe we wszystkich przypadkach.

## Koraliki w rurze z syropem

Mistrz medytacji zen prosi wszystkich czytających tę książkę o zamknięcie oczu, wzięcie głębokiego oddechu i wyobrażenie sobie rury wypełnionej syropem.

Każde sieciowe medium transmisyjne ma pewne graniczne parametry, które wyznaczają maksymalną szerokość pasma i pojemność systemu. Połączenie sieciowe można sobie wyobrazić jako rurę wypełnioną pewnym medium (na przykład syropem), przez które przepływają cząsteczki lub fale (koraliki). Przepływ koralików można rejestrować na kilka sposobów, co z kolei można wykorzystać jako transmisję danych, interpretowanych później jako informacje. Pojedynczy koralik nie ma jednak cech fali, którą można by zmierzyć. Niemniej zasada nieoznaczoności Heisenberga precyzyjnie definiuje, jak ta fala się kształtuje.

Średnica rury wyznacza maksymalną liczbę koralików, które mogą przepłynąć obok dowolnego punktu w dowolnym czasie. W ten sposób określa się szerokość pasma. Ciśnienie wywierane na koraliki wpływa na szybkość ich przemieszczania, ale również w tym przypadku istnieje pewna granica, po której przekroczeniu nie uda się przyspieszyć ruchu koralików.

Ciśnienie odpowiada dostarczanej energii. W przypadku przewodu należy je rozpatrywać jako napięcie elektryczne. Przemieszczanie się koralików z pewną szybkością względem wybranego punktu na rurze pozwala na obserwację strumienia, czyli rejestrowanie liczby koralików w jednostce czasu. Strumień odpowiada przepustowości. W przewodzie przepustowość jest wyznaczana przez prąd, czyli liczbę elektronów przepływających obok danego punktu w jednostce czasu.

Zatem maksymalna szerokość pasma i przepustowość odpowiadają liczbie koralików, które dana rura z syropem może przenieść, a to jest pojemność rury. Niektóre pojemności mają znaczenie praktyczne — metoda wykorzystana do zwiększenia ciśnienia ma pewne ograniczenia. Inne są teoretyczne — prowadzące do pęknięcia rury. W dziedzinie elektroniki odpowiednikiem takiej sytuacji jest przypływ prądu w przewodzie lub przez tranzystor, który powoduje defekt sieci krystalicznej, taki jak elektromigracja, uszkadzający przewód lub złącze tranzystora. Wynikiem elektromigracji jest ubytek materiału w przewodzie, gdyż metal przesuwa się wraz z prądem.

Ponieważ zbiór koralików reprezentuje informację, szybkość transmisji danych odpowiada bezpośrednio szybkości przemieszczania się koralików. Szybkość przemieszczania się koralików zależy natomiast od szerokości rury, w której tworzy się strumień. Szybkość i przepustowość są podstawowymi metrykami wydajnościowymi stosowanymi w szacowaniu efektywności każdej sieci transmisji danych.

Nie są to szczególnie skomplikowane pojęcia i odnoszą się do wszystkich segmentów sieciowych. Oczywiście inne czynniki wpływają na rodzaj zadań, które mogą być realizowane w sieci, czy ilość danych, które można przekazać. Niestety, w tej książce nie ma miejsca na przedstawienie wszystkich fizycznych aspektów związanych z wykorzystaniem elektryczności, optyki czy radiotelegrafii. Jednak zapoznanie się z niezbyt skomplikowanym przykładem zastosowania teorii sygnałów powinno ułatwić przyswajanie sobie kolejnych zagadnień.

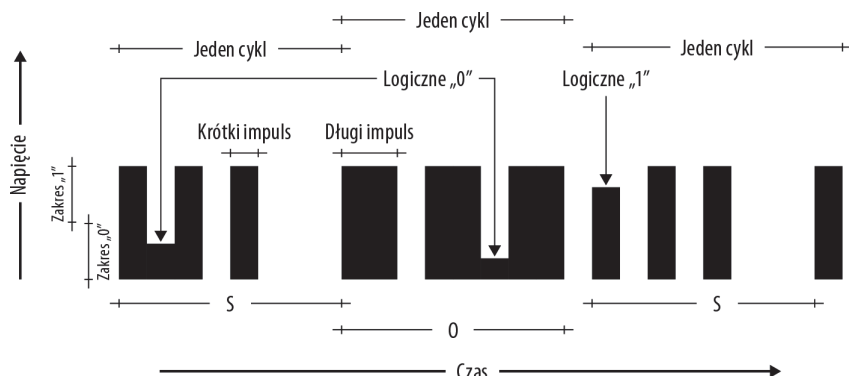
## Teoria sygnałów

Załóżmy, że w przewodzie od pewnego czasu płynie prąd i chcemy go wykorzystać do komunikacji. Wiadomość jest krótka: SOS. Do jej zakodowania posłuży kod Morse'a. Oznacza to, że komunikat będzie się składał z trzech krótkich sygnałów reprezentujących literę *S* (kropki) oraz trzech długich sygnałów odpowiadających literze *O* (kreski), po których znowu wystąpią trzy krótkie sygnały.

Kropce zostanie przypisany sygnał o wartości  $I$  (włączony) o określonym czasie trwania. Natomiast kresce będzie odpowiadał sygnał o wartości  $I$  (włączony) o dwukrotnie dłuższym czasie trwania. Za stan włączenia uznawany jest sygnał o amplitudzie zawierającej się w pewnym zakresie wartości. Natomiast wyłączenie jest reprezentowane przez sygnał o amplitudzie między zerem a wartością wyznaczającą dolną granicę przedziału włączenia. Utworzony w ten sposób cyfrowy sygnał SOS został przedstawiony na rysunku 5.1. W rzeczywistości impulsy nie mają idealnie prostokątnego kształtu, więc tolerowane są pewne odstępstwa w przebiegu sygnału.

Na rysunku 5.1 celowo zostały zaprezentowane pewne problemy z przetwarzaniem sygnału elektrycznego. Sygnał ten jest emitowany w czasie. Częstotliwość pomiaru wynosi osiem próbek amplitudy (napięcia) na jeden okres. Jeśli w czasie pomiaru amplituda sygnału znajduje

**Rysunek 5.1.**  
Cyfrowy sygnał  
komunikatu SOS



się w przedziale logicznej jedynki, należy uznać, że sygnał jest włączony. Jeśli amplituda zawiera się w przedziale logicznego zera — jest wyłączony. Dlatego mimo że pierwsza litera *S* wygląda nieco inaczej niż druga, dane są interpretowane w taki sam sposób.

Przedstawienie komunikatu SOS w formie piktogramu nie sprawia większej trudności, ale opisanie go w sposób matematyczny tak, aby można go było odtworzyć, to już inne zadanie. Gdy sir Isaac Newton chciał obliczyć pole pod krzywą, opracował specjalną technikę wydzielania prostokątnych obszarów, których powierzchnię mógł później łatwo policzyć. Im gęściej rysował prostokąty, z tym większą dokładnością suma ich powierzchni odpowiadała polu pod krzywą. Analiza ta została nazwana całkowaniem, a jej matematyczną reprezentacją jest całka.

W przypadku sygnału o określonej częstotliwości problem jest zdefiniowany nieco inaczej. Nadal konieczne jest rozłożenie kształtu wynikowego na kształty składowe, które można ująć w obliczeniach. Jednak tym razem potrzebne są funkcje okresowo zmienne w czasie. Z analogicznym problemem zetknął się Joseph Fourier podczas analizowania przepływu ciepła. Opracował wówczas rozwiązanie polegające na przekształceniu sygnału w duży zbiór funkcji trygonometrycznych (funkcji o precyzyjnie określonym kształcie).

Proces podziału sygnału na składowe jest nazywany *analizą Fouriera*. Równanie opisujące wynik tej operacji nazywa się *szeregiem Fouriera*, a proces odtwarzania sygnału — *syntezą Fouriera*. W przypadku rozpatrywanych tutaj sygnałów, wykorzystywanymi funkcjami będą: sinus i cosinus.

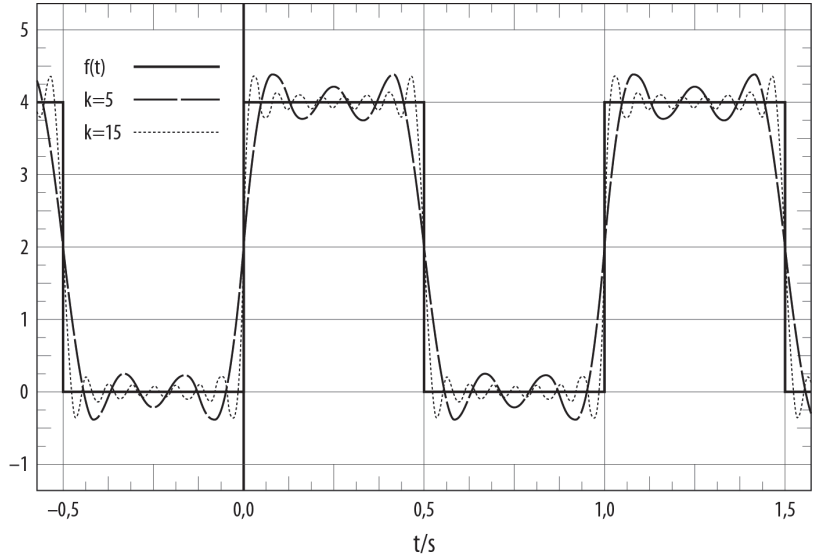
Ogólna postać okresowej funkcji Fouriera (o okresie  $2\pi$ ) to:

$$g(t) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} a_n \cos(2\pi nft) + \sum_{n=1}^{\infty} b_n \sin(2\pi nft)$$

w której częstotliwość  $f$  równa się  $1/T$ , a  $a_n$  i  $b_n$  oznaczają amplitudy  $n$ -tych harmoniczných. Składowa harmoniczna jest falą o częstotliwości odpowiadającej częstotliwości sygnału podstawowego pomnożonej przez wartość całkowitą. Zachowuje więc okresowość przebiegu podstawowego. Powyższe równanie rozwija się w szereg wyrazów o kolejnych wartościach  $n$ . Im więcej wyrazów zostanie zdefiniowanych w szeregu Fouriera, tym dokładniej analizowany sygnał będzie reprezentowany. Równanie można także przekształcić w taki sposób, aby można było wyliczyć stałą każdego wyrazu ( $a_n$ ,  $b_n$  itd.). Niemniej przekształcenie to nie ma znaczenia dla dalszych rozważań.

Na rysunku 5.2 został przedstawiony wynik składania harmonicznych w celu uzyskania przebiegu prostokątnego. Idealny przebieg prostokątny został oznaczony jako  $f(t)$ . Dwa pozostałe przebiegi są jego aproksymacją. Przebieg bardziej odbiegający od wzorca obejmuje harmoniczne do piątej włącznie ( $k=5$ ). Natomiast przebieg zbliżony do wzorca obejmuje harmoniczne do piętnastej włącznie ( $k=15$ ).

**Rysunek 5.2.**  
Przybliżenie przebiegu  
prostokątnego za  
pomocą sygnałów  
harmonicznych



Choć w przykładzie został przedstawiony tylko jeden przebieg prostokątny, synteza Fouriera umożliwia tworzenie także sygnałów schodkowych, trójkątnych, piłokształtnych oraz opisanych innymi funkcjami zmiennymi w czasie. Analogicznie poddanie analizie Fouriera sygnału audio prowadzi do wyznaczenia równania opisującego ten sygnał. Można również zrealizować tę operację na widmie częstotliwościowym sygnału.

Jaki to ma związek z komunikatem SOS? Częstotliwość sygnału wyraża się jako liczbę okresów przypadających na jednostkę czasu, tj.  $f = 1/T$ . Na podstawie samego przebiegu komputer nie może ustalić, kiedy dany okres się zaczyna i kiedy kończy. Komputer dysponuje jednak zegarem. Dane są wysyłane w taki sposób, że każdy znak jest transmitowany przez standardowy czas emisji jego bitów, nazywany *bajtem*.

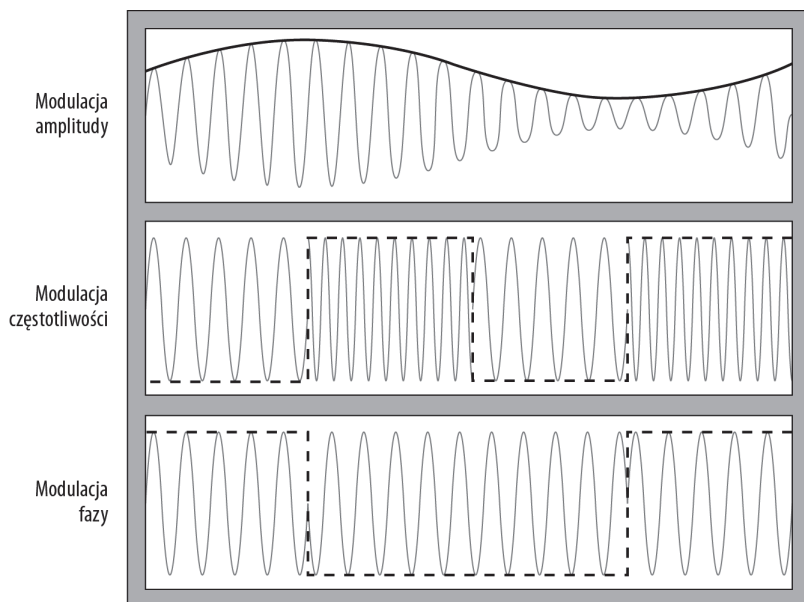
Oczywiście komputery nie posługują się kodem Morse'a. Wykorzystują zestawy znaków zdefiniowane w powszechnie znanych standardach. Jednym ze standardów jest 7-bitowy zestaw ASCII, którego zawartość różni się w zależności od ustawień regionalnych. Innym standardem kodowania jest Unicode. W przypadku zestawu ASCII reprezentującego litery alfabetu łacińskiego literze *S* odpowiada ciąg *1010011*. Natomiast literze *O* — ciąg *1001111*. Jeśli do komunikacji komputer wykorzystuje znaki 8-bitowe, ciąg jest uzupełniany z przodu zerami do uzyskania standardowej długości. W kodowaniu 8-bitowym litera *S* to *01010011*, a *O* to *01001111*. Szeregi Fouriera pozwalają na wyemitowanie tych znaków w odpowiedni sposób.

Technika zmiany amplitudy sygnału w celu zakodowania danych jest nazywana *modulacją amplitudy* (AM) i stanowi podstawową metodę radiowego przekazywania głosu. Inny sposób kodowania danych to *modulacja częstotliwości*. Dzięki niemu działają radia FM. Trzecie rozwiązanie nazywa się *modulacją fazy* i polega na zmianie fazy sygnału w reakcji na włączenie lub wyłączenie sygnału danych. Faza sygnału okresowego jest określana jako przesunięcie fali względem punktu odniesienia na osi czasu.

Przykłady wszystkich trzech wymienionych modulacji zostały przedstawione na rysunku 5.3. Ich działanie polega na modyfikowaniu fali nośnej w sposób zależny od przenoszonych danych. Z pierwszego przykładu (modulacji amplitudy) wynika, że sygnał danych jest odwzorowany w amplitudzie fali nośnej. Analizując przebieg od lewej do prawej strony, można przyjąć, że maksimum amplitudy odpowiada jedynce logicznej (stanowi włączenia), natomiast minimalny poziom amplitudy wyznacza zero logiczne (stan wyłączenia). W prawej części rysunku widać kolejny wzrost amplitudy, co najprawdopodobniej oznacza kolejną jedynkę. Niemniej amplituda mogłaby również pozostać na niskim poziomie (zależnie od sygnału danych). Stosowanie modulacji amplitudy wymaga wykonywania pomiaru poziomu amplitudy w regularnych odstępach czasu.

### Rysunek 5.3.

*Modulacja amplitudy, częstotliwości i fazy pozwala na zakodowanie danych*



Środkowy przebieg reprezentuje modulację częstotliwości. Analizując go od lewej strony, można zauważyć zmiany między niską częstotliwością, wysoką częstotliwością, niską częstotliwością i znowu wysoką częstotliwością. Okresowy pomiar doprowadziłby do wniosku, że transmitowane są bity 0, 1, 0 i 1.

Modulacja fazy jest nieco bardziej wyrafinowana. W dolnej części rysunku są widoczne dwie zmiany skutkujące powstaniem trzech różnych przebiegów fali nośnej. Modulacja fazy występuje w środkowym fragmencie przebiegu. Przesunięcie fazowe sygnału jest inne niż dwóch pozostałych fragmentów. Zmiany fazy umożliwiają zakodowanie w sygnale użytecznych danych.

## Szerokość pasma

Szerokość pasma ma wiele różnych znaczeń. W komunikacji cyfrowej szerokość pasma kanału, połączenia, łącza lub potoku określa ilość danych, która może zostać przesłana w jednostce czasu. Tak definiowana szerokość pasma odpowiada pojemności. Szerokością pasma można również mierzyć przepustowość kanału, która opisuje maksymalną jego pojemność.

W dalszej części tego rozdziału szerokość pasma należy rozumieć jako przedział częstotliwości sygnału przesyłanego w obwodzie, wyrażany w okresach na sekundę, czyli w hercach. Aby ograniczyć szerokość pasma, trzeba zastosować filtry — filtr dolnoprzepustowy ogranicza sygnał do niskich częstotliwości, a szerokość pasma podstawowego opisuje górną granicę częstotliwościową sygnału.

Amplituda sygnału jest kojarzona z napięciem, które jest sposobem na przedstawienie ciśnienia elektrycznego lub energii potencjalnej w miejscu pomiaru napięcia. W czasie przemieszczania się sygnału w przewodzie, istotną staje się rezystancja tego przewodu, powodująca, że część energii potencjalnej zmienia się na energię kinetyczną. Rezultatem tego zjawiska jest wyprodukowanie ciepła i obniżenie mocy sygnału. Jest to jedna z przyczyn ograniczania długości kabla w niektórych technologiach sieciowych. Energia jest też bezpośrednio zależna od częstotliwości. Fizyk Max Planck dowiódł, że energię fotonu opisuje następująca zależność:

$$E = h n$$

w której  $h$  jest stałą Plancka, a  $n$  reprezentuje częstotliwość. Ze wzrostem częstotliwości rośnie energia. Prawo Plancka nie odnosi się do energii elektronów w przewodzie, ale wynika z niego ogólna zasada, stanowiąca, że utrata energii oznacza przede wszystkim zmniejszenie siły sygnału o wysokich częstotliwościach.

Analiza straty sygnału wykazuje zazwyczaj, że powyżej pewnej częstotliwości poziom sygnału radykalnie się obniża. Próg ten jest nazywany *częstotliwością odcięcia*. Celowe zredukowanie poziomu sygnału powyżej częstotliwości odcięcia sprowadza się do włączenia filtra dolnoprzepustowego. Filtry dolnoprzepustowe ograniczają więc szerokość pasma obwodu. Zmniejszają również poziom zakłóceń w sygnale i umożliwiają wzmocnienie wyższych spośród przenoszonych częstotliwości. Dzięki temu odstęp sygnału od szumu jest większy i można w łatwiejszy sposób przekazywać wyższe częstotliwości sygnału danych w obwodzie.

Gdyby filtr został dobrany w taki sposób, że przenoszone byłyby tylko bardzo niskie częstotliwości (na przykład odpowiadające jedynie pierwszej harmonicznej szeregu Fouriera), sygnał okazałby się tak zniekształcony, że stałby się bezużyteczny. Wraz ze zwiększaniem częstotliwości odcięcia filtra dolnoprzepustowego zwiększa się liczba wyrazów szeregu Fouriera, które są obecne w przenoszonym sygnale. Sam sygnał zaś precyzyjnie odwzorowuje przebieg pierwotny. Odnosząc się do rysunku 5.2, można by stwierdzić, że zwiększenie częstotliwości odcięcia o pewną wartość doprowadziłoby do przeniesienia sygnału o współczynniku harmonicznych  $k=5$ . Natomiast kolejne zwiększenie tej częstotliwości objęłoby również przebieg o współczynniku  $k=15$ .

Szumy, rezystancja, zakłócenia i inne czynniki ograniczają maksymalną częstotliwość sygnału przesyłanego w przewodzie. Liczba zmian stanu sygnału w czasie jednej sekundy wyraża się w *bodach*. W prezentowanych wcześniej przykładach amplitudy przebiegów były znormalizowane do wartości 1. Gdyby jednak zmiany napięcia były dostatecznie duże, aby można było wyróżniać poziomy pośrednie, wówczas bitowa szybkość transmisji również uległaby zmianie. W systemach, które umożliwiają przekazywanie jednocześnie dwóch wartości logicznych, każdy impuls odpowiada dwóm bitom informacji. W porównaniu z systemem przenoszącym jedynie stany 0 i 1 szybkość w bodach pozostaje taka sama, ale szybkość bitowa rośnie dwukrotnie.

## Teoria próbkowania

W poprzednich punktach rozdziału zostały opisane techniki formowania sygnału cyfrowego za pomocą okresowych funkcji trygonometrycznych, takich jak funkcja sinus. Przedstawione zostały również zasady kodowania danych (jedynki i zera logicznych) w celu przeniesienia informacji (SOS). Procedura podziału danych na porcje informacji jest nazywana *próbkowaniem*. Natomiast liczbę porcji informacji w jednostce czasu określa *częstotliwość próbkowania*.

Ilość informacji zawartych w pojedynczym punkcie sygnału danych jest funkcją rozmiaru bitowego próbki. Załóżmy, że analizowany sygnał zmienia okresowo kolory na ekranie. Przenoszona informacja jest wartością koloru. Przyjmijmy, że zaprojektowany system zmienia kolory w sposób ciągły, od czarnego do białego, przez wszystkie odcienie szarości. Ponieważ ludzki umysł w idealnych warunkach może rozróżnić jedynie 1000 różnych odcieni, zapiszmy kolor na 256 różnych poziomach. Liczba ta odpowiada 8-bitowemu punktowi danych.

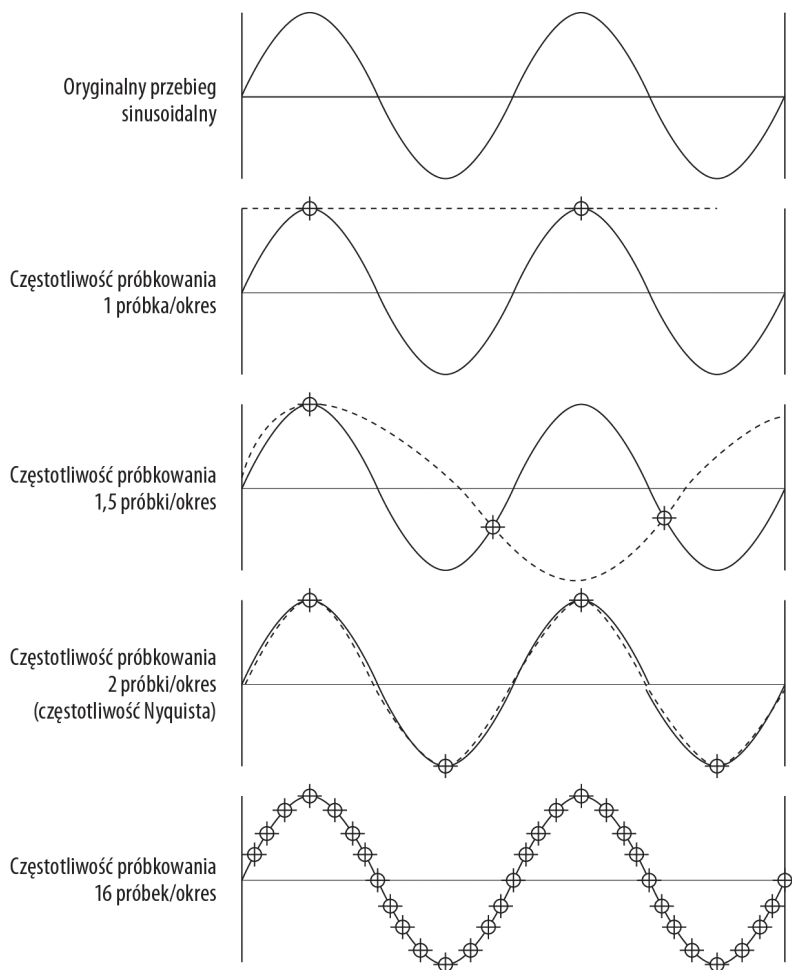
Założmy, że drugi zaprojektowany system ma za zadanie przenosić wszystkie kolory. Aby odwzorować jedną wartość koloru w czasie, można posłużyć się przestrzenią RGB (opisującą kolory: czerwony (*red*), zielony (*green*) i niebieski (*blue*)). Do opisu każdej składowej koloru posłuży 256 wartości (podobnie jak w systemie monochromatycznym). Bitową głębię koloru można wówczas obliczyć jako  $256 \times 256 \times 256$  ( $2^8 \times 2^8 \times 2^8$ ) lub  $2^{24}$ . W tak zdefiniowanej przestrzeni kolorów mamy do dyspozycji 16,8 miliona wartości koloru. Oczywiście można wykorzystać mniejszą lub większą głębię kolorów w zależności od przeznaczenia danych.

W analogiczny sposób można przysyłać dźwięk (muzykę) i emitować go jako sygnał analogowy. Oczywiście nasuwa się wówczas pytanie, ile próbek danych jest do tego potrzebnych? Odpowiedź zależy od przeznaczenia systemu. W przypadku rozmowy telefonicznej częstotliwość próbkowania 8 kHz jest wystarczająca. Chcąc uzyskać lepszą jakość rozmowy, trzeba zapewnić próbkowanie o częstotliwości 11 kHz. Do rejestracji muzyki o niższej jakości (odpowiadającej radiu AM) wystarczą 22 kHz, ale jakość CD wymaga częstotliwości 44 kHz.

Przeanalizujmy teraz sygnał sinusoidalny przedstawiony na rysunku 5.4. Ile próbek należałoby pobrać, aby ustalić częstotliwość fali? Gdyby w każdym okresie była pobierana jedna próbka, podczas próby odtworzenia przebiegu uzyskano by linię prostą. Zwiększenie częstotliwości próbkowania do 1,5 próbki na okres pozwoliłoby na uzyskanie przebiegu sinusoidalnego, ale o niższej częstotliwości niż przebieg odwzorowywany. Pobranie dwóch próbek w jednym okresie umożliwiłoby poprawne odtworzenie częstotliwości sygnału. Jednak aby precyzyjniej odwzorować przebieg pierwotny, należałoby rejestrować próbki z jeszcze większą częstotliwością. Przy wartości 16 próbek na okres można niemal dokładnie oddać przebieg sygnału wejściowego.

**Rysunek 5.4.**

Próbkowanie sygnału sinusoidalnego i częstotliwość próbkowania Nyquista



Z analizy rysunku 5.4 wynika, że dwukrotnie większa częstotliwość próbkowania (w porównaniu z częstotliwością przebiegu badanego) daje możliwość zgromadzenia informacji niezbędnych do ustalenia częstotliwości pierwotnego sygnału. Wyznaczona w ten sposób szybkość próbkowania nazywa się *szybkością próbkowania Nyquista* (została wyznaczona przez Harry'ego Nyquista w 1924 roku). Jeśli pasmo częstotliwościowe sygnału oznaczmy jako  $B$ , to aby odtworzyć ten sygnał, konieczne jest zgromadzenie próbek pobieranych z częstotliwością  $2B$ . Częstotliwość sygnału  $B$  jest nazywana *częstotliwością Nyquista*. Analiza odnosi się do sygnału poddanego działaniu filtra dolnoprzepustowego i transmitowanego w bezzumowym kanale. Zwiększanie częstotliwości próbkowania nie wnosi żadnych dodatkowych informacji, ponieważ wyższe częstotliwości są eliminowane przez filtr.

Z teorii Nyquista opisującej zależność między szerokością pasma  $B$  i maksymalną przepływnością bitową  $C$  wynika, że:

$$C = 2 B \log_2 L$$

$L$  odpowiada liczbie poziomów sygnału wykorzystanych do kodowania próbek. Ton o częstotliwości 262 Hz (reprezentujący dźwięk C4, czyli środkowe C) jest uznawany za medianę wśród nut charakteryzujących ludzki głos. Zgodnie z teorią Nyquista maksymalna przepływność bitowa potrzebna do zarejestrowania wspomnianego tonu w formie cyfrowej wynosi 524 b/s (przy założeniu wartości  $L=2$ ).

W roku 1948 Cladue Shannon opublikował pracę, która matematycznie potwierdziła teorię Nyquista i rozszerzyła ją, dowodząc, że z próbek gromadzonych z częstotliwością 2B można odtworzyć pierwotny sygnał. Ujmując to inaczej, Shannon udowodnił, że przesyłanie sygnału z szybkością 2B jest operacją odwrotną do próbkowania sygnału z częstotliwością 2B. Rozszerzona teoria zyskała miano *twierdzenia o próbkowaniu Nyquista-Shannona*. Prace Shannona są z kolei uznawane przez wielu wykładowców za początek nauki o nazwie „teoria informacji”.

Twierdzenie o próbkowaniu odnosi się do kanału bezszumowego. Jednak w większości kanałów występują szумы, które wprowadzają pewną losowość do zbioru danych. Stopień zawartości szumu w sygnale jest określany jako stosunek sygnału do szumu ( $S/N$ ). Z uwagi na to, że poziom szumu jest zazwyczaj znacznie niższy od poziomu sygnału, współczynnik  $S/N$  przeważnie definiuje się w skali logarytmicznej. Wartość wyrażona w decybelach to  $10 \log_{10} S/N$ . Antena, która tłumi szum odbiornika o 10 dB, zmniejsza poziom szumu w sygnale 10-krotnie. Wysokiej jakości element wieży stereo o współczynniku  $S/N$  równym 75 dB wytworzy dźwięk, w którym stosunek sygnału do szumu będzie wynosił 31 622 776 do 1.

Shannon doszedł do wniosku, że można wyznaczyć maksymalną przepustowość zaszumionego kanału przez zamianę w równaniu Nyquista liczby poziomów sygnału sumą  $1 + S/N$ :

$$C = B \log_2(1 + S/N)$$

Uwzględnienie szumu jest konieczne wówczas, gdy chcemy oszacować maksymalną ilość informacji, którą kanał powinien przenieść. Rozważmy więc kanał z filtrem dolnoprzepustowym o częstotliwości odcięcia wynoszącej 1000 Hz, w którym występuje gaussowski szum termiczny. Współczynnik  $S/N$  w takich przypadkach wynosi zazwyczaj 20 dB, czyli  $S/N = 100$ . Maksymalna przepływność informacji w kanale wynosi więc:

$$C = 1000 \log_2(1+100) = 1000 * 6,658 = 6658 \text{ b/s}$$

Obliczenia wykazują, że analizowany kanał może przenosić sygnały o maksymalnej przepływności 6658 b/s, niezależnie od zastosowanej częstotliwości próbkowania. Wynika z nich również ważny wniosek, że ilość przenoszonych informacji w znacznie większym stopniu zależy od częstotliwości sygnału niż od jakości sygnału (stosunku  $S/N$ ).

W teorii informacji operacje przypisania wartości sygnałom interpretuje się jako formę ujemnej entropii. Oznacza to, że wytworzenie logicznej sekwencji bitów wymaga pewnej energii. Niedostarczenie jej spowodowałoby, że rozkład bitów byłby przypadkowy. Zatem wprowadzanie danych wykraczających poza maksymalną przepływność Shannona byłoby tożsame z wytwarzaniem energii. Ostatecznie jednak najważniejsze jest to, że przedstawiona teoria definiuje maksymalną przepustowość dowolnego kanału.

## Multipleksacja

*Multipleksacja* jest procesem, dzięki któremu określone medium transmisyjne może przetransmitować dwa sygnały (dwa strumienie danych) lub większą ich liczbę. Transmisja multipleksowana jest realizowana w ramach kanału, który z kolei jest ustanowiony między dwoma punktami, tworząc obwód. Przewody, włókna światłowodowe i łącza radiowe są kanałami fizycznymi, nazywanymi fizycznymi obwodami. Kanały danych są więc często nazywane *kanałami wirtualnymi*.

W procesie multipleksacji wykorzystywane jest urządzenie nazywane *multiplekserem* (MUX), które odpowiada za rozdzielanie strumieni danych na poszczególne kanały oraz za składanie strumieni danych z kanałów. Tak naprawdę jest ono połączeniem zasadniczego multipleksera przeznaczonego do łączenia wielu wejść w jedno oraz demultipleksera (DEMUX) realizującego zadanie podziału sygnału na składowe i przesyłania poszczególnych sygnałów składowych do odpowiedniego wyjścia.

Z informacji zamieszczonych wcześniej wiadomo, że istnieją trzy różne techniki modulowania sygnałów nośnych w celu zakodowania w nim danych, są to: modulacja amplitudy, modulacja częstotliwości i modulacja fazy. Multipleksery również wykonują swoje zadania w dziedzinie czasu, częstotliwości i fazy, dokonując podziału (partycjonowania) danych analogowych lub cyfrowych. Taka klasyfikacja umożliwia odróżnienie jednej grupy protokołów od innych lub jednego rodzaju sieci od innych w sposób analogiczny do zasad, które w myśl taksonomii Linneusza definiują drzewo życia, dzieląc je na królestwa, gromady, klasy, rzędy, rodziny, rodzaje i gatunki.

## Multipleksacja z podziałem czasu

Multipleksacja na podstawie czasu — multipleksacja z podziałem czasu (TDM — *Time Division Multiplexing*) — zakłada podział strumienia danych z wykorzystaniem szczelin czasowych. Współdzielenie jednej sieci TDM przez wiele nadajników jest określane mianem *wielodostępu z podziałem czasu* (TDMA — *Time Division Multiple Access*).

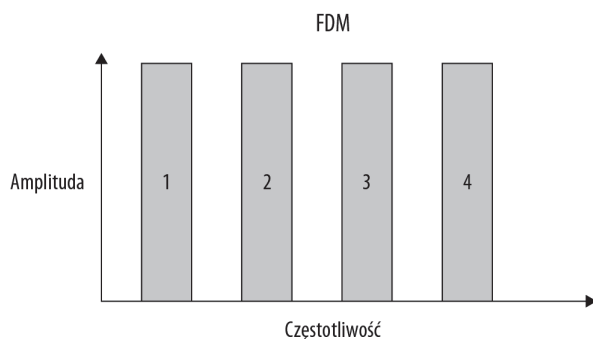
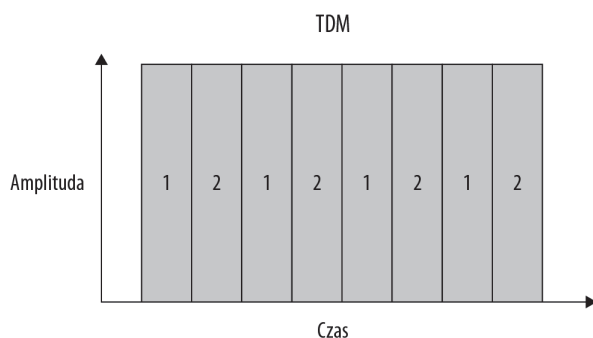
W rozwiązaniu TDM dane analogowe są formowane za pomocą urządzeń nazywanych *kodekami*, które generują strumień danych. Po stronie odbiornika kodek odtwarza pierwotny blok danych na podstawie danych zawartych w poszczególnych szczelinach czasowych. Zasada działania kodeków z pewnością jest znana osobom, które zajmowały się digitalizacją głosu, muzyki lub sekwencji wizyjnych. Operacje te najczęściej bazują na próbkowaniu PCM, czyli modulacji impulsowo-kodowej (ang. *Pulse Code Modulation*). Znacznie rzadziej stosowane są inne techniki modulacji cyfrowych, takie jak modulacja amplitudy impulsu (PAM — *Pulse Amplitude Modulation*), modulacja szerokości impulsu (PWM — *Pulse Width Modulation*) czy modulacja położenia impulsu (PPM — *Pulse Position Modulation*).

Do wyznaczania kolejności cyfrowych danych wykorzystuje się różne techniki. W traktach T- i E- multipleksacji podlegają grupy kanałów. System TDM emituje co 125  $\mu$ s ramkę składającą się z danych pozyskanych z 32 kanałów w przypadku traktu E1 oraz z 25 kanałów w przypadku traktu T1. Istnieją różne standardy formowania sekwencji ramek TDM, w których bity kontrolne są dodawane na końcu danych użytkowych w ramach poszczególnych

kanałów lub na końcu poszczególnych ramek. Do przenoszenia informacji sterujących stosuje się takie same techniki podziału czasowego. Ilustracją do omawianego mechanizmu jest rysunek 5.5.

### Rysunek 5.5.

Porównanie  
multipleksacji  
z podziałem czasu  
z multipleksacją  
z podziałem  
częstotliwości



Szczegółowe informacje na temat linii T i E zostały zamieszczone w rozdziale 13.

Multipleksowane dane są również poddawane kompresji cyfrowej. Wykorzystuje się do tego celu różne metody, opisywane standardami przemysłowymi lub będące własnością firm telekomunikacyjnych. Jednym z powszechnie stosowanych rozwiązań jest *różnicowa modulacja impulsowo-kodowa*. Jej działanie polega na obliczeniu amplitudy sygnału w danej szczeliny czasowej i wyznaczeniu różnicy między wartością z danej szczeliny i wartością właściwą dla następnej szczeliny. Kodek wysyła strumień danych reprezentujący jedynie różnice. Efekt kompresji uzyskuje się dzięki temu, że wartość różnicy nigdy nie przekracza pewnej wartości progowej. Jeśli poziom dźwięku zmienia się bardzo istotnie między dwoma szczelinami czasowymi, wówczas mechanizm kompresji wykorzystuje kolejne szczeliny do doprowadzenia poziomu kodowanego sygnału do poziomu oryginalnego przebiegu.

Na przykład jeśli w danym systemie dźwięk jest rejestrowany na 256 poziomach ( $2^8$ ), można wprowadzić założenie, że między kolejnymi szczelinami nigdy nie wystąpi zmiana o więcej niż 8 poziomów. Wówczas zamiast kodować 8-bitowe próbki sygnału, system umożliwiłby przesyłanie jedynie trzech bitów informacji na szczelinę.

Inna technika, nazywana *modulacją delta*, zakłada zapisywanie zmian tylko za pomocą jednego bitu. Jednak aby wynikowy strumień danych precyzyjnie odwzorowywał sygnał wejściowy, częstotliwość próbkowania w modulacji delta musi być bardzo wysoka. Znanе są również bardziej zaawansowane mechanizmy kompresji, których działanie bazuje na kodowaniu predykcyjnym. Zapewniają one jeszcze skuteczniejsze zmniejszanie rozmiaru danych, ale kosztem jakości sygnału oraz dodatkowego narzutu związanego z przetwarzaniem danych.

## Multipleksacja z podziałem częstotliwości

Multipleksacja na podstawie częstotliwości — multiplikacja z podziałem częstotliwości (FDM — *Frequency Division Multiplexing*) — również wykorzystuje techniki wydzielania różnych sygnałów z pojedynczego strumienia danych. Współdzielenie pojedynczego kanału przez wielu użytkowników technologii FDM nazywa się wielodostępem z podziałem częstotliwości (FDMA — *Frequency Division Multiple Access*). Algorytmy FDMA są stosowane na przykład do rozdzielania radiowych sygnałów pochodzących z różnych nadajników. Znajdują także zastosowanie w telefonii komórkowej, w której obszary działania poszczególnych stacji bazowych nakładają się na siebie.

Multipleksacja FDM może być wykorzystywana do przesyłania danych analogowych i cyfrowych. Jednak ogólniejsza zasada stanowi, że dane cyfrowe łatwiej przysyła się w obwodach TDM, a analogowe w obwodach FDM. Medium transmisyjnym w sieciach FDM może być zarówno kabel, jak i łącze mikrofalowe. Technika FDM jest wykorzystywana w wielu rozwiązaniach kablowych, choć na przykład w przypadku transmisji we włóknach światłowodowych jest nazywana multipleksacją z podziałem długości fali (WDM — *Wavelength Division Multiplexing*), mimo że idea działania jest taka sama. Multipleksacja TDM jest w zasadzie jedynym praktycznie wykorzystywanym rozwiązaniem w transmisji danych cyfrowych.

Przykłady rozwiązań TDM i FDM zostały przedstawione na rysunku 5.5. Poszczególne kanały są na nim oznaczone za pomocą odpowiednio ponumerowanych prostokątów. Transmisja TDM polega na naprzemiennym przekazywaniu danych kanału 1. i 2. Wynikowy strumień danych jest w pełni wykorzystany i składa się z bitów pobieranych w kolejnych szczelinach czasowych z każdego z kanałów. W przypadku rozwiązania FDM kanały są rozdzielone na cztery niezależne przedziały częstotliwościowe — każdy z przedziałów przenosi dane jednego kanału.

Mimo że na rysunku kolejne pasma częstotliwościowe zostały rozdzielone pewnymi pasmami ochronnymi, w praktycznych implementacjach technologii FDM kanały są rozmieszczone tak blisko siebie, że nawet w pewnym stopniu na siebie zachodzą. Nakładanie jest możliwe dzięki temu, że filtry pasmowe mają charakterystyki o ostro nachylonych zboczach, umożliwiającących odseparowanie sygnałów. Na rysunku pasma ochronne zostały przedstawione jako odstępy między czterema kanałami częstotliwościowymi.



W systemach FDM wydzielane są grupy pierwotne złożone z 12 kanałów o szerokości 4000 Hz oraz pasm ochronnych o szerokości 500 Hz, występujących na początku i końcu grupy pierwotnej (3000 Hz + 2x500 Hz). Szerokość pasma kanału odpowiada szerokości potrzebnej do przenoszenia głosu. Zbiór pięciu grup stanowi supergrupę (grupę wtórną), natomiast pięć lub dziesięć supergrup wyznacza grupę nadrzędną.

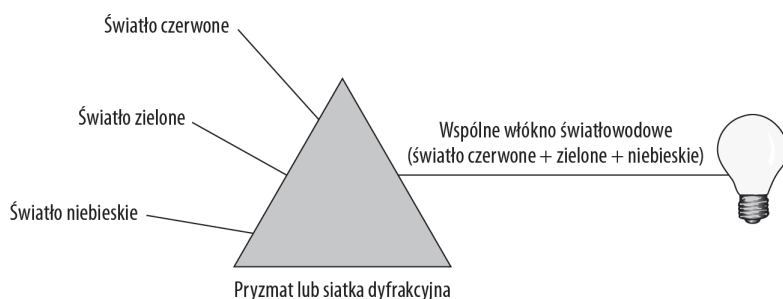
## Inne techniki multipleksacji

Ponieważ długość fali i częstotliwość są ze sobą nierozdzielnie związane szybkością światła, można by sądzić, że technika FDM będzie stosowana również w sieciach optycznych. Jednak ze względów historycznych w rozwiązaniach sieci optycznych multipleksacja w dziedzinie częstotliwości jest nazywana *multipleksacją z podziałem długości fali* (WDM — *Wavelength Division Multiplexing*).

Aby utworzyć łącze WDM, należy po jednej stronie pryzmatu umieścić włókna światłowodowe przenoszące światło o różnych zakresach częstotliwościowych. Natomiast po drugiej stronie pryzmatu musi być zainstalowany światłowód, który odbierze połączone wiązki światła. Zasada działania systemu WDM z pryzmatem lub siatką dyfrakcyjną została przedstawiona na rysunku 5.6.

### Rysunek 5.6.

Rozdzielanie  
i złączanie wiązek  
światła w systemie  
WDM



W rozdziale 13. zostały omówione zasady multipleksacji w łączach międzysieciowych oraz protokoły wykorzystujące tę technikę.

W wielu sieciach optycznych stosowane są techniki multipleksacji polegające na polaryzacji strumienia danych. Światło można spolaryzować na wiele sposobów. Jednak jednym z najczęściej stosowanych rozwiązań jest użycie *multiplekserów dołączających-odłączających* (ADM — *Add-Drop Multiplexer*). Multipleksery ADM zazwyczaj bazują na interferometrach Fabry-Perota w celu wydzielenia lub dołączania wiązek światła o określonej długości fali. Najnowsze wersje tych urządzeń, nazywane *konfigurowalnymi optycznymi multiplekserami dołączającymi-odłączającymi* (ROADM — *Reconfigurable Optical Add-Drop Multiplexer*), są szczególnie często stosowane w sieciach metropolitalnych. Niemniej nie wszystkie sieci optyczne wykorzystują polaryzację światła. W powszechnie stosowanych optycznych sieciach SDH/SONET komunikacja bazuje na algorytmie TDM realizowanym przez impulsowo działające lasery i diody LED.

Polaryzacja sygnału występuje również w komunikacji na częstotliwościach radiowych. Sygnał jest polaryzowany podczas emitowania przez anteny z fazowaną matrycą w celu utworzenia kanałów typu MIMO (o wielokrotnych wejściach i wielokrotnych wyjściach). Odtworzenie sygnału następuje w odbiorczych antenach z fazowaną matrycą. Działanie rozwiązania jest zbliżone do funkcjonowania radaru. Sieci bezprzewodowe MIMO są coraz popularniejsze w domowych bezprzewodowych sieciach komputerowych, ponieważ umożliwiają ustanawianie połączeń o wysokiej przepustowości.



Multipleksacja częstotliwości radiowych również jest opisywana akronimem FDM, co czyni nomenklaturę jeszcze bardziej niezrozumiałą.

Istnieją jeszcze inne formy multipleksacji, które są szczególnie istotne w sieciach komórkowych. Wśród nich najczęściej stosowanym rodzajem transmisji radiowej jest technika rozpraszania widma przez skakanie po częstotliwościach (FHSS — *Frequency-Hopping Spread Spectrum*). Działanie mechanizmu polega na szybkiej zmianie częstotliwości sygnału nośnego. Kolejne dobierane częstotliwości pochodzą z określonego zbioru, ale ich dobór ma charakter pseudolosowy. Oczywiście urządzenia nadawcze i odbiorcze znają kolejność oraz czas zmian częstotliwości. Jednak dla innych wąskopasmowych odbiorników rejestrowany sygnał jest szumem. Fakt ten sprawia, że technika FHSS jest uznawana za bardzo bezpieczną.

Mechanizm skakania po częstotliwościach został opatentowany przez kompozytora George'a Antheila i aktorkę Hedy Lemarr w 1942 roku, którzy wykorzystali urządzenie do zapisu nut w pianoli do przełączania radia między 88 różnymi częstotliwościami. Rozwiązanie miało uniemożliwić zakłócenie komunikacji z radiowo sterowanymi torpedami. System nigdy nie został wdrożony, ale wraz z opracowaniem sieci komórkowych stał się znany pod nazwą wielodostępu ze zwielokrotnieniem kodowym (CDMA — *Code Division Multiple Access*).

## Sterowanie przepływem

Podczas przekazywania danych przez sieć często występuje różnica między szybkością, z jaką system może przetwarzać informacje, a szybkością odbierania danych. Problem uwidacznia się wtedy, gdy system odbiorczy wolniej przetwarza i (lub) buforuje dane, niż są one generowane i wprowadzane do sieci przez system nadawczy. Jeśli system odbiorczy pełni funkcję jednostki docelowej dla strumieni danych pochodzących z wielu innych stacji, wspomniana niezgodność występuje znacznie częściej. Kolejnym problemem jest przeciążenie segmentu sieci, który uniemożliwia systemom odbiorczym odtworzenie danych we właściwym czasie. Zarządzanie przepływem danych jest rozwiązaniem implementowanym w różnych warstwach modelu OSI i obejmuje generowanie komunikatów sterujących, buforowanie danych, stosowanie schematów zależności czasowych itp.

Sterowanie przepływem danych może być implementowane w urządzeniach określanych jako terminale danych (DTE — *Data Terminal Equipment*), w przełącznikach i routerach, a także na poziomie obwodu w urządzeniu kończącym obwód (DCE — *Data Circuit-terminating Equipment*). Wymienione urządzenia nadzorują transmisję przez zmianę szybkości przepływu danych w jednym z dwóch kierunków. Na końcu każdego połączenia musi znajdować się jedno z urządzeń DTE lub DCE.

Problem przepływu danych dotyczy również modemów. Dlatego jednym z realizowanych przez nie zadań jest negocjowanie parametrów wzajemnego połączenia. Ma ono na celu ustalenie zbioru protokołów wykorzystywanych w czasie sesji komunikacyjnej, wybranie szybkości transmisji itp. Większość nowoczesnych modemów pracuje z przepływnością 56 kb/s (jeśli zdołają nawiązać połączenie z pełną szybkością), czyli przekraczającą teoretyczną szybkość transmisji danych Nyquista. Jest to możliwe dzięki zastosowaniu kompresji i innych technik optymalizacyjnych. Niestety, jakość połączeń telefonicznych jest zmienna

(często zmiany mają dość duży zakres), przez co konieczne jest uruchomienie mechanizmów sygnalizujących bieżący stan linii oraz poziom szumów. Wymiana informacji na ten temat jest elementem procedury nawiązywania połączenia, w czasie której modemy nadawczy i odbiorczy negocjują szybkość transmisji danych oraz zestaw protokołów.

Większość modemów wykorzystuje jedną z dwóch form kontroli przepływu danych. Pierwsza polega na przesyłaniu z modemu do komputera instrukcji nazywanych poleceniami XON/XOFF. Komunikaty XON/XOFF mogą być również przekazywane z komputera do modemu. Taki sposób regulowania ruchu nazywa się *programową kontrolą przepływu* (modemy mogą być implementowane programowo). Gdy połączenie jest realizowane bez pętli zwrotnej, tak jak w przypadku opisywanych poleceń, mechanizm kontroli nazywa się sterowaniem przepływem z otwartą pętlą sprzężenia zwrotnego. W jego działaniu nie jest wykorzystywana komunikacja między nadajnikiem a odbiornikiem. Decyzje są podejmowane na podstawie wyników innych operacji, na przykład alokacji zasobów dokonywanych przez mechanizm rezerwacji zasobów. Taki sposób sterowania przepływem danych jest typowy dla sieci ATM.

Drugie rozwiązanie polega na wykorzystaniu znaków sterujących lub odpowiednich linii portu szeregowego (portu RS232) w celu przesłania informacji sterującej do zdalnego systemu. Ta technika jest określana jako *sprzętowa kontrola przepływu*. Typowymi sygnałami kontrolnymi są: gotowość terminalu danych (DTR — *Data Terminal Ready*), gotowość zbioru danych (DSR — *Data Set Ready*), gotowość do nadawania (CTS — *Clear to Send*) oraz żądanie nadawania (RTS — *Request to Send*). Często stan poszczególnych linii jest sygnalizowany za pomocą diod świecących na obudowie modemu. W sprzętowym sterowaniu przepływem danych wykorzystywana jest zależność nadrzędny-podrzędny (ang. *master-slave*). Moduł DTE pełni funkcję urządzenia nadrzędnego, które wysyła sygnały informujące o swoim stanie. Urządzenie podrzędne (DCE) odpowiada na otrzymane informacje. W połączeniu modemowym z komputerem PC linie DTR/DSR są wykorzystywane do utworzenia sesji modemowej, a linie RTS/CTS sterują przepływem danych.

Mechanizmy sterowania przepływem informacji są również wbudowywane bezpośrednio w protokoły. Protokół TCP (protokół warstwy transportowej modelu OSI oraz warstwy internetowej modelu TCP/IP) generuje pakiety zawierające informacje o numerze sekwencyjnym (potrzebnym do odtworzenia kolejności pakietów), priorytecie pakietu itp. Po odebraniu pakietu odsyłane są komunikaty sygnalizujące ewentualny brak pewnych pakietów, wykrycie błędu w pakiecie lub zbyt długi czas dostarczania pakietu. Jeśli dane uda się poprawnie odtworzyć, transfer jest uznawany za poprawny. Opisany mechanizm powiadomień jest formą zamkniętej pętli sprzężenia zwrotnego.

Protokół TCP nie jest jedynym protokołem wykorzystującym system powiadamiania (sygnalizacji) o poprawnym dostarczeniu danych. Protokół Frame Relay — protokół warstwy łącza danych stosowany do łączenia sieci LAN z sieciami WAN — generuje ramki o zmiennej długości przenoszące pakiety. W technologii Frame Relay nie ma co prawda mechanizmów sterowania przepływem danych lub powiadamiania o dostarczeniu danych, ale są zaimplementowane rozwiązania zapewniające powiadamianie o przeciążeniu sieci oraz gwarantujące określoną przepływność danych. Dwa dodatkowe bity sterujące w nagłówku ramki informują system nadawczy o przeciążeniu sieci. Odczytanie wartości tych bitów wymusza na nadajniku zmniejszenie szybkości generowania danych.

## Inżynieria ruchu

Inżynieria ruchu obejmuje zbiór technologii, które są wykorzystywane do sterowania ruchem w sieciach pakietowych, takich jak sieci TCP/IP, czyli internet. Wśród stosowanych rozwiązań wyróżnia się *kształtowanie ruchu* (sterowanie przepływem pakietów w zależności od rodzaju ich zawartości), techniki *zapisz i przekaż* (reprezentowane przez algorytm „cieknącego wiadra”) lub *buforowanie* (algorytm „wiadra z żetonami”). Wszystkie wymienione metody sterowania przepływem informacji są wykorzystywane w celu wymuszenia określonych poziomów jakości usługi, a tym samym regulowania i monitorowania szerokości pasma w połączeniach klienckich.

### Kształtowanie ruchu

Kształtowanie ruchu nie ogranicza się jedynie do sterowania przepływem przez nadzorowanie szybkości przesyłania danych. Jak wiadomo, segmenty można kategoryzować na podstawie użytego protokołu lub numerów portów, do których są adresowane. Parametry te można wykorzystać w regułach opisujących sposób przetwarzania pakietów. Na przykład jeden z dostawców usług internetowych, weryfikując pakiety, sprawdza, czy nie pochodzą one z usługi BitTorrent. Jeśli tak, nadaje im niski priorytet i przesyła z bardzo małą przepływnością w łączu dostępowym. Pakiety BitTorrent można łatwo rozpoznać po charakterystycznym nagłówku, który rozpoczyna się od wartości 19 i zawiera 19-bajtowy ciąg inicjalizacyjny.

Jeśli dany pakiet zostanie rozpoznany jako element strumienia telefonii internetowej (VoIP — *Voice over IP*), dostawca może zwiększyć jego priorytet, zapewniając odpowiedni poziom usługi. Z kolei inny dostawca (na przykład duża firma telekomunikacyjna) może obniżyć wartość QoS pakietu VoIP, aby nie konkutował on z pakietami rozmów telefonicznych generowanych w sieci tego dostawcy. Taki los spotyka w niektórych sieciach pakiety Skype’a. Część kablowych firm ISP tę samą politykę stosuje również w odniesieniu do strumieni wideo.

Kształtowanie ruchu, jak każde inne narzędzie, może być stosowane w dobrych i złych celach. Jednak brak mechanizmów kształtowania ruchu uniemożliwiłby operatorom sieci publicznych zapewnienie odpowiedniego poziomu obsługi, wynikającego z umów zawartych z klientami.

W sieciach ATM weryfikacja komórek odbywa się na podstawie *ogólnego algorytmu wyznaczania szybkości komórek* (GCRA — *Generic Cell Rate Algorithm*). Operacja ta pozwala ustalić, czy komórki odpowiadają regułom zdefiniowanym w odniesieniu do konkretnego obwodu wirtualnego. Komórka to specjalnie sformatowany pakiet danych o niewielkim rozmiarze, przesyłany w sieciach ATM i innych systemach o podobnym działaniu. W zależności od szybkości napływania oraz wariancji szybkości napływania komórki są przekazywane, opóźniane lub odrzucane. Algorytm GCRA zmienia ustawienia bitów (komórki ATM) odpowiedzialnych za sterowanie przepływem, modyfikując automatycznie szybkość przekazywania danych. W sieciach ATM stosuje się rozwiązania opisywane jako *kontrola dostępu*, *rezerwacja zasobów* oraz *kontrola przeciążeń przez zmianę szybkości*.



Komórki zostały szczegółowo opisane w rozdziale 13.

Mechanizm kontroli dostępu jest rozwiązaniem polegającym na przypisywaniu ruchowi wprowadzanemu do sieci odpowiednich wartości szerokości pasma i opóźnienia. Rezerwacja zasobów oznacza wydzielenie pewnych zasobów sieciowych do przenoszenia strumieni danych konkretnych aplikacji. Technikę tę często stosuje się do obsługi rozgłoszeń. Kontrola przeciążeń przez zmianę szybkości transmisji działa niemal identycznie jak automatyczne sterowanie światłami ulicznymi. Ruch wprowadzany do sieci jest utrzymywany na stałym poziomie, co pozwala na ograniczenie przeciążeń sieci.

W sieciach IP kształtowanie ruchu sprowadza się do weryfikacji nagłówków pakietów przesyłanych w połączeniu IP. Jeśli pakiet spełnia kryteria dopasowania zdefiniowanej reguły, realizowana jest czynność powiązana z tą regułą. W ten sposób można ograniczyć szerokość pasma w odniesieniu do określonego typu danych lub adresu IP. Operacja tego typu jest nazywana *dławieniem przepływności*. Ten sam mechanizm służy również do zmiany maksymalnej szybkości przekazywania danych lub do przekierowywania ruchu. Oprócz kształtowania ruchu wykorzystuje się również techniki definiowania *polityki ruchu*. Różnica między wspomnianymi mechanizmami polega na tym, że wyznaczenie polityki ruchu powoduje odrzucanie lub oznaczanie pakietów.

Jak nietrudno się domyślić, kształtowanie ruchu jest bardzo często stosowanym rozwiązaniem w sieciach ISP i jest postrzegane jako forma *inżynierii ruchu*. Kształtowanie ruchu można również interpretować jako technologię zapewnienia odpowiedniej jakości obsługi, co jest często stosowanym sposobem opisu całego mechanizmu przez dostawców usług internetowych.

Funkcje kształtowania ruchu są zazwyczaj uruchomione w oprogramowaniu działającym w urządzeniach brzegowych sieci. Niektóre firmy, takie jak Packeteer, oferują specjalne moduły kształtowania ruchu (np. PacketShaper — w działaniu tego urządzenia zostały uwzględnione wszystkie metody opisane w tym podrozdziale). W czerwcu 2008 roku firma Packeteer została przejęta przez Blue Coat Systems (<http://www.bluecoat.com>).

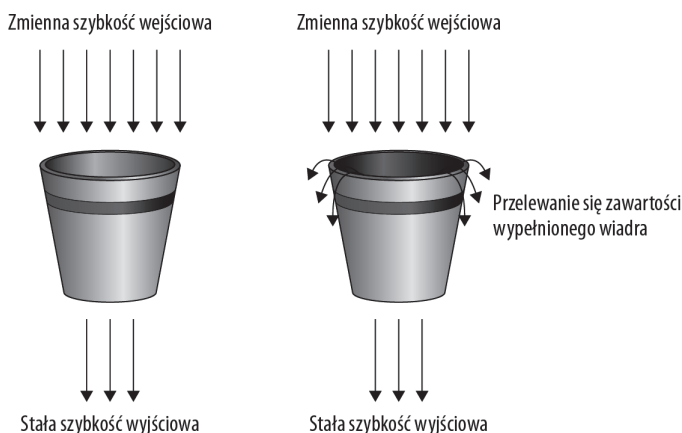
## Algorytm ciekącego wiadra

Mechanizmy odpowiedzialne za kształtowanie ruchu wykorzystują różne metody gromadzenia i przekazywania pakietów. Typowe rozwiązanie polega na umieszczeniu komórek ATM lub pakietów IP w buforze, a następnie zastosowaniu odpowiedniego algorytmu do określenia sposobu ich wysyłania. Do opróżniania bufora, odgrywającego w tym przykładzie rolę *wiadra*, można zastosować technikę opóźniania pakietów — zgodnie z ideą *cieknącego wiadra* — która spowoduje utworzenie zależności FIFO (pierwszy element wejściowy kolejki jest pierwszym elementem wyjściowym), zapewniającej odbiór strumienia o zmiennej szybkości i wysyłanie danych z ustaloną (zazwyczaj mniejszą) szybkością.

Rezultat jest analogiczny do wywiercenia małych dziurek w dnie wiadra, a następnie napełnienia go wodą. Urządzenie odpowiedzialne za kształtowanie ruchu reguluje średnicę dziurek, a przez to szybkość transmisji strumienia wyjściowego. Jeśli szybkość napływania danych przepełni bufor, pakiety „wyleją się z wiadra” i zostaną odrzucone. Idea działania mechanizmu została przedstawiona na rysunku 5.7.

**Rysunek 5.7.**

Algorytm ciekącego wiadra zapewniający stałą szybkość strumienia wyjściowego



Implementacja algorytmu ciekącego wiadra nie stanowi trudności, jeśli rozmiar napływających pakietów jest stały, szybkość ich dostarczania przewidywalna, a łączny rozmiar pakietów zgromadzonych we wiadrze zapewnia utrzymanie określonej szybkości wysyłania danych. Rozwiązanie to okazuje się jednak nieefektywne, gdy rozmiar pakietów się zmienia lub gdy strumień wchodzący ma charakter zbitek danych (następuje krótkookresowy wzrost natężenia ruchu). Oczywiście największą jego wadą jest odrzucanie nadmiarowych pakietów podczas bardzo dużego natężenia ruchu (przekraczającego pojemność wiadra). W celu zwiększenia efektywności działania mechanizmu ciekącego wiadra wyposażono go w algorytm zliczania bajtów.

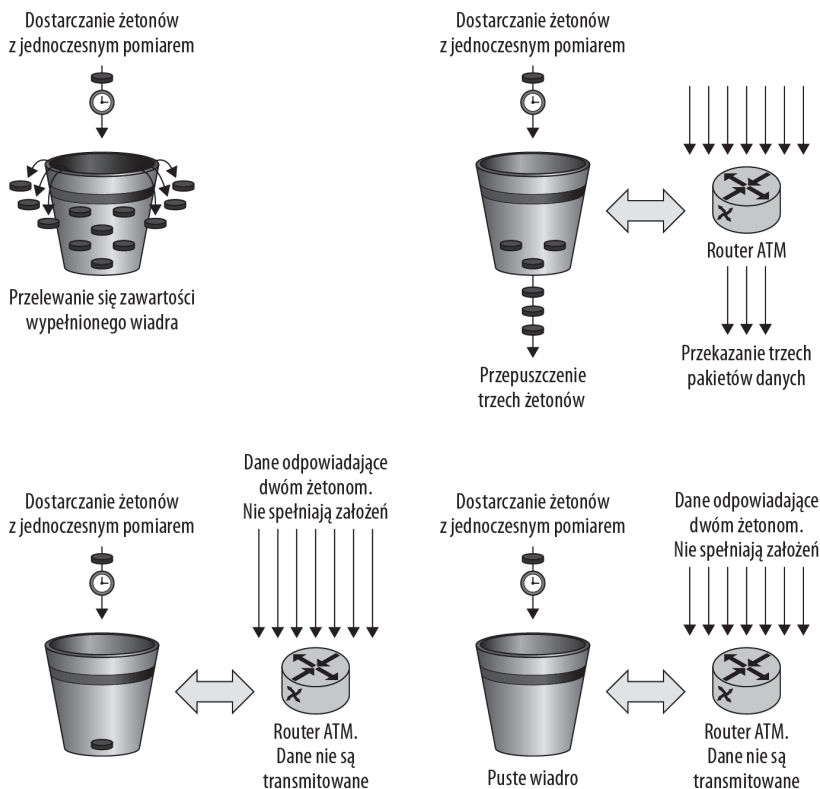
## Algorytm wiadra z żetonami

Drugi z mechanizmów stosowanych w sterowaniu przepływem danych to algorytm *wiadra z żetonami*. W jego działaniu uwzględniono funkcję nadzorowania tego, ile danych może być transmitowanych w sieci, oraz dodano procedurę zliczania bajtów, brakującą w algorytmie ciekącego wiadra. Rozwiązanie znajduje zastosowanie zarówno w obsłudze ruchu o stałym natężeniu, jak i ruchu, którego natężenie okresowo się nasila. W przeciwieństwie do techniki ciekącego wiadra, generującej strumień o stałej przepływności, metoda wiadra z żetonami cechuje się znacznie większą elastycznością w generowaniu strumieni o różnej przepływności.

Działanie mechanizmu jest następujące. Wiadro jest wypełnione żetonami reprezentującymi ilość danych, która może zostać wysłana. Gdy dane są usuwane, żeton odpowiadający określonej ilości danych również jest usuwany z wiadra. Brak żetonów oznacza, że dane nie są transmitowane. Jeśli we wiadrze znajdują się żetony, dane mogą być wysyłane z określoną częstotliwością. Gdy wiadro zapełni się żetonami, ewentualne kolejne żetony będą odrzucane. Rysunek 5.8 stanowi ilustrację do tego opisu.

W tym rozwiązaniu administrator sieci przypisuje żetonom odpowiedni rozmiar bajtowy. Napływanie żetonów do wiadra następuje ze stałą częstotliwością. Wiadro ma jednak ograniczoną pojemność. Po odebraniu pakietu o określonym rozmiarze z wiadra usuwane są żetony w liczbie odpowiadającej rozmiarowi pakietu. Jeśli nie ma dostatecznej liczby żetonów we wiadrze, pakiet jest odrzucany, przechowywany w buforze lub odpowiednio oznaczany i przesyłany.

**Rysunek 5.8.**  
 Algorytm wiadra  
 z żetonami  
 zapewniający  
 zmienną  
 przepływność  
 wyjściowego  
 strumienia danych



## Jakość usługi

Mechanizmy gwarantowania określonego poziomu jakości usługi (QoS) są elementami inżynierii ruchu, których celem jest zapewnienie, że określona usługa otrzyma odpowiednią ilość zasobów sieciowych. Doskonałym przykładem działania mechanizmu QoS jest zapewnienie aplikacji czasu rzeczywistego (generującej informacje wrażliwe na opóźnienia) określonej przepustowości w obwodzie, z którego będzie korzystała. Rozwiązania QoS są szczególnie istotne w telefonii internetowej, grach internetowych, podczas strumieniowania sekwencji wizyjnych i w innych tego typu aplikacjach. Metody QoS są stosowane tylko wtedy, gdy sieć ma ograniczoną przepustowość lub jest przeciążona. Rozwiązania QoS są implementowane w serwerowych systemach operacyjnych, takich jak Windows Server.

QoS nie stanowi metryki, za której pomocą mierzone jest opóźnienie, stosunek sygnału do szumu, częstość odpowiedzi lub inna wielkość, choć parametry te mogą być uwzględnione w działaniu mechanizmu QoS. Same metryki są klasyfikowane jako *poziomy obsługi* (GoS — *Grade of Service*). Akronim QoS jest zarezerwowany jedynie do opisu dostępu do zasobów. Obydwa pojęcia są często ze sobą mylone.

Aby zrozumieć mechanizmy QoS, przeanalizujemy ich implementację w sieciach ATM, w których wyróżniono kilka kategorii usług na poziomie protokołu transportowego. Każda z kategorii jest uwzględniona bezpośrednio w działaniu interfejsów sieciowych ATM oraz przełączników ATM. Ich celem jest zapewnienie właściwej obsługi różnych klas użytkowników sieci.

Dostępne klasy usług ATM to:

- ♦ **Stała przepustowość (CBR — *Constant Bit Rate*).** W tej kategorii nie ma sterowania przepływem danych ani sprawdzania błędów. Klasa CBR jest stosowana w połączeniach E1.
- ♦ **Nieustalona przepustowość (UBR — *Unspecified Bit Rate*).** W tej kategorii nie są stosowane powiadomienia o przeciążeniu sieci. Nie ma również gwarancji przepustowości. Komórki są przekazywane w sieci ATM do wyczerpania pojemności sieci. W przypadku przekroczenia pojemności sieci komórki są odrzucane. Jeśli pojemność nie została wyczerpana, komórki są przesyłane. Z trybu UBR korzystają zazwyczaj programy zawierające własne mechanizmy sterowania przepływem danych i detekcji błędów. Jest to kategoria idealna dla serwerów poczty i serwerów FTP (przesyłania plików).
- ♦ **Przepustowość zmienna w czasie rzeczywistym (RT-VBR — *Real Time Variable Bit Rate*).** Ta kategoria jest wykorzystywana przez aplikacje, które dostarczają dane w sposób nieliniowy. Przykładem może być system wideokonferencyjny, który z uwagi na zastosowanie kompresji generuje ramki w sposób nieliniowy. Tryb RT-VBR gwarantuje określoną pojemność kolejek, aby odtwarzanie sekwencji wideo było niezakłócone i przebiegało w sposób gwarantujący efektywne wykorzystanie kompresji.
- ♦ **Przepustowość zmienna nie w czasie rzeczywistym (NRT-VBR — *Non-Real Time Variable Bit Rate*).** Jest przeznaczona dla aplikacji, które wymagają sterowania przepływem, ale dopuszczają zmienność strumienia danych. Przykładem usługi, która mogłaby korzystać z trybu NRT-VBR, jest usługa wydruku.
- ♦ **Dostępna przepustowość (ABR — *Available Bit Rate*).** Ta kategoria umożliwia przekazywanie danych w sieci z szybkością wynikającą z bieżącej dostępności pasma. Jest przeznaczona do obsługi ruchu o chwilowych wzrostach natężenia oraz do optymalnego wykorzystania pojemności sieci w czasie, w którym ruch utrzymuje się na niskim poziomie. Ruch generowany przez serwery WWW jest doskonałym zastosowaniem usługi ABR.

Dostawcy usług sieciowych korzystają z usług ABR wówczas, gdy spodziewają się krótkookresowego wzrostu obciążenia. Dzięki temu unikają zwiększania pojemności sieci w inwestycjach o krótkim czasie trwania. Aby zaimplementować usługę ABR, trzeba wdrożyć system powiadamiania jednostek nadawczych o przeciążeniu i konieczności zmniejszenia strumienia danych.

Zestawienie poszczególnych kategorii usług ATM znajduje się w tabeli 5.1.

Na podstawie wymienionych kategorii usług operatorzy sieci ATM mogą sporządzać *umowy dotyczące jakości usług* (SLA — *Service Level Agreement*), które gwarantują użytkownikom dostęp do zasobów sieciowych. W umowie jest zawarty opis ruchu włącznie z ewentualnym wskazaniem szerokości pasma i (lub) bieżącej przepływności bitowej oraz z wyszczególnieniem sposobu pomiaru strumienia danych. Pomiary mogą dotyczyć następujących parametrów ruchowych: *stała szybkość przysyłania komórek* (SCR — *Sustained Cell Rate*), *szczytowa szybkość przysyłania komórek* (PCR — *Peak Cell Rate*), *minimalna szybkość przysyłania komórek* (MCR — *Minimum Cell Rate*), *stopa błędnych komórek* (CER — *Cell Error Rate*), *stopa utraty komórek* (CLR — *Cell Loss Rate*), *opóźnienie w dostarczaniu*

**Tabela 5.1.** *Kategorie usług ATM*

	Sterowanie przepływem	Krótkookresowe wzrosty natężenia ruchu	Kontrola przeciążenia	Działanie w czasie rzeczywistym
<b>ABR</b>	Możliwe	Tak	Tak	Nie
<b>CBR</b>	Tak	Nie	Nie	Tak
<b>RT-VBR</b>	Tak	Nie	Nie	Tak
<b>NRT-VBR</b>	Tak	Tak	Nie	Nie
<b>UBR</b>	Nie	Tak	Nie	Nie

*komórek (CTD — Cell Transfer Delay), stopa poważnie uszkodzonych bloków komórek (SECBR — Severely Errored Cell Block Ratio), tolerancja zmienności opóźnienia komórek (CDTV — Cell Delay Variation Tolerance), zmienność opóźnienia komórek (CDV — Cell Delay Variation), stopa błędnie przesłanych komórek (CMR — Cell Misinsertion Rate). Wartości poszczególnych ustawień są wyznaczane niezależnie dla każdego połączenia ATM.*

## Podsumowanie

W tym rozdziale zostały zamieszczone podstawowe informacje z zakresu teorii sygnałów i teorii informacji. Stanowią one podstawę działania wszystkich sieci. Dzięki nim można rozróżniać poszczególne sieci i weryfikować, co jest wykonalne, a czego nie można zrealizować w danej sieci.

Złożone strumienie danych są opisywane matematycznie za pomocą takich technik jak analiza Fouriera. Dzięki nim możliwe jest przechowywanie informacji i odtwarzanie ich w późniejszym czasie. Odtworzenie danych jest determinowane procedurą próbkowania. Istnieje bowiem teoretyczne ograniczenie w częstotliwości próbkowania, które gwarantuje użyteczność danych o określonej szerokości pasma.

Przenoszenie różnych strumieni danych w jednym segmencie sieci jest możliwe dzięki tworzeniu kanałów komunikacyjnych. Są one wydzielane na wiele różnych sposobów — na podstawie czasu, częstotliwości lub polaryzacji. Proces tworzenia kanałów jest nazywany multipleksacją. Natomiast operacja wyodrębniania poszczególnych strumieni danych to demultipleksacja.

Zapewnienie w sieci usług o różnym poziomie jakości wymaga zastosowania technik sterowania przepływem danych, kształtowania ruchu i kontroli przeciążenia.

W kolejnym rozdziale zostały omówione serwery, stacje robocze i urządzenia sieciowe. Dzięki nim w sieciach są dostępne usługi, z których mogą korzystać jednostki klienckie i sama sieć.

# Część II

# Sprzęt

## **W tej części:**

**Rozdział 6.** Serwery i systemy sieciowe

**Rozdział 7.** Interfejsy sieciowe

**Rozdział 8.** Media transmisyjne

**Rozdział 9.** Routing, przełączanie i mostkowanie



# Rozdział 6.

# Serwery i systemy sieciowe

## **W tym rozdziale:**

- ◆ Podstawowe rodzaje serwerów sieciowych
- ◆ Usługi sieciowe
- ◆ Pomiar wydajności sieci
- ◆ Modelowanie sieci i wyszukiwanie zatorów

Tematem niniejszego rozdziału są podstawy funkcjonowania serwerów i usług sieciowych. Omówienie uwzględnia różne rodzaje serwerów, przy czym serwer jest rozumiany jako aplikacja programowa, która udostępnia usługi innym systemom sieciowym. Z uwagi na dużą różnorodność tego typu rozwiązań zaprezentowany został ogólny model procesu systemu serwerowego.

Prawidłowe funkcjonowanie sieci jest uzależnione od właściwego skalowania usług sieciowych, w tym szacowania ich pojemności i obciążalności. Wśród różnych metod zapewnienia odpowiedniej pojemności wyróżnia się takie rozwiązania, jak utrzymywanie pojemności nadmiarowej, dodawanie pojemności na żądanie, dopasowanie pojemności do potrzeb. W projektach wieloetapowych dodawanie pojemności serwera sieciowego jest jednym z ważnych elementów całego przedsięwzięcia. Dlatego w dalszej części rozdziału została opisana metodologia związanych z tym działań.

Aby zwiększyć wydajność sieci, trzeba umieć określić zakres usług realizowanych przez tę sieć. Ponadto niezbędne jest wyznaczenie charakterystyk wydajnościowych, które z kolei wymagają szczegółowego przeanalizowania czasów odpowiedzi, pomiaru przepustowości, określenia niezawodności sieci, jej skalowalności i wielu innych czynników.

Z tego powodu zostały tutaj zaprezentowane różne sposoby pomiaru parametrów wydajnościowych, na których podstawie można wygenerować listę zależności między elementami sieci. Opracowane zależności służą później do ustalenia, który z zasobów sieci stanowi wąskie gardło w jej funkcjonowaniu i zmniejsza efektywność systemu, a w konsekwencji pozwalają na usunięcie zatoru. Zamieszczone zostały również informacje na temat modelowania sieci.

W końcowej części rozdziału zostały przedstawione dwie techniki zwiększania pojemności serwerów — zwiększanie mocy systemów (skalowanie w górę) oraz zwiększanie liczby serwerów (skalowanie wszerek).

## Rodzaje serwerów sieciowych

Serwerem jest program komputerowy, który za pomocą połączenia sieciowego udostępnia usługę innemu komputerowi. Serwer może działać w lokalnym systemie lub w systemie zdalnym, ale jego funkcje muszą zapewniać dostęp do usługi innym systemom sieciowym lub przynajmniej umożliwiać taki dostęp. Każda usługa, w której nie występuje komponent współdzielony, jest klasyfikowana jako demon, czyli usługa lokalna.

Samo słowo *serwer* jest obecnie stosowane w różnych znaczeniach. Serwerem jest również komputer, skonfigurowany w taki sposób, aby działała w nim współdzielona aplikacja lub usługa. Większość nowoczesnych serwerów pracuje pod kontrolą serwerowego systemu operacyjnego (zawierającego wiele funkcji serwerowych), który w tej książce jest określany jako *sieciowy system operacyjny*. W dalszej części rozdziału zostały opisane serwery sieciowe ze szczególnym uwzględnieniem specyfiki udostępnianych przez nie usług i aplikacji.

System operacyjny serwera często jest specjalną wersją systemu stacji roboczej. Choć bardziej precyzyjne byłoby stwierdzenie, że system operacyjny stacji roboczej jest systemem serwerowym, w którym wyłączono pewne moduły, ograniczono wydajność i dodano elementy czyniące z niego oprogramowanie ogólnego przeznaczenia. Założenie to jest prawdziwe w odniesieniu do systemów operacyjnych Windows firmy Microsoft, od wersji Windows Server/Professional 2000, przez Windows Server 2003/XP, po Windows Server 2008/Vista. W innych platformach, takich jak Solaris firmy Sun czy Linux, nie ma nawet specjalnego podziału na systemy klienckie i serwerowe, co umożliwia użytkownikom pełne wykorzystanie mocy sprzętowej i własnej konfiguracji systemu.



Szczegółowe omówienie sieciowych systemów operacyjnych znajduje się w rozdziale 20.

Kolejnym znaczeniem słowa *serwer* jest aplikacja uruchomiona w danym systemie sprzętowym. Serwer, który nie został specjalnie skonfigurowany do obsługi jednej aplikacji lub usługi, jest nazywany *serwerem ogólnego przeznaczenia*. Wszystkie pozostałe serwery są opisywane w sposób zależny od funkcji realizowanej przez najważniejszą aplikację uruchomioną w systemie tego serwera. Do najczęściej spotykanych serwerów sieciowych należą:

- ♦ **Serwery plików i wydruku.** W rozległych sieciach serwery plików i wydruku stanowią nawet 25 procent wszystkich wdrożonych serwerów.
- ♦ **Serwery aplikacji.** Do grupy serwerów aplikacji zalicza się serwery baz danych, serwery WWW, serwery poczty itp. Jeśli w systemie serwera działa oprogramowanie określonego dostawcy, większość osób używa nazwy oprogramowania do opisu jednostki, mówiąc o niej jak o serwerze Apache, serwerze Oracle itp. Serwery aplikacji stanowią zazwyczaj 25 procent wszystkich serwerów w sieci korporacyjnej.
- ♦ **Serwery kopii zapasowych.** Większość osób jest zdziwiona faktem, że serwery kopii zapasowych to trzecia największa grupa serwerów w infrastrukturze informatycznej przedsiębiorstwa. Często nawet 20 procent wszystkich tego typu jednostek odgrywa rolę serwerów kopii zapasowych.

- ♦ **Serwery sieciowe.** Definicja serwerów sieciowych nie jest precyzyjna. Jednak jeśli zaliczy się do nich usługi realizujące routing, odpowiadające za identyfikację systemów (np. DNS i DHCP) oraz wykonujące podobne funkcje, to okaże się, że w sieci korporacyjnej około 15 procent serwerów należy do tej kategorii.
- ♦ **Serwery domenowe.** Serwery domenowe są nieodzownymi elementami większości sieci korporacyjnych, ale stanowią jedynie około 5 procent wszystkich instalowanych jednostek.

Zawarte w zestawieniu wartości procentowe pochodzą z badania przeprowadzonego przy współpracy wielu administratorów. Mogą więc znacznie odbiegać od stanu w danym przedsiębiorstwie w zależności od sposobu działania korporacji oraz rodzaju sieci. Suma wszystkich wartości wynosi 90 procent, ponieważ pozostałe 10 procent odpowiada różnym rozwiązaniom, które nie pasują do żadnej z wymienionych kategorii.

Liczba serwerów, a tym samym udział procentowy poszczególnych grup, może być przekłamana z uwagi na instalowanie elementów nazywanych *urządzeniami serwerowymi* (ang. *server appliance*). Urządzenie serwerowe to platforma sprzętowa przygotowana specjalnie do obsługi określonej aplikacji lub usługi bez konieczności ingerowania w jej działanie. Prawdziwe urządzenie serwerowe wyjąmuje się z pudełka (jak toster), podłącza do gniazdka, uruchamia i zapomina o jego istnieniu. Rozwiązania te znajdują zazwyczaj zastosowanie jako routery, bramy, firewalle, serwery wydruku, serwery WWW itp. Najważniejszą cechą odróżniającą urządzenia serwerowe — w tym urządzenia Oracle 8i lub Google Search Appliance (<http://www.google.pl/enterprise/search/gsa.html>) — od klasycznych serwerów jest łatwość ich użycia.

Doskonałym przykładem urządzeń serwerowych jest seria modułów DNS, DHCP, FTP, NTP, IPAM, RADIUS, sprzedawanych przez firmę Infoblox (<http://www.infoblox.com>). Są to odpowiednio zabezpieczone komponenty, które pracują pod kontrolą systemów operacyjnych czasu rzeczywistego, nie wymagają jakiejkolwiek konfiguracji wstępnej i mogą zastąpić wiele klasycznych serwerów. Wygląd urządzenia Infoblox-2000 Network Service Appliance został pokazany na rysunku 6.1.

### Rysunek 6.1.

Urządzenie Infoblox-2000 Network Service Appliance może zastąpić wiele różnych serwerów sieciowych

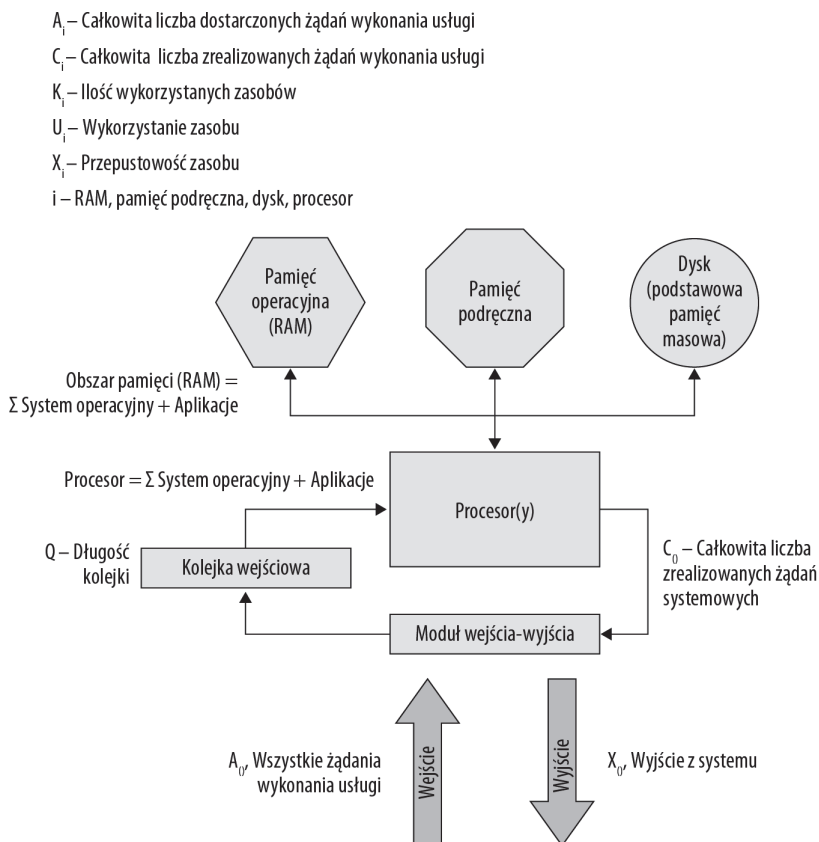


Fotografia z zasobów Infoblox Inc.

Serwery są produkowane w różnych obudowach. Najczęściej są one jednostkami wolno stojącymi (systemami wieżowymi), komponentami o stałej szerokości montowanymi w szafach serwerowych lub pełnosprawnymi modułami wsuwanymi na zasadzie kart rozszerzeń do kasety stełazowej. Oczywiście istnieje również wiele innych form instalowania serwerów, a postęp technologiczny prowadzi do powstawania coraz mniejszych urządzeń.

Ponadto serwery mogą być emulowane programowo. Ich usługi (uogólnione do tego poziomu, że mogą być uruchamiane na dowolnej platformie i sprawiać wrażenie usług lokalnych) pracują w ramach maszyn wirtualnych i mogą być dynamicznie uzupełniane o dodatkowe zasoby (mogą również być pozbawiane tych zasobów). Z tego względu najlepszym sposobem postrzegania serwera jest wyobrażenie sobie funkcji przez niego realizowanych oraz komponentów, z których się składa. Przykładowy zbiór modułów niezbędnych do utworzenia modelu serwera ogólnego przeznaczenia został zaprezentowany na rysunku 6.2. Parametry uwzględnione w modelu są wartościami, które można pomierzyć lub wyznaczyć matematycznie.

**Rysunek 6.2.**  
*Model operacyjny*  
*serwera sieciowego*



Na rysunku 6.2 zostały przedstawione różne moduły funkcjonalne sieciowego systemu operacyjnego, mające bezpośredni wpływ na jego wydajność. Odebrane od klienta sieciowego żądanie zrealizowania usługi ( $A_0$ ) podlega przetworzeniu w serwerze, wynikiem czego jest odpowiedź ( $X_0$ ), wygenerowana z pewnym opóźnieniem, wynikającym z przepustowości systemu.

Żądanie wykonania usługi jest dodawane do kolejki wejściowej, a następnie przekazywane do procesora w celu dalszego przetwarzania. Kolejka może mieć pewną długość, odpowiadającą liczbie oczekujących żądań (z uwzględnieniem ich priorytetów). Wraz z realizacją kolejnych żądań liczba zadań w kolejce się zmniejsza. Zdolność procesora do przetwarzania żądań jest funkcją jego wydajności oraz obciążenia systemem operacyjnym lub systemami operacyjnymi i innymi aplikacjami. W czasie realizacji żądań poszczególne instrukcje

mogą być składowane w różnych podsystemach pamięci oraz pobierane z tych podsystemów. Dostępne są następujące rodzaje pamięci (wymienione według malejącej szybkości działania i rosnącej pojemności): pamięć podręczna, RAM i dyskowa pamięć masowa.

## Pojemność i obciążenie

Pojemność serwera sieciowego określa się jako zdolność do pracy pod pewnym obciążeniem. Obciążenie z kolei wyraża fragment aktualnie wykorzystanej pojemności serwera. Pomiaru pojemności i obciążenia można dokonywać na wiele sposobów. Niektóre rozwiązania są czysto teoretyczne, inne mają charakter całkowicie praktyczny. Jednak o ile sama koncepcja pojemności może się wydawać niejasna, to jej wpływ na wydajność sieci i zyski przedsiębiorstwa już taki nie jest. Dlatego też zrozumienie pojemności oraz obciążenia usług sieciowych, a także umiejętność ich szacowania i modyfikowania są kluczowe dla każdego administratora.

Istnieją różne metody planowania pojemności. Trzy z nich zostały opisane w kolejnym punkcie rozdziału. Planowanie pojemności może mieć charakter proaktywny, reaktywny i analityczny. Każda z technik wymaga zdefiniowania innych założeń i realizacji innych zadań. W dalszej części rozdziału zostały również przedstawione metodologie rozwiązywania problemów, które pozwalają organizacji (o strukturze zespołów) na zmierzenie się z planami projektowymi i zakończenie prac bez błędów charakterystycznych dla dużych projektów.

## Trzy metody działania

Oto trzy różne sposoby planowania pojemności systemu:

1. Utrzymywanie nadmiarowej pojemności przez cały czas działania systemu.
2. Dodawanie pojemności na żądanie.
3. Dostosowanie pojemności do zapotrzebowania.

Każde z wymienionych rozwiązań ma pewne wady i zalety i z każdym wiąże się pewne wymagania dotyczące dostępności zasobów. Strategia przewodzenia (proaktywna) bazuje na założeniu, że zawsze istnieje pewna nadwyżka pojemności, dostępna podczas realizacji każdego żądania. Oznacza to konieczność zapewnienia na miejscu pewnych dodatkowych zasobów albo przynajmniej zapewnienia dostępu do takich zasobów. Ponieważ rozwiązanie to zakłada marnowanie istniejących zasobów, w wielu sieciach, działających zgodnie z tą strategią, stosowane jest podejście wielowarstwowe, w myśl którego dodatkowe zasoby są zajmowane tylko w razie konieczności.

Strategia przewodzenia jest wdrażana przez firmy, które spodziewają się wzrostu natężenia ruchu i koniecznie chcą zapewnić jego obsłużenie. Cechą charakterystyczną takiego podejścia jest to, że zdobyta część rynku jest dla firmy bardziej wartościowa od kosztów zapewnienia zasobów systemowych. Na przykład tak wielka firma jak Amazon z pewnością stosuje to rozwiązanie, ponieważ iloraz wpływów i kosztu sprzętu ma bardzo dużą wartość.

Drugi sposób działania polega na dodawaniu zasobów tylko wtedy, gdy jest to konieczne. Takie podejście jest nazywane strategią reakcyjną lub strategią odraczania. Zwiększanie pojemności następuje dopiero wtedy, gdy firma nie ma wątpliwości, że jest to konieczne.

Wadą rozwiązania jest to, że pewna część ruchu nie zostanie poprawnie obsłużona do czasu uzupełnienia pojemności systemu. Ten tok postępowania jest charakterystyczny dla przedsięwzięć, w których koszt wdrożenia dodatkowych zasobów sieciowych jest wyższy od strat powodowanych brakiem tych zasobów. Strategia odraczania jest rozwiązaniem zachowawczym, wynikającym z różnych założeń. Podczas mierzenia zapotrzebowania na zasoby można w badaniach uwzględnić średni poziom ruchu lub maksymalny poziom ruchu w czasie szczytu.

Jedno z rozwiązań polega na zapewnieniu zasobów, które będą umożliwiały obsługę średniego ruchu lub (co wydaje się rozsądniejsze) ruchu o standardowym odchyleniu. Wówczas jedynie żądania istotnie odbiegające od wartości średniej pozostaną nieobsłużone. Odchylenie standardowe opisuje *rozkład prawdopodobieństwa* wokół wartości średniej. Mała wartość odchylenia standardowego oznacza, że wartości są bardziej zbliżone do wartości średniej. Natomiast duża wartość odchylenia standardowego informuje, że metryki ruchu są rozproszone w większym zakresie wartości.

Choć strategia odraczania jest uznawana za zachowawczą, wiele firm opiera na niej swoje działanie, chcąc maksymalnie wykorzystać udostępniane zasoby. Doskonałym przykładem takiego sposobu działania są sieci pakietowe, stanowiące podstawę działania internetu oraz wielu firm ISP. Przepustowość sieci jest zasobem o ograniczonej wielkości, a celem dostawcy usług internetowych jest doprowadzenie do takiego podziału pasma, aby łącze było zajęte w jak największym stopniu, ale przy jednoczesnym zagwarantowaniu wysokiej dostępności sieci dla użytkowników końcowych. W czasie zwiększonego wykorzystania pasma użytkownicy zauważają zmniejszenie przepływności lub zwiększenie czasu dostępu do usług, lecz przypadki całkowitej niedostępności sieci są bardzo rzadkie.

Trzeci sposób działania — analityczny — wydaje się najlepszym rozwiązaniem. Polega na dostosowaniu pojemności systemu do wymagań użytkowników. Ilość zasobów systemowych jest sukcesywnie zwiększana, dzięki czemu pojemność sieci dostosowuje się do zmieniającego się zapotrzebowania. Strategia dostosowania wymaga implementacji pętli sprzężenia zwrotnego, które pozwoli na dodawanie zasobów w razie potrzeby i zwalnianie ich, gdy przestaną być niezbędne.

## Metodologia prac projektowych

Nietrudno zgodzić się z twierdzeniem, że większość zakrojonych na dużą skalę projektów IT kończy się fiaskiem. Pewnie dlatego ekonomia bywa nazywana „ponurą nauką”. Na potrzeby dalszych rozważań możemy przyjąć, że przyczyną niepowodzenia przedsięwzięcia może być:

- ♦ **Przekroczenie kosztów.** Realizacja projektu znacznie przekracza założone koszty z powodu błędów w specyfikacji lub zmiany celów projektu.
- ♦ **Przekroczenie czasu.** Projekt był wykonywany znacznie dłużej, niż początkowo zaplanowano, lub nigdy nie został zakończony.
- ♦ **Błąd w specyfikacji.** Problem będący przyczyną uruchomienia projektu nie istnieje lub przestał istnieć przed ukończeniem projektu.

- ♦ **Błędna alokacja zasobów.** Wykorzystane zasoby są bardziej potrzebne w innym projekcie. Często rozwiązanie danego problemu prowadzi do wystąpienia innych, poważniejszych problemów.
- ♦ **Zaniedbania.** Projekt kończy się niepowodzeniem z powodu utraty lidera, który miałby wizję jego ukończenia.

Przedsięwzięcia związane z budową lub przebudową sieci są zazwyczaj działaniami o dużej skali, podatnymi na każde z wymienionych zagrożeń, a nawet na różne ich wariacje. Aby nie dopuścić do fiaska projektu, można skorzystać z jednej z kilku różnych technik zarządzania projektowaniem i wdrażaniem rozwiązań informatycznych. Metodologie prac projektowych opisują, w jaki sposób zespoły organizacji, realizując poszczególne etapy projektu, mogą wykonać plan i zakończyć projekt sukcesem. Aby zrozumieć zasadę podziału rozbudowanego projektu sieciowego na poszczególne zadania, przeanalizujemy dwa powiązane ze sobą rozwiązania stosowane w przemyśle.

Prawdopodobnie jedną z najbardziej znanych metodologii prac projektowych opracowało brytyjskie biuro rządowe Office of Government Commerce (OGC). OGC opublikowało zbiór wytycznych związanych z zarządzaniem zasobami IT o nazwie Information Technology Infrastructure Library (ITIL; <http://www.itil-officialsite.com/home/home.asp>), które są powszechnie wykorzystywane, szczególnie w krajach europejskiego wspólnego rynku. Sama nazwa opracowania stała się znakiem handlowym.

Metodologia ITIL definiuje sposoby implementowania najlepszych rozwiązań podczas opracowywania strategii wdrażania, projektowania i funkcjonowania usług sieciowych oraz sposoby zapewnienia odpowiedniej jakości obsługi w czasie zmian warunków ich działania. Opracowanie opublikowano w trzech wersjach, z których ostatnia (wersja 3.0) została wydana w maju 2007 roku w pięciu częściach:

1. **Strategia zarządzania usługami (ang. *Service Strategy*).** Zawiera opis rynku, zbiór zasad postępowania, opis zarządzania usługami, definicję najważniejszych procesów oraz omówienie zarządzania potrzebami.



Chcąc obniżyć koszty i podnieść jakość projektu, warto przeprowadzić bardzo szczegółową weryfikację projektu przed jego rozpoczęciem. Koszt zmian wprowadzanych do projektu na późniejszych etapach jest wykładniczo wyższy od kosztu modyfikacji na etapie przygotowywania.

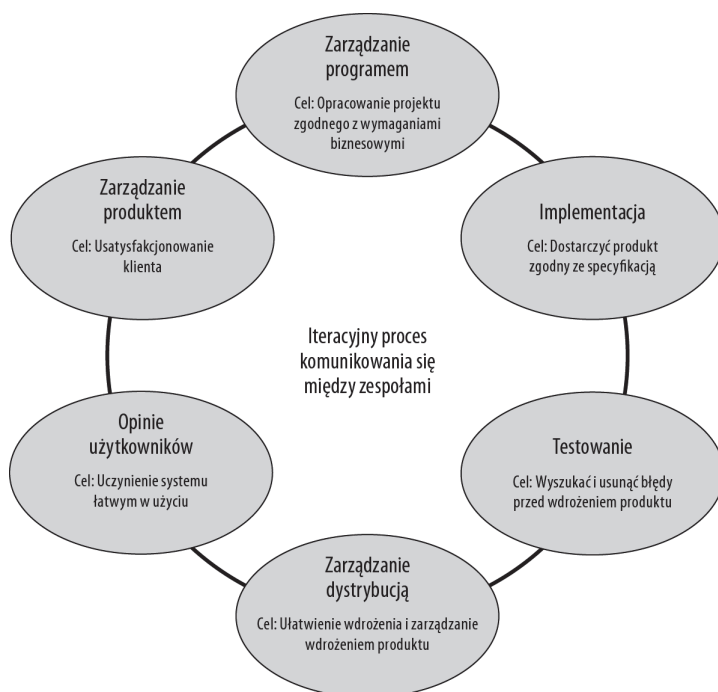
2. **Projektowanie usług (ang. *Service Design*).** W tej części zawarto opis architektury systemów sieciowych, zasady postępowania biznesowego oraz reguły sporządzania dokumentacji. Pakiet projektowania usług (SDP — *Service Design Package*) obejmuje katalog mechanizmów zarządzania usługami, plany utrzymania biznesu, zasady zabezpieczenia sieci, informacje na temat kluczowych dostawców oraz podziału ról w projekcie.
3. **Wdrażanie usług (ang. *Service Transition*).** Publikacja ta opisuje zasady przekazywania systemów prototypowych do zespołu produkcyjnego w celu wdrożenia opracowanego rozwiązania. Zawarto w niej również zasady opracowywania koncepcji nowych projektów, które zmieniają istniejące kategorie usług, oraz zasady zarządzania zasobami i konfiguracjami, w tym także wprowadzanie zmian w konfiguracjach. Zarządzanie zmianami, zarządzanie wiedzą oraz udostępnianie i wdrażanie produktu należy do zadań zespołu odpowiedzialnego za wdrażanie usług.

4. **Eksploracja usług (ang. *Service Operation*).** Część poświęcona eksploatacji usług składa się z szeregu zasad postępowania, które zapewniają ciągłe świadczenie usług uwzględnionych w projekcie. Zespół eksploatacji usług jest odpowiedzialny za codzienne nadzorowanie sieci i systemów użytkowych.
5. **Ciągle udoskonalanie usług (ang. *Continual Service Improvement*).** Program CSI jest proaktywnym podejściem do problemu udoskonalania systemu użytkowego. Zakłada on zbieranie informacji od użytkowników i przekazywanie najwartościowszych sugestii do zespołów, które uwzględnią je w danej lub kolejnej wersji produktu. Zespół CSI ma również za zadanie szkolenie załogi, opracowywanie harmonogramów prac, przydzielanie zadań i sporządzanie raportów.

Iteracyjny mechanizm współdziałania zespołów wynikający z opisanej metodologii został przedstawiony na rysunku 6.3.

### Rysunek 6.3.

*Iteracyjny mechanizm projektowania, testowania i wdrażania usług zapewnia największe szanse na sukces*



W iteracyjnym rozwiązaniu bazującym na pracy zespołowej wymagane jest utworzenie kilku wymienionych poniżej grup. Wraz z postępem prac projektowych każdy zespół powinien przekazywać wyniki swojego działania następnej grupie osób. Oto lista zespołów:

- ♦ **Zarządzanie programem.** Zespół ten inicjuje prace projektowe i definiuje cele projektu. Wynikiem jego działań jest plan projektu.
- ♦ **Implementacja.** Zespół implementacji zamienia plan projektu na produkt.
- ♦ **Testowanie.** Produkt będący wynikiem realizacji projektu jest przekazywany do zespołu testowania w celu sprawdzenia, czy wynik jest zgodny ze specyfikacją i czy nie zawiera błędów.

- ♦ **Zarządzanie dystrybucją.** Zespół testowania przekazuje projekt do zespołu zarządzania dystrybucją, którego zadanie polega na udostępnieniu produktu w sieci.
- ♦ **Opinie użytkowników.** Zespół zbierania opinii użytkowników współdziała z odbiorcami produktu, aby uzyskać pewność, że produkt jest przez nich akceptowany i spełnia ich wymagania.
- ♦ **Zarządzanie produktem.** Zespół ten stanowi grupę wsparcia technicznego dla użytkowników końcowych po udostępnieniu produktu.

Iteracyjne programy projektowe zazwyczaj obejmują etap analizy końcowej, w której wyniki wykonania projektu są porównywane z wynikami działania zespołu zarządzania programem.

Częścią programu ITIL jest zdobywanie certyfikatów z poszczególnych zakresów działań. Certyfikaty są wydawane przez ITIL Certification Management Board. Egzaminacje certyfikacyjne są natomiast przygotowywane przez jednostki OGC (<http://www.ogc.gov.uk>), IT Service Management Forum International (itSMF, <http://www.itsmfi.org>), Examination Institute for Information Science (EXIN, <http://www.exin-exams.com>) oraz Information Systems Examination Board (ISEB, <http://www.bcs.org>). Dwie ostatnie spośród wymienionych instytucji są również odpowiedzialne za przeprowadzanie egzaminów. Poziomy certyfikacji to: Foundation, Intermediate Capability, Intermediate Lifecycle, ITIL Expert oraz ITIL Master.

Grupa konsultacyjna firmy Microsoft zaadaptowała zespołową metodologię ITIL do opracowywania własnych projektów. Powodzenie prac grupy doprowadziło do tego, że firma Microsoft uwzględniła rozwiązania ITIL w dwóch własnych metodologiach — Microsoft Operations Framework (MOF) oraz Microsoft Solutions Framework (MSF). Celem metodologii MOF jest właściwe zarządzanie pracą sieci, natomiast rozwiązanie MSF zapewnia prawidłową budowę sieci.

## Microsoft Operations Framework

Firma Microsoft opisuje platformę Microsoft Operations Framework (MOF, <http://www.microsoft.com/mof>) jako nadzbiór rozwiązań ITIL. W praktyce jednak należy ją postrzegać jako adaptację opracowania ITIL. Środowisko MOF obejmuje przewodniki, szablony, narzędzia wspomagające weryfikację i utrzymanie projektu. Zapewnia również dostęp do dokumentacji, oprogramowania szkoleniowego i opracowań z analizy różnych przypadków. Dodatkowo firma Microsoft udostępnia różnego rodzaju usługi związane z projektem MOF. Zagadnienia objęte metodologią MOF skupiają się wokół problemu powiązania osób z procesami charakterystycznymi dla rozbudowanych środowisk sieciowych. W przewodnikach MOF uwzględniono na przykład rozproszone heterogeniczne sieci. Proponowane rozwiązania wykorzystują opisaną wcześniej ideę iteracyjnego przekazywania pracy między zespołami.

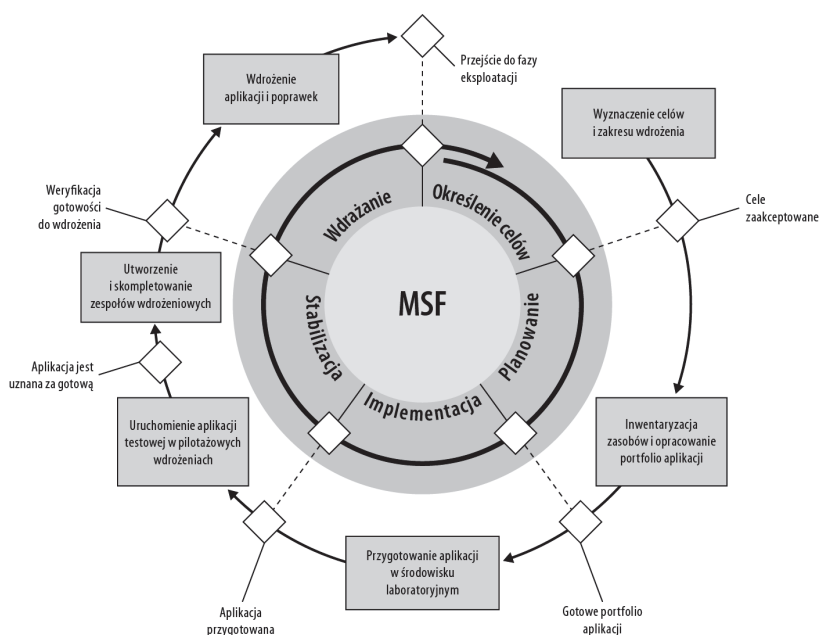
## Microsoft Solutions Framework

W ramach platformy Microsoft Solutions Framework (MSF, <http://www.microsoft.com/msf>) udostępnione zostały rozwiązania, które każdy może pobrać i wykorzystać. Wśród upublicznionych komponentów znajdują się narzędzia do wdrażania produktów lub środowisk, takich jak Windows Server, Exchange Server, Visual Studio Team System, usług WWW i elektronicznego handlu, wielowarstwowych systemów transakcyjnych, systemów zarządzania firmą itp. Jednym z najbardziej reprezentatywnych rozwiązań, które można pobrać ze stron

firmy Microsoft, jest Microsoft Solution Accelerator for Business Desktop Deployment 2007 (BDD, <http://technet.microsoft.com/en-us/library/bb490308.aspx>). Opisuje ono wdrażanie systemów Windows Server 2008 oraz Windows Vista. Wraz z pakietem BDD dostarczanych jest wiele użytecznych narzędzi wspomagających realizację tego zadania.

Aktualna wersja MSF (wersja 4.0) zawiera modele zespołowe i zarządzania, mechanizmy integracji ze środowiskiem Microsoft Operations Framework oraz opracowania w zakresie zarządzania projektem, ryzykiem i gotowością do działania. Osoby, które pobiorą jeden z pakietów rozwiązań biznesowych, znajdą w nim informacje na temat zasad budowania zespołów i współpracy między zespołami, wyników prac poszczególnych zespołów oraz najlepszych zasad postępowania. Przewodnikiem tym towarzyszy zbiór innych zasobów związanych z danym projektem. Ogólnie rzecz ujmując, serwis ten udostępnia zbiór receptur, które można dostosować do sytuacji własnego przedsiębiorstwa. Zależności między zespołami i zadaniami w rozwiązaniach MSF zostały przedstawione na rysunku 6.4.

**Rysunek 6.4.**  
Proces grupowego  
wykonywania zadań  
zawarty w biznesowych  
rozwiązaniach  
Microsoft Solution  
Framework



Rysunek z zasobów Microsoft, Inc.

Zgodnie z informacjami zawartymi na rysunku 6.4 prace nad projektem rozpoczynają się od etapu określenia celów. Następnie przechodzą do fazy planowania, implementacji, stabilizacji i wdrażania. W każdej iteracji poszczególnymi zadaniami zajmuje się powołana do tego celu grupa osób. Romby reprezentują kamienie milowe zdefiniowane w planie projektu. W przypadku wewnętrznego kręgu są one tożsame z przekazaniem prac kolejnej grupie. Krąg zewnętrzny przedstawia konkretne zadania i granice etapów projektu.

Realizacja projektu przebiega zgodnie z kierunkiem ruchu wskazówek zegara, synchronicznie wzdłuż ścieżek etapów i poszczególnych zadań. W założeniach MSF nie występuje konieczność całkowitego przekazania projektu z jednej grupy do kolejnej. W pewnych fazach działań dwie grupy lub większa ich liczba mogą jednocześnie pracować nad produktem.

U podstaw rozwiązywania MSF leży kilka zasad, które firma Microsoft definiuje następująco:

- ♦ **Wspólna wizja.** Każdy zespół powinien mieć jednakową wizję działań oraz ostatecznego wyniku projektu.
- ♦ **Niezawodność i odpowiedzialność.** Współdzielenie i przekazywanie wyników prac powinno przebiegać bez przeszkód.
- ♦ **Jawna komunikacja.** Komunikacja wewnątrz grupy oraz między zespołami powinna być jawna.
- ♦ **Upoważnienia.** Członkowie zespołów powinni mieć możliwość wzięcia odpowiedzialności za podejmowane działania.
- ♦ **Dodawanie wartości.** Wyniki prac muszą być porównywane z potrzebami.
- ♦ **Jakość.** Należy inwestować w jakość i weryfikować jakość produktu, szacując jakość wyników pracy.
- ♦ **Zarządzanie ryzykiem.** Ryzyko musi być monitorowane, a w przypadku zauważenia jakichkolwiek problemów trzeba natychmiast na nie reagować.
- ♦ **Uczenie się na błędach.** Zakończone prace projektowe powinny być tematem analiz poprojektowych.
- ♦ **Elastyczność.** Należy być otwartym na zmiany, jeśli z wcześniejszych doświadczeń wynika, że takie zmiany są konieczne.

## Skalowanie serwerów i systemów sieciowych

Podstawą do podejmowania jakichkolwiek decyzji związanych z siecią jest poznanie parametrów wydajności serwerów, usług i systemów sieciowych. Jeśli określona technologia została wdrożona w nieodległym czasie, najlepszym rozwiązaniem wydaje się poeksperymentowanie z systemem w laboratorium testowym i wyznaczenie w ten sposób potencjału obliczeniowego, który będzie można wykorzystać w środowisku użytkowym. W niektórych przypadkach można wykorzystać wyniki testów wydajnościowych przeprowadzonych przez inne instytucje, symulujące rzeczywiste warunki pracy systemu. Na przykład organizacja Transaction Processing Performance Council często prowadzi badania rozwiązań e-commerce i hurtowni danych w środowiskach odpowiadających typowym zastosowaniom tego typu produktów. Choć oczywiście najwartościowsze zawsze są te dane, które uzyska się, testując własną sieć i własne jednostki sieciowe.

## Definiowanie poziomów usług

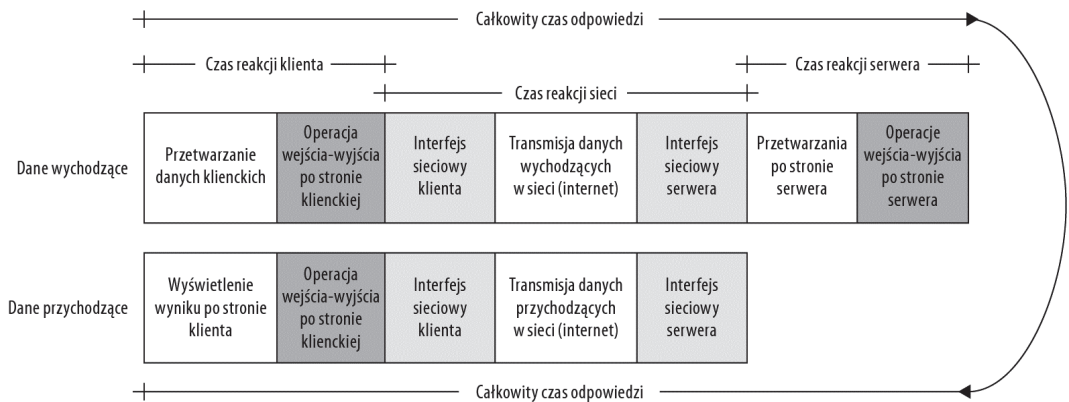
Aby wyznaczyć liczbowe wartości wydajności systemu, trzeba zmierzyć poziom jakości usługi (QoS) w takich obszarach, jak: czas odpowiedzi, przepustowość, dostępność, niezawodność, skalowalność, zdolność do adaptacji oraz bezpieczeństwo.

Niektóre z elementów współczynnika QoS (przede wszystkim niezawodność i zdolność do adaptacji) wynikają z zastosowanej technologii i często muszą być wyznaczane już na etapie projektowania rozwiązania. Sam współczynnik QoS powinien reprezentować mierzalną jakość usługi, wyznaczaną na podstawie analitycznych zależności lub pomiaru wydajności.

## Czas odpowiedzi

Parametr czasu odpowiedzi reprezentuje czas przetwarzania żądania. Pomiar czasu odpowiedzi jest analogiczny do wyznaczenia elementu ograniczającego szybkość reakcji w chemii. Jeśli znamy element ograniczający szybkość reakcji, znamy miarę czynnika ograniczającego wydajność systemu.

W przypadku komunikacji klient-serwer (na przykład podczas przesyłania żądania z przeglądarki do serwera WWW) czas odpowiedzi można podzielić na czas przetwarzania żądania w aplikacji, transmitowania go w sieci oraz generowania odpowiedzi po stronie serwera. Zależności te zostały przedstawione na rysunku 6.5. Zgodnie z zamieszczonymi na nim informacjami żądanie jest inicjowane w jednostce klienckiej, w stosie komponentów przeznaczonych dla informacji wychodzących (znajdującym się w lewej górnej części rysunku). Czas reakcji klienta sieci i serwera składają się na całkowite opóźnienie procesu na trasie od klienta do serwera. Gdy serwer zrealizuje żądanie, generuje odpowiedź, która podlega opóźnieniom w blokach reprezentujących odbieranie odpowiedzi. Realizacja zadania jest przekazywana z górnego stosu komponentów do dolnego i przebiega w kierunku od prawej strony do lewej. Na opóźnienie odbioru odpowiedzi wpływają: czas reakcji sieci (z uwzględnieniem komponentów sieciowych serwera i klienta) oraz czas wyświetlania danych na ekranie.



**Rysunek 6.5.** Komponenty wpływające na czas odpowiedzi w interakcjach klient-serwer

W praktyce rozdzielenie poszczególnych czasów reakcji na przedziały, które można by pomierzyć, bywa niezwykle trudne. Pomiar czasu odpowiedzi sprowadza się więc najczęściej do ustalenia czasu, który upływa od chwili naciśnięcia klawisza *Enter* lub kliknięcia przycisku *OK* do pojawienia się wyników operacji na ekranie. Sam czas reakcji sieci można również ustalić za pomocą polecenia *PING*, które zwraca informacje o czasie potrzebnym na przesłanie komunikatu do wskazanego węzła sieciowego i z powrotem.

## Przepustowość

Przepustowość systemu wyraża się liczbą operacji lub transakcji, które można zrealizować w jednostce czasu. Przed pomiarem tego parametru konieczne należy określić charakterystykę realizowanego zadania. Do wyznaczenia przepustowości można się posłużyć następującą zależnością:

$$\text{Przepustowość} = \text{MINIMUM} \{ \text{pojemność serwera}, \text{dopuszczalne obciążenie} \}$$

W czasie znacznego obciążenia serwera lub sieci wartość przepustowości może istotnie odbiegać od wartości średniej lub pożądanej. Zazwyczaj krzywa przepustowości odpowiada wartościom rosnącym równomiernie aż do uzyskania 100 procent wykorzystania zasobów. Po osiągnięciu tego poziomu przepustowość maleje, czyniąc dany komponent usługi elementem limitującym działanie systemu. Na przykład w wielu systemach stosuje się mechanizmy buforowania danych, które pozwalają na zwiększenie wydajności lub rozszerzenie pamięci produktu. W czasie bardzo intensywnego wykorzystywania takiego systemu przeciążenie dysku może ograniczyć wydajność mimo istnienia mechanizmu buforowania, który ma na celu zapobieganie podobnym przypadkom. Przeciążenie dysku powoduje obniżenie wydajności systemu, gdy w wyniku bardzo dużej liczby żądań wykonania operacji wejścia-wyjścia system nie dysponuje wolną pamięcią RAM, w której mógłby przechować dane potrzebne bieżącym procesom.

Oto kilka przykładów metryk przepustowości:

- ♦ Liczba operacji mikroprocesora na sekundę (wyrażana w milionach; w jednostkach MIPS).
- ♦ Liczba operacji wejścia-wyjścia lub liczba kilobajtów przesłanych w ciągu jednej sekundy (KB/s) przez podsystem dyskowy.
- ♦ Liczba pakietów na sekundę lub liczba megabitów (Mbit/s) na sekundę przesyłanych w segmencie sieci.
- ♦ Liczba transakcji na sekundę wykonywanych przez aplikację.
- ♦ Liczba pobrań strony na sekundę.
- ♦ Liczba żądań HTTP na sekundę lub liczba kilobajtów na sekundę (KB/s) przesłanych przez serwer WWW lub serwisy sieciowe.
- ♦ Liczba wiadomości na sekundę przetwarzanych przez serwer pocztowy.
- ♦ Liczba wyszukiwań na sekundę lub liczba sesji bazodanowych na sekundę.

Przepustowość jest miarą wyrażającą liczbę pewnych operacji w jednostce czasu. Jest ona użyteczna tylko wtedy, gdy tę liczbę i czas można porównywać z innymi pomiarami. Na przykład nie ma sensu porównywanie metryk operacji przesłania listu elektronicznego o rozmiarze 4 KB z wartościami zarejestrowanymi podczas przesyłania listu z załącznikiem o rozmiarze 1 MB.

Dobrze przygotowany test musi uwzględniać pewne różnice w specyfice zadań i obejmować zarówno czynności opatrzone niskim priorytetem, jak i operacje o wysokim priorytecie. Musi także uwzględniać inne zmieniające się czynniki pracy systemu. Na przykład w teście TPC-C V5.10 (<http://www.tpc.org/tpcc/default.asp>) wykonywanych jest wiele transakcji w ramach typowego systemu OLTP, przeznaczonego do składania zamówień. Badanie

obejmuje składanie zamówień i dostarczanie produktów oraz monitorowanie stanów magazynowych. Test dostarcza informacji na temat liczby zamówień realizowanych przez hipotetyczny system w czasie jednej minuty.



Należy pamiętać, że testy wydajnościowe są użyteczne tylko wtedy, gdy do porównania dwóch systemów jest wykorzystywana spójna metodologia. Wyniki badania efektywności przenoszenia przez sieć pakietów o małym rozmiarze z pewnością będą istotnie odbiegały od wyników uzyskanych w czasie testowania pakietów o dużym rozmiarze. Trzeba więc zachować ostrożność w ich interpretowaniu.

## Dostępność

Dostępność jest definiowana jako współczynnik czasu dostępności usługi do czasu pomiaru i stanowi podstawowy parametr wielu systemów sieciowych. Firmy utrzymujące sklepy internetowe dążą do uzyskania dostępności na poziomie 99,99 %, co oznacza, że serwis może być niedostępny przez 52 minuty w roku. Taki poziom dostępności jest uznawany przez firmę za wartość graniczną, od której zależy powodzenie przedsięwzięcia. Jednak w przypadku systemów monitorujących parametry życiowe pacjentów jest niedopuszczalny. Dostępność stanowi więc jedno z najważniejszych założeń projektowych sieci.

## Niezawodność

Niezawodność jest miarą prawdopodobieństwa, że sieć będzie działać poprawnie w pewnym okresie. Wiele osób myli pojęcie niezawodności z dostępnością. Choć są one od siebie zależne, każdy, kto projektuje lub rozbudowuje sieć, powinien znać różnice między nimi. Sieć może być dostępna i realizować operacje, które nie są niezawodne. Na przykład w mocno obciążonej sieci pakietowej systemy mogą być dostępne, choć zwiększająca się stopa błędów będzie zmniejszała niezawodność sieci. Wzrost niezawodności jest ograniczony poziomem dostępności systemu.

## Skalowalność

Skalowalność opisuje zdolność systemu do obsłużenia dodatkowego obciążenia bez zmniejszenia wydajności. Wartość obciążenia można wyrazić liczbą użytkowników, liczbą jednoczesnych sesji lub współczynnikami o podobnym znaczeniu. Jeśli zwiększenie obciążenia wpływa na zmianę parametrów wydajnościowych sieci (zwykle negatywnie), system jest uznawany za nieskalowalny (od momentu, gdy wpływ obciążenia na wydajność jest szczególnie zauważalny).

## Zdolność do adaptacji

Zdolność do adaptacji odzwierciedla możliwość rozbudowywania sieci o nowe usługi. Jest jednym z parametrów uwzględnianych podczas projektowania sieci lub jej modernizowania.

## Bezpieczeństwo

Zagwarantowanie bezpieczeństwa sieci polega na zapewnieniu dostępu do danych przy jednoczesnym zachowaniu poufności wymiany informacji i weryfikacji poczynąń użytkowników oraz innych systemów sieciowych.

## Szacowanie wydajności

Administrator powinien mieć ogólne pojęcie na temat elementów wpływających na jakość usług w instalowanych lub rozbudowywanych serwisach. Jeszcze lepiej jest jednak, gdy administrator umie oszacować ilościowo wydajność sieci, wykorzystując do tego celu odpowiedni zbiór metryk rzeczywistego systemu. Doświadczenie uczy, że najwłaściwszym rozwiązaniem jest w tym przypadku gromadzenie przez pewien czas informacji wydajnościowych w dziennikach zdarzeń, na których podstawie można później wyznaczyć trendy w funkcjonowaniu sieci oraz wyodrębnić problemy. Analiza trendów umożliwia podejmowanie proaktywnych działań podczas rozbudowywania lub modyfikowania konfiguracji sieci. Ponieważ zarejestrowane informacje odzwierciedlają podstawowe metryki systemu, mogą posłużyć do diagnozy ewentualnych błędów. Dzienniki zdarzeń zawierają bowiem szczegółowe dane na temat stanu sieci w całym analizowanym okresie.

Oto kilka parametrów związanych z wykorzystaniem zasobów, które warto monitorować:

- ♦ **Zajętość procesora.** Zebranie średnich i szczytowych wartości obciążenia procesora umożliwia wyznaczenie zależności zajętości od czasu, na przykład w okresie typowego tygodnia pracy.
- ♦ **Wykorzystanie pamięci.** Rejestracji i analizie są poddawane dane o ilości zaalokowanej pamięci, liczbie błędnych stron, wydajności buforowania itp.
- ♦ **Wykorzystanie dysku.** Monitorowanie obejmuje zajęty obszar dysku, liczbę operacji wejścia-wyjścia w ciągu sekundy, a także inne parametry, które umożliwiają określenie trendów korzystania z podsystemu dyskowego w czasie typowego tygodnia pracy. Analiza powinna obejmować różne typy i struktury pamięci masowej, w tym różne warianty macierzy RAID, dedykowane macierze dyskowe itp.
- ♦ **Wykorzystanie sieci.** Wśród sieciowych parametrów objętych rejestracją powinny się znaleźć: przepustowość, czasy odpowiedzi, współczynniki kolizji itp.



Nowoczesne systemy operacyjne udostępniają użytkownikowi wiele różnych liczników wydajnościowych. Jednak tylko część z nich jest dostępna w standardowej konfiguracji systemu. Większość dodatkowych rejestratorów należy zainstalować lub po prostu włączyć. Ponadto część aplikacji, szczególnie aplikacji przeznaczonych dla serwerów korporacyjnych, jest wyposażonych we własne narzędzia monitorowania wydajności, które są instalowane wraz z samą aplikacją. Warto więc sprawdzić w dokumentacji systemu oraz aplikacji, czy są one dostępne dla użytkownika końcowego. Trzeba jednak pamiętać, że użycie niektórych liczników może negatywnie wpłynąć na wydajność komponentu, który będzie monitorowany. Zastrzeżenie to odnosi się przede wszystkim do dysków.

Aby uzyskać wymienione parametry, trzeba włączyć odpowiednie liczniki wydajnościowe na serwerze, w routerze, a niekiedy również w reprezentatywnych systemach klienckich. Lista najważniejszych informacji podlegających rejestracji została zamieszczona w tabeli 6.1.

## Zależności wydajnościowe

Próbując ustalić, czy konieczne jest dodanie kolejnych zasobów systemowych, należy przede wszystkim przeanalizować stopień wykorzystania zasobu. Pełne wykorzystanie oznacza, że zasób nie dysponuje pojemnością, która umożliwiłaby wykonanie zadania. Zgodnie

**Tabela 6.1.** Najważniejsze dane wydajnościowe, które można zarejestrować

Symbol	Opis
<b>Dane uzyskane z pomiaru (zmienne operacyjne)</b>	
T	Okres obserwacji.
K	Ilość wykorzystanych zasobów.
B <sub>i</sub>	Czas zajętości zasobu i w okresie T.
A <sub>i</sub>	Całkowita liczba żądań wykonania usługi przekazana do zasobu i w czasie T.
A <sub>0</sub>	Całkowita liczba żądań wykonania usługi (określonego typu) skierowana do całego systemu w czasie T.
C <sub>i</sub>	Całkowita liczba żądań zrealizowanych przez zasób i w czasie T.
C <sub>0</sub>	Całkowita liczba żądań zrealizowanych przez system w czasie T.
<b>Dane wynikające z obliczeń</b>	
S <sub>i</sub>	Współczynnik średniego czasu wykonywania usługi w zasobie i. $S_i = B_i / C_i$
U <sub>i</sub>	Wykorzystanie zasobu i. $U_i = B_i / T$
X <sub>i</sub>	Przepustowość zasobu i. $X_i = C_i / T$
I <sub>i</sub>	Częstość odwołań do zasobu i. $I_i = A_i / T$
X <sub>0</sub>	Całkowita przepustowość systemu. $X_0 = C_0 / T$
V <sub>i</sub>	Średnia liczba odwołań do zasobu i w czasie obsługi żądania. $V_i = C_i / C_0$

Źródło: *Performance by Design*, Daniel A. Menasce, Virgilio A.F. Almeida i Lawrence W. Dowdy, Prentice Hall 2004

z informacjami zawartymi w tabeli 6.2 stopień wykorzystania zasobu definiuje się jako  $U_i = B_i / T$ . Aby wyliczyć średni czas realizowania zadania przez zasób, można przemnożyć wynik wcześniejszego równania przez czynnik  $C_i / C_0$ , co w konsekwencji prowadzi do uzyskania zależności:

$$U_i = (B_i / C_i) / (T / C_i)$$

Ponieważ czynnik  $B_i / C_i$  odpowiada średniemu czasowi wykonywania usługi, a  $T / C_i$  jest odwrotnością przepustowości zasobu ( $X_i$ ), równanie można uprościć do postaci:

$$U_i = S_i \times X_i$$

Powyższa zależność jest matematyczną reprezentacją *reguły wykorzystania* (ang. *utilization law*) zasobu, która stanowi, że stopień wykorzystania zasobu jest iloczynem średniego czasu wykonywania usługi i przepustowości. Jeśli wartość współczynnika realizacji zadań odpowiada przypadkowi, w którym wszystkie żądania dostarczone w czasie obserwacji zostały obsłużone ( $C_i = A_i$ ), wówczas  $X_i = I_i$ , a wcześniejsza reguła może być przedstawiona jako:

$$U_i = S_i \times I_i$$

Jeżeli analizowany zasób występuje w kilku egzemplarzach (na przykład jako kilka połączeń, kilka procesorów itp.), prawo wykorzystania zasobu musi zostać zmienione tak, aby uwzględniało liczbę egzemplarzy:

$$U_i = (S_i \times X_i) / m$$

gdzie m odpowiada liczbie serwerów danego zasobu.

Odwwołanie do usługi niemal zawsze wymaga wykorzystania kilku zasobów krytycznych dla funkcjonowania systemu. Na przykład obsługa żądania HTTP dostarczonego do serwera wiąże się z koniecznością wykonania kilku operacji odczytu, które zwrócą dane niezbędne do wygenerowania odpowiedzi. Jeśli dane te znajdują się w pamięci podręcznej, wykorzystywanym zasobem jest pamięć RAM. W przeciwnym razie informacje muszą zostać odczytane z dysku (dysków). Jeśli dany zasób jest wykorzystywany podczas obsługi grupy żądań, możliwe jest wyznaczenie współczynnika wydajnościowego o nazwie *zapotrzebowania na usługę* (ang. *service demand*). Zapotrzebowanie na usługę  $D_i$  odpowiada całkowitemu czasowi, w którym przeciętne żądanie (będące przedmiotem badania) jest obsługiwane w zasobie  $i$ . Wzór opisujący wartość parametru  $D_i$  został zamieszczony poniżej.

$$D_i = (U_i \times T) / C_0 = U_i / X_0$$

Alternatywnie wartość tę można wyrazić jako:

$$D_i = V_i \times S_i$$

Zgodnie z tą zależnością (nazywaną *regulą zapotrzebowania na usługę* (ang. *service demand law*)) zapotrzebowanie na usługę jest wyrażane przez iloczyn liczby odwołań i czasu obsługi lub jako iloraz stopnia wykorzystania zasobu i całkowitej przepustowości systemu. W przypadku dowolnego zasobu o wielu egzemplarzach przedstawione wcześniej równanie można uogólnić w następujący sposób:

$$D_i = U_{i,r} / X_{0,r} = V_{i,r} \times S_{i,r}$$

gdzie  $r$  reprezentuje różne klasy zapotrzebowań na usługę, a każda z tych klas jest obliczana niezależnie.

Żałujemy, że analizując zasób  $i$ , zarejestrowaliśmy, że liczba odwołań do zasobu wynikająca z realizacji żądania wynosi 4, a przepustowość zasobu to 3,5 żądania na sekundę. Gdyby rzecz dotyczyła dysku, wartość 3,5 żądania na sekundę odpowiadałaby takiej liczbie operacji wejścia-wyjścia (zapisu lub odczytu) w czasie sekundy (IOPS — *Input/Output Operations per Second*). Odnosząc przepustowość zasobu  $X_i$  do przepustowości systemu  $X_0$ , można wykorzystać wzór:

$$X_i = V_i \times X_0$$

którego ogólna postać to:

$$X_{i,r} = V_{i,r} \times X_{0,r}$$

Zależność ta jest nazywana *regulą wymuszonego przepływu* (ang. *forced flow law*). Zastosowanie reguły w analizowanym przykładzie oznaczałoby, że przepustowość dysku wynosi  $3,5 \times 4$  IOPS, czyli 14 IOPS.

Wartości średniej liczby żądań, przepustowości oraz średniego czasu realizacji żądania są ze sobą związane *regulą Little'a*:

$$A_i = X_i \times S_i$$

Jako przykład zastosowania reguły rozważmy nieskomplikowany przypadek, w którym podsystem dyskowy obsługuje jedno żądanie lub nie obsługuje żadnych żądań. Prawdopodobieństwo tego, że żądanie jest obsługiwane, odpowiada poziomowi wykorzystania podsystemu dyskowego. Gdy żądania nie są dostarczane, wartość prawdopodobieństwa

reprezentuje czas pracy jałowej podsystemu dyskowego. Przedstawione powyżej równanie jest pewnym przekształceniem reguły wykorzystania zasobu.

Jeśli istnieje mechanizm kolejkowania żądań w podsystemie dyskowym i zarejestrowano w nim określoną liczbę aktywnych żądań, możliwe jest wyznaczenie zależności między długością kolejki i liczbą aktywnych żądań ( $N_i$ ) a średnim czasem realizacji żądania ( $R_i$ ) oraz przepustowością ( $X_i$ ):

$$N_i = R_i \times X_i$$

Proste przestawienie elementów równania prowadzi do wniosku, że znając długość kolejki oraz przepustowość systemu, można obliczyć szybkość generowania odpowiedzi:

$$R_i = N_i / X_i$$

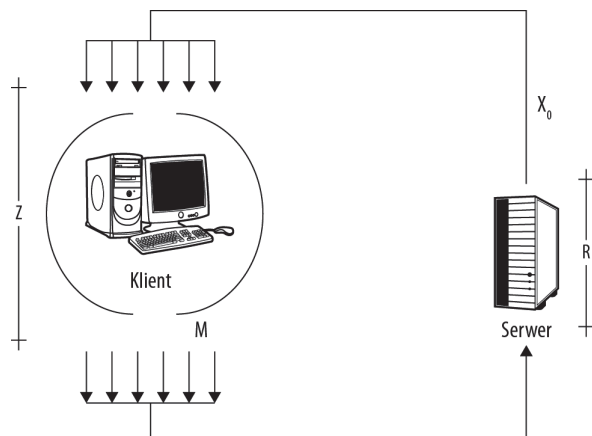
Prawo Little'a znajduje zastosowanie w operacjach szacowania wydajności systemu niezależnie od rodzaju zasobów i zasad ich wykorzystywania. Ma jednak pewne ograniczenia, które trzeba uwzględnić. Aby reguła Little'a dawała poprawne wyniki, żądania nie mogą być tworzone ani anulowane w analizowanym systemie. Żądanie zapisane w kolejce musi po pewnym czasie zostać przetworzone przez system. Czas przechowywania żądań w kolejce nie ma znaczenia, a kolejność pobierania danych może być dowolna (FIFO, LILO, losowa) — w regule Little'a są bowiem uwzględniane wartości średnie.

Przeanalizujmy system typu klient-serwer z wieloma klientami ( $M$ ) odwołującymi się do serwera w sposób przedstawiony na rysunku 6.6. W danym czasie jednostka kliencka przetwarza żądanie lub nie wykonuje żadnego zadania. Średnia liczba jednostek klienckich przetwarzających żądania jest opisana jako  $M_{avg}$ . Natomiast średnia liczba jednostek pracujących w stanie jałowym jest wyrażona za pomocą zmiennej  $N_{avg}$ . Ponieważ jednostka kliencka może mieć dowolny stan, całkowita liczba klientów wynika z równania:

$$M = M_{avg} + N_{avg}$$

### Rysunek 6.6.

*Model  
żądania-odpowiedzi  
w systemie  
klient-serwer*



Na rysunku 6.6 przedstawiono przypadek dostarczenia do serwera wielu żądań klienckich (grupa strzałek widocznych w dolnej części rysunku). Średni czas pozostawania systemu klienckiego w stanie pracy jałowej ( $Z$ ) reprezentuje słupek zamieszczony po lewej stronie jednostki klienckiej. Natomiast średni czas odpowiedzi serwera ( $R$ ) jest odzwierciedlony za

pomocą słupka znajdującego się po prawej stronie rysunku. Z reguły Little’a wynika również, że średnia liczba klientów pozostających w stanie przetwarzania żądania zależy od przepustowości systemu ( $X_0$ ) pomnożonej przez czas odpowiedzi serwera:

$$M_{avg} = X_0 \times Z$$

co oznacza, że średnia liczba żądań w jednostce czasu (przepustowość) równa się liczbie zrealizowanych żądań w jednostce czasu (przepustowości systemu ( $X_0$ )).

Odniesienie reguły Little’a do serwera prowadzi do wyznaczenia zależności:

$$N_{avg} = X_0 \times R$$

Z kolei połączenie obydwu wyrażeń pozwala na uzyskanie równania, które jest nazywane *regułą czasu interaktywnej odpowiedzi*:

$$R = (M / X_0) - Z$$

Ogólniejszy zapis odnoszący się do zwielokrotnionych systemów to:

$$R_r = (M_r / X_{0,r}) - Z_r$$

Z powyższej reguły wynika, że czas odpowiedzi serwera jest równy liczbie klientów podzielonej przez przepustowość i pomniejszonej o czas nieaktywności.

Wszystkie omówione reguły operacyjne zostały zestawione w tabeli 6.2.

**Tabela 6.2.** Reguły operacyjne

Reguła	Zależność	Opis
Reguła wykorzystania	$U_i = X_i \times S_i = I_i \times S_i$	Odnosi wykorzystanie zasobu do przepustowości i średniego czasu przetwarzania żądania. Ostatni człon równania jest prawdziwy tylko wtedy, gdy wszystkie odwołania są przetwarzane.
Reguła wymuszonego przepływu	$X_i = V_i \times X_0$	Przepustowość zasobu jest równa liczbie odwołań (żądań) pomnożonej przez przepustowość systemu.
Reguła zapotrzebowania na usługę	$D_i = V_i \times S_i = U_i / X_0$	Zapotrzebowanie na usługę jest zależne od liczby odwołań pomnożonej przez średni czas realizacji żądania lub od stopnia wykorzystania zasobu podzielonego przez przepustowość systemu.
Reguła Little’a	$N_i = R_i \times X_i$	Długość kolejki i liczba aktywnych żądań są zależne od średniego czasu przetwarzania żądania pomnożonego przez przepustowość.
Reguła czasu interaktywnej odpowiedzi	$R = (M / X_0) - Z$	W interaktywnym systemie szybkość generowania odpowiedzi jest równa liczbie klientów podzielonej przez przepustowość i pomniejszonej o czas nieaktywności.

## Eliminowanie zatorów

Najważniejszym celem wszystkich opisywanych operacji jest uzyskanie jak największej przepustowości i jak najmniejszych czasów odpowiedzi podczas realizowania usług w ramach aktualnie posiadanej technologii. Aby zastosować którąkolwiek z pięciu opisanych reguł, trzeba umieć wyodrębnić parametry wydajnościowe występujące w równaniu, co w przypadku złożonych systemów sieciowych bywa skomplikowanym zadaniem. Ponadto poszczególne zależności opisują jedynie podstawowe mechanizmy wydajnościowe, które stanowią podstawę do obliczeń lub aproksymacji wartości w konkretnym rozważanym modelu wydajnościowym.

Osoby, które muszą zmierzyć się z problemem przeanalizowania całej sieci w celu zwiększenia jej wydajności, często stają przed niezwykle trudnym zadaniem. W niemal wszystkich przypadkach wydajność usługi zależy głównie od jednego podsystemu lub jednego czynnika. Znacznie rzadziej problem odnosi się do dwóch czynników. Każdy przypadek ograniczenia wydajności wynika z powstania *zatoru*. Zator z kolei sprawia, że dany zasób ma największy poziom wykorzystania i najmniejszą szybkość odpowiedzi — pracuje na granicy przepustowości. Zwiększanie wydajności polega na sukcesywnym eliminowaniu zatorów, aż do uzyskania zadowalających rezultatów. Na przykład gdyby w analizowanej sieci występowały trzy połączenia 10Base-T ograniczające szybkość wymiany informacji, usunięcie najbardziej spowalniającego ruch połączenia spowodowałoby, że zator tworzyłby się na jednym z pozostałych połączeń. Z kolei usunięcie wszystkich połączeń 10Base-T doprowadziłoby do wystąpienia zatoru zupełnie innego rodzaju, który mógłby wynikać na przykład z pracy koncentratorów.

Rozważmy istnienie czterech hipotetycznych zasobów oznaczonych literami od A do D, których wykorzystanie i przepustowość była rejestrowana przez pewien czas. Wykres zależności wykorzystania od przepustowości odpowiadający każdemu z tych zasobów został przedstawiony na rysunku 6.7. Każdy z symboli (znak plus, trójkąt, kwadrat i kółko) reprezentuje punkt pomiaru danych. Zasoby od B do D wykazują wolną pojemność w badanym zakresie przepustowości. Jednak wykorzystanie zasobu A rośnie liniowo do osiągnięcia przepustowości o wartości 7, po czym obsługa żądań staje się mniej wydajna, co obrazuje spłaszczona krzywa. Zwiększenie wydajności zasobu A wyeliminowałoby ten obserwowany zator.

Ponieważ reguła zapotrzebowania na usługę uzależnia zapotrzebowanie na zasób od jego wykorzystania i przepustowości, nic nie stoi na przeszkodzie, aby użyć wartości wyznaczonych eksperymentalnie do oszacowania zapotrzebowania na usługę zasobu zgodnie z poniższą zależnością:

$$D_{i,r} = U_{i,r}/X_0 = U_A/X_0 + U_B/X_0 + U_C/X_0 + U_D/X_0$$

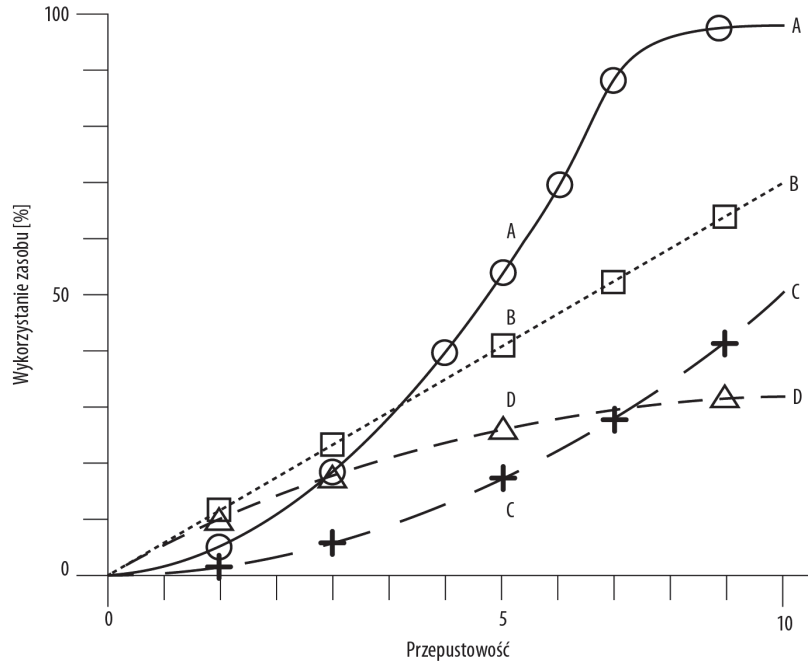
Wynik odpowiada całkowitemu zapotrzebowaniu na zasób systemowy z uwzględnieniem całościowej przepustowości systemu, która została zmierzona. Zasób, który cechuje się najwyższym zapotrzebowaniem na usługę, ma również największe wykorzystanie i vice versa. Stanowi jednocześnie zator dla systemu, opisany poniższym równaniem:

$$X_0 = 1 / (\text{Max}\{D_i\})$$

Wyrażenie jest prawdziwe w przypadku zasobu A w czasie dużego obciążenia (widocznego na rysunku 6.7) i wyznacza górną granicę przepustowości przy dużym obciążeniu.

**Rysunek 6.7.**

Wykres wykorzystania w funkcji przepustowości dla czterech zasobów (przypadek zatoru w zasobie A)



Różnym rodzajom zasobów odpowiadają różne poziomy ostrożnościowe stopnia wykorzystania. Na przykład dyski należy monitorować po przekroczeniu 50 procent wykorzystania, a powodem do zmartwienia jest przekroczenie progu 70 procent. Sytuacja staje się krytyczna, gdy wykorzystanie osiągnie 80 procent. Po przekroczeniu wartości 85 procent wiele operacji dyskowych kończy się niepowodzeniem. Problem ten jest szczególnie dokuczliwy w aplikacjach bazodanowych i graficznych, które przechowują kopie całego zbioru danych w tymczasowych plikach dyskowych.

Analiza liczby odwołań (żądań) w zależności od zapotrzebowania na usługę i przepustowości pozwala na ustalenie przyczyn zatoru w czasie niewielkiego obciążenia zasobu — co jest problemem o zupełnie innym charakterze niż opisywany na przykładzie dużego obciążenia. Zależność między wymienionymi wielkościami definiuje reguła Little’a. W mało obciążonym systemie o  $N$  transakcjach, przy założeniu braku kolejki, reguła Little’a stanowi, że:

$$N = X \times R \Rightarrow (K_{S_{i-1}} D_i) \times X_0$$

Przekształcenie nierówności z wyznaczeniem  $X_0$  prowadzi do zależności:

$$X_0 \leq N / (K_{S_{i-1}} D_i)$$

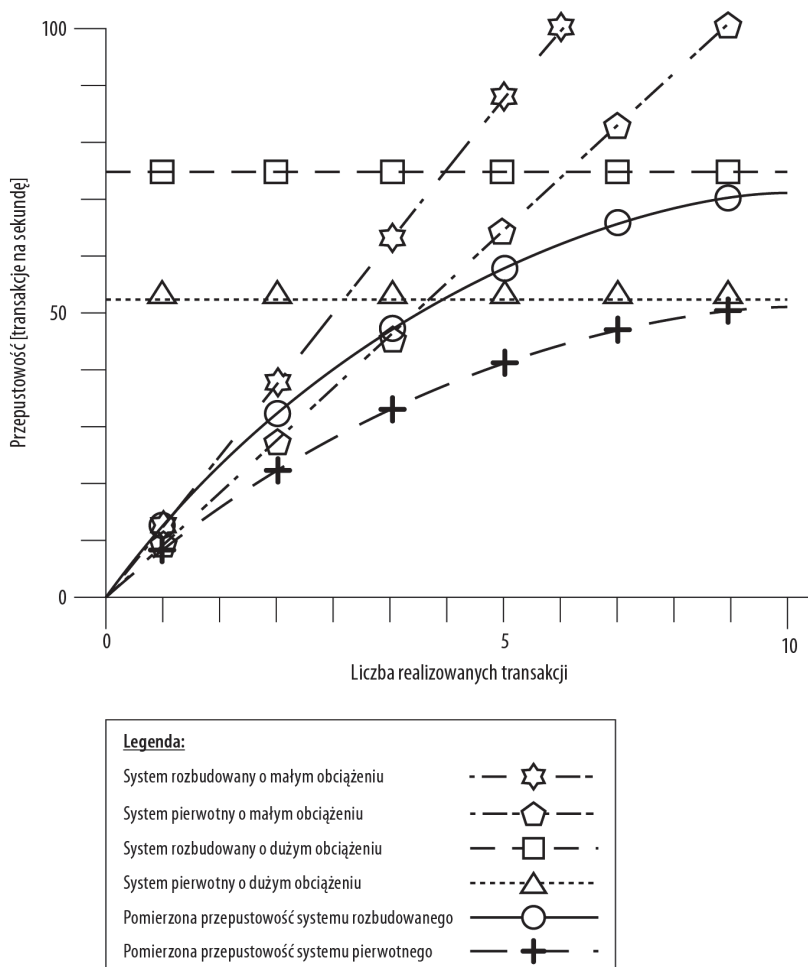
Zależność ta opisuje górną granicę przepustowości w czasie niewielkiego obciążenia. Porównanie obydwu zależności odnoszących się do górnej granicy przepustowości umożliwia wyznaczenie następującej nierówności:

$$X_0 \leq \min [(1 / \max \{D_i\}), (N / (K_{S_{i-1}} D_i))]$$

Na rysunku 6.8 została przedstawiona zależność między dwoma górnymi ograniczeniami przepustowości w przypadkach dużego i małego obciążenia. Zaprezentowano także wpływ rozbudowy (zwiększenia efektywności działania) zasobu na tę zależność. Zmierzona

**Rysunek 6.8.**

Poziomy graniczne przepustowości przy małym i dużym obciążeniu rozbudowanego zasobu



przepustowość pierwotnego systemu jest przedstawiona za pomocą linii ze znakami plus. Z analizy wykresu wynika, że krzywa przepustowości zbliża się do poziomu wyznaczonego przez linię oznaczoną trójkątami, który odpowiada górnej granicy przepustowości w mocno obciążonym systemie. Po rozbudowaniu systemu wykres jego przepustowości (linia z symbolami kółek) jest ograniczony przez nowy poziom maksymalnej przepustowości w warunkach silnego obciążenia (linia z punktami pomiarowymi oznaczonymi za pomocą kwadratów).

Ograniczenia te nie wpływają na system działający pod niewielkim obciążeniem. W przypadku niewielkiego obciążenia system skaluje się liniowo. Dwie krzywe — pierwotnego systemu działającego pod niewielkim obciążeniem (z punktami pomiaru danych w kształcie pięciokątów) oraz rozbudowanego systemu o niewielkim obciążeniu (z punktami w formie gwiazdek) — potwierdzają bezproblemowe skalowanie zasobu w całym badanym zakresie. Rozbudowanemu systemowi odpowiada krzywa o większym nachyleniu, oznaczająca, że system może szybciej osiągnąć większą przepustowość. Warto jednak zwrócić uwagę na ograniczenie liczby transakcji w nieznacznie obciążonym systemie. System oryginalny może obsługiwać jedynie sześć jednoczesnych transakcji, natomiast system rozbudowany — dziewięć.

## Modelowanie sieci

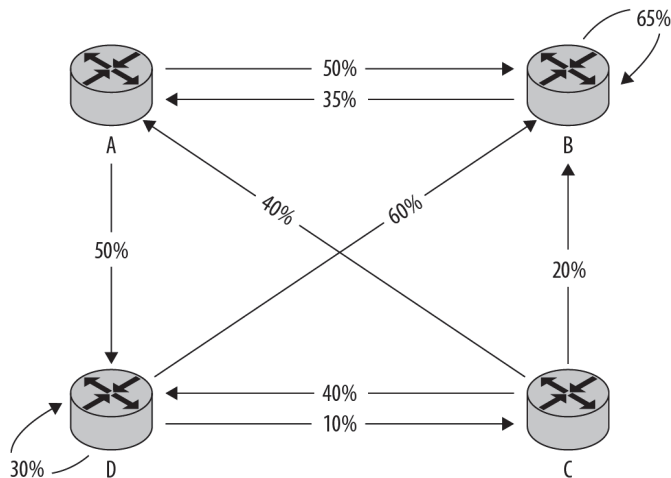
Proces modelowania sieci komputerowej polega na definiowaniu różnych stanów, w których sieć może pracować, prawdopodobieństwo występowania tych stanów oraz zależności między poszczególnymi stanami. Załóżmy, że operujemy sześcioma stanami (od A do F). Jakie są warunkowe prawdopodobieństwa tego, że określony stan będzie prowadził do innych stanów? Odpowiedzi na to pytanie udziela model Markowa (lub łańcuch Markowa), który jest opisywany przez proces stochastyczny spełniający własność Markowa. Własność Markowa stanowi, że przejście z bieżącego stanu procesu do przyszłego stanu jest niezależne od stanów przeszłych. Oznacza to, że przeszłość nie determinuje przyszłości.



Strona rankingowa serwisu Google działa na podstawie łańcucha Markowa.

Aby zbudować model Markowa, należy przeanalizować losowe przejścia między poszczególnymi stanami, rejestrując prawdopodobieństwa każdego z przejść. Wynikiem jest graf węzłów reprezentujących każdy ze stanów wraz z zależnościami między węzłami, odpowiadającymi prawdopodobieństwom przejść. Jako przykład rozważmy sieć pakietową z czterema routerami (o nazwach od A do D), połączonych ze sobą za pośrednictwem segmentów sieci. Na rysunku 6.9 został przedstawiony model Markowa z informacjami na temat prawdopodobieństwa przesłania pakietu w określonym segmencie sieci. Prawdopodobieństwo, że pakiet opuści router, w każdym przypadku wynosi 1,0. Analogicznie prawdopodobieństwo dostarczenia pakietu do każdego routera wynosi 1,0. Aby wyznaczyć sumę prawdopodobieństw, wystarczy dodać wszystkie wartości umieszczone obok strzałek symbolizujących wysyłanie pakietów z routera lub dostarczanie pakietów do routera. Pojedyncza strzałka wskazuje najbliższy router na trasie pakietu.

**Rysunek 6.9.**  
Schemat Markowa  
odnoszący się do  
czterech routerów  
sieciowych



Po wyznaczeniu wartości prawdopodobieństwa przejść między routerami można wykorzystać powstały schemat do przewidywania zachowania sieci i rozwiązywania problemów takich jak typowanie routerów lub segmentów sieci narażonych na największe obciążenie. Chcąc rozwiązać wspomniany problem, trzeba zdefiniować zbiór stanów, które następnie zostaną poddane analizie MVA (analizie wartości średnich). Na przykład jeśli trasa przez

router zostanie opisana jako (Segment 1, Router, Segment 2), to pełną przestrzeń routerów wraz ze zbiorem zmian stanów można opisać w następujący sposób:

(BA, A, AC), (BA, A, AD), (CA, A, AB)...(AD, D, DB), (BD, D, DC), (CD, D, DA)

Prawdopodobieństwo wykorzystania poszczególnych segmentów jest znane, więc wszystkim wymienionym stanom (ścieżkom) można przypisać odpowiednie wagi. Niektóre z wyrazów zostaną odrzucone, innym będzie odpowiadała wyższa wartość prawdopodobieństwa. Zapis wektorów ścieżek jest wówczas następujący:

~~(0.35 BA, A, 0 AC)~~, (0.35 BA, A, 0.5 AD), (0.4 CA, A, 0.5 AB)...  
 (0.5 AD, D, 0.6 DB), ~~(0 BD, D, 0.1 DC)~~, ~~(0.4 CD, D, 0 DA)~~

Wyrazy przekreślone zostały odrzucone, ponieważ zawierają elementy o zerowej wartości prawdopodobieństwa. Opisują więc ścieżki, z których nie można skorzystać. Dzięki temu, że wszystkim ścieżkom przypisano względne wagi, wystarczy zsumować poszczególne wartości, znormalizować je, a następnie wyznaczyć ścieżkę o największym prawdopodobieństwie wykorzystania oraz router, który będzie przenosił ruch o największym natężeniu.

Schematy Markowa znajdują wiele zastosowań. W ten sam sposób można reprezentować dyski w macierzy dyskowej, procesory, zespoły procesorów i dysków lub inne komponenty systemu, które nie są deterministyczne. Tak naprawdę diagram Markowa umożliwia zajęcie do czarnej skrzynki, która jest abstrakcyjnie opisywana przez regułę Little'a.

Choć modele Markowa są stosowane w wielu dziedzinach nauki, nie rozwiązują wszystkich problemów. Zgodnie z zamieszczonymi wcześniej informacjami nie nadają się do wykorzystania w przypadkach, w których wcześniejszy stan systemu wpływa na stan kolejny. Jeśli jeden router jest znacząco wolniejszy w działaniu od innych lub jeśli wykrycie przez router pętli wpływa na wybór kolejnego etapu trasy, to aby model ten dostarczał wiarygodnych wyników, trzeba uwzględnić dodatkowe informacje w samym modelu. Z kolei im więcej dodatkowych czynników model obejmuje, tym bardziej złożone staje się jego wykorzystanie i zwiększa się prawdopodobieństwo uzyskania niewłaściwego wyniku.

Kolejną wadą modelu Markowa jest to, że jego działanie bazuje na założeniu, że względne prawdopodobieństwa są określone za pomocą niezależnych od siebie wag. Jeśli z routera są poprowadzone dwie ścieżki wyjściowe o równym prawdopodobieństwie (50 procent) i dla pierwszego pakietu zostanie wybrana trasa B, prawdopodobieństwo wyboru trasy A dla kolejnego pakietu pozostaje na poziomie 50 procent. Wartości prawdopodobieństw nie wymuszają konkretnej trasy kolejnego pakietu, mimo że w praktyce taka sytuacja nie występuje. W takim przypadku mamy do czynienia z założeniem wykładniczego rozkładu prawdopodobieństwa. Doskonałym przykładem takiej sytuacji jest wykonanie 10 rzutów monetą. Prawdopodobieństwo tego, że będą wypadły jedynie reszki, jest jak 1 do  $2^{10}$  (0,098 %), mimo że w każdym rzucie istnieje 50-procentowa szansa na wypadnięcie reszki.

Aby wykorzystać model Markowa w analizie dwóch ścieżek, konieczne jest wyznaczenie w dwóch segmentach niezależnych stanów, z założeniem wykładniczego rozkładu prawdopodobieństwa. Taki podział prowadzi do uzyskania dokładniejszych wyników, ale jednocześnie zwiększa złożoność obliczeniową algorytmu.

Teoretycznie model Markowa można zastosować do rozwiązania dowolnego problemu. Jednak gdy liczba stanów przekroczy pewien próg, równania stają się bardzo trudne do

obliczenia, a sam model okazuje się trudny do intuicyjnego zrozumienia. Z tego względu tworzone są pewne odmiany modeli Markowa oraz innych modeli analitycznych. Ponieważ kwestia modelowania sieci wiąże się w znacznie większym stopniu z zagadnieniami matematycznymi niż sieciowymi, szczegółowych informacji na temat modelowania wydajności systemów należy szukać w publikacjach poświęconych konkretnie tej tematyce.

## Rozbudowa serwerów

Przeanalizujmy konkretny przykład zastosowania modelu Markowa do określenia sposobu rozbudowy wybranego serwera sieciowego. Załóżmy, że w danej sieci funkcjonują serwery domenowe, których poziom wykorzystania zaczyna osiągać wysokie wartości. Można z tego wywnioskować, że konieczna jest rozbudowa serwerów. Poniżej zostało wymienionych kilka informacji, które są potrzebne, aby można było wybrać spośród komponentów serwera ten, który będzie miał największy wpływ na zwiększenie wydajności systemu.

1. **Maksymalne obciążenie.** Zakładamy, że okres największego obciążenia przypada na godziny od 8.30 do 10.00 w poniedziałek. Wówczas należy dokonać pomiaru poziomu obciążenia.
2. **Charakterystyka aplikacji.** Sposób działania aplikacji jest kluczowym zagadnieniem w przypadku szacowania wielkości pamięci RAM, rozmiaru sektora dyskowego, szerokości pasma sieciowego oraz wielu innych parametrów.
3. **Wydajność dysku.** Właściwe dopasowanie charakterystyki operacji wejścia-wyjścia aplikacji do konfiguracji dysku pozwala na istotne zwiększenie wydajności rozwiązania oraz na obniżenie wymagań sprzętowych wobec dysku.
4. **Oddzielenie funkcji serwera i pamięci masowej.** Dzięki oddzieleniu funkcji serwera od funkcji pamięci masowej system staje się bardziej dostępny, niezawodny i elastyczny.
5. **Wydajność sieci.** Przyjmujemy, że serwery domenowe generują znaczny ruch wynikający z replikacji danych. Wysokie natężenie ruchu wpływa na wydajność sieci. Rozwiązaniem może być zastosowanie mniejszej liczby serwerów, ale o większej efektywności działania. Replikacje powinny być realizowane w ramach oddzielnych segmentów sieciowych. Za zadawalający poziom dostępności tej usługi sieciowej uznaje się wartość 99,95%.
6. **Poziom zwrotu z inwestycji (ROI — *Return on Investment*).** Szacowanie współczynnika ROI w projekcie rozbudowy (udoskonalenia) sieci wynika z konieczności uzasadnienia wydatków. Operacja ta wymaga przeanalizowania czynników, które w innej sytuacji mogłyby zostać pominięte — na przykład czas życia systemów i oprogramowania. Dlatego jest ono istotnym elementem całego projektu i nie wolno go ignorować.

Projekt rozbudowy sieci opracowany z uwzględnieniem powyższych założeń składałby się z następujących etapów:

- ♦ Analiza danych historycznych.
- ♦ Planowanie pojemności.
- ♦ Wybór i projektowanie systemu.

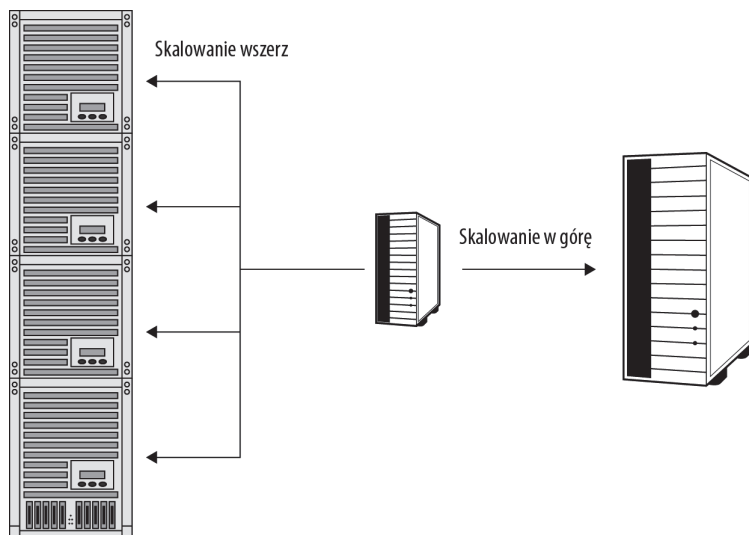
- ♦ Testowanie i dostrajanie.
- ♦ Wdrożenie pilotażowe.
- ♦ Przekazanie do użytkowania.

Jednym z wniosków wynikających z przeprowadzonej analizy jest ustalenie, że należy skonsolidować serwery domenowe, zwiększyć ich moc obliczeniową oraz wydzielić dedykowane połączenia między poszczególnymi maszynami. Nasuwa się więc pytanie, jaki sposób konsolidacji będzie najlepszy. Konsolidacja serwerów może polegać na:

- ♦ **skalowaniu wszerz** — zwiększeniu liczby procesorów przez dodanie kolejnych systemów,
- ♦ **skalowaniu w górę** — zwiększeniu liczby procesorów przez uruchomienie mniejszej liczby wydajniejszych serwerów.

Każde z wymienionych rozwiązań ma inny wpływ na aplikacje serwerów sieciowych oraz na samą infrastrukturę sieci. Graficzna ilustracja procesu skalowania wszerz i w górę została przedstawiona na rysunku 6.10. Skalowanie wszerz polega na dodaniu do istniejącego serwera (po oszacowaniu jego pojemności) kolejnej jednostki tego samego typu. W ten sposób powstaje „farma serwerów”. Skalowanie w górę sprowadza się do zwiększenia pojemności działającego serwera. Oznacza to zwiększenie pojemności aplikacji przez przydzielenie jej większej liczby procesorów. Obydwa rozwiązania mają pewne wady i zalety.

**Rysunek 6.10.**  
Skalowanie wszerz  
(z lewej strony)  
zwiększa liczbę  
serwerów, natomiast  
skalowanie w górę  
oznacza małą liczbę  
serwerów o większej  
mocy obliczeniowej



Skalowanie wszerz można przeprowadzać etapami. Ponadto w porównaniu ze skalowaniem w górę zapewnia więcej możliwości w doborze dostawców urządzeń oraz w konfigurowaniu tych urządzeń. Skalowanie w górę okazuje się zazwyczaj mniej kosztowne, ponieważ ogranicza się do powielenia określonych komponentów składowych systemu w celu uzyskania większej wydajności. W odniesieniu do sieci komputerowych skalowanie wszerz prowadzi do zwiększenia liczby kanałów komunikacyjnych, a to z kolei stanowi punkt wyjściowy do wdrażania technologii związanych z rozkładaniem obciążenia lub zapewnienia tras zapasowych. Fakt większej ceny i niższej niezawodności wynikających z instalowania

dotatkowego sprzętu w skalowaniu wszcz jest rekompensowany przez elastyczność tego rozwiązania. Umożliwia ono bowiem pracę z mniejszymi jednostkami serwerowymi i gwarantuje większą dostępność dzięki nadmiarowości. Z założenia skalowanie wszcz wymaga więc większych nakładów pracy na zarządzanie niż skalowanie w górz.

Jeśli dana aplikacja nie wymaga ustanawiania trwałych połączeń z serwerem (jest bezstanowa), tak jak usługa WWW, to doskonale nadaje się do skalowania wszcz. Rozwiązanie to stosuje się często w wielkich farmach serwerów obsługujących serwisy internetowe, w farmach serwerów terminali oraz innych systemach. Skalowanie wszcz doskonale sprawdza się w sytuacjach, w których działanie aplikacji nie jest ograniczane przez wydajność procesora lub rozmiar pamięci RAM, lecz przez zatory w sieci.

Skalowanie w górz ma również wiele zalet. Stosując tę technikę, zmniejsza się liczbę serwerów, a tym samym liczbę ewentualnych miejsc awarii. Mniej skomplikowana jest architektura sieci, a w związku z tym jest mniej serwerów do utrzymywania i aktualizowania. W rozbudowanych systemach wieloprocesorowych większą uwagę przykładą się do jakości ich komponentów. Serwery te działają pod kontrolą systemów operacyjnych klasy enterprise i zazwyczaj towarzyszy im lepsza obsługa ze strony dostawców. Skalowanie w górz srowadza się do umieszczania większej liczby komponentów w jednym urządzeniu, czyniąc to urządzenie efektywniejszym w działaniu i odporniejszym na usterki.

Jako ogólną zasadę można przyjąć, że wprowadzenie systemów wieloprocesorowych (o znacznej liczbie wysokowydajnych procesorów) nie zwiększa liczby operacji wejścia-wyjścia realizowanych w sieci. Dlatego są one przeznaczone przede wszystkim dla aplikacji, które korzystają na wzroście mocy obliczeniowej i których działanie nie jest ograniczane przez określony poziom operacji wejścia-wyjścia. Doskonałym przykładem są w tym przypadku hurtownie danych, które przetwarzają bardzo duże zbiory danych, ale wymagają połączeń sieciowych o niewielkiej przepustowości. Rozbudowa aplikacji tego typu wymaga więc zastosowania techniki skalowania w górz.

## Podsumowanie

Serwery odgrywają istotną rolę w funkcjonowaniu sieci. Zapewniają innym systemom dostęp do świadczonych usług. W tym rozdziale zostały omówione kluczowe zagadnienia związane z wyznaczaniem pojemności i obciążenia systemów, gdyż informacje te są niezbędne do projektowania właściwie działających sieci. Zaprezentowane zostały różne metodologie rozszerzania pojemności serwerów.

Dane na temat wydajności umożliwiają administratorom określenie podstawowych zależności między komponentami sieci. Na tej podstawie z kolei można wskazać zasoby sieciowe będące przyczyną zatorów i opracować plan usunięcia ograniczeń komunikacyjnych. Szczególnie pomocny w tych działaniach jest omówiony tutaj model Markowa.

Tematem kolejnego rozdziału są interfejsy sieciowe. Interfejsy sieciowe, podobnie jak serwery, są podstawowymi elementami sieciowymi, implementowanymi zarówno w warstwie sprzętowej, jak i programowej.



# Rozdział 7.

## Interfejsy sieciowe

### W tym rozdziale:

- ♦ Interfejsy fizyczne i logiczne
- ♦ Adresy interfejsów fizycznych
- ♦ Wpływ kolejności wyboru powiązań i dostawców
- ♦ Izolacja wielokrotnych połączeń i routing
- ♦ Cechy kart sieciowych

Interfejs jest elementem łączącym dwa różne media lub komponenty. Każde przyłącze do sieci komputerowej jest interfejsem sieciowym, który stanowi element łączący fizyczne warstwy transportowe (odpowiedzialne za przesyłanie informacji) z warstwami przygotowującymi dane do wykorzystania w aplikacji. Interfejs sieciowy dysponuje adresem. Oznacza to, że sygnał przekazywany w medium fizycznym może zostać skierowany do jednego konkretnego interfejsu.

W większości publikacji na temat sieci komputerowych interfejsy sieciowe nie są jednoznacznie zdefiniowane i są prezentowane jedynie w odniesieniu do innych zagadnień. Jednak w tej książce rozdział poświęcony interfejsom sieciowym rozpocznie się właśnie od ich definicji. Uwzględnione zostały tutaj właściwości połączeń sieciowych, które są charakterystyczne dla różnych rodzajów sieci. Dla użytkownika zewnętrznego interfejs sieciowy jest jedynym urządzeniem sieciowym, z którym ten użytkownik ma kontakt.

## Czym jest interfejs sieciowy?

Rozpocznijmy analizę zagadnienia od ustalenia, czym w ogóle jest interfejs sieciowy. Interfejs sieciowy wyznacza granicę między dwoma różnymi mediami sieciowymi. Termin *interfejs sieciowy* może być stosowany w odniesieniu do:

- ♦ punktu styku dwóch różnych sieci, w szczególności styku uwidocznionego na schemacie topologii lub architektury sieci;
- ♦ karty sieciowej, czyli układu scalonego o specjalnym zastosowaniu (ASIC — *Application Specific Integrated Circuit*), stanowiącego element płyty bazowej komputera, karty PC w notebooku, przyłącza USB lub Ethernet bądź innego urządzenia o podobnym przeznaczeniu;

- ♦ obiektu wirtualnego systemu operacyjnego, którym można operować w sposób programowy;
- ♦ punktu przyłączenia terminalu do sieci;
- ♦ punktu połączenia publicznej sieci telefonicznej z prywatną siecią telefoniczną.

Niekiedy stosowane jest również określenie *moduł interfejsu sieciowego* (NIU — *Network Interface Unit*), które odnosi się do elementu łączącego urządzenie w lokalnej sieci komputerowej (LAN — *Local Area Network*). Komponent NIU odpowiada za wysyłanie i odbieranie danych oraz za przekształcanie wymienianych komunikatów w jednostki transmisyjne protokołu wykorzystywanego w sieci. Często moduł ten jest wyposażony w bufor pamięci, który w razie konieczności zapewnia retransmisję danych bez konieczności ponownego pobierania ich z jednostki nadawczej.

## Fizyczne interfejsy sieciowe

Karta sieciowa (NIC — *Network Interface Card*), nazywana niekiedy adapterem sieciowym lub rzadziej adapterem LAN, jest jednym z przykładów interfejsów sieciowych. Zgodnie z definicją modelu odniesienia IOS/OSI (omówionego w rozdziale 2.) karta sieciowa jest urządzeniem warstwy 1. i warstwy 2. — obejmuje zarówno warstwę fizyczną, jak i warstwę łącza danych. Jej zadanie polega na odbieraniu danych z sieci oraz na przekształcaniu danych w sposób, który umożliwi przekazanie ich do kolejnego urządzenia sieciowego (pod kolejny adres) — czyli za wysłanie danych w formacie zrozumiałym dla innego komponentu sieciowego, który następnie zmodyfikuje dane tak, aby mogły zostać wykorzystane w aplikacji. Karta sieciowa jest pewnym rodzajem modułu NIU.

Karta sieciowa nie zmienia przesyłanych danych użytkowych. Przetwarza jedynie ramki, modyfikując w razie konieczności pola nagłówkowe (otoczkę dla porcji danych). W większości kart sieciowych przetwarzanie jest nadzorowane przez układy scalone karty, ale realizowane przez procesor systemowy. Wydajność sieciowych operacji wejścia-wyjścia jest jednym z parametrów, które w szczególny sposób rzutują na wydajność systemu.

Obciążone interfejsy sieciowe mogą zajmować znaczną ilość zasobów procesora i doprowadzić do przeciążenia komputera. Problem ten nie występuje raczej w systemach użytkowników końcowych, ale bywa uciążliwy w wysoko wydajnych rozwiązaniach sieciowych, których efektywność jest ograniczona przez operacje wejścia-wyjścia. Na przykład wydajność serwerów WWW jest bezpośrednio zależna od efektywności sieciowych operacji wejścia-wyjścia i często przez nie ograniczana. Niektóre karty sieciowe oraz nowoczesne płyty główne zawierają specjalne układy ASIC odciążające system i przenoszące obsługę stosu TCP/IP do kontrolera sieciowego. Technologia ta nazywa się *TCP offload*. Mechanizm TCP offload (TOE — *TCP Offload Engine*) jest zoptymalizowany do przetwarzania stosu TCP/IP.



Więcej informacji na temat technologii TCP offload znajduje się w rozdziale 16.

Układy scalone interfejsów sieciowych są obecnie implementowane na niemal każdej płycie głównej komputera, ponieważ nie są szczególnie kosztowne, a dostępność wbudowanej karty sieciowej jest mile widziana przez użytkowników. Wiele płyt głównych o bardzo dużej

wydajności (przeznaczonych do gier lub wykorzystywanych w stacjach roboczych bądź serwerach) zawiera dwa interfejsy sieciowe. Takie rozwiązanie rozszerza zakres możliwości konfiguracyjnych. Dwa interfejsy sieciowe zapewniają:

- ♦ **Nadmiarowość.** Jeśli jeden interfejs ulegnie awarii, drugi przejmie jego zadania.
- ♦ **Wysoka wydajność.** Nic nie stoi na przeszkodzie, żeby dwa interfejsy pracowały jednocześnie.
- ♦ **Izolacja.** Każdy z interfejsów może być przypisany do innej sieci, co jest podstawą działania routera.

## Logiczne interfejsy sieciowe

Interfejsy sieciowe są realizowane zarówno jako komponenty fizyczne, jak i logiczne. Większość definicji zawartych we wcześniejszych wyliczeniach odnosi się do fizycznych interfejsów sieciowych. Jednak można je również rozpatrywać jako logiczne punkty styku systemu z siecią. Logiczne interfejsy sieciowe należy postrzegać jako programowe moduły lub funkcje, które emulują pracę urządzeń sprzętowych. Odbierają i generują ruch sieciowy. Mogą również działać jako elementy przekierowujące strumienie wejściowe i wyjściowe. Trzeba jednak pamiętać, że logiczne interfejsy sieciowe wymagają dostępności fizycznych interfejsów, aby możliwe było przetwarzanie ruchu sieciowego.

Jednym z ważniejszych logicznych interfejsów sieciowych (nazywanych też interfejsami wirtualnymi) jest interfejs pętli zwrotnej, czyli moduł programowy emulujący wewnętrzną kartę sieciową, która przyjmuje żądania systemowe i generuje na nie odpowiedzi. Pętla zwrotna znajduje zastosowanie w testowaniu oprogramowania sieciowego.

W wersji 4. protokołu IP interfejs pętli zwrotnej jest dostępny pod adresem:

```
127.0.0.1
```

Natomiast w wersji 6. protokołu IP jego adres to:

```
::1
```

Wykonanie polecenia PING w odniesieniu do jednego z wymienionych adresów niemal zawsze powoduje odesłanie odpowiedzi (jeśli funkcje sieciowe systemu zostały uaktywnione). W przypadkach niewłaściwego działania kart sieciowych lub nieodpowiedniej konfiguracji niektóre systemy operacyjne zwracają adres pętli zwrotnej podczas wykonywania każdego polecenia PING z lokalnego systemu. Interfejs pętli zwrotnej jest elementem diagnostycznym, niedostępnym poza testowanym systemem.

Nowoczesne systemy operacyjne reprezentują interfejsy sieciowe jako obiekty, których właściwości można zmieniać w sposób programowy. Obiektowe języki programowania pozwalają na powoływanie (tworzenie) obiektów interfejsów sieciowych, sprawdzanie ich ustawień, wysyłanie danych oraz na zmianę właściwości, a tym samym zmianę ustawień działających kart sieciowych.

Na przykład w języku Java interfejsy sieciowe są reprezentowane przez obiekty klasy `java.net.NetworkInterface`. Kierując odpowiednie zapytania do systemu, można uzyskać listę wszystkich obiektów interfejsów sieciowych. Utworzenie listy wykorzystywanych

adresów IP sprowadza się do wykonania instrukcji `getInetAddresses()`. Inne metody umożliwiają wykonywanie właściwych im operacji z użyciem interfejsów oraz programową zmianę parametrów tych interfejsów. Analogiczne instrukcje i obiekty istnieją we wszystkich obiektowych językach programowania. Jednym z przykładów jest język C#, udostępniający szeroką gamę obiektów związanych z interfejsami sieciowymi, które wchodziły w skład platformy Microsoft .NET Framework.



Krótki kurs na temat sposobów posługiwania się interfejsami sieciowymi z poziomu języka Java jest dostępny pod adresem <http://download.oracle.com/javase/tutorial/networking/nifs/index.html>. Podobny przewodnik po obiektach platformy .NET znajduje się pod adresem <http://msdn.microsoft.com/en-us/library/system.net.aspx>.

Nazwa interfejsu logicznego to nazwa interfejsu fizycznego uzupełniona o dodatkowy identyfikator. W takich systemach operacyjnych jak Solaris format zapisu nazwy jest następujący:

```
<nazwa_sterownika><interfejs_fizyczny>:<numer_interfejsu_logicznego>
```

Istnienie numeru interfejsu logicznego sugeruje możliwość zdefiniowania w systemie wielu interfejsów logicznych. Istotnie, administrator systemu może tworzyć logiczne interfejsy sieciowe i przypisywać im adresy IP, które wcale nie muszą należeć do tego samego zakresu (podsieci) co adres interfejsu fizycznego. Dzięki temu pojedynczy system może być w sieci widoczny jako kilka systemów.

Zgodnie z tą konwencją nazwy interfejsów mogą być następujące:

```
hme0:1  
hme0:2  
hme0:3
```

itd.

Na przykład jeśli w danym systemie jest uruchomione środowisko przeznaczone do wirtualizacji (np. Microsoft Virtual PC lub VMWare Workstation), to każda z utworzonych maszyn wirtualnych może skorzystać z interfejsu wirtualnego lub większej liczby takich interfejsów. Każdemu interfejsowi logicznemu można przypisać nie tylko odrębny adres IP, ale również niezależną nazwę komputera. Taki przypadek został przedstawiony na rysunku 7.1, na którym są widoczne dwa interfejsy wirtualne — jeden przeznaczony dla systemu Ubuntu, a drugi dla systemu Windows Server 2008.

Wielokrotne wirtualne interfejsy sieciowe znajdują na przykład zastosowanie w **izolacji aplikacji**. Określony interfejs może być skojarzony z wybraną aplikacją lub egzemplarzem tej aplikacji.

Na przykład nowoczesne serwery WWW, takie jak Internet Information Services (IIS) firmy Microsoft lub Apache, pozwalają na tworzenie wirtualnych witryn WWW, dostępnych za pośrednictwem wskazanego interfejsu logicznego. Poszczególne serwisy WWW są widoczne dla użytkownika sieciowego tak, jakby były uruchomione w niezależnych systemach.

Tworząc wirtualne interfejsy sieciowe, uruchamia się programową emulację urządzenia bez ponoszenia jakichkolwiek kosztów finansowych. Dzięki wirtualnym interfejsom sieciowym można się odwoływać do poszczególnych jednostek w bezpośredni sposób, co ułatwia wykonywanie niektórych zadań (takich jak sporządzanie kopii zapasowych lub zarządzanie wieloma osobnymi systemami).

Trzeba jednak pamiętać, że wszystkie wirtualne interfejsy sieciowe wymagają dostępności fizycznej karty sieciowej lub modułu NIU, za których pośrednictwem dane są przekazywane do sieci. Zwiększanie liczby interfejsów wirtualnych prowadzi zatem do wzrostu obciążenia sieci w czasie rzeczywistej pracy systemu. Ponadto konieczność powoływania poszczególnych interfejsów wirtualnych w czasie uruchamiania systemu powoduje wydłużenie czasu rozruchu serwera. Interfejsy sieciowe są skomplikowanymi obiektami, więc w przypadku dużej ich liczby (niezależnie, czy są to komponenty rzeczywiste, czy wirtualne), czas uruchamiania systemu może się istotnie wydłużyć.

## Adresy sieciowe

Z punktu widzenia użytkownika sieci interfejs sieciowy jest tożsamy z systemem. To w interfejsie jest zapisany niepowtarzalny adres i to interfejs realizuje sieciowe operacje wejścia-wyjścia, dzięki którym dane mogą być dostarczane do systemu i z niego wysyłane. Adres interfejsu sieciowego jest wartością wyróżniającą daną kartę sieciową spośród wszystkich innych kart, nawet jeśli pochodzą one od jednego producenta i są to urządzenia jednego modelu.

## Adresy fizyczne

W sieciach Ethernet adres jest 48-bitową niepowtarzalną wartością, nazywaną adresem MAC. Każda karta sieciowa musi posiadać adres MAC. Wartość adresu MAC jest zapisywana w pamięci ROM (tylko do odczytu) karty na etapie produkcji. Zasady, na których podstawie producenci dobierają adresy MAC, są zdefiniowane w standardach opracowanych przez organizację Institute of Electrical and Electronics Engineers (IEEE). Niepowtarzalność wartości gwarantuje rejestr dostawców. Podczas tworzenia wirtualnego interfejsu sieciowego adres MAC jest przypisywany przez środowisko wirtualizacyjne.

Adres MAC jest adresem fizycznym, ponieważ jest przypisany do urządzenia. Można go zmieniać (fałszować), ale nie wolno go duplikować.

Aby umożliwić bezproblemowe przenoszenie interfejsów sieciowych z jednej sieci do innej, każdemu interfejsowi przypisuje się również adres sieciowy. Operację tę należy traktować jako przydzielenie interfejsowi adresu logicznego, którego dobór należy do zadań administratora. Adres sieciowy na stałe przypisany do interfejsu jest nazywany *adresem statycznym*. Z kolei adres przydzielony automatycznie na pewien czas nazywa się *adresem dynamicznym*. Aby sieć działała poprawnie, nie mogą w niej wystąpić dwie takie same wartości adresu logicznego. Dany adres sieciowy może być wykorzystany w innej sieci lub innej podsieci, ale powielenie go w jednej podsieci prowadzi do błędnego działania sieci.

Typowy sposób odwoływania się do fizycznego interfejsu sieciowego został przedstawiony poniżej, na przykładzie składni nazw obowiązujących w systemie Solaris:

```
<nazwa_sterownika><numer_modułu_fizycznego>
```

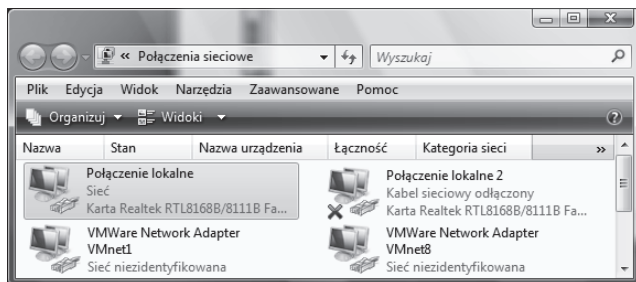
Nazwy interfejsów są więc następujące:

```
hme0  
hme1
```

W systemach UNIX i Linux schemat nazewniczy jest bardzo podobny. Z kolei w systemach Windows do wyróżniania interfejsów wykorzystywane są długie, opisowe nazwy.

Na rysunku 7.1 zostało pokazane okno *Połączeń sieciowych* systemu Windows Vista. Wynika z niego, że komputer dysponuje czterema interfejsami sieciowymi. Interfejsy *Połączenie lokalne* oraz *Połączenie lokalne 2* są fizycznymi interfejsami 1000Base-T odpowiadającymi kontrolerom Realtek zainstalowanym na płycie głównej. Jedna z kart pracuje, natomiast druga jest odłączona (co jest symbolizowane za pomocą czerwonego znaku X). Dwie pozostałe ikony odpowiadają interfejsom wirtualnym *VMnet1* i *VMnet8*. Karta *VMnet1* została skojarzona z systemem Ubuntu 8.04 (Hardy Heron), uruchomionym w ramach maszyny wirtualnej. Natomiast karta *VMnet8* należy do systemu Windows Server 2008 Enterprise Edition, działającego na drugiej maszynie wirtualnej.

**Rysunek 7.1.**  
*Ikony interfejsów  
sieciowych widoczne  
w oknie Połączenia  
sieciowe systemu  
Windows Vista*



W różnych sieciach stosuje się różne schematy adresowania, jednak niezależnie od wybranego rozwiązania adres sieciowy przypisany określonej jednostce musi być niepowtarzalny w danej sieci. W przypadku powielenia adresu sieciowego system operacyjny zazwyczaj wyświetla stosowny komunikat o błędzie, jednak w niektórych sytuacjach można zaobserwować nietypowe zachowanie sieci.

## Konfiguracja interfejsów sieciowych

Interfejsy sieciowe są tak ważnymi elementami komputera, że każdy sieciowy system operacyjny udostępnia przynajmniej dwie metody (a zazwyczaj więcej metod) ich weryfikowania, tworzenia i modyfikowania. Aby sprawdzić ustawienie wszystkich interfejsów sieciowych wykorzystujących stos TCP/IP, należy wykonać wszystkie etapy przedstawionej poniżej procedury:

W systemie Windows:

1. Kliknij ikonę *Start* i wybierz opcję *Uruchom*. Na ekranie zostanie wyświetlone okno umożliwiające wpisanie polecenia.
2. Wpisz instrukcję `CMD` i naciśnij *Enter*.
3. Wpisz instrukcję `IPCONFIG /ALL` i naciśnij *Enter*.

W oknie wiersza poleceń wyświetli się zestawienie wszystkich interfejsów sieciowych wraz z informacjami o adresach MAC, adresach sieciowych i statusie. Przykładowy wygląd opisywanego okna został zaprezentowany na rysunku 7.2.

**Rysunek 7.2.**

Dane na temat wszystkich interfejsów sieciowych wyświetlone po wykonaniu polecenia `IPCONFIG /ALL` w systemie Windows Vista

```
c:\>ipconfig /all

Konfiguracja IP systemu Windows

Nazwa hosta . . . . . : lajfbuk
Sufiks podstawowej domeny DNS . . : 
Typ węzła . . . . . : Hybrydowy
Routing IP włączony . . . . . : Nie
Serwer WINS Proxy włączony . . . : Nie

Karta Ethernet Bluetooth:
Stan nośnika . . . . . : Nośnik odłączony
Sufiks DNS konkretnego połączenia : 
Opis . . . . . : Bluetooth Personal Area Network
Adres fizyczny. . . . . : 00-03-7A-DD-81-47
DHCP włączone . . . . . : Tak
Autokonfiguracja włączona . . . : Tak

Karta Ethernet Połączenie lokalne:
Stan nośnika . . . . . : Nośnik odłączony
Sufiks DNS konkretnego połączenia : 
Opis . . . . . : Marvell Yukon 88E8055 PCI-E Gigabit Et
Adres fizyczny. . . . . : 00-17-42-2E-7E-8E
DHCP włączone . . . . . : Tak
Autokonfiguracja włączona . . . : Tak

Karta bezprzewodowej sieci LAN Połączenie sieci bezprzewodowej:
Sufiks DNS konkretnego połączenia : 
Opis . . . . . : Intel(R) Wireless WiFi Link 4965AGN
Adres fizyczny. . . . . : 00-1D-E0-A1-F1-CF
DHCP włączone . . . . . : Tak
Autokonfiguracja włączona . . . : Tak
Adres IPv6 połączenia lokalnego . : fe80::39f8:ddba:2630:ddid:10(Preferowa
Adres IPv4 . . . . . : 192.168.2.102(Preferowane)
Maska podsieci . . . . . : 255.255.255.0
Dzierżawa uzyskana. . . . . : 3 października 2010 09:07:20
Dzierżawa wygasa. . . . . : 4 października 2010 09:07:26
Brama domyślna. . . . . : 192.168.2.1
Serwer DHCP . . . . . : 192.168.2.1
Identyfikator IAD DHCPv6 . . . . : 167770800
Serwery DNS . . . . . : 62.233.233.233
                        87.204.204.204
NetBIOS przez Tcpip . . . . . : Włączony

Karta tunelowa Połączenie lokalne*:
Sufiks DNS konkretnego połączenia : 
Opis . . . . . : Karta Microsoft ISATAP
Adres fizyczny. . . . . : 00-00-00-00-00-00-E0
DHCP włączone . . . . . : Nie
Autokonfiguracja włączona . . . : Tak
Brama domyślna. . . . . : 
NetBIOS przez Tcpip . . . . . : Wyłączony

Karta tunelowa Połączenie lokalne* 6:
```

W systemie Ubuntu 8.04:

1. Wybierz z menu opcję *Aplikacje/Akcesoria/Terminal*. Na ekranie wyświetli się okno terminalu.
2. Wpisz polecenie `ifconfig` i naciśnij *Enter*.

Na rysunku 7.3 został przedstawiony wynik wykonania instrukcji w oknie terminalu systemu Ubuntu. Widać na nim jeden interfejs sieci Ethernet (`eth0`) oraz interfejs pętli zwrotnej (`lo`).

Warto zwrócić uwagę na to, że adres fizyczny jest w tym przypadku wymieniony w polu `Hwaddr`, w pierwszym wierszu zestawienia odnoszącego się do każdego z interfejsów. W drugim wierszu wyświetlony został adres sieciowy protokołu IP w wersji 4. Natomiast w trzecim wierszu jest widoczny adres IP wersji 6.

Polecenie `IPCONFIG` w systemie Windows oraz odpowiadająca mu instrukcja `ifconfig` systemów Macintosh, Linux, Solaris, UNIX umożliwiają dołączenie wielu parametrów i opcji. W przypadku systemu Windows opcje polecenia `IPCONFIG` pozwalają na wyświetlenie szczegółowych danych, a także na odnowienie adresu IP kart sieciowych. Instrukcja `ifconfig` daje o wiele większe możliwości tworzenia interfejsów sieciowych i modyfikowania ich parametrów. Choć składnia instrukcji `ifconfig` jest bardzo zbliżona w różnych systemach operacyjnych (szczególnie w systemach UNIX, Linux i Macintosh), istnieją pewne różnice

**Rysunek 7.3.**

Wyświetlenie listy  
interfejsów sieciowych  
w systemie Ubuntu  
Linux sprowadza się  
do wykonania  
polecenia `ifconfig`

```

marek@devel:~$ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:31:33:CF
          inet addr:10.254.137.11  Bcast:10.254.137.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe31:33cf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4865255  errors:0  dropped:0  overruns:0  frame:0
          TX packets:2749325  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:456278314 (435.1 MiB)  TX bytes:445785664 (425.1 MiB)
          Base address:0x2000  Memory:d8920000-d8940000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4285  errors:0  dropped:0  overruns:0  frame:0
          TX packets:4285  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:11774791 (11.2 MiB)  TX bytes:11774791 (11.2 MiB)

marek@devel:~$

```

w poszczególnych implementacjach. Dlatego chcąc zapoznać się ze szczegółowymi informacjami na ich temat, należy skorzystać ze stron MAN wymienionych systemów albo z podręcznika systemowego w przypadku systemu Windows. Na rysunku 7.4 została pokazana strona MAN polecenia `ifconfig` wyświetlona w systemie Ubuntu. Strona MAN jest kartą podręcznika systemowego zawierającą opis wskazanego polecenia.

**Rysunek 7.4.**

Strona MAN  
w systemie  
Ubuntu Linux

```

marek@devel
IFCONFIG(8)          Podręcznik programisty linuxowego          IFCONFIG(8)

NAZWA
    ifconfig - konfiguruje interfejs sieciowy

SKŁADNIA
    ifconfig [interface]
    ifconfig interface [atype] options | address ...

OPIS
    Ifconfig jest używany do konfigurowania (a później opiekowania się) rezydującymi
    w jądrze interfejsami sieciowymi. Jest używany podczas bootowania do skonfigurowania
    większości z nich do stanu pracy. Później jest zwykle potrzebny tylko
    przy debuggowaniu lub tuningowaniu systemu.

    Jeśli nie poda się argumentów, ifconfig po prostu wyświetli status aktywnych
    interfejsów. Jeśli podany jest pojedynczy argument interface, to wyświetla on
    status podanego interfejsu. Jeżeli użyto pojedynczego argumentu -a, to wyświetlony
    zostanie status wszystkich interfejsów, nawet tych, które są nieaktywne. W
    przeciwnym wypadku zakłada, że trzeba coś skonfigurować.

Rodziny Adresów
    Jeśli pierwszy argument po nazwie interfejsu jest rozpoznany jako nazwa wspieranej
    rodziny adresów, to ta rodzina adresów jest używana do dekodowania i
    wyświetlania wszystkich adresów protokołowych. Obecnie wspierane rodziny adresów
    to inet (TCP/IP, domyślne), inet6 (IPv6), ax25 (AMPR Packet Radio), ddp
    (Appletalk Phase 2), ipx (Novell IPX) i netrom (AMPR Packet radio).

:

```



Wyszukiwarki internetowe, takie jak Google, indeksują podręczniki systemowe dostępnych w sieci systemów operacyjnych, dlatego są bardzo pomocne w wyszukiwaniu informacji na temat poleceń. Na przykład wpisanie hasła `ifconfig` spowoduje wyświetlenie odsyłaczy do plików pomocy licznych dystrybucji systemu Linux. Aby uzyskać dane na temat instrukcji `ifconfig` systemu Sun Solaris, wystarczy w polu wyszukiwania wprowadzić hasło `ifconfig site:sun.com`.

Nowoczesne systemy operacyjne są wyposażone również w graficzne narzędzia zarządzania interfejsami sieciowymi. Dostępne w systemie Windows okno *Połączenia sieciowe* (prezentujące wszystkie zainstalowane interfejsy sieciowe) zostało już wcześniej przedstawione. Aby je wyświetlić, należy wybrać odpowiednią opcję w *Panelu sterowania* lub kliknąć ikonę sieci na pasku zadań. Niemal wszystkie powszechnie wykorzystywane sieciowe systemy operacyjne udostępniają pewną formę panelu sterowania, od którego można rozpocząć konfigurowanie interfejsów sieciowych.

Inna metoda konfiguracji interfejsów sieciowych polega na zastosowaniu języków skryptowych oraz interfejsów zarządzania siecią. W przypadku urządzeń obsługujących protokoły SNMP zapytania o parametry lub żądania zmian konfiguracji można kierować bezpośrednio do kart sieciowych. Podobne rozwiązanie zapewnia technologia WMI w systemie Windows. Jednak interfejsy wirtualne nie są elementami fizycznymi i nie podlegają bezpośredniemu zarządzaniu. Wirtualny interfejs sieciowy jest wytworem systemu operacyjnego i dlatego weryfikacja jego stanu musi być zainicjowana przez system. Platformy UNIX udostępniają bardzo rozbudowany interfejs wiersza poleceń (CLI — *Command-Line Interface*), przeznaczony do operowania ustawieniami systemowymi, w tym funkcjami sieciowymi. Autorzy systemu Windows przez wiele lat pracowali nad udostępnieniem równie użytecznego środowiska skryptowego, co doprowadziło do opracowania technologii Windows Scripting Host, a później do włączenia (do systemów Windows Vista i Windows Server 2008) powłoki PowerShell.

## Powiązania i dostawcy

Zbiór modułów programowych (związanych z siecią TCP/IP), które występują pomiędzy warstwą łącza danych (warstwą 2., właściwą dla kart sieciowych) a warstwą aplikacji (warstwą 7.) modelu ISO/OSI, jest nazywany *stosem sieciowym* lub *stosem TCP/IP*. Ruch przychodzący jest przekształcany w bloki danych podczas propagowania z warstwy 3. do 6. W trakcie wysyłania informacji odpowiednie formowanie danych jest realizowane w czasie przekazywania ich przez poszczególne warstwy, od 6. do 3. Szczegółowo zagadnienie to zostało omówione w rozdziale 2.

W stosie TCP/IP systemu Windows wszystkie zainstalowane komponenty sieciowe są domyślnie powiązane ze wszystkimi zainstalowanymi interfejsami sieciowymi. Oznacza to, że gdy przez stos są przekazywane różne rodzaje danych (różne formy ruchu sieciowego), wybrane mogą zostać różne ścieżki propagacji. System operacyjny przekazuje dane lub odebrany strumień do pierwszego modułu — protokołu — wymienionego na liście komponentów sieciowych. Jeżeli dany protokół nie może poprawnie obsłużyć dostarczonych informacji, są one przekazywane do kolejnego protokołu, aż do wyczerpania listy.

Kolejność użycia poszczególnych komponentów stosu sieciowego jest nazywana *kolejnością powiązań* i jest ustawieniem, które administrator może zmienić w celu zwiększenia wydajności komunikacji. Gdy system operacyjny wyznacza kolejność powiązań, nie dysponuje informacjami o protokołach preferowanych przez użytkownika. A jeśli wymagany protokół nie zostanie wcześniej zainstalowany, związana z nim forma komunikacji w ogóle nie będzie możliwa do realizacji. Rozwiązanie wydaje się oczywiste — potrzebny komponent musi zostać dodany do zestawu powiązań. Z kolei pozostawienie w zestawieniu niepotrzebnych protokołów stanowi nieuzasadnione obciążenie systemu.

Każdy interfejs przechowuje własny zbiór powiązań. Dzięki temu administrator może dodawać lub usuwać komponenty i protokoły każdego interfejsu niezależnie. Może również niezależnie zmieniać kolejność występowania poszczególnych komponentów na liście powiązań. Nie wszystkie systemy operacyjne zapewniają narzędzia do modyfikowania kolejności powiązań, ponieważ jest to uznawane za zaawansowaną operację. Jednak większość systemów przeznaczonych do stosowania w serwerach ma tę funkcję. Zmiana kolejności powiązań w systemie klienckim nie wpływa na wydajność pracy, ponieważ komputery typu desktop przez większość czasu nie korzystają z sieci. Niemniej w przypadku systemów, których niedostateczna efektywność wynika z ograniczeń w sieciowych operacjach wejścia-wyjścia, zmiana kolejności powiązań może istotnie wpłynąć na wydajność systemu, obniżając zużycie procesora i zwiększając przepustowość danych. Rozwiązanie to znajduje zastosowanie w serwerach WWW, serwerach terminali (takich jak serwerowe oprogramowanie firmy Citrix lub serwer terminali Windows), serwerach telefonii, przełącznikach i routerach klasy enterprise oraz wielu innych rodzajach serwerów.

Aby wyświetlić okno zmiany kolejności powiązań w systemach Vista lub Windows Server 2003, należy wykonać kolejne etapy poniższej procedury:

1. Kliknij ikonę *Start*, a następnie wybierz opcję *Panel sterowania/Siec i Internet*.
2. Kliknij odsyłacz *Centrum sieci i udostępniania*, a później odsyłacz *Zarządzaj połączeniami sieciowymi*.
3. Naciśnij klawisz *Alt* (tylko w systemie Vista; w systemie Windows Server 2008 nie jest konieczne), kliknij opcję *Zaawansowane*, a następnie *Ustawienia zaawansowane*.
4. Kliknij zakładkę *Karty i powiązania* i wybierz połączenie do przejrzania lub modyfikacji.
5. Kliknij pozycję na liście *Powiązania dla <nazwa połączenia>* i za pomocą przycisków strzałek w górę i w dół zmień kolejność powiązań, tak jak to zostało pokazane na rysunku 7.5.

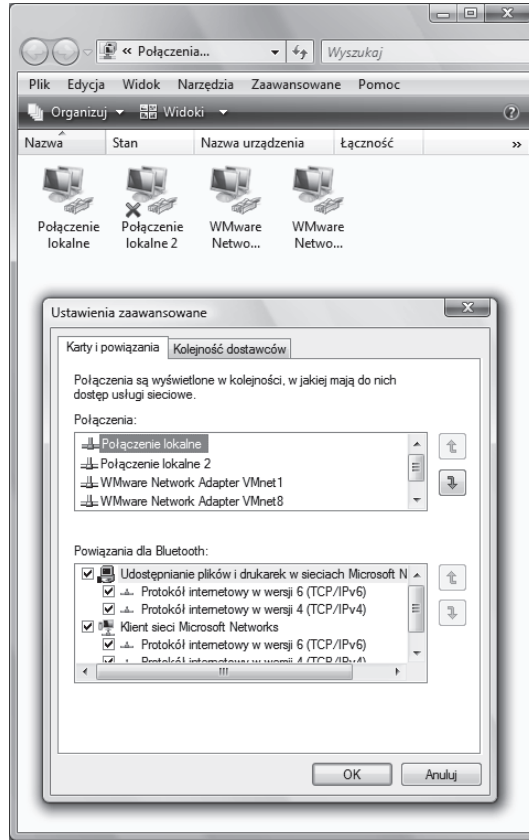
Aby zmodyfikować lub zweryfikować kolejność wykorzystania dostawców sieci, wystarczy wybrać zakładkę *Kolejność dostawców* (pokazaną na rysunku 7.6). Kolejność dostawców jest wykorzystywana przez interfejs sieciowy do wybierania pożądanej formy komunikacji z innym urządzeniem sieciowym. Zmiana priorytetów poszczególnych opcji sprowadza się do odpowiedniego użycia klawiszy strzałek w górę lub w dół.

Zmiana kolejności powiązań lub dostawców wpływa bezpośrednio na efektywność pracy interfejsu, więc koniecznie trzeba przetestować wprowadzone ustawienia.

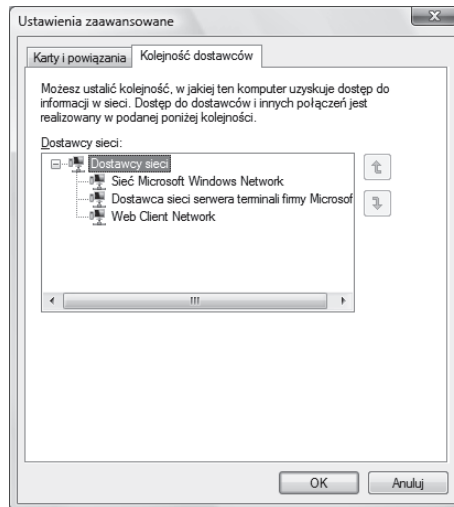
W systemie Windows termin *dostawca sieci* oznacza bibliotekę DLL, która zawiera funkcje niezbędne do ustanowienia połączenia z innym typem sieci, takim jak Novell, udostępnionym za pośrednictwem interfejsu API dostawcy sieci. Każdy dostawca jest klientem sterownika sieciowego Windows i jest odpowiedzialny za tworzenie i utrzymywanie połączeń.

Stos sieciowy nie musi być elementem systemu operacyjnego, ale taka architektura zapewnia wygodniejsze dodawanie nowych funkcji oraz łatwiejsze optymalizowanie kodu niż w przypadku zaimplementowania funkcji sieciowych w module sprzętowym. Wraz ze zmianą

**Rysunek 7.5.**  
*Kolejność powiązań  
w systemie Vista*



**Rysunek 7.6.**  
*Kolejność dostawców*



wersji systemu Windows z XP i Server 2003 na Vista i Server 2008 stos sieciowy został całkowicie przebudowany, w wyniku czego istotnie wzrosła wydajność różnych operacji sieciowych (na przykład transmisji plików z użyciem protokołu SMB).

## Izolacja i routing

Komputery ogólnego przeznaczenia, a także jednostki specjalnego przeznaczenia, realizujące pewne zadania sieciowe, często są wyposażane w dwie karty sieciowe lub większą ich liczbę.

Instalowanie większej liczby kart sieciowych jest uzasadnione wieloma względami. Z pewnością są wśród nich:

- ♦ **Zwiększona wydajność.** Dodawanie kart sieciowych zwiększa przepustowość transmisji danych.
- ♦ **Odporność na awarie.** System można skonfigurować w taki sposób, aby w przypadku awarii jednej karty sieciowej cały ruch został skierowany do interfejsu zapasowego.
- ♦ **Różne przeznaczenie.** Gdy jedna z kart sieciowych obsługuje standardową komunikację sieciową, inne interfejsy mogą służyć do zarządzania systemem, pozostawać w gotowości na wypadek awarii podstawowego lub brać udział w komunikacji, zwiększając wydajność połączenia.

Pierwsze płyty główne ze zwielokrotnionymi kartami wbudowanymi były wyposażane w jeden interfejs o wysokiej przepustowości i jeden o niskiej szybkości transmisyjnej — na przykład karty Ethernet o wydajności odpowiednio 100 Mb/s (100Base-T) i 10 Mb/s (10Base-T). W późniejszych modelach płyt głównych stosowano karty 1000Base-T (gigabitowy ethernet), uzupełniane o karty 100Base-T. Jednak wraz ze znacznym spadkiem cen ethernetowych układów scalonych powszechnie zaczęto produkować płyty główne z dwoma interfejsami o wysokiej przepustowości.

- ♦ **Routing.** Dwie karty sieciowe (lub większa ich liczba) umożliwiają definiowanie tras, którymi można zarządzać na podstawie różnych wyznaczonych przez administratora kryteriów.
- ♦ **Izolacja.** Routing wprowadza dwa kluczowe dla bezpieczeństwa komunikacji elementy — izolację fizyczną i izolację protokołów. Każde z tych zagadnień zostało krótko opisane w dalszej części rozdziału.

Wszystkie wymienione powyżej zalety są dostatecznym uzasadnieniem zakupu dodatkowego interfejsu sieciowego do każdego komputera. Funkcje sieciowe są jednymi z najczęściej wykorzystywanych komponentów systemu i niestety zawodzą częściej niż inne moduły. Im komputer jest starszy, tym bardziej prawdopodobne wydaje się, że dodanie nowego interfejsu sieciowego zwiększy wydajność komunikacji sieciowej, poprawi bezpieczeństwo, a co najważniejsze, pozwoli na skorzystanie z aktualnego sterownika urządzenia. Niezależnie od systemu operacyjnego sterownik interfejsu sieciowego ma największy wpływ na szybkość pracy, stabilność oraz zgodność urządzenia z samym systemem.

### Izolacja fizyczna

Aby jedno urządzenie sieciowe mogło odnaleźć inne urządzenie, interfejsy sieciowe obydwu urządzeń muszą należeć do tego samego zakresu adresów sieciowych, a dokładniej muszą być przyłączone do tej samej podsieci. Jeśli jeden z komputerów miałby adres IP o wartości 4.2.2.1 (co w tym przypadku oznacza adres serwera DNS firmy Verizon), a druga jednostka posługiwałaby się adresem 4.2.3.1, odszukanie drugiej z wymienionych stacji

byłoby niemożliwe. Jeśli jednak drugi system korzystałby z adresu 4.2.2.224, jego odszukanie nie stanowiłoby problemu. W tym przykładzie przyjęto założenie, że poszczególnym adresom odpowiada maska podsieci z klasy C o wartości 255.255.255.0. Takie rozwiązanie jest nazywane izolacją fizyczną i stanowi podstawę działania firewalli, bram, routerów oraz innych urządzeń zabezpieczających komunikację sieciową.

Z izolacją fizyczną miał do czynienia każdy, kto konfigurował firewall, bramę, modem kablowy lub router bezprzewodowy we własnej sieci. Urządzenia te są standardowo wyposażane w dwa interfejsy sieciowe. Jeden z nich służy do przyłączenia sieci zewnętrznej i jest ustawiany w taki sposób, aby przyjmował adres IP (dynamicznie) z usługi uruchomionej na serwerze w sieci zewnętrznej. Dynamiczne adresy w sieciach TCP/IP pochodzą z pul adresowych należących do sieci dostawcy usług internetowych. Drugi z interfejsów otrzymuje prywatny adres, ustawiony domyślnie przez producenta urządzenia. Adres ten można zmienić. Zazwyczaj pochodzi on z puli prywatnych adresów IP, które zostały zarezerwowane do użycia w sieciach wewnętrznych i nie mogą być stosowane w sieciach WAN, takich jak internet.

Na potrzeby omówienia przyjmijmy, że wewnętrznemu interfejsowi urządzenia (interfejsowi sieci LAN) przypisano adres 192.168.1.1 (właściwy dla klasy C), a komputery w istniejącej sieci LAN wykorzystują adres z przedziału od 192.168.3.1 do 192.168.3.255. Komputer administratora posługuje się adresem 192.168.3.52. Włączone do sieci urządzenie nie zostanie odnalezione ani za pomocą protokołu przeglądania sieci (na przykład NetBEUI systemu Windows), ani z użyciem protokołu HTTP. Aby uzyskać kontakt z urządzeniem, najpierw administrator musi zmienić adres karty sieciowej komputera, przypisując mu wartość z przedziału 192.168.1.x.

Po tej operacji (gdy dwie jednostki będą należały do jednej podsieci) można odszukać urządzenie i skonfigurować je w sposób opisany przez dostawcę. Urządzeniom starszego typu zazwyczaj towarzyszą specjalne narzędzia do zarządzania, umożliwiające przeprowadzenie konfiguracji. Jednak w przypadku nowszych urządzeń niemal wszystkie są wyposażone w prosty serwer WWW, który pozwala na sparаметryzowanie urządzenia za pomocą przeglądarki. Zatem kończąc przykładowe zadanie, należałoby uruchomić przeglądarkę i wpisać w polu adresu następujący ciąg:

`http://192.168.1.1`

Na ekranie powinna się wyświetlić strona logowania. Wpisanie odpowiednich danych uwierzytelniających zapewnia dostęp do ustawień interfejsu LAN urządzenia, w tym do samego adresu IP. Po zmianie adresu na 192.168.3.2 (co z reguły wiąże się z ponownym uruchomieniem) urządzenie stanie się dostępne dla pozostałych stacji w sieci. Aby było dostępne również z systemu, z którego została przeprowadzona konfiguracja, trzeba w tym systemie przywrócić adres 192.168.3.52 (zastępując wartość 192.168.1.x).



Domyślna nazwa użytkownika, hasło oraz standardowy adres interfejsu LAN urządzenia zapewniającego fizyczną izolację powinny zostać zmienione możliwie szybko, ponieważ są one doskonale znane hakerom, którzy chcieliby uzyskać dostęp do sieci.

Fizyczna izolacja jest możliwa dzięki temu, że jednostki sieci zewnętrznej mogą dostarczyć ruch tylko na adres zewnętrznego interfejsu urządzenia separującego. Adres komputera sieci wewnętrznej nie jest znany systemom zewnętrznym wysyłającym strumień danych. Oczywiście w urządzeniu odpowiedzialnym za routing musi istnieć mechanizm, który wskaże

adres jednostki wewnętrznej. Ten mechanizm jest implementowany w routerze na bazie tablicy translacji adresów sieciowych (NAT — *Network Address Translation*) lub w systemie przekazywania pakietów, który jest elementem serwera pośredniczącego. Serwer pośredniczący (serwer proxy) jest jednostką, która odbiera ruch z urządzeń zewnętrznych, przetwarza go w określony sposób (filtruje, buforuje, pozbawia cech identyfikujących użytkownika itp.), a następnie przekazuje do innego systemu. Przykładem takiego rozwiązania może być serwer firmy Microsoft Internet Security and Acceleration Server (ISA Server).

## Izolacja protokołów

Izolacja protokołów polega na wykorzystaniu jednego protokołu w sieci zewnętrznej i innego w komunikacji w ramach sieci wewnętrznej. W rozwiązaniach bazujących na protokołach TCP/IP pakiety podlegają routinngowi — użytkownik zewnętrzny, który ma czas i odpowiednie zasoby, może ominąć wdrożone systemy zabezpieczające. Izolacja protokołów wprowadza jeszcze jeden poziom złożoności do takiej operacji. Jeśli w sieci wewnętrznej jest stosowany inny protokół sieciowy, taki jak NetBEUI firmy Microsoft lub IPX/SPX firmy Novell, to dostęp do współdzielonych zasobów (na przykład do udziałów plikowych) wymaga formatowania danych zgodnie z zasadami tych protokołów. Ponieważ obydwa wymienione protokoły nie podlegają routinngowi, komunikacja nie może być inicjowana w sieci zewnętrznej.

Izolacja protokołów okazuje się pomocna w zabezpieczeniu danych przekazywanych przez sieć, ale nie stanowi dodatkowej bariery przed włamaniami z sieci zewnętrznej. Jeśli nie zostaną wprowadzone dodatkowe mechanizmy blokowania ruchu TCP/IP, systemy pracujące w wewnętrznej sieci LAN będą dostępne dla innych systemów. Jednak dzięki temu, że nie współdzielą żadnych zasobów w ramach protokołów TCP/IP, systemy zewnętrzne nie będą mogły skorzystać z żadnego z zasobów. Izolacja protokołów jest doskonałym rozwiązaniem dla urządzeń, które nie wymagają protokołów TCP/IP do komunikacji.

## Magistrale komunikacyjne kart sieciowych

Interfejsy sieciowe są dostarczane w różnych odmianach i znajdują zastosowanie w różnych rodzajach sieci. Jednym z wyróżników interfejsów sieciowych jest sposób umiejscowienia układów logicznych. Układy te można znaleźć w:

- ♦ kontrolerach sieciowych zintegrowanych z płytą główną;
- ♦ kartach rozszerzeń przyłączonych za pośrednictwem magistrali komunikacyjnej;
- ♦ przewodowych magistralach, takich jak USB;
- ♦ technologiach bezprzewodowych, takich jak 802.11x lub Bluetooth.

Oczywiście produkcja kart sieciowych nadąża za bieżącymi technologiami. Pierwsze karty rozszerzeń przeznaczone dla komputerów PC były przystosowane do współpracy z magistralami ISA. Natomiast najpowszechniej obecnie stosowane interfejsy sieciowe są wykonane w formie kart PCI.

Wysoko wydajne karty sieciowe wymagają dostępności magistral o szczególnej efektywności działania. Obecnie takimi rozwiązaniami są interfejsy PCI-X. W sprzedaży są więc dostępne karty sieciowe przeznaczone do przyłączania do magistrali PCI-X, obejmujące

jednokanałowe interfejsy Ethernet i mieszczące się w niewielkich złączach 1 x PCI-X, umieszczonych na płycie głównej. Cena pojedynczej karty ethernetowej zawiera się w przedziale od 50 zł do 300 zł. Ponieważ nie zapewniają szczególnie istotnego zwiększenia wydajności, są traktowane jako zwykłe zamienniki karty poprzedniej generacji (PCI). Karty PCI-X są zgodne ze starszymi magistralami PCI dzięki zachowaniu zgodności poziomów napięć. Starsze karty PCI były urządzeniami zasilanymi napięciem 5 V. Jednak ostatnia poprawka do standardu PCI (poprawka 3.0) definiuje zasilanie o napięciu 3,3 V. Ponieważ karty PCI-X również są zasilane napięciem 3,3 V, mogą być przyłączane do magistrali PCI. Analogicznie karty PCI można umieszczać w złączach PCI-X, ale pod warunkiem, że karta jest przystosowana do zasilania właściwego dla standardu PCI-X i jej złącze pasuje fizycznie do złącza magistrali.

Magistrala PCI-X jest dwa razy szersza niż PCI i pracuje z czterokrotnie wyższą częstotliwością taktowania, ale wykorzystuje ten sam protokół komunikacyjny oraz parametry elektryczne sygnałów. Teoretyczna przepustowość pojedynczego złącza PCI-X (1x) wynosi 1,06 GB/s — przepustowość magistrali PCI to 532 MB/s. Szybkość komunikacji w ramach magistrali PCI lub PCI-X jest limitowana przez wydajność najwolniejszej karty. Dlatego w celu zwiększenia wydajności systemu nowoczesne płyty główne separują złącza PCI-X, wydzielając niezależne kanały komunikacyjne.

W standardzie PCI-X zdefiniowano wiele ciekawych funkcji dodatkowych, w tym możliwość restartowania urządzenia, wymiany w czasie pracy oraz skalowania. Wymiana w czasie pracy (rozwiązanie typu *hot swap*) jest szczególnie użyteczna w przypadku serwerów, które muszą być ciągle aktywne. Złącza PCI-X są dostępne w wersjach czterokanałowych (4x) oraz szesnastokanałowych (16x) o teoretycznej przepustowości 4,2 GB/s i 17 GB/s. Dlatego serwerowe wieloportowe karty sieciowe oraz interfejsy pracujące zgodnie z bardziej zaawansowanymi standardami (takimi jak InfiniBand lub iSCSI), wymagającymi dużych przepustowości, są dostarczane w wersjach 4x i 16x.

Powszechnie stosowane karty rozszerzeń notebooków były nazywane kartami PCMCIA, jednak obecnie określa się je mianem kart PC. Pierwotny akronim pochodził od słów Personal Computer Memory Card International Association, czyli od nazwy międzynarodowego stowarzyszenia producentów kart pamięci dla komputerów osobistych. Obecnie obowiązującą wersją standardu PCMCIA jest wersja 2.0.

Standard kart PC jako taki nie jest standardem magistrali — jest definicją opakowania. Początkowo karty PC były przeznaczone do rozszerzania pamięci systemu. Później stopniowo wprowadzano modemy wykonane w tej technologii, a nawet twarde dyski. Jednak najczęstszym sposobem ich wykorzystania okazało się dodawanie do notebooków dodatkowych interfejsów sieciowych. W użyciu są cztery standardy — typ I, II, III i IV — które różnią się przede wszystkim grubością obudowy karty. Typ II definiuje rozmiar charakterystyczny dla kart sieciowych, czyli grubość między 5 a 5,5 mm. Karty tego typu udostępniają 16-bitowe i 32-bitowe interfejsy komunikacyjne i są zasilane napięciem 3,3 V. Przyłącze do sieci Ethernet ma formę złącza RJ45.

Inny sposób przyłączenia karty sieciowej do istniejącej magistrali komputera polega na wykorzystaniu portu USB. Zarówno karty przewodowe, jak i bezprzewodowe są na tyle rozpowszechnionymi i wartościowymi urządzeniami, że warto jest mieć je zawsze pod ręką. Jeśli funkcje sieciowe komputera przestaną poprawnie działać, wystarczy włączyć urządzenie do wolnego portu USB i sprawdzić, czy zostanie ustanowione nowe połączenie.

### Magistrala PCI-X a magistrala PCI Express (PCI-E)

Magistrala PCI-X to nie to samo co magistrala PCI Express (PCI-E lub PCIe) — z uwagi na podobieństwo nazw często obydwa rozwiązania są ze sobą mylone. Magistrala PCI-E jest magistralą pracującą w pełnym duplexie, wykorzystywaną we współpracy z urządzeniami zewnętrznymi, wymagającymi dużej przepustowości, takimi jak macierze dyskowe (RAID). Standard PCI-X odnosi się do magistral równoległych, zapewniających dwukierunkową, półdupleksową komunikację. W urządzeniach półdupleksowych połowa kanałów musi obsługiwać transmisję przychodzącą, a połowa transmisję wychodzącą. W pełni duplexowe dwukierunkowe urządzenie może realizować komunikację w ramach dowolnej liczby kanałów przychodzących lub wychodzących.

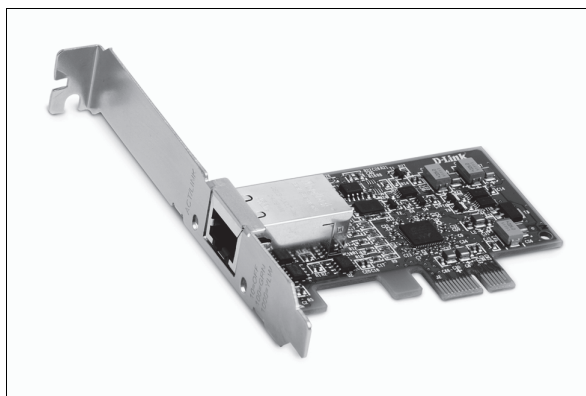
Różnice występują również w parametrach elektrycznych oraz w częstotliwości taktowania sygnałów. Standard PCI-E 1.0 x1 definiuje 32 linie danych o przepustowości po 250 MB/s w każdym kierunku, co pozwala na uzyskanie łącznej przepustowości 16 GB/s, po 8 GB/s w kierunku przychodzącym i wychodzącym. Architektura szeregową ułatwia zarządzanie kartami PCI-E i umożliwia niezależne negocjowanie przepustowości w ramach każdej linii danych. W rozwiązaniu PCI-X przepustowość jest natomiast ograniczana do najwolniejszego urządzenia.

## Przykładowa karta sieciowa

Analiza przedstawionej na rysunku 7.7 gigabitowej karty sieciowej D-Link DGE-560T PCI-X pozwala na wyróżnienie pewnych cech typowych dla wszystkich interfejsów tego typu. Prezentowane urządzenie wykorzystuje złącze PCI-X 1x i umożliwia przekazywanie ruchu ethernetowego z przepustowością do 2 Gb/s w ramach 16-bitowej lub 32-bitowej magistrali. Przepustowość o wartości 2 Gb/s odpowiada szybkości 0,25 GB/s, czyli 250 MB/s. Karta współdziała z wieloma rozwiązaniami z zakresu zarządzania, w tym z protokołem SNMP, mechanizmami rozruchu sieciowego PXE i RPL, systemem zaawansowanego zarządzania energią oraz techniką włączania komputera przez sieć (Wake-On LAN). Ponadto można ją wymieniać w czasie pracy systemu.

### Rysunek 7.7.

Karta sieciowa D-Link  
DGE-560T PCI-X



Fotografia z archiwum firmy D-Link, Inc.

Największy widoczny (czarny) układ scalony to kontroler sieciowy. Prezentowana karta jest zgodna ze standardami 10Base-T, 100Base-T oraz 1000Base-T i jak większość urządzeń przystosowanych do pracy z różnymi szybkościami transmisyjnymi zawiera diody świecące, informujące o bieżącym trybie pracy. Dioda umieszczona poniżej złącza RJ45 jest wyłączona, gdy karta wykryje połączenie 10Base-T. Z kolei po wykryciu połączenia 100Base-T

przyjmuje kolor zielony, a gdy komunikacja odbywa się w standardzie 1000Base-T — żółty. W wielu kartach to samo zadanie realizują dwie lub trzy diody. Ten interfejs jest dostarczany z ciekawym narzędziem, które pozwala na wykrycie problemu z kablem przyłączonym do gniazda karty.

System operacyjny Windows może wyświetlać ikonę informującą o aktywności interfejsu sieciowego na pasku zadań. W systemie Vista włączenie opcji polega na zaznaczeniu odpowiedniej pozycji na karcie *Obszar powiadomień* w ramach okna *Właściwości paska zadań i menu Start*. W systemie XP opcję tę należy uaktywnić niezależnie dla każdego interfejsu w oknie właściwości danego interfejsu. Ikona pełni te same funkcje co diody świecące na karcie sieciowej. Jak nietrudno zauważyć na rysunku 7.8, ikona składa się z dwóch symboli komputerów.

### Rysunek 7.8.

*Ikona karty sieciowej  
na pasku zadań  
systemu Windows*



Komputer widoczny na pierwszym planie reprezentuje jednostkę lokalną. Gdy jest podświetlony, interfejs sieciowy odbiera dane. Komputer w tle odpowiada jednostce zdalnej. Jest on podświetlany w chwili, gdy komputer lokalny wysyła informacje do zdalnego. Obserwacja zmian stanu ikony jest więc dobrym sposobem na szybką analizę pracy interfejsu sieciowego. W innych systemach operacyjnych są dostępne podobne narzędzia, w tym również aplikacje *Monitora zasobów*, które z bardzo dużą dokładnością monitorują liczbę sieciowych operacji wejścia-wyjścia.

## Sterowniki sieciowe

Opisywane interfejsy sieciowe mogą realizować swoje zadania, ponieważ każda karta zawiera układ kontrolera sieciowego, który współdziała z określoną magistralą systemową. Karty sieciowe pochodzą od różnych dostawców i przybierają różne formy, ale wykorzystuje się w nich niewielką liczbę różnych kontrolerów. Oprogramowanie niezbędne do komunikacji z poszczególnymi układami logicznymi i sterownikami sieciowymi jest często zawarte w samej dystrybucji systemu operacyjnego. Jeśli w danym systemie operacyjnym jest włączona opcja automatycznej konfiguracji urządzeń, a system wykryje określony kontroler, odpowiedni sterownik zostanie załadowany automatycznie. Doskonałym przykładem systemu automatycznej konfiguracji jest rozwiązanie Windows Plug and Play (PnP).

W przeciwieństwie do kart graficznych, których sterowniki są często zmieniane, sterowniki sieciowe przeznaczone dla określonego systemu operacyjnego nie podlegają szczególnie istotnym modyfikacjom. Nie jest czymś niezwykłym, że sterownik sieciowy, który współdziałał ze starszą wersją systemu operacyjnego (na przykład z systemem Windows Server 2003), będzie poprawnie realizował swoje zadania w nowszym systemie (na przykład Windows Server 2008). Oczywiście zalecanym sposobem postępowania jest instalowanie zawsze najnowszych wersji sterowników. Najnowsza wersja oprogramowania jest zazwyczaj udostępniana przez producenta karty (a w przypadku interfejsów osadzanych na płycie głównej — przez producenta płyty głównej) na stronie internetowej firmy.

Nie należy zakładać, że dysk z oprogramowaniem dostarczony wraz z kartą lub systemem operacyjnym zawiera najnowszą wersję sterownika. Różnice w sposobie działania wcześniejszych wersji i bieżącego wydania oprogramowania często są nieznaczne, ale niekiedy bywają istotne. Może się okazać, że najnowsza wersja zagwarantuje wyższą wydajność działania, zmniejszy stopę błędów lub zapewni zgodność z innymi rozwiązaniami. Oczywiście nie zawsze się tak zdarza, a niekiedy nawet nowsze sterowniki pogarszają działanie interfejsu. Jednak w większości przypadków dostawcy sprzętu dbają o okresowe udoskonalanie oprogramowania.

Nowoczesne systemy operacyjne wykorzystują do komunikacji z kartami sieciowymi standardowe interfejsy programistyczne (API). Interfejs API dostępny w systemach firmy Microsoft jest określany jako specyfikacja interfejsu sterownika sieciowego (NDIS — *Network Driver Interface Specification*). Został on opracowany wspólnie przez firmy Microsoft i 3Com w czasie, gdy firma 3Com dominowała na rynku interfejsów ethernetowych. Interfejs NDIS jest w zasadzie elementem podwarstwy sterowania łączem logicznym (LLC — *Logical Link Control*), zawartym w warstwie 2. modelu OSI/ISO. Stanowi element pośredni między tą warstwą a warstwą sieciową (warstwą 3.). Poniżej podwarstwy LLC znajduje się podwarstwa sterowania dostępem do medium (MAC — *Media Access Control*) oraz sterownik urządzenia stanowiący element warstwy 1. (warstwy fizycznej). Interfejs NDIS to niskopoziomowy mechanizm przekazywania danych sieciowych, generowania i usuwania informacji adresowych oraz formowania ramek transmisyjnych.

Niektóre dystrybucje systemu Linux zawierają oprogramowanie umożliwiające wykorzystanie kart zgodnych z interfejsem NDIS. Niemniej większość systemów używa własnych standardów API do komunikowania się z kartami sieciowymi. W systemach Macintosh jako oprogramowanie podwarstwy LLC firma Apple stosuje interfejs ODI, który został opracowany wraz z firmą Novel. Rozwiązanie ODI jest podobne do NDIS, gdyż zapewnia obsługę kart sieciowych różnych producentów.

Dostępne są również inne odmiany oprogramowania sterowników sieciowych, w tym ujednolicony interfejs sterownika (UDI — *Uniform Driver Interface*). Projekt UDI ma za zadanie doprowadzić do powstania standardu przenośnego interfejsu sterowników sieciowych. Jest dostępny w kilku dystrybucjach systemów Linux i UNIX. Kolejną odmianą jest specyfikacja API uniwersalnego interfejsu urządzenia sieciowego (UNDI — *Universal Network Device Interface*) implementowana w kontrolerach zintegrowanych z płytami głównymi firm takich jak Intel. Zastosowanie tego rozwiązania umożliwia karcie sieciowej współdziałanie z protokołem PXE i BIOS-em komputera. Mechanizm PXE dzięki niewielkiemu i niezależnemu systemowi operacyjnemu umożliwia administratorowi zdalne zarządzanie systemami, instalowanie nowych systemów operacyjnych oraz realizację zadań związanych z utrzymaniem systemu.

## Podsumowanie

Interfejs sieciowy jest elementem systemu operacyjnego; można go konfigurować za pomocą odpowiedniego oprogramowania. Każdy interfejs sieciowy ma pewien zbiór właściwości, który wyróżnia go spośród innych obiektów tego typu. Do wspomnianych właściwości z pewnością trzeba zaliczyć niepowtarzalny adres fizyczny, nazywany adresem MAC, który jest definiowany przez producenta karty lub kontrolera. Przypisywane do interfejsu adresy logiczne są właściwie tylko dla sieci, w której dana karta pracuje (na przykład dla sieci TCP/IP).

Interfejsy sieciowe mogą być urządzeniami fizycznymi lub logicznymi. Logiczny interfejs sieciowy jest tworzony przez system operacyjny jako karta sieciowa maszyny wirtualnej, jako element oprogramowania odpowiedzialnego za przekierowywanie ruchu sieciowego lub innego z wielu możliwych rozwiązań. Konfiguracja interfejsu logicznego nie odbiega w żaden sposób od ustawień innych interfejsów sieciowych, ale jego działanie wymaga dostępności interfejsu fizycznego, który generuje i odbiera ruch sieciowy.

Zakres zastosowań oraz wydajność interfejsów sieciowych są determinowane przez listę komponentów sieciowych skojarzonych z danym interfejsem. Lista ta jest przedstawiana jako zestawienie kolejności powiązań. Z kolei wykaz rodzajów sieci, z którymi dany interfejs może współpracować, jest prezentowany jako lista kolejności dostawców. Porządek elementów na każdej z list decyduje o sposobie przetwarzania danych odbieranych przez interfejs i wysyłanych z interfejsu — wyznacza zasady przekazywania danych w ramach stosu sieciowego. Obydwie listy można modyfikować.

Gdy komputer zostanie wyposażony w dwie karty sieciowe lub większą ich liczbę, możliwe staje się przypisanie mu większej liczby adresów sieciowych, a to z kolei pozwala na fizyczną izolację sieci. Jeśli poszczególne interfejsy sieciowe pracują pod kontrolą różnych protokołów lub z użyciem różnych dostawców sieciowych, system może izolować jedną kartę od innych zgodnie z zasadą izolowania protokołów.

W kolejnym rozdziale zostały omówione rodzaje mediów transmisyjnych, wykorzystywanych do budowania sieci, w tym kable, połączenia bezprzewodowe itp.



# Rozdział 8.

## Media transmisyjne

### W tym rozdziale:

- ♦ Standardy okablowania
- ♦ Skrętki, kable współosiowe (koncentryczne) i włókna światłowodowe
- ♦ Okablowanie w sieciach Ethernet
- ♦ Propagacja światła we włóknach światłowodowych
- ♦ Połączenia bezprzewodowe

Tematyka tego rozdziału obejmuje trzy rodzaje mediów transmisyjnych, występujących w warstwie fizycznej modelu sieci — kable przeznaczone do przekazywania sygnałów elektrycznych, włókna światłowodowe, przenoszące impulsy świetlne, oraz łącza bezprzewodowe, działające na częstotliwościach radiowych i mikrofalowych.

Wykorzystanie różnych rodzajów okablowania wymaga stosowania różnych technik układania przewodów, łączenia urządzeń oraz rozmieszczania poszczególnych komponentów. Dlatego w dalszej części rozdziału zostały zamieszczone informacje na temat instalowania sieci wewnątrz budynków.

## Media kablowe

Większość osób nie przykładą należytej wagi do warstwy fizycznej budowanych sieci. Biorąc pod uwagę fakt, że wykonane okablowanie będzie służyło przez 10 do 15 lat, warto poświęcić chwilę na zastanowienie się, który ze standardów będzie najkorzystniejszy, nie tylko w bieżącej sytuacji, ale również w przyszłości.

Oto cztery rodzaje połączeń kablowych:

- ♦ **Skrętka ekranowana** — miedziany, ekranowany kabel o skręconych parach przewodów. Ten rodzaj okablowania występuje w sieciach lokalnych, szczególnie w starszych instalacjach.
- ♦ **Kabel współosiowy (koncentryczny)** — gruby dwuprzewodowy kabel koncentryczny, który zapewnia szerokie pasmo transmisyjne oraz dużą dostępność połączeń.

- ♦ **Skłętka nieekranowana** — miedziany, nieekranowany kabel o skręconych parach przewodów. Skłętka nieekranowana (UTP — *Unshielded Twisted Pair*) jest powszechnie stosowanym kablem w sieciach Ethernet.
- ♦ **Włókno optyczne** — szklane lub plastikowe włókno optyczne. Kable optyczne są podstawą działania sieci o wysokiej przepustowości.

Każdy z wymienionych kabli zapewnia inną szybkość transmisji danych, inną szerokość pasma oraz narzuca różne topologie sieciowe i połączenia fizyczne. W dalszej części rozdziału szczegółowo zostały opisane zastosowania poszczególnych rodzajów okablowania.



Fizyczne podstawy transmisji sygnałów są tematem rozdziału 5.

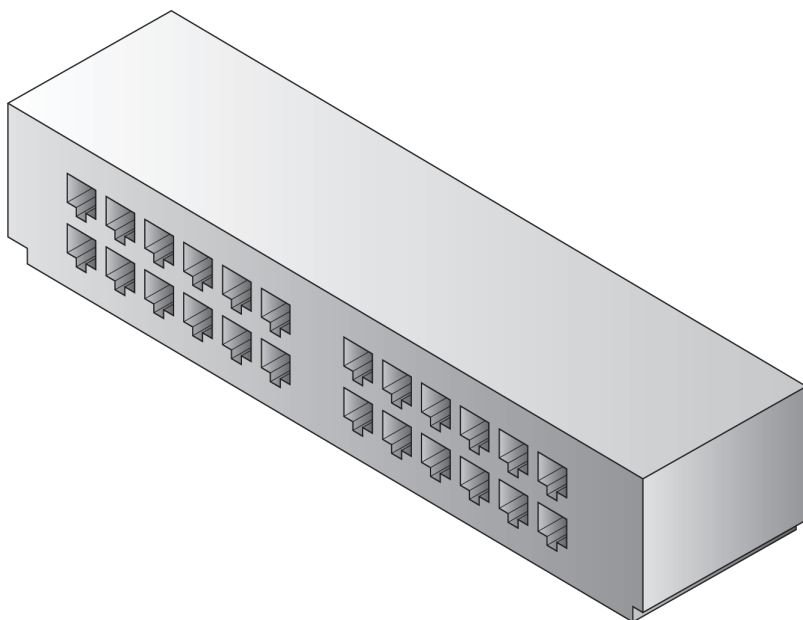
## Przygotowanie okablowania

Ułożenie kabli musi zostać poprzedzone pewnymi czynnościami przygotowawczymi, szczególnie jeśli dotyczy to większej liczby segmentów, rozciągających się na obszarze kilku pokoi, pięter lub budynków. W wielu organizacjach przestrzegane są pewne zasady (takie jak obowiązek wykorzystania kanałów kablowych), w tym również standardy, które muszą być przestrzegane. Dlatego często za ułożenie kabli sieciowych odpowiada uprawniony do tego elektryk. Same kable muszą być izolowane i powinny być ułożone w sposób umożliwiający łatwą rozbudowę sieci w późniejszym czasie.

W wielu sieciach kable doprowadza się do elementów nazywanych *panelami krosowymi* (ang. *patch panel*) lub do zespołów paneli krosowych nazywanych węzłami dystrybucyjnymi (ang. *wiring closet*). Panele krosowe umożliwią szybką zmianę połączenia podczas przenoszenia systemów lub gdy konieczna jest zmiana rodzaju połączenia. Przykład panelu krosowego został pokazany na rysunku 8.1. Zgodnie z zaleceniami dotyczącymi projektowania okablowania warto opracować schemat oznaczania łączy na podstawie kolorów, co ułatwia później rozróżnianie poszczególnych rodzajów przyłączy. W celu zwiększenia przejrzystości połączeń administratorzy dodatkowo oznaczają kable numerami i przygotowują zestawienia przyłączy w formie arkusza kalkulacyjnego programu Excel. Grupy kabli wprowadzanych do szaf typu rack lub do serwerowni są powiązane ze sobą w wiązki, ułatwiające określenie tego, dokąd wiodą poszczególne połączenia. Przemyślana organizacja kabli pozwala na zaoszczędzenie znacznej ilości czasu i na zmniejszenie frustracji w przypadku późniejszego rozwiązywania problemów z siecią.

Przepisy budowlane wymagają niekiedy otoczenia kabli materiałem izolującym. Izolatorami są najczęściej elementy wykonane z teflonu (PTFE), polichlorku winylu (PVC) lub polietylen (PE). Teflon jest najdroższym z wymienionych materiałów, ale zapewnia ochronę przed ogniem. Polichlorek winylu jest tańszy, ale płonie, wydzielając toksyczny gaz. Polietylen również nie jest ogniotrwały, ale wydzielane przez niego spaliny nie są szkodliwe.

Kable narażone na zginanie, deptanie, rozciąganie lub ściskanie mogą ulegać uszkodzeniu. Uszkodzenia tego typu są jednak najmniej uciążliwym problemem, ponieważ można je w relatywnie łatwy sposób zlokalizować, a następnie usunąć przez wymianę wadliwego odcinka. Znacznie poważniejsze okazują się awarie, w których kabel przestaje spełniać swoją funkcję w nieregularnych odstępach czasu. Losowość występowania problemu sprawia, że

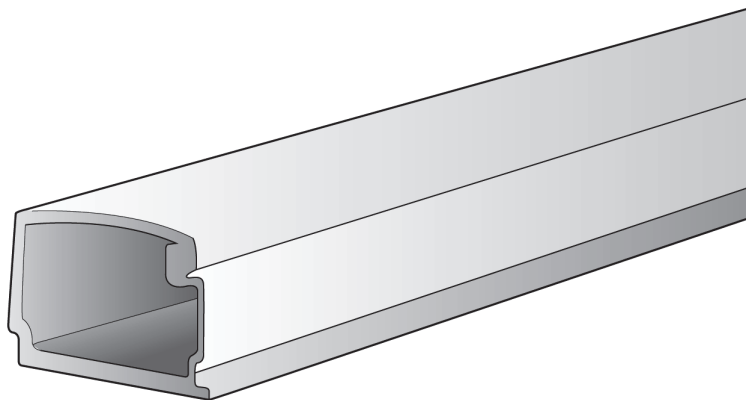
**Rysunek 8.1.***Panel krosowy*

znacznie trudniejsze jest jego zlokalizowanie i ustalenie przyczyn występowania. Nie wiadomo, czy przyczyną jest uszkodzenie sprzętowe, czy programowe, błędne ustawienie parametrów połączenia, wadliwy port przełącznika lub routera itd. Losowość problemu sprawia, że czas poświęcony na jego rozwiązanie rośnie wykładniczo. Niekiedy nawet przyczyna pozostaje nieustalona i trzeba się pogodzić z występowaniem problemu. Lepiej więc zapobiegać, niż leczyć.

Istnieje wiele sposobów przygotowania okablowania zgodnie z obowiązującymi zasadami i bez naruszania reguł bezpieczeństwa. Jeśli w pokojach są podwieszane sufity, doskonałą metodą wydaje się ułożenie kabli (przywiązanych do stelażu konstrukcji) ponad nimi. Ten sam rezultat można uzyskać, zawieszając pod sufitem specjalne koryta kablowe. Z kolei kable układane w podłodze są prowadzone wewnątrz specjalnych kanałów kablowych. W pomieszczeniach komputerowych często budowane są podłogi techniczne (podniesione podłogi), które pozwalają na rozłożenie instalacji podobnie jak w przypadku podwieszanych sufitów. Na rysunku 8.2 przedstawiony został przykład dwuelementowego kanału kablowego. Kable są mocowane do dolnej części kanału, natomiast górny element stanowi jego zabezpieczenie. Rozwiązaniem alternatywnym jest stosowanie otwartych koryt (podwieszanych do sufitu), przytwierdzanie kabli do ścian lub sufitów bądź prowadzenie ich w podłodze.

Dobrym rozwiązaniem jest również układanie kabli sieciowych w duktach i szybach budynkowych. Trzeba jednak pamiętać, aby razem z kablami sieciowymi nie były w nich umieszczane kable energetyczne. Linie zasilające zakłócają bowiem sygnały komputerowe transmitowane w miedzianych przewodach — wysokie napięcie powoduje obniżenie poziomu sygnału, a w niektórych przypadkach może nawet doprowadzić do uszkodzenia urządzeń przyłączonych do kabla sieciowego. Występuje tutaj efekt dynama. Przepływający prąd elektryczny wytwarza zmienne pole magnetyczne, które następnie indukuje prąd w przewodniku umieszczonym w takim polu.

**Rysunek 8.2.**  
Zamknięty kanał  
kablowy



Źródłem zakłóceń elektromagnetycznych (EMI — *Electromagnetic Interference*) są przede wszystkim silniki elektryczne, lampy jarzeniowe, pompy, urządzenia chłodnicze itp. Podobnie urządzenia takie jak routery bezprzewodowe, kuchenki mikrofalowe czy telefony bezprzewodowe stanowią źródła zakłóceń radiowych (RFI — *Radio Frequency Interference*). Zakłócenia te również przyczyniają się do obniżenia jakości sygnału w kablach sieciowych. Z tego względu sieć komputerową należy układać z dala od źródeł zakłóceń lub w sposób gwarantujący odpowiednie ekranowanie. Zagadnienie to jest szczególnie istotne w przypadku długich odcinków połączeniowych, gdyż siła sygnału obniża się wraz z pokonywaną odległością.

## Skretka

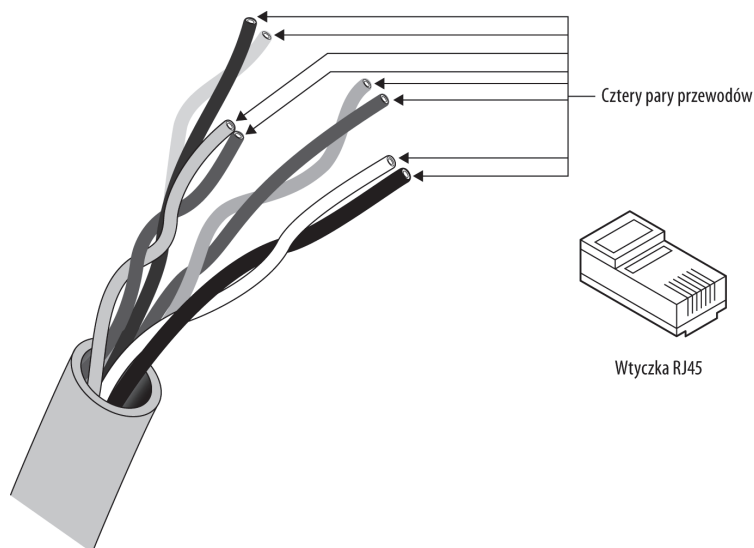
Skretka jest obecnie najczęściej stosowanym rodzajem kabla sieciowego (szczególnie skretka nieekranowana). Wykorzystuje się ją do przesyłania sygnałów analogowych i cyfrowych. Posłużyła nawet do przeprowadzenia pierwszej rozmowy telefonicznej, wykonanej przez Aleksandra Grahama Bella. W obecnych systemach telefonii analogowej stosowane są dwie pary skretki, z których jedna pozostaje niewykorzystana. Niewykorzystana para okazuje się pomocna w przypadku instalowania łączy DSL, ISDN lub połączeń sieciowych w ramach linii telefonicznej biura lub domu.

Popularność skretki wynika z niewielkiego kosztu jej produkcji przy jednoczesnym zapewnieniu izolacji i ekranowania przewodów. Skręcenie przewodów w kablu pozwala na ograniczenie wpływu zewnętrznych zakłóceń elektromagnetycznych na transmisję danych w wyniku uśrednienia ich na kilka przewodów oraz obniża negatywne skutki przesłuchów, czyli wewnętrznych zakłóceń między transmitowanymi sygnałami. Skretka ma również wiele zalet kabla współosiowego. Na rysunku 8.3 został pokazany kabel UTP (skretka bez ekranowania) wraz z wtyczką RJ-45, która umożliwia przyłączenie kabla do odpowiedniego gniazda.

W latach 80. ubiegłego stulecia firma IBM wprowadziła na rynek skretkę ekranowaną (STP — *Shielded Twisted Pair*), która do dzisiaj jest stosowana w sieciach token ring. Ta forma okablowania nigdy nie była tak powszechnie stosowana jak połączenia UTP, co wynikało prawdopodobnie ze zwiększonego kosztu produkcji kabla oraz z trudności w wykonywaniu połączeń.

**Rysunek 8.3.**

*Skръtka  
nieekranowana  
i wtyczka RJ-45*



W kablu STP przewody są grupowane w pary, a każda z tych par jest otoczona ekranem. Ekran stanowi metalowa folia lub opłot z siatki drucianej. Ekran musi zostać uziemiony z jednej strony kabla. W przypadku zastosowania folii metalowej kabel niekiedy opisuje się akronimem FTP, pochodzącym od angielskiej nazwy foliowanej skръtki (ang. *foil twisted pair*).

Choć skръcenie przewodów zapobiega przesłuchom na trasie sygnału, użycie kabla STP nie chroni przed przesłuchami i zakłóceniami EMI na końcach połączenia kablowego. Odporność na przesłuchy, a tym samym zapobieganie błędom transmisyjnym jest tym większe, im więcej jest skръceń przewodów na jednostkę długości. Współczynnik liczby skръceń na metr jest parametrem różnym dla poszczególnych par kabla, co również zapobiega zniekształceniom sygnału.



Do opisu przesłuchów służą parametry przesłuchu zbliżnego (NEXT — *Near End Crosstalk*) oraz przesłuchu zdalnego (FEXT — *Far End Crosstalk*). Wartość NEXT odpowiada interferencjom wnoszonym przez jedną parę do przewodów drugiej pary, mierzonym na tym samym końcu kabla. Natomiast parametr FEXT odzwierciedla poziom zakłóceń między dwoma parami, który jest mierzony na dwóch różnych końcach kabla.

W większości sieci stosowane są kable UTP. Składają się one z kilku par miedzianych przewodów — skръconych, ale nieizolowanych. Typowym zastosowaniem kabli UTP są sieci Ethernet oraz linie telefoniczne. W przypadku zastosowania skръtki UTP w połączeniach E1 konieczne jest regenerowanie sygnału co 1,8 km.

Kable UTP zostały podzielone na kategorie, opisane standardami EIA/TIA (organizacji Electronic Industries Alliance i Telecommunications Industry Association). Najpowszechniej stosowaną kategorią w dzisiejszych sieciach komputerowych jest kategoria 5e (CAT 5e), która została wprowadzona w 1988 roku. Kable CAT 1 są wykorzystywane w telefonii, a CAT 3 w starszych sieciach komputerowych. Przewody kabla UTP są oznaczone kolorami o standardowych barwach. Większość produkowanych kabli jest zgodna z zaleceniem Underwriters Laboratories (UL) i ma na izolacji nadrukowaną informację o kategorii skръtki. Do przyłączania kabli UTP służą wtyczki RJ-45, które przypominają wyglądem standardowe wtyczki telefoniczne, ale są rozszerzone o dodatkowe styki.

Kilka najpopularniejszych rodzajów skrętki (zarówno UTP, jak i STP) zostało wymienionych w tabeli 8.1. Zestawienie to nie obejmuje jednak wszystkich wariantów, między innymi brakuje w nim okablowania stosowanego w połączeniach szkieletowych. Wiele połączeń szkieletowych UTP jest pewną kombinacją kabli 25-parowych.

**Tabela 8.1.** *Skrętki*

Kategoria	Maksymalna szybkość transmisji danych	Liczba par przewodów	Zastosowanie
CAT 1 (UTP)	< 1 Mb/s	2	Dane analogowe, telefonia analogowa i ISDN
Typ 1 (STP)		2	Sieci token ring
CAT 2 (UTP)	4 Mb/s	2	Sieci token ring
Typ 2 (STP)		4	Głos i dane
CAT 3 (UTP, STP)	10 Mb/s	4	Głos i dane, Ethernet 10Base-T, telefonia
CAT 4 (UTP, STP)	16 Mb/s	4	Sieci token ring
CAT 5 (UTP, STP)	1 Gb/s	4	Ethernet 10Base-T, 100Base-T, Ethernet gigabitowy, ATM, CDDI (TP-DDI)
CAT 5e (UTP, STP)	1 Gb/s	4	Sieci ATM, CDDI (TP-DDI)
CAT 6 (UTP, STP)	10 Gb/s	4	10-gigabitowy Ethernet
CAT 6e (UTP, STP)	10 Gb/s	4	10-gigabitowy Ethernet
Typ 6 (STP)		2	Sieci token ring
CAT 7 (STP)	10 Gb/s	4	Gigabitowy Ethernet, VIA, High Speed Interconnect, transmisja audiowizualna
CAT 7a (STP)	100 Gb/s	4	Wideo w wysokiej rozdzielczości, teleradiologia, centra danych
Typ 8 (STP)		2	Dane
Typ 9 (STP)		2	Połączenia szkieletowe

Opisy typów kabli STP pochodzą ze starszych standardów firmy IBM, odnoszących się do sieci token ring. Wymienione kable STP są przyłączane do jednostek MAU za pomocą specjalnych złączy opracowanych przez firmę IBM, w których nie wyróżnia się elementu będącego wtyczką lub gniazdem — kable można łączyć w dowolny sposób dzięki spince blokującej. Niepodłączone kable token ring stanowią niezależną pętlę, do której dodawane są dwa (lub jedno) złącza danych i niekiedy złącze RJ-45. Okablowanie STP zostało w znacznym stopniu zastąpione przez popularniejsze i tańsze kable UTP.

## Kable współosiowe

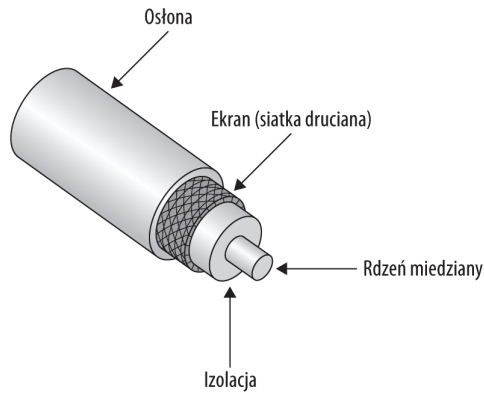
Kable współosiowe (koncentryczne) są powszechnie używane w wielu rodzajach instalacji. Były wykorzystywane jako podstawowy sposób okablowania w początkowej fazie Ethernetu, a dotychczas znajdują zastosowanie w połączeniach telewizyjnych. Kable współosiowe

zostały wprowadzone na rynek w 1929 roku i stały się bazą dla długodystansowych połączeń firmy AT&T. Dopiero w latach 80. zostały wyparte z sieci szkieletowych przez włókna światłowodowe.

Struktura kabla współosiowego jest widoczna na rysunku 8.4. Jak nietrudno zauważyć, centralnie umiejscowiony przewód miedziany jest otoczony izolatorem (*dielektrykiem*). W bardziej kosztownych wykonaniach środkowy przewód miedziany bywa pokrywany srebrem w celu poprawienia charakterystyki przenoszenia sygnału w zakresie wysokich częstotliwości. Warstwa wykonana z materiału dielektrycznego jest następnie otaczana siatką drucianą lub folią metalową, które chronią przewód wewnętrzny przed przenikaniem zakłóceń EMI i RFI. Zewnętrzna powłoka jest zazwyczaj wykonywana z plastiku, teflonu lub kynaru.

#### Rysunek 8.4.

Przekrój kabla  
współosiowego



Obecnie wykorzystuje się wiele rodzajów kabli współosiowych. Poszczególne odmiany zostały przedstawione w tabeli 8.2. Różnią się grubością, zdolnością do przenoszenia prądu elektrycznego oraz obszarem zastosowań. Kable współosiowe są również wykonywane w wersjach Twinax (kabel z dwoma przewodami rdzeniowymi) oraz Trinax (kabel z trzema przewodami rdzeniowymi).

**Tabela 8.2.** Kable współosiowe

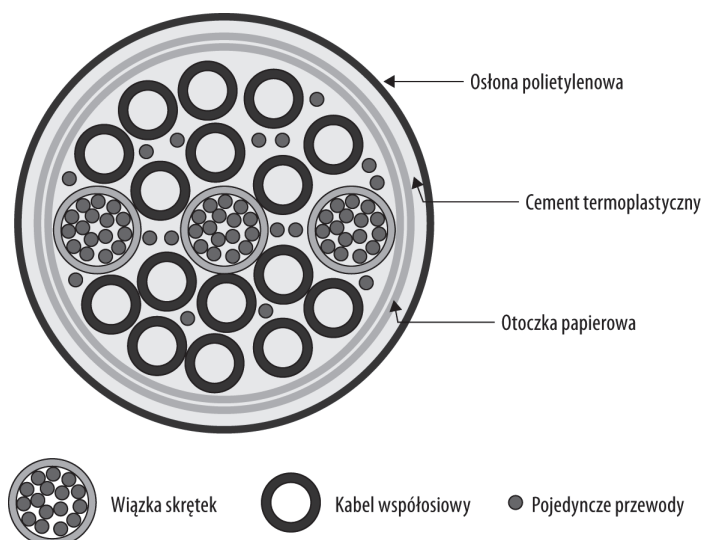
Typ	Średnica rdzenia [mm]	Impedancja [ $\Omega$ ]	Zastosowanie
RG-6	1,0	75	Telewizja kablowa.
RG-8	2,17	50	Ethernet 10Base5 (gruby Ethernet). Pierwszy kabel stosowany w sieciach Ethernet. Zastąpiony przez skrętkę.
RG-11	1,63	75	Kabel telewizyjny.
RG-58/U	0,9	50	Ethernet 10Base2 (cienki Ethernet).
RG-58 A/U	0,9	50	Cienki Ethernet.
RG-58 C/U	0,9	50	Cienki Ethernet.
RG-59	0,81	75	Telewizja kablowa, sieć ARCNET.
RG-62	6,4	93	Sieć ARCNET oraz systemy IBM 3270 (przestarzałe).

Wykorzystanie kabli współosiowych w cienkim Ethernetie i grubym Ethernetie jest obecnie bardzo ograniczone. Głównym ich przeznaczeniem są instalacje audiowizualne, takie jak połączenia w sieciach kablowych, przyłącza do kamer CCTV lub inne rozwiązania szerokopasmowe. Kable współosiowe są sukcesywnie wypierane przez włókna światłowodowe (wraz ze spadkiem cen włókien światłowodowych).

Linie transmisyjne bazujące na kablach współosiowych są budowane w formie tuby obejmującej wiele kabli współosiowych oraz skrętek zabezpieczonych papierową otoczką, termoplastycznym cementem i osłoną polietylenową. Przekrój linii transmisyjnej zawierającej kable współosiowe został przedstawiony na rysunku 8.5. Ostatni standard międzykontynentalnych połączeń kablowych L-5 (wprowadzony w 1972 roku) zawiera definicję, zgodnie z którą kabel składa się z 22 wewnętrznych kabli współosiowych, sygnał jest przekazywany na częstotliwości 57 MHz, jest regenerowany co 2 mile i przenosi 132 000 kanałów głosowych.

### Rysunek 8.5.

Linia transmisyjna  
z kablami  
współosiowymi



## Okablowanie sieci Ethernet

W terminologii związanej z sieciami Ethernet stosowane są oznaczenia odnoszące się do każdego rodzaju kabla wykorzystywanego w tych sieciach. Jednym z nich jest oznaczenie 100Base-T, w którym są zawarte wszystkie potrzebne parametry kabla. Słowo *Base* (podstawowy) oznacza, że sygnał jest transmitowany w paśmie podstawowym, czyli że jego częstotliwość może być mierzona od zera herców do wartości maksymalnej. Takie oznaczenie nie może więc być stosowane w odniesieniu do systemu wykorzystującego multipleksację częstotliwościową. Praca w paśmie podstawowym jest analogiczna do posługiwania się filtrami dolnoprzepustowymi (filtrami z odpowiednią częstotliwością odcięcia). Jednocześnie jest przeciwieństwem systemów pasmowych, w których dopuszcza się transmisję w pewnym zakresie częstotliwości sygnału.

Litera „T” w nazwie 100Base-T informuje, że w danym rozwiązaniu jest stosowana skrętka (od angielskich słów *twisted-pair*). Ogólnie dostępne kable ethernetowe składają się z czterech par przewodów, zakończonych ośmiostykowym złączem RJ-45. Obsługiwane są różne

rodzaje dupleksu, od dwóch pełnodupleksowych połączeń do czterech półdupleksowych. Jednak nie wszystkie sieci ethernetowe bazują na skrętcie. Standardy opisane jako 10Base2 i 10Base5 odnoszą się do Ethernetu wykorzystującego kable współosiowe, w których stosowane są złącza BNC i rozgałęźniki typu T. Nazwy takie jak 100Base-T opisują poszczególne technologie ethernetowe zdefiniowane w standardach IEEE. Na przykład standard 802.3 (14) definiuje sieci 10Base-T, a standard 802.3 (24) sieci 100Base-TX.

Kategorie CAT wyznaczają jedynie sposób wykonania kabla. Natomiast wspomniane wcześniej standardy opisują parametry sygnałów elektrycznych przekazywanych w przewodach oraz zasady łączenia tych przewodów. Na przykład kable CAT 5 są powszechnie stosowanym rodzajem okablowania w szybkich sieciach Ethernet. Jednak aby utworzyć system 100Base-TX, należy wykorzystać określony mechanizm sygnalizacji oraz kabel CAT 5 z dwoma skręconymi parami przewodów. Do transmisji danych z szybkościami przekraczającymi 1 Gb/s stosuje się kable CAT 5E i CAT 6. Wszystkie instalacje ethernetowe obsługują przepustowość w zakresie od najmniejszej (10Base-T) po właściwą dla danego standardu.

Na potrzeby sieci Ethernet bazujących na kablach CAT 5 organizacje TIA/EIA zdefiniowały dwa standardy łączenia przewodów, przedstawione w tabeli 8.3. Różnica między nimi polega jedynie na zamianie pary nadawczej (Tx) z parą odbiorczą (Rx).

**Tabela 8.3.** Oznaczenia przewodów ethernetowych w standardach TIA/EIA

Standard	Wyprowadzenie	Para	Polaryzacja	Kolor
568-A	1	3	dodatnia	biało-zielony
568-A	2	3	ujemna	zielony
568-A	3	2	dodatnia	biało-pomarańczowy
568-A	4	1	ujemna	niebieski
568-A	5	1	dodatnia	biało-niebieski
568-A	6	2	ujemna	pomarańczowy
568-A	7	4	dodatnia	biało-brązowy
568-A	8	4	ujemna	brązowy
568-B	1	2	dodatnia	biało-pomarańczowy
568-B	2	2	ujemna	pomarańczowy
568-B	3	3	dodatnia	biało-zielony
568-B	4	1	ujemna	niebieski
568-B	5	1	dodatnia	biało-niebieski
568-B	6	3	ujemna	zielony
568-B	7	4	dodatnia	biało-brązowy
568-B	8	4	ujemna	brązowy

W różnych standardach ethernetowych zostały zdefiniowane różne poziomy napięcie sygnałów. Na przykład w rozwiązaniach 10Base-T i 100Base-T podczas nadawania (Tx) wykorzystuje się dwa napięcia  $\pm 2,5$  V. Natomiast w połączeniach 100Base-TX nadajnik generuje sygnał o trzech poziomach napięciowych:  $\pm 1,0$  V oraz 0 V.

W gigabitowym Ethernetie (1000Base-T) wykorzystywane są różne poziomy napięcie w zależności od implementacji standardu. Na przykład w przypadku modulacji impulsowo kodowej (PAM) sygnał może mieć napięcie  $\pm 2,0$  V,  $\pm 1,0$  V oraz 0 V. Choć w praktyce często okazuje się, że są to poziomy  $\pm 1,0$  V,  $\pm 0,5$  V oraz 0 V. Rozmieszczenie przewodów w kablu jest odpowiednio odwzorowywane w karcie sieciowej.

Standardowe połączenia są wykonywane w taki sposób, że numery wyprowadzeń odpowiadają sobie wzajemnie na obydwu końcach kabla. Oznacza to, że pary nadawcze i pary odbiorcze znajdują się na tych samych stykach wtyczki. Kable takie nazywają się kablami prostymi. Inny sposób wykonania kabli polega na połączeniu par nadawczych z parami odbiorczymi, w wyniku czego powstaje kabel z przeplotem. W rozwiązaniach 10Base-T i 100Base-TX wykorzystywane są jedynie dwie pary przewodów. Natomiast w połączeniach 1000Base-T (w gigabitowym Ethernetie) używane są wszystkie cztery pary. W standardowym rozwiązaniu węzeł sieciowy (router) lub komputer wysyła sygnały przez wyprowadzenia 1. i 2., a odbiera sygnały przez wyprowadzenia 3. i 6. Gdy wspomniany węzeł jest przyłączony do koncentratora ethernetowego, to koncentrator nadaje sygnały przez wyprowadzenia 3. i 6., a odbiera przez wyprowadzenia 1. i 2.



Zastosowanie kabla z przeplotem w połączeniu wymagającym kabla prostego spowoduje, że komunikacja nie będzie możliwa. Warto więc opracować pewną metodę szybkiego odróżniania kabli z przeplotem od kabli prostych, na przykład przez użycie innego koloru lub trwałego oznaczania obydwu końcówek kabli.

Chcąc połączyć ze sobą dwa komputery, routery lub dwa koncentratory ethernetowe, należy zastosować kabel z przeplotem. Oba urządzenia nadają sygnały na wyprowadzeniach 1. i 2. i odbierają na wyprowadzeniach 3. i 6. Zamiana par w kablu pozwala na prawidłową transmisję. Nowsze ethernetowe karty sieciowe dysponują funkcją automatycznego wykrywania rodzaju połączenia i mogą we własnym zakresie zmienić sposób przekazywania sygnałów, gdy ustalą, że potrzebny jest przeplot.

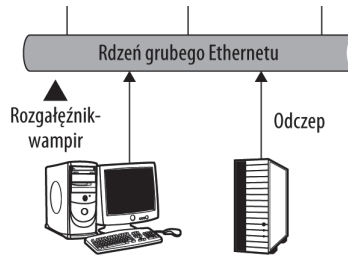
Podczas przyłączania koncentratora lub przełącznika do innego urządzenia tego typu konieczne jest wprowadzenie przeplotu. Jednak producenci komponentów sieciowych wykonują przeplot wewnętrznie i opisują port jako *uplink* lub *X*. Dzięki temu wymienione urządzenia można łączyć kablem prostym. Niekiedy aby uaktywnić funkcję portu uplink, trzeba nacisnąć specjalny przycisk. Jeśli jednak do połączenia dwóch koncentratorów muszą być użyte klasyczne porty, należy zastosować kabel z przeplotem. Większość nowoczesnych koncentratorów i przełączników nie zawiera wyróżnionych portów uplink, lecz automatycznie rozpoznaje stan połączenia, umożliwiając wykorzystanie kabla prostego w łączy, w którym powinien być zastosowany kabel z przeplotem. Funkcja ta jest opisywana najczęściej jako *Auto-Uplink* lub *Auto-MDI-X*. Skrót MDI odpowiada angielskim słowom *Medium Dependent Interface* oznaczającym *interfejs zależny od medium* transmisyjnego, a litera X reprezentuje wewnętrzny przeplot. Interfejs MDI-X jest portem koncentratora, routera lub przełącznika, za którego pomocą można dane urządzenie przyłączyć do kolejnego koncentratora, routera lub przełącznika bez potrzeby użycia kabla z przeplotem. Konieczność rozróżnienia portów MDI i MDI-X wynika z tego, że w standardowym połączeniu portów

sygnał nadawany w przełączniku musi zostać dostarczony do wyprowadzeń wejściowych karty sieciowej, a sygnał przekazywany ze styków wyjściowych karty sieciowej musi być przekazany do wyprowadzeń odbiorczych przełącznika. Port MDI-X zapewnia zamianę pary nadawczej z parą odbiorczą.

We wcześniejszych sieciach Ethernet stosowano połączenia 10Base5 (gruby Ethernet) oraz 10Base2 (cienki Ethernet). Pierwszy z wariantów sprowadzał się do ułożenia kabla magistralnego (zazwyczaj w podwieszanych sufitach), od którego odchodziły linie przyłączeniowe. Odczepy były wydzielane za pomocą złączy typu N lub rozgałęźnika wczepianego w kabel („wampira” (ang. *vampire tap*)). Typowy segment sieci grubego Ethernetu został przedstawiony na rysunku 8.6. Instalacja wymagała uziemienia ekranu z jednej strony kabla oraz umieszczenia na obydwu końcach terminatorów. Komputery były przyłączone do sieci za pomocą transceiverów połączonych z jednostką 15-wyprowadzeniowym złączem typu D (nazywanym interfejsem AUI). Koszt wdrożenia grubego lub cienkiego Ethernetu był znacznie wyższy niż koszt rozwiązań bazujących na skrętce. Dlatego obydwa rodzaje sieci należą już do historii.

### Rysunek 8.6.

Gruby Ethernet  
i kable przyłączeniowe



## Kable optyczne

W kablach optycznych jako medium transmisyjne wykorzystuje się krzem, szkło lub plastik. Pierwszy patent związany z transmisją sygnałów optycznych został przyznany firmie AT&T w 1934 roku. Jednak praktycznego zastosowania technologia ta doczekała się dopiero w 1960 roku. W roku 1970 firma Corning Glass Works (obecnie Corning Incorporated) opracowała i opatentowała proces produkcji światłowodów, który umożliwił zmniejszenie tłumienności włókna z ponad 1000 dB/km do mniej niż 20 dB/km. W latach 90. ubiegłego stulecia zaczęto produkować znacznie tańsze światłowody z wykorzystaniem plastiku oraz krzemu w osłonie plastiku (PCS — *Plastic-Clad Silica*).

Włókna jednomodowe są przeznaczone do przenoszenia pojedynczych modów (promieni świetlnych). Natomiast światłowody wielomodowe przesyłają wiele różnych modów. Światłowody wielomodowe są stosowane na relatywnie krótkich odcinkach tras, co wynika z występowania dyspersji modowej. Dyspersja modowa powstaje na skutek różnej szybkości propagacji poszczególnych modów sygnału optycznego.

Optyczny system transmisyjny składa się ze źródła światła, kabla światłowodowego (lub innego medium transmisyjnego) oraz detektora optycznego. Źródło światła musi emitować impulsy świetlne, które w detektorze są interpretowane jako bit 1 lub stan włączenia. Brak sygnału jest traktowany jako logiczne 0 lub stan wyłączenia. Im szybciej operacja włączania i wyłączania źródła światła może być wykonywana, tym większą uzyskuje się szybkość

transmisji danych. Jako źródła światła stosowane są diody LED lub lasery półprzewodnikowe. Samo światło podróżuje wzdłuż włókna, odbijając się na granicy dwóch warstw o różnym współczynniku załamania światła.



Światłowód, który jest ułożony, ale nie przenosi sygnału, nazywa się często ciemnym światłowodem. Olbrzymia liczba ciemnych kabli światłowodowych ułożonych między kontynentami w latach 90. pozwoliła na rozkwit sieciowej rewolucji komputerowej.

Kable optyczne nie ulegają wpływom zakłóceń EMI lub RMI, ale wiążą się z nimi zupełnie inne zagrożenia. Prawdopodobnie najbardziej dokuczliwe jest to, że są one znacznie delikatniejsze niż kable miedziane. Włókno jest przecież zrobione ze szkła lub z plastiku. Kable światłowodowe są również trudniejsze do przechowywania i kosztowniejsze niż kable miedziane.

W kolejnych punktach zostały opisane (od strony teoretycznej) mechanizmy rozchodzenia się światła we włóknie światłowodowym.

## Tłumienie i dyspersja

Wybór materiału na światłowód jest podyktowany koniecznością przeniesienia fal świetlnych o określonym zakresie długości z możliwie najmniejszą stratą podczas transmisji. Zmniejszenie mocy sygnału jest określane jako *tłumienie*. Tłumienie wynika zarówno z rozpraszania światła, jak i z jego absorpcji. Rozpraszanie światła wynika z występowania odchyłek w przewidywanej trasie przesyłania sygnałów. Absorpcja jest z kolei wynikiem przekazywania energii impulsów do szkła oraz występowania zanieczyszczeń ograniczających moc transmitowanego sygnału.

Tłumienie światłowodu jednomodowego zawiera się w przedziale od 0,25 dB/km do 0,5 dB/km. Wartość tłumienia wyznacza się jako iloraz mocy nadawczej do mocy odbieranego sygnału zgodnie z zależnością:

$$\text{Tłumienie [dB]} = 10 \log_{10}(\text{moc nadawcza} / \text{moc sygnału odbieranego})$$

Tłumienie sygnału optycznego przesyłanego w światłowodzie jest determinowane kilkoma czynnikami. Na granicy szkło-powietrze promienie świetlne są załamywane w taki sposób, że sygnał jest wprowadzany z powrotem do przewodu pod kątem równym co do wartości kątowni padania. Stosunek współczynników załamania światła w rdzeniu i płaszczu wyznacza dopuszczalną wartość kąta padania, który jest wyrażony wzorem:

$$Q_c = \arccos(n_2 / n_1)$$

gdzie  $Q_c$  jest wartością krytyczną kąta (mierzonych do osi rdzenia), powyżej której wprowadzane światło nie będzie przenoszone we włóknie. Zmienne  $n_1$  i  $n_2$  odpowiadają współczynnikom załamania światła w płaszczu i w rdzeniu. W przypadku standardowych wartości współczynnika  $n$  kąt graniczny może wynosić około  $8,5^\circ$ , co oznacza przenoszenie bardzo wąskiej wiązki.

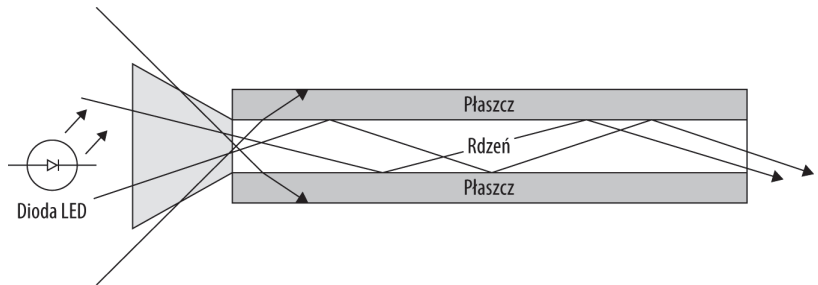
Powyższe równanie można przekształcić tak, aby uwzględniło efekt przejścia światła z powietrza, definiując kąt zewnętrzny  $Q_{\text{ext}}$  i wykorzystując współczynnik załamania światła w powietrzu o wartości  $n_0$  (1,00029):

$$Q_{\text{ext}} = \arcsin[(n_1/n_0) \sin(Q_c)]$$

Uwzględnienie ośrodka, jakim jest powietrze, powoduje zwiększenie wartości kąta krytycznego do 12,5 stopni.

Zagwarantowanie kąta wprowadzenia światła o wartości niższej od krytycznej powoduje całkowite uwięzienie światła we włóknie. Powyżej tej wartości sygnał jest tracony. Na rysunku 8.7 został przedstawiony przykład odbicia światła wyemitowanego przez diodę LED i transmitowanego we włóknie światłowodowym. Rdzeń włókna jest wykonany ze szkła. Płaszcz stanowi otoczkę wykonaną z plastiku lub innego materiału. Stożek z pionowymi liniami reprezentuje zakres kątów padania światła, które gwarantują odbicie wiązki na granicy rdzenia i płaszcza, a tym samym przekazanie jej do odbiornika. Wprowadzenie wiązki pod większym kątem spowoduje wyciek światła do płaszcza i utratę sygnału.

**Rysunek 8.7.**  
*Odbicie światła  
we włóknie  
światłowodowym*



Istnieje możliwość utworzenia włókna, które pozwala na przenoszenie jedynie światła o niewielkim zakresie fal. Jest to cecha charakterystyczna światłowodów jednomodowych. We włóknaach jednomodowych światło propaguje tak, jakby włókno było falowodem. W światłowodzie wielomodowym można wyróżnić wiele ścieżek propagacji światła, z których każda wynika z różnych kątów odbicia poszczególnych modów świetlnych.

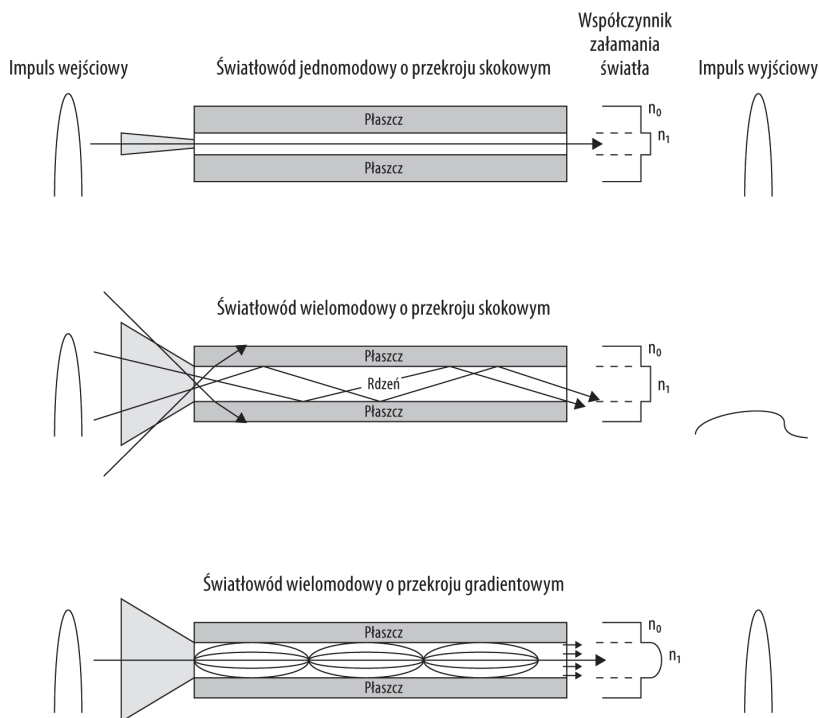
Podróżujące w światłowodzie impulsy świetlne wykazują tendencję do rozpraszania się wraz z pokonywaną odległością oraz do interferowania z innymi modami. Powstaje wówczas efekt dyspersji, którego rozmiar jest funkcją długości fali świetlnej. W celu zmniejszenia wpływu dyspersji można zmniejszyć częstotliwość generowania impulsów sygnału lub zmienić kształt tych impulsów.

Na rysunku 8.7 została przedstawiona transmisja w światłowodzie wielomodowym, w którym współczynnik załamania światła zmienia się nagle na krótkim odcinku (występuje skokowa zmiana współczynnika). Jeśli średnica rdzenia jest mniejsza — zbliżona do szerokości wiązki światła — światło jest wprowadzane pod bardzo małym kątem i propaguje we włóknie niemal całkowicie bez odbijania się na granicy ośrodków.

Inna technologia produkcji włókien zakłada gradientową zmianę współczynnika odbicia — zakres zmian wartości współczynnika rozciąga się od wartości współczynnika obowiązującego w rdzeniu do wartości typowej dla płaszcza. Gradientowy światłowód wielomodowy umożliwia załamywanie światła pod większą liczbą kątów, co w konsekwencji prowadzi do uzyskania impulsów o ostrzejszym kształcie niż podczas przesyłania sygnału w światłowodzie skokowym. Na rysunku 8.8 zostały zaprezentowane trzy różne metody transmisji światła odpowiadające różnym ścieżkom propagacji wiązki. Pierwszy z przykładów jest charakterystyczny dla włókien jednomodowych, w których następuje skokowa zmiana współczynnika załamania światła. Światło może być przekazywane w obszarze

**Rysunek 8.8.**

Transmisja  
jednomodowa  
i wielomodowa



szklanego rdzenia z niewielkimi stratami. Jednak ten rodzaj światłowodu wymaga wprowadzania silnie skupionej wiązki światła, czyli wprowadzania pojedynczego modu światła. Termin *mod* odnosi się do różnych kątów, pod którymi można wprowadzać światło do rdzenia.

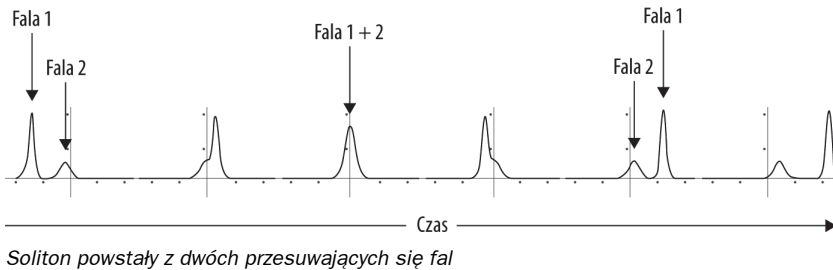
Zakresy fal świetlnych są na rysunku reprezentowane przez trzy identyczne parabole odpowiadające impulsom sygnału (widoczne wzdłuż lewej krawędzi rysunku). Znajdujący się po ich prawej stronie stożek wyznacza różne kąty padania światła, które gwarantują poprawne przekazanie impulsu przez włókno. Po prawej stronie włókna przedstawione zostały profile współczynników załamania światła. Współczynnik załamania światła określa zdolność ośrodka do spowolnienia szybkości rozchodzenia się światła w odniesieniu do szybkości właściwej dla próżni. Wiązka światła ulega zakrzywieniu lub odbiciu, gdy dotrze do granicy ośrodków o różnej gęstości optycznej. W przypadku prawidłowego załamania wiązki sygnał jest przekazywany wzdłuż włókna, w wyniku czego obserwowane są impulsy wyjściowe (pokazane po prawej stronie rysunku). W przypadku nieudanego odbicia światło wycieka z rdzenia i sygnał jest tracony. Górna część rysunku odnosi się do światłowodu, w którym zmiana współczynnika załamania światła jest funkcją skokową. Wiązka musi zostać wprowadzona pod kątem nie większym niż określona przez stożek widoczny po lewej stronie włókna. Światłowody jednomodowe przenoszą tylko promienie padające prosto — światło propaguje w rdzeniu bez odbić. Aby spełnić to założenie, konieczne jest stosowanie źródeł światła generujących silnie skupione wiązki, takich jak lasery.

W środkowej części rysunku przedstawiony został przykład transmisji światła we włóknie wielomodowym o przekroju skokowym. Światłowód umożliwia wprowadzanie wielu modów świetlnych, pozwalając na wprowadzanie wiązki pod znacznie większymi kątami

### Solitony

Wytworzenie impulsu o kształcie zbliżonym do wykresu funkcji cosinusa hiperbolicznego (podstawowego i odbitego) pozwala na zniesienie efektu dyspersji niezależnie od kierunku transmisji. Impulsy o takim kształcie są nazywane solitonami. Solitony charakteryzują się tym, że mogą pokonywać bardzo duże dystanse (tysiący kilometrów) bez zniekształcenia. Solitony (samopodtrzymujące się odosobnione fale) powstają wówczas, gdy dwie fale (lub większa ich liczba) zachowują się jak cząstki i podróżują ze stałą szybkością bez zmiany kształtu.

Na rysunku zostały przedstawione dwie fale o różnej amplitudzie i prędkości, zbliżające się do siebie (fale o różnych długościach są przekazywane w tym samym ośrodku z różnymi prędkościami). W pewnym momencie obydwie impulsy zostają połączone, po czym impuls fali szybszej (fali 1) wydziela się ze złączonego impulsu (fale 1 + 2), zachowując kształt, który miał przed połączeniem z wolniejszą falą 2. Zjawisko to zaobserwował John Scott-Russell na kanale blisko Edynburga w 1834 roku. Opracowanie matematycznej teorii potwierdzającej obserwację zajęło aż 50 lat. Efekt zbliżony do transmisji solitonów można zauważyć podczas przyływu w zatoce Fundy. Solitony mogą odgrywać pewną rolę w przekazywaniu impulsów elektrycznych przez neurony, choć jest to wciąż kontrowersyjna teoria. Solitony są już przedmiotem badań laboratoryjnych, ale technologia ich wykorzystania nie została jeszcze opracowana.



(zgodnie z rozmiarem stożka). Porównując wynik transmisji impulsu z wcześniej omawianym rozwiązaniem, można zauważyć, że podczas przekazywania sygnału w światłowodzie wielomodowym następuje zmniejszenie amplitudy oraz rozmycie impulsów (w przykładzie z zastosowaniem światłowodu wielomodowego kształt impulsu wyjściowego odpowiada dokładnie kształtowi impulsu wejściowego).

W ostatnim przykładzie (widocznym na dole rysunku 8.8) analizie poddano włókno wielomodowe o gradientowym współczynniku załamania światła. W przeciwieństwie do dwóch poprzednich rozwiązań, w których występowały skokowe zmiany współczynnika i niewielkie zakresy kątów wprowadzania wiązki, zastosowanie gradientowych zmian współczynnika załamania światła pozwala na przekazywanie wielu modów świetlnych bez szkody dla kształtu impulsu (widocznego po prawej stronie rysunku). Jest to jednak bardziej skomplikowane rozwiązanie, które prowadzi do rozproszenia światła i poszerzenia jego widma, co jest wadą w przypadku przesyłania na dużych odległościach. Dlatego na połączeniach długodystansowych lepiej sprawują się światłowody o przekrojach skokowych.

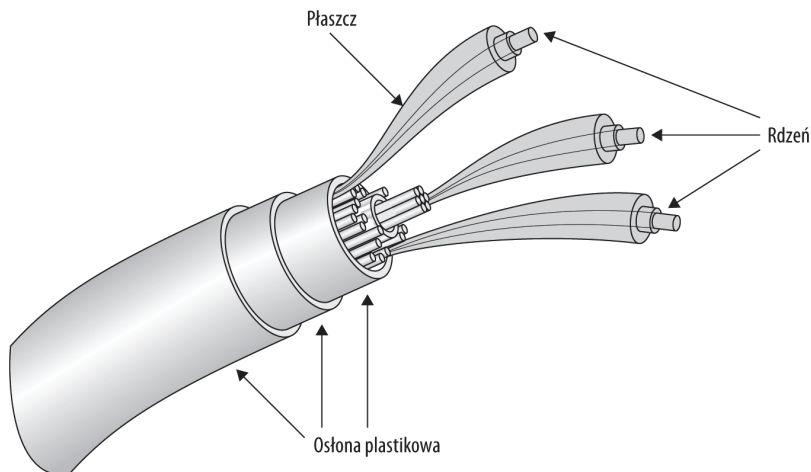
### Parametry fizyczne

Rdzeń wielomodowego włókna optycznego ma średnicę 50  $\mu\text{m}$  lub 62,5  $\mu\text{m}$ , co odpowiada grubości ludzkiego włosa. Otacza go płaszcz wykonany z materiału o niższym współczynniku załamania światła. Płaszcz występuje w każdym rodzaju włókna światłowodowego.

Zapobiega on wyciekowi światła z rdzenia — odbija wiązkę światła z powrotem do rdzenia. Rdzeń z płaszczem stanowią włókno o średnicy 125  $\mu\text{m}$ . W światłowodach jednomodowych średnica rdzenia wynosi 9  $\mu\text{m}$ . Również w przypadku tych włókien dodanie płaszcza powoduje, że powstały światłowód ma średnicę 125  $\mu\text{m}$ . Zatem w zależności od rodzaju światłowodu parametry fizyczne są opisywane w skrócie jako 50  $\mu\text{m}$  / 125  $\mu\text{m}$ , 62,5  $\mu\text{m}$  / 125  $\mu\text{m}$  lub 9  $\mu\text{m}$  / 125  $\mu\text{m}$ . W każdym przypadku światłowód jest otoczony izolacją ochronną, wykonaną z włókna szklanego, kewlaru lub stali, a następnie osłoną plastikową. Połączenie rdzenia, płaszcza i powłoki ochronnej jest potocznie nazywane *włóknem*. Budowa kabla optycznego została przedstawiona na rysunku 8.9.

### Rysunek 8.9.

*Kabel światłowodowy*



Światłowód jednomodowy ma praktycznie nieograniczoną szerokość pasma, co nie jest prawdą w przypadku światłowodu wielomodowego. Obydwa rodzaje włókien zapewniają doskonałą jakość sygnału, a w przypadku włókna jednomodowego ta wysoka jakość jest zachowana na dłuższych odległościach transmisyjnych. Głównym czynnikiem wpływającym na uszkodzenie sygnału w światłowodach jednomodowych jest dyspersja chromatyczna. Natomiast w światłowodach wielomodowych — dyspersja modowa. Przyczyną powstawania dyspersji chromatycznej jest to, że wiązka światła załamuje się w różnym stopniu, zależnie od długości fali. Typowym przykładem występowania tego zjawiska jest przepuszczenie światła przez pryzmat, który rozczepia wiązkę na barwy składowe. Dyspersja modowa powstaje podczas przesyłania sygnału wzdłuż światłowodu wielomodowego, gdyż poszczególne mody światła są przekazywane z różną prędkością. Włókna światłowodowe są tworzone w taki sposób, aby współczynnik załamania światła był niejednakowy wzdłuż średnicy włókna. Zmiana współczynnika załamania może mieć charakter skokowy lub gradientowy. W światłowodach wielomodowych stosowane są obydwa rozwiązania. Natomiast włókna jednomodowe zawsze są włóknami skokowymi. Jako regułę można przyjąć, że światłowody jednomodowe mają uniwersalne zastosowanie, szczególnie w odniesieniu do sieci ethernetowych. Natomiast włókna wielomodowe są niekiedy stosowane w Ethernetie, a także podczas przekazywania analogowych sygnałów wizyjnych i w systemach komunikacji na krótkich odległościach.

Kable optyczne są grupowane w pary zapewniające komunikację dwukierunkową, a następnie dołączane do kolejnych kabli aż do uzyskania 96 włókien jednomodowych w tubie. Grupy kabli mogą być umieszczone luźno lub ściśle w tubie osłonowej. Ścisłe tuby są wykorzy-

stywane poza budynkami oraz na dłuższych odległościach z uwagi na ich fizyczne właściwości. Kable światłowodowe znajdują zastosowanie w instalacjach napowietrznych, podziemnych i podmorskich.

W przeciwieństwie do kabli miedzianych transmisja w kablach światłowodowych nie jest zakłócana przez źródła elektryczne, magnetyczne ani radiowe. Ponadto włókna światłowodowe zapewniają szersze pasmo i umożliwiają zwiększenie odległości między regeneratorami. Jako źródła światła wykorzystuje się diody LED lub lasery (szczególnie gdy wymagana jest transmisja na dłuższym dystansie). Do typowych modulacji impulsów świetlnych należy zaliczyć:

- ♦ **Kluczowanie amplitudy (ASK) (modulacja intensywności światła).** Amplituda sygnału generowanego przez źródło światła jest zależna od sygnału modulującego. Modulacja intensywności jest stosowana w połączeniach sieci LAN, w których używane są diody LED.
- ♦ **Kluczowanie fazy (PSK).** Jest to modulacja cyfrowa, która odpowiada za zmianę fazy fali nośnej w zależności od kombinacji bitowej strumienia danych.
- ♦ **Kluczowanie częstotliwości (FSK).** Modulacja FSK gwarantuje kodowanie informacji cyfrowych przez zmianę częstotliwości fali nośnej.
- ♦ **Modulacja polaryzacji.** W modulacji polaryzacji zmianie ulega polaryzacja fali nośnej. Rodzaj zmian odpowiada kodowanym wartościom bitowym.

W tabeli 8.4 zostały zestawione cechy diod LED i laserów półprzewodnikowych wykorzystywanych jako źródła światła w generatorach sygnałów.

**Tabela 8.4.** Porównanie diod LED i laserów półprzewodnikowych jako źródeł światła

Właściwość	Dioda LED	Laser półprzewodnikowy
Koszt	Tania	Droga
Żywotność	Długa	Krótką
Niezawodność	Duża	Średnia
Tryb pracy	Tylko wielomodowy	Jednomodowy lub wielomodowy
Moc	Średnia	Duża
Liniiowość	Wysoka (szersze impulsy)	Niska (ostrzejsze impulsy)
Efektywność sprzęgania	Średnia	Duża
Dystans propagacyjny	Krótki	Długi
Szybkość transmisji	Niska	Wysoka
Wrażliwość na zmiany temperatury	Niska	Wysoka

Zazwyczaj nie wymagają regeneracji sygnału na odcinkach krótszych niż 3 km. W przypadku długodystansowych włókien szkieletowych, które są zasilane laserami, odcinki między regeneratorami mogą wynosić nawet 100 km. W sieciach LAN stosuje się zazwyczaj diody LED. Natomiast połączenia szkieletowe bazują na laserach. Dzięki światłowodom przekazywanie informacji na kilkukilometrowych odległościach nie jest więc szczególnym wyzwaniem.

Do przyłączania światłowodów jednomodowych stosuje się wiele rodzajów złączy, w tym połączenia skręcane SMA (typ 905 i 906) oraz złącza typu ST, SC i LC. Włókna jednomodowe często łączy się w pary, aby zapewnić dwukierunkową wymianę danych. Złącza typu SC mają kwadratowy przekrój oraz obudowę gwarantującą, że włókna nie zostaną zamienione podczas instalacji. Każde połączenie zbliżeniowe wprowadza do światłowodu straty na poziomie 10 do 20 procent mocy sygnału, zależnie od rodzaju światłowodu (tzn. od tego, czy został wykonany ze szkła, plastiku, czy jest gradientowy, czy skokowy).

Kable światłowodowe są zazwyczaj droższe niż połączenia miedziane. Jednak znajdują powszechne zastosowanie w wysokowydajnych sieciach Ethernet, SONET/SDH (optycznych sieciach pierścieniowych), ATM, 10Base-F oraz FDDI. Ich zaletami są: większa szerokość pasma, dłuższe odcinki bez regeneracji sygnału, odporność na zakłócenia EMI i RFI oraz zwiększone bezpieczeństwo danych. Wyższy poziom bezpieczeństwa danych wynika z tego, że włączenie się do toru optycznego jest bardzo trudnym zadaniem. Jednak praca ze światłowodami może być również uciążliwa. Są zawodne, łatwo można je złamać, trudno zakłada się elementy zakończenia i muszą być układane w rurach ochronnych lub prowadnicach. Trzeba też umiejętnie dobierać określone rodzaje kabli światłowodowych do danych zastosowań.

## Sieci optyczne

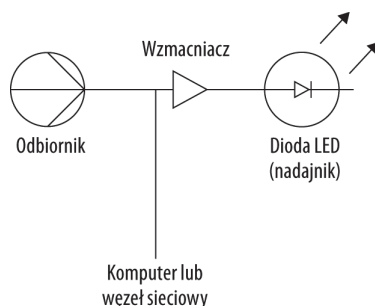
Topologia sieci optycznej jest determinowana przez kilka elementów instalacji. Poza komponentami takimi jak źródła sygnału, media transmisyjne i odbiorniki niezbędne mogą się bowiem okazać również regeneratory lub rozgałęźniki zapewniające odczep do innych mediów transmisyjnych.

Rozgałęźniki (połączenia typu T) mają charakter aktywny lub pasywny. Składają się z kilku wewnętrznie połączonych włókien światłowodowych, zapewniających podział sygnału lub jego łączenie. Elementy pasywne wydzielają sygnał, wprowadzając pewne straty. Natomiast rozgałęźniki aktywne wzmacniają sygnał przed przekazaniem go do światłowodu. Rozgałęźniki pasywne są wyposażane w dwa odczepy zespolone z głównym włóknem. W wyniku ich działania sygnał ulega stłumieniu.

Rozgałęźniki aktywne są wyposażone w laser lub diodę LED umieszczone po jednej stronie komponentu oraz detektor (fotodiodę) (odbierający sygnały od innej jednostki sieciowej) po drugiej stronie rozgałęźnika. Ta część rozgałęźnika, która przenosi światło na wprost, jest elementem pasywnym (zgodnie z rysunkiem 8.10). Dzięki temu awaria układu aktywnego powoduje jedynie wyłączenie odczepu, a nie toru transmisyjnego, który jako komponent pasywny nie przestaje realizować swoich zadań. Rozwiązania tego typu zapewniają niezawodność sieci optycznych.

### Rysunek 8.10.

Rozgałęźnik światłowodowy



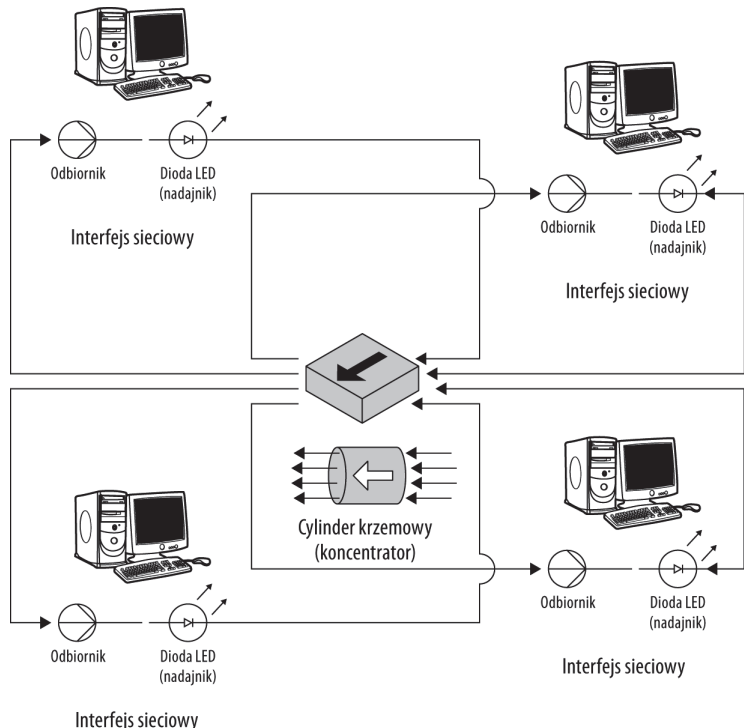
Światło może być przenoszone we włóknach optycznych na bardzo dużych odległościach. Niemniej co kilka kilometrów konieczne jest wtarczenie do toru transmisyjnego regeneratora optycznego, który odtworzy pierwotną moc i jakość sygnału. Pierwsze komponenty tego typu zawierały obwody konwersji optyczno-elektronicznej, które przechwytywały sygnał, a następnie generowały go z odpowiednią mocą w nadajniku. Najnowsze urządzenia wykorzystują technikę optycznego przechwytywania sygnałów. Nie wymagają więc konwersji na postać elektryczną, a w związku z tym mogą pracować w znacznie szerszych pasmach niż regeneratory starszego typu. Regenerator zawiera te same komponenty co rozgąłęźnik przedstawiony na rysunku 8.10, z pominięciem odczepu prowadzącego do węzła sieciowego.

Większość sieci optycznych jest budowana zgodnie z topologią pierścieniową. Doskonałym przykładem jest tutaj sieć SONET, opisana w rozdziale 13. Przerwanie pierścienia może doprowadzić do wyłączenia jednego z nadmiarowych połączeń, ale nie skutkuje uszkodzeniem całej sieci. Wiele topologii pierścieniowych zakłada występowanie łączy dwukierunkowych, co sprawia, że każde połączenie jest samodzielną pętlą. Połączenia jednokierunkowe ulegają bowiem uszkodzeniu wraz z uszkodzeniem pojedynczego łącza.

W niektórych przypadkach sieci optyczne są budowane zgodnie z topologią pasywnej gwiazdy, przedstawionej na rysunku 8.11. Pasywna gwiazda składa się z centralnego elementu, którym jest krzemowy cylinder pełniący funkcję koncentratora optycznego. Przyłączone do niego linie światłowodowe są umiejscowione w taki sposób, że pewna część światła z każdego nadajnika optycznego jest dostarczana do każdego z odbiorników. Z cylindra wyprowadzone są kable światłowodowe prowadzące do poszczególnych odbiorników. Każdy optyczny interfejs sieciowy jest wyposażony w odbiornik sygnałów oraz nadajnik optyczny wprowadzający sygnały do sieci.

### Rysunek 8.11.

*Połączenia światłowodowe w topologii pasywnej gwiazdy*



System wykonany w topologii pasywnej gwiazdy umożliwia poszczególnym segmentom sieciowym bezpośrednią komunikację z innymi segmentami. Konstrukcja koncentratora gwarantuje przekazanie światła z dowolnego wejścia na wszystkie wyjścia. Współczynnik rozgałęzienia jest w tym przypadku zależny od czułości fotodiod odbiorników wykorzystanych w sieci.

## Łączność bezprzewodowa

Kable nie są jedynymi mediami, które mogą być stosowane w komunikacji sieciowej. Sygnały informacyjne można również przesyłać w powietrzu lub nawet w próżni. Gdzieś w przestrzeni kosmicznej, oddalona o 23 lata świetlne cywilizacja z pewnością właśnie ogląda pierwszy odcinek *Klanu*.

W kolejnych punktach rozdziału zostało opisane zastosowanie fal elektromagnetycznych w połączeniach sieciowych.

## Promieniowanie elektromagnetyczne

Częstotliwość i długość fali są pojęciami ściśle ze sobą związanymi (prędkością światła), które wyznaczają szybkość rozchodzenia się fal. W próżni fale elektromagnetyczne rozchodzą się z prędkością światła zgodnie z zależnością:

$$c = f \lambda \text{ lub } \lambda = c / f$$

Zależność między energią i długością fali (a tym samym częstotliwością) jest określona równaniem:

$$E = h f \text{ lub } E = (h c) / \lambda$$

gdzie  $f$  odpowiada częstotliwości,  $\lambda$  reprezentuje długość fali,  $c$  prędkość światła ( $3 \times 10^8$  m/s), a  $h$  jest stałą Plancka ( $6,6 \times 10^{-34}$  Js). Oznacza to, że w próżni światło pokonuje jeden metr w ciągu trzech nanosekund. Promieniowanie elektromagnetyczne w próżni nie podlega żadnym ograniczeniom. Jednak gdy światło jest przenoszone w ośrodkach takich jak szkło lub woda, jego prędkość zmniejsza się odpowiednio do około dwóch trzecich i jednej drugiej prędkości światła. Fale elektromagnetyczne przekazywane w przewodnikach takich jak miedź również ulegają spowolnieniu do około dwóch trzecich prędkości światła. Ostatnie badania dowiodły, że można nawet zatrzymać światło w magnetycznej pułapce kondensatu Bosego-Einsteina. Być może kiedyś będzie można w ten sposób przechowywać informacje.

Bieżące technologie pozwalają na wykorzystanie jedynie fragmentu widma elektromagnetycznego do przesyłania danych — fal radiowych, zakresu mikrofalowego, podczerwieni, światła widzialnego i nadfioletu. Wysokoenergetyczne (krótkofalowe) promieniowanie Roentgena i gamma nie są wykorzystywane ze względów finansowych i praktycznych (są zbyt energetyczne). Dłuższe fale o niższej energii (o częstotliwościach poniżej częstotliwości radiowych) są zbyt wolne, aby były użyteczne w połączeniach sieciowych (wnosiłyby zbyt dużo opóźnień). Międzynarodowa Unia Telekomunikacyjna (ITU) podzieliła widmo elektromagnetyczne na zakresy przedstawione w tabeli 8.5.

**Tabela 8.5.** Zakresy częstotliwości

Pasmo	Klasa częstotliwości radiowych według ITU	Częstotliwość	Długość fali	Energia
g (promieniowanie gamma)	-	30 EHz – 300 EHz	10 pm – 1 pm	124 keV – 1,24 keV
HX (twarde promieniowanie rentgenowskie)	-	3 EHz – 30 EHz	100 pm – 10 pm	12,4 keV – 124 keV
SX (miękkie promieniowanie rentgenowskie)	-	30 PHz – 3 EHz	1 nm – 100 pm	1,24 keV – 12,4 keV
EUV (wysoki ultrafiolet)	-	3 PHz – 30 PHz	100 nm – 10 nm	12,4 eV
NUV (bliski ultrafiolet)	-	300 THz – 3 PHz	1 μm – 100 nm	1,24 eV
NIR (bliska podczerwień)	-	30 THz – 300 THz	10 μm – 1 μm	124 meV
MIR (średnia podczerwień)	-	3 THz – 30 THz	100 μm – 10 μm	12,4 meV
FIR (daleka podczerwień)	-	300 GHz – 3 THz	1 mm – 100 μm	1,24 meV
EHF	EHF (ekstremalnie wysokie częstotliwości)	30 GHz – 300 GHz	1 cm – 1 mm	124 μeV
SHF	SHF (superwysokie częstotliwości)	3 GHz – 30 GHz	10 cm – 1 cm	12,4 μeV
UHF	UHF (fale ultrakrótkie)	300 MHz – 3 GHz	100 cm – 10 cm	1,24 μeV
VHF	VHF (fale ultrakrótkie)	3 MHz – 300 MHz	10 m – 1 m	124 neV
HF	HF (fale krótkie)	3 MHz – 30 MHz	100 m – 10 m	12,4 neV
MF	MF (fale średnie)	300 kHz – 3 MHz	1 km – 100 m	1,24 neV
LF	LF (fale długie)	30 kHz – 300 kHz	10 km – 1 km	124 peV
VLF	VLF (fale bardzo długie)	3 kHz – 30 kHz	100 km – 10 km	12,4 peV
VF/ULF (częstotliwość głosu)	ULF (fale ultradługie)	300 Hz – 3 kHz	1000 km – 100 km	1,24 peV
SLF	SLF (superniskie częstotliwości)	30 Hz – 300 Hz	10 000 km – 1000 km	124 feV
ELF	ELF (ekstremalnie niskie częstotliwości)	3 Hz – 30 Hz	100 000 km – 10 000 km	12,4 feV

Zakresy radiowe fal długich (LW, 153 – 279 kHz), średnich (MW, 531 – 1620 kHz) i krótkich (SW, 2310 – 25 820 kHz) nie są uwzględniane w specyfikacjach ITU.

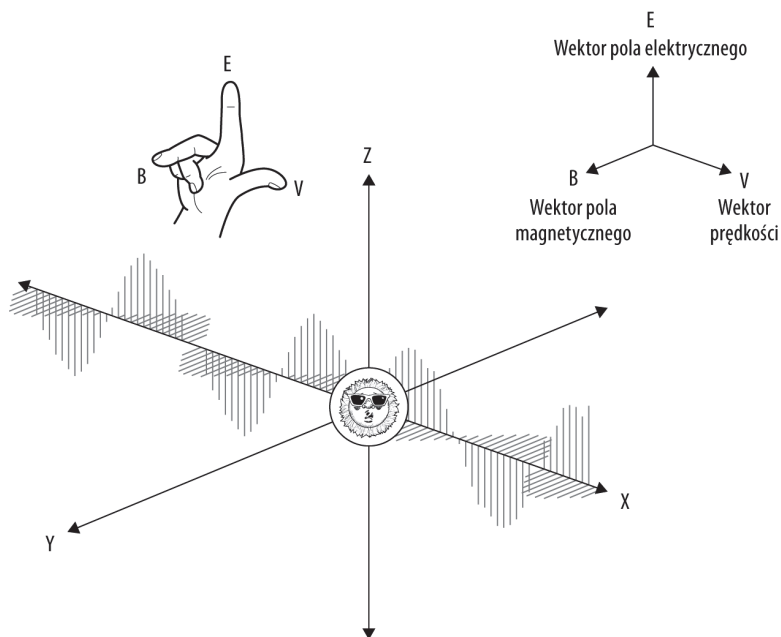
W muzyce dźwięki są podzielone na zakresy częstotliwościowe wyznaczane na podstawie potęgi dwójki, zwane *oktawami*. Oktawy wyznaczają również zakresy częstotliwościowe w widmie elektromagnetycznym. Z dwukrotnym wzrostem częstotliwości moc wzrasta czterokrotnie, czyli  $\pm 6$  dB na oktawa. Wzmacniacz lub filtr elektryczny cechuje się jednooktawową odpowiedzią, jeśli jego moc lub napięcie zmienia się czterokrotnie bądź o  $\pm 6$  dB. Wykorzystywane są również inne podziały częstotliwościowe bazujące na potędze dziesiątki — wyznaczające zakresy nazywane *dekadami*. Odpowiedź o mocy zwiększonej lub zmniejszonej dziesięciokrotnie oznacza zmianę o  $\pm 10$  dB na dekadę.

Detekcja sygnałów jest możliwa w zakresie 65 oktaw widma elektromagnetycznego (od fal radiowych do promieniowania gamma). Teoretycznie zakres ten można rozszerzyć do 81 oktaw, od możliwie najdłuższych fal (rozmiaru wszechświata) do długości określonej przez Plancka ( $1,6 \times 10^{-35}$  m), przy której załamują się prawa promieniowania elektromagnetycznego, odległość i czas stają się niemierzalne i nie można wymieniać żadnych informacji.

Promieniowanie elektromagnetyczne rozchodzi się w formie okresowych fal (oscylacji) opisanych na dwóch osiach, z czołem przesuającym się w kierunku zewnętrznym wzdłuż trzeciej osi. Ilustracją do tego opisu może być rysunek 18.12, w którym źródłem promieniowania jest Słońce. Emitowane światło jest spolaryzowane w jednym kierunku (na płaszczyźnie XZ). Polaryzacja upraszcza analizę rysunku 8.12 przez eliminację innych kołowych pól elektrycznych i magnetycznych.

### Rysunek 18.12.

*Promieniowanie elektromagnetyczne i propagacja fal*



Rozważając przedstawiony przykład, warto zwrócić uwagę na kilka elementów. Falę opisują wektory pola elektrycznego i magnetycznego, które mają jednakową wartość oraz fazę zależną od siebie nawzajem. Wektory te zostały przedstawione w prawym górnym narożniku rysunku. Rozchodzenie się fal elektromagnetycznych jest zgodne z regułą prawej dłoni, której ilustracja została pokazana w lewej górnej części rysunku 8.12. Zgodnie z nią kciuk

wskazuje kierunek przesuwania się fali (wielkość  $V$ , skierowana wzdłuż osi  $X$ ), palec wskazujący określa kierunek linii pola elektrycznego (wielkość  $E$ , skierowana wzdłuż osi  $Z$ ), a palec środkowy reprezentuje kierunek linii pola magnetycznego (wielkość  $B$ , skierowana wzdłuż osi  $Y$ ). Trzy wymienione osie opisują ruch, pole elektryczne oraz pole magnetyczne. Spolaryzowane światło przemieszcza się wzdłuż osi  $X$ . Pole elektryczne jest reprezentowane przez oscylacyjne zmiany amplitudy wzdłuż osi  $Z$ , natomiast pole magnetyczne — wzdłuż osi  $Y$ . Reguła prawej dłoni dostarcza również informacji o tym, który kierunek jest uznawany za dodatni — dodatni jest kierunek wskazywany przez palec. Warto o tym pamiętać podczas analizowania sposobu emitowania i odbierania sygnałów radiowych przez urządzenia bezprzewodowe.

## Informacja i transmisja

Widmo elektromagnetyczne jest wykorzystywane do bezprzewodowego przesyłania informacji w wyniku określonej modulacji (zmian) fali. Trzy najważniejsze metody modulacji zostały wymienione poniżej.

- ♦ **Modulacja impulsowa (PM — *Pulse Modulation*)**. Działanie modulacji impulsowej polega na włączaniu i wyłączaniu światła zależnie od wartości bitów danych. Jedyne logiczne odpowiada włączenie światła, a zero wyłączenie.
- ♦ **Modulacja amplitudy (AM — *Amplitude Modulation*)**. W modulacji AM dane są odwzorowywane w amplitudzie sygnału nośnego. Jeśli wspomniana amplituda przekracza pewną wartość progową, transmitowany bit jest jedynką logiczną. Jeśli amplituda pozostaje poniżej progu, reprezentuje zero logiczne. Modulacja polega na zsumowaniu sygnału nośnego z sygnałem danych.
- ♦ **Modulacja częstotliwości (FM — *Frequency Modulation*)**. W modulacji FM przekazywane informacje są odwzorowywane w zmianach częstotliwości sygnału nośnego. Gdy częstotliwość przekracza wartość progową, przesyłana jest jedynka logiczna. W przeciwnym razie transmitowane jest zero logiczne.

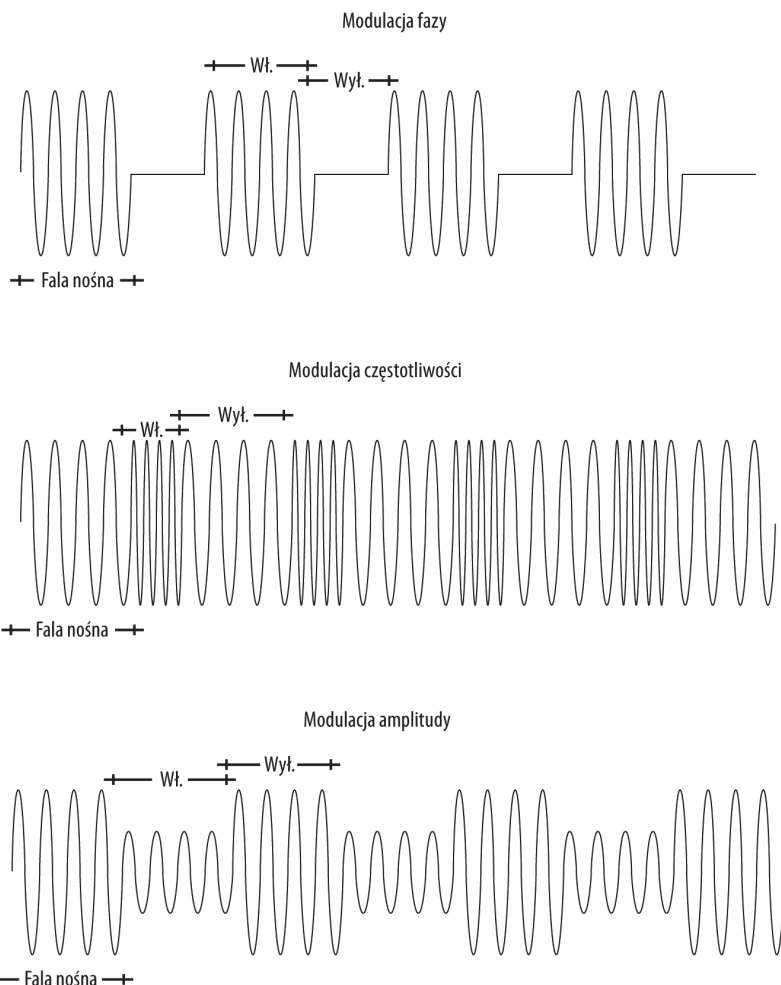
Wszystkie trzy wymienione techniki przekazywania sygnałów informacyjnych zostały przedstawione na rysunku 8.13. W górnej jego części znajduje się przykład modulacji impulsowej. Sygnał nośny jest w nim włączany i wyłączany w takt jedynek i zer logicznych. Podczas zmiany stanu z 0 na 1 zmienia się również faza przebiegu i to właśnie w zmianach fazy odwzorowywane są informacje użytkowe.

W środkowej części rysunku 8.13 przedstawiona została modulacja częstotliwości fali nośnej. Działanie mechanizmu polega na zwiększaniu częstotliwości przebiegu nośnego w chwili, gdy sygnał danych ma wartość jedynki logicznej (stan włączenia), oraz zmniejszaniu częstotliwości w reakcji na zero logiczne (stan wyłączenia). Zmiany te kodują więc informację.

Prawdopodobnie najłatwiejszą do zaprezentowania modulacją jest pokazana na dole modulacja amplitudy. Technika kodowania informacji sprowadza się do zwiększania amplitudy powyżej pewnej wartości progowej w odpowiedzi na jedynkę logiczną sygnału informacyjnego oraz zmniejszania amplitudy poniżej progu, gdy transmitowane jest zero logiczne.

**Rysunek 8.13.**

Trzy rodzaje modulacji  
umożliwiających  
przekazywanie danych  
w połączeniach  
bezprowadowych



Z teorii sygnałów wynika, że ilość informacji, którą można przesłać z użyciem fal elektromagnetycznych, jest z góry ograniczona niezależnie od systemu transmisyjnego. Aby zrozumieć istotę tego ograniczenia, należy wyznaczyć częstotliwość z zależności między częstotliwością, długością fali i prędkością światła, a następnie zróżniczkować względem długości fali, co prowadzi do uzyskania następującego równania:

$$(f / \lambda) = (c / \lambda^2)$$



Zależność między modulacją częstotliwości oraz modulacją amplitudy a mechanizmem multipleksowania sygnałów w transmisjach przewodowych została opisana w rozdziale 5.

Ponieważ informacje są przekazywane przez zmianę kształtu fali nośnej (na przykład amplitudy lub częstotliwości), interesująca jest jedynie częstość zmiany znaku równania. Innymi słowy, ważne jest to, ile razy w czasie sekundy pochodna zmienia znak. Równanie można więc przekształcić tak, aby uwzględniało skończoną liczbę różnic, dzięki czemu będzie się odnosiło do mierzalnych wartości:

$$\Delta f = (c \Delta \lambda) / \lambda^2$$

## Połączenia bezprzewodowe

Wszystkie połączenia cyfrowe obejmują kilka ogólnych komponentów, które niezależnie od częstotliwości (lub długości fali) muszą być wykorzystywane do przekazywania danych. Są to:

- ♦ nadajnik,
- ♦ medium transmisyjne,
- ♦ odbiornik.

W niemal wszystkich połączeniach komputerowych jako medium transmisyjne jest wykorzystywane powietrze lub próżnia. Nadajnik i odbiornik muszą być odpowiednio skonstruowane i wycenione. Zadaniem nadajnika jest wytworzenie fali elektromagnetycznej o określonej częstotliwości i mocy. Moc wiąże się z amplitudą fali — amplituda musi być dostatecznie duża, aby odbiornik określonego typu mógł rozpoznać sygnał po przesłaniu go na właściwą dla połączenia odległość. Przeanalizujmy zatem przykład transmisji radiowej.

### Łącza radiowe

Zgodnie z informacjami zawartymi w tabeli 8.5 transmisja radiowa obejmuje bardzo szeroki zakres częstotliwości. W ramach tego zakresu pewne pasma zostały wydzielone na potrzeby radioastronomii. Pasma te to według SETI: 3,36 – 13,41 MHz, 25,55 – 25,67 MHz, 73,00 – 74,60 MHz, 150,05 – 153,00 MHz, 406,10 – 410,00 MHz oraz 1400,0 – 1427,00 MHz. Pasma 73, 150 i 406 MHz są zajęte przez sygnały z pulsarów, a częstotliwość 1400 MHz odpowiada liniom widmowym wodoru. W radioastronomii do „połączeń” wykorzystuje się nadajniki o bardzo dużej mocy (pozwalające na transmitowanie sygnałów na ogromne odległości) oraz niezwykle duże anteny lub zestawy antenowe, z których część ma rozmiary zbliżone do kilometrowych. Zgodnie z klasyfikacją ITU pasma te znajdują się w przedziałach HF, VHF i UHF o długościach fal pomiędzy 100 m a 50 cm.

Nawet przy tak potężnych nadajnikach i detektorach sygnału ogromny dystans, który fale radiowe muszą pokonać, sprawia, że sygnału niemalże nie można odebrać. Aby uzmysłowić sobie, jak mała jest moc odbieranych sygnałów, wystarczy wziąć pod uwagę fakt, że całkowita ilość energii zgromadzonej przez wszystkie radioteleskopy od początku radioastronomii jest mniejsza niż energia potrzebna do zaświecenia żarówki przez milionową część sekundy. Odnosząc to do ciepła emitowanego przez źródło fal radiowych, można stwierdzić, że maksymalna temperatura fal nie przekracza kilku stopni powyżej zera absolutnego. Jest nieznacznie wyższa od promieniowania kosmicznego tła.

Radio AM nadaje na częstotliwościach między 520 kHz a 1620 kHz. W Stanach Zjednoczonych maksymalny poziom mocy nadawczej wynosi 50 000 W. Emitowane w ten sposób fale radiowe są odbierane w promieniu około 150 km (w czasie dnia) i mogą w pewnym zakresie przenikać do budynków. W nocy zasięg radia AM zwiększa się o setki kilometrów (w zależności od warunków propagacyjnych) dzięki odbiciu fal w jonosferze, czyli w warstwie atmosfery rozciągającej się na wysokości od 100 do 500 km.

Utrata mocy wynikająca z dookólnego sposobu nadawania sygnału jest funkcją  $1/r^3$ , gdzie  $r$  odpowiada promieniowi sfery wytworzonej wokół punktu źródłowego.

Nadajniki radiowe mogą być budowane również w taki sposób, aby wykorzystywały wyższe częstotliwości o krótszych długościach fali i większej mocy. Sygnały Wi-Fi o częstotliwości 2,4 GHz (i długości fali 12,5 cm) mają dostatecznie dużą moc, aby przenikać przez ściany. Typowe urządzenia Wi-Fi dysponują dostatecznie dużą mocą, aby inne urządzenia tego typu odbierały dane, gdy są oddalone od nadajnika o 50 lub 100 metrów. Jeśli wiązka nadajnika zostanie skierowana bezpośrednio do odbiornika, wówczas odległość między urządzeniami można wydłużyć do kilometra. Jednak skoncentrowanie wiązki oraz duża odległość sprawiają, że sygnał jest bardzo podatny na zakłócenia i nawet liście drzew mogą przeszkodzić w jego odebraniu. W transmisjach kierunkowych konieczne jest więc zwiększenie mocy nadawczej.

## Łącza mikrofalowe

Częstotliwości mikrofalowe są wykorzystywane w transmisji danych na długich dystansach, ponieważ zapewniają dużą szerokość pasma w łączach o bezpośredniej widoczności. Komunikacja mikrofalowa jest stosowana w łączach szkieletowych telefonii komórkowej, w łączach telewizyjnych i telefonicznych oraz połączeniach satelitarnych. Umożliwia bowiem uzyskanie wysokiej przepustowości przy niskich kosztach instalacji.

Przy częstotliwości około 200 MHz długość fali jest mniejsza niż 2 m, co pozwala na bardzo dokładne skupienie wiązki nadawczej oraz na efektywne zbieranie sygnału za pomocą czasz antenowych. W przypadku bezpośredniej widoczności urządzeń i transmisji z poziomu 30-kondygnacyjnego budynku sygnał musi być regenerowany co około 100 km.



W projektowaniu łączy mikrofalowych o bezpośredniej widoczności pomocne jest narzędzie Google Maps Microwave Link Planning Tool. Aby z niego skorzystać, należy wyświetlić stronę <http://members.chello.at/stephen.joung/indexDistanceElevation.html> i wpisać na niej współrzędne lokalizacji. Znajac wyniki, można przejść do strony [http://members.chello.at/stephen.joung/indexMW\\_Distance20.html](http://members.chello.at/stephen.joung/indexMW_Distance20.html), ustawić parametry łącza mikrofalowego i sprawdzić, jaki wpływ na wydajność będzie miała zmiana częstotliwości, mocy i rozmiaru anteny.

Mikrofałe w znacznie mniejszym stopniu przenikają do budynków niż fale radiowe, ponieważ fale krótsze charakteryzują się większą liczbą interakcji z materiałami stałymi. Dzięki temu kuchenki mikrofalowe spełniają swoje zadanie; nie produkuje się kuchenek pracujących na częstotliwościach radiowych. W „kuchniach radiowych” konieczne byłoby istotne zwiększenie mocy promieniowania.

Wraz ze wzrostem długości łącza mikrofalowego wiązka fal staje się coraz bardziej rozmyta i może być załamywana przez warstwy atmosferyczne. Dlatego podczas odbioru sygnału radiowego często dochodzi do zaników związanych z wielodrogowością sygnału i odstrajaniem się od częstotliwości wzorcowej. Ten sam efekt jest również zauważalny w transmisjach radiowych.

Czasami, gdy się słucha w samochodzie stacji radiowej o słabym sygnale, można zauważyć, że wystarczy przejechać samochodem kilka metrów (od jednego postoju do drugiego), aby jakość odbioru istotnie się zmieniła. Jest to efekt zaników wynikających z wielodrogowości sygnału.

W Stanach Zjednoczonych komunikacja bezprzewodowa jest realizowana w następujących zakresach częstotliwościowych:

- ♦ 1,7 MHz (AM),
- ♦ 27 MHz (FM),
- ♦ 43 – 50 MHz (FM),
- ♦ 902 – 928 MHz (ogólnoswiatowe pasmo do dowolnego wykorzystania, telefonia komórkowa i Wi-Fi),
- ♦ 1920 – 1930 MHz (ogólnoswiatowe pasmo do dowolnego wykorzystania, telefonia komórkowa),
- ♦ 2,4 GHz (ogólnoswiatowe pasmo do dowolnego wykorzystania, Wi-Fi),
- ♦ 5,8 GHz (ogólnoswiatowe pasmo do dowolnego wykorzystania, Wi-Fi).

Pasmo częstotliwości w zakresie od 2,4 GHz do 2,484 GHz jest przeznaczone do dowolnego wykorzystania na całym świecie. Często określa się je jako pasmo ISM (od angielskich słów oznaczających pasmo przemysłowe, naukowe i medyczne). W tym zakresie pracują urządzenia takie jak Wi-Fi, ponieważ nadawanie na tych częstotliwościach nie wymaga licencji nadawczych. Telefony komórkowe pracujące na częstotliwości 900 MHz z mocą 100 mW mają zasięg około 30 m.

## Podsumowanie

W tym rozdziale zostały opisane standardy okablowania stosowane w sieciach komputerowych. Szczególnie dużo informacji zamieszczono na temat skrętek oraz kabli współosiowych, a także ich zastosowań w sieciach Ethernet.

Z treści rozdziału można również się dowiedzieć, że włókna optyczne gwarantują połączenia o dużej szerokości pasma, a światło z lasera lub diody LED jest przesyłane wzdłuż szklanego lub plastikowego światłowodu jednomodowego bądź wielomodowego. Omówione zostały także fizyczne podstawy rozchodzenia się światła.

Ostatni temat to transmisja bezprzewodowa w powietrzu lub próżni z wykorzystaniem częstotliwości radiowych i mikrofalowych. Ta część rozdziału zawiera informacje na temat widma elektromagnetycznego oraz zasad wykorzystania go do przenoszenia informacji.

W kolejnym rozdziale zostały opisane sposoby „inteligentnego” łączenia urządzeń sieciowych.



## Rozdział 9.

# Routing, przełączanie i mostkowanie

### **W tym rozdziale:**

- ♦ Porównanie przełączania obwodów i przełączania pakietów
- ♦ Koncentratory, regeneratory, mosty, routery i bramy
- ♦ Techniki routingu
- ♦ Routery cebulowe

Działanie sieci wymaga wykorzystania urządzeń, które mogą tworzyć obwody komunikacyjne. W tym rozdziale zostały opisane i porównane koncentratory, mosty, przełączniki, routery i bramy. Ponadto jego tematyka obejmuje przełączanie obwodów i pakietów, czyli dwie podstawowe kategorie komunikacji sieciowej. Obwodem jest pewna zdefiniowana ścieżka między dwoma punktami końcowymi. Sieci z przełączanymi obwodami są rozwiązaniami stanowymi, które można opisywać w odniesieniu do punktów końcowych lub ścieżki między nimi. Dane przesyłane w obwodzie docierają do odbiorcy w określonej kolejności. Sieci pakietowe są rozwiązaniami bezstanowymi. Wyróżnia się w nich punkty końcowe, lecz ścieżka między tymi punktami może być inna dla każdego pakietu (zależnie od bieżących uwarunkowań).

Urządzenia przełączające klasyfikuje się, biorąc pod uwagę najwyższą warstwę modelu OSI, w której dane urządzenie funkcjonuje. Koncentratory i regeneratory są najmniej skomplikowanymi komponentami sieciowymi — są jedynie formą fizycznego przyłącza. Mosty to urządzenia, które łączą dwa różne segmenty sieci, ale nie zapewniają translacji protokołu. Routery mogą być przyłączone do dwóch sieci różnego typu. Natomiast przełączniki i bramy to określenia opisujące wiele różnych systemów.

## **Przełączanie obwodów i pakietów**

Przełączanie w sieci realizuje się w dwojaki sposób — poprzez przełączanie obwodów lub przełączanie pakietów. Sieć z przełączaniem obwodów jest definiowana przez fizyczne lub wirtualne obwody (połączenia), które spinają dwa punkty końcowe i zapewniają określoną

szerokość pasma. Obwód musi być zestawiony jedynie na czas przekazywania danych. Dzięki temu, że urządzenia przełączające mają zaimplementowane funkcje zestawiania różnych połączeń, sieć o przełączanych obwodach można konfigurować niemal dowolnie.

Najpopularniejszą siecią o przełączanych obwodach jest publiczna sieć telefoniczna (PSTN — *Public Switched Telephone Network*). Zainicjowanie rozmowy z drugą osobą wiąże się bowiem z utworzeniem obwodu między dwoma aparatami telefonicznymi, który jest utrzymywany przez czas trwania połączenia. Sieci o przełączanych obwodach są wykorzystywane zarówno do przenoszenia głosu, jak i transmisji danych. Kolejnym przykładem opisywanego rozwiązania jest sieć telefonii cyfrowej ISDN.

Aby zrozumieć, w jaki sposób działa sieć o przełączanych obwodach, wystarczy sobie przypomnieć, że jest ona siecią stanową. Oznacza to, że do opisu transferu komunikatów wykorzystuje się następujące elementy:

- ♦ źródło danych,
- ♦ jednostkę docelową,
- ♦ ścieżkę lub obwód,
- ♦ koszt wykorzystania ścieżki wynikający z czasu, wydajności lub innej metryki.

W przypadku sieci o przełączanych obwodach poszczególne jej komponenty można przedstawić w formie wierzchołków grafu, a połączenia jako krawędzie łączące poszczególne wierzchołki. Łatwiejsze staje się wówczas wyznaczanie ścieżek zdefiniowanych lub preferowanych przez graf, które są nazywane trasami. W praktyce komunikaty są przekazywane między punktami końcowymi w formie kompletnych jednostek transmisyjnych. Jeśli muszą zostać podzielone na wiele pakietów IP (datagramów), wszystkie pakiety zostaną przekazane tą samą trasą.

Sieć pakietowa działa na podstawie innego założenia — do przekazywania informacji jest wykorzystywana najlepsza z dostępnych tras. W rozwiązaniach tego typu pakiety są przekazywane z jednostki źródłowej do docelowej w ramach połączeń, które są uznawane za najlepsze w chwili przełączania pakietów. Opisana technika została opracowana z myślą o sieciach, które z założenia są zawodne i nie pozwalają na ustanawianie trwałych połączeń. W przypadku zerwania połączenia kolejny pakiet jest przesyłany przez inny węzeł w sieci. W sieciach pakietowych nie można zagwarantować, że dane będą przekazywane wzdłuż określonej ścieżki. Co więcej, pewna liczba pakietów nie zostanie w ogóle dostarczona do odbiorcy, co spowoduje ich usunięcie. W jednostce docelowej pakiety mogą być odbierane w innej kolejności, niż zostały wysłane. Z tego względu konieczne jest stosowanie mechanizmów, które zapewnią retransmisję utraconych pakietów oraz odtworzenie poprawnej kolejności odebranych danych.

Oczywiście typowym przykładem sieci pakietowej jest internet lub, ogólnie rzecz biorąc, sieci bazujące na protokole IP. Sieciami pakietowymi są sieci X.25, Frame Relay, ATM, MPLS i inne.

Najlepszym sposobem uświadomienia sobie, jakie jest przeznaczenie sieci pakietowych, jest zapamiętanie, że są to sieci bezstanowe. Bezstanowość oznacza, że transfer komunikatów można opisać za pomocą takich elementów, jak:

- ♦ źródło danych,
- ♦ jednostka docelowa,
- ♦ pozycja pakietu w sekwencji,
- ♦ czas życia pakietu (TTL — *Time To Live*), który może być zdefiniowany przez liczbę węzłów na trasie lub wartość czasu, po którego upływie pakiet jest usuwany (przez najbliższe urządzenie, które ten pakiet odbierze).



Terminy „obwód” i „połączenie” nie są wymienne. Połączenie opisuje transfer danych między dwoma punktami końcowymi i może mieć charakter stanowy lub bezstanowy.

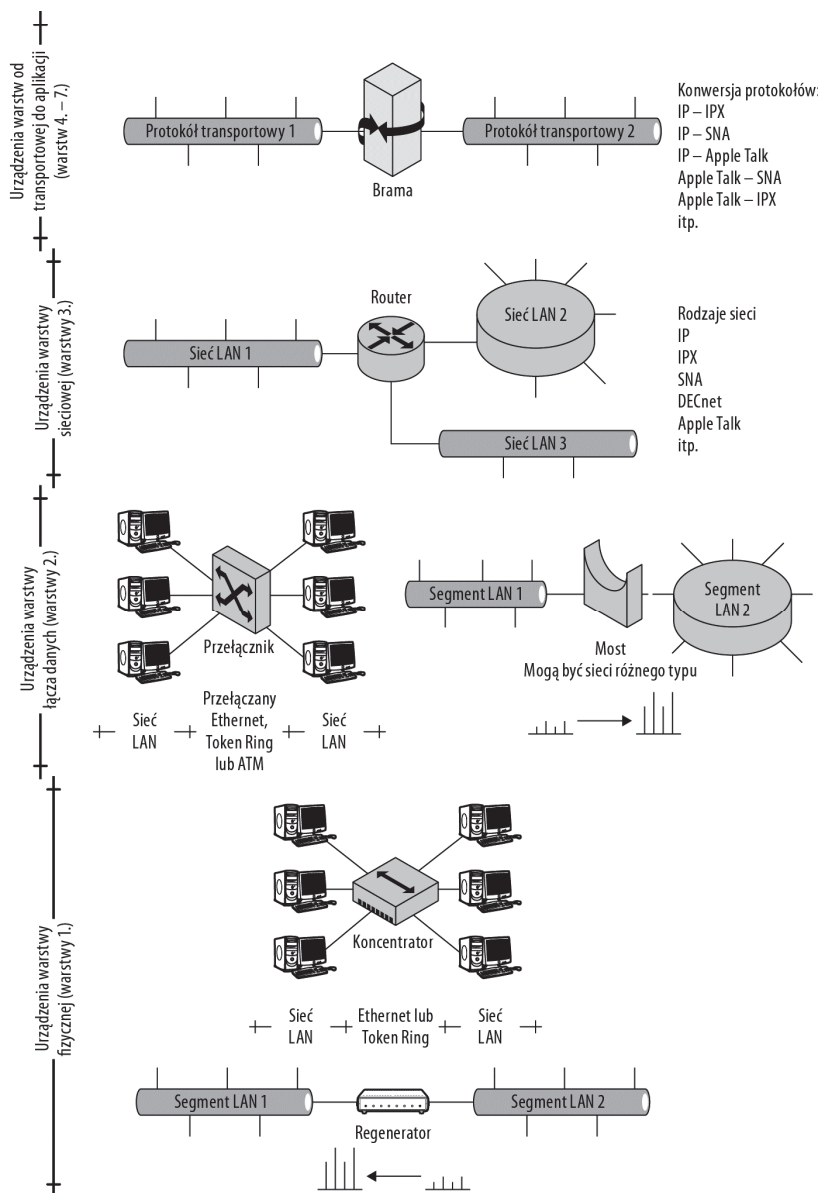
Zarówno sieci o przełączanych obwodach, jak i sieci pakietowe mają pewne wady i zalety. W sieciach o przełączanych obwodach cały komunikat jest przekazywany w ramach tego samego obwodu, co z pewnością jest szybsze niż przesyłanie poszczególnych fragmentów komunikatu różnymi trasami. Odbierane informacje docierają w odpowiedniej kolejności, więc nie trzeba tej kolejności odtwarzać. Z drugiej strony sieci pakietowe w znacznie lepszy sposób wykorzystują bieżącą pojemność sieci, ponieważ rozkładają ruch na wiele połączeń. Dodatkowy narzut związany z koniecznością odtwarzania kolejności odbieranych pakietów i obniżenie wydajności są rekompensowane przez wydajniejsze wykorzystanie sieci i znacznie większą niezawodność komunikacji. Nie można więc powiedzieć, który z modeli jest lepszy. Są one po prostu różne.

Cechą wspólną techniki przełączania obwodów i przełączania pakietów jest to, że bazują one na przełącznikach, które zmieniają topologię sieci. Aby zrozumieć sposób działania nowoczesnych sieci, trzeba najpierw zapoznać się z zasadami działania przełączników. Urządzenia te nie tylko wyznaczają fizyczne połączenia między segmentami sieci. Pewne klasy przełączników mają zaimplementowane funkcje pomiaru wydajności poszczególnych ścieżek, mechanizmy wyznaczania tras i optymalizacji preferowanych tras (tras do węzłów sieciowych, których definicje są przechowywane w specjalnej dynamicznej tabeli). Sieci szkieletowe nie funkcjonowałyby poprawnie bez urządzeń zapewniających wybór tras.

Na rysunku 9.1 zostało przedstawione zestawienie poszczególnych kategorii urządzeń sieci przełączanych. W ich klasyfikacji uwzględnia się najwyższą warstwę modelu OSI, w której działają. Urządzenia warstwy fizycznej (warstwy 1.) nie dysponują „inteligencją”. Są zwykłymi przyłączami fizycznymi lub łącznikami z funkcją regeneracji sygnału (jak w przypadku regeneratorów). Do urządzeń warstwy łącza danych (warstwy 2.) zalicza się przełączniki i mosty, które mają funkcje rekonfiguracji połączeń, parametryzowane przez system zarządzania urządzeniem.

Wszystkie wymienione dotychczas urządzenia działają w sieciach o podobnej konstrukcji, w których zazwyczaj pracują jednakowe protokoły. Aby połączyć sieci różnego typu, niezbędne są dodatkowe funkcje, co wymaga zastosowania urządzeń implementujących wyższe warstwy stosu protokołów. W łączeniu sieci istotną rolę odgrywają dwie klasy urządzeń — routery i bramy. Routery łączą sieci różnego typu na poziomie warstwy sieciowej (warstwy 3.). Natomiast bramy umożliwiają współdziałanie sieci o różnych protokołach i funkcjonują na poziomie warstwy transportowej i wyższych (warstwy 4. do 7.). Na rysunku 9.1 zostały one przedstawione w górnej części. Charakteryzują się znacznie większymi możliwościami przetwarzania ruchu, są w większym stopniu zarządzalne, a także kosztowniejsze.

**Rysunek 9.1.**  
Różne rodzaje urządzeń przełączających



Na rysunku 9.1 zostały wymienione poszczególne warstwy modelu OSI (po lewej stronie), od warstwy 1. (u dołu) do warstwy 7. (na górze). Każdej warstwie zostały przypisane odpowiednie urządzenia, czyli:

1. Warstwa fizyczna (warstwa 1.) — regeneratory i koncentratory.
2. Warstwa łączy danych (warstwa 2.) — przełączniki i mosty.
3. Warstwa sieciowa (warstwa 3.) — routery.
4. Warstwy od transportowej do aplikacji (warstwy od 4. do 7.) — bramy.

Wszystkie wymienione urządzenia zostały opisane w kolejnych punktach rozdziału. W treści opisów znajdują się również wyjaśnienia przyczyn takiej kategoryzacji urządzeń.

## Urządzenia warstw 1. i 2.

Urządzenia warstw 1. i 2. stanowią większość sprzedawanych obecnie komponentów sieciowych. Zalicza się do nich koncentratory, regeneratory, mosty i przełączniki. Regeneratory (aktywne koncentratory) oraz pasywne koncentratory są urządzeniami, którymi nie można zarządzać. Z kolei mosty i przełączniki mogą być komponentami zarządzalnymi. Urządzenia zarządzalne obsługują protokół SNMP i mogą być konfigurowane za pomocą oprogramowania przeznaczonego do zarządzania siecią. Elementy niezarządzalne nie mają funkcji zdalnej konfiguracji lub diagnostyki. Spośród wszystkich urządzeń opisanych w tym rozdziale przełączniki są komponentami najtrudniejszymi do scharakteryzowania. Nie zostały bowiem zdefiniowane przez żadną organizację standaryzacyjną, a poszczególni producenci implementują w nich mnóstwo różnych funkcji. Niemniej w kolejnych punktach zostały opisane zarówno przełączniki, jak i regeneratory, mosty i koncentratory.

### Koncentratory pasywne

Koncentrator jest nieskomplikowanym komponentem, który łączy urządzenia określonego segmentu sieci, zazwyczaj za pomocą skrętki lub kabla optycznego. Koncentrator jest elementem pasywnym, jeśli jego zadanie sprowadza się do zapewnienia połączenia między jednym urządzeniem a drugim. Z kolei koncentratorem aktywnym nazywa się komponent, który dodatkowo wzmacnia sygnał. Często pełni wówczas także funkcję regeneratora.

W modelu OSI koncentratory są zaliczane do elementów warstwy fizycznej i pełnią tę samą funkcję co zwykle przyłącza — rozszerzają segment sieci przez złączenie dwóch przewodów w jeden. Zazwyczaj koncentratory sieciowe są jednocześnie rozgałęźnikami i umożliwiają przyłączenie 4, 8, 16 lub większej liczby urządzeń. Koncentratory mogą działać jako urządzenia pasywne, które po prostu przenoszą sygnały między portami, lub jako komponenty aktywne, które wzmacniają (regenerują) sygnał.

Koncentratory nie realizują żadnych funkcji logicznych lub realizują je w niewielkim zakresie. Nie są też urządzeniami zarządzalnymi. Każdy pakiet dostarczany do portu koncentratora jest wysyłany przez wszystkie pozostałe porty. Poza tym wszystkie przyłączone do koncentratora jednostki należą do jednej domeny kolizyjnej. Konsekwencją takiego sposobu działania jest większa liczba kolizji niż w przypadku zastosowania urządzeń takich jak routery i przełączniki. Co gorsza, liczba kolizji rośnie wykładniczo wraz ze wzrostem liczby koncentratorów łączących urządzenia końcowe. Zgodnie z ogólnie przyjętą zasadą sieci ethernetowe o przepustowości 100 Mb/s nie powinny zawierać więcej niż dwa koncentratory łączące ze sobą trzy segmenty sieci.

Nowsze koncentratory działają jako wieloportowe regeneratory. Mają zdolność wykrywania kolizji, podczas której wysyłają sygnał zagłuszający, nakazując wszystkim urządzeniom zaprzestanie nadawania. Niektóre z koncentratorów mają nawet zaimplementowaną funkcję, która po wykryciu odpowiednio dużej liczby kolizji na jednym porcie uniemożliwia komunikację między tym portem a pozostałymi portami.

Koncentratory często są wyposażane w port uplink, który pozwala na łączenie ze sobą dwóch urządzeń w taki sposób, jakby stanowiły jeden koncentrator. Niekiedy zawierają również port umożliwiający utworzenie stosu koncentratorów o dużej wydajności. Porty przeznaczone do łączenia w stos są rozwiązaniami firmowymi, więc aby wdrożyć taką konfigurację, trzeba wykorzystać urządzenia jednego producenta.

W przeszłości główną zaletą koncentratorów była ich niska cena i duża niezawodność. Obecnie są to urządzenia uznane za przestarzałe i praktycznie niedostępne na rynku. Choć można jeszcze kupić koncentratory ethernetowe 10/100 Mb/s, większość ze sprzedawanych dzisiaj urządzeń to przełączniki (na pewno w przypadku urządzeń przeznaczonych do sieci gigabitowych). Ze względu na to, że większość komponentów sieciowych jest budowana na bazie układów logicznych dostarczanych przez niewielką grupę producentów, oraz z uwagi na nieduży koszt implementacji funkcji logicznych różnica w cenie między koncentratorom a przełącznikiem jest znikoma.

Większość urządzeń sprzedaje się jako przełączniki, nawet jeśli w ich nazwie występuje słowo „koncentrator” (ang. *hub*). Nowoczesne przełączniki są koncentratorami tylko wówczas, gdy wyłączą się w nich wszystkie dodatkowe funkcje i sprowadzi się je do roli prostych rozgałęźników umożliwiających przyłączanie urządzeń sieciowych.

## Regeneratory

Regeneratory (lub aktywne koncentratory) są urządzeniami warstwy fizycznej, które przedłużają zasięg fizycznego medium transmisyjnego przez wzmocnienie i odtworzenie zależności czasowych sygnału przed przekazaniem go do kolejnego odcinka trasy. Operacja ta jest konieczna, ponieważ wraz z przebytą odległością sygnał traci swój pierwotny kształt. Regenerator odtwarza poprawny przebieg sygnału, retransmitując go z właściwą fazą i częstotliwością. Regeneratory mogą łączyć ze sobą różne media fizyczne, rozszerzając jednocześnie domenę kolizyjną, ale bez wprowadzania nowego ruchu. Nie mogą natomiast łączyć sieci o różnej architekturze ani filtrować informacji. Przekazywanie sygnału przez regenerator wiąże się z wprowadzeniem pewnego dodatkowego opóźnienia, opisywanego jako opóźnienie propagacyjne. Cecha ta jest powodem ograniczenia liczby regeneratorów w jednym segmencie sieci.

W standardzie Ethernet są zdefiniowane dostatecznie duże odległości między urządzeniami, aby zaspokajały wymagania większości budowanych sieci LAN. Dlatego stosowanie regeneratorów nie jest powszechne. Większość regeneratorów ethernetowych sprzedaje się jako aktywne koncentratory, nazywane czasami wieloportowymi regeneratoremi. Kupienie regeneratorem okazuje się niezwykle trudne, ponieważ koncentratory i przełączniki są obecnie dostępne za relatywnie niską cenę. Z tego względu regeneratory ethernetowe są przez większość organizacji uznawane za urządzenia przestarzałe. Nie dotyczy to jednak wszystkich rodzajów sieci.



Korzystając z regeneratorów, należy wydzielić segmenty sieci o jednakowej długości w celu maksymalnego wykorzystania funkcji wzmacniania.

Ograniczony zasięg działania jest cechą charakterystyczną sieci bezprzewodowych w standardzie 802.11x. Dlatego często stosuje się w nich regeneratory, które mają na celu zwiększenie obszaru obejmowanego przez taką sieć. Choć można kupić specjalne regeneratory

bezprowadowe, zazwyczaj zadanie to jest realizowane przez punkty dostępowe skonfigurowane do pracy w trybie regeneratora (ang. *repeater*).

Regeneratory odgrywają również bardzo istotną rolę w łączach przenoszących fale świetlne. W zależności od tłumienia światłowodu niezbędne może się okazać umiejscowienie ich w określonych odległościach na trasie. Konfiguracja tego typu jest charakterystyczna chociażby dla sieci SDH, które przenoszą większość rozmów telefonicznych w Europie. Regeneratory okazują się więc bardzo użyteczne w sieciach WAN.

## Przełączniki

Przełącznik jest urządzeniem aktywnym, które łączy dwa segmenty sieci w ramach jednej warstwy lub większej liczby warstw modelu OSI. Termin *przełącznik* (ang. *switch*) jest stosowany w odniesieniu do różnorodnych urządzeń i w przeciwieństwie do *mostu* (ang. *bridge*), opisanego w standardzie IEEE 802.1D, nie jest zdefiniowany w żadnym zaleceniu. W rzeczywistości przełączniki funkcjonujące w warstwie 2. modelu OSI są zgodnie ze standardem IEEE 802.1D mostami, mimo że większość producentów sprzedaje je jako przełączniki. Przełączniki mają zdolność do wyznaczania wirtualnych obwodów dla przenoszonych przez nie ramek, ale często nie są wyposażane w funkcje dynamicznej rekonfiguracji tych obwodów (wymagają interwencji z zewnątrz). Zdolność do dynamicznej rekonfiguracji obwodów polega na możliwości przekazania ruchu z jednego portu na inny w zależności od bieżącej konfiguracji sieci lub w wyniku działania algorytmu optymalizacji.

Przełączniki mogą być urządzeniami zarządzalnymi lub niezarządzalnymi. Komponentów niezarządzalnych nie można konfigurować za pośrednictwem sieci. Natomiast urządzenia zarządzalne taką konfigurację umożliwiają. W przełącznikach zarządzalnych jest zazwyczaj wbudowany moduł agenta SNMP, a także interfejs wiersza poleceń (ang. *CLI* — *Command Line Interface*) lub interfejs WWW. Wśród przełączników wyróżnia się te, które udostępniają jedynie niewielki zbiór parametrów konfiguracyjnych, oraz urządzenia klasy enterprise (w pełni zarządzalne), które umożliwiają tworzenie i przechowywanie wielu konfiguracji. Przełączniki korporacyjne (klasy enterprise) zwykle mają większą liczbę portów i pozwalają na budowanie stosów zarządzanych przez administratora jak jedno urządzenie.

Analizując przełącznik, warto zwrócić uwagę na następujące cechy:

- ♦ **Porty** — liczba portów, możliwość zmiany priorytetów portów oraz funkcja monitorowania (kopiowania na wskazany port) ruchu (ang. *port mirroring*).
- ♦ **Szybkość** — szybkość portów oraz tryb duplexu wpływają na przepustowość przełącznika.
- ♦ **Agregacja połączeń** — zdolność do tworzenia wirtualnych portów (połączeń) składających się z kilku fizycznych portów (połączeń) w celu zwiększenia przepływności i niezawodności.
- ♦ **SNMP** — możliwość zarządzania urządzeniami za pośrednictwem sieci.
- ♦ **Filtrowanie** — możliwość klasyfikowania ruchu na podstawie cech urządzeń (na przykład filtrowanie na podstawie adresów MAC). Translacja adresów sieciowych (NAT) jest funkcją firewalla lub routera i zazwyczaj nie jest implementowana w przełącznikach, choć są odstępstwa od tej reguły.

- ♦ **Kontrola dostępu do sieci** — zdolność przełącznika do przyznawania urządzeniom dostępu do sieci w określonym zakresie na podstawie zdefiniowanych reguł.
- ♦ **VLAN** — zdolność do wydzielania wielu sieci logicznych w ramach większej sieci fizycznej, dzięki czemu uzyskujemy separację ruchu pomiędzy sieciami logicznymi.

Na rynku są dostępne przełączniki o funkcjach właściwych dla wszystkich warstw modelu OSI, od warstwy łącza danych do warstwy aplikacji. Jedynie urządzenia warstwy fizycznej — regeneratory i koncentratory — nie są nazywane przełącznikami.

W sieciach Ethernet wszystkie porty koncentratora odbierają te same dane, które w tym przypadku mają charakter rozgłoszeniowy — koncentratory nie wprowadzają segmentacji, co oznacza, że wszystkie połączenia należą do tej samej domeny kolizyjnej. Aby ograniczyć liczbę kolizji, koncentratory pracują w trybie półdupleksowym, współdzieląc połączenie. Przełączniki segmentują ruch w taki sposób, że każdy segment sieciowy dysponuje własną szerokością pasma, działa w ramach własnej domeny kolizyjnej (w której nie występują kolizje) i w trybie pełnego duplexu.

Prawdopodobnie najwłaściwszym opisem przełącznika jest przedstawienie jego funkcji w odniesieniu do poszczególnych warstw modelu OSI. W warstwie 2. przełącznik w zasadzie w pełni odpowiada zapisom standardu IEEE 802.1D definiującego most. Funkcje przełącznika realizowane na poziomie warstwy łącza danych zostały szczegółowo opisane w dalszej części rozdziału. Gdy przełącznik wykonuje zadania właściwe dla warstwy sieciowej modelu OSI, w rzeczywistości działa jak router — funkcja routingu również została opisana w dalszej części rozdziału. Wieloportowe urządzenia przełączające o dużym zagęszczeniu portów, nazywane przełącznikami typu director, są urządzeniami warstwy 3., wykorzystywanymi często w sieciach PSTN lub sieciach pamięci masowej bazujących na połączeniach Fibre Channel do łączenia setek urządzeń. Często ich działanie nie podlega prostym regułom kategoryzacji i należy je zaliczyć do usług dwóch lub nawet większej liczby warstw. Przełączniki tego typu są powszechnie nazywane przełącznikami wielowarstwowymi.

Istnieją również przełączniki warstwy 4. i warstwy 7. Przełącznik warstwy 4. odpowiada za translację adresów (NAT — *Network Address Translation*) oraz za równoważenie obciążenia między portami. Przełączniki warstwy 4. mogą również obejmować firewalles, bramy IPSec i koncentratory VPN. Najczęściej są one sprzedawane właśnie pod nazwą „firewall”, aby zwiększyć ich znaczenie na rynku. Przełączniki warstwy 7. udostępniają usługi warstwy aplikacji i pełnią zazwyczaj funkcję serwerów dostarczania treści lub urządzeń buforowania danych internetowych. Bardzo rzadko spotyka się przełączniki warstwy 7., nazywane rzeczywiście przełącznikami. Przeważnie określa się je mianem serwerów, ponieważ termin ten jest korzystniejszy z marketingowego punktu widzenia.

## Mosty

Most jest urządzeniem sieciowym, które łączy dwa segmenty sieci (jedną podsieć) na poziomie warstwy łącza danych. Mosty analizują docelowe adresy MAC przekazywanych ramek, ale nie przetwarzają w żaden sposób protokołów warstwy sieciowej, takich jak IP, IPX, NetBEUI lub inne. Mostów można używać także do łączenia sieci o różnych rodzajach medium fizycznego, np. 100Base-T i Wi-Fi lub 100Base-T i 100Base-TX.

W sieci Ethernet most jest przezroczystym, adaptacyjnym urządzeniem sieciowym, które odbiera dane z podłączonych do niego segmentów sieci. Na tej podstawie buduje tablicę mostowania (ang. *Forwarding Table*), w której przechowuje adresy MAC urządzeń i odpowiadający im segment sieci (port mostu). Porównując adresy MAC przychodzących ramek z tablicą mostowania, podejmuje decyzje o przełączeniu ramki do innego segmentu. Gdy w tabeli mostowania nie ma odpowiedniego wpisu, ramka zostaje wysłana na wszystkie porty z wyjątkiem portu źródłowego. Dopiero przetwarzając odpowiedź na tę ramkę, most rejestruje adres MAC zawarty w odpowiedzi i kojarzy go z określonym segmentem sieci. Adaptacyjne przełączanie jest operacją, która może być realizowana w jednym z trzech trybów:

- ♦ **Store and forward.** Technika ta polega na buforowaniu nadchodzących ramek, sprawdzaniu wartości kontrolnych, a następnie przekazywaniu ich do urządzeń docelowych.
- ♦ **Cut through.** Działanie tego mechanizmu polega na odczytaniu początkowej części ramki do pola adresu MAC, odszukaniu portu wyjściowego w tablicy przełączania i rozpoczęciu wysyłania przez port wyjściowy przed odebraniem całej ramki na porcie wejściowym. W rozwiązaniu tym nie występuje etap sprawdzania błędów.
- ♦ **Fragment free.** Przed rozpoczęciem przekazywania danych odczytywane są 64 bajty ramki. Zakłada się, że sprawdzenie początkowej części ramki wraz z adresem niemal zawsze pozwala wywnioskować, czy dane są nienaruszone lub czy wystąpiła kolizja, która sprawiła, że są one bezużyteczne.

Mosty w sieciach Token Ring wykorzystują inną metodę określania sposobu przekazywania ruchu, nazywaną mostkowaniem na podstawie trasy źródłowej (SRB — *source route bridging*). Przykładowy most przełącza ramki w odpowiednim kierunku na podstawie informacji, które zostały zawarte w tych ramach przez urządzenie nadające. Urządzenie nadające przed wysłaniem właściwych pakietów wysyła ramkę, której zadaniem jest zebranie informacji o sieci. Każdy most, który otrzymuje taką ramkę, rozsyła je na wszystkie swoje porty (oprócz źródłowego), jednocześnie dopisując informacje trasowania. Urządzenie docelowe odpowiada na każdą ramkę, używając do tego pełnej informacji trasowania. Urządzenie nadające wybiera trasę na podstawie różnych parametrów — najczęściej jest to trasa z ramki, która najszybciej wróciła.

Mosty znajdują zastosowanie przede wszystkim w konfiguracjach, w których wydzielone są dwie grupy komputerów komunikujących się intensywnie w ramach własnych grup i sporadycznie między grupami. Przykładem może tutaj być sieć obejmująca dwa piętra budynku, na których pracują zespoły finansowy i inżynierski. Innym przykładem wykorzystania może być wydzielenie klastrów systemów Linux i Macintosh. W każdej z opisanych sytuacji mosty zwiększają wydajność sieci przez partycjonowanie większości ruchu — ograniczenie ruchu do obszaru połowy sieci — i zmniejszenie liczby kolizji.

Jedyne urządzenia, które można kupić jako mosty, to punkty dostępu bezprzewodowego skonfigurowane do łączenia dwóch sieci lub dwóch segmentów sieci. W rozwiązaniach przewodowych działanie w charakterze mostu jest trybem pracy przełącznika. Dlatego czasami termin „przełącznik sieciowy” jest używany jako synonim mostu sieciowego. W większości przypadków pojęcie mostu lub mostu sieciowego odnosi się do sieci Ethernet, gdyż opisuje ono każde urządzenie zgodne ze standardem IEEE 802.1D. Opisany również w tym zaleceniu protokół drzewa rozpinającego (STP — *Spanning Tree Protocol*) został omówiony w dalszej części rozdziału (jest to protokół warstwy 2. zapobiegający powstawaniu pętli).

Oto kilka charakterystycznych cech mostu sieciowego:

- ♦ Most nie przetwarza żadnych protokołów sieciowych na poziomie wyższym niż wyznaczony przez protokół odwzorowania adresów (ARP).
- ♦ Most wydziela dwie domeny kolizyjne, przetwarzając i regenerując pakiety.
- ♦ Niezależnie od liczby dostępnych portów most dysponuje jednym portem, za którego pomocą są przekazywane informacje, oraz drugim, służącym do dystrybuowania informacji. Zatem od strony sieci most ma tylko jeden interfejs sieciowy.
- ♦ Most nie wykonuje operacji routingu, ale może filtrować ramki na podstawie ich adresów docelowych.
- ♦ W sieci może pracować dowolna liczba mostów, a ograniczenia nakładane na segment sieci nie odnoszą się do segmentu znajdującego się po drugiej stronie mostu.
- ♦ Dany port przynależy logicznie tylko do jednego mostu.
- ♦ Dodany do mostu port staje się portem niezarządzalnym, ponieważ mosty sieciowe konfiguruje się we własnym zakresie.

Mostem sieciowym lub niezarządzalnym przełącznikiem jest urządzenie, które nie dysponuje własnym adresem IP i które nie odpowiada na polecenia sieciowe takie jak ping. Funkcja przenoszenia datagramów między segmentami sieci przyłączonymi do mostu nie wymaga od samego mostu, by był on zarządzalny. Niemniej wiele urządzeń, na przykład przełączniki realizujące zadania logicznych mostów, umożliwia zdalne zarządzanie, dysponuje adresami IP, bierze udział w komunikacji SNMP i jest dostępnych za pośrednictwem usług SSH, TELNET lub RLOGIN. Za pomocą wymienionych mechanizmów można połączyć się z zarządzalnym przełącznikiem, aby przypisać adres IP do wirtualnego interfejsu, który z kolei pozwala na komunikację z innymi interfejsami sieciowymi. Ruch pochodzący z innych punktów końcowych sieci jest przenoszony przez zarządzalny most bez jakichkolwiek modyfikacji.

Osoby, które posługują się systemem Windows XP lub Vista, mogą skonfigurować programowy most sieciowy w ramach systemu operacyjnego. Most sieciowy w systemie Windows jest interfejsem wirtualnym, który obejmuje dwie lub większą liczbę sieci. Jeśli komputer jest wyposażony na przykład w kartę sieci stałej oraz kartę bezprzewodową, można wykorzystać funkcję mostkowania do udostępnienia komputerom działającym w każdej z sieci zasobów wydzielonych na komputerze-moście. Ponadto most sieciowy zapewnia systemom z jednej sieci dostęp do zasobów systemów znajdujących się po jego drugiej stronie.



Nie należy tworzyć mostów między połączeniem internetowym a siecią wewnętrzną, gdyż umożliwia to internautom uzyskanie dostępu do zasobów sieci wewnętrznej.

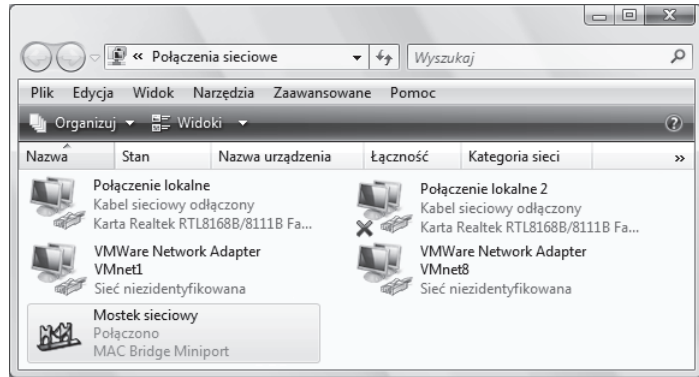
Aby utworzyć most sieciowy w systemie Windows, należy wykonać przedstawioną poniżej procedurę:

1. Otwórz folder *Połączenia sieciowe* (*Panel sterowania/Wyświetl stan sieci i zadania/Zarządzaj połączeniami sieciowymi*).
2. Trzymając naciśnięty klawisz *Ctrl*, kliknij połączenia sieciowe (interfejsy), z których chcesz utworzyć most.

3. Kliknij prawym przyciskiem myszy zaznaczony interfejs i wybierz opcję *Połączenia mostkowe*. Jeśli to konieczne, wpisz hasło administratora. Na rysunku 9.2 zostało pokazane okno *Połączenia sieciowe* w systemie Vista po utworzeniu mostu sieciowego.

**Rysunek 9.2.**

*Ikona mostu sieciowego w oknie połączeń sieciowych systemu Windows Vista*



Most sieciowy jest w tym przypadku wirtualnym interfejsem sieciowym, którym można operować tak samo jak każdym innym interfejsem systemu. Można na przykład wyświetlić odpowiadające mu okno *Właściwości*, dodać lub usunąć komponenty sieciowe, a nawet dodać kolejne interfejsy. Aby usunąć interfejs z mostu sieciowego lub cały most sieciowy, wystarczy wybrać opcję usunięcia z menu kontekstowego, wyświetlanego po kliknięciu ikony połączenia prawym przyciskiem myszy.

Mostkowanie i routing są dwiema metodami wyboru tras dla danych przekazywanych przez sieć. Jednak routing odnosi się do zadań realizowanych na poziomie warstwy sieciowej. Router kieruje ruch sieciowy do kolejnych węzłów na podstawie adresu logicznego, takiego jak adres IP, podczas gdy most posługuje się jedynie identyfikatorem sprzętowym (adresem MAC). Z tego względu routery dysponują informacją o tym, kiedy komunikacja obejmuje różne sieci, a mosty takich danych nie mają. Jako ogólną zasadę można przyjąć, że mosty są stosowane do łączenia segmentów sieci, natomiast routery pozwalają na łączenie różnych sieci. Mosty są tanimi urządzeniami — droższymi od koncentratorów i regeneratorów, lecz mniej kosztownymi niż przełączniki (zazwyczaj) i routery (zawsze). Ponieważ mosty buforują ramki w celu wyznaczenia ich dalszej trasy, cechują się mniejszą przepływnością niż regeneratory, których działanie ogranicza się do odtworzenia sygnału.

## Routery

Router sieciowy jest urządzeniem, które łączy dwie różne sieci. Routery wydzielają domeny kolizyjne, filtrują i blokują ruch rozgłoszeniowy oraz wyznaczają optymalne trasy dla pakietów. Wysokowydajne routery są po prostu efektywnymi komputerami, zdolnymi do przetwarzania dużej ilości danych w krótkim czasie.

Routery jako urządzenia logiczne pierwotnie były uruchamiane w formie serwerów o wielu interfejsach sieciowych. Jednym z pierwszych urządzeń tego typu był produkt firmy BBN Technologies (wcześniej Bolt, Beranek and Newman), zastąpiony ostatecznie przez systemy DEC PDP-11, przeznaczone do trasowania ruchu IP. W latach 80., gdy zaczęto komercjalizować internet, firma Sun Microsystems spopularyzowała tanie serwery SPARC, które wielu

dostawców usług internetowych kupowało z przeznaczeniem do wykonywania zadań routingu. W tym czasie rozpoczęła także swoją działalność firma Cisco, która przekształciła routery w niezależne urządzenia i zdominowała rynek ich producentów.

Funkcje routingu są implementowane w wielu sieciowych systemach operacyjnych, włączając w to systemy UNIX, Linux i Windows Server. Niewielki koszt systemu Linux sprawia, że bardzo często występuje on w roli routera. Również urządzenia firmy Cisco korzystają z systemu operacyjnego (IOS), lecz jest to oprogramowanie specjalnie przygotowane do wykonywania zadań związanych z routingiem i przełączaniem, udostępniające administratorom interfejs wiersza poleceń. Wiele rozwiązań opisanych w tym rozdziale jest wynikiem prac firmy Cisco. Inni dostawcy urządzeń stosują własne systemy operacyjne — w przypadku Juniper Networks jest to system (JUNOS), a firma Extreme Networks korzysta z systemu XOS.



Jeśli podstawowym przeznaczeniem routera miałyby być segmentacja ruchu (bez wykorzystania funkcji routingu lub translacji protokołów), warto się zastanowić nad wykorzystaniem mostu zamiast niego.

Wyznaczanie tras dla pakietów w małej sieci nie jest zadaniem szczególnie obciążającym procesor, więc wiele osób przekształca przestarzałe komputery w routery sieciowe. Oprogramowanie, które zapewnia realizację zadań routingu z użyciem komputera PC, to:

- ♦ **Quagga** ([www.quagga.net](http://www.quagga.net)) — usługa routingu przeznaczona dla systemów UNIX, Linux i Solaris, która bazując na projekcie Zebra, umożliwia korzystanie z protokołów OSPF, RIP i BGP (projekt typu open source).
- ♦ **SmoothWall** ([www.smoothwall.org](http://www.smoothwall.org)) — dystrybucja systemu Linux udostępniająca łatwy w użyciu graficzny interfejs użytkownika (projekt typu open source).
- ♦ **Untangle** ([www.untangle.com](http://www.untangle.com)) — aplikacja bramy, która tworzy router brzegowy wyposażony w funkcje antywirusowe, mechanizmy zapobiegające działaniu programów szpiegowskich, filtry, blokady oraz firewall (projekt typu open source).
- ♦ **XORP** ([www.xorp.org](http://www.xorp.org)) — otwarta rozszerzalna platforma routingu (*eXtensible Open Router Platform*) obejmująca obsługę protokołów RIP, OSPF, IGMP, BGP i innych. Aplikacja XORP jest dostępna w wersjach dla systemów Linux, Mac OS X (9.2 i późniejszych) oraz Windows Server 2003 (projekt typu open source).

Osoby interesujące się sieciami z pewnością słyszały określenie *brouter*. Brouter jest urządzeniem stanowiącym połączenie mostu (ang. *bridge*) i routera. Gdy do brouteru zostaną dostarczone pakiety protokołu routowalnego (takiego jak TCP/IP), będą przetworzone zgodnie z zasadami routingu (zostaną przeniesione z sieci źródłowej do docelowej). Natomiast wszystkie pakiety, które są przenoszone w ramach nieroutowalnego protokołu (takiego jak NetBEUI), są przekazywane zgodnie z zasadami działania mostu.

Sposób działania routerów jest charakteryzowany przez dwa oddzielne systemy funkcjonalne — warstwę sterującą i warstwę przełączania, które wybierają porty i przekazują dane do odpowiedniego interfejsu wyjściowego. Metodologia postępowania jest opisana przez wyrafinowane algorytmy odpowiedzialne za optymalizację wydajności sieci. W zależności od obsługiwanych przez router protokołów administrator może utworzyć różne topologie trasowania. Wiele aspektów funkcjonowania routerów zostało opisanych w punktach tego rozdziału.

## Warstwa sterująca

Routery składają się z dwóch płaszczyzn operacyjnych — *warstwy sterującej*, która wskazuje port wyjściowy uczestniczący w przekazywaniu pakietów do sieci docelowej, oraz *warstwy przełączania*, która przenosi odebrane pakiety z interfejsu wejściowego do wyjściowego. Warstwa sterująca uczestniczy w wymianie danych z innymi urządzeniami sieciowymi, mającej na celu zbudowanie tablicy routingu. Jest także odpowiedzialna za filtrowanie i blokowanie ruchu oraz za ewentualne zaimplementowane przez producenta mechanizmy QoS.

Warstwa sterująca przechowuje tablicę routingu, której podstawowe zadanie polega na gromadzeniu adresów wykorzystywanych w bezpośredniej komunikacji między dwoma punktami końcowymi. Administrator ma możliwość osobistego zdefiniowania tras statycznych lub określenia zasad wykorzystania takich tras. Niektóre wpisy w tablicy routingu mogą się odnosić do logicznych grup systemów, które są wykorzystywane w operacjach multimedii. Większość routerów, wykonując zadania routingu, polega na tablicach routingu lub bazach danych informacji o trasach (RIB — *Routing Information Base*). Niemniej niektóre z routerów utrzymują również bazy danych przełączania (FIB — *Forwarding Information Base*), które są zapisywane przez warstwę sterującą w pamięci w celu ich wykorzystania z poziomu warstwy przełączania.

Administratorzy sieci zwykle decydują się na włączenie routingu dynamicznego, który umożliwia danemu routerowi wymianę informacji na temat sieci z innymi routerami, a w konsekwencji na samodzielne wyznaczanie najlepszych tras przez sieć. Większość protokołów routingu dynamicznego pozwala na przypisanie routerowi priorytetu, który jest najważniejszym czynnikiem definiującym rolę routera oraz określającym to, w których trasach zostanie on uwzględniony.

Podczas wyznaczania tras przez sieć wykorzystywane są fizyczne połączenia routerów. Jednak nic nie stoi na przeszkodzie, aby utworzyć w routerze również logiczny interfejs sieciowy. Routery umożliwiają przypisywanie dowolnej liczby interfejsów logicznych do interfejsu fizycznego. Dzięki temu mogą obsługiwać wirtualne sieci LAN (VLAN). Obsługa sieci VLAN jest regulowana standardem IEEE 802.1Q. Część routerów współdziała także z protokołami tunelowania ruchu, takimi jak GRE i MPLS. Tunelowanie ruchu jest szczegółowo opisane w rozdziale 29.

## Warstwa przełączania

Warstwa przełączania (lub warstwa danych) jest tym komponentem routera, który weryfikuje pakiety w interfejsie wejściowym i transportuje je do odpowiedniego interfejsu wyjściowego. Routery zazwyczaj zawierają wiele warstw przełączania połączonych krzyżowo, dzięki czemu mogą przekazywać wiele strumieni równolegle. Poszczególne warstwy przełączania mogą być dodawane w formie kart rozszerzeń z układami ASIC przeznaczonymi do przetwarzania danych. Routery są bowiem wyposażane w płyty montażowe (ang. *backplane*) (mają budowę kasetową), w które wkłada się odpowiednie karty. Fizyczna budowa wielu routerów przypomina konstrukcję serwerów kasetowych. Aby zmierzyć wydajność routera, można zastosować technikę opracowaną przez grupę IETF Benchmarking Working Group (BMWG, RFC 2544); w technice tej się zakłada, że jedna połowa portów routera jest wykorzystywana do przesyłania pakietów adresowanych do drugiej połowy portów.

Działanie opisywanego podsystemu polega na wyszukiwaniu w tabeli wpisów, które odwzorują identyfikatory sieciowe (adresy MAC) na trasy. Zgodnie z informacjami przedstawionymi wcześniej system przełączania czasami wykorzystuje bazę FIB zamiast RIB, co przyspiesza wykonanie operacji. Przeszukiwanie baz danych bazuje na algorytmach zoptymalizowanych do przetwarzania adresów IP, w tym drzewach binarnych, strukturach typu radix tree i Patricia tree oraz innych rozwiązaniach opracowywanych przez producentów urządzeń.

Routerzy przechowują reguły określające, które pakiety należy przekazać, a które odfiltrować. Odfiltrowane pakiety zostają odrzucone. Nie towarzyszy temu odesłanie do nadawcy stosownego komunikatu ICMP. Zadania tego typu są bowiem realizowane po to, by router był niezauważalny dla hakerów. Jeśli w pamięci podręcznej routera lub w tablicy routingu nie występuje informacja, na której podstawie można podjąć decyzję o przesłaniu pakietu, a pakiet nie został odfiltrowany, router odsyła do nadawcy komunikat ICMP informujący o tym, że stacja docelowa jest nieosiągalna.

Ponieważ routery stanowią most między różnymi sieciami na poziomie warstwy sieciowej (warstwy 3.), pakiety o jednakowych protokołach sieciowych mogą być przekazywane bezpośrednio, bez szczególnego przetwarzania. Operacja ta często jest nazywana korzystaniem z szybkiej ścieżki przetwarzania. Pakiety wymagające dodatkowego przetwarzania są przekazywane wzdłuż wolniejszej ścieżki przetwarzania.

Routerzy realizują również inne zadania. Mogą służyć jako urządzenia zabezpieczające transmisję — szyfrujące transmisję w sposób właściwy dla zaimplementowanej technologii. Moduł odpowiedzialny za wykonywanie tych zadań jest często nazywany warstwą usługową. Sama realizacja wspomnianej funkcji wymaga od routera zdekodowania nagłówka pakietu w warstwie sieciowej, wyodrębnienia i przetworzenia danych zawartych w pakiecie i w razie potrzeby odczytania innych pól pakietu.

Routerzy mogą również wymuszać zachowanie odpowiedniego poziomu QoS, segregując pakiety, gdy jest to konieczne. Przepelnienie bufora wiąże się z tym, że router nie może przetwarzać nadchodzących danych i musi je odrzucać. Sposób wyboru pakietów do odrzucenia zależy od zastosowanego algorytmu. Najczęściej stosowane techniki to:

- ♦ **Algorytm odrzucania ostatnich pakietów (ang. *tail drop*).** Mechanizm zarządzania kolejką sprawdza zawartość bufora i gdy wykryje przekroczenie maksymalnego poziomu zapełnienia, odrzuca wszystkie nadchodzące pakiety, aż do zwolnienia miejsca. W rozwiązaniu tail drop nie stosuje się rozróżnienia na rodzaje pakietów, źródła danych lub inne właściwości, które miałyby wpływ na podejmowane decyzje.

Gdy system nadawczy przez pewien czas nie będzie odbierał segmentów ACK, uzna, że generowane przez niego pakiety są odrzucane. Wówczas znacznie zmniejsza częstotliwość wysyłania danych aż do uzyskania równomiernego strumienia potwierdzeń. Wadą mechanizmu tail drop jest to, że systemy nadawcze równocześnie rozpoczynają retransmisję pakietów, co prowadzi do zalewu danymi.

- ♦ **Wczesne losowe wykrywanie (RED — *Random Early Detection*).** Zasada działania tego algorytmu polega na monitorowaniu średniej długości kolejki i odrzucaniu pakietów na podstawie funkcji probabilistycznych. Uwzględnienie w działaniu algorytmu RED danych statystycznych daje gwarancję, że pakiety pochodzące ze źródła generującego duże ilości danych będą odrzucane z większym

prawdopodobieństwem niż pakiety wysyłane przez źródło dostarczające niewiele danych. W przypadku tego rozwiązania nie występuje problem zalewu pakietami (globalnej synchronizacji), charakterystyczny dla techniki tail drop.

- ♦ **Ważony algorytm RED i adaptacyjny (aktywny) algorytm RED.** Pierwszy z wymienionych algorytmów wykorzystuje technikę RED, ale dodatkowo przypisuje pakietom pewne wartości priorytetów. Z kolei adaptacyjny lub aktywny algorytm RED wprowadza zmiany w funkcji statystycznej w zależności od stanu kolejki.

## Topologie routingu

Routing (trasowanie) jest procedurą wyboru trasy, którą dane zostaną przesłane przez sieć. Routing jest niezbędny w każdej sieci, ponieważ wyznaczanie fizycznych obwodów odpowiadających każdej możliwej trasie transmisji danych jest po prostu niepraktyczne. W sieciach, w których ruch jest przekazywany od określonej stacji źródłowej do jednostki docelowej przez urządzenia pośrednie, istnieje możliwość wyznaczenia więcej niż jednej ścieżki. Dlatego sposób wyboru tras istotnie wpływa na wydajność sieci.

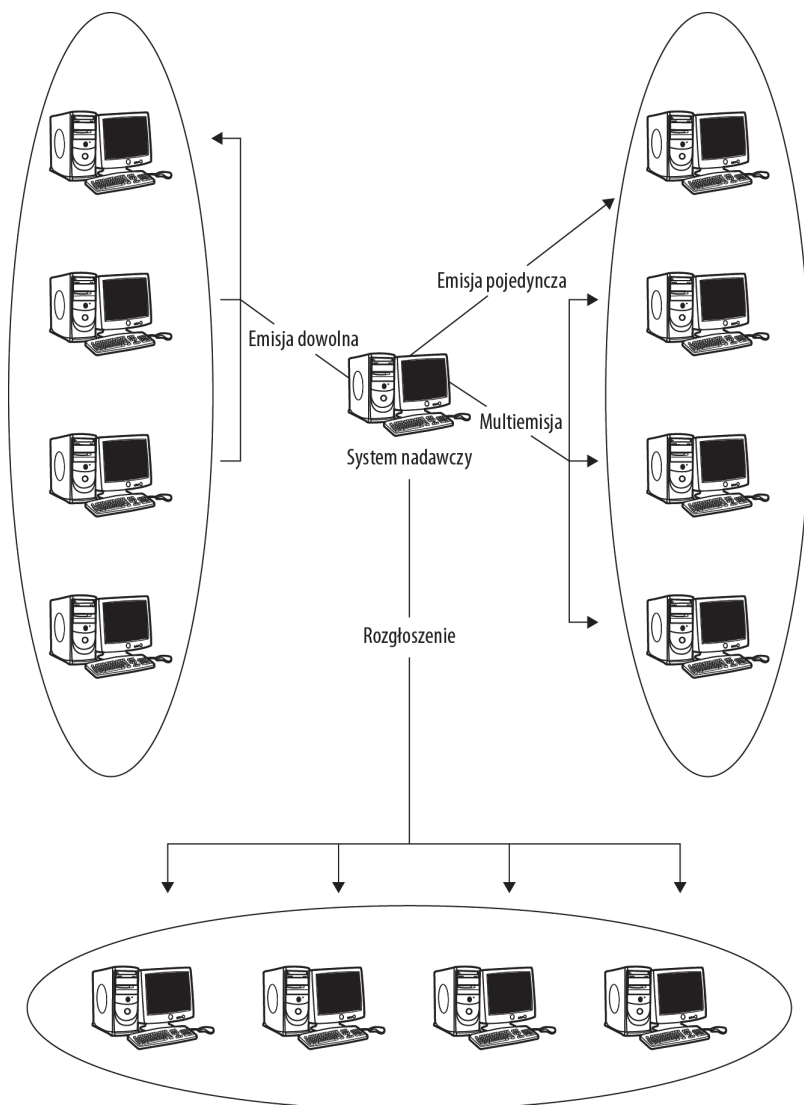
W procesie trasowania pakietów wyróżnia się cztery metody ich wysyłania:

- ♦ **Emisja pojedyncza (unicast)** — komunikat jest przesyłany z jednego węzła do innego węzła.
- ♦ **Rozgłoszenie (broadcast)** — komunikat jest wysyłany z jednego węzła do wszystkich pozostałych.
- ♦ **Multiemisja (multicast)** — komunikat jest wysyłany z jednego węzła do grupy węzłów (zazwyczaj tych węzłów, które zażądały dostarczenia komunikatu).
- ♦ **Emisja dowolna (anycast)** — komunikat jest wysyłany z jednego węzła do dowolnego (dowolny węzeł grupy może odebrać wiadomość i ją wykorzystać). Dostarczenie komunikatu kończy komunikację.

Wszystkie cztery wymienione topologie trasowania zostały przedstawione na rysunku 9.3. Każda elipsa reprezentuje oddzielną sieć lub podsieć.

Routing jest istotny nie tylko ze względu na fakt, że nie można fizycznie utworzyć wszystkich potencjalnych połączeń. Zainstalowanie sprzętu nie stanowi bowiem rozwiązania problemu. Wyobraźmy sobie sytuację, w której po zaobserwowaniu dużego natężenia ruchu między dwoma punktami końcowymi administrator tworzy łącznie szkieletowe o podobnej pojemności, ale o mniejszej długości i większej szybkości działania. Routery wykrywają nowe połączenie i ustalają, że jest ono trasą o najniższym koszcie. Cały ruch zostaje wówczas skierowany do nowego łącza szkieletowego, wysycając je i ograniczając ogólną wydajność sieci. Opisana sytuacja jest znana jako paradoks Braessa. Gdy wybór tras ogranicza się do wyszukiwania ścieżki o najniższym koszcie, dodatkowa pojemność sieci zostanie całkowicie wyczerpana, co w niektórych przypadkach może prowadzić do obniżenia wydajności systemu. Analogiczną zależność zaobserwowano w Bostonie, gdzie zamknięcie bardzo obciążonej drogi spowodowało rozłożenie ruchu na inne ulice, prowadząc w konsekwencji do zwiększenia efektywności transportu.

**Rysunek 9.3.**  
Cztery topologie  
trasowania



Paradoks Braessa wynika z teorii gier opracowanej przez Johna Forbesa Nasha, fizyka z uniwersytetu w Princeton, który za swoją pracę otrzymał Nagrodę Nobla. Zgodnie z zasadą równowagi Nasha w dowolnym systemie z wieloma graczami, w którym każdy gracz działa we własnym interesie, biorąc pod uwagę postępowanie innych uczestników gry, żadnemu z graczy nie opłaca się jednostronnie zmienić strategię, gdyż nie przyniesie to dodatkowych korzyści. Z twierdzenia tego wynika, że systemy pozostające w równowadze Nasha nie zawsze uzyskują najlepsze wyniki jako całość. Aby osiągać najlepsze indywidualne rezultaty, od równowagi Nasha muszą odstępować całe grupy systemów.

To jest przestrzeń działania protokołów routingu. Aby routing był efektywny, musi mieć dynamiczny charakter. W dynamicznych systemach sieć reaguje na zdarzenia w celu kontynuowania pracy i wybiera trasy do grup systemów, których poszczególne systemy samodzielnie

nie byłby w stanie wybrać. Na przykład jeśli koparka zniszczy ułożony w ziemi kabel telefoniczny, adaptacyjny protokół routingu doprowadzi do przekazania ruchu do innego łącza. Analogicznie, jeśli krótkie, wysokowydajne łącze stanie się dostępne, mechanizm routingu dynamicznego rozłoży ruch w taki sposób, aby obciążenie całego systemu było równomierne. W konkretnym analizowanym przypadku wybrana trasa może się okazać dłuższa, ale całkowita wydajność systemu będzie optymalna.

## Metody optymalizacji

W niewielkich sieciach administrator może osobiście zdefiniować preferowane trasy między punktami końcowymi, dodając wpisy do tablicy routingu. Rozwiązanie to okazuje się niepraktyczne w sieciach o dużym rozmiarze. Z tego względu wykorzystuje się w nich trasy, które zostały wstępnie obliczone lub są obliczane na bieżąco w przypadku wystąpienia takiej konieczności. W sieciach PSTN stosuje się rozwiązania, w których tablice są wstępnie wypełniane preferowanymi (wyliczonymi) trasami oraz trasami zapasowymi. Wraz z rozwojem sieci telefonicznej zaczęto wprowadzać technologie routingu adaptacyjnego, których tablice routingu były generowane przez protokoły routingu i mogły uwzględniać automatyczne zmiany tras. W przypadku internetu mechanizm routingu jest całkowicie inny — jest w pełni dynamiczny.

Mechanizmy routingu są wdrażane w ramach systemów autonomicznych lub między systemami autonomicznymi. Systemem autonomicznym (AS — *Autonomous System*) nazywa się zbiór jednostek działających w ramach wspólnej struktury administracyjnej. Systemem autonomicznym może być sieć, grupa sieci, zbiór sieci dostawcy usług internetowych lub cały internet. Protokoły routingu działające w systemach autonomicznych są nazywane protokołami bram. Protokoły bram wewnętrznych (IGP — *Interior Gateway Protocol*) są stosowane do przenoszenia pakietów w ramach sieci systemu autonomicznego. Typowymi przykładami protokołów IGP są protokół informowania o trasach (RIP — *Routing Information Protocol*), opracowany przez firmę Cisco protokół routingu bramy wewnętrznej (IGRP — *Interior Gateway Routing Protocol*), otwarty protokół wyszukiwania najkrótszych tras (OSPF — *Open Shortest Fast First*) i protokół łączenia systemów pośrednich (IS-IS — *Intermediate System to Intermediate System*). Protokoły bram zewnętrznych (EGP — *Exterior Gateway Protocol*) obejmują pierwotny standard EGP (obecnie uznany za przestarzały) oraz protokół bramy brzegowej (BGP — *Border Gateway Protocol*). Poszczególne protokoły routingu są omówione dalej.

## Algorytm wektora odległości

Algorytm wyznaczania wektora odległości (DV — *Distance Vector*) wyraża koszt trasy liczbą przeskoków pakietu (liczbą węzłów na trasie). Dane są przekazywane wzdłuż trasy, której sumaryczna liczba przeskoków jest najniższa. Każdy węzeł w sieci tworzy własną tablicę odległości i przekazuje ją do węzłów sąsiednich. Routing DV jest bardzo popularnym rozwiązaniem w sieciach pakietowych i jest podstawą działania protokołów RIP (w wersji 1. i 2.) oraz IGRP. Podobna metodologia działania została uwzględniona w protokołach BGP, czyli w podstawowym protokole internetowym, oraz EGP, czyli w starszej i obecnie niestosowanej wersji protokołu routingu zewnętrznego.

Sam algorytm wektora odległości nie wykrywa pętli w sieci i nie eliminuje ich, dlatego protokoły routingu wykorzystujące ten algorytm są wyposażone w szereg dodatkowych mechanizmów pozwalających na wyeliminowanie tego problemu. Tablice routingu są budowane na podstawie informacji o możliwych trasach dostarczania pakietów, zoptymalizowanych w odniesieniu do poszczególnych odcinków połączeniowych. Optymalizacja wyznaczonych tras polega na użyciu algorytmu Bellmana-Forda w odniesieniu do danych zawartych w tablicy routingu. W wyniku jego działania informacje o preferowanych trasach są przekazywane do routerów sąsiednich, które aktualizują własne tablice routingu.

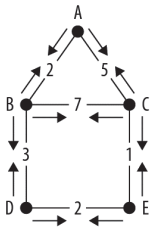
## Algorytm Bellmana-Forda

Algorytm Bellmana-Forda prowadzi do wyznaczenia najkrótszej trasy w grafie o ważonych krawędziach. Mechanizm został opracowany niezależnie przez Richarda Bellmana w 1958 roku oraz Lestera Forda Jr. w 1956 roku. Większość protokołów bazujących na algorytmie Bellmana-Forda wykorzystuje jego wersję rozproszoną. Rozproszony algorytm Bellmana-Forda zakłada użycie trzech mechanizmów w celu zapewnienia tablicy routingu w każdym z węzłów:

- 1. Stan początkowy.** Każdy router zawiera tablicę routingu z trasami (wektorami) do bezpośrednio przyłączonych sieci. Poszczególne wpisy składają się z trzech wartości [cel, dystans, następca]. Następcą jest router lub węzeł o jeden krok bliżej celu (jest to kolejny węzeł na trasie) i jest jednocześnie najbliższym sąsiadem analizowanego routera. Dystans może być wyrażony liczbą przeskoków pakietu lub wartością kosztu wyznaczoną na podstawie przepustowości połączenia lub innego czynnika.
- 2. Wysyłanie.** Każdy węzeł wysyła znane sobie wektory tras [cel, dystans] do bezpośrednich sąsiadów. Operacja jest ponawiana okresowo (zależnie od ustawień z interwałem od sekundy do minuty) oraz każdorazowo po zmianie wpisu w tablicy routingu.
- 3. Odbieranie.** Każdy router oblicza koszt tras do sieci odległych na podstawie informacji odebranych od najbliższych sąsiadów. Po zaktualizowaniu tablicy routingu router przystępuje do realizacji kroku 2. i wysyła nowe informacje do najbliższych sąsiadów.

Opisana operacja została zilustrowana na rysunku 9.4. Tablica routingu przedstawiona w górnej części rysunku jest wypełniona informacjami o najbliższych sąsiadach. Ponieważ router A nie zna najkrótszej trasy do routera E, pole wektora jest puste. Środkowa tablica routingu reprezentuje stan po przesłaniu pierwszej aktualizacji z węzła D do B. W wyniku tej operacji router B może uzupełnić pole wektora opisującego trasę z B do E wartością 5. Choć nadal nie ma pewności, czy jest to najniższy koszt przejścia z B do E. Do czasu uzupełnienia wektora E-C router B nie ma informacji o tym, że trasa B-D-E rzeczywiście ma najniższy koszt (wartość 5) — trasa B-C-E ma koszt 8. Dolna tablica routingu odzwierciedla stan po zaktualizowaniu tablic routingu najbliższych sąsiadów, przesłaniu aktualizacji z węzła E do C i wykonaniu dostatecznej liczby aktualizacji, aby tabela wypełniła się wektorami o najniższych kosztach.

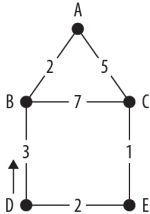
**Rysunek 9.4.**  
Algorytm Bellmana-Forda wypełniający  
tablice routingu



1. Etap początkowy. Pobranie wektorów od routerów sąsiednich

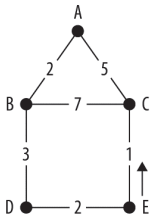
		Odległość				
Wektory	—	A	B	C	D	E
	A	0	2	5	—	—
	B	2	0	7	3	—
	C	5	7	0	—	1
	D	—	3	—	0	2
	E	—	—	1	2	0

2. Aktualizacja wektorów pobranych z routerów D i B. Powtórzenie kroku 1.



		Odległość				
Wektory	—	A	B	C	D	E
	A	0	2	5	—	—
	B	2	0	7	3	5
	C	5	7	0	3	1
	D	—	3	—	0	2
	E	—	—	1	2	0

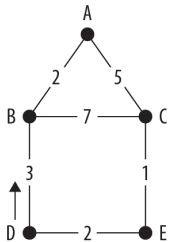
3. Zapisanie wektorów o najniższym koszcie (po kilku aktualizacjach)



		Odległość				
Wektory	—	A	B	C	D	E
	A	0	2	5	5	6
	B	2	0	6	3	5
	C	5	6	0	3	1
	D	5	3	3	0	2
	E	6	5	1	2	0

Tablica routingu przechowywana w poszczególnych routerach ma format podobny do przedstawionego na rysunku 9.5, różniący się od zestawienia najniższych kosztów zaprezentowanego na rysunku 9.4. Jako przykład pokazana została tablica routera B, której wektory [cel, dystans, następca] zaprezentowano w formie tabeli. Każdy wiersz odpowiada określonemu celowi, kolumna wyznacza następcę, a dystans jest wpisany w polu tabeli.

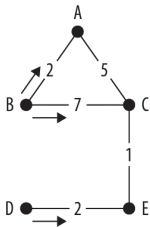
**Rysunek 9.5.**  
Tablica routingu  
pojedynczego routera  
— w tym przypadku  
routera B



		Następny router		
Cel	—	A	C	D
	A	2	12	8
	C	7	7	6
	D	7	10	3
	E	8	8	5

Przeanalizujemy, co się stanie, gdy połączenie między węzłami B i D zostanie uszkodzone (rysunek 9.6). Przerwa zostanie wykryta przez obydwa routery. Każdy z nich wyśle więc natychmiast aktualizację do najbliższych sąsiadów. W wyniku tej operacji w tablicy routingu zmienia się wiele wektorów. Wartość każdego z nich została pogrubiona.

**Rysunek 9.6.**  
Wpływ przerwania  
łącza na tablicę  
routingu



Uszkodzenie połączenia B-D. Wysłanie aktualizacji z routerów B i D

	Odległość					
	—	A	B	C	D	E
Wektory	A	0	2	5	8	6
	B	2	0	6	10	8
	C	5	7	0	3	1
	D	8	10	3	0	2
	E	6	8	1	2	0

**Liczenie do nieskończoności**

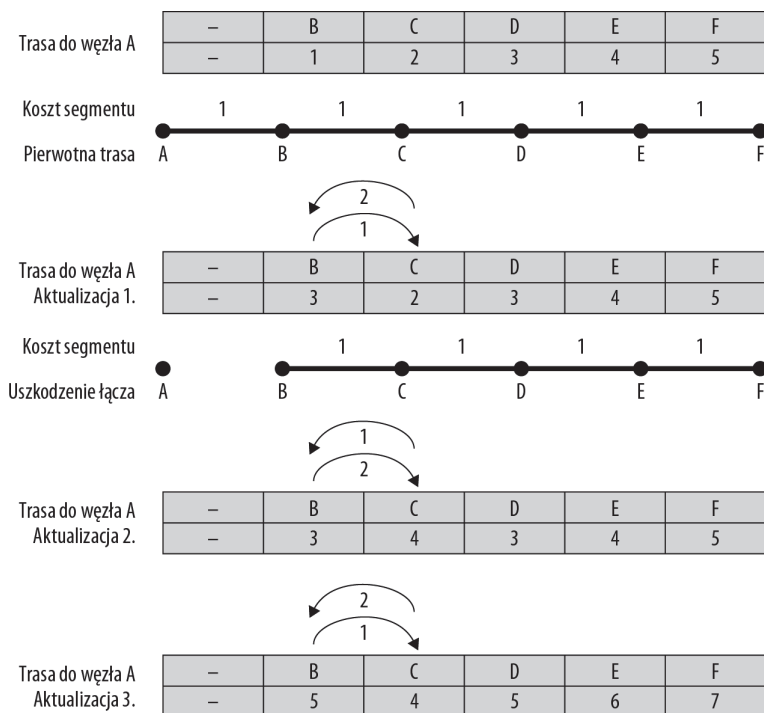
W systemie DV każda zmiana w sieci (uszkodzenie łącza lub urządzenia) jest wykrywana w czasie okresowej aktualizacji tablicy routingu. Wówczas wpisy odnoszące się do danego łącza lub urządzenia są modyfikowane lub usuwane. Zmiany są następnie propagowane do węzłów sąsiednich. Przekazywanie informacji jedynie pomiędzy węzłami jest procesem znacznie wolniejszym niż jednorazowe zaktualizowanie wszystkich węzłów sieci, choć wymaga mniejszej szerokości pasma i mniejszej mocy obliczeniowej. Oznacza jednak, że zanim ostatnie węzły zostaną poinformowane o zmianach, mogą prowadzić komunikację, wykorzystując pierwotne dane jako poprawne. Problem ten nazywa się problemem liczenia do nieskończoności.

Przeanalizujmy trasę z węzła A do F, wzdłuż której każdy skok (segment) ma koszt o wartości 1. Przypadek ten został zilustrowany na rysunku 9.7. Załóżmy, że połączenie A-B ulega uszkodzeniu, a router B wykrywa problem. Jednak pierwsza wymieniana aktualizacja jest przekazywana z routera C do B. Na jej podstawie węzeł B uznaje, że router C zna trasę do węzła A, a koszt tej trasy to 2 skoki. Węzeł B aktualizuje swoją tablicę routingu — dodaje koszt przejścia B-C do kosztu raportowanego przez węzeł C i umieszcza wartość 3 w swojej tablicy routingu. Jednocześnie przyjmuje, że trasa do węzła A wiedzie przez węzeł C. Router C nadal uznaje, że węzeł B jest najbliższym pośrednikiem na trasie do A, i gdy odbiera aktualizację z routera B (o wartości 3), zmienia wartość kosztu na 4. Zmiana jest wprowadzana również we wszystkich routerach za węzłem C. Trzecia aktualizacja powieliła błąd pierwszej aktualizacji — węzeł B zmienia koszt przez dodanie do wartości zapisanej w węźle C kosztu przejścia z B do C. Procedura wykonuje się nieskończenie długo, prowadząc do zatrzymania ruchu sieciowego. Rozwiązaniem jest zastosowanie techniki relaksacji, w której okresowo sprawdza się, czy istnieje trasa o mniejszym koszcie niż ten, który jest wpisany do tablicy routingu.

**Protokół RIP**

Pierwszym i zarazem najbardziej znanym protokołem wykorzystującym algorytm wektora odległości jest protokół informowania o trasach RIP. Znajduje on zastosowanie w sieciach wewnętrznych systemu autonomicznego zarówno w połączeniach LAN, jak i WAN. Pierwsza wersja protokołu została opisana w zaleceniu IEEE RFC 1058 w roku 1988. Wersja druga jest zdefiniowana w dokumencie RFC 2453. RIP był pierwszym protokołem routingu stosowanym w internecie. W rozwiązaniu tym metryką kosztu jest liczba przeskoków. Maksymalna liczba węzłów na trasie wynosi 15, a czas przetrzymywania jednej trasy (bez odświeżenia wpisu) wynosi 180 sekund. Interwał ponawiania okresowych aktualizacji oscyluje nieznacznie wokół standardowej wartości (30 sekund), dzięki czemu routery nie są obciążane zbyt wieloma aktualizacjami w jednym czasie.

**Rysunek 9.7.**  
Problem liczenia  
do nieskończoności



Dawniej protokół RIP był stosowany powszechnie, jednak obecnie jest uznawany za mniej efektywny niż protokoły stanu łącza, takie jak OSPF czy IS-IS (zdefiniowany przez organizację ISO). Opracowano również wersję RIP (o nazwie RIPng) przeznaczoną do współdziałania z protokołem IPv6, w której dodatkowo zaimplementowano rozwiązania gwarantujące, że przedawnione lub niekompletne informacje nie są przekazywane w sieci. Jeden z mechanizmów — nazywany *dzielonym horyzontem* — uniemożliwia routerowi przesyłanie informacji o trasie do węzła, od którego pozyskał informację o tej trasie.

Mechanizm dzielonego horyzontu skutecznie eliminuje problem liczenia do nieskończoności i zabezpiecza sieć przed powstawaniem pętli routingu. W przypadku rozpatrywanym powyżej router C w aktualizacji wysyłanej do routera B pominie informacje o trasach prowadzących przez router B. Dzięki temu w przypadku uszkodzenia połączenia A-B router C nie przekaże aktualizacji do routera B o trasie do routera A wiodącej przez B, co zapobiegnie powstaniu pętli.

Istnieje odmiana metody dzielonego horyzontu — technika *dzielonego horyzontu z zatrzymaniem wstecznym*. Trasy wsteczne są rozgłaszane, jednak w momencie, kiedy router wykryje, że regularnie otrzymuje trasę do zdalnego systemu ze zwiększoną metryką, w swojej aktualizacji zwrotnej zatrzuwa tę trasę poprzez zwiększenie metryki do 16 (dla protokołu RIP — sieć nieosiągalna). Technika dzielonego horyzontu jest wykorzystywana również w protokołach IGRP, EIGRP oraz w usłudze wirtualnych sieci prywatnych (VPLS — *Virtual Private LAN Service*).

## Algorytm wektora odległości z numerami sekwencyjnymi

Algorytm wektora odległości z numerami sekwencyjnymi sieci docelowych (DSDV — *Destination-Sequenced Distance Vector Routing*) jest pewną odmianą systemu DV przeznaczoną do wykorzystania w tworzonych ad hoc sieciach Wi-Fi (sieciach mobilnych). W rozwiązaniu DSDV do tablicy routingu został dodany jeden parametr — numer sekwencyjny, który jest przypisywany do określonego łącza. Generowanie numeru należy do zadań węzła docelowego; numer ten musi być przesyłany przez nadawcę aktualizacji. Cała tablica routingu jest przekazywana sporadycznie. Poszczególne aktualizacje zawierają jedynie przyrostowe informacje o wektorach. Zazwyczaj numer sekwencyjny ma wartość parzystą. Wartość nieparzysta jest stosowana w przypadku wykrycia uszkodzenia łącza. Aktualizacja zawierająca informacje o istniejącym połączeniu, dostępnym za pośrednictwem trasy o niższym koszcie, nadpisuje bieżącą trasę, ale nie numer sekwencyjny. Okresowo niewykorzystywane trasy są usuwane z tablicy. Mechanizm DSDV powstał dość dawno, ale nigdy nie doczekał się komercyjnej implementacji. Stanowi jednak podstawę działania protokołu AODV, który został opracowany przez grupę MANET, zajmującą się mobilnymi sieciami zestawianymi na żądanie (Mobile Ad hoc Network). W przyszłości protokół AODV może znaleźć zastosowanie w sieciach telefonii komórkowej.

## Algorytmy stanu łącza

Zasada działania protokołu stanu łącza polega na tym, że każdy router informuje pozostałe routery w sieci o swoich sąsiadach. Każdy węzeł może wówczas utworzyć mapę (graf) sieciowych powiązań poszczególnych routerów ze sobą w centrum tej topologii. Utworzone mapy służą do obliczenia najkrótszych tras. Zazwyczaj za ustalenie najkrótszej trasy odpowiada algorytm Dijkstry. Protokoły wektora odległości wymuszają na routerach wymianę tablic routingu, natomiast protokoły stanu łącza przekazują jedynie informacje, w których zawiera się identyfikator routera wysyłającego informację, dane o stanie łączy, jakie posiada, i informację o sąsiadach, którzy są podłączeni przez te łącza. Gdy stan łącza ulegnie zmianie (z włączonego na wyłączony lub z wyłączonego na włączony), generowana jest aktualizacja i informacja o bieżącym stanie łącza jest dostarczana do wszystkich routerów w sieci w obszarze działania protokołu.

Działanie protokołu stanu łącza przebiega zgodnie z poniższą procedurą:

1. Router wysyła do wszystkich węzłów informacje o stanie swoich łączy, a odebrane informacje zapisuje w bazie topologii.
2. Algorytm routingu przypisuje każdej trasie numer sekwencyjny.
3. Ogłoszenie o stanie łącza (LSA — *Link State Advertisement*) jest wysyłane okresowo do wszystkich węzłów w obszarze działania protokołu.
4. Jeśli nie został wcześniej zarejestrowany numer sekwencyjny aktualizacji pochodzącej z określonego węzła, nowa informacja jest zapisywana w bazie topologii. Jeśli odebrana informacja ma wyższy numer sekwencyjny niż zapisany w bazie topologii, nadpisuje wcześniejszą informację.

Kroki 3. i 4. są powtarzane przez wszystkie routery w domenie routingu. Aktualizacje są przesyłane do wszystkich węzłów za pomocą multiemisji. Router z włączonym protokołem stanu łącza okresowo wysyła pakiet o nazwie HELLO w celu sprawdzenia stanu łączy.

5. Algorytm stanu łącza analizuje bazę topologii i tworzy mapę sieci z danym routerem (z routerem, w którym algorytm działa) w środku. Za poprawne uznawane są te łącza, które są ustanowione między punktami końcowymi zgłaszającymi siebie nawzajem jako węzły sąsiednie.
6. Dostępność łączy jest testowana ponownie, gdy algorytm powtórzy krok 1. i rozpocznie ponownie całą procedurę.
7. Dane zebrane w bazie topologii są poddawane działaniu algorytmu Dijkstry, który wyznacza najkrótsze trasy między punktami końcowymi i zapisuje stosowne informacje w tablicy routingu.

Tablica routingu w routerze z działającym protokołem stanu łącza zawiera trasy o najniższym koszcie do wszystkich węzłów sieci objętej działaniem protokołu.

Najczęściej wykorzystywane protokoły stanu łącza to:

- ♦ otwarty protokół wyszukiwania najkrótszych tras — OSPF,
- ♦ protokół systemów pośrednich — IS-IS,
- ♦ protokół usług połączeń NetWare firmy Novell — NLSP.

W zależności od rodzaju protokołu do szacowania kosztu trasy wykorzystywane są takie parametry, jak przepustowość łączy, bieżące pasmo, koszt finansowy lub inne właściwości zdefiniowane przez administratora. Protokoły stanu łącza są preferowanymi rozwiązaniami w dużych sieciach komputerowych, ponieważ gwarantują szybszą reakcję na zmiany w sieci niż protokoły wektora odległości. Są dominującymi protokołami stosowanymi wewnątrz systemów autonomicznych.

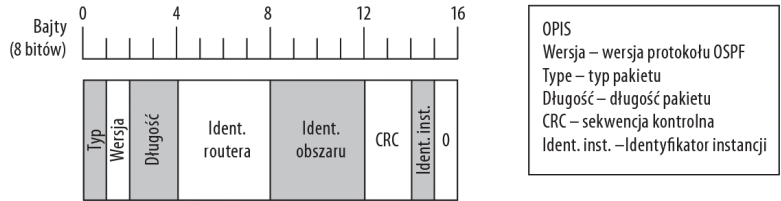
## Protokół OSPF

Protokół OSPF jest najczęściej stosowanym protokołem routingu z algorytmem stanu łącza. Jest powszechnie wykorzystywany jako protokół wewnętrzny w ramach AS-ów oraz w wielu innych sieciach. Ostatnia opracowana — trzecia — wersja standardu OSPF jest opisana w dokumencie RFC 5340, wydanym w roku 2008. Wersja ta obsługuje protokół IPv6.

Działanie protokołu OSPF bazuje na algorytmie Dijkstry z uwzględnieniem dodatkowych funkcji routerów — routerów wyznaczonych (ang. *designated*) (podstawowych) oraz routerów zapasowych. Wybór routera do pełnienia określonej funkcji wynika z przypisanego urządzeniu priorytetu. Routery o priorytecie 0 nie mogą pełnić funkcji węzłów wyznaczonych ani zapasowych. Wyznaczony router jest zobowiązany do wysyłania powiadomień o stanie łącza (LSA — *Link State Advertisement*) do wszystkich pozostałych węzłów w obszarze. Pakiety protokołu OSPF zawierają nagłówek składający się z dziewięciu pól, przedstawionych na rysunku 9.8. Standard OSPF definiuje kilka rodzajów pakietów: pakiety HELLO, pakiety opisu bazy danych, żądania informacji o stanie łącza, aktualizacje informacji o stanie łącza oraz potwierdzenia informacji o stanie łącza.

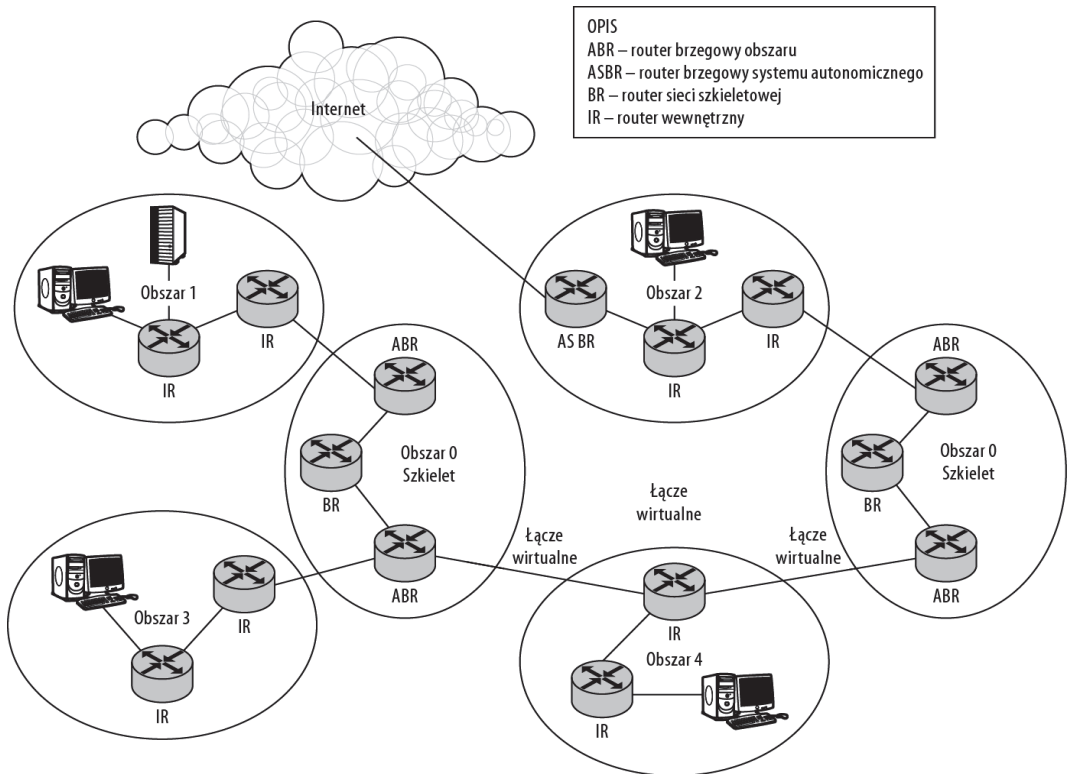
Protokół OSPF jest wykorzystywany w systemach autonomicznych. System autonomiczny może natomiast składać się z jednej sieci lub wielu sieci zarządzanych przez jedną organizację. Alternatywną nazwą dla wszystkich jednostek systemu autonomicznego uwzględnionych w tej samej mapie topologicznej jest „domena routingu”. Protokół OSPF wydziela

**Rysunek 9.8.**  
*Nagłówek pakietu OSPF*



obszary jako osobne jednostki topologiczne, dzięki czemu dany obszar nie ma informacji o routingu w innym obszarze. Rozwiązanie ma na celu obniżenie natężenia ruchu sieciowego oraz przyspieszenie procesu wyszukiwania najlepszych tras do poszczególnych obszarów.

Grupy obszarów są łączone ze sobą przez routery brzegowe obszarów w sieć szkieletową OSPF. Sieć szkieletowa sama jest zorganizowana na zasadzie obszaru OSPF, a informacje o routingu w ramach tego obszaru są niezależne od informacji wymienianych w obszarach dołączonych. Można również zorganizować sieć szkieletową OSPF w taki sposób, aby stanowiła ona dwie lub większą liczbę niepołączonych grup. Aby przekształcić sieć szkieletową na ciągłą, należy wyznaczyć łącza wirtualne wiodące przez routery w obszarach innych niż szkieletowy, które funkcjonują jako połączenia między routerami grup szkieletowych. W obszarze szkieletowym OSPF są wyznaczane routery brzegowe, które zapewniają połączenie z routerami obsługującymi protokoły routingu zewnętrznego, takie jak BGP lub EGP. Na rysunku 9.9 została przedstawiona sieć z kilkoma obszarami, obszarem szkieletowym oraz łączem wirtualnym.



**Rysunek 9.9.** *Routing OSPF w sieci o kilku obszarach z obszarem szkieletowym*

## Protokół IS-IS

Protokół IS-IS jest drugim pod względem popularności protokołem stanu łącza wykorzystywanym w sieciach pakietowych. Najczęściej znajduje zastosowanie w sieciach dostawców usług internetowych oraz dużych sieciach korporacyjnych, gdzie funkcjonuje jako protokół wewnętrzny w ramach systemu autonomicznego. Wymianę danych z innymi systemami autonomicznymi zapewniają protokoły routingu zewnętrznego.

Protokół IS-IS został opracowany przez Digital Equipment Corporation jako element protokołu DECnet w latach 80. i został przyjęty jako standard ISO — ISO/IEC 10589.2002. Ponieważ IS-IS nie jest publicznym standardem, nie jest stosowany w internecie — choć w 1990 roku organizacja IETF opublikowała zalecenie 10589.2002 jako dokument RFC 1142. Pierwotna wersja protokołu IS-IS została rozszerzona o obsługę protokołu IP w sieciach TCP/IP i w starszej literaturze była wyróżniana jako zintegrowany protokół IS-IS (ang. *Integrated IS-IS*).

Protokół IS-IS stanowi konkurencję dla protokołu OSPF — jego działanie również opiera się na algorytmie Dijkstry. Choć w obydwu rozwiązaniach uwzględniono wiele identycznych funkcji, mechanizm IS-IS jest uznawany za nieco stabilniejszy niż OSPF, ale o gorszych parametrach wydajnościowych. Dodatkowe funkcje protokołu OSPF wprowadzają większe obciążenie związane z przetwarzaniem komunikatów i prawdopodobnie dlatego protokół IS-IS lepiej się skaluje.

W standardzie IS-IS wyróżniono trzy rodzaje obszarów routingu: poziom 1. (wewnętrzny), poziom 2. (zewnętrzny) oraz poziom 1.-2. (wewnętrzny-zewnętrzny). Routery poziomów 1. i 2. mogą wymieniać informacje jedynie z routerami tego samego poziomu. Obydwie grupy mogą również komunikować się z routerami poziomu 1.-2. W przeciwieństwie do protokołu OSPF, w którym do wymiany informacji między obszarami wykorzystuje się obszar szkieletowy (obszar 0) i w którym router brzegowy obszaru jest punktem wspólnym dla obydwu obszarów, w rozwiązaniu IS-IS nie wydziela się obszarów szkieletowych, a obszary sieci nigdy na siebie nie nachodzą.

## Algorytm wektora ścieżki

Algorytm routingu typu wektor ścieżki (ang. *path vector*) jest ostatnim z trzech omówionych w tej książce najważniejszych mechanizmów budowania tablic routingu. Poprzednie to algorytmy wektora odległości i stanu łącza. Algorytm wektora ścieżki jest pochodną mechanizmu DV. W rozwiązaniu tym wektory odległości od celu węzeł otrzymuje od węzłów sąsiednich wraz z pełną informacją o ścieżce, która musi zostać pokonana, aby dojść do elementu docelowego. Znając pełną ścieżkę, algorytm może znacznie łatwiej wykryć pętlę i dostosować swoją pracę do tej sytuacji niż w przypadku mechanizmów wektora odległości. W systemach obsługujących ten typ routingu przechowywane są dwie tablice — tablica bieżących ścieżek do wszystkich węzłów oraz tablica routingu z identyfikatorem najbliższego routera w ramach każdej trasy.

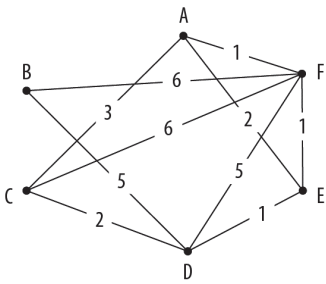
## Przykład wykorzystania algorytmu

Rozważmy nieskomplikowany przykład wykorzystania algorytmu wektora ścieżki, przedstawiony na rysunku 9.10. Wektory przyjmują postać:

[Cel, Koszt, Liczba węzłów ścieżki, Lista węzłów ścieżki]

**Rysunek 9.10.**  
*Ilustracja sposobu  
działania algorytmu  
wektora ścieżki*

- 1. Wysłanie pakietu HELLO z A do sąsiadów  
[cel, koszt, liczba węzłów, lista węzłów]  
[C, 3, 1, AC], [E, 2, 1, AE], [F, 1, 1, AF]
  
- 2. Aktualizacja z C do A  
[cel, koszt, liczba węzłów, lista węzłów]  
[C, 0, 1, C], [A, 3, 1, AC], [D, 2, 1, CD], [F, 6, 1, CF]
  
- 3. Aktualizacja z A do C, E, F  
[cel, koszt, liczba węzłów, lista węzłów]  
[A, 0, 1, A], [C, 3, 1, AC], [D, 5, 2, ACD], [F, 1, 1, AF]
  
- 4. Wymiana pakietów HELLO między wszystkimi węzłami
  
- 5. Aktualizacja z E do A  
[cel, koszt, liczba węzłów, lista węzłów]  
[E, 0, 1, E], [A, 2, 1, AE], [B, 6, 2, BDE], [C, 3, 2, CDE], [D, 1, 1, DE], [F, 1, 1, EF]
  
- 6. Aktualizacja z A do B – F  
[cel, koszt, liczba węzłów, lista węzłów]  
[A, 0, 1, A], [B, 7, 3, AFB], [C, 3, 2, AC], [D, 3, 3, AED], [E, 2, 2, AE], [F, 1, 2, AF]



Tablica routingu routera A (po kroku 3.)

Cel	Koszt	Węzły na trasie
C	3	AC
D	5	ACD
E	2	AE
F	1	AF

Tablica routingu routera A (po kroku 5.)

Cel	Koszt	Węzły na trasie
B	7	AFB
C	3	AC
D	3	AED
E	2	AE
F	1	AF

W kroku 1. węzeł A wysłał pakiet HELLO i gromadzi informacje na temat węzłów sąsiednich. Analogiczną operację wykonuje węzeł C. Następnie router C przesyła własne wektory do węzła A. W kroku 3. węzeł A przebudowuje swoją tablicę routingu zgodnie z pozyskanymi informacjami. Wektory routera C umożliwiają węzłowi A zdefiniowanie trasy do węzła D, ale nie wpływają na żadne inne trasy, co zostało pokazane w lewej dolnej tabeli na rysunku 9.10. W kroku 4. został przedstawiony stan po tym, jak wszystkie węzły zgromadziły informacje o sąsiadach dzięki wykorzystaniu pakietów HELLO. W kroku 5. router E wysłał własne wektory do routera A. Ten z kolei może utworzyć tablicę routingu obejmującą wszystkie węzły sieci. Informacje dostarczone z węzłów E i F powodują dodanie trasy do routera B (A-F-B) — informacja z węzła F — oraz zmianę trasy D (A-E-D) — informacja z węzła E. W ostatnim kroku węzeł A może wysłać tablicę routingu, widoczną w prawym dolnym narożniku rysunku, do wszystkich pozostałych węzłów.

W systemie routingu działającym na podstawie algorytmu wektora ścieżki jeden lub większa liczba węzłów — nazywanych *węzłami rozgłaszającymi* (ang. *speaker node*) — przechowuje tablice routingu przeznaczone dla innych przyłączonych węzłów. Odległości zawarte w tych tablicach są wyznaczane właśnie przez węzły rozgłaszające. Węzły rozgłaszające wysyłają powiadomienia o dostępnych ścieżkach do innych węzłów rozgłaszających. Algo-

rytm wektora ścieżki ma zadanie zminimalizowania liczby domen, przez które są transportowane komunikaty, co sprawia, że jest on odpowiedni, aby stosować go jako mechanizm routingu między systemami autonomicznymi. Opisana tutaj metodologia działania jest podstawą funkcjonowania protokołu BGP.

Spośród trzech zaprezentowanych algorytmów routingu — wektor odległości, wektor ścieżki i wektor stanu łącza — jedynie protokoły wektora ścieżki znajdują praktyczne zastosowanie w routingu międzysystemowym. W przypadku algorytmu wektora odległości każdy dodatkowy węzeł pokonywany przez komunikat zwiększa prawdopodobieństwo wyboru trasy przedawnionej lub uszkodzonej. Działanie protokołów stanu łącza wymaga przeniesienia przez sieć intensywnego ruchu w przypadku zaistnienia zmiany, której prawdopodobieństwo wzrasta w zależności od liczby obsługiwanych systemów oraz dostępności w każdym węźle odpowiedniej ilości zasobów do sporządzenia mapy sieci.

## Protokół BGP

Protokół BGP jest niezwykle łatwym w skalowaniu protokołem routingu zewnętrznego, wykorzystywanym do wymiany informacji między systemami autonomicznymi. Jego działanie bazuje na algorytmie wektora ścieżki, który został opisany we wcześniejszym punkcie rozdziału. BGP jest podstawowym protokołem routingu w internecie — następcą protokołu EGP. Mechanizm EGP był pierwszym protokołem routingu internetowego, opracowanym przez firmę BBN Technologies w 1980 roku. Z kolei aktualna wersja protokołu BGP (wersja 4.) została opublikowana w dokumencie RFC 4271 w 2006 roku.

Rozwiązanie to jest stosowane zazwyczaj przez dostawców usług internetowych oraz przez korporacje, w których funkcjonują sieci o bardzo dużym zasięgu. Jednak z uwagi na fakt, że BGP reguluje ruch w internecie, warto poświęcić trochę czasu na zapoznanie się z zasadami jego działania. BGP jest jedynym protokołem, który wykorzystuje protokół TCP jako mechanizm transportowy. Wymienia pakiety na porcie 179. Protokół BGP jest uruchamiany w dwóch odmianach — eBGP (zewnętrzny BGP) i iBGP (wewnętrzny BGP). Router BGP pracujący wewnątrz systemu autonomicznego jest routerem iBGP. Natomiast routery działające pomiędzy systemami autonomicznymi są routerami eBGP. Każdy router pracujący wewnątrz systemu autonomicznego, komunikujący się z jednostkami innych systemów autonomicznych, jest nazywany routerem brzegowym. Z kolei routery działające poza systemami autonomicznymi są nazywane routerami szkieletu internetowego.

Routery największych dostawców usług internetowych przechowują obecnie tablice routingu BGP złożone z około 150 000 tras. Jeśli więc ktoś uruchamia router BGP i dysponuje szybkim połączeniem (np. E1) z dużą firmą telekomunikacyjną, może pobrać 150 000 tras z każdego serwisu, do którego jest przyłączony. Mechanizm BGP dzieli trasy na podstawie atrybutów (parametrów trasy), dzięki czemu można nimi wydajniej zarządzać. Wspomniane atrybuty to:

- ♦ **Adres następnego routera** — adres pierwszego routera na trasie do wskazanej sieci.
- ♦ **Źródło danych** — informacja o tym, czy dane pochodzą z routingu eBGP, czy iBGP.
- ♦ **Ścieżka systemów autonomicznych** — identyfikatory systemów autonomicznych zarejestrowanych na trasie powiadomienia.

- ♦ **Preferowane wyjście lokalne** — preferowany router wyjściowy w danym systemie autonomicznym.
- ♦ **Dyskryminator wielu wyjść** — atrybut niestandardowy, obsługiwany w urządzeniach firmy Cisco.
- ♦ **Wyróżnik społeczności** — dopuszczalne wartości to no-export (bez eksportu), no-advertise (bez powiadomień) lub internet (powiadomienia do wszystkich).
- ♦ **Koszt lub waga trasy** — atrybut niestandardowy firmy Cisco, która stosuje określenie „waga”.

Ponieważ zgodnie z hierarchią sieci internetowych dalsze uszczegółowienie tablic routingu zapewniają protokoły routingu bezklasowego (CIDR), między routerami BGP można wymieniać całe bloki adresów. System CIDR, który zastępuje starszą notację klas sieci, został szczegółowo omówiony w rozdziale 18.

## Protokół drzewa rozpinającego

Protokół drzewa rozpinającego (STP — *Spanning Tree Protocol*) został opisany w standardzie IEEE 802.1D i jest technologią adaptacyjnego wydzielania ścieżek komunikacyjnych, która rozwiązuje problem pętli w sieci przez zastosowanie adaptacyjnego i dynamicznego mechanizmu wytyczania połączeń. STP jest podstawową technologią wykorzystywaną w sieciach przełączanych, która zapewnia tworzenie wirtualnych obwodów z pominięciem ewentualnych wykrytych pętli. Połączenia te są tworzone przez węzły pełniące funkcję mostów. W praktyce zazwyczaj oznacza to wykorzystanie przełączników, które wykonują zadania mostów sieciowych. Rolę tę mogą również odgrywać routery uruchomione w trybie mostów. Dodatkowa funkcja jest przez nie wykorzystywana również w różnych mechanizmach routingu.

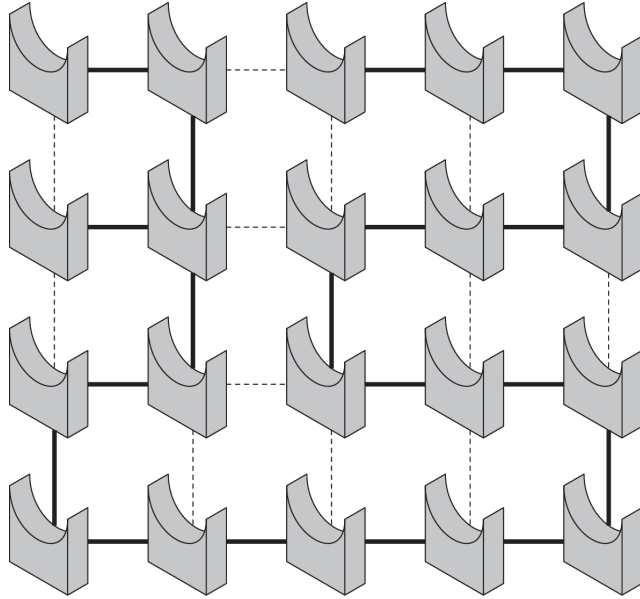
Algorytm STP (DEC STP) został opracowany przez Radę Perlman w 1985 roku w firmie Digital Equipment Corporation przed rozwojem sieci WWW. Protokół STP działa na poziomie warstwy łącza danych modelu OSI, ponad warstwą fizyczną, i jest implementowany w urządzeniach takich jak przełączniki i routery.

W sieci hierarchicznej główny węzeł jest połączony z pewną liczbą węzłów pierwszego poziomu, a te z kolei z następnymi węzłami. Opisana hierarchia przypomina drzewo odwrócone korzeniem do góry, w którym wyłączenie jednego węzła powoduje niedostępność węzłów umiejscowionych na niższym poziomie hierarchii. W konfiguracji w pełni hierarchicznej komunikacja między danym węzłem a węzłem innej gałęzi wymaga przekazania informacji w górę drzewa, do poziomu węzła głównego, a następnie w dół, do węzła docelowego. Z tego względu jedynie sieci o niewielkich rozmiarach są w pełni zgodne ze strukturą drzewa.

Rozwiązanie stosowane w dużych sieciach polega na utworzeniu połączeń krzyżowych między poszczególnymi gałęziami drzewa. Połączenia tego typu skracają trasy i zapewniają większą wydajność komunikacji. Dodatkowo zapewniają nadmiarowość połączeń, ponieważ większość potencjalnych połączeń może być zrealizowana za pomocą kilku ścieżek komunikacyjnych. Jednak połączenia krzyżowe mogą doprowadzić do powstania pętli w sieci.

W teorii grafów drzewa rozpinające są tworzone za pomocą algorytmu, który wyznacza zbiór tras przez system połączonych ze sobą węzłów, ale w taki sposób, że każdy węzeł należy przynajmniej do jednej gałęzi, a wśród połączeń nie występują pętle. Przykład drzewa rozpinającego został pokazany na rysunku 9.11. Linie ciągłe reprezentują połączenia wchodzące w skład drzewa rozpinającego, natomiast linie przerywane symbolizują odcinki wykluczone.

**Rysunek 9.11.**  
*Drzewo rozpinające*



Do wyznaczenia drzewa rozpinającego można zastosować wiele algorytmów. W jednym z rozwiązań każdej krawędzi przypisuje się pewną wagę (otrzymujemy graf ważony), a algorytm drzewa rozpinającego wyznacza ścieżki przez system, które cechują się najniższą sumą wag, generując w rezultacie minimalne drzewo rozpinające. W systemach wielodomenowych połączenie kilku minimalnych drzew rozpinających jest nazywane minimalnym lasem rozpinającym.

Dopuszczalne jest wprowadzanie także innych mechanizmów optymalizacyjnych, takich jak wyznaczanie drzewa rozpinającego o największej liczbie krawędzi, minimalnej średnicy, najmniejszej liczbie liści lub minimalnej dylatacji. Krawędź jest trasą między dwoma węzłami, obliczoną przez algorytm drzewa. Liśćmi są węzły końcowe gałęzi. Średnica określa liczbę przełączników, które występują na trasie łączącej dwa przełączniki sieci. Dylatacja reprezentuje różnicę między najkrótszą ścieżką między dwoma węzłami drzewa a ścieżką wyliczoną przez algorytm drzewa rozpinającego.

## Hierarchia węzeł-most

Celem administratora sieci jest utworzenie połączeń, w których nie będą występowały pętle, ale przy jednoczesnym zapewnieniu połączeń nadmiarowych, które umożliwią wymianę danych nawet w przypadku awarii jednego z węzłów lub połączeń. W praktycznych rozwiązaniach zamiast ważonych krawędzi stosuje się pojęcie ścieżek o najniższym koszcie. Aby wyznaczyć ścieżki o najniższym koszcie, definiowane są dwa parametry:

- ♦ priorytet węzła,
- ♦ identyfikator węzła.

Koszt (waga) węzła jest wyznaczany na podstawie obydwu wymienionych parametrów. W protokole STP jako pierwszy (ważniejszy) jest uwzględniany priorytet węzła. Węzeł o najniższej wartości priorytetu jest węzłem o najwyższym priorytecie — poprzedzającym w analizie wszystkie pozostałe węzły. W przypadku węzłów o jednakowej wartości priorytetu porównywane są identyfikatory węzłów, czyli adresy MAC. Adres MAC o najniższej wartości wyznacza pierwszeństwo węzła wśród innych węzłów o tym samym priorytecie. Aby wskazać główny węzeł (most główny), należy ustawić niższą wartość priorytetu niż w innych urządzeniach obsługujących protokół STP. Domyślnie wartość priorytetu przełączników i routerów Cisco wynosi 32 768.

Algorytm STP wyznacza takie trasy przez system, które zapewniają przesyłanie komunikatów z dowolnego punktu końcowego do węzła głównego wzdłuż ścieżek o najniższym koszcie. Koszt ścieżki oblicza się jako sumę kosztów poszczególnych segmentów na trasie. Ponieważ każdy most w systemie ma konfigurowalną wartość priorytetu, protokół STP może zmienić ścieżki o najniższym koszcie zależnie od bieżącego stanu sieci. Podczas obliczania ścieżek o najniższym koszcie uwzględnia się dwie poniższe zasady:

- ♦ musi zostać obliczona ścieżka o najniższym koszcie prowadząca z każdego węzła,
- ♦ musi zostać obliczona ścieżka o najniższym koszcie prowadząca do każdego segmentu sieci.

Port przełącznika lub routera, przez który wiedzie trasa o najniższym koszcie do węzła głównego, jest nazywany portem głównym (ang. *root port*). Port występujący na trasie o najniższym koszcie, ale prowadzący do segmentu sieciowego, jest nazywany portem wyznaczonym (ang. *designated port*). Na potrzeby tej analizy można przyjąć, że segment sieciowy składa się z węzłów przyłączonych do wspólnej warstwy fizycznej i wykorzystujących jednakowy model zabezpieczeń. W tym rozumieniu dwie podsieci jednej sieci LAN będą stanowiły dwa segmenty, podobnie jak dwie grupy robocze (lub domeny).

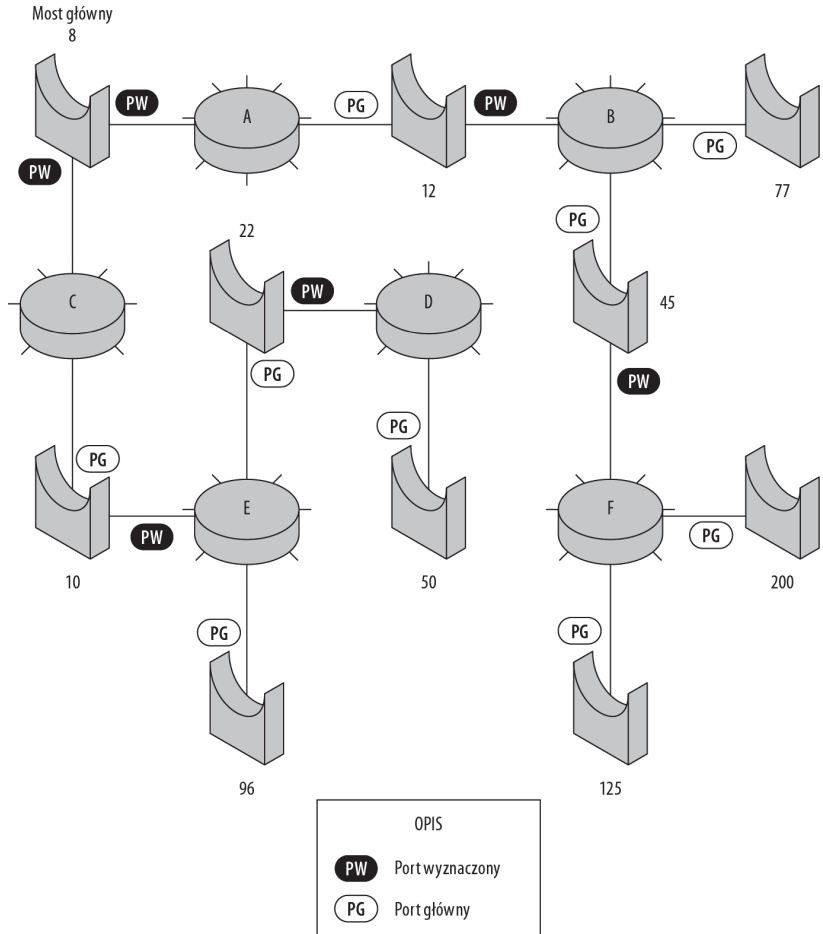
Gdy algorytm STP określi porty główne i wyznaczone, wszelkie pozostałe porty zostają zablokowane. Często zdarza się sytuacja, w której dwie ścieżki (lub większa liczba ścieżek) z mostu do węzła głównego mają jednakowy (najniższy) koszt. Wówczas wybierana jest trasa wiodąca przez most o niższym identyfikatorze. Port tego mostu staje się portem głównym. Jeśli do danego segmentu są przyłączone dwa mosty (lub większa liczba mostów), które dysponują ścieżkami o najniższym koszcie prowadzącymi do mostu głównego, portem wyznaczonym staje się port tego mostu, który jest połączony z mostem o najniższej wartości identyfikatora.

Na rysunku 9.12 została przedstawiona sieć z uruchomionym protokołem drzewa rozpinającego. Aby ułatwić analizę rysunku, przyjęto założenie, że każdemu segmentowi sieci przypisano ten sam koszt jednostkowy. Uzyskanie konfiguracji pokazanej na rysunku 9.12 zostało poprzedzone poniższą analizą.

1. Most o wartości priorytetu 8 ma najwyższy priorytet (najniższą wartość), więc zostaje wybrany mostem głównym. Most główny niekoniecznie musi być urządzeniem o największej wydajności. Zazwyczaj jest to centralny komponent sieci. Można

**Rysunek 9.12.**

Sieć, w której zastosowano algorytm drzewa rozpinającego



przyjąć zasadę, że węzłem głównym powinno być urządzenie najrzadziej przenoszone lub modyfikowane. Z tego względu węzłami głównymi są z reguły przełączniki rdzeniowe. Warto zauważyć, że most główny jest jedynym mostem w sieci, który nie ma portu głównego.

- Od mostu głównego odchodzą dwie ścieżki do węzłów o priorytetach 10 i 12. Ponieważ wartość 10 jest najwyższym priorytetem, most o tym priorytecie łączy się z następnym mostem o najwyższym priorytecie (o wartości 22).
- Spośród dwóch niepodłączonych węzłów o wartościach 12 i 22 węzeł o priorytecie 12 ma pierwszeństwo. Most ten może utworzyć połączenie pozbawione pętli z mostem o priorytecie 45.
- Na tym etapie przyłączenia nie są poprowadzone do mostów o priorytetach 22 i 45. Zatem most o priorytecie 22 zostanie połączony z węzłem o kolejnym najwyższym priorytecie (50).
- Z dwóch pozostałych priorytetów, tj. 45 i 50, pierwszeństwo ma 45. Most o tym priorytecie jest więc łączony z węzłem o priorytecie 125.

6. Na tym etapie pozostają trzy mosty o priorytetach 77, 96 i 200, które zostaną podłączone w takiej właśnie kolejności. Staną się jednocześnie punktami końcowymi poszczególnych gałęzi drzewa.

W pewnych przypadkach algorytm nie jest w stanie określić, który z dwóch lub większej liczby mostów jest ważniejszy w hierarchii STP. Taka sytuacja ma miejsce wówczas, gdy dwa mosty są połączone z innymi za pomocą co najmniej dwóch łączy. Wybór jest wówczas dokonywany na podstawie priorytetu portu — wybrany port staje się portem głównym lub wyznaczonym.

**Koszty segmentów**

Analiza rysunku 9.12 została przeprowadzona przy założeniu, że każdemu segmentowi sieci odpowiada jednakowy koszt przekazywania danych, co zazwyczaj jest nieprawdą w rzeczywistych sieciach. Zgodnie z zamieszczonymi wcześniej informacjami koszt segmentu sieciowego jest jednym z parametrów uwzględnianych podczas wyznaczania ścieżki o najniższym koszcie. Niektóre połączenia sieciowe mają większą przepustowość, inne mniejszą. Nawet w niezbyt skomplikowanych konfiguracjach, w których most jest przyłączony do sieci Fast Ethernet, może funkcjonować most połączony z urządzeniami bezprzewodowymi, cechującymi się niższą przepustowością. Aby zoptymalizować działanie protokołu STP, koszty segmentów sieciowych są liczone na podstawie zalecenia IEEE 802.1D z 1998 roku. Standard ten został zaktualizowany w 2001 roku (i oznaczony jako 802.1T) przez wprowadzenie dodatkowego podziału przepustowości. Standardowe koszty segmentów zostały przedstawione w tabeli 9.1.

**Tabela 9.1.** Koszty segmentów sieciowych w protokole STP

Przepustowość segmentu	Koszt według standardu 802.1T	Koszt według standardu 802.1D
10 Gb/s	2 000	2
2 Gb/s	10 000	3
1Gb/s	20 000	4
100 Mb/s	200 000	19
16 Mb/s	1 250 000	62
10 Mb/s	2 000 000	100
4 Mb/s	5 000 000	250

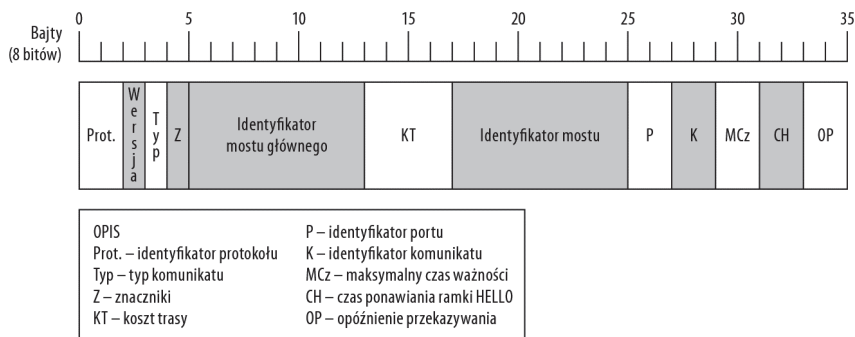
**Dynamiczna optymalizacja**

W kolejnym z prezentowanych przykładów został przedstawiony stan sieci po uwzględnieniu przez protokół STP wszystkich priorytetów mostów. Ma on na celu zilustrowanie funkcji, która istotnie podnosi wartość protokołu STP — zdolności do adaptacji do zmieniającej się topologii sieci. Jednym ze sposobów wykrywania zmian w sieci jest użycie protokołu mostów, który rozsyła specjalne ramki, nazywane jednostkami danych protokołu mostów (BPDU — *Bridge Protocol Data Units*), zawierające informacje o koszcie segmentu oraz identyfikatorach dostępnych węzłów. Dzięki aktualizacji informacji trasa do mostu głów-

nego może być dostosowywana do bieżących potrzeb. Na rysunku 9.13 został przedstawiony format ramki BPDU. Poszczególne jej pola przenoszą dane na temat identyfikatora mostu, priorytetu oraz adresów MAC wykorzystywanych przez przełącznik. Pozostałe informacje to priorytet ścieżki oraz inne jej parametry, takie jak koszt.

**Rysunek 9.13.**

Ramka BPDU



Przełączniki i routery — urządzenia pełniące w nowoczesnych sieciach funkcję mostów — rozsyłają ramki BPDU, uwzględniając w nich adres MAC portu źródłowego oraz adres multemisji właściwy dla protokołu STP o wartości 01:80:C2:00:00:00. Ramki te są generowane co kilka sekund i wyznaczają puls sieci wykorzystywany do utrzymywania tablic ścieżek. Domyślny okres ponawiania emisji (opisany w standardzie) wynosi 2 sekundy. Jego wartość można jednak zmienić.

W działaniu protokołu stosowane są trzy rodzaje jednostek BPDU:

- ♦ jednostka konfiguracyjna (CBPDU — *Configuration BPDU*),
- ♦ powiadomienie o zmianie topologii (TCN — *Topology Change Notification*),
- ♦ potwierdzenie powiadomienia o zmianie topologii (TCA — *Topology Change Acknowledgement*).

Za każdym razem, gdy nowe urządzenie jest dodawane do sieci, jego port jest wprowadzany w stan nasłuchu, w trakcie którego urządzenie odbiera jednostki BPDU i poznaje konfigurację sieci. Urządzeniami tymi mogą być dowolne punkty końcowe wyposażone w interfejs sieciowy. Domyślny czas nasłuchiwania wynosi 15 sekund. Po jego upływie urządzenie przechodzi w stan uczenia się, który również trwa 15 sekund. Całkowity czas nasłuchiwania i uczenia się jest parametrem konfigurowalnym, znanym jako opóźnienie przekazywania (ang. *forward delay*). Dzięki opóźnieniu włączane do sieci urządzenia mają czas, aby odebrać informacje z węzła głównego. Gdy urządzeniem tym jest komputer, serwer lub drukarka (jednostka niepełniująca funkcji mostu), wraz z zakończeniem procesu uczenia się port przechodzi do trybu przekazywania i rozpoczyna nadawanie jednostek BPDU.

Gdy do portu działającego mostu dodawany jest nowy most, procedura uruchamiania portu jest nieco inna. Każdy nowy przełącznik lub router może wprowadzić pętlę do topologii sieci, więc jego port pozostaje w trybie blokowania aż do zakończenia cyklu nasłuchu i uczenia się. Port ten wysyła również ramki TCN do głównego mostu. Po odebraniu powiadomienia TCN most główny odsyła potwierdzenie za pomocą komunikatu TCA, w którym określa status nowego portu. Od tego momentu nowy port wysyła jednostki BPDU w standardowych odstępach czasu, aby wszystkie pozostałe węzły mogły zaktualizować

odpowiednio swoje tablice tras. Most główny modyfikuje standardową jednostkę BPDU w taki sposób, aby było wiadomo, że sieć jest w trakcie zmian, a następnie przesyła informację o zmianie do wszystkich węzłów. Każdy z mostów modyfikuje tablicę tras i potwierdza wykonanie polecenia.

Port mostu (przełącznika lub routera) może pracować w jednym z pięciu trybów:

- ♦ **Nasłuchu** — przychodzące jednostki BPDU są odbierane i przetwarzane, ale żadne ramki nie są wysyłane.
- ♦ **Uczenia się** — port dodaje adresy mostów do tablicy ścieżek, ale nie przekazuje żadnych ramek. Port uczący się może być uwzględniony w aktywnej topologii.
- ♦ **Przekazywania** — port może odbierać i wysyłać dane sieciowe. Proces STP równolegle przetwarza odbierane jednostki BPDU. Wszystkie porty mostu głównego i każdy port główny nieustannie pracują w trybie przekazywania. Ten tryb pracy jest również charakterystyczny dla wszystkich portów wyznaczonych.
- ♦ **Blokowania** — ustawienie portu nie pozwala na wysyłanie ani odbieranie danych. Niemniej odbierane są jednostki BPDU, a port może zmienić stan w razie konieczności. Każdy port mostu, który obsługuje połączenie z innym mostem i nie jest portem głównym lub wyznaczonym, musi być zablokowany.
- ♦ **Wyłączenia** — port może być wyłączony programowo (na przykład w wyniku wykonania polecenia SMTp), ale nie w ramach mechanizmu STP.

## Szybki protokół drzewa rozpinającego

W przypadku zastosowania klasycznego protokołu STP reakcja na zmianę topologii może zająć mostom nawet jedną minutę. W roku 1995 takie rozwiązanie wydawało się wystarczające. Organizacja IEEE zdefiniowała szybszą odmianę protokołu STP — RSTP (*Rapid Spanning Tree Protocol*). Standard otrzymał oznaczenie 802.1w i został opublikowany w 1998 roku. W roku 2004 organizacja IEEE połączyła zalecenia 802.1D, 802.1t-2001 oraz 802.1w w jeden standard 802.1D-2004. Wiele zmian uwzględnionych w protokole RSTP stało się częścią implementacji STP w przełącznikach ethernetowych firmy Cisco.

Działanie RSTP bazuje na mechanizmach STP, ale z istotnymi zmianami w porównaniu z pierwotnym protokołem. Modyfikacje umożliwiły skrócenie czasu rekonfiguracji do okresu poniżej dwóch sekund w przypadku awarii węzła głównego.

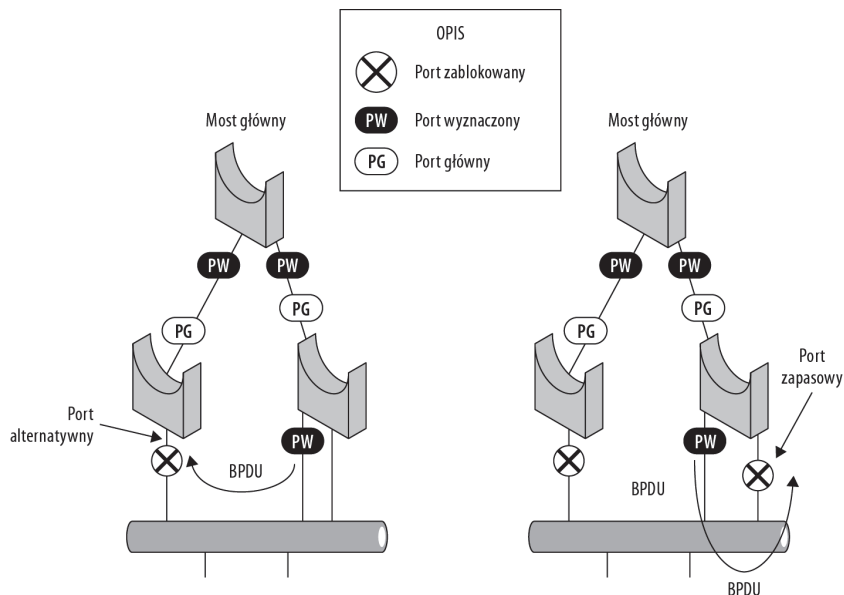


Włączenie więcej niż jednego wariantu protokołu STP może doprowadzić do nieprzewidywalnego zachowania sieci.

W RSTP blokowane porty są podzielone na dwie kategorie — porty alternatywne i porty zapasowe. Port alternatywny odbiera jednostki BPDU od innego mostu o wyższym priorytecie. Port zapasowy otrzymuje jednostki BPDU od tego samego mostu co inny port danego mostu. Rozróżnienie to pozwala na znacznie szybsze użycie alternatywnych ścieżek do mostu głównego po uszkodzeniu portu głównego. Port zapasowy zapewnia nadmiarowe połączenie z tym samym segmentem sieci, ale nie gwarantuje połączenia z mostem głównym. Pozostałe rozwiązania RSTP pokrywają się z funkcjami STP. Przykład zastosowania portów alternatywnych i zapasowych został przedstawiony na rysunku 9.14.

**Rysunek 9.14.**

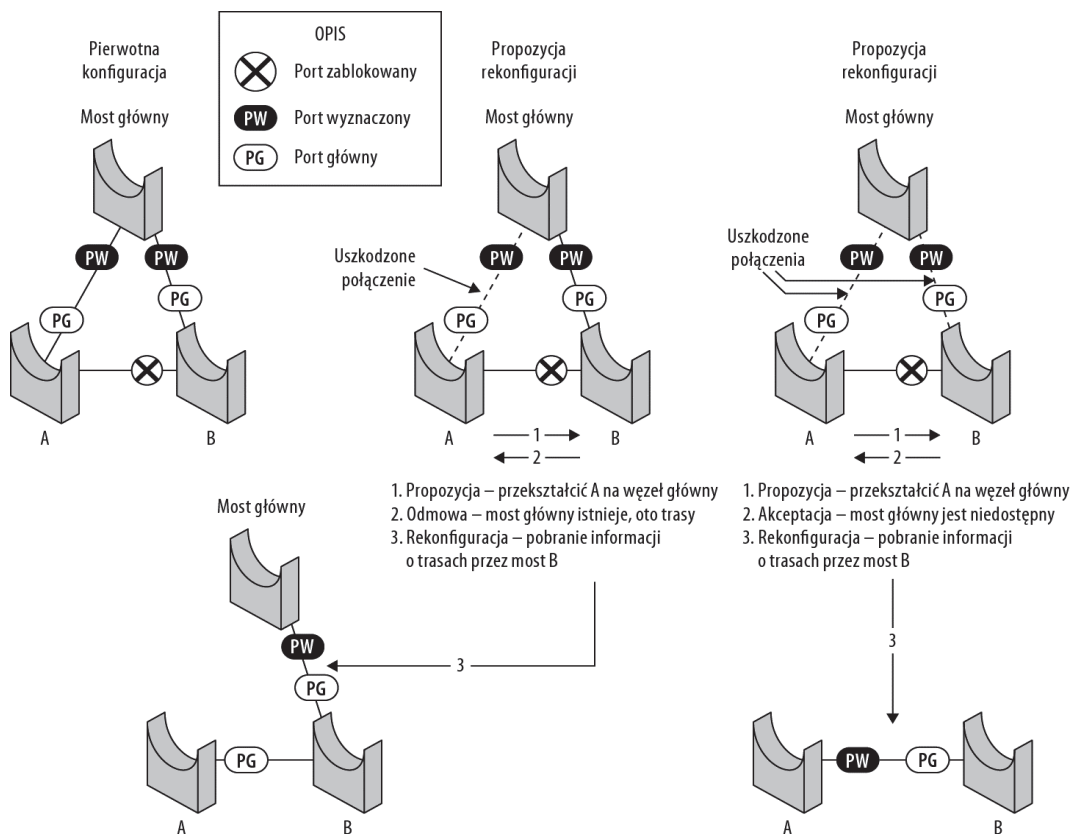
*Przykłady użycia  
portów zapasowych  
i alternatywnych*



Jednostki BPDU protokołu RSTP zostały zmienione w sposób gwarantujący szybsze przedawianie się informacji — konieczne jest więc stosowanie komunikacji podtrzymującej połączenie między węzłami. Po upływie trzech okresów ponawiania ramki bez odbioru jednostki BPDU most uznaje, że wystąpił błąd, i wysyła powiadomienie o tym fakcie, prosząc jednocześnie most o niższym priorytecie o zaakceptowanie siebie jako mostu głównego. Most odbierający propozycję przy braku innej ścieżki do mostu głównego i po stwierdzeniu wyższego priorytetu mostu dostarczającego propozycję zmienia port główny, przypisując tę funkcję do portu połączonego z nadawcą propozycji. Jeśli jednak most odbierający propozycję dysponuje poprawną ścieżką do pierwotnego mostu głównego, wysyła jednostkę BPDU do mostu, który wygenerował propozycję, informując ten most o statusie oryginalnego mostu głównego i powodując aktualizację tras oraz rekonfigurację procesu STP w tym węźle.

Na rysunku 9.15 zaprezentowana została idea proponowania zmiany mostu głównego oraz operacja wyboru łącza zapasowego. W lewym górnym narożniku widoczna jest pierwotna konfiguracja. Gdy łącze zostaje uszkodzone (jak na środkowym górnym przykładzie), węzeł A przekazuje do węzła B propozycję przekształcenia siebie na węzeł główny. Ponieważ węzeł B wciąż dysponuje połączeniem z mostem głównym, propozycja zostaje odrzucona, a do węzła A są przesyłane informacje o ścieżkach węzła B. Przełączenie tras kończy się w chwili zmiany konfiguracji w węźle A (pokazanej w lewej dolnej części rysunku), która wyznacza trasę z węzła A przez węzeł B do mostu głównego.

Gdy następuje uszkodzenie dwóch połączeń, odpowiedź na propozycję jest inna. Po dostarczeniu przez węzeł A propozycji do węzła B most B akceptuje zmianę węzła głównego, ponieważ nie ma już kontaktu z dotychczasowym węzłem głównym. Wynik operacji został przedstawiony w prawym dolnym narożniku rysunku 9.15. Węzeł A ustawia jeden z portów jako port wyznaczony, a węzeł B przekształca port łącza w port główny. W wyniku przełączenia istnieje bezpośrednie łącze między mostami A i B.



**Rysunek 9.15.** Wykorzystanie protokołu RSTP do rekonfiguracji w przypadku awarii

W sieci pracującej pod kontrolą protokołu RSTP żaden port przyłączony do stacji końcowej nie może utworzyć pętli, ponieważ jednostki końcowe są z założenia jednoportowe. Wszystkie porty tego typu są oznaczane jako porty brzegowe i przełączane w tryb przekazywania bez konieczności uruchamiania trybu nasłuchiwania i uczenia się. Porty brzegowe pozostają takimi nawet wówczas, gdy protokół RSTP przelicza i modyfikuje topologię drzewa rozpinającego. Niemniej gdy tylko port odbierze ramkę BPDU, zostanie natychmiast przekształcony na port drzewa.

Natychmiastowe przejście do stanu przekazywania może być wykonane również w przypadku portów, które obsługują połączenia punkt-punkt. Porty działające w trybie pełnego duplexu są uznawane za elementy połączeń punkt-punkt. Z kolei połączenia półdupleksowe są realizowane przez porty określone jako współdzielone. Ponieważ niemal wszystkie nowoczesne przełączniki wykorzystują pełnoduplexowy tryb pracy portów, protokół RSTP może w bardzo krótkim czasie przełączyć je w tryb przekazywania. Szybka zmiana stanu jest możliwa dzięki mechanizmowi propozycji-akceptacji, który propaguje przez sieć, zmieniając kolejno stan portów na każdym łączu.

Technika szybkiej zmiany stanu portu w protokole RSTP została zilustrowana na rysunku 9.16. Propozycja wyznaczenia portu głównego (oznaczona numerem 1) zostaje zaakceptowana (w odpowiedzi o numerze 2), tak jak to zostało pokazane na lewym przykładzie. Przełącznik



mostu trzeciego poziomu, do którego przyłączone jest nowe łącze. Ostateczny wynik jest taki sam jak w poprzedniej operacji, jednak zamiast oczekiwania na przekazanie komunikatu w dół gałęzi i z powrotem do węzła głównego (zgodnie z mechanizmem STP) protokół RSTP inicjuje szereg niezależnych zmian, realizowanych w bardzo krótkim czasie. Im więcej jest mostów pośrednich między mostem głównym a węzłem z nowym łączem, tym większa jest różnica w działaniu obydwu protokołów.

Mechanizm RSTP w bardzo agresywny sposób przekazuje informacje o zmianie topologii. W przypadku protokołu STP powiadomienie o zmianach musi być dostarczone do mostu głównego, z którego jest przekazywane w dół do wszystkich pozostałych węzłów. W rozwiązaniu RSTP węzeł rejestrujący zmianę w topologii rozsyła powiadomienia w sieci, eliminując opóźnienie związane z koniecznością przekazania informacji do węzła głównego.

Osoby korzystające z przełączników Catalyst firmy Cisco z pewnością zauważyły, że w urządzeniach tych zaimplementowano niestandardową odmianę protokołu STP. Obsługując wirtualne sieci LAN (VLAN), przełączniki Cisco wyznaczają oddzielne drzewo rozpinające w każdej sieci VLAN (opisanej w standardzie IEEE 802.1Q). Mechanizm ten jest oznaczany przez firmę Cisco skrótem PVST, pochodzącym od angielskich słów określających drzewo rozpinające w każdym VLAN-ie (*Per-VLAN Spanning Tree*). W przełącznikach Catalyst jest również implementowana wersja protokołu PVST+, wykorzystująca dodatkowo mechanizm tunelowania ruchu. Także organizacja IEEE opracowała standard protokołu wielokrotnych drzew rozpinających (MSTP — *Multiple Spanning Tree Protocol*) — zdefiniowany w dokumentach IEEE 802.1s/Q — który umożliwia tworzenie niezależnych drzew rozpinających w każdej grupie sieci VLAN. Wersja mechanizmu MSTP implementowana w urządzeniach Cisco jest nazywana protokołem drzewa rozpinającego o wielu instancjach (MISTP — *Multiple Instances Spanning Tree Protocol*). Z kolei inne rozwiązanie firmy Cisco — R-PVST — jest połączeniem protokołów RSTP i PVST zapewniającym utworzenie jednego drzewa w każdym VLAN-ie.

## Routerzy cebulowe

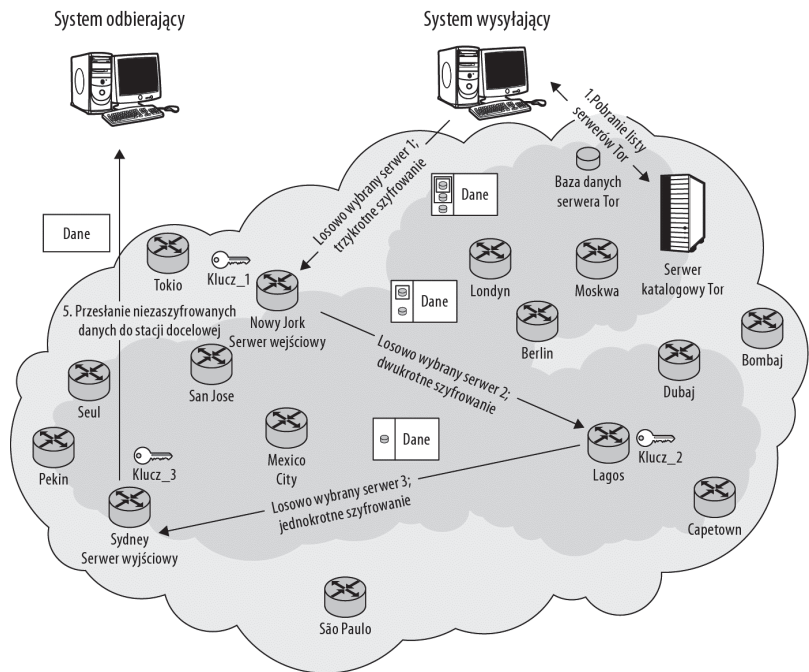
Wszyscy widzieliśmy takie sceny w filmach. Żli chłopcy wysyłają komunikat do dobrych chłopców. Dobrzy chłopcy próbują zlokalizować serwer w Nowym Jorku, ale gdy są gotowi do schwytania złych chłopców, nadchodzi kolejna wiadomość. Tym razem z Singapuru, a potem następna z Berlina. Każda przesyłka jest wysyłana z innego serwera, co sprawia, że ustalenie lokalizacji nadawcy jest niemożliwe. Anonimowa komunikacja stanowi właśnie cel działania routerów cebulowych.

W systemie routerów cebulowych komunikaty sieciowe podlegają wielokrotnemu (trzykrotnemu) szyfrowaniu w jednostce źródłowej i są wysyłane w losowy sposób przez sieć routerów IP (serwery cebulowe). Każdy router usuwa jedną warstwę szyfrowania — tak, jakby się obierało cebulę. Serwer wejściowy jest wybierany losowo spośród mniejszego zbioru serwerów nazywanych strażnikami wejść. Każdy z trzech serwerów — jeden losowo wybrany spośród strażników wejść i dwa inne losowo wskazane spośród ogólnosiwiatowej sieci serwerów cebulowych — wykorzystuje własny klucz prywatny do usunięcia jednej warstwy szyfrowania.

Wiadomość dostarczana do węzła docelowego jest rozszyfrowana, ale odbiorca nie może ustalić, skąd ona pochodzi ani jaką trasę przebyła. Znany jest jedynie adres ostatniego serwera przekazującego dane. Nie tylko odbiorca nie dysponuje informacjami o pochodzeniu przesyłki. Również węzły pośrednie, umiejscowione między źródłem danych i routerem wyjściowym, nie znają adresu źródłowego, treści i przeznaczenia pakietów. Dzięki temu nikt w sieci cebulowej nie może ingerować w komunikację.

Zasada działania systemu routerów cebulowych (Tor — *The onion router*) została zaprezentowana na rysunku 9.17. System nadawczy pobiera listę serwerów Tor z serwera katalogowego Tor (1). Następnie z listy wybiera serwer wejściowy i przesyła do niego trzykrotnie zaszyfrowane dane (2). Serwer wejściowy usuwa pierwsze szyfrowanie i przekazuje informacje do losowo wybranego serwera (3). Ten z kolei usuwa kolejną warstwę szyfrowania. Drugi serwer przesyła dane do trzeciego serwera (4), gdzie pakiety zostają całkowicie rozszyfrowane i w takiej formie przekazane do systemu odbiorczego (5).

**Rysunek 9.17.**  
System routerów  
cebulowych  
gwarantujący  
anonimowość  
w przesyłaniu danych



Celem sieci Tor jest uchronienie użytkowników przed atakami wynikającymi z analizy ruchu. Ataki tego typu polegają na analizowaniu grupy komunikatów po obydwu stronach trasy pakietów w celu ustalenia, które routery sieci są wykorzystywane, i w celu wyznaczenia pewnych wzorców ruchu. Im większą liczbę pakietów uda się przechwycić, tym lepiej. Format komunikatów (to, czy są zaszyfrowane, czy nie) nie ma znaczenia. Celem jest przechwycenie określonej wiadomości. Rozszyfrować można ją później. Często celem bywa również przerwanie komunikacji.

Jeden z rodzajów ataków wymagających przejęcia komunikacji służy do utworzenia połączenia SSH z jednostką atakowaną i określenia zależności czasowych między zwracanymi komunikatami. Czas między poszczególnymi znakami jest analizowany pod względem statystycznym z wykorzystaniem modelu Markowa, na którego podstawie można wydedukować

hasło. Systemy Tor znacznie utrudniają przeprowadzenie podobnych ataków, ale nie uniemożliwiają ich. Trzeba również pamiętać, że ruch opuszczający system routerów cebulowych nie podlega szyfrowaniu i może zostać spreparowany, podobnie jak inne wiadomości.

## Sieci Tor

Routing cebulowy jest technologią, która obecnie została wdrożona jedynie w ramach projektu Tor. Jak nietrudno się domyślić, bezpieczna komunikacja jest kluczowa dla działań wojskowych. Z tego względu początkowo rozwojem routingu cebulowego zajmowało się laboratorium badawcze marynarki wojennej Stanów Zjednoczonych. Projekt drugiej generacji o nazwie The Onion Router (Tor) został zapoczątkowany przez organizację Electronic Frontier Foundation (<http://www.eff.org>) w 2004 roku, a w roku 2006 stał się projektem otwartym o nazwie The Tor Project (<http://www.torproject.org>), prowadzonym przez organizację non profit.

Choć mechanizm routingu cebulowego jest rozwiązaniem, które może zostać zaimplementowane przez każdego, sieć Tor jest jedyną, w której praktycznie je wdrożono. Obecnie lista ogólnosięciowych serwerów Tor zawiera ponad 1800 pozycji — chociaż liczba jednostek działających w danym czasie jest zmienna.

## Jednostki klienckie Tor

Ruch Tor jest generowany przez cebulowe serwery proxy, instalowane w systemie nadawczym. Komponent proxy komunikuje się z usługą katalogową Tor i ustala wirtualny obwód w sieci. Oprogramowanie to jest interfejsem mechanizmu SOCKS. Zatem aplikacje, które tworzą gniazda, mogą skorzystać z komponentu proxy do przesyłania ruchu w sieci Tor w ramach wirtualnego obwodu. Wiadomości są multipleksowane, a następnie wysyłane ustaloną trasą. Wśród aplikacji zdolnych do korzystania z mechanizmu SOCKS są przeglądarki, komunikatory internetowe oraz aplikacje klientów IRC.

Aby w pełni skonfigurować komponent proxy sieci Tor, potrzebne są następujące aplikacje:

- ♦ **Privoxy** (<http://www.privoxy.org>). Aplikacja Privoxy jest filtrującym, pozbawionym buforowania komponentem proxy dla sieci Web. Ułatwia zachowanie prywatności, zarządza danymi cookies, modyfikuje treść stron WWW, przechwytyjąc wyskakujące okna, banery itp. Jest to program darmowy, bazujący na kodzie komponentu Internet Junkbuster. Obecna jego wersja to 3.0.17.
- ♦ **Tor** (<http://www.torproject.org>). Klient Tor zapewnia obsługę protokołu Tor oraz innych komponentów, które umożliwiają korzystanie z sieci Tor.
- ♦ **Torbutton** (<https://www.torproject.org/torbutton>). Program instaluje w przeglądarce Firefox przycisk, który umożliwia włączanie i wyłączanie trybu pracy z siecią Tor.
- ♦ **Vidalia** (<http://www.torproject.org/vidalia>). Graficzny interfejs, który umożliwia monitorowanie i zarządzanie konfiguracją Tor.

Programiści skupieni w ramach projektu Tor ułatwili instalację wymienionych powyżej komponentów i udostępnili pojedynczy instalator ze wszystkimi niezbędnymi elementami. Aby pobrać program kliencki Tor, wystarczy skorzystać z jednej z poniższych stron WWW:

**♦ Instalator dla systemu Windows**

— <https://www.torproject.org/docs/tor-doc-windows.html.en>.

**♦ Instalator dla systemu Mac OS X**

— <https://www.torproject.org/docs/tor-doc-osx.html.en>.

**♦ Instalator dla systemów Linux, BSD, UNIX**

— <https://www.torproject.org/docs/tor-doc-unix.html.en>.

Po zainstalowaniu klienta Tor należy sprawdzić, czy działa poprawnie. Jeden ze sposobów polega na odwołaniu się do ukrytego serwera (opisanego w kolejnym punkcie) w sieci Tor. Wystarczy wpisać w przeglądarce adres <http://duskgytldkxiuqc6.onion> i po transferze danych trwającym około minuty sieć Tor powinna odwzorować adres.

## Ukryte usługi

Serwery Tor pracują w prywatnej domenie o sufiksie *.onion*. Własna domena najwyższego poziomu umożliwia usługom sieciowym — takim jak serwery WWW lub serwery komunikatorów — „ukrywanie” się w sieci Tor. Każda z usług działa niezależnie od innych, a wszystkie one są rozproszone w całej sieci Tor. Każdy użytkownik może skonfigurować własne ukryte usługi i udostępnić je innym użytkownikom w sposób anonimowy. Gdy użytkownik sieci Tor korzysta z usługi, nie jest znana tożsamość ani nadawcy, ani odbiorcy, ani nawet serwerów przetwarzających żądania.

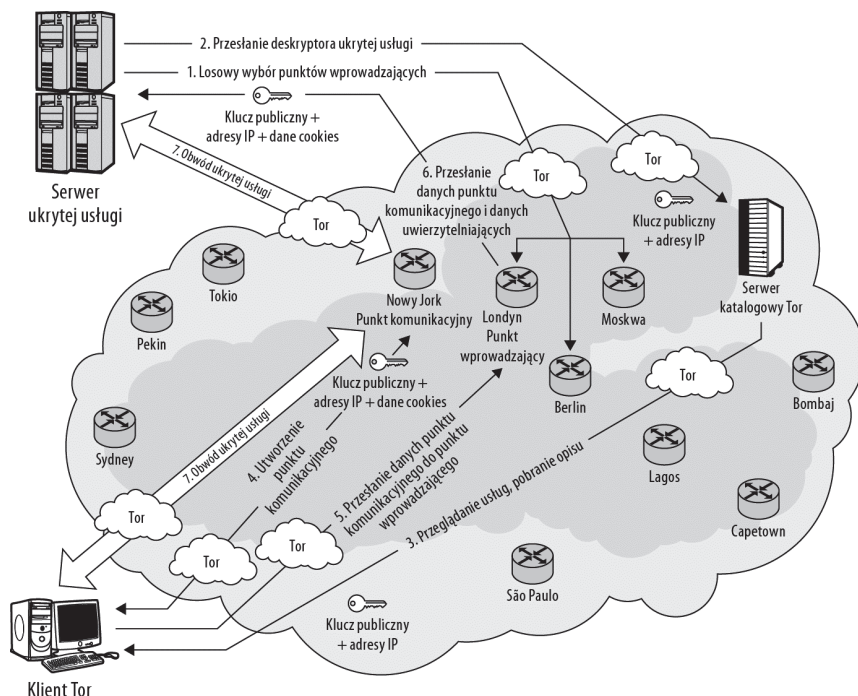
Aby utworzyć ukrytą usługę, wystarczy działający komponent kliencki Tor oraz serwer WWW. Programiści Tor polecają pakiety Samant lub Apache dla systemu Windows bądź `thttpd` dla systemów UNIX i Mac OS X. Serwer WWW musi być skojarzony z portem 5222 jednostki lokalnej. Przypisanie niestandardowego portu powoduje, że system zewnętrzny nie może ustalić, czy usługa jest uruchomiona w systemie lokalnym. Serwer WWW powinien zostać uruchomiony jako niezależny proces — inny niż ewentualne wcześniejsze serwery WWW, szczególnie te, które są udostępniane w internecie lub intranecie.

Schemat działania ukrytych usług został przedstawiony na rysunku 9.18. Zainstalowana usługa powiadamia jednostki klienckie o swojej dostępności (1) za pomocą rozgłoszeń, dostarczanych za pośrednictwem specjalnego protokołu (losowo wybranymi trasami) do serwerów katalogowych Tor, które przechowują taką informację wraz z przypisanym usługę kluczem publicznym. Wspomniane serwery przyjmują rolę punktów wprowadzających i utrzymują klucz publiczny ukrytej usługi (2). Ponieważ trasa między serwerem ukrytej usługi i punktem wprowadzającym obejmuje losowo wybierane obwody wirtualne, klient nie może skojarzyć dwóch systemów, aby poznać adres IP ukrytego serwera.

Klient Tor dowiadyuje się, że usługa pochodzi z serwera katalogowego Tor (3) i tworzy punkt komunikacyjny. Następnie ustanawia połączenie z jednym z serwerów wprowadzających (4). Punkt komunikacyjny dysponuje zarówno kluczem publicznym, jak i danymi cookies, które są potrzebne do szyfrowania (lub deszyfrowania) informacji oraz do generowania informacji umożliwiających przekazanie danych z serwera usługi do klienta Tor. Gdy punkt wprowadzający przekaże informacje klienckie do serwera ukrytej usługi, tworzony jest wirtualny obwód (oznaczony cyfrą 7 i grubszą strzałką). System oddziela punkt wprowadzający od punktu komunikacyjnego, gwarantując zachowanie anonimowości klienta.

**Rysunek 9.18.**

*Ukryte usługi  
w sieci Tor*



Ukryta usługa tworzy deskryptor zawierający klucz publiczny i opis usługi, a następnie podpisuje go kluczem prywatnym. Deskryptor ukrytej usługi jest przekazywany w formie zaszyfrowanej do serwera katalogowego Tor, gdzie jest replikowany i rozsyłany w sieci. Operacja ta zapewnia ukrycie usługi. Serwer katalogowy automatycznie generuje nazwę domenową *<UkrytaUsługa>.onion*, która może być wykorzystywana przez oprogramowanie klienckie Tor. Na tym etapie konfiguracja ukrytej usługi jest zakończona.

Gdy klient chce sprawdzić działanie usługi, pobiera jej deskryptor z serwera katalogowego. Deskryptor zawiera listę punktów wprowadzających oraz klucz publiczny usługi. Klient ustanawia połączenie z losowo wybranym serwerem Tor, żąda od niego pracy w charakterze punktu komunikacyjnego i przesyła do serwera dane cookies z jednorazowym hasłem. Do zaszyfrowania wiadomości wprowadzającej wykorzystywany jest klucz publiczny ukrytego serwera. Sama wiadomość składa się z adresu punktu komunikacyjnego oraz danych cookies z jednorazowym hasłem. Wymiana informacji jest realizowana przez sieć Tor w klasyczny sposób.

Ukryty serwer wykorzystuje informacje zawarte w wiadomości wprowadzającej do utworzenia obwodu z punktem komunikacyjnym, a następnie przesyła do niego hasło, które potwierdza połączenie z klientem Tor. Punkt komunikacyjny przesyła do klienta komunikat informujący o ustanowieniu połączenia. Dwustronna komunikacja między klientem i serwerem ukrytej usługi jest realizowana w ramach wirtualnego obwodu z wykorzystaniem punktu komunikacyjnego jako pośrednika. Obwód składa się z sześciu przekaźników, z których trzy są wybierane przez kliencki komponent obsługi obwodu wirtualnego, a trzy kolejne są wskazywane przez analogiczny komponent po stronie serwera. Wspólnym przekaźnikiem jest punkt wprowadzający.

## Bramy

Brama sieciowa jest urządzeniem lub oprogramowaniem umożliwiającym komunikację między dwoma różnymi sieciami. Bramy tłumaczą adresy, protokoły sieciowe, a nawet dane. Czasami kupuje się je w formie odrębnych urządzeń. W innych przypadkach są instalowane jako oprogramowanie komputera, który pełni funkcję łącznika sieci. Przykładem bramy może być program, który pobiera dane z modułu składania zamówień serwisu WWW i przekazuje stosowne informacje do serwera obsługi płatności, nazywanego bramą kart kredytowych. Innym przykładem może być firewall lub serwer proxy. Adres bramy sieciowej musi zostać określony w każdym interfejsie sieci TCP/IP. Powszechnie są także stosowane bramy pocztowe i bramy stacji roboczych.

Określenie „brama” jest więc raczej terminem marketingowym i musi być postrzegane w szerszym kontekście. Pewne elementy bramy są zawarte w routerze. Nawet funkcja udostępniania połączenia internetowego jest pewnym rodzajem bramy. Tym, co wyróżnia bramy wśród innych urządzeń sieciowych (np. routerów), jest zdolność do wykorzystywania wyższych warstw modelu OSI. Bramy działają w warstwie transportowej, a często również w warstwie aplikacji, czyli najwyższej w stosie protokołów — routery mogą działać w warstwie 4., ale nigdy w warstwie 7.

## Podsumowanie

W tym rozdziale zostały omówione urządzenia przełączające. Przełączniki są niezbędne zarówno w sieciach o przełączanych obwodach, jak i w sieciach pakietowych. Obydwa wymienione rodzaje sieci również zostały tutaj pokrótce opisane.

Klasyfikacja urządzeń przełączających odnosi się do najwyższej warstwy stosu protokołów, która w danym urządzeniu jest wykorzystywana. Koncentratory i regeneratory zapewniają połączenia fizyczne. Mosty wydzielają dwa segmenty sieciowe na poziomie warstwy łącza danych i nie zapewniają translacji protokołów. Routery pracują w warstwie sieciowej, służą do łączenia sieci. „Przełączniki” i „bramy” są określeniami odnoszącymi się do urządzeń, które mogą pełnić różne funkcje.

Tematyka tego rozdziału obejmuje również podstawy routingu. Wyjaśnione zostały różnice między routerami rdzeniowymi i routerami brzegowymi. Przedstawiony został system Tor, który gwarantuje zachowanie anonimowości w czasie pracy sieciowej.

W kolejnym rozdziale opisano różnego rodzaju sieci domowe.



# Część III

# Rodzaje sieci

## **W tej części:**

**Rozdział 10.** Sieci domowe

**Rozdział 11.** Sieci peer-to-peer i osobiste sieci LAN

**Rozdział 12.** Tworzenie sieci lokalnych

**Rozdział 13.** Sieci szkieletowe i rozległe WAN

**Rozdział 14.** Sieci bezprzewodowe

**Rozdział 15.** Sieć pamięci masowej

**Rozdział 16.** Łącza o dużej szybkości



# Rozdział 10.

## Sieci domowe

### **W tym rozdziale:**

- ◆ Elementy sieci domowych
- ◆ Technologie połączeń szerokopasmowych
- ◆ Połączenia bezprzewodowe
- ◆ Różne sposoby przyłączania domowych urządzeń sieciowych
- ◆ Linie telefoniczne i transmisja w sieciach elektrycznych

Z biegiem czasu sieci domowe stają się coraz bardziej zaawansowane technicznie, łatwiejsze w użyciu i powszechniejsze. Większość osób buduje sieci domowe przede wszystkim po to, by mieć dostęp do wspólnego łącza internetowego oraz zasobów i aplikacji sieciowych.

Poszczególne instalacje zazwyczaj są mieszaniną różnych technologii (której elementem mogą być na przykład sieci Wi-Fi, gdy niezbędna jest mobilność urządzeń). Dlatego podczas wyboru odpowiedniego rozwiązania należy wziąć pod uwagę przede wszystkim to, w jaki sposób sieć zostanie przyłączona do internetu oraz jak zostaną połączone różne części domu.

W tym rozdziale omówione zostały niektóre powszechnie stosowane technologie, takie jak Ethernet, HomePNA i HomePlug, ze szczególnym uwzględnieniem ich użyteczności w określonych zastosowaniach.

HomePNA jest rozwiązaniem wykorzystującym linie telefoniczne. Natomiast HomePlug umożliwia przekazywanie danych za pośrednictwem linii energetycznych. Technologie HomePNA i HomePlug są relatywnie nowymi rozwiązaniami oferującymi wyższe szybkości transmisji danych niż starsze techniki komunikacji o podobnym sposobie działania. Interfejsy sieciowe HomePNA są przyłączane bezpośrednio do gniazda telefonicznego. Natomiast interfejsy HomePlug podłącza się do gniazdek napięciowych. Tematyka rozdziału obejmuje również standard Power over Ethernet, który umożliwia zasilanie urządzeń przyłączonych do sieci Ethernet. Rozwiązania te mogą się okazać użyteczne w przypadku łączenia urządzeń znajdujących się w różnych częściach domu, ponieważ stanowią alternatywę dla przeciągania kabli ethernetowych przez ściany.

W dalszej części rozdziału zostały opisane technologie połączeń szerokopasmowych, w tym rozwiązania najczęściej obecnie stosowane, czyli ISDN, DSL, modemy kablowe, połączenia satelitarne i światłowodowe.

Końcowa część jest poświęcona serwerom w sieciach domowych, umożliwiającym zarządzanie instalacją z jednego miejsca oraz pozwalającym na współdzielenie usług sieciowych. W omówieniu tego zagadnienia został uwzględniony krótki opis systemu Windows Home Server.

## Elementy sieci domowej

W ostatnich latach w sieciach domowych można zaobserwować tendencję, która zasługuje na miano renesansu. Częściowo wynika to z faktu, że wiele osób zostaje w domu, zamiast iść do kina lub teatru, częściowo wskutek upowszechnienia się komputerów domowych, a w pewnej części również z powodu większego rozgłosu, jakim cieszą się sieci w ogóle. Postęp w sieciach domowych jest również powodowany dużą liczbą nowych technologii wprowadzanych na rynek oraz starzeniem się wielu dotychczas stosowanych rozwiązań. Tendencja ta jest szczególnie wyraźna, gdy przeanalizuje się dostępność serwerów domowych, wysokowydajnych komponentów sieciowych, wyrafinowanych firewalli i wielu nowych rozwiązań. W dalszej części rozdziału zostało opisanych kilka przewodowych technologii, które zastosowane w domu umożliwiają łączenie urządzeń, często w bardzo wygodny sposób — za pomocą linii telefonicznych lub elektrycznych.

Większość sieci domowych jest tworzona w celu:

- ♦ współdzielenia połączenia internetowego pomiędzy dwoma systemami lub większą ich liczbą;
- ♦ współdzielenia zasobów, takich jak dyski, drukarki i inne urządzenia peryferyjne;
- ♦ sporządzania kopii zapasowych z wykorzystaniem dysków zdalnych;
- ♦ transmitowania strumieni audiowizualnych do domowych urządzeń audio-wideo;
- ♦ wykorzystania telefonii internetowej (VoIP);
- ♦ zapewnienia mobilności laptopów, urządzeń PDA i innych komponentów sieciowych;
- ♦ wspólnego grania w gry komputerowe lub konsolowe.

Biorąc pod uwagę przyczyny budowania sieci, można od razu określić pewne użyteczne rozwiązania:

- ♦ Jeśli niezbędna jest mobilność urządzeń, sieć musi obejmować segment Wi-Fi, zlokalizowany w miejscu, w którym będą działały urządzenia mobilne.
- ♦ Jeśli użytkownicy sieci będą przysyłali pliki o znacznych rozmiarach, należy sprawdzić przepustowość łączy przenoszących ruch. Jako ogólną zasadę można przyjąć, że przekazywanie treści audiowizualnych wymaga zastosowania łączy o przepustowości co najmniej 100 Mb/s (im większa, tym lepiej).

- ♦ Jeżeli w domu są obszary niepołączone ze sobą, trzeba się zastanowić nad sposobem wprowadzenia stosownych łączy. Często oznacza to konieczność przeciągnięcia kabla ethernetowego przez ściany lub wykorzystania linii telefonicznej, kabli elektrycznych bądź utworzenia mostu radiowego (z użyciem komponentów Wi-Fi).
- ♦ W przypadku współdzielenia połączenia internetowego niezbędne jest zastosowanie urządzenia takiego jak router, firewall, brama lub serwer bądź innego komponentu, który zrealizuje zadanie translacji adresów sieciowych (NAT — *Network Address Translation*). Umieszczenie firewalla na styku internetu i sieci domowej może się okazać jedną z najlepszych inwestycji, gdyż zapewni on bezpieczne korzystanie ze współdzielonego połączenia internetowego.
- ♦ Zasoby sieciowe — drukarki, udziały plikowe i różnego rodzaju urządzenia peryferyjne — są obsługiwane przez niemal wszystkie systemy operacyjne. Jeśli są one wykorzystywane w mniejszym stopniu, komunikacja na zasadzie stacji równorzędnych (peer-to-peer) może się okazać wystarczająca. Jednak w przypadku współdziałania większej liczby systemów warto rozważyć uruchomienie serwera lub urządzenia serwerowego, które zagwarantuje wdrożenie centralnego mechanizmu zabezpieczeń.

Połączenia sieci domowej są najczęściej realizowane z wykorzystaniem:

- ♦ Ethernetu (rozwiązanie przewodowe),
- ♦ technologii Wi-Fi zgodnie ze standardami IEEE 802.11x (rozwiązanie bezprzewodowe),
- ♦ linii telefonicznych (rozwiązanie przewodowe) na przykład w technologii HomePNA,
- ♦ kabli elektrycznych (rozwiązanie przewodowe) na przykład w technologii HomePlug,
- ♦ połączeń Bluetooth (rozwiązanie bezprzewodowe).

Dzięki wyjątkowej elastyczności konfiguracji w sieciach domowych powszechnie wykorzystywane są technologie bezprzewodowe — większość sieci tego typu zawiera punkt dostępu bezprzewodowego. Szczegółowo standardy połączeń bezprzewodowych (takie jak Wi-Fi i Bluetooth) zostały opisane w rozdziale 14. Jednak krótka wzmianka na ich temat jest również zamieszczona w tym rozdziale. Większość osób preferuje bowiem łączenie różnych technologii w instalacjach domowych. Lista najczęściej wykorzystywanych technologii sieci domowych została przedstawiona w tabeli 10.1. W zestawieniu zawarto także porównanie najważniejszych cech każdego rozwiązania, takich jak przepustowość, zasięg, koszt, niezawodność, bezpieczeństwo, zachowanie prywatności oraz wady i zalety poszczególnych pozycji.

## Połączenia szerokopasmowe

Określenie „szerokopasmowe” ma wiele znaczeń. Może odnosić się do szerokiego spektrum częstotliwości realizowanej komunikacji. Może także opisywać połączenia z siecią lub internetem o wysokiej przepustowości. Większość użytkowników sieci domowych stosuje je jednak w odniesieniu do połączeń internetowych o dużej szybkości transmisyjnej. Współczynnik liczby łączy szerokopasmowych w zbiorze wszystkich połączeń internetowych jest przez wielu ekonomistów postrzegany jako jeden z kluczowych wskaźników rozwoju gospodarki.

Tabela 10.1. Technologie stosowane w sieciach domowych

Rodzaj	Przepustowość i zasięg	Zastosowania	Koszt	Niezawodność	Bezpieczeństwo i prywatność	Zalety	Wady
Ethernet (802.3)	Do 1 Gb/s w zależności od standardu — kabel CAT 5E. Zasięg 100 m dla 10Base-T, 100Base-TX, 1000Base-T.	AV, K, Z, P	wysoki	wysoka	duże	Szybka transmisja danych, duża popularność standardu, duża dostępność urządzeń, największa elastyczność.	Rozwiązanie kosztowne, szczególnie w przypadku adaptowania starszych instalacji. Wymaga specjalnego okablowania.
Bluetooth (SIG)	W najnowszej wersji (3.0) do 24 Mb/s, w powszechnym użyciu wersja 2, przepustowość do 3,1 Mb/s w obszarze 10 m (klasa 2). Połączenie na częstotliwości radiowej.	K, US, M	umiarkowany	odpowiednia	umiarkowane	Automatyczna konfiguracja i mobilność, technologia stosowana w komputerach, urządzeniach peryferyjnych, urządzeniach przenośnych. Nie wymaga parametryzowania.	Niska przepustowość i mały zasięg.
Wi-Fi (standardy IEEE 802.11x)	600 Mb/s (802.11n), 54 Mb/s (802.11g) na częstotliwości 2,4 GHz. Zasięg 100 m w przypadku standardu 802.11n z dookólnymi antenami, 3 km z antenami kierunkowymi o skupionej wiązce.	AV, K, M, Z	od niskiego do dużego	odpowiednia	umiarkowane	Rozwiązanie standardowe. Duża dostępność urządzeń, duża elastyczność, duża szybkość transmisji w urządzeniach nowego typu. Bezproblemowe współdziałanie z innymi urządzeniami.	Rozwiązanie kosztowne, ograniczony zasięg, podatność na zakłócenia. Wymaga konfiguracji.

HomePNA — sieć z użyciem linii telefonicznych (HomePNA Association 3.1 oraz ITU G9954)	320 Mb/s — linia telefoniczna. Zasięg 300 m.	AV, K, US, Z, P	niski	wysoka	odpowiednie	Szybkość działania, wykorzystanie istniejącej instalacji kablowej, niski koszt, nieskomplikowana instalacja.	Wykorzystanie sieci komputerowej do przyłączania urządzeń.
HomePlug — sieć z użyciem kabli elektrycznych (IEEE P1901)	200 Mb/s w zastosowaniach AV, 14 Mb/s w wersji 1.0. Zasięg 1000 m.	AV, K, US, M, Z, P	umiarkowany	od niskiej do umiarkowanej	wysokie	Szybkość działania, wykorzystanie kabli energetycznych, wygoda, nieskomplikowana instalacja.	Skomplikowany mechanizm transmisyjny. Wymagana bezpośrednia dostępność linii energetycznych.

Opis: AV — multimedia, K — komunikacja głosowa, US — urządzenia sterujące, M — urządzenia mobilne, Z — współdzielenie zasobów, P — planowanie (kalendarz).

Jedna z definicji określa połączenia szerokopasmowe jako te, które zapewniają przepustowość o co najmniej kilkakrotnie wyższej wartości niż gwarantowana w połączeniach modemowych. W 2008 roku Federalna Komisja Komunikacji Stanów Zjednoczonych opisała połączenia szerokopasmowe jako połączenia o szybkości pobierania danych przekraczającej 768 kb/s. W Europie Międzynarodowa Unia Telekomunikacyjna (Sektor Standaryzacji) wyznaczyła minimalną przepustowość łącza określanego mianem szerokopasmowego na 2 Mb/s, odpowiadającą szybkości łącza PRI w standardzie ISDN.

Wartość przepustowości wyznaczająca dolną granicę połączenia szerokopasmowego będzie się oczywiście zwiększać wraz z upływem czasu. Z kolei do jej określenia celowo przyjęto szybkość pobierania danych, ponieważ większość osób wykorzystuje połączenia szerokopasmowe do pobierania treści, a nie do wysyłania danych. Dlatego większość łączy tego typu ma charakter asymetryczny.

Dostawcy usług internetowych, określając szybkość połączenia, zazwyczaj podają wartości odpowiadające najbardziej optymistycznemu wariantowi. Wiele usług współdzielących pasmo z grupą abonentów sieci (w przypadku sieci osiedlowych lub instalacji budynkowych) ma znacznie mniejszą szybkość działania w czasie zwiększonego natężenia ruchu. Aby wyeliminować ten problem, część dostawców usług internetowych stosuje techniki kształtowania ruchu, dławienia ruchu lub nakładania trwałych ograniczeń, które prowadzą do uzyskania zadowalającej wydajności usług.

Gdy powstawała ta książka, większość połączeń szerokopasmowych była realizowana w ramach cyfrowych linii abonenckich, łączy DSL lub sieci kablowych. Sieci optyczne były dopiero wdrażane przez kilka firm i miały ograniczony zasięg geograficzny.

Oto lista powszechnie stosowanych technologii szerokopasmowych:

- ♦ **Transmisja danych w liniach telefonicznych standardu ISDN.** Łącza ISDN są instalowane w dwóch wariantach — ISDN-BRI o dwóch kanałach B o przepływności 64 kb/s każdy i łącznej przepustowości dla użytkownika końcowego 128 kb/s oraz ISDN-PRI o 30 kanałach B o łącznej przepustowości dla użytkownika końcowego 1 920 kb/s (w Stanach Zjednoczonych obowiązuje standard ISDN o 23 kanałach i łącznej przepustowości dla użytkownika końcowego 1472 kb/s). Całkowita przepustowość poszczególnych łączy ISDN jest większa, co wynika z potrzeby przesyłania sygnalizacji i synchronizacji. Dla łącza BRI wynosi 144 kb/s (16 kb/s — sygnalizacja), PRI Europa — 2 048 kb/s (128 kb/s sygnalizacja i synchronizacja), PRI USA — 1544 kb/s (72 kb/s — sygnalizacja i synchronizacja). Łącza ISDN tracą popularność z uwagi na większe zainteresowanie użytkowników połączeniami DSL i kablowymi.

Kanały B są wykorzystywane w telefonii jako kanały rozmówne, stąd ich przepustowość 64 kb/s.

Technologie ISDN i DSL zostały szczegółowo opisane w rozdziale 13.



- ♦ **Cyfrowe linie abonenckie (DSL — *Digital Subscriber Line*).** Instalacje DSL wykorzystują linie telefoniczne do świadczenia usług cyfrowych i łączenia abonentów z siecią internetową. Większość oferowanych łączy DSL to połączenia asymetryczne — ADSL. Przepływność strumienia danych skierowanych do abonenta zawiera się zazwyczaj w przedziale od 512 kb/s do 20 Mb/s. Z kolei szybkość wysyłania danych do sieci wynosi od 256 kb/s do 1 Mb/s.

- ♦ **Modemy kablowe.** Technologia ta jest powszechnie stosowana w Ameryce Północnej, Europie, Australii, Nowej Zelandii i niektórych krajach Ameryki Środkowej. Typowa przepustowość modemu kablowego wynosi od 1 Mb/s do 120 Mb/s w kierunku do użytkownika oraz od 128 kb/s do 10 Mb/s w kierunku do sieci.

Modemy kablowe odgrywają rolę mostów sieciowych (są urządzeniami warstwy łącza danych), które łączą sieci domowe z internetem za pośrednictwem sieci telewizji kablowej. Po stronie sieci interfejs modemu jest zgodny ze standardem Ethernet. Natomiast po stronie instalacji telewizyjnej obsługuje standard DOCSIS. System DOCSIS jest następcą opracowanego przez firmę Motorola protokołu łącza danych w sieciach kablowych (CDLP — *Cable Data Link Protocol*) na poziomie warstwy fizycznej oraz mechanizmu warstwy łącza danych przygotowanego przez firmę LANcity do pracy w standardzie NTSC. W Europie stosowana jest technologia zgodna ze standardem emisji PAL o nazwie EuroDOCSIS.

- ♦ **Łącza satelitarne.** Wykorzystanie łącz satelitarnych w celu zapewnienia dostępu do internetu jest powszechną praktyką w obszarach nieurbanizowanych, w których układanie instalacji kablowych okazuje się niepraktyczne. System składa się z satelitów geostacjonarnych, usytuowanych 35 786 km nad ziemią, czyli 42 164 km od środka Ziemi. Aby łączność była możliwa, konieczne jest skierowanie anteny w stronę satelity.

Z uwagi na odległość między Ziemią a satelitą w łączności satelitarnej obserwuje się relatywnie duże opóźnienia (około 200 milisekundowe). Ogólnie zasada stanowi, że szybkość pobierania danych jest porównywalna z innymi technologiami szerokopasmowymi i zawiera się w przedziale od 256 kb/s do 4 Mb/s. Niestety, przesyłanie informacji do sieci jest znacznie mniej efektywne i ogranicza się do 64 kb/s lub 384 kb/s. Opóźnienia i niewielka przepustowość wysyłania sprawiają, że technologie satelitarne mają ograniczone zastosowania.

- ♦ **Połączenia światłowodowe.** Połączenia światłowodowe są wykorzystywane w dostępie do internetu, telefonii i usługach telewizji kablowej. Oferowane są łącza o różnej przepustowości. Szybkość pobierania danych mieści się w przedziale od 10 Mb/s do 1 Gb/s, natomiast wysyłania od 2 Mb/s do 400 Mb/s.

## Połączenia bezprzewodowe

Połączenia bezprzewodowe są wyjątkowo wygodną formą łączenia urządzeń sieci domowej. Z tego względu część instalacji domowych w całości bazuje na komunikacji bezprzewodowej. Niemniej w większości przypadków połączenia bezprzewodowe są stosowane jedynie do przyłączania urządzeń mobilnych lub złączania obszarów domu, w których nie można zastosować klasycznego połączenia kablowego. Routery bezprzewodowe i łącza radiowe są także wykorzystywane przez wielu dostawców usług internetowych w świadczonych przez nich usługach.

Niemal wszystkie urządzenia sieciowe przeznaczone na rynek komponentów domowych są zgodne ze standardami IEEE, które definiują zbiór technologii operujących w kilku pasmach częstotliwościowych między 900 MHz a 5 GHz. Wszystkie rozwiązania zgodne z zaleceniami są oznaczane symbolem Wi-Fi. Prawa do korzystania z oznaczenia udziela grupa producentów, która zarządza standardami i czuwa nad tym, aby produkowane układy logiczne i urządzenia były ze sobą zgodne.



Technologie bezprzewodowe zostały szczegółowo opisane w rozdziale 14. Jest on w całości poświęcony rozwiązaniom Wi-Fi. Zawiera szczegółowe omówienia poszczególnych wersji standardu, a także zasad wykorzystania częstotliwości radiowych, technik budowania sieci i połączeń między różnymi komponentami. W rozdziale tym zostały również opisane metody kodowania sygnałów Wi-Fi oraz zasady konfigurowania połączeń.

## Połączenia stałe

We wcześniejszej części rozdziału zamieszczone zostały informacje o szerokopasmowych połączeniach sieci domowej z internetem. Wydawałoby się, że budowanie sieci sprowadza się do doprowadzenia łączy internetowego do routera bezprzewodowego i przyłączenia do niego urządzeń bezprzewodowych lub jednostek sieci stałej (jeśli ktoś mieszka w nowym budynku, w którym kabel Cat5e lub Cat6 znajduje się w każdym pomieszczeniu). Niestety, wiele osób nie ma tyle szczęścia, aby na tym zakończyć pracę. Bardzo często zdarza się tak, że urządzenia są rozmieszczone w różnych obszarach domu, które są okablowane niezależnie od siebie. Powstaje wówczas problem połączenia tych obszarów. Przykładem takiej sytuacji może być oddzielne okablowanie sypialni znajdującej się na piętrze budynku, salonu zlokalizowanego na parterze czy biura przeniesionego do piwnicy.

Oczywiście problem może rozwiązać zatrudnienie elektryka, który wywierci dziury w ścianach lub stropach i przeciągnie kable łączące poszczególne części domu. Jednak wykonanie instalacji w ten sposób jest niewygodne i kosztowne, a w niektórych przypadkach może się okazać niepraktyczne lub nieopłacalne, choć z drugiej strony gwarantuje uzyskanie najszybszych możliwych połączeń. W kolejnych punktach podrozdziału zostały opisane rozwiązania umożliwiające zrealizowanie zadania przez wykorzystanie istniejącej instalacji kablowej (linii telefonicznych i kabli elektrycznych) i utworzenie za jej pomocą łączy między poszczególnymi obszarami sieci domowej. Omówienie obejmuje okablowanie ethernetowe, rozwiązania Power over Ethernet (PoE), połączenia HomePNA realizowane na bazie linii telefonicznych oraz wykorzystanie sieci energetycznych w rozwiązaniach HomePlug.

## Ethernet

Bezpośrednie połączenia ethernetowe z siecią WAN nie są powszechnie stosowanym rozwiązaniem w sieciach domowych. Usługa ta jest jednak coraz powszechniej oferowana klientom korporacyjnym i najprawdopodobniej kiedyś będzie także dostępna dla klientów indywidualnych. Protokoły ethernetowe przeznaczone do wykorzystania w łączu dostępowym zostały zdefiniowane w standardzie IEEE 802.3ah.

Standard ten znany jest pod nazwą Ethernet in the First Mile (EFM) — Ethernet na pierwszej mili — i opisuje następujące rodzaje mediów fizycznych:

- ♦ **Przewody miedziane.** Jest to rozwiązanie o nazwie EMF over Copper (EFMCu) — EMF na bazie miedzi — przeznaczone do wykorzystania w łączach charakterystycznych dla połączeń głosowych, które mogą być agregowane w kilka niezależnych linii. Zdefiniowano dwa warianty technologii EFMCu — 2BASE-TL oraz 10PASS-TS.

- ♦ **Włókno dla światła o dużej długości fali.** Przyłącze internetowe może zostać wykonane w ramach pojedynczego lub podwójnego włókna światłowodowego.
- ♦ **Włókno w rozwiązaniu punkt-wielopunkt (P2MP — *Point to Multipoint*).** Przyłącza ethernetowe tego typu są oferowane pod nazwą Ethernetu w pasywnych sieciach optycznych (EPON — *Ethernet over Passive Optical Networks*).

Opracowany przez organizację IEEE standard EFM odnosi się również do zasad instalacji i zarządzania połączeniami ethernetowymi, a także sposobów zagwarantowania współdziałania technologii z innymi powszechnie stosowanymi rozwiązaniami. Obecnie opracowanie mechanizmów EFM EPON należy do zadań grupy IEEE Metro Ethernet Forum, która pracuje nad wersją EPON o przepustowości 10 Gb/s, nazywaną XEPON.



Szczegółowe omówienie Ethernetu znajduje się w rozdziale 12.

## Linie telefoniczne

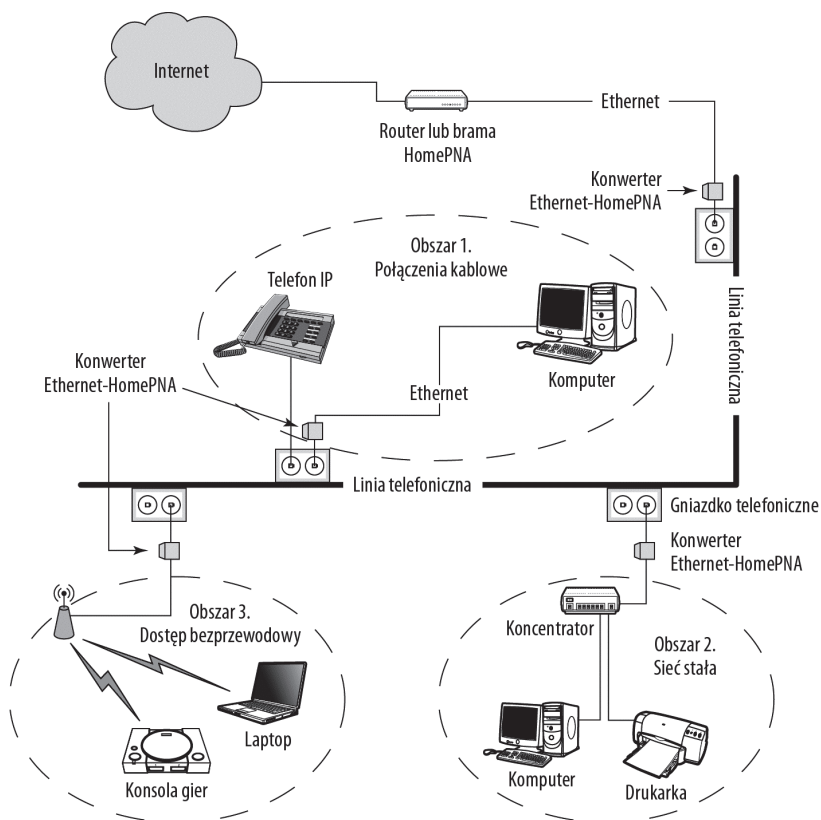
Urządzenia łączące komputery za pomocą linii telefonicznych wewnątrz budynków są dostępne na rynku od wielu lat. Jednym z pierwszych systemów tego typu było oferowane przez firmę Farallon (obecnie Netopia) rozwiązanie, które umożliwiało jednostkom Macintosh komunikowanie się bez konieczności wykorzystania połączeń Apple LocalTalk. Jako medium fizyczne wykorzystano wolne pary kabla telefonicznego. Działo się to w czasach, gdy linie telefoniczne były jedynymi przyłączami telekomunikacyjnymi doprowadzanymi do domów. Dzisiaj wydaje się, że wszystko, co się porusza, ma własny numer telefonu, a pojęcie wolnych przewodów telefonicznych w ogóle nie ma zastosowania.

Najnowsza wersja rozwiązania została zaprojektowana z myślą o wykorzystaniu przewodów telefonicznych będących w ciągłym użyciu. Jest to możliwe dzięki zastosowaniu częstotliwości zbędnych w komunikacji głosowej. Posłużono się również innymi modulacjami, które zapewniają, że dane są poprawnie odbierane w jednostce docelowej. Najpowszechniej wykorzystywaną technologią wymiany informacji w łączach telefonicznych jest mechanizm HomePNA. Osoby, którym znane są starsze rozwiązania bazujące na liniach telefonicznych (zapewniające transfer danych nawet na poziomie 10 Mb/s), powinny zainteresować się najnowszym standardem HomePNA. Jest on bowiem przeznaczony do przekazywania plików multimedialnych o dużych rozmiarach z relatywnie dużą przepływnością bitową.

Urządzenia wchodzące w skład systemu HomePNA zostały przedstawione na rysunku 10.1. Widoczny na nim router jest połączony z internetem oraz z siecią Ethernet. Zapewnia on dostęp do internetu innym urządzeniom sieciowym, które są z kolei przyłączone do niego za pomocą konwerterów Ethernet-PNA stanowiących zakończenie poszczególnych linii telefonicznych. W każdym z przedstawionych obszarów konwerter Ethernet-PNA jest włożony do gniazdka telefonicznego. Z kolei kabel ethernetowy jest doprowadzany do każdego z urządzeń sieciowych. Na rysunku zostały zaprezentowane trzy różne obszary domu, połączone ze sobą siecią PNA — obszar 1. jest zbiorem urządzeń sieci stałej, obszar 2. obejmuje jednostki przyłączone do koncentratora sieciowego, natomiast w obszarze 3. działa punkt dostępu bezprzewodowego, z którym komunikują się stacje bezprzewodowe.

**Rysunek 10.1.**

Technologia HomePNA, umożliwiająca łączenie sieci komputerowych z wykorzystaniem linii telefonicznych bez dodatkowych modyfikacji



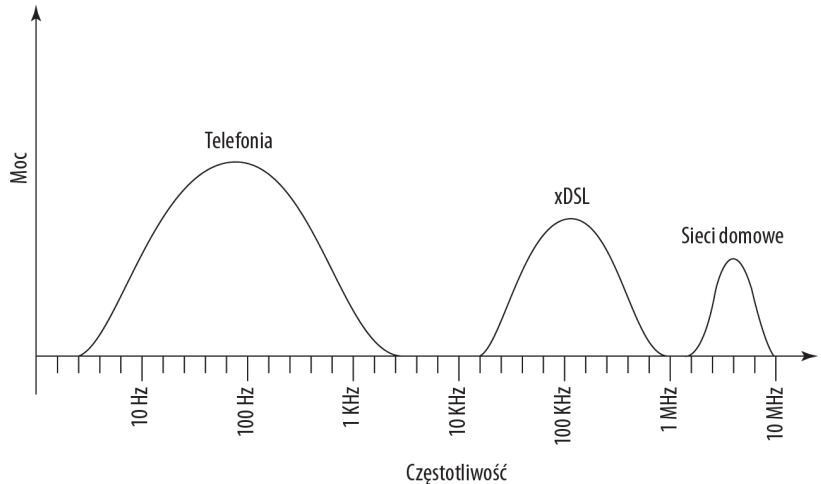
Połączenia sieciowe bazujące na instalacji telefonicznej są wyjątkowo wygodnym rozwiązaniem. Pozwalają na przyłączenie urządzeń do sieci bezpośrednio za pomocą interfejsu telefonicznego lub konwertera Ethernet-telefon. Nie ma w tym przypadku znaczenia rodzaj usługi telefonicznej — opisany system wykorzystuje przewody telefoniczne jedynie jako fizyczne medium transmisji danych i działa niezależnie od samej telefonii. Ważne jest jednak to, aby poszczególne linie były elementami jednego obwodu telefonicznego. Jeśli instalacja domowa obejmuje kilka linii telefonicznych, konieczne jest utworzenie niezależnych połączeń sieciowych w ramach każdej z tych linii.

Najnowsze wersje produktów HomePNA są zgodne ze standardem HomePNA 3.1, opracowanym przez stowarzyszenie producentów urządzeń sieciowych wykorzystujących linie telefoniczne (<http://www.homepna.org>). Umożliwiają one dostarczanie usług IP, takich jak transfer danych, telefonia internetowa oraz telewizja internetowa (czyli usług „triple play” realizowanych w przedziale częstotliwościowym przedstawionym na rysunku 10.2), za pośrednictwem istniejących kabli współosiowych lub telefonicznych. Standard HomePNA 3.1 posłużył również jako podstawa opracowanego (w styczniu 2007 roku) przez Międzynarodową Unię Telekomunikacyjną standardu G.9953.

Na rysunku 10.2 została przedstawiona zależność między mocą sygnału a jego częstotliwością w przypadku transmisji w linii telefonicznej. Sieci HomePNA zapewniają współdziałanie różnych technologii — telefonii (usług wąskopasmowych), łączy DSL oraz połączeń

**Rysunek 10.2.**

*Podział sieci HomePNA na pasma głosowe, internetowe i sieci domowe*



ethernetowych. Dzięki zastosowaniu oddzielnych przedziałów częstotliwościowych sygnały mogą być przekazywane w ramach jednego medium fizycznego bez wzajemnych interferencji.

Standard HomePNA bazuje na rozwiązaniach firm Broadcom i Copper Solutions. Firma Broadcom sprzedaje dwa układy ASIC niezbędne w komunikacji z innymi urządzeniami, stanowiące główne elementy architektury. Komponent MC4100 jest urządzeniem nadawczo-odbiorczym sygnału analogowego — przetwornikiem analogowo-cyfrowym — odpowiedzialnym za wysyłanie i odbieranie sygnałów linii telefonicznej. Z kolei kontroler PCI/MSI BCM4110 wysyła dane lub odtwarza dane, wykorzystując multipleksację z podziałem częstotliwości (FDM), dzięki czemu możliwe jest wykorzystanie tych samych przewodów, w których są przekazywane sygnały telefoniczne.

Przyłączenie komputera do gniazda telefonicznego RJ-11 wymaga zastosowania konwertera sieciowego HomePNA. Jest on produkowany w formie karty rozszerzeń PCI (lub kart PC) bądź jako urządzenie USB. Przyłącze może mieć długość do 300 m i obsługiwać do 50 urządzeń. Sieci HomePNA obejmują budynki o powierzchni do 900 metrów kwadratowych. W wersji 3.1 standardu przewidziano przepustowość 320 Mb/s podczas transmisji w kablu współosiowym. Jednak obecnie dostępne urządzenia pracują z przepustowością do 128 Mb/s. Rozwiązania HomePNA są adresowane głównie do dostawców usług internetowych i firm telekomunikacyjnych, gdyż umożliwiają zdalne zarządzanie łączami i ich diagnozowanie, zagwarantowanie współczynnika QoS oraz ujednolicanie taryfikacji. Twórcy technologii HomePNA zapewniają, że system jest zgodny z 99 procentami instalacji domowych w Stanach Zjednoczonych. W segmentach, w których telefony lub faksy wprowadzają zbyt wiele zakłóceń, urządzenia te powinny być przyłączane z wykorzystaniem filtra dolnoprzepustowego — podobnie jak w przypadku połączeń DSL.

Wśród przetestowanych i certyfikowanych produktów znajdują się moduły typu set-top box, bramy ADSL i VDSL, mosty Ethernet-HomePNA 3.1 i routery bezprzewodowe Wi-Fi. Pełna lista komponentów, które uzyskały certyfikat HomePNA, znajduje się na stronie internetowej [http://www.homepna.org/products/member\\_products](http://www.homepna.org/products/member_products) (lista ta zawiera również odnośniki do witryn producentów poszczególnych urządzeń).

## Zasilanie przez Ethernet

Zasilanie przez Ethernet (PoE — *Power over Ethernet*) jest rozwiązaniem, które pozwala na wymianę danych i jednocześnie doprowadzenie zasilania z komponentu nazywanego urządzeniem źródła zasilania (PSD — *Power Sourcing Device*) do urządzenia zasilanego (PD — *Power Device*). Dzięki niemu urządzenie PD jest mobilne — można je przyłączyć do dowolnego portu ethernetowego bez konieczności doprowadzania linii zasilającej. Technologia została opracowana przez firmę Cisco w roku 2000, aby ułatwić instalację urządzeń telefonii, punktów dostępowych, kamer internetowych oraz innych komponentów sieciowych.

Technika PoE stała się standardem IEEE wraz z opublikowaniem specyfikacji IEEE 802.3-2005 (802.3af). Niemal wszystkie produkowane od tego czasu urządzenia PoE są zgodne z tym standardem. Część całościowej specyfikacji odnosząca się do zasilania przez Ethernet jest oznaczana jako 802.3af. Gama urządzeń PoE rozciąga się od prostych konwerterów, które pozwalają na połączenie gniazdka sieciowego z jednym przyłączem (lub dwoma przyłączami) Ethernet RJ-45, do przełączników korporacyjnych, które umożliwiają przyłączanie różnych urządzeń do jednego z 48 portów PoE. Systemy PoE w większości przypadków wykorzystują istniejące okablowanie budynkowe. Nie wymagają eksponowania gniazd zasilających. Są też odporniejsze na zaniki prądu, ponieważ zasilanie komponentów PSD można podtrzymywać za pomocą urządzeń zasilania zapasowego (UPS) — połączenia pozostaną wówczas aktywne. Przyłączone do sieci PoE urządzenia można przenosić dowolnie w zasięgu sieci, co w przypadku bezprzewodowych instalacji LAN oznacza dużą łatwość planowania pokrycia terenu zasięgiem sygnału Wi-Fi.

Zgodnie ze standardem 802.3af zasilanie może być przekazywane za pomocą dwóch nieużywanych par przewodów lub w czterech parach przewodów kabla CAT3 (CAT 5e) razem z danymi. Komponenty PSD i PD mogą wykorzystywać wolne pary lub pary sygnałowe, ale muszą być zgodne z jednym z tych rozwiązań. Niezależnie od wybranej konfiguracji dostarczane jest zasilanie o napięciu 48 V i mocy 13 W (w najnowszym standardzie 802.3at określanym jako PoE plus zdefiniowane jest zasilanie o mocy do 25,5 W; część producentów posiada w swojej ofercie urządzenia pozwalające na dostarczenie zasilania o mocy do 60 W). Obydwa warianty rozwiązania zostały przedstawione na rysunku 10.3. W pierwszym zasilanie jest dostarczane za pomocą osobnych przewodów. Natomiast w drugim jest przekazywane wraz z danymi.

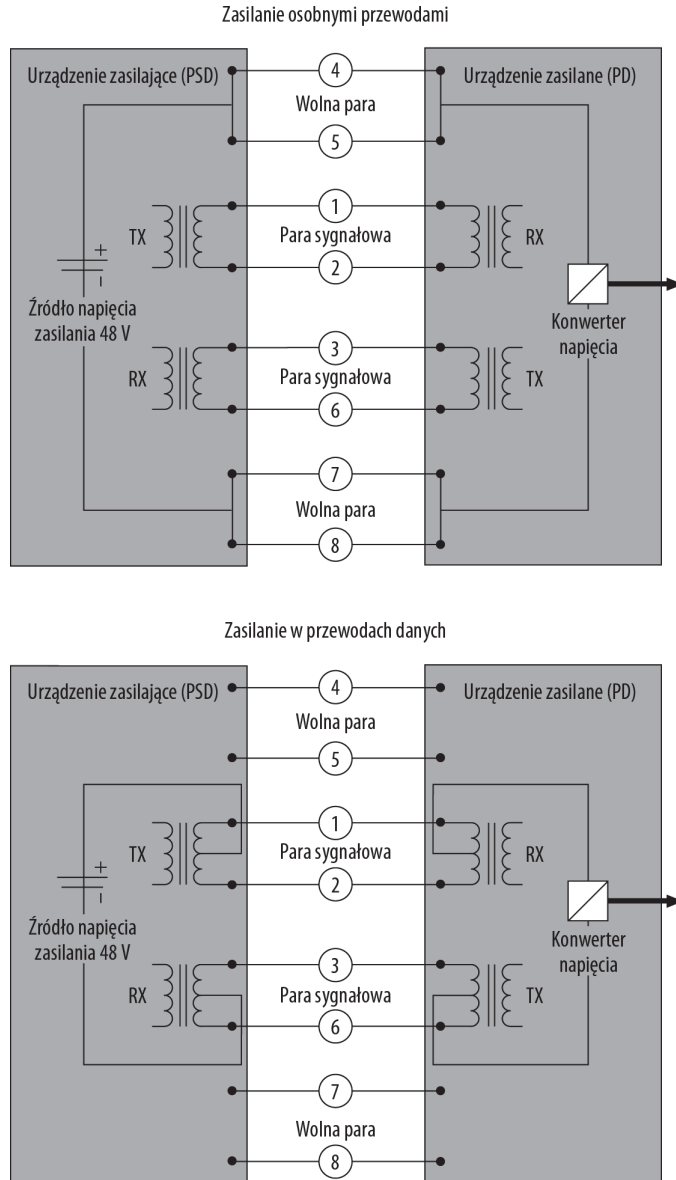
## Technologia HomePlug

Urządzenia technologii HomePlug wykorzystują domową instalację elektryczną do łączenia ze sobą komponentów sieci Ethernet. W zależności od zastosowanej modulacji przepustowość łączy HomePlug zawiera się w granicach od 1 Mb/s do 13,8 Mb/s. Opracowane zostały dwie wersje standardu — HomePlug 1.0 oraz HomePlug AV. Rozwiązanie HomePlug AV jest przeznaczone do obsługi aplikacji audiowizualnych, takich jak transmisja sygnału telewizji wysokiej rozdzielczości w sieci komputerowej. Przepustowość łączy w tym przypadku może wynosić nawet 200 Mb/s.

W produktach HomePlug działanie mechanizmu komunikacji bazuje na specyfikacji opracowanej przez stowarzyszenie HomePlug Powerline Alliance. Organizacja IEEE opracowuje standard oznaczony jako IEEE P1901, który ma zunifikować systemy HomePlug konkurujących ze sobą producentów (między innymi firm Panasonic i Universal Powerline Association).

**Rysunek 10.3.**

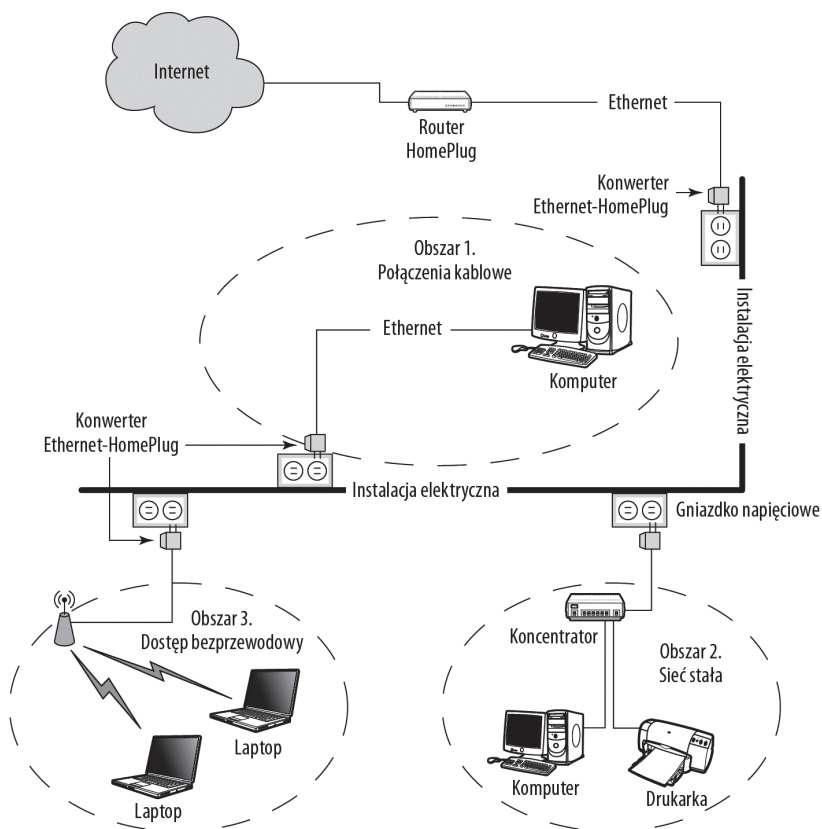
*Dwa sposoby  
dostarczania zasilania  
przez przewody  
ethernetowe*



Na rysunku 10.4 został pokazany sposób użycia kabli elektrycznych do łączenia ze sobą urządzeń znajdujących się w różnych pomieszczeniach domu. W rozwiązaniu tym wykorzystywana jest topologia identyczna z omawianą wcześniej technologią HomePNA. Router HomePlug łączy internet z siecią elektryczną domu, w czym pośredniczy konwerter ethernetowy przyłączony do gniazdka napięciowego. Każdy z obszarów budynku jest przyłączony do sieci za pomocą kolejnych konwerterów.

Zastosowanie routerów, mostów i odpowiednich konwerterów umożliwia połączenie obszarów o różnym przeznaczeniu. Zazwyczaj użytkownik wtyka do gniazdka elektrycznego specjalny konwerter, który następnie łączy z urządzeniem sieciowym za pomocą portu USB

**Rysunek 10.4.**  
Sieć elektryczna  
łącząca trzy różne  
obszary domu



lub Ethernet. Taki sposób tworzenia połączeń sieciowych jest relatywnie nowy, więc należy się spodziewać zwiększenia szybkości wymiany danych wraz z opracowywaniem kolejnych generacji elementów sieciowych. Trzeba jednak pamiętać, że w domach ze starszą instalacją elektryczną mogą wystąpić ograniczenia w przepustowości połączeń. Poza tym transmisja w sieciach elektrycznych jest narażona na zakłócenia. Dlatego przed zakupem określonego modelu urządzenia warto się upewnić, że będzie je można zwrócić lub wymienić na inne, gdyby się okazało, że nie będzie realizowało swoich zadań w określonym środowisku.

Biorąc pod uwagę ilość zakłóceń i zmienne warunki transmisyjne, możliwość przekazywania danych w sieciach energetycznych wydaje się nieco zaskakująca. Obciążenie każdego z połączeń ma przecież inną impedancję, a sposób wykonania instalacji jest różny w różnych miejscach. Amplituda i faza sygnału zmieniają się wraz z częstotliwością, nierzadko tak istotnie, że na niektórych częstotliwościach sygnał jest niemal całkowicie wytłumiony, przy jednoczesnym braku jakiegokolwiek tłumienia w innym przedziale częstotliwościowym. Parametry kanału transmisyjnego podlegają zmianom w czasie i zależą od bieżącego obciążenia linii. Wiele urządzeń wnosi bowiem zakłócenia do linii energetycznych, które mogą przesłonić sygnał danych. Dotyczy to przede wszystkim oświetlenia halogenowego, silników elektrycznych oraz przełączników, które generują oscylacje i impulsy elektryczne.



Konwertery HomePlug muszą być włączane bezpośrednio do gniazdek elektrycznych. Stosowanie listew zasilających wprowadza zakłócenia w transmisjach radiowych.

## Modulacja w połączeniach HomePlug

W rozwiązaniach HomePlug stosowana jest technologia transmisji nazywana ortogonalną multipleksacją w dziedzinie częstotliwości (OFDM — *Orthogonal Frequency Division Multiplexing*). Tę samą technikę modulacji wykorzystuje się w łączach DSL, telewizji oraz połączeniach Wi-Fi 802.11a i 802.11g.

Modulacja OFDM polega na podzieleniu dostępnego przedziału częstotliwościowego na wąskie pasma, co w przypadku sieci HomePlug oznacza wydzielenie 84 równomiernie rozmieszczonych nośnych w przedziale od 4,5 MHz do 21 MHz. Sygnał jest transmitowany w oddzielnych kanałach składowych w taki sposób, że poszczególne nośne nakładają się na siebie, ale pozostają wzajemnie ortogonalne. Wszystkie nośne są modulowane zgodnie z jedną z wielu technik modulacji. W przypadku systemu HomePlug stosowane jest różnicowe binarne kluczowanie fazy (DBPSK — *Differential Binary Phase-Shift Keying*) oraz różnicowe kwadraturowe kluczowanie fazy (DQPSK — *Differential Quadrature Phase-Shift Keying*). Siła sygnału każdego kanału jest niezależna od zaników obserwowanych w innych kanałach. Na podstawie sygnałów odebranych w części kanałów można ustalić przebieg całego sygnału, i to bez konieczności stosowania elektronicznych obwodów kształtowania sygnału. Jego odtworzenie jest zadaniem matematycznym, wykonywanym dzięki mechanizmom wyprzedzającej korekcji błędów oraz technice przeplatania danych. Metoda wyprzedzającej korekcji błędów (FEC — *Forward Error Correction*) polega na wysyłaniu nadmiarowych informacji, które pozwalają na ustalenie, czy dane użytkowe nie zostały przekłamanie, oraz na naprawienie nieznacznych zniekształceń. Przeplatanie danych jest z kolei techniką dzielenia bloków danych i transmitowania ich w różnych nienastępujących po sobie okresach, dzięki czemu kolejno następujące po sobie błędy można łatwo skorygować.

Ponieważ warunki transmisyjne w instalacji elektrycznej są różne w poszczególnych miejscach, urządzenia HomePlug mierzą przepływność poszczególnych kanałów składowych i wyłączają te z kanałów, które są szczególnie mocno tłumione lub zakłócone. Proces ten nazywa się *alokacją tonów*. Ponadto w zależności od parametrów połączenia mogą być wybierane różne techniki modulacji — w tym  $\frac{1}{2}$  DBPSK,  $\frac{1}{2}$  DQPSK oraz  $\frac{3}{4}$  DQPSK. Połączenie odpowiedniego doboru modulacji z mechanizmem wyprzedzającej korekcji błędów znacznie obniża stopień błędów w przekazywanych strumieniach danych. Sam proces dostosowywania parametrów transmisji nazywa się optymalizacją kanału i jest bardzo ważnym elementem komunikacji.

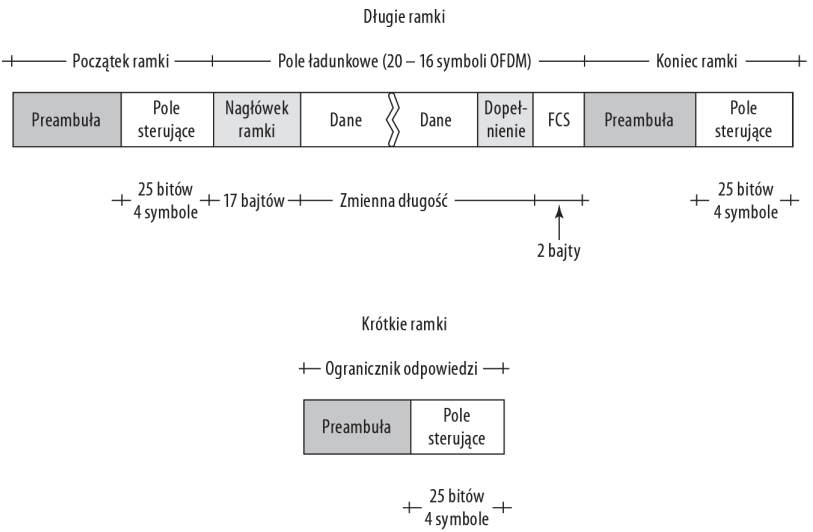
Ponieważ wymiana danych w łączach HomePlug ma charakter połączenia punkt-punkt, do realizacji transmisji rozgłoszeniowej potrzebne są inne mechanizmy. Rozwiązanie polega na zastosowaniu modulacji DBPSK i wysyłaniu wielu kopii każdego bitu w różnym czasie, na różnych częstotliwościach, przy wykorzystaniu wspólnego mechanizmu korekcji błędów. W terminologii HomePlug postępowanie to jest określone mianem modulacji ROBO. W operacjach ROBO zmianie ulega także struktura wysyłanych ramek, co jest związane z dostosowaniem transmisji do parametrów kanału.

Ramki i sekwencje danych

Protokół kontroli dostępu do medium transmisyjnego (MAC — *Medium Access Control*) w systemie HomePlug wywodzi się z mechanizmu formowania ramek IEEE 802.3. W obydwu standardach stosowane są ramki o dużej pojemności. Gwarantuje to wysoką zgodność połączeń HomePlug z połączeniami ethernetowymi, wymagającą jedynie nieznacznego narzutu na dodatkowe przetwarzanie informacji. Warstwa MAC sieci HomePlug szyfruje ramki wprowadzane do sieci elektrycznej i dodaje do nich specjalny nagłówek. Urządzenie odbiorcze odtwarza pierwotną kolejność ramek i rozszyfrowuje ich treść, a następnie przekazuje ją dalej. Jeśli ramka ethernetowa została zaszyfrowana przed wysłaniem z komputera (na przykład za pomocą mechanizmu IPSec), będzie dostarczona do jednostki docelowej w formie zaszyfrowanej.

W standardzie HomePlug wyróżniono dwa rodzaje ramek — krótkie, do przekazywania komunikatów związanych z utrzymaniem łącza, oraz długie, przeznaczone do przenoszenia danych. Format obydwu rodzajów ramek został pokazany na rysunku 10.5. Ramki powiadomień są wykorzystywane między innymi do zasygnalizowania, że ramka danych została poprawnie dostarczona lub że wymaga retransmisji. W długich ramkach wydzielono sekcje początku i końca ramki obejmujące wiele pól sterujących. Ponieważ ramki muszą zachowywać standardowy rozmiar, niekiedy konieczne jest dopełnienie danych bitami pola *Dopełnienie*. Pole FCS przechowuje informacje potrzebne do korekcji błędów.

**Rysunek 10.5.**  
Format krótkiej i długiej ramki HomePlug



Krótką ramką jest wykorzystywana do zainicjowania funkcji automatycznego powtarzania danych w przypadkach, gdy odebrane informacje nie spełniają kryteriów poprawności wyznaczanych przez mechanizm korekcji błędów. Ramki tego typu funkcjonują jako ogranicznik odpowiedzi, składający się z preambuły i pola sterującego. Preambuła jest sygnałem o poszerzonym widmie, która wyznacza początek ramki. Natomiast pole sterujące niesie informacje zakodowane zgodnie ze specyfikacją Turbo Product Code standardu HomePlug i może zostać odczytane nawet po bardzo mocnym tłumieniu (do poziomu kilku decybeli poniżej szumu). Pole danych długiej ramki również jest wyznaczone za pomocą specjalnego ogranicznika, którego kodowanie zmienia się w zależności od zastosowanej techniki optymalizacji kanału.

Podobnie jak w przypadku ramek 802.3, pierwsze 17 bajtów sekwencji zawiera adres źródłowy, adres docelowy i numer segmentu, niezbędny do odtworzenia właściwej kolejności ramek. Dzięki umieszczeniu bajtów adresu na samym początku możliwe jest odesłanie komunikatu o potrzebie retransmisji, nawet jeśli część ramki jest uszkodzona. Zachowanie standardowej długości ramki jest gwarantowane przez pole dopełnienia. Dane są natomiast zabezpieczone za pomocą sekwencji kontrolnej ramki.

Aby obniżyć liczbę kolizji w sieci elektrycznej, do sterowania przepływem danych wykorzystano algorytm wielodostępu z wykrywaniem nośnej i unikaniem kolizji (CSMA/CA — *Carrier Sense Multiple Access with Collision Avoidance*). Mechanizm CSMA/CA zawiera funkcje wykrywania fizycznej nośnej (PCS — *Physical Carrier Sense*) oraz wykrywania wirtualnej nośnej (VCS — *Virtual Carrier Sense*). Ich działanie umożliwia wyszukanie przerw w transmisji innych ramek oraz priorytetowego obsługiwanie wybranych emisji. PCS jest mechanizmem warstwy fizycznej, którego celem jest wykrycie preambuły. Z kolei VCS jest komponentem warstwy łącza danych, który wykorzystuje informacje pozyskane z ogranicznika do wykrywania następujących bloków danych:

- ♦ **początkowego ogranicznika ramki** — blok ten zawiera informacje na temat rodzaju wymaganej odpowiedzi, długości ramki, priorytetu, numeru schematu tonów (lub parametrów optymalizacji kanału);
- ♦ **końcowego ogranicznika ramki** — blok ten składa się z informacji na temat typu wymaganej odpowiedzi oraz priorytetu;
- ♦ **ogranicznika odpowiedzi** — odpowiedź może zawierać potwierdzenie (ACK), potwierdzenie negatywne (NACK), potwierdzenie negatywne wynikające z zajętości zasobów (FAIL); obejmuje także informację o priorytecie poprzedniej ramki.

Priorytety poszczególnych transmisji są przypisywane na podstawie priorytetów aplikacji użytkownika. Pozostają jednak pod kontrolą specjalnego algorytmu, który ogranicza współzawodnictwo aplikacji i odpowiednio redukuje priorytety. System HomePlug zapewnia kilka poziomów jakości usługi, umożliwiając korzystanie z aplikacji strumieniowych, takich jak telefonia internetowa, programy multimedialne itp.

## Bezpieczeństwo

Każde urządzenie jest dostarczane z naklejką informującą o hasle głównym nadanym mu przez producenta. Hasło to stanowi podstawę do wyznaczania innych hasel. Aby skorzystać z funkcji szyfrowania zaimplementowanych w urządzeniu HomePlug, trzeba zainstalować dostarczone wraz z nim oprogramowanie. Większości produktów towarzyszą aplikacje przeznaczone dla systemu Windows. Dlatego osoby posługujące się systemami Macintosh lub Linux powinny wcześniej sprawdzić, czy pakiet zawiera oprogramowanie dla tych systemów lub czy jest ono dostępne na stronach internetowych.

Mechanizm zabezpieczający transmisję bazuje na 56-bitowym standardzie szyfrowania danych (DES — *Data Encryption Standard*). Stacja HomePlug (punkt końcowy połączenia) przechowuje tabelę kluczy szyfrowania oraz odpowiadających im numerów kluczy szyfrowania (EKS — *Encryption Key Select*). Wartość EKS jest zapisywana wewnątrz nagłówka ramki i służy jednostce końcowej do wyznaczenia klucza, który pozwoli na rozszyfrowanie danych. W każdej sieci stosowany jest inny współdzielony klucz szyfrowania, a każda ze stacji przechowuje wartość EKS z nim stowarzyszoną.

Dodatkowe zabezpieczenie wprowadza także mechanizm optymalizacji kanału, który dobiera odpowiedni zestaw parametrów transmisyjnych.

## Serwery sieci domowych

Serwery sieci domowych są przeznaczone do realizacji usług przydatnych użytkownikom niewielkich sieci. Są one projektowane w taki sposób, aby były łatwe w użyciu, ale jednocześnie gwarantowały dostęp do całej gamy funkcji potrzebnych w instalacjach tego typu. Niewielka liczba jednostek sieci oznacza, że wymagania sprzętowe dotyczące serwerów nie są wygórowane. Wiele osób przeznacza na ten cel stare komputery, a wielu dostawców dostosowuje do funkcji serwera domowego starsze lub okrojone wersje serwerowych systemów operacyjnych. Na przykład Microsoft Windows Home Server jest systemem wywodzącym się z systemu Windows Server 2003, w którym wyłączono pewne funkcje administracyjne i dodano aplikacje kreatorów, ułatwiające konfigurację. Wiele serwerów domowych jest sprzedawanych jako niezależne urządzenia, w których wstępnie zainstalowano wybrane dystrybucje systemów Linux lub BSD UNIX.

Oto lista typowych składników serwerów domowych:

- ♦ Usługi adresacji, takie jak DHCP i DNS.
- ♦ Firewallle i serwery proxy przeznaczone do połączeń internetowych.
- ♦ Serwery WWW wykorzystywane przez jednostki sieci lokalnej (intranet), rzadziej udostępniane w internecie.
- ♦ Mechanizmy współdzielenia zasobów dyskowych (wymiana plików), drukarek i innych urządzeń peryferyjnych.
- ♦ Funkcje zdalnego dostępu umożliwiające korzystanie z systemu przez sieć.
- ♦ Funkcje strumieniowania plików multimedialnych (plików audiowizualnych).
- ♦ Serwery poczty elektronicznej i komunikatorów.
- ♦ Mechanizmy zabezpieczania sieci.
- ♦ Aplikacje ułatwiające wykonywanie codziennych zadań, takie jak kalendarze grupowe, listy spraw do załatwienia itp.

Rozpatrywane jako osobna gałąź produktów serwery domowe mają bardzo mały udział w rynku. W ciągu dwóch lat dostępności platformy Microsoft Home Server (<http://www.microsoft.com/windows/products/winfamily/windowshomeserver/default.mspx>) sprzedano mniej niż 100 000 egzemplarzy systemu.

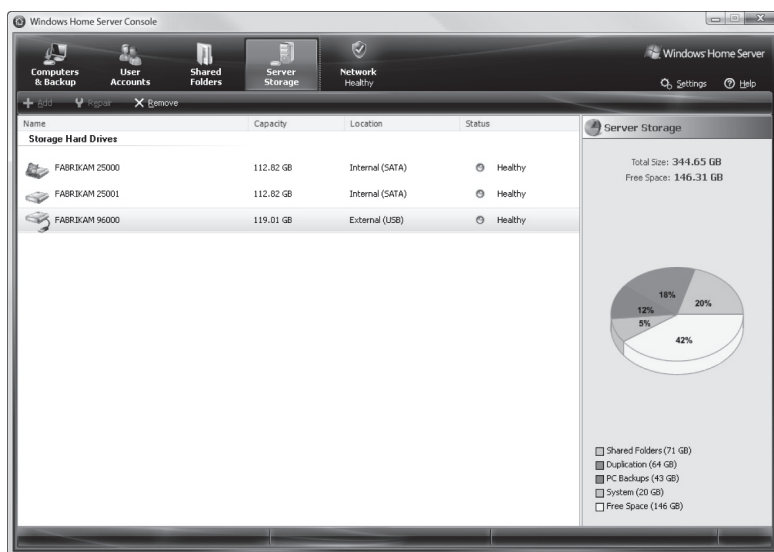
W ciągu ostatniej dekady w sprzedaży było dostępnych także kilka urządzeń serwerowych, z których żadne nie uzyskało popularności systemu Microsoft Home Server. Jednym z urządzeń serwerowych przeznaczonych dla sieci domowych jest Toshiba Magnia — rozwiązanie udostępnione w 2001 roku, bazujące na systemie Red Hat Linux. Zawiera ono interfejs administracyjny (WWW); serwery DHCP, DNS, FTP, WWW i wydruku; firewall i mechanizmy filtrowania oraz buforowania treści WWW, a wszystko to w jednostce o rozmiarze laptopa. Inne warte wspomnienia urządzenia z tej kategorii to: Sun Cobalt Qube, IT-100

firmy EmergeCore Network, Mirra Personal Server, PowerElf II firmy Greencomputer Innovation, IOGEAR BOSS, Trittom Technologies ASAP oraz Chili Systems ChiliBox. Wszystkie były przeznaczone na rynek sieci domowych i małych firm (SOHO — *Small Office/Home Office*).

Pomysł zainstalowania serwera domowego w sieci wydaje się zasadny, nawet jeśli rozwiązania te nie zdobędą popularności na rynku. Prawdopodobnie osoby o technicznych inklinacjach będą jednak optowały za zaadaptowaniem do tych celów standardowych wersji serwerowych systemów operacyjnych, takich jak Windows Server, Solaris czy Red Hat Linux. Nie zmienia to jednak faktu, że z czasem uaktywnią się firmy próbujące wprowadzić nowe produkty z tej kategorii. Już teraz pojawiają się doniesienia o tym, że firma Apple opracowuje system, który ma konkurować z platformą Microsoft Windows Home Server, ale z Apple'em nigdy nic nie wiadomo.

Wynika z tego, że obecnie Microsoft Windows Home Server jest jedynym liczącym się systemem operacyjnym w tej kategorii. Jest to rozwiązanie dopracowane w szczegółach. Stworzone przy współudziale 60 firm zewnętrznych. Warto więc rozważyć jego zakup przede wszystkim ze względu na funkcje sporządzania kopii zapasowych, klonowania danych oraz zdolności do agregowania wszystkich dysków, jakie tylko uda mu się rozpoznać. Urządzenia serwerowe z zainstalowanym systemem Windows Home Server są produkowane przez takie firmy, jak HP, Acer, Shuttle i Via. Na rysunku 10.6 zostało pokazane okno konsoli zarządzania pamięcią masową systemu Microsoft Windows Home Server.

**Rysunek 10.6.**  
System Microsoft  
Windows Home  
Server wykorzystuje  
wszystkie dyski,  
które potrafi rozpoznać



## Podsumowanie

W tym rozdziale zostały opisane sieci domowe oraz pełnione przez nie funkcje. Instalacje tego typu umożliwiają współdzielenie zasobów, co zapewnia znaczne oszczędności czasu i pieniędzy. Zazwyczaj w sieciach domowych wykorzystywane są różne technologie komunikacyjne, oferujące maksymalną wygodę pracy przy minimalnej złożoności i niskim koszcie.

Tematyka niniejszego rozdziału została skoncentrowana na dwóch zagadnieniach — przyłączaniu sieci do internetu oraz sposobach łączenia ze sobą poszczególnych obszarów domu. Z tego względu omówione zostały takie technologie, jak Ethernet, HomePNA, HomePlug oraz Wi-Fi.

W kolejnym rozdziale przedstawiono połączenia peer-to-peer, w tym również rozwiązania wykorzystujące inne magistrale komputerowe.

# Rozdział 11.

## Sieci peer-to-peer i osobiste sieci LAN

### **W tym rozdziale:**

- ♦ Osobiste sieci lokalne
- ♦ Modele sieci peer-to-peer (P2P)
- ♦ Rozległe systemy P2P
- ♦ Magistrale komputerowe łączące wiele urządzeń

Osobiste sieci lokalne (pLAN) są sieciami złożonymi z niewielkiej liczby urządzeń i (lub) pokrywającymi niewielki obszar fizyczny. W tym rozdziale zostały opisane technologie umożliwiające implementację tego typu rozwiązań.

Wśród poruszanych zagadnień uwzględnione zostały również sieci węzłów równorzędnych, czyli sieci peer-to-peer (P2P). Doskonałym przykładem zależności P2P jest grupa robocza złożona z dziesięciu lub mniejszej liczby stacji. Sieci P2P są również często tworzone przez aplikacje rozproszone. Ogólna zasada stanowi, że systemem P2P jest system, który jednocześnie odgrywa rolę serwera i klienta. W rozwiązaniach tego typu nie istnieje mechanizm centralnego zarządzania komunikacją lub dostępem do usług, nie ma też funkcji przekazywania ruchu.

Sieci peer-to-peer występują w wielu odmianach. Wzorcowa konfiguracja nie może zawierać jakiegokolwiek usługi centralnej. Jednak powszechnie stosuje się hybrydowe konfiguracje P2P, w których istnieje wspólny katalog stacji, udostępniający funkcje wyszukiwania, ale sama wymiana danych jest realizowana między jednostkami końcowymi.

W dalszej części rozdziału omówione zostały najbardziej znane rozwiązania P2P oraz ich wpływ na architekturę sieciową. Analiza obejmuje między innymi systemy wymiany plików Gnutella i Freenet, które jako przykłady czystych konfiguracji P2P wykorzystują odpowiednie mechanizmy wyszukiwania stacji i pobierania danych ad hoc. Jako przykłady rozwiązań hybrydowych zostały opisane systemy Napster i BitTorrent.

Tematyka rozdziału uwzględnia również zagadnienia związane z bezpieczeństwem i anonimowością oferowanymi przez sieci przyjacielskie (F2F — *Friend-to-Friend*).

Ponieważ funkcję sieci osobistych często pełnią również niektóre magistrale komputerowe, w końcowej części rozdziału zostało zamieszczone omówienie standardów USB, FireWire (IEEE 1394) oraz Bluetooth. Z informacji tam przedstawionych wynika, że połączenia USB stanowią odmianę struktury drzewiastej. Topologia FireWire odpowiada łańcuchowi. Natomiast wymiana danych w standardzie Bluetooth polega na ustanawianiu połączeń ad hoc w ramach konfiguracji nazywanej pikosieciami.

## Sieci peer-to-peer

Sieć peer-to-peer (P2P) jest przykładem takiej konfiguracji, w której każdy węzeł może pełnić funkcję klienta i serwera, utrzymując bezpośrednie połączenia z innymi węzłami. Cechą charakterystyczną tego typu sieci jest to, że nie ma w niej centralnego punktu zarządzania komunikacją. Określenie „sieci P2P” jest stosowane zarówno w odniesieniu do komputerów sieci LAN, jak i do opisu rozproszonych aplikacji współdzielenia zasobów w ramach sieci LAN lub WAN.

Podstawowe zadanie systemów P2P polega na współdzieleniu rozproszonych zasobów, a tym samym na unikaniu duplikowania informacji oraz dodatkowych kosztów utrzymania systemów. Dowolna liczba komputerów może bowiem korzystać z tych samych plików, drukarek, napędów optycznych i innych komponentów systemowych. Rozproszone oprogramowanie umożliwia upublicznienie ogromnej ilości danych, a także wykorzystanie wielu komputerów w projekcie wymagającym bardzo dużych mocy obliczeniowych.

Pierwsze sieci komputerów osobistych były wykonane zgodnie z założeniami topologii P2P. Pierwszym komputerem osobistym, który obsługiwał komunikację P2P, był Macintosh Plus (w roku 1984). W przypadku systemów Windows pierwsza sieciowa wersja systemu została wydana w październiku 1992 roku i miała nazwę Microsoft Windows for Workgroups 3.11. System ten — nazywany w skrócie WfW — wykorzystywał protokoły: SMB (protokół warstwy aplikacji służący do wymiany plików), NetBIOS (protokół warstwy sesji przeznaczony do identyfikacji stacji) oraz NBF/IPX (protokoły warstwy transportowej odpowiedzialne za obsługę ramek NetBIOS oraz wymianę pakietów między sieciami). Programem obsługi sieci był plik *VSHARE.386*, który działał jako sterownik urządzenia wirtualnego, nakładający blokady na pliki. Po wprowadzeniu systemów takich jak Windows NT sieci P2P stały się rozwiązaniami przeznaczonymi dla niewielkich biur i domów.

Mimo że przez lata zmieniły się protokoły i możliwości komputerów, mechanizm wymiany danych między jednostkami równorzędnymi jest implementowany w każdej wersji systemu Windows przeznaczonej dla użytkownika końcowego. Jest dostępny jako opcja pracy grupowej. Jednak po przekroczeniu pewnej liczby połączeń (od 12 do 20) praca w grupie roboczej staje się mało wydajna. Z tego względu w systemach Windows XP i Windows Vista firma Microsoft ustanowiła sztuczne ograniczenie do 10 jednoczesnych połączeń.

Po zalogowaniu do grupy roboczej bezpieczeństwo pracy jest gwarantowane przez lokalny system oraz prawa dostępu do lokalnych plików. Publikowane w sieci zasoby nazywa się *udziałami*. Administrator systemu może zastosować określone prawa dostępu do zasobu, operując użytkownikami i grupami użytkowników. Skuteczność tego rozwiązania daleko odbiega od bezpieczeństwa oferowanego przez centralny mechanizm uwierzytelniania. Dlatego w większości sieci, w których wymagany jest wysoki poziom bezpieczeństwa danych,

stosowane są modele klient-serwer (najczęściej w połączeniu z usługami katalogowymi). Jest to też przyczyna znacznego ograniczenia funkcjonalności pracy w grupie roboczej w porównaniu z działaniami w domenie.

Niestety, instalacja serwera wiąże się z istotnymi kosztami i dodatkową złożonością konfiguracji. Z tego powodu grupy robocze nadal pozostają w użyciu. Nie ma wątpliwości, że brak zabezpieczeń, niska wydajność, rozproszone zarządzanie i brak centralnego mechanizmu ochrony zasobów czynią w dłuższym czasie sieci P2P bardziej kosztownymi. Jednak próg wejścia jest w tym przypadku znacznie niższy.

Model jednostek równorzędnych sprawdza się także w odniesieniu do sposobu działania oprogramowania. Zgodnie z założeniami modelu wszystkie komputery, na których zainstalowano aplikację, są jednakowo ważne w sieci i mogą się komunikować ze wszystkimi pozostałymi stacjami. W kolejnych punktach rozdziału zostały omówione różne typy sieci peer-to-peer, z których część stanowią bardzo znane produkty.

Oprogramowanie P2P wywarło ogromny wpływ na architekturę nowoczesnej aplikacji. Programy tego typu mogą udostępniać znaczne ilości danych, często za niską cenę. W niektórych przypadkach mogą również realizować wspólne zadanie, tworząc superkomputer wykonujący skomplikowane obliczenia (np. rozwiązujący problem zwijania białka lub poszukujący życia pozaziemskiego).

## Czyste sieci P2P

Czystymi sieciami P2P nazywa się te sieci, w których usługi są udostępniane całkowicie zgodnie z modelem peer-to-peer. Aby system można było uznać za w pełni zgodny z ideą P2P, musi spełniać następujące warunki:

- ♦ Wszystkie jednostki muszą być jednocześnie klientami i serwerami.
- ♦ W sieci nie mogą być dostępne żadne serwery.
- ♦ Stacje klienckie muszą zarządzać własnymi usługami. Nie może istnieć centralna konsola zarządzania.
- ♦ Nie są wykorzystywane funkcje przekazywania ruchu. Każda jednostka może bezpośrednio komunikować się z inną jednostką.

Przykładem czystego rozwiązania P2P jest grupa robocza systemu Windows. Model ten jest także wykorzystywany przez niektóre aplikacje, szczególnie te, które pozwalają na przekazywanie plików i treści, generują strumienie multimedialne, obsługują czaty IRC i realizują połączenia telefoniczne.

## Sieci małego świata

Sieciami małego świata nazywa się sieci, w których większość węzłów nie należy do najbliższych sąsiadów analizowanego węzła, ale każdy węzeł jest połączony z innym za pomocą przynajmniej jednej ścieżki, a zazwyczaj za pomocą większej ich liczby. Sieci tego rodzaju można analizować zgodnie z teorią grafów. Dlatego stanowią podstawę funkcjonowania różnorodnych systemów, w tym mechanizmów socjologicznych oraz sieci komputerowych. Przykładem sieci małego świata jest teoria, w której przyjmuje się, że każdy człowiek jest

spokrewniony z innym człowiekiem na Ziemi o nie więcej niż sześć stopni oddalenia (teoria ta jest również nazywana teorią Kevina Bacona). Podobnie pamięć krótkoterminowa wykorzystuje sieci małego świata neuronów. Innym przykładem są czyste sieci P2P.

Całkowicie przypadkowe sieci małego świata cechują się najmniejszą średnią wartością najkrótszych ścieżek. Większość sieci małego świata nie jest przypadkowa i zawiera ścieżki o większym natężeniu ruchu między węzłami. W grafie takim musi być też co najmniej jedna krótka trasa łącząca dowolną parę węzłów. Sieci małego świata są wypełnione dużą liczbą koncentratorów, czyli węzłów o dużej liczbie połączeń i znacznie mniejszej liczbie węzłów brzegowych. Gdy sieć małego świata zawiera większą liczbę koncentratorów, może być opisywana jako rozkład długoogonowy.

## Gnutella

Prawdopodobnie najbardziej znaną czystą aplikacją P2P jest internetowy system wymiany plików o nazwie Gnutella. Nazwa pochodzi od nazwy kremu orzechowo-czekoladowego Nutella, uwielbianego przez twórców serwisu, oraz rodzaju licencji (GNU), zgodnie z którą program był dystrybuowany. Gnutella została opracowana w celu wyeliminowania niektórych problemów obecnych w aplikacji Napster (serwis Napster został opisany w dalszej części rozdziału). Gnutella jest systemem, który umożliwia jednostkom sieciowym przeglądanie zbioru plików innych komputerów bez konieczności odwoływania się do centralnej bazy danych.

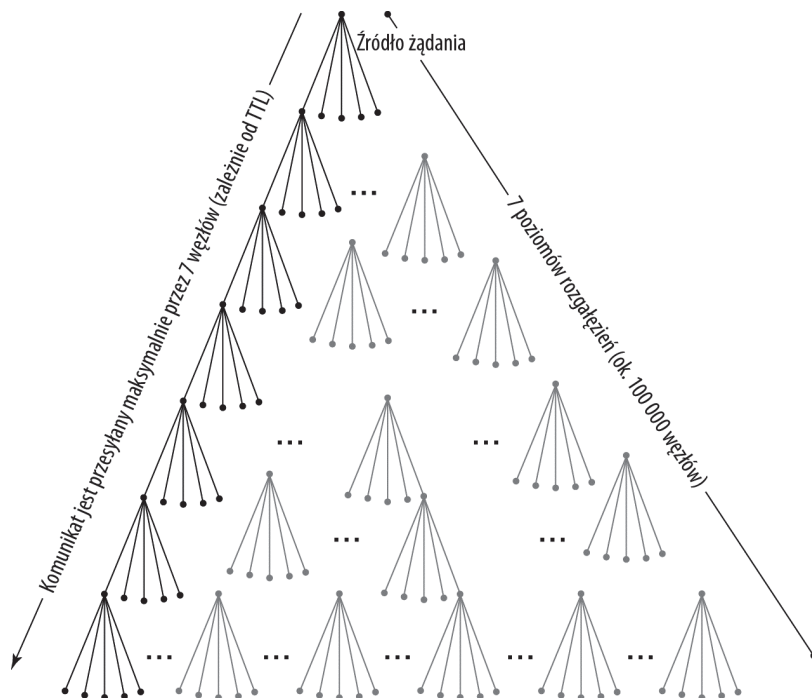
Rozwiązanie to jest wykorzystywane w wielu aplikacjach. Programy systemu Gnutella są dostępne na różnych platformach. Najpopularniejsze aplikacje klienckie to BearShare, Gnucleus, LimeWire, Morpheus, WinMX i XoloX.

Po uruchomieniu klient Gnutella wyszukuje wszystkie dostępne jednostki równorzędne. Niekiedy oprogramowanie jest dostarczane z listą potencjalnych partnerów komunikacji. W innych przypadkach konfiguracja programu zawiera informację o sieciowym rejestrze stacji, do którego można się odwołać. W początkowych wersjach program wyszukiwał pierwszą jednostkę zdalną, a następnie sprawdzał, czy kolejne systemy są dostępne. Lista potencjalnych partnerów komunikacji była ograniczona do pięciu systemów. Każdy z węzłów utrzymywał informację o pięciu komputerach zdalnych. Zatem gdy jedna ze stacji generowała żądanie dostarczenia pliku, było ono powielane do wszystkich jednostek odległych o nie więcej niż siedem skoków od stacji inicjującej żądanie (z uwzględnieniem parametru czasu życia żądania — TTL). Dzięki temu w razie konieczności można było uzyskać połączenie z 97 655 systemami. Każda jednostka, która odpowiedziała na wysłany przez pierwszy węzeł pakiet ping (pakietem pong), była zapisywana na liście stacji przechowywanej przez program Gnutella do późniejszego wykorzystania.

Ta nieskomplikowana i jednocześnie efektywna architektura P2P została przedstawiona na rysunku 11.1. Wynika z niego, że system ma strukturę drzewiastą, która rozgałęzia się do siódmego poziomu. Komunikat może więc podróżować przez siedem stacji, czego reprezentacją jest ciemniejsze drzewo, widoczne z lewej strony rysunku. Pozostałe drzewa i kółka informują o tym, że sieć ma wiele rozgałęzień, które pozwalają na odwołania do stacji znajdujących się na niższych poziomach struktury. Pokazanie wszystkich elementów drzewa jest niemożliwe ze względu na rozmiar kartki.

**Rysunek 11.1.**

Hierarchiczna  
struktura zapytań  
i transferu danych  
w czystej sieci P2P  
Gnutella



Niektóre programy odwołujące się do systemu Gnutella wykorzystują węzły końcowe, które mogą się łączyć z trzema ultrastacjami. Każda ultrastacja może z kolei przyłączyć do 32 kolejnych ultrastacji. Dopuszczalne jest wykorzystanie maksymalnie czterech poziomów struktury. Stopień rozgałęzienia takiego systemu jest niewyobrażalnie duży — wynosi  $4,38 \times 10^{48}$  węzłów. Z tego względu jednostki systemu wykorzystują protokół routingu żądań odpowiedzialny za wymianę tabel routingu żądań (QRT — *Query Routing Table*). Tabele te zawierają wartości skrótów, które są scalane z wartościami pozyskanymi z innych tabel na poziomie ultrastacji. Żądanie wygenerowane przez klienta jest przekazywane w dół łańcucha, aż do natrafienia na wartość skrótu, która jest z nim zgodna. Wówczas stacja inicjująca komunikację nawiązuje połączenie z jednostką, która wygenerowała wartość skrótu, i żąda dostarczenia wskazanego pliku.

Po znalezieniu właściwej stacji rozpoczyna się negocjowanie parametrów transferu pliku. Jeśli jednak stacja dostarczająca treść znajduje się za firewallem i nie może odpowiedzieć na żądanie przesłania pliku do systemu zewnętrznego, system żądający dostarczenia danych wysyła komunikat z prośbą o to, by jednostka usytuowana za firewallem zainicjowała transfer pliku. Jeśli również to rozwiązanie nie jest możliwe do zastosowania, wykorzystywany jest system pośredni (często ultrastacja).

System Gnutella nie nakłada ograniczeń na rodzaj wymienianych plików. Generowane przez programy żądania nie są też łatwe do przechwycenia, ponieważ działanie mechanizmu polega na tworzeniu tymczasowych połączeń. Z kolei rozproszony charakter i brak centralnej bazy danych gwarantuje wysoką wydajność komunikacji i brak zatorów.



Rozwiązanie o podobnym stopniu rozgałęzienia, jak w przypadku Gnutelli, jest wykorzystywane w innym systemie wymiany plików — Kazaa.

## Freenet

Kolejnym przykładem czystego systemu P2P jest projekt open source o nazwie Freenet (opracowywany zgodnie z licencją GNU). Zamiast znanych z Gnutelli tabel wartości skrótów zastosowano w nim protokół routingu wykorzystujący wartości kluczy. Algorytm sprawdza klucze i ustanawia połączenie z węzłami, które znajdują się najbliżej systemu generującego żądanie lub jednostki ustanawiającej połączenie. Klucz jest wynikiem działania funkcji skrótu, uwzględniającej treść pliku lub jego położenie. W rozwiązaniu Freenet wykorzystywane są obydwie informacje.

W przeciwieństwie do innych systemów P2P Freenet tworzy rozproszony system pamięci masowej i wypełnia tę pamięć treścią. Zazwyczaj jedna stacja wnosi do sieci 10 GB przestrzeni dyskowej. Operacja dodania pliku lub strony WWW do pamięci jest nazywana *wstawieniem*. Użytkownik nie kontroluje tego, co jest zapisywane w jego przestrzeni dyskowej. Pewnymi odmianami sieci Freenet są systemy Darknet — w którym użytkownicy ustanawiają połączenia z wybraną liczbą zaufanych stacji lub sieci — oraz OpenNet — w którym nie nakłada się żadnych ograniczeń. Sieć Darknet pozwala na uzyskanie bardzo dużego stopnia rozgałęzienia, ale połączenia muszą mieć charakter zaufanych. Mechanizm Freenet jest cały czas w fazie testowania, ale są już dostępne użyteczne stabilne wersje oprogramowania.

## Systemy hybrydowe

Hybrydową siecią peer-to-peer jest rozwiązanie, w którym funkcjonują niezależne jednostki, ale przy udziale pewnych centralnych usług. Konfiguracje tego typu są powszechnie wykorzystywane w rozproszonych aplikacjach internetowych i odgrywają istotną rolę w popularyzacji sieci P2P.

Sieci jednostek równorzędnych tworzone na podstawie łączy, w których każda ze stacji ma informację o dostępności drugiej jednostki przed ustanowieniem połączenia, nazywają się *sieciami ustrukturyzowanymi*. Przykładami sieci tego typu są rozwiązania Napster i Torrent. Działanie ustrukturyzowanej sieci wymaga użycia pewnego globalnego protokołu, niezbędnego do zarządzania wskaźnikami do systemów zawierających wymieniane treści. W wielu sieciach P2P informacje te są przechowywane w rozproszonych tabelach skrótów (DHT — *Distributed Hash Table*).

## Napster

Napster był usługą wymiany plików muzycznych zaimplementowaną w formie sieci P2P. System został zaprojektowany przez Shawna Fanninga w czasie, gdy studiował on na Uniwersytecie Northeastern. W rozwiązaniu tym został wykorzystany centralny serwer przechowujący informacje o położeniu plików MP3. Dane były odpowiednio zaindeksowane i zapisane w bazie danych. Pliki muzyczne były z kolei rozproszone po systemach klien-

kich. Gdy użytkownik wybierał utwór z bazy danych, zawartość pliku była przekazywana z miejsca jego składowania do jednostki użytkownika aplikacji. System został skomercjalizowany, a firma nim zarządzająca przyjęła jako nazwę pseudonim Shawna — Napster.

Napster stał się niezwykle popularny i przyczynił się do nagłego zwiększenia liczby wymienianych plików muzycznych. To z kolei spowodowało sprzeciw przedstawicieli branży muzycznej, którzy wytoczyli firmie procesy o naruszenie praw autorskich. W lutym 2001 roku (w najlepszym okresie działalności Napstera) serwis miał 24 miliony użytkowników na całym świecie. Przedstawiciele Napstera dowodzili, że udostępniają jedynie usługę katalogową, a kopiowanie plików jest wykonywane bez ich zgody. Ostatecznie zgodnie z nakazem sądu usługa została usunięta z sieci.

Logo i marka firmy zostały wykupione i wykorzystane w płatnej usłudze dystrybucji plików najpierw przez firmę Roxio, a następnie w 2008 roku przez firmę Best Buy. Jednak popularność późniejszych serwisów była znacznie mniejsza. Przypadek Napstera uświadomił wszystkim, jak istotną siłę oddziaływania ma hybrydowa architektura P2P. Obecnie wiele firm — przede wszystkim internetowych — korzysta z tego modelu.

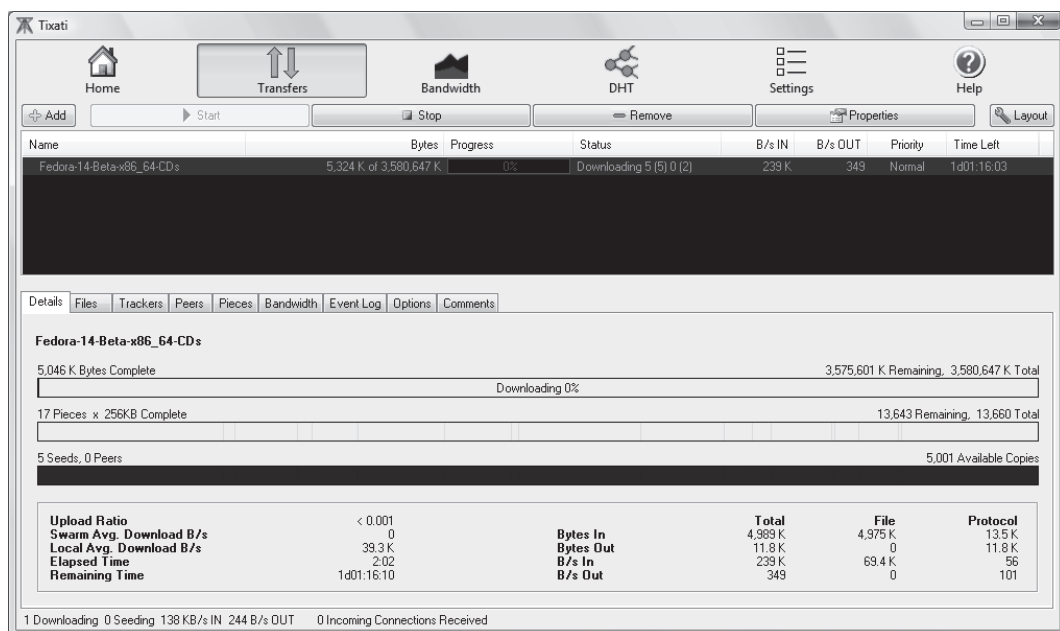
## Torrent

Jednym z następców Napstera, wykorzystujących ten sam model, jest protokół wymiany plików BitTorrent, działający zgodnie z założeniami hybrydowych sieci peer-to-peer. Protokół ten jest powszechnie wykorzystywany, a badania dowodzą, że stanowi istotną część ruchu internetowego. Serwis isoHunt.com udostępnia wyszukiwarkę BitTorrent, która zawiera milion zaindeksowanych wpisów. W 2008 roku firma isoHunt mogła udokumentować ruch o rozmiarze przewyższającym 1 petabajt. Innym popularnym indeksem jest serwis Torrent-Box. Protokół BitTorrent został opracowany przez Bramę Cohena i jest udostępniany przez jego firmę BitTorrent.

W internecie dostępnych jest wiele programów klienckich BitTorrent. Według informacji pochodzących z serwisu *About.com* wśród ośmiu najpopularniejszych aplikacji znajdują się:

1. Tixati (<http://www.tixati.com>) — program pokazany na rysunku 11.2.
2. uTorrent (<http://www.utorrent.com>).
3. Vuze (<http://azureus.sourceforge.net>).
4. Deluge Torrent (<http://deluge-torrent.org>).
5. Transmission Bittorrent (<http://www.transmissionbt.com>).
6. ABC (Another Bit Torrent) (<http://pingpong-abc.sourceforge.net>).
7. TurboBT (<http://turbobt.sourceforge.net/indexen.htm>).
8. BitComet (<http://www.bitcomet.com>).

Gdy użytkownik chce udostępnić plik, program tworzy plik *.TORRENT* zawierający informacje o udostępnianym pliku oraz o serwerze, który będzie przechowywał metadane opisujące ten plik. Plik *.TORRENT* jest następnie przekazywany do serwera Torrent, nazywanego *serwerem śledzącym* (ang. *tracker*), gdzie zostaje zapisany w bazie danych. Inni użytkownicy mogą od tego momentu pobierać plik *.TORRENT*, aby poznać lokalizację poszukiwanego



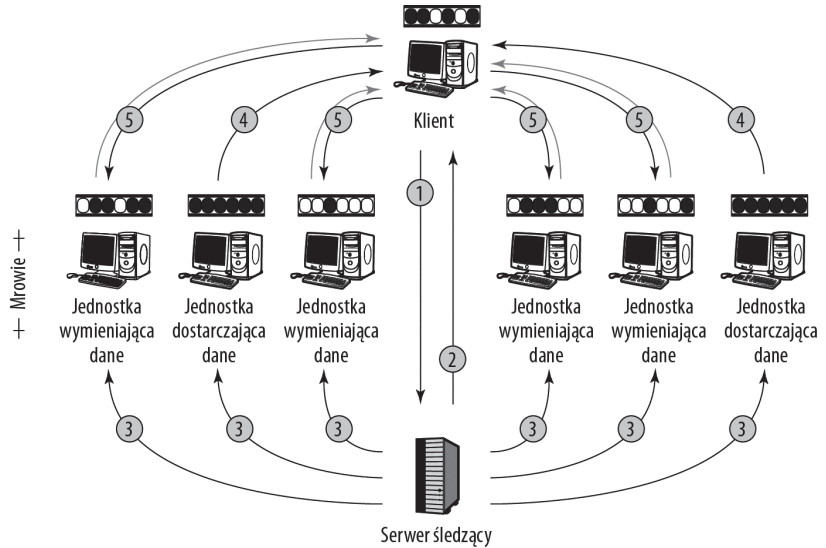
**Rysunek 11.2.** Tixati jest obecnie najpopularniejszym klientem BitTorrent

zasobu. Po przesłaniu pliku *.TORRENT* do zdalnego komputera jednostka zdalna może zainicjować transfer pliku zasadniczego, wykorzystując odwołania peer-to-peer. Klient dysponujący plikiem jest nazywany *udostępniającym* (ang. *seeder*). To samo określenie stosuje się w odniesieniu do każdej stacji, która posiada pełną kopię pliku.

Po pewnym czasie każdy z plików jest udostępniany przez wiele jednostek klienckich, często rozproszonych geograficznie. Nie jest wówczas konieczne pobieranie całego pliku z pojedynczego systemu, serwer śledzący utrzymuje aktualną listę udostępniających, którą program kliencki okresowo odświeża, co umożliwia pobieranie fragmentów pliku z różnych stacji klienckich — grupa stacji klienckich wymieniających fragmenty pliku jest nazywana *mrowiem* (ang. *swarm*). Rozwiązanie to gwarantuje odciążenie pojedynczych komputerów.

Na rysunku 11.3 została przedstawiona architektura systemu P2P BitTorrent wraz z procedurą wymiany plików, która obejmuje następujące odwołania:

1. Klient do jednostki śledzącej: Które komputery przechowują plik lub jego fragmenty?
2. Serwer śledzący do klienta: Pod tymi adresami możesz znaleźć fragmenty pliku.
3. Serwer śledzący do mrowia: Przesłać do klienta i odebrać od klienta fragmenty pliku.
4. Jednostka udostępniająca do klienta: Plik jest przesyłany.
5. Mrowie do klienta: Oto brakujące fragmenty.

**Rysunek 11.3.**Architektura  
BitTorrent

Na rysunku 11.3 zostały odwzorowane poszczególne etapy opisanej powyżej procedury. Udostępniany plik — przedstawiony na rysunku jako taśma filmowa ponad ikonami komputerów — jest w całości przechowywany w systemach udostępniających (stan ten jest na rysunku symbolizowany wszystkimi czarnymi klatkami filmu). Systemy wymieniające dane dysponują jedynie pewnym podzbiorem klatek (niezamalowane klatki oznaczają brakujące fragmenty filmu). Przesyłanie filmu do klienta polega na tym, że z różnych jednostek przekazywana jest odpowiednia porcja, która składa się na cały plik wynikowy.

Oczywiście nikomu nie trzeba tłumaczyć, że taki sposób działania nie jest korzystny dla przedstawicieli branży filmowej. Nie jest także mile widziany przez dostawców usług internetowych, ponieważ zgodnie z badaniami przeprowadzonymi przez firmę CacheLogic (zajmującą się analizą ruchu internetowego) transmisja *BitTorrent stanowi 35 procent całego ruchu internetowego* (dane pochodzą z 2005 roku). Wiele dostawców internetowych wykorzystuje więc narzędzia do monitorowania ruchu i filtruje pakiety BitTorrent.

Gdyby usługa BitTorrent działała na jednym powszechnie znanym porcie, jej zablokowanie nie stanowiłoby żadnej trudności. Niestety, system ten nie korzysta z portu 80, tak jak przeglądarki. Dzieli natomiast dane na kilka strumieni i używa kilku portów TCP do przekazywania danych w losowej lub najróżniej stosowanej sekwencji. Dzięki temu komunikacja jest efektywniejsza i trudniejsza do zablokowania. Niemniej wprowadza pewien dodatkowy narzut (szczególnie na początku transmisji), gdyż wymaga ustanowienia wielu połączeń. Sam protokół nie obsługuje treści strumieniowych, ponieważ podstawą jego działania jest pobieranie informacji w formie fragmentów.

System BitTorrent dzieli pliki na części o równej wielkości od 32 kB do 4 MB. Każdy fragment otrzymuje sumę kontrolną, która jest sprawdzana po odbiorze paczki i odtworzeniu kolejności bloku danych. Rozwiązanie to ma wielu konkurentów; niektórzy z nich wykorzystują serwer metadanych (serwer śledzący), a inni nie. Dzięki usługom śledzenia stacje klienckie mogą dystrybuować metadane między sobą. Konfiguracje pozbawione tego rodzaju serwerów są czystymi systemami P2P, a nie hybrydowymi, tak jak BitTorrent.

Korzystanie z sieci BitTorrent jako takiej nie jest nielegalne. Rozwiązanie to jest po prostu mechanizmem wymiany plików. Kontrola treści należy do zadań aplikacji korzystającej z sieci. Firma BitTorrent sprzedała swoje oprogramowanie wielu korporacjom zajmującym się multimediami do rozpowszechniania treści objętych prawami autorskimi. Jedną z najpopularniejszych gier — „Word of Warcraft” — jest w istocie usługą Torrent. Ostatnio prowadzone są również prace nad uwzględnieniem w komunikacji BitTorrent przekazów RSS i podcastów. Celem jest obniżenie kosztów dystrybucji tego rodzaju mediów.

Witryny BitTorrent oferują bardzo wiele usług, legalnych i nielegalnych. Bez względu na ich status prawny, korzystając z serwisów, warto wiedzieć o kilku sprawach. Po pierwsze, podczas korzystania z sieci BitTorrent adres lokalnego systemu jest znany i może być wyśledzony niezależnie od tego, czy system ten pełni funkcję źródła danych, czy jest ich odbiorcą. Po drugie, system BitTorrent ma bardzo duże zapotrzebowanie na pasmo transmisyjne. Wymaga więc dostępności łącza szerokopasmowego.

Aby ograniczyć wykorzystanie systemu przez osoby, które chcą pobierać dane, ale nie pozwalają komputerom na pełnienie funkcji dostarczycieli treści, mechanizm BitTorrent wylicza współczynniki współdzielenia danych. Jeśli w danej jednostce na jeden bit pobranych danych przypada mniej niż jeden bit udostępnionych informacji, system może wstrzymać transmisję ostatniego strumienia danych lub wykonać inną operację, która obniży chwilowo aktywność określonego użytkownika. Są również użytkownicy, którzy pobierają pliki, ale nie wprowadzają do systemu żadnych nowych treści. Muszą oni jednak udostępniać dane, które sami pobierają.

Z powodu olbrzymiej ilości informacji przechowywanych w systemie nie ma możliwości bieżącego monitorowania przekazywanych treści. Często więc zdarza się, że ktoś wprowadza pliki stanowiące zagrożenie dla innych komputerów. Z tego względu, pobierając jakiegokolwiek dane, należy się upewnić, że pochodzą z zaufanego źródła, i dodatkowo je sprawdzić.

Nie można opisać oprogramowania P2P bez wzmianki o kontrkulturowych bohaterach z The Pirate Bay. The Pirate Bay (<http://thepiratebay.org>) jest szwedzką witryną internetową znaną jako największy na świecie serwer śledzący i jeden ze 100 najczęściej odwiedzanych serwisów WWW. Jednocześnie jest to jedna z najbardziej kontrowersyjnych i zabawnych grup. Choć ostatnie plany piratów, aby kupić własną wyspę, osiadły na mieliźnie, nigdy nie wiadomo, gdzie zawiśnie flaga z czaszką i skrzyżowanymi kośćmi.

## Sieci przyjacielskie

Niektóre sieci P2P umożliwiają zachowanie anonimowości, co oznacza, że ukrywają identyfikatory użytkowników. Ponieważ jednak komunikacja w sieciach P2P bazuje na założeniu, że poszczególne jednostki mogą się ze sobą kontaktować, zachowanie anonimowości wymusza użycie dodatkowych mechanizmów ukrywania stacji w sieci. W większości przypadków zadanie to realizują odpowiednie techniki routingu.

Użytkownicy korzystają z anonimowych sieci P2P z wielu powodów. Niekiedy chcą zachować prywatność, w innych przypadkach uniknąć wyśledzenia, zabezpieczyć informacje przed upublicznieniem, uniknąć cenzury lub nie dopuścić do kontrowersji. Zachowanie anonimowości w sieciach P2P nie jest jednak tylko potrzebą zwykłych ludzi, ten sam problem dotyczy organizacji i rządów.

Opisany wcześniej system wymiany plików Freenet jest znany przede wszystkim z tego, że gwarantuje anonimową pracę sieciową. W sieci OpenNet każda ze stacji jest widoczna we wszystkich pozostałych węzłach. W takim systemie zachowanie anonimowości jest bardzo trudne. Z kolei system Darknet umożliwia nawiązywanie połączeń jedynie z zaufanymi węzłami. Niekiedy tego rodzaju sieci są nazywane sieciami przyjacielskimi (F2F — *friend-to-friend*).

W sieciach F2F połączenia podlegają uwierzytelnieniu z użyciem haseł lub podpisów cyfrowych. Ponadto mechanizm ten gwarantuje większe bezpieczeństwo danych, gdyż połączenia są zabezpieczane kryptograficznie. Kontrolowana i zabezpieczana jest również szerokość pasma. Z drugiej strony ustanowienie połączenia wymaga dodatkowej konfiguracji i może się zakończyć zerwaniem połączenia. Ponadto trzeba się liczyć z tym, że zasoby mogą być niedostępne wtedy, gdy są potrzebne.

Rozważmy sytuację, w której trzy węzły są połączone ze sobą za pomocą dwóch łączy F2F. Środkowy węzeł jest przyjacielem obydwu punktów końcowych i nie istnieje relacja zaufania między punktami końcowymi. Mimo przekazywania danych z jednego punktu końcowego do drugiego węzeł pośredni może ukryć tożsamość każdego z punktów końcowych. W sieciach tego typu wystarczy usunąć pierwotny źródłowy adres IP przed przesłaniem pakietów do jednostki docelowej. Element środkowy staje się wówczas jednostką proxy w komunikacji między węzłami końcowymi.

Sieć, w której połączenia między dwoma punktami końcowymi składają się z dwóch odcinków — łączy w jednej, znanej sieci i łączy w drugiej, nieznannej sieci — nazywają się *sieciami nakładkowymi*. Dwie wymienione sieci sprawiają wrażenie, jakby jedna nakładała się na drugą. Poszczególne węzły są wówczas łączone za pomocą wirtualnych kanałów, często złożonych z wielu łączy fizycznych. Siecią nakładkową jest na przykład komutowane połączenie z systemem operatora telefonii, który zapewnia dostęp do internetu. Nakładanie sieci jest cechą charakterystyczną wielu systemów P2P. Doskonałymi przykładami są w tym przypadku systemy Gnutella i Freenet.

## Magistrale

Magistrala komputerowa jest fizycznym połączeniem komputera z urządzeniami peryferyjnymi. Niekiedy jest wbudowana w samo urządzenie, a w innych przypadkach wymaga dołączenia do komputera za pomocą karty rozszerzeń lub urządzenia zewnętrznego. Termin *magistrala komputerowa* oznacza, że tylko kilka urządzeń może być przyłączonych do określonego podsystemu. Na przykład magistrala SCSI w początkowych wersjach była przystosowana jedynie do przyłączenia 8 urządzeń, z których jednym był sam komputer. Kolejne wersje mechanizmu SCSI umożliwiały obsługę do 16 urządzeń. Niemniej większość użytkowników przyłącza do magistrali SCSI jedynie kilka komponentów.

Istnieje jednak kilka magistrali komputerowych, które umożliwiają przyłączenie wielu urządzeń (węzłów). Dzięki temu można je rozpatrywać w kategorii sieci, mimo że cały stos sieciowy jest w tym przypadku zawarty w samym komputerze. Magistrale tego typu udostępniają warstwę fizyczną, a wszelkiego rodzaju oprogramowanie warstwy łącza danych lub warstwy sieci znajduje się w programowym sterowniku magistrali.

W kolejnych punktach podrozdziału zostały omówione najczęściej wykorzystywane magistrale komputerowe — uniwersalna magistrala szeregową (USB — *Universal Serial Bus*) oraz FireWire (IEEE 1394) — które można postrzegać jako pewne odmiany osobistych sieci lokalnych (pLAN).

## Uniwersalna magistrala szeregową

Uniwersalna magistrala szeregową (USB) znajduje powszechne zastosowanie w przyłączaniu urządzeń peryferyjnych. Od roku 1999 znalezienie płyty głównej, która nie obsługiwałaby tego standardu, jest niemalże niemożliwe. Teoretycznie magistrala USB obsługuje do 127 urządzeń za pomocą jednego kontrolera. W praktyce jednak maksymalna liczba zewnętrznych komponentów jest nieco niższa, niż wynika z przestrzeni adresowej. Standard został opracowany przez grupę przemysłową o nazwie USB Implementers Forum (<http://www.usb.org>). Organizacja ta wydała trzy wersje standardu — 1.0, 2.0 i 3.0.

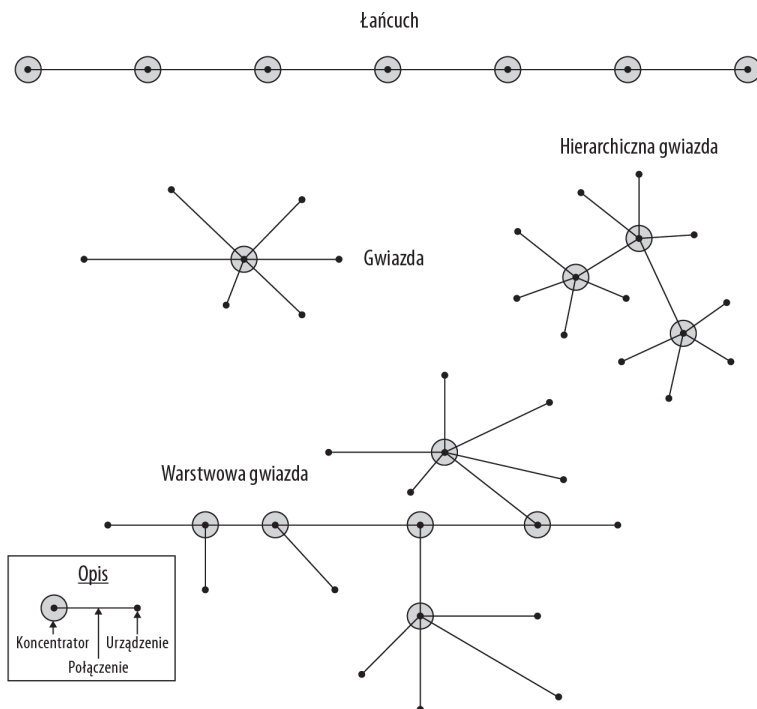
Największą zaletą technologii USB jest to, że urządzenia można przyłączać i odłączać bez konieczności wyłączania systemu. Nie mniej istotna jest również obsługa mechanizmu plug-and-play. Zgodnie ze standardem urządzenia zewnętrzne mogą dysponować własnym zasilaniem lub wykorzystywać zasilanie magistrali. Rozwiązanie to jest więc często stosowane w obsłudze urządzeń wprowadzania danych, komponentów wyjściowych, interfejsów sieciowych oraz zewnętrznych kart rozszerzeń. Zasilanie portów USB pozwala na przyłączanie urządzeń, które wymagają ładowania (choć niezbyt szybkiego). Są również dostępne wersje portów USB o nazwie PoweredUSB, wyposażone w cztery dodatkowe złącza, które można obciążyć prądem 6 A przy napięciu 5 V, 12 V lub 24 V. Jeśli jakiegokolwiek urządzenie wymaga do pracy zasilania o większej mocy, musi zostać wyposażone we własny zasilacz.

Magistrale USB są nadzorowane przez główny kontroler stacji, który odpowiada za przyłączanie urządzeń i tworzenie sieci pLAN o topologii hierarchicznej gwiazdy (przedstawionej na rysunku 11.4). W topologii tej każde urządzenie, które jest połączone z dwoma komponentami lub większą ich liczbą, pełni funkcję koncentratora. Punkty końcowe odpowiadają urządzeniom USB. Natomiast doprowadzone do nich linie reprezentują poszczególne połączenia USB (kable). Dołączenie kolejnego kontrolera pozwala na uzyskanie większego współczynnika rozgałęzień. Budowana struktura może się składać maksymalnie z pięciu poziomów komponentów. Dodatkowe kontrolery również są nazywane *koncentratorami*. Ograniczenie do 127 urządzeń odnosi się do każdego z kontrolerów stacji oddzielnie. Kontrolery stacji są instalowane w formie układów logicznych na płycie głównej, w kartach rozszerzeń lub w koncentratorach USB. Technologia jest powszechnie wykorzystywana i niedroga, dlatego kontrolery znajdują się w urządzeniach różnego typu.

Urządzenia USB komunikują się z kontrolerem stacji za pomocą kanałów logicznych nazywanych *potokami*. W przeciwieństwie do sieci komputerowych za punkt końcowy uznawany jest jedynie komponent znajdujący się na końcu potoku, po stronie urządzenia. Każde urządzenie może utworzyć 32 aktywne potoki jednokierunkowe z ograniczeniem do 16 potoków wejściowych i 16 potoków wyjściowych. Jeden punkt końcowy, nazywany *zerowym punktem końcowym*, jest zarezerwowany do sterowania urządzeniem. Z kolei zbiór punktów końcowych realizujących wspólne zadanie jest określony mianem *grupy*.

**Rysunek 11.4.**

Warstwowa gwiazda  
zawiera elementy  
topologii łańcucha  
i gwiazdy



W czasie przyłączania urządzenia do magistrali USB kontroler stacji otrzymuje sygnał o konieczności odpytania komponentów magistrali i sporządzenia ich listy. Nowo przyłączony element zostaje zresetowany, a po ponownym wykryciu jest konfigurowany. W tym czasie otrzymuje 7-bitowy adres. Ponieważ w magistralach szeregowych istnieje tylko jedna ścieżka przesyłania danych, komunikacja z poszczególnymi urządzeniami odbywa się sekwencyjnie w wyznaczonej kolejności.

Urządzenia USB 2.0 tworzą interfejsy nazywane rozszerzonymi interfejsami kontrolerów stacji (EHCI — *Enhanced Host Controller Interface*). Ich zadanie polega na wyznaczaniu klas urządzeń obsługiwanych przez system operacyjny. Dzięki nim dostawcy systemów operacyjnych mogą przygotowywać ogólne sterowniki, współpracujące z całą gamą urządzeń.

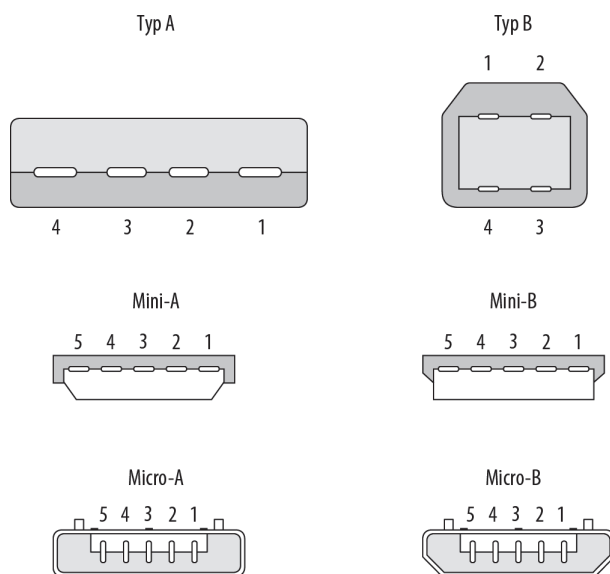
Porty USB 2.0 wymieniają dane z przepływnością 480 Mb/s, a w przypadku pracy w trybie zgodności z wersją 1.0 umożliwiają komunikację z pełną przepustowością 12 Mb/s lub obniżoną przepustowością 1,5 Mb/s. W wersji 3.0 szybkość wymiany danych może osiągnąć nawet 4,8 Gb/s. Podane wartości odnoszą się do najkorzystniejszego wariantu komunikacji. Większość komponentów USB 2.0 uzyskuje szybkość wymiany danych na poziomie 65 procent maksymalnej wartości. Kabel USB to skrętka umożliwiająca przesyłanie informacji w trybie półduplexowym. Dane można przechwytywać za pomocą specjalnych analizatorów protokołu USB, co umożliwia przeprowadzenie czynności diagnostycznych.

Dane USB są transmitowane w formie ramek o rozmiarze będącym krotnością 8 bitów. Na początku każdej ramki przesyłany jest nagłówek synchronizacyjny, a na końcu krótki sygnał znacznika końcowego. Komunikacja rozpoczyna się od przesłania ramki z kontrolera stacji do urządzeń. Jeśli kontroler znajduje się na najwyższym poziomie w hierarchii, trasa, którą

przesyłane są ramki, wiedzie przez główny koncentrator. Urządzenia odpowiadają na za-inicjowane przez stację połączenie pakietami akceptacji połączenia, które z kolei są potwierdzane przez tę stację. W komunikacji wykorzystuje się znaczniki, pakiety danych (dwa rodzaje) oraz pakiety typu PRE. W połączeniach USB stosowany jest model odpłytywania, w którym kontroler stacji zarządza całą komunikacją.

Kable USB mogą być zakończone sześcioma różnymi wtyczkami: typu A, typu B, Mini-A, Mini-B, Micro-A i Micro-B. Złącza typu A i B mają cztery wyprowadzenia. Natomiast wtyczki Mini-A i Mini-B oraz Micro-A i Micro-B mają sześć wyprowadzeń. Oczywiście wszystkim wtyczkom towarzyszą gniazda. Na rysunku 11.5 zostały przedstawione poszczególne odmiany wtyczek. Bardzo często stosowane są kable, które zawierają złącza różnego typu. Niemniej zgodnie z ogólną zasadą po stronie urządzenia powinny być wykorzystywane wtyczki typu B. Kable celowo zostały zakończone różnymi złączami, aby użytkownicy nie mogli tworzyć pętli, które uniemożliwiłyby pracę magistrali. Mniejsze złącza są zazwyczaj stosowane w mniejszych urządzeniach — na przykład w telefonach komórkowych lub aparatach fotograficznych. Format Micro-USB powinien w przyszłości zastąpić wtyczki z grupy mini. Urządzenia USB 3.0 będą wyposażane w złącza jednego typu, podobne do złączy A i B w standardzie 2.0, ale uzupełnione o pięć dodatkowych wyprowadzeń.

**Rysunek 11.5.**  
Rodzaje wtyczek USB



Standardowa długość kabla USB nie może przekroczyć 5 m, ponieważ dłuższe odległości doprowadziłyby do utraty jakości sygnału. Na rynku są jednak dostępne regeneratory, które istotnie zwiększają moc sygnału i pozwalają na znaczne przedłużenie odcinka przyłączeniowego. Zazwyczaj są to koncentratory mini-USB przyłączone do kabla USB. Złączając pięć koncentratorów USB, można uzyskać 30-metrowe połączenie. W standardzie USB 3.0 kable zostały całkowicie zmienione. Wyglądem przypominają kable ethernetowe. Ich maksymalna długość została zmniejszona do 3 m, ale za to umożliwiają transmisje w trybie pełnego duplexu. Niektórzy producenci akcesoriów komputerowych oferują również bezprzewodowe koncentratory USB, jednak są to ich rozwiązania firmowe. Organizacja USB-IF aktualnie pracuje nad specyfikacją bezprzewodowego połączenia szerokopasmowego o przepływności 480 Mb/s.

## FireWire

FireWire jest wymyśloną przez firmę Apple nazwą marketingową standardu magistrali szeregowej IEEE 1394. Interfejs IEEE 1394 jest alternatywnym rozwiązaniem w stosunku do USB 2.0, które gwarantuje szybką wymianę danych i jest wykorzystywane w połączeniach z cyfrowymi aparatami fotograficznymi, cyfrowymi urządzeniami audiowizualnymi i twardymi dyskami. Standard IEEE 1394 wyparł w tych zastosowaniach technologię SCSI jako łatwiejszy w zastosowaniu i konfiguracji. Choć magistrale FireWire często są uwzględniane w budowie płyt głównych komputerów PC lub mogą być dodawane do komputerów PC, nie są nawet w części tak popularne, jak w przypadku komputerów Macintosh. To właśnie w systemach Macintosh po raz pierwszy wykorzystano ten rodzaj magistrali. Inne nazwy standardu IEEE 1394 to i.LINK w produktach firmy Sony oraz Lynx w produktach Texas Instruments.

Magistrala FireWire umożliwia przyłączenie do 63 urządzeń w topologii drzewa. W strukturze tej występuje jeden węzeł główny, o najwyższej wartości identyfikatora. Podczas resetowania magistrali przyłączone do niej urządzenia otrzymują adresy wyznaczone przez mechanizm przeszukiwania w głąb (DFS — *Depth First Search*). Na rysunku 11.6 zostało przedstawione działanie algorytmu przeszukiwania drzewa. Jako pierwsza jest analizowana najdłuższa krawędź (w tym przypadku). Po dotarciu do najniższego węzła proces przeszukiwania jest kontynuowany w kierunku węzła głównego. Zatem cała procedura rozpoczyna się w węźle głównym, który jest analizowany jako pierwszy. Następnie przeszukiwana jest pierwsza gałąź (węzły od 2. do 8.). Jeśli nie zostanie znaleziony potrzebny element, algorytm kontynuuje poszukiwania w kolejnych gałęziach, analizując je od góry do dołu (w kolejności węzłów: 9., od 10. do 14. i na końcu 15.).

Mechanizm DFS został wybrany jako podstawowy sposób analizy drzewa, ponieważ jest łatwiejszy w implementacji niż algorytm przeszukiwania wszerz (BFS — *Breadth First Search*), i choć nie należy do najefektywniejszych technik wyszukiwania, niewielka pojemność magistrali IEEE 1394 usprawiedliwia jego zastosowanie.

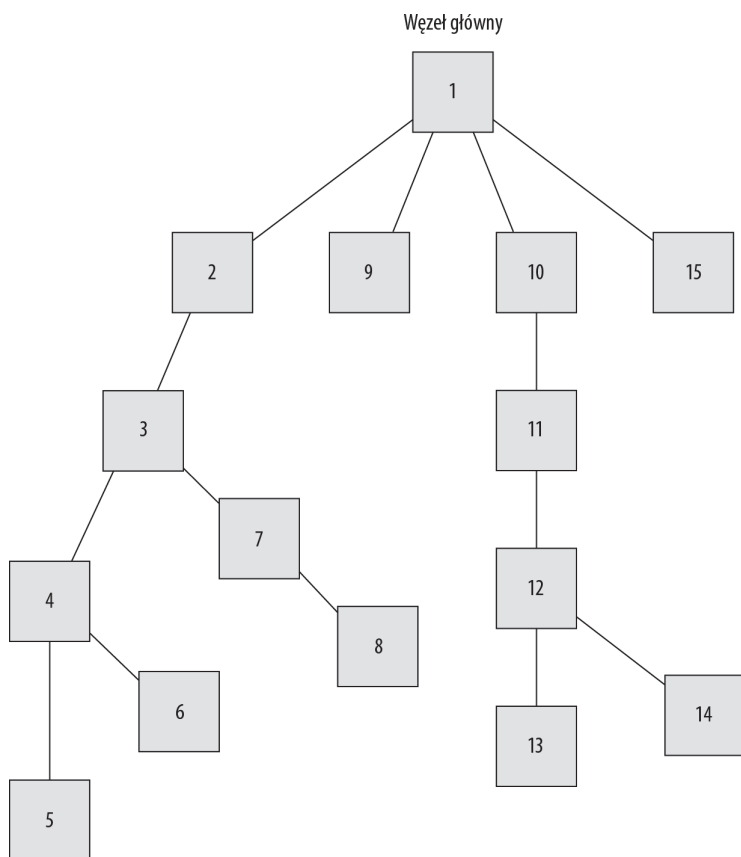
Urządzenia standardu IEEE 1394 są sobie równorzędne. Nie mogą być wyłączone w czasie pracy i nie udostępniają funkcji automatycznej konfiguracji (plug-and-play). Mechanizm sporządzania listy urządzeń FireWire bazuje na identyfikatorach IEEE EUI-64, a nie na 48-bitowych ethernetowych adresach MAC. Pierwsza z form adresacji stanowi nadzbiór w stosunku do drugiego ze zbiorów adresów — adresy zawierają dodatkowe informacje o rodzaju urządzenia i obsługiwanych protokołach.

Od 1995 roku technologia FireWire została opisana w kilku standardach. Pierwotna specyfikacja FireWire 400 (IEEE 1394-1995) i jej rozszerzona wersja (IEEE 1394a-2000) są najczęściej implementowanymi standardami urządzeń. Zgodnie z założeniami FireWire 400 komunikacja ma charakter półdupleksowy i może być realizowana z przepływnością od 100 Mb/s do 400 Mb/s w połączeniu o długości do 4,5 m.

Podobnie jak w przypadku standardu USB, istnieje możliwość przekształcenia magistrali w łańcuch o maksymalnej liczbie 16 połączeń. Urządzenia FireWire mają znacznie większe zapotrzebowanie na moc w porównaniu z komponentami USB i wymagają stosowania aktywnych regeneratorów — koncentratorów FireWire. Typowe połączenie — z użyciem szścioprzewodowego obwodu FireWire 400 — wymaga zasilania od 25 V do 30 V i zapewnia

**Rysunek 11.6.**

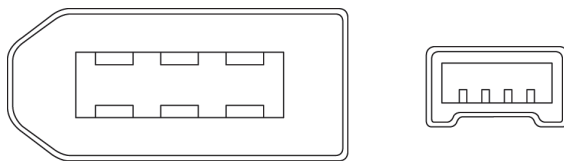
*Działanie  
algorytmu DFS  
wykorzystywanego  
do wykrywania  
urządzeń FireWire*



pobór mocy do 8 W. Jest to wystarczająco duża moc, aby zasilić takie urządzenia zewnętrzne, jak skanery lub drukarki, co przez wielu użytkowników jest postrzegane jako duża zaleta rozwiązania. Złącza FireWire 400 zostały pokazane na rysunku 11.7.

**Rysunek 11.7.**

*Sześćcio-  
i czteroprzewodowe  
złącza FireWire 400*



Wykorzystanie magistrali FireWire stanowi ułamek zastosowań standardu USB. Komponenty USB 2.0 pracują jednak nieco wolniej od urządzeń FireWire 400 z powodu dodatkowego narzutu protokołu USB. Połączenia FireWire 800 umożliwiają przekazywanie danych z przepływnością do 3200 Mb/s, podczas gdy połączenia USB typu high-speed gwarantują jedynie 25 procent tej szybkości (480 Mb/s). Okazuje się jednak, że szybkość transmisji nie jest najważniejszym argumentem. Kluczowa wydaje się cena urządzeń zewnętrznych. Do magistrali FireWire zazwyczaj przyłączone jest jedno lub dwa urządzenia. Rzadko kiedy ich liczba jest większa. Rynek urządzeń USB rozwijał się znacznie szybciej i obecnie jest to dominująca technologia w sieciach pLAN.

Standard FireWire umożliwia tworzenie połączeń sieciowych między komputerami w formie łączy bezpośrednich (połączenia jednostek równorzędnych) lub z wykorzystaniem koncentratora FireWire. Urządzenia mogą posługiwać się adresacją IPv4 lub IPv6. Obsługa sieci na bazie magistrali FireWire jest zawarta w systemach operacyjnych Mac OS X, Free BSD, Linux, Windows ME/2000/XP oraz Windows Serwer 2003. Microsoft zaprzestał rozwijania oprogramowania dla sieci FireWire w 2004 roku. Nawet firma Sony, która jako pierwsza zastosowała łącze i.LINK w komunikacji sieciowej, uznała, że większość użytkowników woli korzystać z kart ethernetowych.

Aby przeciwdziałać niekorzystnym trendom, ostatnia wydana specyfikacja — FireWire S800T (IEEE 1394c-2006), opublikowana w lipcu 2007 roku — uwzględnia współpracę z sieciami Ethernet. Zdefiniowano w niej port o przepustowości 800 Mb/s, do którego za pomocą złącza RJ-45 przyłączana jest skrętka kategorii 5e. Jest to więc taki sam kabel, jaki jest stosowany w gigabitowym Ethernetie. Sam standard zapewnia natomiast automatyczne rozpoznawanie urządzeń Ethernet i FireWire korzystających z portu. Najnowsze rozwiązanie, choć intrygujące, nie jest jeszcze wdrażane w żadnych oferowanych produktach. Być może pewnego dnia zostanie dostrzeżone i stanie się atrakcyjniejsze.

## Bluetooth

Bluetooth jest technologią osobistych bezprzewodowych sieci LAN, która umożliwia tworzenie bezpiecznych połączeń z urządzeniami niezbyt odległymi od siebie. Rozwiązanie to jest znane przede wszystkim jako sposób łączenia telefonów komórkowych z zestawami słuchawkowymi. Jednak znajduje także zastosowanie w drukarkach, klawiaturach, urządzeniach PDA i GPS, czytnikach kodów paskowych i innych komponentach peryferyjnych. Jednostki sieci Bluetooth automatycznie wykrywają inne jednostki tego typu i mogą się z nimi komunikować. Standard Bluetooth został opracowany przez organizację Bluetooth Special Interest Group (<http://www.bluetooth.com>).



Nazwa technologii pochodzi od nazwiska dziesięciowiecznego króla Danii — Haralda Bluetootha — który zjednoczył większą część Norwegii, Szwecję i Danię — trzy kraje usytuowane w bliskim sąsiedztwie.

Rozwiązania stosowane w systemach Bluetooth są zbliżone do wykorzystywanych w telefonii komórkowej. Transmisja odbywa się zgodnie z techniką rozpraszania widma z przesłakiwaniem po częstotliwościach. W Stanach Zjednoczonych i w Europie wykorzystywane jest pasmo w okolicach częstotliwości 2,45 GHz. Ponieważ jest ono uznawane za ogólnodostępne, urządzenia mogą bez przeszkód nadawać swoje informacje. Ten sam przedział częstotliwości wykorzystuje się też w sieciach bezprzewodowych 802.11g, wielu telefonach komórkowych i innych urządzeniach. Niestety, tę częstotliwość mają również fale emitowane przez kuchenki mikrofalowe, co jest przyczyną zakłócania pracy komponentów sieci 802.11g oraz Bluetooth.

Dokładny zakres częstotliwości wynosi 2400 – 2483,5 GHz i jest podzielony na 79 niezależnych kanałów o szerokości pasma 1 MHz. W Japonii używane są 23 kanały o szerokości 1 MHz. Aby uzyskać przepływność bitową transmisji między urządzeniami na poziomie 1 Mb/s, stosowana jest modulacja GFSK, czyli gaussowskie kluczowanie częstotliwości.

Nadajniki Bluetooth są zaliczane do trzech klas:

- ♦ Klasa 1. — 100 mW o zasięgu 100 m.
- ♦ Klasa 2. — 2,5 mW o zasięgu 10 m.
- ♦ Klasa 3. — 1 mW o zasięgu 1 m.

Trzy wymienione klasy odnoszą się do urządzeń, które odgrywają rolę dookolnych nadajników. Niska moc nadawcza oznacza, że sygnały Bluetooth nie mogą przenikać ścian. Dla porównania telefony komórkowe emitują sygnał o mocy 3 W. Użycie urządzenia sklasyfikowanego jako komponent o mniejszym zasięgu (na przykład jako element klasy 2.) w sieci urządzeń o większym zasięgu (na przykład w sieci klasy 1.) zwiększa w pewien sposób obszar oddziaływania tego urządzenia.

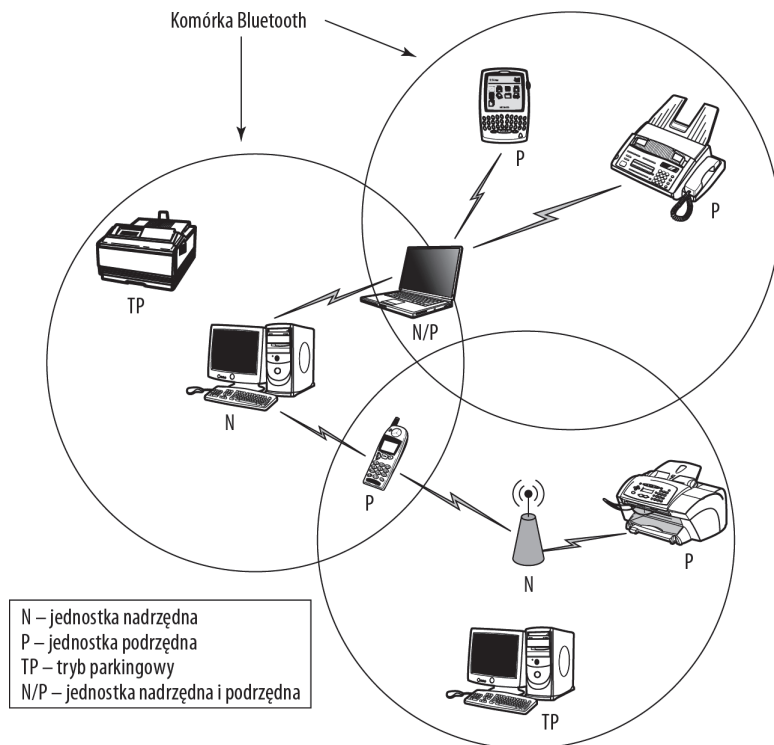
## Połączenia

Aby utworzyć sieć Bluetooth — nazywaną *pikosiecią* — potrzebny jest koncentrator Bluetooth z własnym modulem radiowym. Pikosieć (przedstawiona na rysunku 11.8) jest definiowana jako tworzona ad hoc sieć połączeń między urządzeniami Bluetooth (zarówno aktywnymi, jak i pasywnymi). Z założenia jest to rozwiązanie zdecentralizowane, w którym każdy węzeł może przekazywać dane do innych węzłów. Do opisu tego typu konfiguracji używa się również określenia *sieć rozproszona* (ang. *scatternet*). Obsługa standardu Bluetooth jest uwzględniana w wielu laptopach oraz urządzeniach im towarzyszących, takich jak klawiatura Logitech diNovo. Dostępne są również koncentratory Bluetooth przyłączane do portów USB, instalowane w formie kart PC (PCMCIA) lub PCI. Standard Bluetooth umożliwia jednoczesną pracę z jedynie ośmioma urządzeniami.

Jednostki klienckie mogą w dowolnej chwili przyłączyć się do sieci lub ją opuścić. Taki sposób działania jest charakterystyczny dla wielu sieci bezprzewodowych. Zadanie ustanawiania połączeń jest wykonywane przez specjalne adaptacyjne funkcje wyboru tras.

W całej sieci może pracować do  $2^8-1$  (255) urządzeń. Natomiast pikosieć może się składać z ośmiu elementów, z których jeden jest komponentem nadrzędnym (ang. *master*), a siedem pozostałych pracuje jako urządzenia podrzędne (ang. *slave*). Role urządzeń zostały przedstawione na rysunku 11.8. Dana jednostka może pełnić funkcję nadrzędną w większej liczbie pikosieci. Analogicznie poszczególne jednostki mogą być urządzeniami nadrzędnymi i podrzędnymi w dwóch pikosieciach lub większej ich liczbie. Komponenty zarejestrowane, ale nieaktywne, pracują w trybie „parkingowym”, co na rysunku zostało oznaczone symbolem TP. Włączenie urządzenia powoduje rozpoczęcie procedury wyszukiwania innych elementów sieci zdolnych do nawiązania komunikacji. Aby przyłączyć daną jednostkę do sieci, trzeba jej przypisać nazwę, adres (w formacie ###.###.###.###.###.### — sześć par cyfr) oraz hasło (PIN). Hasło jest wspólne dla wszystkich urządzeń biorących udział w komunikacji i służy do kryptograficznego uwierzytelniania poszczególnych punktów końcowych względem siebie. Adres jest niepowtarzalnym identyfikatorem, przypisywanym urządzeniu przez producenta i zależnym od klasy komponentu. Identyfikator ten nie jest wykorzystywany w czasie nawiązywania połączenia, ponieważ zamiast niego użytkownicy posługują się łatwiejszymi do zapamiętania nazwami.

**Rysunek 11.8.**  
Pikosieć Bluetooth



Dane są przekazywane w formie pakietów o maksymalnym rozmiarze 2745 bitów. Niemal 80 procent rozmiaru stanowi pole ładunkowe (dane), a pozostałą część zajmuje nagłówek oraz pola parametrów protokołu. Komunikacja rozpoczyna się z chwilą, gdy urządzenie wybierze jeden spośród 79 losowo dobieranych kanałów i rozpocznie przysyłanie danych. Zmiana kanału następuje co 625 mikrosekund, czyli blisko 1600 razy na sekundę. Jeden pakiet bywa przesyłany w pięciu różnych szczelinach czasowych. Gdyby inne urządzenie wybrało ten sam kanał, procedura detekcji błędów wykryłaby dostarczenie niepoprawnych informacji i wymusiłaby retransmisję pakietów.

Ponieważ prawdopodobieństwo wystąpienia kolizji wynosi 1 do 79 (1,3 procent), liczba przypadków jednoczesnej transmisji na tym samym kanale jest znikoma. Prawdopodobieństwo wystąpienia dwóch kolizji po sobie wynosi 1 do  $79^2$  (0,016 procent), a trzech 1 do  $79^3$  (0,000021 procent).

Połączenia Bluetooth mogą być realizowane w trybie półduplexu lub pełnego duplexu. W trybie pełnego duplexu urządzenie nadaje i odbiera informacje w tym samym czasie. W transmisji półduplexowej operacje te są wykonywane naprzemiennie. Urządzenia działające w trybie pełnego duplexu, takie jak telefony, mogą transmitować i odbierać dane głosowe z przepływnością 64 kb/s. Taka szybkość przesyłania umożliwia budowanie wielopołączeniowych telefonów, które obsługują kilka jednoczesnych konwersacji. Półduplexowe połączenie Bluetooth komputera z drukarką jest znacznie wydajniejsze i osiąga przepływność do 721 kb/s. Gdy jest ono realizowane z wykorzystaniem dwóch półduplexowych kanałów, przepustowość jednego kanału nie przekracza 432 kb/s.

Połączenia Bluetooth są klasyfikowane jako synchroniczne połączeniowe (SCO — *Synchronous Connection Oriented*) lub asynchroniczne bezpołączeniowe (ACO — *Asynchronous Connectionless Oriented*). Połączenia synchroniczne wymagają utworzenia relacji nadrzędny-podrzędny, w której jedno urządzenie nadrzędne może nawiązać komunikację z maksymalnie trzema komponentami podrzędnymi. Przepustowość każdego połączenia wynosi 64 kb/s. W komunikacji nie występują kolizje, ponieważ jednostka nadrzędna zarządza wykorzystaniem kanałów. Połączenia asynchroniczne są możliwe tylko między urządzeniem nadrzędnym a jednym komponentem podrzędnym. Niemniej zadanie zarządzania przepływem danych nadal należy do urządzenia nadrzędnego.

## Profile

W standardzie Bluetooth zdefiniowano system profili, które precyzują sposób działania poszczególnych urządzeń w sieci, gwarantujący dostępność określonych usług. Każde urządzenie musi przesłać swoją nazwę, informację o klasie, listę usług i funkcji, dane producenta, informacje o przesunięciu czasowym oraz wersję obsługiwanego protokołu Bluetooth. Poszczególne profile umożliwiają zastosowanie różnych protokołów i formatów wymienianych danych oraz dopracowywanie zakresu funkcji, które muszą realizować jednostki o określonym profilu. Same profile należy postrzegać jako pewną formę opisu interfejsu sieciowego Bluetooth.

Organizacja Bluetooth SIG zdefiniowała 28 profili, a cztery kolejne oczekują na zatwierdzenie. Przeanalizujemy kilka profili związanych z sieciami. Urządzenia starszego typu, które mogą być przyłączane do sieci LAN (na przykład koncentrator Bluetooth), prawdopodobnie korzystają z profilu dostępu do sieci LAN (LAP — *LAN Access Profile*). Profil LAP umożliwia urządzeniom łączenie się z siecią IP w ramach dowolnego połączenia fizycznego. W specyfikacji LAP zdefiniowano zasady korzystania z protokołu PPP w komunikacji radiowej (RFCOMM — *Radio Frequency Communication*).

Nowsze urządzenia wykonują to samo zadanie w ramach profilu sieci osobistych (PAN — *Personal Area Networking*), który bazuje na innym protokole warstwy sieciowej (3. warstwy modelu OSI). Osoby wykorzystujące moduł Bluetooth telefonu do łączenia komputera (laptopa) z internetem najczęściej używają profilu połączeń komutowanych (DUN — *Dial-Up Networking*), który jest podobny w działaniu do profilu portu szeregowego (SPP — *Serial Port Profile*), posługującego się poleceniami modemowymi serii AT i protokołem PPP. Wybór profilu jest negocjowany między punktami końcowymi połączenia Bluetooth. Dzięki temu obydwie jednostki stosują jednakowy format danych.

## Podsumowanie

W tym rozdziale zostały przedstawione zasady budowania sieci o niewielkim obszarze działania i (lub) skupiających niewielu użytkowników — tzw. osobistych sieci lokalnych (pLAN).

Niewielka liczba użytkowników i często mały obszar działania bywa również cechą sieci peer-to-peer (P2P). Typowym przykładem rozwiązania P2P jest bowiem grupa robocza, która zazwyczaj składa się z kilku systemów. Jednak model P2P opisuje także sposób działania aplikacji rozproszonych, funkcjonujących w wielu systemach rozmieszczonych na dużym obszarze geograficznym.

Tematyka rozdziału obejmuje zagadnienia związane z czystymi systemami P2P oraz hybrydowymi systemami P2P. Przykładami tych rozwiązań są sieci Gnutella, Freenet, Napster i BitTorrent.

Niektóre magistrale komputerowe pełnią funkcje sieci osobistych. Dlatego wśród poruszanych zagadnień zostały uwzględnione standardy USB, FireWire i Bluetooth, które można analizować jako instalacje sieciowe.

W kolejnym rozdziale zostały przedstawione lokalne sieci komputerowe. Rozdział 12. jest poświęcony różnym sposobom budowania sieci LAN z uwzględnieniem ich oprogramowania, adresacji i innych elementów, które nie są związane ze sprzętem.



# Rozdział 12.

# Tworzenie sieci lokalnych

## W tym rozdziale:

- ♦ Wprowadzenie do sieci LAN
- ♦ Technologia transmisji i problemy sieciowe
- ♦ Sieć Ethernet
- ♦ Sieci Token Ring i FDDI
- ♦ Sieci w automatyce przemysłowej
- ♦ Automatyzacja domu za pomocą sieci X10

Niniejszy rozdział przedstawia główne rodzaje sieci lokalnych LAN (ang. *Local Area Network*) z wyjątkiem sieci bezprzewodowych. Zawarto tu opis różnych technologii i informacje na temat tego, jak można je wykorzystać w budowie sieci LAN. Omówiono następujące typy sieci: Ethernet, Token Ring, sieci światłowodowe FDDI, X10 oraz kilka standardów magistrali wykorzystywanych w automatyce przemysłowej. Wymienione rodzaje sieci zostały ujęte odpowiednimi normami IEEE 802.x, które są również przedstawione.

Ethernet jest przykładem sieci, w której transmisja danych odbywa się przy użyciu ramek. Ramki zawierają standardowo pola z adresami źródłowym i docelowym, a także pola synchronizacji, kontroli błędów itp. W dalszej części rozdziału znajduje się pełny opis ramki sieci Ethernet. W tym rozwiązaniu wykorzystuje się protokół wielodostępu CSMA/CD (ang. *Carrier Sense Multiple Access with Collision Detection* — protokół wielodostępu do łącza ze śledzeniem dostępności nośnej i wykrywaniem kolizji).

W sieciach Token Ring użyto innej metody dostępu. W tym przypadku sieć składa się z węzłów, które mogą transmitować pakiety po otrzymaniu specjalnej ramki, zwanej tokenem. Sieci Token Ring są obecnie w dużej mierze realizowane przez IBM, ich szczególną odmianą są sieci FDDI, utworzone za pomocą światłowodów umożliwiających przesyłanie danych z bardzo dużą prędkością. Tego typu sieci były powszechnie stosowane w przeszłości, zwłaszcza w branży telekomunikacyjnej.

Sieci X10 umożliwiają wykorzystanie istniejących sieci energetycznych, co stosuje się przy budowie systemów automatyzacji w domu (tzw. dom inteligentny). W niniejszym rozdziale omówiono sygnalizację i podstawowe standardy automatyzacji używane w tych sieciach.

Opisano tu również sieci obecne w automatyce przemysłowej. Umożliwiają one gromadzenie danych z czujników, siłowników, przełączników, zaworów i innych urządzeń, a następnie przekazywanie ich do węzła centralnego, zawierającego interfejs użytkownika HMI (ang. *Human Machine Interface*). Omówiono tu w szczególności standard Modbus<sup>1</sup>, kontrolery programowalne, standard OPC (ang. *OLE for Process Control*)<sup>2</sup>, a także systemy SCADA (*Supervisory Control And Data Acquisition* — system nadzorujący przebieg procesu technologicznego lub produkcyjnego).

## Wprowadzenie

Sieci LAN to lokalne sieci komputerowe o zasięgu ograniczonym liczbą elementów administrowanych, takich jak domeny i podsieci. Sieci LAN można scharakteryzować następującymi parametrami:

- ♦ topologia,
- ♦ medium transmisyjne,
- ♦ standard, technologia,
- ♦ rozmiar,
- ♦ sposób zarządzania.

W rozdziale 3. przedstawiono topologie możliwe do zastosowania między innymi w sieciach lokalnych. Dostępne media transmisyjne opisano w rozdziale 8., a w rozdziale 30. zaprezentowano sposoby zarządzania siecią. W niniejszym rozdziale omówiono standardy i technologie sieci lokalnych, a także ich rozmiary pod względem liczby węzłów, połączeń i długości; przedstawiono kilka najważniejszych standardów LAN:

- ♦ Ethernet, najpowszechniejszy standard,
- ♦ Token Ring, umożliwiający synchroniczny dostęp do sieci,
- ♦ FDDI, który jest protokołem dużej prędkości dla sieci Token Ring,
- ♦ X10 RF, który umożliwia komunikację urządzeń poprzez sieć elektryczną, oraz inne podobne standardy,
- ♦ standardy definiujące magistrale i wymianę danych w przemyśle (automatyka przemysłowa).

---

<sup>1</sup> Modbus — protokół komunikacyjny opracowany przez firmę Modicon dla sterowników programowalnych. Protokół Modbus umożliwia zarządzanie urządzeniami automatyki przemysłowej, połączonymi w sieć. Modbus jest obecnie standardem otwartym — *przyp. tłum.*

<sup>2</sup> OPC, *OLE for process control*, standard komunikacyjny automatyki przemysłowej. OPC jest standardem otwartym — *przyp. tłum.*

Wymieniono tu pięć typów standardów, które są wykorzystywane w budowie sieci lokalnych LAN. Zostanie tu przybliżone, jak można zaprojektować sieć LAN oraz w jaki sposób wygląda przetwarzanie i transmisja danych w określonej sieci. Obecnie w budowie sieci lokalnych dość powszechnie stosuje się technologie bezprzewodowe. Aby w pełni zapoznać się ze współczesnymi sieciami lokalnymi, warto zajrzeć do rozdziału 14., gdzie przedstawiono standardy sieci bezprzewodowych (Wi-Fi).

Aby przy tworzeniu sieci Ethernet można było skorzystać z elementów różnych typów, trzeba zapewnić ich współdziałanie. Poszczególne elementy sieci muszą być produkowane z uwzględnieniem przyjętych i powszechnie znanych standardów. Większość standardów Ethernet powstała dzięki instytutowi IEEE (Instytut Inżynierów Elektryków i Elektroników — ang. *Institute of Electrical and Electronics Engineers*). W następnym rozdziale zaprezentowano kilka stosowanych obecnie wersji standardów IEEE. Zasadniczą cechą każdej sieci jest obsługiwany obszar, w którym komunikacja odbywa się bez konieczności modyfikacji. Takim obszarem jest domena rozgłoszeniowa. Domeny rozgłoszeniowe i ich związek z sieciami Ethernet przedstawiono w podrozdziale poświęconym standardom IEEE.

## Standardy sieci LAN

W trakcie powstawania kolejnych standardów sieci lokalnych w instytucie IEEE sprawdzono, które z nich są wykorzystywane w praktyce, i opracowano oficjalny zestaw standardów. Poszczególne standardy powstały w wyniku prac pojedynczych dostawców urządzeń sieciowych (np. technologia Token Ring została opracowana przez IBM), grupy kilku dostawców, której przykładem jest DIX (grupę tworzą firmy DEC, Intel i Xerox; ta grupa wprowadziła standard Ethernet), lub innych grup roboczych.

W miarę możliwości instytut IEEE stara się uogólniać specyfikacje standardów, tak aby urządzenia różnych producentów mogły bezawaryjnie ze sobą współpracować. Przykładem standardu, który powstał na bazie technologii firmy IBM, jest Token Ring. Koncern IBM zgłosił wymaganie konkretnego medium transmisyjnego dla sieci Token Ring, po czym instytut IEEE zaproponował odpowiednie wymagania przygotowywanego standardu. W wyniku wstępnych prac instytutu powstała specyfikacja RFC, która była modyfikowana w trakcie dalszych prac. Zwykle specyfikacje RFC są wielokrotnie modyfikowane, zanim powstanie stabilna wersja dokumentu. Gdy odpowiednie dokumenty RFC zostały zaktualizowane po przeglądzie w grupach roboczych, instytut IEEE utworzył oficjalną wersję standardu i opublikował ją.

W ten sposób powstał zestaw piętnastu standardów, które są rozwijane od 30 lat. Wykaz omawianych standardów znajduje się w tabeli 12.1. Na bazie standardów definiuje się warianty (standardy pochodne). Dobrym przykładem jest standard sieci bezprzewodowej 802.11 — w ciągu ostatniej dekady powstały warianty 802.11a, 802.11b, 802.11g oraz 802.11n tego standardu.

**Tabela 12.1.** Rodzaje standardów rodziny IEEE 802

Standard	Przeznaczenie	Standardy pokrewne
802.1	Określa sposób współdziałania między sieciami LAN i WAN; standardy mostowania i zarządzania sieciami LAN/MAN	802.1b, zarządzanie LAN/MAN; 802.1D, mosty MAC; 802.1e, protokół System Load Protocol; 802.1f, definicje procedury zarządzania informacją w 802.1; 802.1G, zdalne mostowanie MAC; 802.1H, most MAC w sieciach Ethernet; 802.1Q, sieci VLAN; 802.1x, zarządzanie dostępem do sieci na podstawie portów; 802.1AB, protokół LLD; 802.1ad, mostowanie dostawców usług; 802.1AE, zabezpieczenia MAC; 802.1af, zabezpieczenia oparte na kluczach <sup>3</sup> ; 802.1ag, zarządzanie błędami połączenia; 802.1ah, Provider Backbone Bridge (PBB) — umożliwienie stosowania MAC w MAC-u; 802.1aj, Two Port Mac Relay (TPMR); 802.1ak, protokół MRP 802.1ap, MIBs; 802.1aq, SPB; 802.1AR, identyfikacja urządzeń (DevID); 802.1AS, definicja czasu synchronizacji dla aplikacji w sieciach mostkowanych LAN; 802.1Qat, protokół Stream Reservation Protocol; 802.1Qau, zarządzanie natłokiem ruchu; 802.1Qav, kolejkovanie strumieni; 802.1Qaw, zarządzanie błędami połączeń 802.1Qay, standard PBB-TE; 802.1Qaz, rozszerzenia transmisji; 802.1BA, systemy mostowania audio-wideo.
802.2	Warstwa LLC — zarządzanie łączem logicznym	Brak standardów pokrewnych. Warstwa LLC odpowiada za zarządzanie komunikacją i adresacją łączy, definiuje punkty dostępu do usług (SAP — <i>Service Access Points</i> ) oraz zapewnia sekwencjonowanie.
802.3	CSMA/CD	W tej grupie znajdują się standardy przeznaczone dla sieci Ethernet. W tabeli 12.2 znajduje się wykaz standardów pokrewnych tej grupy.
802.4	Token Bus	802.4a, LAN — szerokopasmowa szyna Fiber Optic Token Bus.
802.5	Token Ring	802.5a, dodatek do zalecenia 802.5 (zarządzanie stacją w sieciach LAN); 802.5n, skrętka nieekranowana dla prędkości 4/16 Mbit/s; 802.5q, sieci LAN — część 5.: przegląd MAC; 802.5, LAN: regulacje związane z siecią Token Ring.
802.6	Magistrala światłowodowa DQDB	802.6bm, rozszerzenie standardu 802.6 MAN; 802.6e, DQDB MAN; 802.6g, zarządzanie warstwą 802.6 MAN; 802.6i, zdalne mostowanie LAN z wykorzystaniem 802.6 MAN; 802.6l, interfejs punkt-punkt dla sieci MAN; 802.6m, podsieć w MAN.
802.7	Szerokopasmowa sieć LAN	
802.8	Sieci światłowodowe LAN/MAN	
802.9	Usługi zintegrowane	802.9a, suplement do zintegrowanych usług LAN; 802.9 zgodny z CSMA/CD MAC; 802.9b, wsparcie dla specyfikacji funkcjonalnych AU — współpraca z AU 802.9; 802.9c, dodatek do 802.9: zarządzanie zgodnością obiektów; 802.9d, dodatek do 802.9: deklaracja zgodności implementacji protokołów; 802.9e, ATM CBM; 802.9f, ISTE.

<sup>3</sup> Dla krótkich sesji — *przyj. tłum.*

**Tabela 12.1.** Rodzaje standardów rodziny IEEE 802 — ciąg dalszy

Standard	Przeznaczenie	Standardy pokrewne
802.10	Bezpieczeństwo sieci LAN/MAN	802.10, standard SILS; 802.10a, model SILS; 802.10c, SILS — zarządzanie kluczami; 802.10d, SILS — zarządzanie zabezpieczeniami; 802.10g, standard bezpieczeństwa wymiany danych; 802.10h, dodatek do zabezpieczeń LM: PICS.
802.11	Sieci bezprzewodowe LAN	802.11a, 5 GHz, 54 Mbit/s; 802.11b, 2,4 GHz, 11 Mbit/s; 802.11c, procedury mostowania; 802.11d, rozszerzenia roamingu międzynarodowego; 802.11e, rozszerzenia parametrów jakości QoS; 802.11g, 2,4 GHz, 54 Mbit/s; 802.11h, zarządzanie widmem 802.11a (Europa); 802.11i, rozszerzenie bezpieczeństwa; 802.11j, rozszerzenia dla Japonii; 802.11k, rozszerzenia standardu zarządzania radiem; 802.11m — obsługa standardu; 802.11n — wyższa przepustowość z wykorzystaniem anten MIMO, 5 GHz lub 2,4 GHz, 600 Mbit/s (poprzez kanały 4×40 MHz); 802.11p, WAVE — bezprzewodowy dostęp do obiektów ruchomych (pojazdy, karetki pogotowia); 802.11r, szybki roaming (w przygotowaniu); 802.11s, sieci kratowe (Mesh), zestaw usług rozszerzonych ESS (w przygotowaniu); 802.11T, predykcja WPP — metody i metryki testowe; 802.11u, współpraca z innymi sieciami (na przykład komórkowymi; w trakcie projektowania); 802.11v, zarządzanie siecią bezprzewodową (w trakcie projektowania); 802.11w, bezpieczne zarządzanie ramkami (w trakcie projektowania); 802.11y, wprowadzenie pasma 3650 – 3700 MHz w USA; 802.11z, rozszerzenia dla DLS (w przygotowaniu); 802.11aa, bezawaryjna transmisja strumieniami audio-wideo (w przygotowaniu).
802.12	Sieci LAN dużej prędkości	802.12a, praca w prędkościach wyższych niż 100 Mbit/s; 802.12b, specyfikacje interfejsu zależnego od nośnika 2-TP PMD; 802.12c, 100 Mbit/s w trybie pełnego duplexu 802.12d, 100 Mbit/s, z uwzględnieniem łącza redundantnego.
802.13	Standard nieużywany	Standard pokrewny o numerze 13 nie istnieje z tego samego powodu, z którego nie buduje się piętra 13. w budynkach (triskaifobia).
802.14	Sieci oparte na telewizji kablowej	
802.15	Bezprzewodowe sieci osobiste WPAN (tzw. minisieci)	802.15.1, Bluetooth; 802.15.2, zasady współdziałania sieci WPAN i Wireless LAN; 802.15.3, sieci WPAN dużych prędkości.
802.16	Sieci szerokopasmowe (WiMAX2, WirelessMAN)	Połączenia pierwszej i ostatniej mili; 802.16e, zapewnienie mobilności dostępu; 802.16f, definicja bazy MIB ( <i>Management Information Base</i> — baza danych informacji zarządzania, wykorzystywana do zarządzania sprzętem w sieci; 802.16g, procedury i usługi zarządzania obszarem; 802.16h, zaktualizowana procedura zwalniania licencji (w trakcie tworzenia); 802.16i, definicja MIB dla urządzeń mobilnych (w trakcie tworzenia); 802.16j, specyfikacja Multihop (w trakcie tworzenia); 802.16k, mostowanie; 802.16m, zaawansowany interfejs radiowy (propozycja).

**Tabela 12.1.** Rodzaje standardów rodziny IEEE 802 — ciąg dalszy

Standard	Przeznaczenie	Standardy pokrewne
802.17	Protokół RPR	Wykorzystywany w sieciach dużej prędkości SONET; 802.17b, Opis warstwy SAS.
802.18	Regulacje związane z dostępem radiowym	
802.19	Koegzystencja	
802.20	Szerokopasmowy, mobilny dostęp do sieci	Standard przeznaczony dla sieci LAN I MAN, standard interfejsu radiowego zapewniającego wsparcie szerokopasmowego, mobilnego dostępu, specyfikacja warstwy fizycznej i MAC.
802.21	Zapewnienie ciągłości transmisji niezależnie od wykorzystanego medium	Zapewnia wymianę informacji pomiędzy sieciami komórkowymi GSM, GPRS, Wi-Fi, Bluetooth, 802.11 i 802.16 dzięki odpowiednim mechanizmom przełączania niezależnie od medium MIH. Protokół MIH jest podobny do protokołu Unlicensed Mobile Access (UMA), który zapewnia przełączanie pomiędzy GSM, UMTS, Bluetooth i sieciami 802.11.
802.22	Regionalne sieci bezprzewodowe WRAN	W sieciach WRAN stosuje się niewykorzystywane fragmenty pasma używanego w telekomunikacji rozsiwczej (telewizja). Jest to stosunkowo nowy standard, zawierający propozycję technologii takiej sieci.

<sup>1)</sup> Standardy, które uległy połączeniu lub wykluczeniu, nie zostały wymienione. 2) WiMAX oznacza standard szerokopasmowego, radiowego dostępu do danych. W Korei Południowej jest określany mianem WiBro.

## Kanały rozgłoszeniowe

Jednym z największych problemów sieci lokalnych, który trzeba było rozwiązać w trakcie opracowywania standardu, jest przekazywanie informacji w trybie rozgłoszeniowym (ang. *broadcasting*). Połączenia typu punkt-punkt tworzą ogromną liczbę możliwych dróg transmisji informacji, która rośnie wykładniczo do liczby punktów w sieci. Aby zapewnić możliwość przekazywania informacji w trybie rozgłoszeniowym, można zastosować przełączniki, podobnie jak w wirtualnych połączeniach (punkt-punkt) w sieci WAN, ale umieszczanie w sieci lokalnej dużej liczby przełączników jest niepraktyczne.

W rozdziale 5. przedstawiono koncepcję kanału. Kanał jest elementem sieci umożliwiającym transmisję informacji w sposób określony w warstwie MAC, należącej do warstwy łącza danych. Można wyróżnić kanały pojedyncze lub wielokrotne, z dostępem dedykowanym, z zapewnieniem wielodostępu bądź dostępu losowego. W sieciach, które używają kanałów wirtualnych, takich jak sieci telekomunikacyjne, sieci oparte na FDM (ang. *Frequency Division Multiplexing* — wielodostęp częstotliwościowy), pasmo transmisji jest dzielone na podpasma przydzielane poszczególnym użytkownikom<sup>4</sup>. Do realizacji usług głosowych wykorzystuje się powszechnie kanały E0, umożliwiające transmisję z prędkością 64 Kbit/s.

<sup>4</sup> FDM polega na podziale dostępnego pasma na podpasma o określonej szerokości, zwane kanałami. Poszczególne kanały są wykorzystywane do zapewnienia transmisji pomiędzy dwoma dowolnymi urządzeniami systemu — *przyj. tłum.*

FDM jest dobrą techniką zapewniania wielodostępu do tych sieci, w których natężenie ruchu jest dostatecznie przewidywalne. Tu zakładamy, że z sieci zawsze korzysta zaledwie kilku użytkowników jednocześnie, a dane mogą być bez problemu buforowane w pamięci podręcznej urządzeń sieciowych. W przypadku środowiska, w którym liczba użytkowników może się bardzo dynamicznie zmieniać w czasie, chwilowe obciążenie staje się nieprzewidywalne. Wówczas mamy do czynienia z przesyłaniem wielu porcji informacji o różnym rozmiarze, a natężenie ruchu w sieci ma charakter impulsowy. W takim środowisku technologia oparta na FDM jest nieskuteczna. Innym rozwiązaniem jest zapewnienie czasowego wielodostępu do łącza (*Time Division Multiplexing* — TDM). W tej metodzie dostęp do kanału jest przydzielany za pomocą szczelin czasowych; mamy w niej również do czynienia z tymi samymi problemami co w FDM. Z tego powodu nowoczesne technologie LAN działają na bazie modelu rozgłoszeniowego (ang. *broadcast*). Poszczególne fragmenty informacji są transmitowane do sieci tak długo, aż zostanie potwierdzony ich odbiór przez węzeł przeznaczenia.

W komunikacji rozgłoszeniowej kanałem nazywamy ścieżkę, dzięki której możemy za pośrednictwem medium fizycznego przesłać dane. Ścieżkę transmisji można fizycznie wytyczyć na wiele sposobów, co nazywamy „metodą wielościeżkową” (ang. *multipath*). Dostęp do kanału może być przydzielony w następujący sposób:

- ♦ **Dostęp sekwencyjny do kanału.** W tej metodzie mamy do czynienia z jednym kanałem współdzielonym przez wiele stacji. W danym momencie tylko jedna stacja ma przydzieloną szczelinę czasową, w której ma pełny dostęp do kanału, a kolejność przydzielania szczeliny dla poszczególnych stacji jest ściśle określona. W tym modelu nie ma rywalizacji o dostęp do kanału, a także nie jest nadawany priorytet przesyłanych danych.

Technologie dostępu z wykorzystaniem pojedynczego kanału nie są skuteczne w realizacji połączeń w pełnym duplexie, ale są wystarczające do zapewnienia półdupleksowej transmisji danych. Ponieważ w tym przypadku nie ma dodatkowego, bezpośredniego kanału do transmisji wiadomości pomiędzy punktami końcowymi, metody te nie są efektywne.

- ♦ **Dostęp do kanału z wykorzystaniem tokenu.** W tej metodzie pomiędzy stacjami przekazywany jest token, który działa na zasadzie zezwolenia na transmisję danych. Po wysłaniu danych stacja przekazuje token kolejnej, umożliwiając w ten sposób transmisję danych następnej jednostce. Sieci oparte na tej metodzie umożliwiają transmisję danych o dużych rozmiarach, ale działają wolniej niż w przypadku zastosowania pozostałych metod rozgłoszeniowych.
- ♦ **Dostęp do kanału z detekcją kolizji.** W tej metodzie wszystkie stacje transmitują dane w tym samym czasie — nie korzystamy tu np. ze szczelin czasowych. Jeśli do jednej stacji jednocześnie przybędą dwa pakiety danych, powstanie kolizja. Kolizja uruchomi mechanizm wykrywania i usuwania skutków kolizji, który wymusi retransmisję pakietów.
- ♦ **Badanie stanu kanału.** Stacje znajdujące się w sieci dokonują transmisji danych jedynie wtedy, gdy nośnik jest wolny. W ten sposób zmniejsza się ryzyko wystąpienia kolizji, ale nie eliminuje się go w całości. Ta metoda jest skuteczniejsza niż dostęp z kolizją.

- ♦ **Technika oparta na wielokanałowym systemie rozgłoszeniowym.** Transmisja wielokanałowa oferuje największą przepustowość i jest efektywniejsza od technik z wykorzystaniem pełnego duplexu. W sieciach wielokanałowych jeden z kanałów służy do transmisji danych, a dodatkowy kanał może być zastosowany do transmisji wiadomości sygnalizacyjnych (sterujących), co zwiększa efektywność całego systemu. Sieci wielokanałowe wymagają zapewnienia buforowania danych i dodatkowego systemu koordynacji. W tej technice jest możliwość użycia kanałów dedykowanych.

## Ethernet

Ethernet jest obecnie dominującą technologią przewodową sieci LAN. Standard definiuje ramki transmitowane przez media warstwy fizycznej i sygnalizację warstwy łącza danych w oparciu o wielodostęp do łącza sieci z badaniem stanu kanału i unikaniem kolizji (ang. *Carrier Sense Multiple Access z Collision Detection* — CSMA/CD). Ethernet jest zdefiniowany przez standard IEEE 802.3. Węzły w sieci Ethernet są identyfikowane przez unikalne, 48-bitowe adresy MAC. Istnieją dwa rodzaje węzłów sieci w sieci Ethernet:

- ♦ **Urządzenia końcowe DTE (ang. *Data terminal Equipment* — DTE).** Ta kategoria obejmuje wszystkie elementy źródłowe lub docelowe dla ramki Ethernet. Komputery, serwery, drukarki i inne urządzenia tego rodzaju są czasem nazywane *stacjami końcowymi*.
- ♦ **Urządzenia komunikacyjne DCE (ang. *Data Communications Equipment* — DCE).** Urządzenie sieciowe, które otrzymuje i przekazuje ramki Ethernet i jednocześnie nie jest urządzeniem źródłowym lub docelowym, jest DCE. Ta kategoria obejmuje switchy, routery, mosty, stacje oraz wszelkie interfejsy sieciowe, takie jak karty sieciowe lub modemy.



Pakiet transmitowany za pomocą przewodu transmisyjnego nazywany jest ramką.

Ethernet został opracowany przez grupę Xerox PARC w 1970 roku, gdy Robert Metcalfe, David Boggs, Chuck Thacker i Butler Lampson utworzyli protokół CSMA/CD. Nazwa „Ethernet” pochodzi od słowa *ether*, oznaczającego czyste powietrze lub niebo. W trakcie rozwoju nauki eterem nazywano różne środki transportu dla pola elektromagnetycznego, światła, grawitacji; termin ten był również używany w kontekście zaniku substancji w wyniku wczesnych doświadczeń chemicznych i wielu innych niewyjaśnionych zjawisk.



W rozdziale 8. opisano różne standardy okablowania wykorzystywane w sieciach Ethernet.

Prototyp sieci Ethernet działał z prędkością 3 Mbit/s i został zaprojektowany w celu zapewnienia wysokiej wydajności nawet w sytuacji dużego obciążenia sieci. W 1980 roku grupa złożona z firm Digital Equipment Corporation, Intel i Xerox opracowała pierwszą wersję omawianego standardu, o nazwie Ethernet 1.0 (nazywanego również standardem DIX), który umożliwiał transmisję z prędkością 10 Mbit/s. Standard 802.3 sieci Ethernet został utworzony w oparciu o wspomnianą wersję Ethernet 1.0.

We wczesniej wersji standardu Ethernet o nazwie StarLAN do okablowania wykorzystano nieekranowaną skrętkę UTP. StarLAN stanowił podstawę standardu szybkiej sieci LAN, którą ostatecznie zdefiniowano jako 1BASE5 Ethernet. W roku 1980 StarLAN był standardem wyjątkowym, ponieważ umożliwiał używanie standardowego złącza telefonicznego RJ-45, powszechnie używanego w telekomunikacyjnych instalacjach w budynkach. Standard 10BASE-T stanowi adaptację StarLAN, gdzie zastosowano jego modulację, mechanizm wykrywania połączenia i zachowano schemat okablowania.



Standard 10BASE-T przedstawiono w rozdziale 8.

Nazwa 10Base-T powstała od prędkości sieci (10 Mbit/s), metody sygnalizacji oraz medium fizycznego rozwiązania, którym jest skrętka. Dla standardu 100Base-T4 prędkość transmisji wynosi 100 Mbit/s, a medium fizycznym są cztery skrętki. Standard 1000Base-LX Ethernet odnosi się do sieci, w których sygnał transmitowany jest przez kabel światłowodowy. W nazwach wariantów standardu sieci Ethernet znajduje się najczęściej słowo *Base*, będące skrótem od terminu *baseband* (pasmo podstawowe), który jest związany ze sposobem sygnalizacji, opisanym w rozdziale 5. Dzisiaj dane sieci Ethernet są przesyłane przez łącza szerokopasmowe, z wykorzystaniem wielu ścieżek transmisji danych, zdefiniowanych przez częstotliwość lub amplitudę sygnału, niezależnie od prędkości łącza sygnalizacji. Rzadko używa się terminu 100Broad<sup>5</sup> w przypadku połączeń dużych prędkości. Pozostałe metody sygnalizacji sieci szerokopasmowych i wąskopasmowych nie są stosowane w sieciach Ethernet.

W tabeli 12.2 zebrano różne warianty normy 802.3, opisującej standard Ethernet. Norma 802.3 definiuje najważniejsze rodzaje przewodowej sieci Ethernet, które są najczęściej wykorzystywane w nowoczesnych sieciach lokalnych. Liczby w nawiasach oznaczają teoretyczną przepustowość danego standardu.

**Tabela 12.2.** Standardy sieci Ethernet (norma 802.3)

Standard	Data	Przeznaczenie
Experimental Ethernet	1972	2,94 Mbit/s (367 KB/s) z wykorzystaniem kabla koncentrycznego.
Ethernet II (DIXv2.0)	1982	10 Mbit/s (1,25 MB/s) z wykorzystaniem cienkiego kabla koncentrycznego (ang. <i>Thinnnet</i> ); w ramach znalazło się pole <i>Type</i> (typ). Ten format ramki jest obecnie używany we wszystkich rodzajach sieci Ethernet i zestawie protokołów internetowych.
IEEE 802.3	1983	10Base5 10 Mbit/s (1,25 MB/s) z wykorzystaniem grubego kabla koncentrycznego (ang. <i>Thicknet</i> ). Standard podobny do DIX, z wyjątkiem pola <i>Type</i> , które zostało zamienione na pole <i>Length</i> (długość), nagłówek 802.2 LLC występuje po nagłówku 802.3.
802.3a	1985	10BASE2 10 Mbit/s (1.25 MB/s) z wykorzystaniem cienkiego, współosiowego kabla koncentrycznego (ang. <i>Thinnnet</i> lub <i>cheapernet</i> ).
802.3b	1985	10BROAD36, standard nieużywany.
802.3c	1985	Specyfikacja koncentratora 10Mbit/s (1.25 MB/s).

<sup>5</sup> Autor odwołuje się tu do nazwy 100Broad, gdzie *Broad* oznacza transmisję szerokopasmową (ang. *broadband* — szerokopasmowy) — przyp. tłum.

**Tabela 12.2.** *Standardy sieci Ethernet (norma 802.3) — ciąg dalszy*

Standard	Data	Przeznaczenie
802.3d	1987	Łączy światłowodowe FOIRL (ang. <i>Fiber Optic Inter Repeater Link</i> — połączenie światłowodowe pomiędzy dwoma wtórnymi).
802.3e	1987	1BASE5 lub StarLAN.
802.3i	1990	10BASE-T 10 Mbit/s (1.25 MB/s) z wykorzystaniem skrętki.
802.3j	1993	10BASE-F 10 Mbit/s (1.25 MB/s) z wykorzystaniem o światłowodu.
802.3u	1995	100BASE-TX, 100BASE-T4, 100BASE-FX — Fast Ethernet o prędkości 100 Mbits/s (12.5MB/s) z autonegociacją.
802.3x	1997	Pełny duplex, zawiera również ramkowanie DIX i usuwa podział na DIX/802.3.
802.3y	1998	100BASE-T2 100 Mbits/s (12.5 MB/s) z wykorzystaniem skrętki niskiej jakości.
802.3z	1998	1000BASE-X Gbit/s — Ethernet z wykorzystaniem światłowodu; prędkość 1 Gbit/s (125 MB/s).
802.3ab	1999	1000BASE-T Gbit/s — Ethernet z wykorzystaniem skrętki.
802.3ac	1998	Maksymalny rozmiar ramki przedłużony do 1522 bajtów o znacznik Q-tag. Q-tag zawiera informacje związane z siecią wirtualną, oznaczony jako 802.1Q VLAN oraz priorytet ramki Ethernet 802.1p.
802.3ad	2000	Agregacja łączy równoległych.
802.3ae	2003	10 Gbit/s (1250 MB/s) — Ethernet z wykorzystaniem światłowodu; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW.
802.3af	2003	Zasilanie urządzeń sieciowych przez okablowanie Ethernet.
802.3ah	2004	Ethernet pierwszej mili.
802.3ak	2004	10GBASE-CX4 10 Gbit/s (1250 Mbit/s) — Ethernet z wykorzystaniem kabla koncentrycznego; cztery pary, 8 przewodów.
802.3an	2006	10GBASE-T 10 Gbit/s (1250 MB/s) — Ethernet z wykorzystaniem nieekranowanej skrętki (UTP).
802.3ap	2007	Magistrala danych Ethernet (1 i 10 Gbit/s (125 i 1250 MB/s) na płytkach drukowanych urządzeń sieciowych).
802.3aq	2006	10GBASE-LRM 10 Gbit/s (1250 MB/s) — Ethernet z wykorzystaniem światłowodu wielomodowego.
802.3as	2006	Rozszerzenie ramki.
802.3at	2008	Zasilanie urządzeń sieciowych przez okablowanie Ethernet — rozszerzenia standardu.
802.3av	2009	10 Gbit/s EPON ( <i>Ethernet Passive Optical Network</i> — pasywna sieć optyczna Ethernet).
802.3az	2007	Poprawa efektywności wykorzystania energii w sieci Ethernet.
802.3ba	2009	Grupa standardów sieci Ethernet dużych prędkości. Pierwszą grupą stanowią połączenia o maksymalnej prędkości 40 Gbit/s: z wykorzystaniem czteroprzewodowego kabla o długości maksymalnej 1 m; dzięki zastosowaniu kabla TWINAX można osiągnąć prędkość 100 Gbit/s (łączy 4×25 Gbit lub 10×10 Gbit) na maksymalnej długości 10 m. Łącze o 100 m długości wymaga zastosowania wielomodowych światłowodów, natomiast światłowody jednomodowe umożliwiają przesyłanie danych nawet na 40 km.

W sieciach Ethernet informacja jest kodowana w postaci odpowiedniej sekwencji sygnałów, które w transmisji przez sieć ulegają zniekształceniu. Stacja odbiorcza musi przefiltrować przychodzące dane, dokonać wyrównania dryftu czasu lub zsynchronizować dane do odpowiedniej prędkości zegara w celu pobrania danych z przychodzącego sygnału. Aby zniwelować wpływ zniekształceń powstałych w trakcie transmisji, powstało wiele różnych systemów kodowania. Na początku w sieciach Ethernet wykorzystywano kodowanie Manchester (opisane w dalszej części rozdziału). W gigabitowym Ethernetie użyto systemu korekcji błędów FEC. Na poziomie protokołu Ethernet wykrywane są błędy poszczególnych bitów. Następnie informacja jest przekazywana do stosu protokołów warstw wyższych, gdzie następuje złożona kontrola, umożliwiająca korekcję poważniejszych błędów.

## Ramki protokołu Ethernet

Ramki są porcjami danych, przygotowanymi odpowiednio do transmisji przez sieć. Są one tworzone za pomocą odpowiedniego programu w warstwie łącza danych. Program dokonuje podziału większych porcji danych na pakiety odpowiednich rozmiarów bądź generuje bity wypełnienia, gdy rozmiar przesyłanej informacji jest mniejszy od rozmiaru pola danych pojedynczej ramki. Blok danych jest „opakowany” dopełniającymi bitami, które stanowią dodatkowe informacje dotyczące transmitowanych danych, miejsca źródłowego i docelowego, a także służą między innymi do kontroli i korekcji błędów. Ramki Ethernet są pierwowzorem wykorzystywania ramek w różnych sieciach. Ramki są stosowane nie tylko w sieciach pakietowych, takich jak TCP/IP, internet, ale właśnie te sieci stanowią prawdopodobnie najbardziej znany przykład użycia ramek.

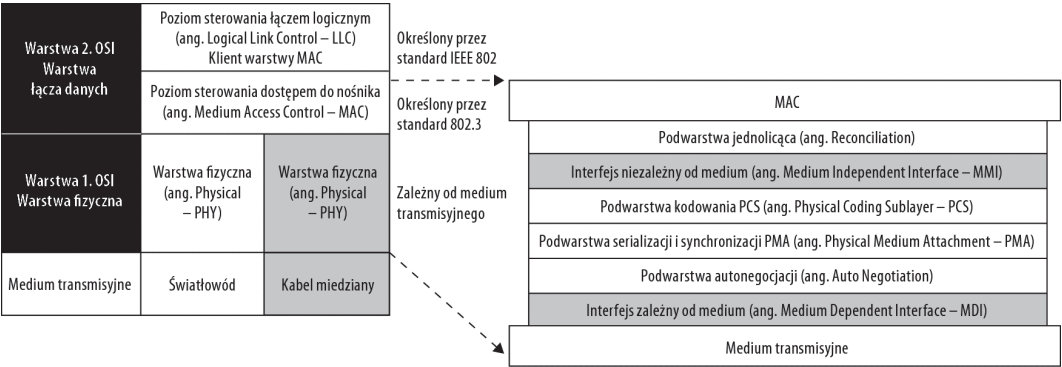
Wykorzystanie ramek pomaga w realizacji transmisji danych w sieci, ponieważ zapewniają one kontekst, dzięki któremu strona odbiorcza jest w stanie poprawnie zinterpretować przychodzące dane. Z punktu widzenia każdego systemu odbierającego dane w sieci sygnały są przekazywane prawie cały czas, w zależności od aktualnego wykorzystania sieci. Gdy tylko pojawi się sekwencja początkowa, następuje synchronizacja, dzięki której wiadomo, kiedy pojawi się pierwszy bit i jaką długość ma ramka. Niemal każda ramka stosowana w transmisji danych posiada następujące cechy:

- ♦ Ramka ma określony cel — niektóre służą do przesyłania danych, inne do wydawania poleceń albo do przekazywania innych informacji.
- ♦ Ramka posiada sekwencję oznaczającą początek i koniec. W niektórych ramkach stosuje się dodatkowo pola separatorów.
- ♦ Ramki na ogół zawierają pole przechowujące liczbę znaków, które określa wielkość ramki i jest częścią mechanizmu kontroli błędów. Niektóre ramki są zdefiniowane jako elementy o stałej długości i nie wymagają pola z informacją o liczbie znaków.
- ♦ Pola danych mają stałą lub zmienną długość. W zależności od typu w ramce znajduje się pole z danymi bądź go nie ma. W systemach używających stałej długości ramki niewykorzystane pola trzeba uzupełnić *bitami dopełniającymi* (najczęściej zerami).
- ♦ Mechanizm kontroli błędów jest używany do sprawdzenia poprawności przesyłanych danych.

Kontrola błędów jest niezwykle ważnym aspektem związanym z transmisją ramki, gdyż jest to jedyny sposób, aby upewnić się, że do miejsca docelowego dotrze poprawna ramka. Wprawdzie dane przesyła się z zachowaniem określonego odstępu czasu pomiędzy poszczególnymi ramkami, ale to nie jest wystarczający środek zapewniający poprawność transmisji. Jeśli do stacji docelowej dotrą dwie ramki mniej więcej w tym samym czasie, dojdzie do wystąpienia kolizji. Wówczas może okazać się, że obydwie ramki zostaną zinterpretowane w stacji docelowej jako ta sama ramka. W ten sposób do momentu kontroli danych wystąpi błąd. Czasami zdarza się, że pomimo wykorzystania mechanizmów kontroli błędów niektóre z nich przenikają do systemu docelowego. Te dodatkowe błędy (dotyczące zazwyczaj przesyłanych danych) są przekazywane do protokołów warstw wyższych w celu zdiagnozowania i korekcji.

Znana jest ośmiobitowa reprezentacja znaków, utworzona np. w oparciu o tabele ASCII. Tak zwany oktet jest jedną z wielu możliwości reprezentacji znaków. Zestawy zawierające więcej znaków, których dobrym przykładem jest Unicode, korzystają z szerszej reprezentacji. W praktyce liczba bitów stosowana do reprezentacji znaków nie ma żadnego znaczenia — nie musi to być 8 bitów lub multiplikacja tej liczby. Z punktu widzenia standardów sieciowych istnieje potrzeba pewnej elastyczności, jeśli chodzi o długość ramki (liczbę bitów). Z tego powodu ramka danych jest ograniczona do określonej długości, do której dostosowywane są przesyłane dane.

Rysunek 12.1 przedstawia fragment modelu OSI, gdzie przyporządkowano różne protokoły sieciowe Ethernet. Standard Ethernet definiuje odpowiednie protokoły na poziomie warstwy fizycznej (warstwa 1. modelu OSI) i warstwie łącza danych (warstwa 2. modelu OSI). W zależności od rodzaju medium transmisyjnego (kabel miedziany lub światłowód) odpowiednie protokoły są zaimplementowane w warstwie fizycznej. Ze względu na to, że w obydwu przypadkach korzystamy z tego samego systemu adresacji MAC, warstwa MAC jest wspólna dla obydwu mediów, przy czym dla każdego z nich utworzono odpowiednie podwarstwy łączące MAC z medium transmisyjnym.



**Rysunek 12.1.** Warstwy stosu Ethernet i ich odniesienie do modelu OSI

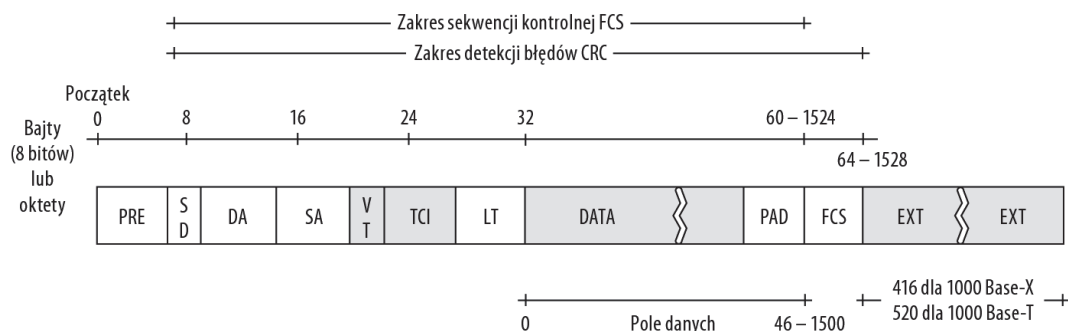
Warstwa MAC (ang. *Medium Access Control* — sterowanie dostępem do nośnika) odpowiada za zbudowanie ramek zawierających dane i sterowanie dostępem do nośnika. Odpowiada ona za kontrolę sekwencji i integralności ramek oraz wykrywania błędów, zarówno w trakcie odbierania danych, jak i po weryfikacji. MAC decyduje o rozpoczęciu transmisji ramki i zapewnia odpowiednie środki do retransmisji w przypadku wystąpienia błędów.

Warstwa LLC (ang. *Logical Link Control* — sterowanie łączem logicznym), którą widać na rysunku 12.1, jest klientem warstwy MAC. Ta warstwa jest wykorzystywana wtedy, gdy elementem odbiorczym jest urządzenie końcowe DTE. Powyżej klienta MAC znajdują się protokoły warstw wyższych, takie jak TCP/IP. Jeśli klientem danej warstwy MAC jest element mostowania lub urządzenie komunikacyjne DCE, powyżej LLC nie znajdziemy protokołów warstw wyższych i będziemy mieli do czynienia z połączeniem Ethernet-to-Ethernet.

## Struktura ramki

Ramki standardu Ethernet mogą zawierać 11 pól. W obrębie ramki dane są przesyłane szeregowo bez dodatkowych odstępów. Rysunek 12.2 przedstawia strukturę ramki Ethernet 802.3, zawierającej 11 pól:

- ♦ **Preambula PRE.** To pole składa się z sekwencji 7 bajtów 10101010, które sygnalizują urządzeniom odbiorczym początek ramki. Wzorec złożony z naprzemiennie ustawionych zer i jedynek ułatwia synchronizację interfejsu zależnego od medium (MDI) warstwy fizycznej.
- ♦ **Ogranicznik początku ramki SFD.** Ten ogranicznik jest jednobajtowym znacznikiem o wartości 10101011. Ostatnia jedyńska oznacza, że tuż za nią znajduje się właściwa zawartość ramki.
- ♦ **Adres odbiorcy DA.** Jest to sześciobajtowe pole, które wskazuje adres urządzenia docelowego lub adresy urządzeń docelowych (w przypadku transmisji multicast) ramki. Pierwszy bit to 0, gdy mamy do czynienia z adresem jednego urządzenia, lub 1, gdy ramka jest skierowana do grupy urządzeń. Ostatnim bitem jest 0, gdy mamy do czynienia z adresem globalnym, lub 1, gdy jest to adres lokalny. Pozostałe 46 bitów stanowi unikalny adres MAC przeznaczenia ramki — urządzenia końcowego (transmisja unicast), grupy urządzeń (transmisja multicast) lub wszystkich urządzeń w sieci (transmisja broadcast).
- ♦ **Adres nadawcy SA.** Jest to sześciobajtowe pole przechowujące adres urządzenia źródłowego. Pierwszy bit jest zawsze zerem, a kolejne 46 bitów reprezentuje adres.
- ♦ **Identyfikator sieci wirtualnej VT.** Jest to dwubajtowe pole opcjonalne, wykorzystywane do oznaczenia ramki transmitowanej w sieci wirtualnej. Aby można było obsługiwać sieci VLAN, wszystkie urządzenia końcowe muszą wspierać standard sieci wirtualnych.
- ♦ **Znacznik kontrolny TCI.** Jest to czterobitowe pole opcjonalne dla sieci VLAN, które zawiera informacje o priorytecie ramki i identyfikatorze grupy roboczej VLAN, do której ramka jest adresowana.
- ♦ **Pole długości lub typu LT.** To jest 2-bajtowe pole, które wskazuje na rozmiar pola danych wyrażony w bajtach (wartości od 46 do 1536) lub rodzaj ramki (wartości większe niż 1536).
- ♦ **Pole danych.** W tym polu znajdują się przesyłane dane. Pole ma rozmiar od 46 do 1500 bajtów. Jeśli mamy do czynienia z danymi o rozmiarze mniejszym od minimalnego rozmiaru, pozostała część pola będzie wypełniona zerami, aby otrzymać 46 bajtów.

**Legenda:**

DATA – pole danych  
 EXT – pole rozszerzenia  
 FCS – pole sumy kontrolnej ramki  
 LT – pole długości/typu  
 PAD – pole wypełnienia  
 PRE – preambuła  
 SA – adres źródłowy  
 SD – ogranicznik początku ramki  
 TCI – znacznik kontrolny (pole opcjonalne dla sieci wirtualnych VLAN)  
 VT – identyfikator sieci wirtualnej (pole opcjonalne dla sieci wirtualnych VLAN)

**Rysunek 12.2.** Struktura ramki Ethernet 802.3

- ♦ **Pole dodatkowego wypełnienia PAD.** To pole stanowią bity wypełnienia, gdy przekazywana informacja jest mniejsza od najmniejszego rozmiaru pola danych.
- ♦ **Pole sekwencji kontrolnej ramki FCS.** Jest to 4-bajtowe pole, posiadające 32-bitowy znacznik sumy kontrolnej CRC, używany do detekcji błędów. Na rysunku 12.2 przedstawiono zakres bitów wykorzystywanych do generowania sumy kontrolnej, oznaczony paskiem „Zakres sekwencji kontrolnej FCS”. Pola objęte zakresem tego paska są używane do generowania wartości CRC, która jest następnie umieszczona w polu FCS. Do wykrywania błędów są wykorzystywane bity oznaczone paskiem „Zakres sekwencji kontrolnej FCS” wraz z polem FCS, co oznaczono paskiem „Zakres detekcji błędów CRC”.
- ♦ **Pole rozszerzenia EXT.** Pole rozszerzenia ma rozmiar 12 bajtów, jest wykorzystywane w celu ułatwienia wysyłania ramek Ethernet przez sieci bardzo dużych prędkości — Gigabit Ethernet. Pole ma do 416 bajtów dla standardu 1000Base-X i 520 bajtów dla standardu 1000Base-T.

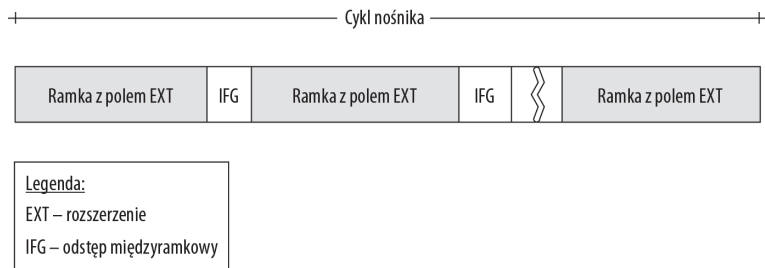
Format ramki może być różny w zależności od rodzaju standardu Ethernet. Obecnie dąży się do wykorzystywania ogólnego formatu przedstawionego na rysunku 12.2. Spośród różnych wersji ramek Ethernet warto wspomnieć o ramkach Novell Raw 802.3 (tak zwana surowa ramka, bez nagłówka LLC), IEEE 802.2 LLC, 802.2 LLC/SNAP oraz Ethernet wersji II. Aby zapewnić wsparcie różnych wersji ramek Ethernet, wprowadzono pole określające długość lub typ LT. Umieszczono je w nagłówku MAC, tuż za polem adresu źródłowego. Dzięki LT można jednocześnie używać różnych wersji standardu Ethernet w danej sieci.

## Tryb wiązkowy

Wraz z pojawieniem się standardu Gigabit Ethernet wprowadzono do transmisji CSMA/CD tryb wiązkowy. W tym trybie dane są wysyłane w postaci wiązek o rozmiarze do 8192 bajtów (65,536 bitów). Wiązka zawiera wiele ramek oddzielonych odstępami międzyramkowymi (ang. *Interframe Gap* — IFG). Dzięki wykorzystaniu wiązek stacja nadawcza może dłużej kontrolować sieć, wskutek czego przepustowość niewielkich ramek zwiększa się do trzech razy w porównaniu z Gigabit Ethernet bez wykorzystania wspomnianego trybu. Tryb wiązkowy jest dostępny wyłącznie dla sieci dużych prędkości. Wolniejsze wersje sieci Ethernet nie obsługują pola rozszerzenia EXT, dzięki któremu można utrzymać kontrolę transmisji poprzez wstrzymanie innych stacji nadawczych. Rysunek 12.3 przedstawia ramkę sieci Gigabit Ethernet ze wskazaniem cyklu nośnika.

### Rysunek 12.3.

Tryb wiązkowy  
w sieciach Gigabit  
Ethernet



## Ramki sieci wirtualnych VLAN

Sieć wirtualna to grupa węzłów tworzących logicznie jedną grupę (domenę), niezależną od fizycznego rozmieszczenia elementów sieci. Dane przesyłane z węzła jednej sieci do węzła znajdującego się fizycznie w innej sieci są traktowane tak, jakby obydwa węzły znajdowały się w tej samej sieci. Ruchem w sieci wirtualnej VLAN można zarządzać z poziomu pojedynczej konsoli. Odpowiednikiem sieci wirtualnych VLAN, definiowanych w warstwie drugiej, są podsieci IP definiowane w warstwie trzeciej.



Rozdział 16. zawiera informacje o produktach wspierających sieci wirtualne VLAN.

W celu wsparcia funkcji VLAN dwa pola są wstawiane do ramki Ethernet tuż przed LT. Pierwsze to 2-bajtowe pole VLAN ID, oznaczające VLAN, a drugie to 2-bajtowe pole TCI, które zawiera priorytet od 0 do 7 (najwyższy) i identyfikator sieci VLAN ID (będący identyfikatorem grupy). Aby móc korzystać z VLAN, trzeba upewnić się, że we wszystkich węzłach opcja VLAN jest zainstalowana i obsługiwana.

## Protokół CSMA/CD

CSMA/CD umożliwia dostęp do łącza w trybie półdupleksowym (transmisja jednokierunkowa). Protokół umożliwia przesyłanie danych z wielu węzłów sieci jednocześnie (zapewnia wielodostęp). CSMA/CD miał być alternatywą dla sieci realizowanych w oparciu o tokeny i umożliwić efektywniejsze wykorzystanie fizycznej przepustowości medium transmisyjnego. Ze względu na to, że w omawianym protokole jest możliwe jednoczesne przesłanie dwóch ramek do węzła docelowego, po stronie odbiorczej może wystąpić błąd spowodowany

nieprawidłową detekcją strumieni danych transmitowanych ramek. Taki błąd nazywamy *kolizją*. Protokół CSMA/CD posiada mechanizm wykrywania kolizji i korekcji błędów związanych z wystąpieniem kolizji.

Akronim protokołu CSMA/CD pochodzi od następujących terminów z języka angielskiego:

- ♦ **Carrier Sense, CS** (*badanie nośnej*). Badanie stanu kanału umożliwia stacjom końcowym określenie początku i końca ramki na podstawie przerw (luk) transmisji.
- ♦ **Multiple Access, MA** (*wielodostęp*). Dzięki mechanizmowi wielodostępu każda stacja znajdująca się w sieci może rozpocząć transmisję, jeśli tylko łącze w danym momencie jest wolne.
- ♦ **Collision Detection, CD** (*wykrywanie kolizji*). W przypadku wystąpienia kolizji mechanizm spowoduje powtórna transmisję błędnie odebranych ramek po czasie wyznaczonym na podstawie odpowiedniego algorytmu pseudolosowego.

Sieć zbudowana w oparciu o standard Ethernet CSMA/CD jest w jednym z następujących stanów:

- ♦ **Transmisja**. W tym stanie dane są przesyłane z węzła źródłowego do węzła docelowego.
- ♦ **Bezczynność**. W tym stanie w sieci nie są transmitowane żadne dane.
- ♦ **Kolizja (konflikt)**. Dane pochodzące z dwóch źródeł są transmitowane jednocześnie.

Zjawisko kolizji w sieciach Ethernet występuje bardzo często: im większe wykorzystanie sieci, tym większy odsetek ramek biorących udział w kolizji. Mimo częstych kolizji sieci Ethernet mogą osiągnąć sprawność wynoszącą ponad 90 procent teoretycznej przepustowości łącza dzięki zastosowaniu protokołu i mechanizmów CSMA/CD.

Dłuższa droga transmisji danych w sieci prowadzi do wystąpienia różnic w czasie detekcji kolizji przez stacje biorące udział w transmisji. Możliwość wystąpienia opóźnień czasowych detekcji kolizji jest powodem ograniczenia fizycznej długości łączy w sieci Ethernet i wyboru poznanej wcześniej długości ramki. W trakcie prac nad standardem trzeba było wziąć pod uwagę zależność minimalnej długości ramki od wybranej maksymalnej długości łącza. Gdy wprowadzono sieci o większej prędkości (100 Mbit/s lub więcej), wpływ wspomnianych opóźnień detekcji kolizji zmniejszył się, zatem trzeba było zmodyfikować ramkę lub maksymalną długość łącza. W sieciach Ethernet pracujących w prędkościach do 100 Mbit/s podjęto decyzję, aby zachować wcześniej ustalony rozmiar ramki i skrócić maksymalną długość łącza<sup>6</sup>. Dla sieci Gigabit Ethernet zachowano długość łącza ustaloną przy standardach 100 Mbit/s, natomiast ramka została rozszerzona o pole EXT, aby zwiększyć jej minimalny rozmiar. Dla standardu 1000Base-X minimalna długość ramki wynosi 416 bajtów, a dla 1000Base-T jest zwiększona do 512 bajtów. W tabeli 12.3 zebrano dane długości połączeń i ramek dla wybranych prędkości sieci Ethernet.

Transmisja ramki Ethernet zgodnie z protokołem CSMA/CD przebiega w następujący sposób:

1. Ramka jest uformowana i przygotowana do transmisji.
2. Urządzenie nadawcze sprawdza dostępność nośnika (medium transmisyjnego).

---

<sup>6</sup> Z 2,5 km do 100 m — *przyp. tłum.*

**Tabela 12.3.** Długości łącza i rozmiary ramek w sieciach Ethernet<sup>1</sup>

Czynnik	10 Mbit/s	100 Mbit/s	1000 Mbit/s
Minimalny rozmiar ramki (w bajtach)	64	64	416 dla 1000Base-X 512 dla 1000Base-T
Maksymalna średnica (w metrach) <sup>2</sup>	100 skrętka	100 skrętka 412 światłowód	100 skrętka 316 światłowód
Maksymalna odległość między regeneratorami w metrach)	2500	205	200
Maksymalna dozwolona liczba regeneratorów w łączu	5	2	1

<sup>1)</sup> Wartości wyznaczone dla transmisji półdupleksowej (jednokierunkowej).

<sup>2)</sup> Największa odległość pomiędzy dowolnymi urządzeniami DTE w domenie

3. Jeśli medium jest wolne, dane zostaną wysłane. Jeśli medium jest zajęte, to transmisja będzie opóźniona o czas ustalony na podstawie konkretnego protokołu. W sieciach Ethernet ten czas jest nazywany odstępem między ramkami IFG lub odstępem między pakietami IPG.
4. Stacja źródłowa sprawdza, czy wystąpiło zjawisko kolizji. Jeśli dane odebrane są takie same jak wcześniej nadane, kolizja nie wystąpiła. W przypadku wystąpienia kolizji system nadawczy przerywa transmisję kolejnych ramek i przystępuje do wykonania procedury naprawczej, opisaney w dalszej części rozdziału. Wykonanie procedury naprawczej w tym kroku jest ważne dlatego, że w ten sposób można uniknąć próby wykorzystania łącza przez inną stację nadawczą.
5. Po otrzymaniu wymaganych potwierdzeń stacji docelowej o poprawnej transmisji/retransmisji stacja źródłowa kończy transmisję i ustawia liczniki CSMA/CD na 0.

Odstęp IFG to minimalny czas bezczynności łącza, który musi upłynąć, zanim urządzenie rozpocznie wysyłanie ramki. Ten czas umożliwia pozostałym urządzeniom w sieci zresetowanie stosów sieciowych i przygotowanie się na otrzymanie nowej ramki. Długość odstępu IFG zależy od wykorzystywanego w sieci protokołu. Najczęściej spotykanymi wartościami są:

- ♦ dla sieci 10 Gigabit Ethernet (10 Gbit/s) — 9,6 ns,
- ♦ dla sieci 1 Gigabit Ethernet (1 Gbit/s) — 96 ns,
- ♦ dla sieci Fast Ethernet (100 Mbit/s) — 960 ns,
- ♦ dla sieci Ethernet (10 Mbit/s) — 9,6 ms.

Podane wartości mogą ulec zmianie. Producenci kart sieciowych korzystają z coraz szybszych układów, dzięki czemu mogą zmniejszyć odstęp IFG w celu poprawy przepustowości łącza. Przykładem takiej karty jest Intel EtherExpress PRO/100B NIC. Regeneratory, czyli urządzenia wzmacniające, przesyłające sygnały w celu realizacji transmisji na większych odległościach, również są projektowane tak, aby jak najbardziej zmniejszyć konieczny odstęp IFG. Gdy ramki z danymi zostaną dostarczone do stacji docelowej, pewne zdarzenia w sieci mogą wpływać na zmniejszenie się parametru IFG: transmisja przez regeneratory,

łączenie pakietów w trakcie transmisji bądź przeciążenie sieci. IFG można zredukować do 40 bitów (5 bajtów) w sieciach 10 Gigabit Ethernet, 64 bitów (8 bajtów) dla sieci Gigabit Ethernet albo 47 bitów w sieci Ethernet o prędkości 10 Mb/s.

Po detekcji kolizji zgodnie z protokołem CSMA/CD mają miejsce następujące zdarzenia:

1. Wysłanie dodatkowych pakietów z informacją o kolizji, przeznaczonych dla innych węzłów.
2. Zwiększenie licznika CSMA/CD.
3. W przypadku transmisji z maksymalnym obciążeniem łącza następuje próba przerwania transmisji.
4. Zatrzymanie na czas określony na podstawie liczby kolizji.
5. Retransmisja pakietu, wspomniana w poprzedniej procedurze.

## **Transmisja w trybie pełnoduplexowym (dwukierunkowym)**

W trakcie opracowywania szybszych wersji sieci Ethernet zaczęto przechodzić z półdupleksowego protokołu CSMA/CD do protokołów zapewniających transmisję w trybie pełnodupleksowym. Dzięki trybowi pełnodupleksowemu dane są przysyłane dwukierunkowo bez ryzyka wystąpienia kolizji. Pozwala to na szybsze przekazywanie mniejszych ramek Ethernet ze względu na wyeliminowanie pola rozszerzenia EXT, a przepustowość sieci wzrasta niemal dwukrotnie. Ramki przysyłane w trybie pełnego duplexu połączeń dwupunktowych (punkt-punkt) są oddzielone odstępami IFG, podobnie jak w transmisji w półduplexie. W tym przypadku ramki są wysyłane natychmiast po przygotowaniu w węźle źródłowym.

Aby praktycznie wykorzystać tryb pełnoduplexowy, należy wprowadzić mechanizm kontroli przepływu w przełącznikach lub routerach w celu uniknięcia przeciążenia sieci. Dodatkowo w transmisji tego typu trzeba zapewnić odpowiednie bufor między ramkami w obydwu kierunkach. Ramka przerwania jest wysyłana od węzła docelowego do źródłowego pierwotnej transmisji w przypadku, gdy liczba utraconych pakietów przekroczy określoną wartość progową. Ramki przerwania są skonstruowane w ten sposób, że nie mogą być przetwarzane przez warstwy wyższe.

Tryb pełnoduplexowej transmisji z kontrolą przepływu można stosować w każdym standardzie sieci Ethernet i przy każdej prędkości. Aby skorzystać z tej metody, należy wyposażać łącze w odpowiednie urządzenia warstwy fizycznej, niezbędne do wspierania trybu pełnodupleksowego.

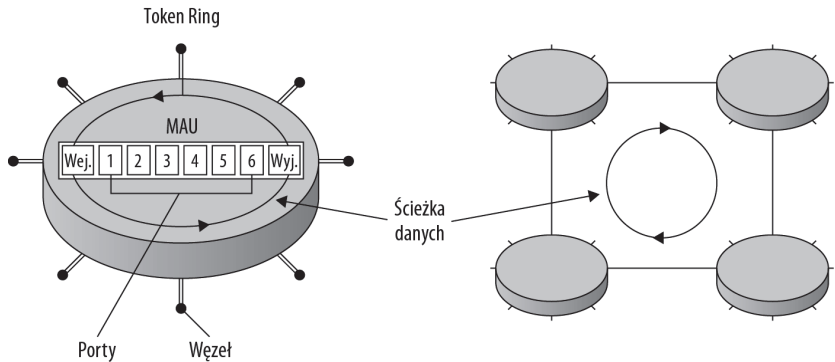
## **Sieci Token Ring**

W sztafecie uczestnicy biegną po kolei, przekazując sobie pałeczkę w wyznaczonej strefie zmian. Podobną technikę zastosowano w sieciach Token Ring, gdzie rolę pałeczki odgrywa token. Token jest specjalną ramką, która daje prawo do transmisji danych po-

między węzłami sieci. Prawo transmisji nadane węzłowi za pomocą tokenu jest nadawane na krótki czas. Ze względu na to, że w sieci tylko jeden węzeł dokonuje transmisji danych, w sieciach zbudowanych z wykorzystaniem tokenu nie występuje zjawisko kolizji. W tych sieciach dodatkowo można przysyłać dane w o wiele większych porcjach w porównaniu z sieciami Ethernet. W celu umożliwienia okresowego lub cyklicznego dostępu do danych sieci działające z wykorzystaniem tokenu są zbudowane w topologii pierścienia, co przedstawiono na rysunku 12.4.

#### Rysunek 12.4.

Topologia sieci  
Token Ring (lewa  
część rysunku)  
i cztery pierścienie  
połączone (prawa  
część rysunku)



Lewa część rysunku 12.4 przedstawia pojedynczy pierścień sieci Token Ring, zbudowany w oparciu o jedną jednostkę dostępu MAU (ang. *Multiple Access Unit*). Jednostka MAU zapewnia routing pomiędzy połączonymi urządzeniami. Ma port wejściowy, określoną liczbę dodatkowych portów (o numerach 1 – 6 na rysunku) oraz port wyjściowy. Każdy punkt widoczny na rysunku reprezentuje węzeł, który posiada dwa przewody, jeden dla przychodzących i jeden dla wychodzących danych. Dane w pierścieniu są zawsze transmitowane w jednym kierunku. Sieć Token Ring można rozszerzać, łącząc ze sobą kilka pierścieni. Koncepcja sieci Token Ring powstała pod koniec lat siedemdziesiątych w korporacji IBM. Warto zauważyć, że niemal w tym samym czasie Xerox PARC opracowywał standard sieci Ethernet, a sieci ARCNET były właśnie wprowadzane do użytku komercyjnego. Na początku Token Ring umożliwiał transmisję danych z prędkością 4 Mb/s. Dla porównania Ethernet umożliwiał transmisję do 10 Mb/s. W 1989 r. wprowadzono standard Token Ring umożliwiający transmisję z prędkością 16 Mbit/s. Sieci Token Ring miały wówczas przewagę nad standardem Ethernet ze względu na wydajność, dlatego że pomimo mniejszej prędkości umożliwiały transmisję znacznie większych pakietów, co skutkowało większą przepustowością.

Ta niezaprzeczalna przewaga sieci Token Ring nad sieciami była okupiona wyższymi cenami przełączników i kart sieciowych. Dodatkowym problemem był fakt, że z technologią wprowadzoną przez IBM nie współpracowały sieci utworzone przez konkurencję, takie jak Apollo Computer czy Proteon. Standard IEEE 802.5 opiera się wprawdzie na pierwotnej wersji Token Ring wprowadzonej przez IBM, ale uniezależniono go od określonego typu medium lub topologii.

Sieci ARCNET zniknęły z rynku sieci LAN w połowie lat 80., a właściwie zostały wyparte przez Ethernet, chociaż ten standard jest w małym stopniu stosowany w urządzeniach wbudowanych. Sieci Fast Ethernet (100 Mbit/s) wyparły technologię Token Ring. Gdy pojawił się standard Fast Ethernet, producenci przełączników zastosowali metody umożliwiające znaczne zredukowanie występowania zjawiska kolizji w sieciach Ethernet. Niższy koszt

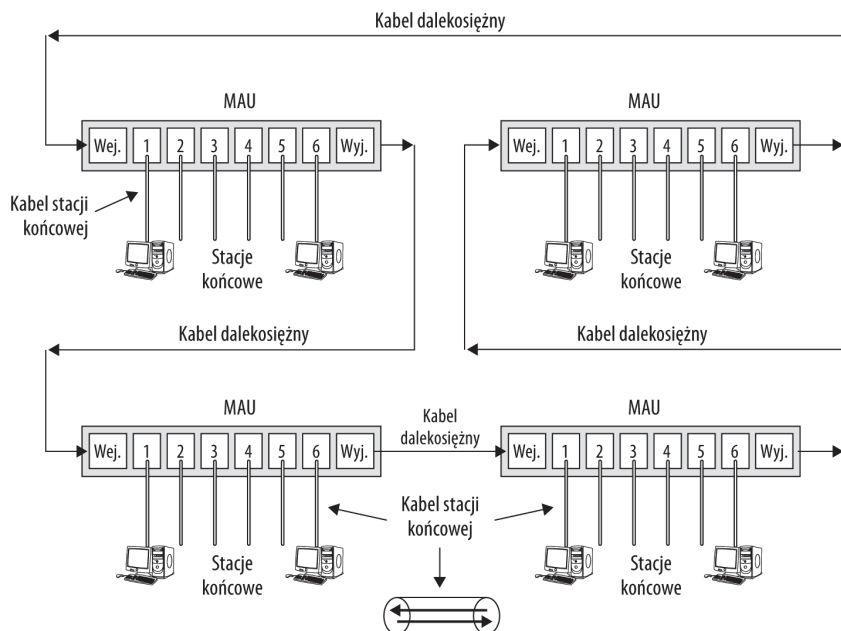
wdrożenia sieci Ethernet uniemożliwił technologii Token Ring zdominowanie rynku sieci lokalnych LAN. Obecnie bardzo trudno znaleźć implementację tej sieci poza IBM. Mimo to technologia Token Ring odgrywa ważną rolę w rozwoju technologii sieciowych i nadal ma wpływ na ich ewolucję i z tego powodu warto bliżej ją poznać.

W sieciach Token Ring logiczną topologię pierścienia uzyskuje się poprzez odpowiednie połączenie urządzeń w sieci. W przypadku Token Ring zbudowanego w IBM przełącznik nazywany jest jednostką MAU lub MSAU. Gdybyśmy chcieli zbudować sieć Token Ring, najpierw umieścilibyśmy jednostkę MAU w centralnym punkcie, a następnie połączyli ją z poszczególnymi stacjami końcowymi.

Omawiana sieć ma zatem fizycznie topologię gwiazdy z ramionami skierowanymi na zewnątrz od centralnego huba. Wykorzystuje się tu specjalną skrętkę przeznaczoną do łączenia stacji końcowych, która została uznana za standard okablowania strukturalnego IBM. Idea pierścienia w sieci Token Ring jest zaimplementowana w jednostce MAU. Wszystkie stacje są podłączone za pomocą kabla stacji końcowej, a każda jednostka MAU posiada port wejściowy IN i port wyjściowy OUT, które można wykorzystać w celu rozszerzenia sieci o kolejne pierścienie.

Rysunek 12.5 przedstawia zestaw czterech pierścieni sieci Token Ring, które połączone tworzą sieć o większym rozmiarze. Do każdej jednostki MAU można podłączyć maksymalnie sześć stacji końcowych, ale na rysunku znajdują się tylko dwie, aby go nie zaciemnić. Rysunek 12.5 pokazuje fizyczną realizację topologii, którą zaprezentowano w prawej części rysunku 12.4. Warto zwrócić uwagę na kabel dalekosiężny. Ten kabel służy do połączenia wszystkich jednostek MAU. W kablu dalekosiężnym dane są przekazywane tylko w jednym kierunku, natomiast kable stacji końcowych umożliwiają transmisję dwukierunkową. W dolnej części rysunku 12.5 przedstawiono dwukierunkowość kabla stacji końcowej.

**Rysunek 12.5.**  
*Sieć Token Ring  
złożona z czterech  
pierścieni*



Token w sieci Token Ring jest trójkietową ramką, przekazywaną pomiędzy węzłami. Jeśli węzeł otrzyma token, ma prawo do przejęcia kontroli nad łączem i wysłania danych. Dane poprzez wszystkie węzły sieci są przekazywane do węzła docelowego, węzeł docelowy kopiuje dane do bufora i przekazuje ramkę dalej, aż do węzła nadającego. Jest to potwierdzenie poprawności dostarczenia danych. Węzeł nadający kasuje ramkę i wysyła wolny token do następnego węzła. W trakcie transmisji danych lub tokenu w pierścieniu nie może wystąpić dodatkowa transmisja, chyba że sieć obsługuje funkcję *szybkiego uwalniania tokenu* (ETR — *Early Token Release*). W sieciach o prędkości 4 Mbit/s można korzystać z pojedynczego tokenu, ale w standardzie umożliwiającym transmisję z prędkością 16 Mbit/s jest dozwolone przesyłanie kilku tokenów jednocześnie. System zasadniczo eliminuje zjawisko kolizji ramek, dzięki czemu jest solidniejszym i bardziej przewidywalnym systemem w porównaniu z innymi standardami.

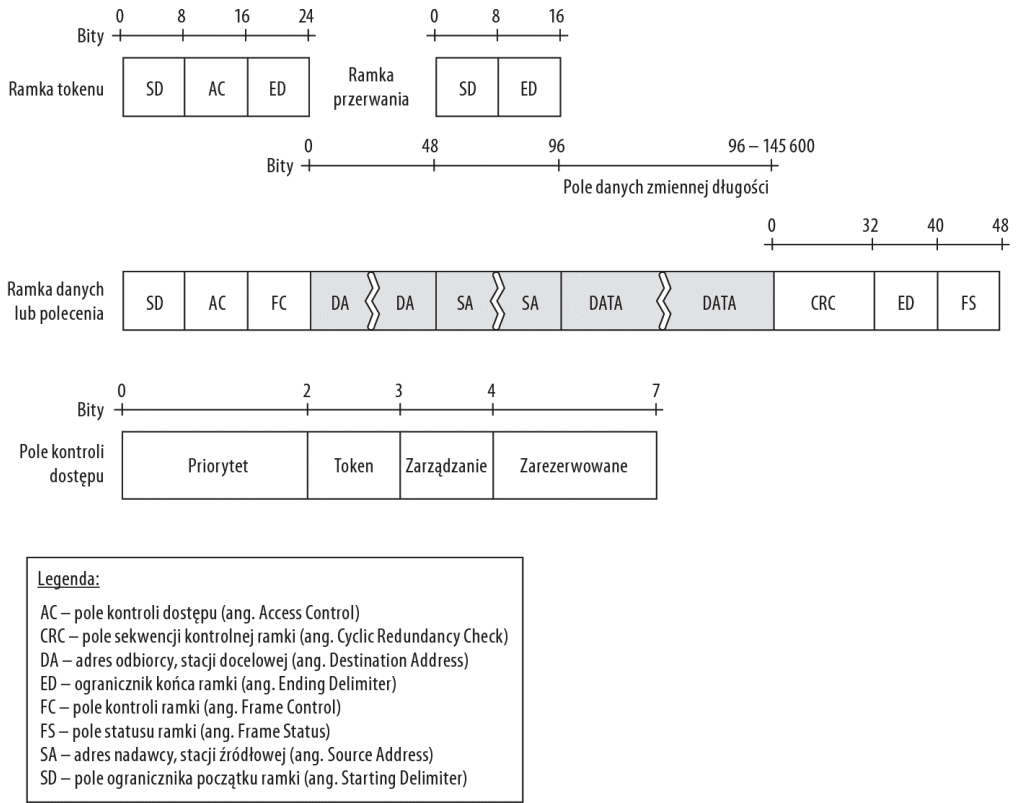
W sieciach Token Ring ruch kontrolowany jest za pomocą pola priorytetu i pola rezerwacji. Priorytet jest nadawany zarówno do stacji, jak i do tokenu. Jeśli stacja otrzyma token o niższym lub równym priorytecie, może go przechwycić i rozpocząć nadawanie. W czasie nadawania stacje, przez które przechodzą ramki i których priorytet jest większy, mogą dokonać rezerwacji tokenu dla transmisji w następnym obiegu. W ten sposób węzły są obsługiwane zgodnie z nadanymi im priorytetami.

Rysunek 12.6 przedstawia strukturę ramek tokenu, danych lub polecenia i przerwania. Ramka danych lub polecenia może mieć rozmiar do 18 200 bajtów. Pole kontroli dostępu AC, pokazane w dolnej części rysunku 12.6, zawiera informacje o priorytecie transmisji. Dzięki tej informacji można określić węzeł, który powinien w danym momencie dostać dostęp do sieci i dokonać transmisji danych. Pole AC znajduje się również w ramce tokenu i jest przydatne do zapewnienia określonego poziomu jakości usług (QoS).

Sieć Token Ring wykorzystuje *różnicowe kodowanie Manchester* (tzw. różnicową modulację bifazową), odmianę *kodowania Manchester*. Kod Manchester jest sposobem fazowej modulacji sygnału. Logicznemu zeru odpowiada zmiana stanu w środku bitu z niskiego na wysoki, jedynie — z wysokiego na niski. W odmianie różnicowej kodowania Manchester logicznemu zeru odpowiada zmiana stanu na początku bitu, a jedynie brak zmiany, w środku bitu zawsze występuje zmiana stanu. W porównaniu ze standardowym kodowaniem Manchester istotny jest jedynie fakt występowania zmian stanu logicznego, takie rozwiązanie pozwala na uniezależnienie kodowania od polaryzacji linii.

Kod różnicowy Manchester jest ujęty w specyfikacji 805.2 protokołu Token Ring i jest używany w standardzie Token Ring firmy IBM. Ponieważ częstotliwość modulacji jest dwa razy większa od częstotliwości transmisji binarnej, efektywność wykorzystania pasma wynosi 50%.

Ze względu na to, że zawsze istnieje możliwość wystąpienia błędów w trakcie transmisji danych, w sieci Token Ring znajduje się jedna stacja końcowa wyposażona w mechanizm kontroli o nazwie *monitor aktywny* (ang. *Active Monitor*). Monitor aktywny przede wszystkim kontroluje stan tokenu i dokonuje korekcy ewentualnych błędów. Omawiana funkcjonalność ma znaczenie krytyczne dla całej sieci i z tego powodu sieć jest zwykle wyposażona w monitor zapasowy. Gdy w sieci występują dwa pierścienie, monitor z jednego pierścienia jest aktywny. Jeśli w określonym czasie nie ma sygnału w sieci, aktywny monitor nie zostanie wykryty lub gdy nie można wykryć ramki tokenu, system podejmie decyzję o ustanowieniu nowego monitora aktywnego. Zgodnie z protokołem Token Ring monitorem aktywnym może być dowolna stacja końcowa.



**Rysunek 12.6.** Struktura ramek używanych w sieciach Token Ring

Monitor aktywny odgrywa kluczową rolę w sieci Token Ring. Uruchamia zegar sieci (taktowanie), wprowadza opóźnienia buforowania, przeciwdziała próbom transmisji tokenu w trakcie przesyłania ramki z danymi bądź ramki polecenia. W sieci Token Ring znajduje się *mechanizm drogowskazu* (ang. *Beaconing*). Dzięki temu monitor rozpoznaje poważne uszkodzenie sieci i wysyła ramkę beacon definiującą uszkodzoną domenę. Omawiany mechanizm może rozpocząć proces automatycznej rekonfiguracji, który zasadniczo prowadzi do zdiagnozowania problemu, a następnie usunięcia błędu, co w krytycznym przypadku kończy się restartem jednostki MAU. W trakcie trwania tej operacji transmisja danych jest zablokowana.

Specjalne ramki sterujące, zwane tokenami, są wykorzystywane nie tylko w sieciach Token Ring. Jednym z przykładów sieci, w których używa się tokenów, jest FDDI — sieć opisana w kolejnym rozdziale.

## Sieci FDDI

FDDI (ang. *Fiber Distributed Data Interface* — standard transmisji danych oparty na technologii światłowodowej) to standard utworzony na bazie Token Ring, przeznaczony do tworzenia sieci światłowodowych, zapewniających duże prędkości transmisji danych. Protokół jest określony jako standard IEEE 802.4, a technologia jest znana jako standard ANSI X3T12. FDDI w porównaniu ze standardem 802.5, opisującym sieć Token Ring,

działa przez wykorzystanie mechanizmu wymiany tokenu w oparciu o czas. W FDDI medium fizycznym jest światłowód. Ten sam protokół wykorzystuje sieć CDDI (ang. *Copper Data Distribution Interface* — standard transmisji danych oparty na technologii kabla miedzianego). Rysunek 12.7 przedstawia odniesienie protokołu FDDI w modelu OSI.

### Rysunek 12.7.

Protokół FDDI  
w modelu OSI

Warstwa 2. OSI Warstwa łącza danych  Warstwa 1. OSI Warstwa fizyczna	Poziom sterowania łączem logicznym (ang. Logical Link Control – LLC)		
	Zarządzanie stacją SMT (ang. Station Management Task)	Poziom sterowania dostępem do nośnika (ang. Medium Access Control – MAC)	
		PHY	TP-PHY
		PMD	TP-PMD
Medium transmisyjne		Światłowód	Kabel miedziany

#### Legenda:

PHY – warstwa fizyczna PHY  
PMD – nośnik warstwy fizycznej (ang. Physical Medium Dependent Interface), służy do zamiany sygnałów elektrycznych na fale świetlne  
SMT – zarządzanie stacją (ang. Station Management Task). Moduł odpowiedzialny za: zarządzanie pierścieniem (RMT – Ring Management), zarządzanie połączeniem (PCM – Connection Management), zarządzanie konfiguracją (CFM – Configuration Management), koordynację jednostki (ECM – Entity Coordination Management)  
TP – skrętka

Na rysunku 12.7 dwie warstwy modelu OSI są oznakowane w lewej kolumnie nad warstwą Medium. Token Ring ma protokół SMT obejmujący warstwę fizyczną i część warstwy łącza danych. Mimo że LLC dla FDDI i Token Ring są takie same, podwarstwa SMT w Token Ring jest podzielona pomiędzy warstwy MAC i różne protokoły warstwy fizycznej. W zależności od tego, czy w FDDI wykorzystuje się światłowody, czy też kable miedziane, mamy odpowiednio protokoły PMD i PHY oraz TP-PMD i TP-PHY.

W sieci FDDI można wyróżnić dwa typy urządzeń:

- ♦ **Stacje.** Stacjami nazywamy komputery, drukarki i inne urządzenia aktywne. W FDDI istnieją dwa typy stacji: stacja podłączana do pojedynczego pierścienia SAS (ang. *Single Attached Stations*) i stacja podłączana do podwójnego pierścienia DAS (ang. *Dual-Attachment Station*).
- ♦ **Koncentratory.** Koncentrator podłączany do podwójnego pierścienia DAC (*Dual-Attachment Concentrator*) jest urządzeniem łączącym stacje SAS z siecią FDDI. W koncentratorach DAC mamy trzy rodzaje portów: A (pierścień podstawowy), B (pierścień dodatkowy) i M (główny port koncentratora). W sieciach FDDI mamy dwa typy koncentratorów: koncentratory pojedyncze SAC, tworzące pierścień pojedynczy oraz koncentratory DAC, dzięki którym można podłączać stacje do podwójnego pierścienia.

W sieciach FDDI mamy trzy rodzaje połączeń:

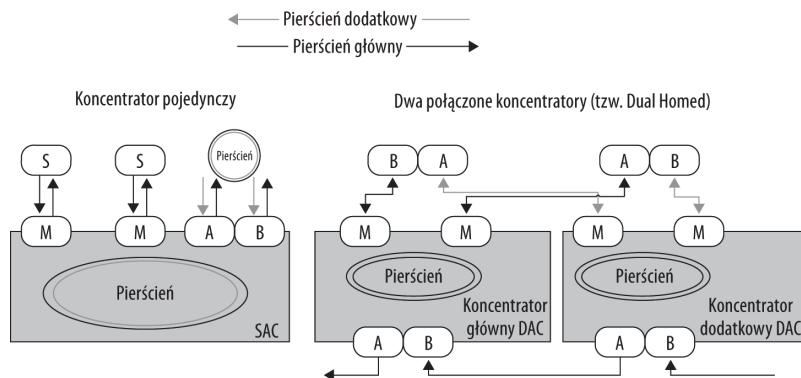
- ♦ **Połączenia stacji pojedynczych SAS.**
- ♦ **Połączenia podwójnego pierścienia DAS.** Stacje DAS są połączone w pierścień. Aby mogły w pełni funkcjonować, muszą należeć do pierścienia.

- ♦ **Połączenie podwójne Dual Homed.** Połączenie Dual Homed polega na połączeniu koncentratora lub stacji DAS z dwoma innymi koncentratorami. To połączenie odpowiada dwom łączom SAS.

Na rysunku 12.4 sieć Token Ring jest zbudowana z wykorzystaniem jednej jednostki MAU. Podobnie na rysunku 12.8 zaprezentowano sieć FDDI z jedną jednostką SAC. W ten sposób standard FDDI zapewnia prostą strukturę sieci. Jeśli można skorzystać z dwóch koncentratorów DAC do budowy sieci, można utworzyć strukturę odporną na awarie. Wspomniane dwa typy sieci FDDI przedstawiono na rysunku 12.8. Połączenia pomiędzy portami M i S można zrealizować, wykorzystując światłowód bądź skrętkę. Na rysunku 12.8 główny pierścień oznaczono czarną linią, a pierścień dodatkowy — linią szarą. Dane są przesyłane zgodnie z kierunkiem zaznaczonym strzałkami.

### Rysunek 12.8.

*Sieć zbudowana z wykorzystaniem jednego lub dwóch koncentratorów DAC*



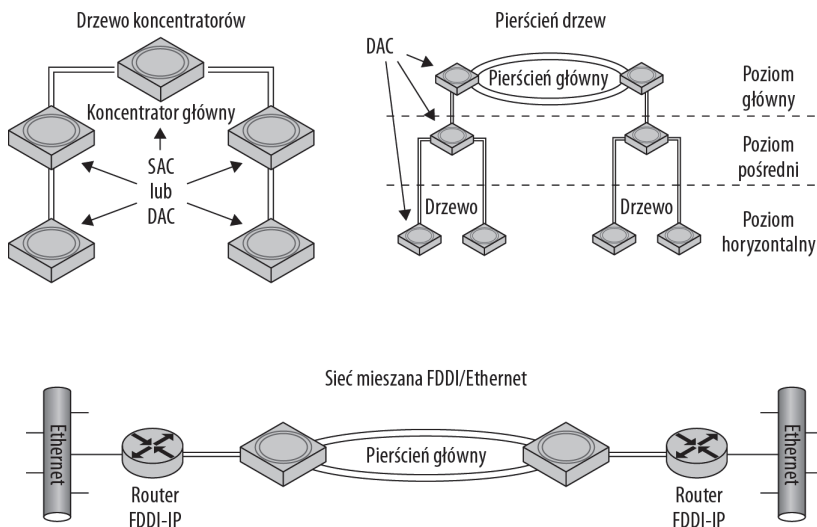
Aby dodać więcej węzłów sieci FDDI, można podłączyć jeden lub więcej portów AB koncentratora głównego do innych koncentratorów i utworzyć hierarchiczną strukturę drzewa. Można również utworzyć pierścień drzew, zastępując główny koncentrator podwójną strukturą pierścienia FDDI. Topologia pierścienia drzew jest często używana w sieciach LAN kampusów uczelnianych. Bardzo często sieci FDDI są podłączone do sieci Ethernet i współtworzą topologię mieszaną. Taka topologia wymaga zastosowania routerów FDDI/IP jako urządzeń brzegowych, rozdzielających wspomniane rodzaje sieci (drzewo koncentratorów, pierścień drzew i sieć mieszaną FDDI/Ethernet).

Rysunek 12.9 przedstawia trzy topologie. Te rodzaje sieci ilustrują różne podejście do wykorzystania standardu FDDI w coraz większej liczbie typów sieci. FDDI mogą być stosowane jako szkielet koncentratorów, w postaci drzewa koncentratorów, pokazanych na omawianym rysunku. Topologia pierścienia drzew pozwala na hierarchiczną strukturę sieci, gdzie każdy z koncentratorów znajdujących się w pierścieniu zarządza ruchem elementów podległego mu drzewa. Każdy poziom w pierścieniu drzew jest odpowiednio nazwany. W takiej sieci mamy poziom nadrzędny, poziom pośredni i poziom horyzontalny. Można również tworzyć sieci mieszane, łącząc pierścienie FDDI z sieciami Ethernet poprzez routery FDDI/IP.

FDDI jest szeroko stosowanym standardem w telekomunikacyjnych sieciach szkieletowych. Systemy budowane w oparciu o FDDI są wypierane przez szybki Ethernet. Wersja druga standardu FDDI (FDDI-II) wprowadziła możliwość transmisji danych w trybie połączeniowym. W przeszłości wiele zainwestowano w rozwój sieci FDDI i między innymi z tego

**Rysunek 12.9.**

Trzy typy topologii FDDI: drzewo koncentratorów, pierścień drzew i topologia mieszana FDDI/Ethernet



powodu są one wykorzystywane do transmisji danych głosowych i wideo<sup>7</sup>. Sieci FDDI są obecnie często łączone z sieciami SDH (ang. *Synchronous Digital Hierarchy* — synchroniczna hierarchia systemów cyfrowych), nowoczesnymi sieciami szerokopasmowymi.



Sieci SDH są opisane w rozdziale 13.

Sieć FDDI posiada dwa pierścienie. W każdym z nich dane są wysyłane w przeciwnym kierunku. Te dwupierścieniowe sieci są często stosowane w niewielkich sieciach LAN. Pierścień podstawowy pozwala na transmisję danych z prędkością 100 Mbit/s, a drugi pełni funkcję łącza zapasowego albo stanowi dodatkowy kanał, rozszerzający przepustowość sieci do 200 Mbit/s. Interfejsy routerów łączy się z dwoma pierścieniami, tworząc połączenia podwójne. Stacje robocze podłącza się do sieci pojedynczym łączem. Podobnie jak w przypadku innych systemów optycznych, urządzenia zwane koncentratorami umożliwiają zapewnienie komunikacji wielu komputerom przy użyciu jednego łącza światłowodowego.

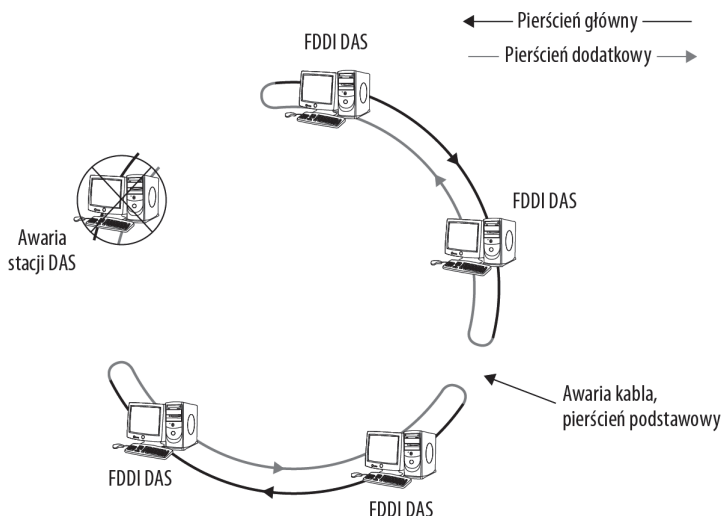
Jeśli drugi pierścień jest skonfigurowany jako łącze zapasowe, a pierścień główny posiada połączenia podwójne, w razie awarii sieć może przełączyć się na komunikację w oparciu o pierścień zapasowy. Na rysunku 12.10 przedstawiono działającą sieć FDDI, gdzie wystąpiły dwie awarie: zepsuł się jeden z kabli pierścienia podstawowego oraz jedna stacja DAS. W przypadku wystąpienia jednej awarii sieć przełącza się na pierścień zapasowy i jest w pełni funkcjonalna, ale gdy wystąpią dwie awarie — sieć jest dzielona na dwie mniejsze sieci.

Sieci FDDI to kombinacja szybkości, możliwości połączeń dalekosiężnych i możliwości podłączenia dużej liczby stacji roboczych. W sieci FDDI można podłączyć do 500 węzłów DAS lub 1000 SAS. Kabel światłowodowy sieci FDDI może mieć długość do 200 km i stanowić połączenie dla dużej liczby użytkowników (liczonej w tysiącach). Pierścienie mają średnicę około 100 km, co sprawia, że FDDI jest bardzo popularnym standardem budowy sieci MAN.

<sup>7</sup> Wymagających zachowania odpowiedniej jakości usługi — *przyp. tłum.*

**Rysunek 12.10.**

*FDDI jest przykładem szybkiej sieci LAN odpornej na awarie — wystąpienie nawet dwóch poważnych problemów powoduje podział sieci*



Odmianą sieci FDDI jest CDDI. CDDI jest siecią zbudowaną zgodnie ze standardem FDDI w wersji dla przewodów miedzianych. Te sieci mają maksymalną prędkość 100 Mbit/s, a maksymalna długość połączenia to 100 m dla skrętki nieekranowanej UTP.

## Sieci wykorzystywane w automatyce

Do sieci można podłączać nie tylko komputery, chociaż większa część tej książki poświęcona jest właśnie sieciom komputerowym. Sieci umożliwiają łączenie szerokiej gamy urządzeń. Sieci LAN zbudowane w samochodach i samolotach łączą komputery pokładowe z licznymi czujnikami i innymi urządzeniami, tworząc często bardzo złożone systemy. Trzeba też wspomnieć o urządzeniach diagnostycznych używanych przez mechaników samochodowych, którzy w praktyce korzystają z dobrodziejstwa zainstalowanych urządzeń sieciowych.

Aby zgłębić zagadnienia związane z domem inteligentnym, warto zapoznać się z zaleceniem X10 automatyki domowej. Ten protokół opisano w kolejnym punkcie. Obecnie w każdym nowoczesnym wieżowcu systemy HVAC (systemy ogrzewania, wentylacji i klimatyzacji) i oświetlenie są sterowane komputerowo, często z jednej konsoli lub jednego komputera. Ogólnie rzecz ujmując, można zauważyć, że systemy sieciowe są wykorzystywane w sterowaniu wszelkiego rodzaju urządzeniami przemysłowymi. Roboty przemysłowe w fabrykach samochodów, urządzenia do produkcji farmaceutyków, moduły sterowania ruchem kolejowym, urządzenia do śledzenia paczek — to wszystko przykłady zastosowań rozwiązań sieciowych w sterowaniu różnych systemów.

Wymienione przykłady zastosowania sieci w automatyce zawierają urządzenia połączone w sieć i odpowiednie oprogramowanie z interfejsami umożliwiającymi kontrolę i sterowanie. W omawianych sieciach łączy się czujniki, wyłączniki, zawory do hubów lub przełączników sieciowych, gdzie dzięki zaimplementowanym sterownikom można zbierać dane przekazywane z wymienionych urządzeń. Dane z przełączników trafiają do komputera centralnego, gdzie odpowiednie oprogramowanie jest wykorzystywane do analizy danych i wysyłania poleceń sterujących. Taki komputer centralny jest określany jako interfejs HMI (ang.

*Human Machine Interface* — interfejs „człowiek — maszyna”) lub system nadzorujący przebieg procesu technologicznego lub produkcyjnego SCADA (ang. *Supervisory Control And Data Acquisition*).

Urządzenia sieciowe, znajdujące się w sieci przemysłowej, są łączone i obsługiwane w oparciu o specjalistyczne standardy automatyki przemysłowej, których przykładem jest protokół SNMP. Urządzenia wykorzystywane do zbierania danych z czujników i przekazywania poleceń są określane mianem programowalnych sterowników logicznych PLC (ang. *Programmable Logic Controller*). Oprogramowanie tych sterowników to prawnie zastrzeżone aplikacje albo narzędzia zbudowane z użyciem otwartych standardów, takich jak Java, Microsoft OLE, DCOM, a nawet .NET Framework.

Większość rozwiązań sieciowych wykorzystywanych w automatyce przemysłowej jest własnością ich producentów. Istnieją jednak również otwarte standardy. W kolejnych punktach omówiono kilka z nich; doczekały się one wielu implementacji.

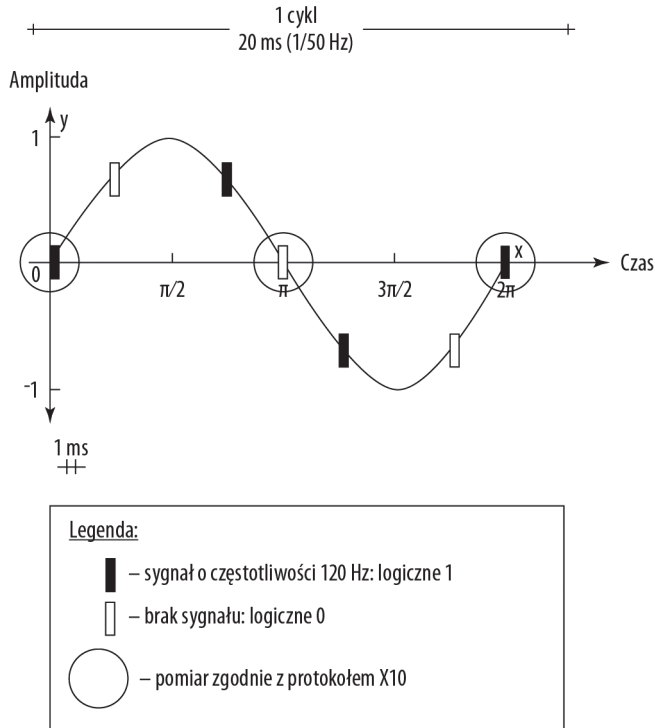
## Standard X10 i automatyka domowa

Standard X10 to otwarty standard komunikacji urządzeń i sterowania nimi za pośrednictwem instalacji elektrycznej. Jest on powszechnie stosowany (USA, Indie, Wiek Brytania) do automatyzacji domów — powstają w ten sposób sieci *automatyki domowej*, nazywane *domem inteligentnym*. X10 definiuje protokół, dzięki któremu można przekazywać sygnały na podstawie modulacji amplitudowej. Dane są transmitowane z wykorzystaniem krótkich wiązek (ang. *bursts*), wysyłanych synchronicznie z napięciem sieci elektrycznej po detekcji przejścia przez zero. W tym momencie na przebiegu napięcia sinusoidalnego jest nakładana wiązka, interpretowana przez odbiornik jako jedynka logiczna. Brak nałożonej wiązki oznacza logiczne zero.

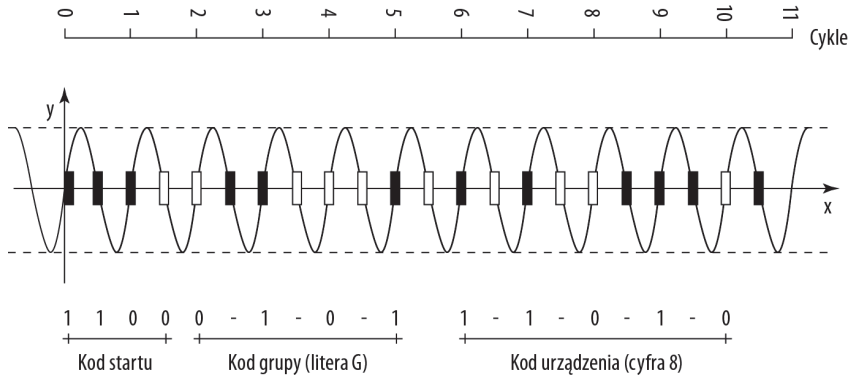
Ponieważ sygnał transmisji danych ma wyższą częstotliwość niż sygnał nośnej (którym jest przebieg o częstotliwości 50 Hz), sygnał z danymi jest faktycznie powtórzony dwa razy w półokresie od 0 do  $\pi$  i jeszcze dwa razy w drugim półokresie — od  $\pi$  do  $2\pi$ . Te dodatkowe wystąpienia są używane do pomiaru czasu i wprawdzie nie są traktowane jako dane, ale odgrywają bardzo ważną rolę. W systemach kodowania przeważnie nie bierze się pod uwagę wyłącznie reprezentacji logicznych wartości 0 i 1 w postaci niskiego i wysokiego poziomu. Aby wygenerować na przykład logiczną jedynkę, trzeba przesłać sygnał zmiany poziomu z wysokiego na niski. W celu przesłania logicznego zera, należy najpierw wygenerować wysoki, a potem niski poziom. Takie kodowanie ułatwia generowanie i bezbłędny odczyt informacji w odbiorniku. Rysunek 12.11 przedstawia nałożony sygnał X10 (wiązki o długości 1 ms) na sinusoidalny przebieg napięcia sieci elektrycznej.

Załóżmy, że posiadamy kontroler X10, którym możemy sterować za pośrednictwem pilota lub przycisku na konsoli. Po naciśnięciu przycisku zostanie wygenerowany kod binarny, który jest przesyłany przez instalację elektryczną. Kod jest zestawem trzech binarnych identyfikatorów: kodu startu (4 bity, 1110), kodu danych (8 bitów) i kodu sterowania (10 bitów), które razem określono mianem ramki X10. Kod sterowania reprezentuje liczbę bądź literę przypisaną do określonej funkcji. W informacji wykorzystuje się tylko bity danych, ignorując bity synchronizacji. Rysunek 12.12 przedstawia informację, której wysłanie wymaga 11 pełnych cykli sygnału podstawowego, co ilustruje pełną długość kodu sterowania. Dzięki definicji różnych długości kodów i odstępów między nimi zapewniono ich unikatowość i jednoznaczny przekaz informacji.

**Rysunek 12.11.**  
Wiązki sygnału X10  
na tle sygnału linii  
elektrycznej



**Rysunek 12.12.**  
Zakodowany  
sygnał X10. Wiązki  
synchronizacyjne  
zostały usunięte,  
aby poprawić  
czytelność rysunku



Standard X10 definiuje pełny zestaw kodów możliwych do transmisji pomiędzy sterownikiem a urządzeniem odbiorczym. Dodatkowo zdefiniowano znak odstępu złożony z trzech pełnych cykli sygnału elektrycznego oraz mechanizm powtarzania kodów. Ponadto standard narzuca konieczność stosowania odstępu trzech zerowych bitów w trakcie transmisji poleceń adresowanych do różnych urządzeń. Kody służące do rozjaśniania lub ściemniania światła powinny być przesyłane w sposób ciągły, bez zachowania przerw między poszczególnymi wystąpieniami. Te kody powinny być powtórzone co najmniej dwukrotnie, ale lepiej jest zachować większą liczbę powtórzeń. Tabela 12.4 przedstawia kody standardu X10.

**Tabela 12.4.** *Kody poleceń standardu X10*

Kod	Bit 1.	Bit 2.	Bit 3.	Bit 4.	
START	1	1	1	0	–
Kod grupy	Bit 1.	Bit 2.	Bit 3.	Bit 4.	
A	0	1	1	0	
B	1	1	1	0	
C	0	0	1	0	
D	1	0	1	0	
E	0	0	0	1	
F	1	0	0	1	
G	0	1	0	1	
H	1	1	0	1	
I	0	1	1	1	
J	1	1	1	1	
K	0	0	1	1	
L	1	0	1	1	
M	0	0	0	0	
N	1	0	0	0	
O	0	1	0	0	
P	1	1	0	0	
Kod urządzenia (polecenia)	Bit 1.	Bit 2.	Bit 3.	Bit 4.	Bit 5.
1	0	1	1	0	0
2	1	1	1	0	0
3	0	0	1	0	0
4	1	0	1	0	0
5	0	0	0	1	0
6	1	0	0	1	0
7	0	1	0	1	0
8	1	1	0	1	0
9	0	1	1	1	0
10	1	1	1	1	0
11	0	0	1	1	0
12	1	0	1	1	0

**Tabela 12.4.** *Kody poleceń standardu X10 — ciąg dalszy*

Kod urządzenia (polecenia)	Bit 1.	Bit 2.	Bit 3.	Bit 4.	Bit 5.
13	0	0	0	0	0
14	1	0	0	0	0
15	0	1	0	0	0
16	1	1	0	0	0
Wyłącz wszystko	0	0	0	0	1
Włącz wszystkie światła	0	0	0	1	1
Włącz	0	0	1	0	1
Wyłącz	0	0	1	1	1
Ściemnij	0	1	0	0	1
Rozjaśnij	0	1	0	1	1
Wyłącz wszystkie światła	0	1	1	0	1
Kod rozszerzenia	0	1	1	1	1
Przywołanie <sup>1</sup>	1	0	0	0	1
Potwierdzenie przywołania	1	0	0	1	1
Ściemnij — ustawienie fabryczne	1	0	1	—	1
Rozszerzone dane analogowe	1	1	0	0	1
Włącz status	1	1	0	1	1
Wyłącz status	1	1	1	0	1
Zażądaj statusu	1	1	1	1	1

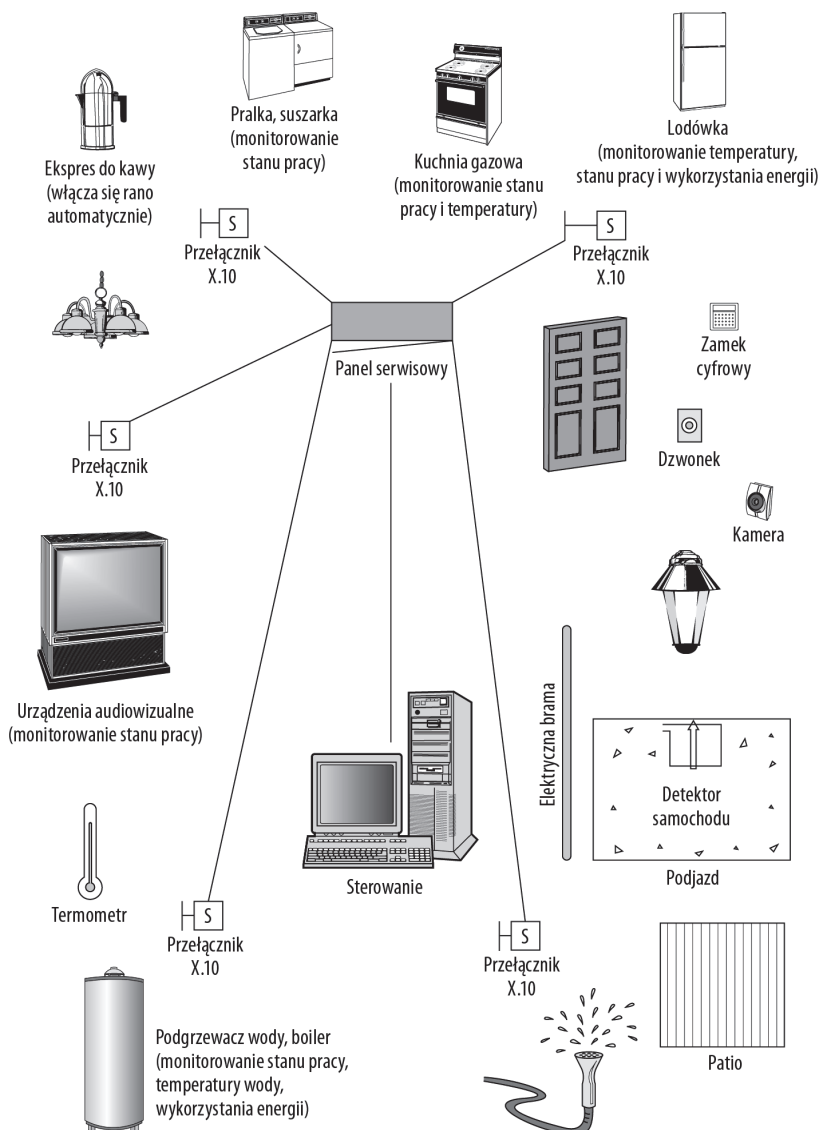
<sup>1)</sup> Poza ściemnianiem i rozjaśnianiem pomiędzy transmisjami wymagane są trzy puste cykle.

Sieć X10 działa poprzez podłączenie odbiornika do gniazdka elektrycznego w domu, a następnie przyłączenie kontrolowanego urządzenia do odbiornika X10. Za pomocą X10 można sterować oświetleniem, urządzeniami elektronicznymi w domu i regulatorami (np. temperatury). Urządzenia wymagają zastosowania odpowiednich modułów X10. W niektórych przypadkach moduły są zaprojektowane tak, aby możliwość zdalnego sterowania była włączana za pośrednictwem specjalnego przełącznika. Większość modułów służących do sterowania oświetleniem posiada funkcję *lokalnego ściemniania*, która pozwala na włączanie i wyłączanie światła oraz stopniową regulację jego natężenia. Rysunek 12.13 pokazuje wybrane urządzenia domowe, które mogą być kontrolowane w sieci X10. Na przykład wąż do podlewania ogrodu, przedstawiony w prawym dolnym rogu, jest kontrolowany przez odpowiedni układ oparty na standardzie X10.

W celu identyfikacji każdy odbiornik X10 ma przypisany unikalny adres. Nadajnikiem omawianego standardu może być pilot zdalnego sterowania albo program komputerowy podłączony do systemu za pośrednictwem odpowiedniego układu przyłączonego do gniazdka elektrycznego. Użycie klawiatury spowoduje wygenerowanie jednego z kodów poleceń przedstawionych w tabeli 12.4, co umożliwi komunikację z określonym urządzeniem.

**Rysunek 12.13.**

Przykład urządzeń domowych sterowanych za pomocą urządzeń sieci X10



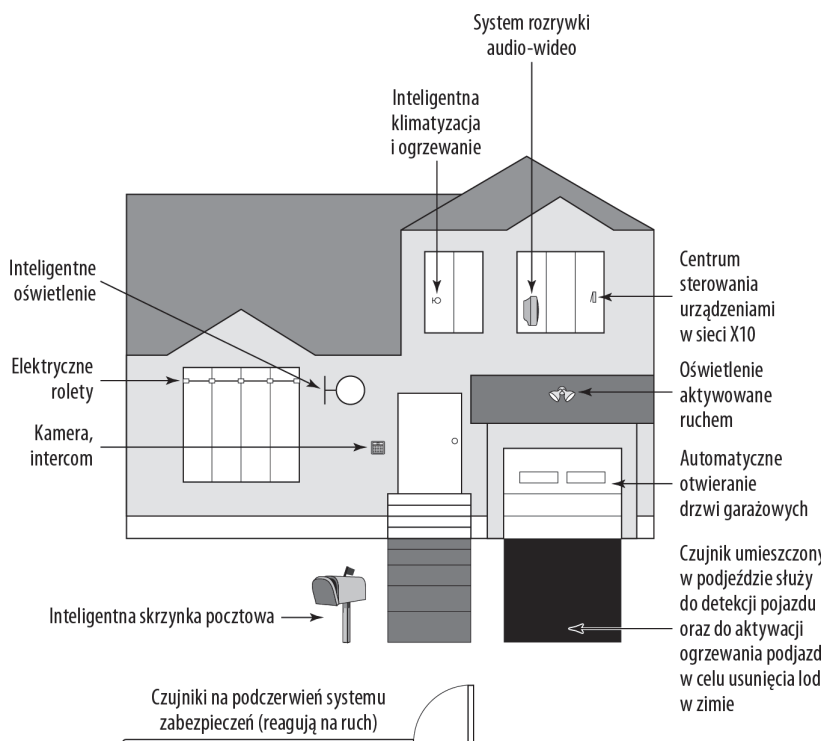
W oprogramowaniu sterującym można zaprogramować dowolne funkcje, wszystko zależy od stopnia zaawansowania aplikacji. Takie aplikacje mogą być wykorzystywane do kontroli kina domowego, realizować z góry zaprogramowany porządek zdarzeń, tworzyć dziennik zdarzeń, wysyłać komunikaty wyzwolone określonymi zdarzeniami i realizować inne zadania. Wśród najbardziej znanych programów automatyki domowej warto wymienić Central Home Automation Director (CHAD) Software, HAL 2000 Voice Control Software, Home Controls, HAI Web-Link, HomeSeer Software, Indigo, PowerHome, Smarthome Manager PLUS, Superna ControlWare i Thinking Home.

Protokół X10 umożliwia także współpracę z urządzeniami pracującymi na częstotliwościach radiowych, takie jak klawiatury, breloki, alarmy antywłamaniowe, włączniki na podczerwień itp. W USA częstotliwości radiowe, które mogą być użyte przez te urządzenia, to pasmo

310 MHz, w Europie — 433 MHz. Odbiornik radiowy zapewnia odpowiedni most potrzebny do przekazywania poleceń do sieci przewodowej. Niektóre z urządzeń radiowych przedstawiono na rysunku 12.14.

### Rysunek 12.14.

Urządzenia domowe,  
które można połączyć  
w sieci X10



Jedną z najpopularniejszych komercyjnych witryn internetowych, gdzie można znaleźć ofertę produktów do automatyzacji domu, jest [www.Smarthome.com](http://www.Smarthome.com).

X10 jest najbardziej znanym systemem sieci do automatyzacji urządzeń domowych. Istnieje wiele innych rozwiązań umożliwiających automatyzację domu, których użycie warto rozważyć przy projektowaniu takiego systemu, na przykład INSTEON, UPB, ZigBee i Z-Wave. Tabela 12.5 zawiera wykaz niektórych standardów stosowanych w sieciach domowych i porównanie ze standardami sieci komputerowych.

W tabeli 12.5 przedstawiono różne systemy automatyki domowej. Sieci odgrywają również istotną rolę w systemach automatyki przemysłowej. W kolejnym punkcie zostaną omówione najczęściej stosowane systemy sterowania procesami PCS (ang. *Process Control System*).

## systemy sterowania procesami

Sieci automatyki przemysłowej, wykorzystywane w sterowaniu procesami produkcyjnymi, są najczęściej zbudowane z jakiejś formy rozproszonego systemu sterowania DCS (ang. *Distributed Control System*). System sterowania procesami przemysłowymi może kontrolować temperaturę pieca w piekarni, synchronizować dostawy części na linii produkcyjnej, sterować natężeniem światła w hali produkcyjnej itp. Elementy sieci są rozmieszczone

**Tabela 12.5.** *Sieci stosowane w automatyce domowej*

Sieć	Medium transmisyjne	Prędkość	Maksymalna długość łącza
Bluetooth	radio	1 – 10 Mb/s	10 – 20 m
Ethernet	skrętka lub światłowód	10 Mb/s – 1 Gb/s	100 m – 15 km
HomePlug	sieć elektryczna	14 – 200 Mb/s	200 m
HomePNA	linia telefoniczna	10 Mb/s	300 m
INSTEON	sieć elektryczna	IRDA 9,6 Kb/s – 4 Mb/s	2 m (z zapewnieniem widoczności łączonych urządzeń)
IRDA	podczerwień	9,6 Kbit/s – 4 Mbit/s	2 m (zasięg widoczności)
LonWorks	skrętka, sieć elektryczna, radio, podczerwień, Ethernet	1.7 Kb/s – 1.2 Mb/s	1500 – 2700 m
Wi-Fi (IEEE 802.11)	radio	11 – 248 Mb/s	30 – 100 m
X10	sieć elektryczna	50 – 60 b/s	500 m
Z-Wave	radio	9,6 – 40 Kb/s	30 m
ZigBee	radio	20 – 250 Kb/s	10 – 75 m

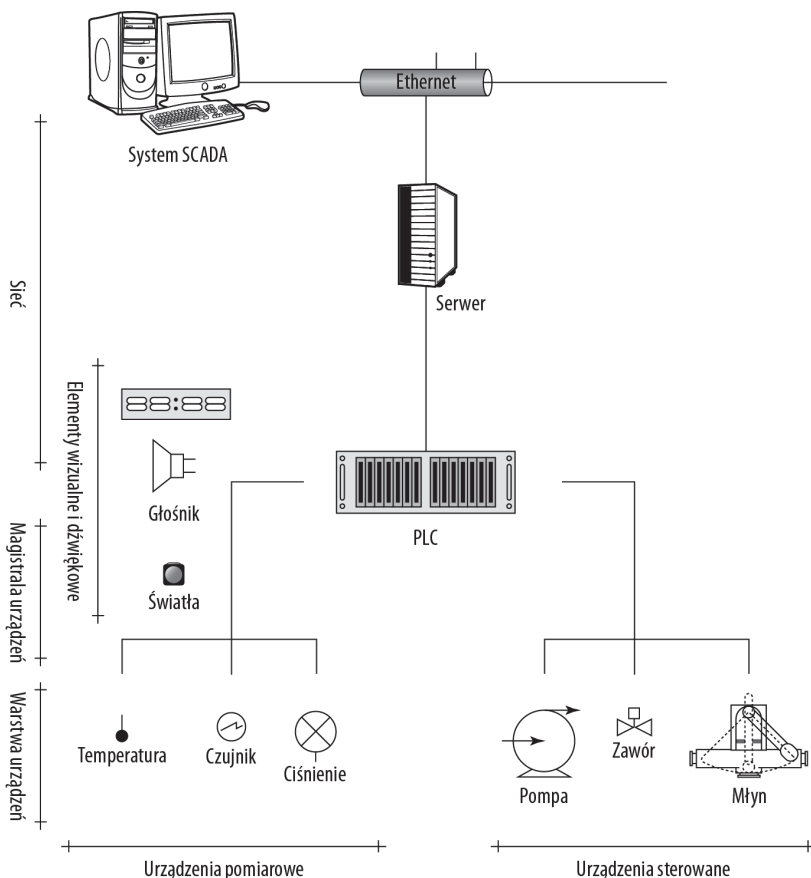
w punktach obsługi urządzeń, które służą do monitoringu i (lub) sterowania. Wspomniane elementy sieci pozwalają dodatkowo na odbiór danych, zebranych z różnych czujników i przekształconych na postać umożliwiającą transmisję w danej sieci. Systemy DCS są wykorzystywane w zakładach chemicznych, energetycznych, elektrociepłowniach i chłodniach, rafineriach ropy naftowej, zakładach farmaceutycznych, a także w sieciach sensorów, w pojazdach, przedsiębiorstwach wodno-kanalizacyjnych i wielu innych branżach.

Najłatwiej wyobrazić sobie system DCS jako dwie sieci łączące trzy warstwy urządzeń. Rozproszoną część systemu stanowi grupa czujników, urządzeń sterujących, siłowników i innych elementów umożliwiających zarządzanie i sterowanie systemem produkcyjnym. Wspomnianą część systemu DCS nazywamy warstwą urządzeń.

Rysunek 12.15 przedstawia przykład systemu sterowania, gdzie elementem umożliwiającym wydawanie poleceń jest konsola lub jednostka SCADA. SCADA zwykle zawiera odpowiednio przygotowany interfejs HMI, często w postaci wyświetlacza wskazującego aktualny stan systemu i pozwalającego operatorowi dokonać pożądaných modyfikacji ustawień. Polecenia i dane otrzymane z czujników są przekazywane do jednostki PLC. Jednostka PLC jest połączona ze wszystkimi urządzeniami przesyłającymi i odbierającymi dane. Omawiany rysunek jest przykładem architektury rozproszonej, gdzie najwyższym elementem w hierarchii jest sieć Ethernet, a poniżej znajduje się magistrala urządzeń oraz warstwa urządzeń.

Proste procesory lub układy ASIC znajdujące się w urządzeniach gromadzą dane i przekazują je do PLC. Większość urządzeń pomiarowych posiada zaimplementowany protokół Wire Protocol, który jest wykorzystywany do sterowania. Sygnały pomiarowe mogą być sygnałami analogowymi lub cyfrowymi, wartościami logicznymi (np. *włącz* lub *wyłącz*, 1 lub 0), tablicami zawierającymi wartości aktualizowane w czasie rzeczywistym.

**Rysunek 12.15.**  
Sieć z wykorzystaniem  
układu PLC



W zależności od mierzonych wielkości przepływ danych z sensorów może być tak duży, że tylko znikomy procent jest próbkowany i poddawany dalszej analizie. Większość czujników pomiarowych próbuje dane w odstępach milisekundowych, tworząc setki wartości na sekundę. W oprogramowaniu służącym do magazynowania pomiarów i ich prezentacji większość z danych przekazanych z czujników jest kasowana; zostają tylko najbardziej pożądane wartości.

Warstwa urządzeń jest podłączona poprzez magistralę do modułu multipleksera, którego zadaniem jest multipleksacja i demultipleksacja danych pochodzących z poszczególnych czujników bądź dla nich przeznaczonych. Moduły multipleksacji mają różne nazwy, zwykle pochodzące od producentów lub związane z obsługiwany protokołami i technologiami. Jednym z uniwersalnych modułów jest kontroler PLC, używany w wielu implementacjach sieci przemysłowej. Kontrolery PLC są specjalnymi urządzeniami, obsługującymi wiele interfejsów wejścia-wyjścia. PLC zostały opracowane pod koniec lat sześćdziesiątych w ramach dążenia do integracji automatyki w przemyśle motoryzacyjnym w sposób umożliwiając tworzenie urządzeń przez różnych producentów.

Sterowniki PLC są urządzeniami czasu rzeczywistego, służącymi do sterowania innymi urządzeniami i systemami. Niektóre sterowniki mają wewnętrzną logikę, która pozwala im utrzymać stan równowagi z wykorzystaniem sprzężenia zwrotnego, utworzony na podsta-

wie danych z podłączonego urządzenia. Na przykład w przypadku reaktora wymagającego określonej temperatury sterownik będzie odczytywać dane z czujnika temperatury, a następnie dostosuje napięcie doprowadzane do elementu grzejnego.

Kontroler PLC często służy jako interfejs pomiędzy dwoma typami sieci, pozwalający na otwarcie wielu połączeń wejścia-wyjścia, umożliwiający odczyt danych analogowych lub cyfrowych, sterowanie silnikami, przekąźnikami i innymi elementami. Kontrolery PLC są programowalne, co oznacza, że można na przykład przesłać do nich zestaw poleceń wydawanych przez inne urządzenia. PLC może być skonfigurowany między innymi z portami szeregowymi RS 232 lub RS 485 oraz portem RJ-45 Ethernet. Większość układów PLC można wykorzystać w różnych zastosowaniach ze względu na ich elastyczność. Wystarczy zaopatrzyć się w układ i skonfigurować go dla odpowiedniego interfejsu.

PLC często komunikuje się z urządzeniami za pomocą określonego protokołu. Przykładem powszechnie stosowanych protokołów są Modbus i DF1. Do komunikacji wykorzystuje się różne magistrale, na przykład DeviceNet lub Profibus. Istnieje wiele protokołów i magistrali zamkniętych, utworzonych przez producentów gotowych systemów. Wśród dostawców systemów PLC warto wyróżnić takie jak: ABB, Allen-Bradley, IDEC, Honeywell, Omron, General Electric, Mitsubishi, Siemens.

Nie wszystkie systemy DCS są zbudowane z wykorzystaniem sterowników PLC. Niektóre technologie wymagają bardzo wysokiej prędkości przesyłu danych, co sprawia, że sterowniki PLC nie nadążają z przetwarzaniem i transmisją. Dobrym przykładem są systemy sterowania instalowane w samolotach. Niektóre zadania są na tyle powtarzalne, że można je zautomatyzować za pomocą urządzeń mechanicznych, zmniejszając koszt systemu. W przeszłości zamiast sterowników PLC często stosowano urządzenia o nazwie RTU. Te urządzenia mają podobne funkcjonalności jak PLC, ale nie są tak elastyczne i programowalne jak PLC, przez co obecnie rzadziej się je stosuje. Mimo to zadania układów PLC i RTU są podobne.

Obecnie różnice między systemami zbudowanymi w oparciu o DCS, PLC i RTU zacierają się i trudno na pierwszy rzut oka stwierdzić, z którą technologią mamy do czynienia. Zwykle z terminem DCS kojarzą się rozległe i kosztowne systemy automatyki przemysłowej. Niektóre projekty takich systemów to wydatek wielu milionów euro. Sterowniki PLC współpracują z nowymi, otwartymi standardami, niezależnymi od producentów poszczególnych urządzeń. Otwarte systemy automatyzacji nie są niezależne od platformy; tutaj znaczenie słowa „otwarte” należy rozumieć inaczej niż w przypadku np. otwartego oprogramowania. Możliwość stosowania różnych platform sprzętowych z dowolnym oprogramowaniem jest bardzo ograniczona; trzeba zawsze dobrać komponenty do pożądanej architektury rozwiązania. Dzięki wykorzystaniu technologii OLE firmy Microsoft powstał otwarty standard komunikacji przemysłowej OLE for Process Control, w skrócie OPC. Systemy automatyki zostały zbudowane z wykorzystaniem Java, .NET Framework i innych powszechnie stosowanych narzędzi programistycznych.

Trzecią częścią systemu DCS poza urządzeniami i magistrali urządzeń jest sieć zawierająca oprogramowanie sterujące SCADA. SCADA może być zaimplementowane jako zestaw narzędzi uruchamianych z wiersza poleceń. Częściej te systemy są realizowane z wykorzystaniem wyświetlaczy graficznych (interfejsy HMI), umożliwiających operatorowi sterowanie systemem zgodnie z nadanymi uprawnieniami przez programistę lub administratora.

System SCADA zbudowany na bazie systemu operacyjnego Microsoft Windows wykorzystuje w pełni nowoczesne metody programowania obiektowego, oferując odpowiednie narzędzia kontroli dostępu: użytkownicy i grupy, zabezpieczenia, skrypty i inne funkcje.

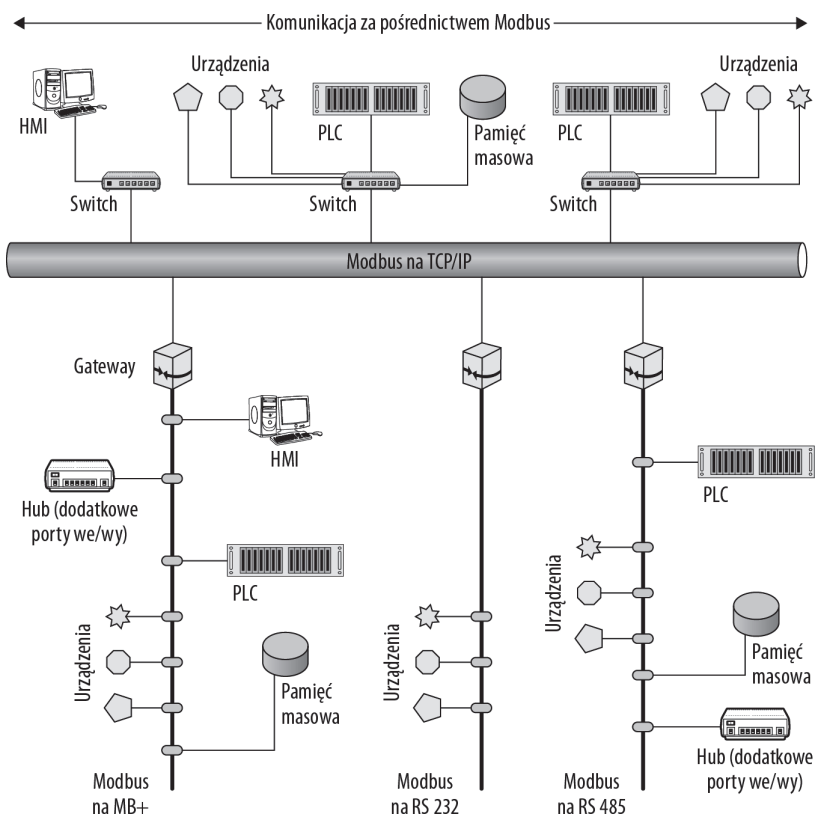
W kolejnych punktach opisano dwie najważniejsze i najczęściej stosowane magistrale urządzeń: Modbus i BACnet, jak również standardy OPC zapewniające transmisję danych w sieciach Windows.

## Modbus

Modbus jest najczęściej spotykanym szeregowym protokołem komunikacyjnym używanym w sieciach automatyki przemysłowej. Ten otwarty standard został opublikowany w 1979 r. przez firmę Modicon (obecnie część Schneider Electric) na potrzeby układów PLC tej firmy. Standard Modbus istnieje w wersji dla portu szeregowego i sieci Ethernet, a protokół umożliwia transmisję w sieciach TCP/IP. Istnieje wiele wariantów standardu Modbus, które są obecnie wykorzystywane, między innymi Modbus RTU (kodowanie danych w formacie binarnym), Modbus ASCII (umożliwiający translację danych na czytelny format), Modbus + (znany jako MB +), który jest własnością firm Modicon i Modbus/TCP, dla sieci Ethernet. Na rysunku 12.16 przedstawiono różne rodzaje połączeń sieciowych dla wymienionych wersji protokołu Modbus i rodzaje topologii tych sieci.

**Rysunek 12.16.**

Przykłady implementacji standardu Modbus

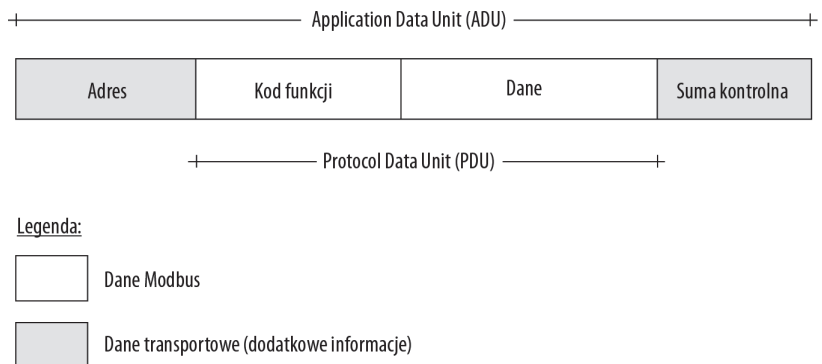


Na rysunku 12.16 przedstawiono różne typy sieci, do których podłączono system oparty na Modbus. Protokół ten uruchomiono za pośrednictwem sieci Ethernet. Powyżej głównego łącza znajdują się trzy switchy, które umożliwiają podłączenie różnych urządzeń (interfejs HMI, układy PLC, pamięć masową i inne urządzenia). Modbus można uruchomić również w sieci innego typu, nie musi to być Ethernet. Na rysunku pierwsza od lewej to implementacja oparta na MB+. Kolejną implementacją jest system zbudowany z wykorzystaniem magistrali szeregowej RS 232, a z prawej strony znajduje się implementacja zrealizowana na bazie szeregowej, półdupleksowej, dwuprzewodowej magistrali RS 485.

We wszystkich wariantach standardu Modbus do zapewnienia poprawności transmisji danych wykorzystano sumy kontrolne. Strumień danych musi być przesyłany bez luk w transmisji. Z tego powodu urządzenia działające w sieci Modbus, odbierając dane, korzystają ze specjalnego bufora, który eliminuje luki. Urządzenia mogą również podjąć decyzję o konieczności retransmisji danych. Rysunek 12.17 przedstawia podstawową ramkę standardu Modbus. Do pola danych w warstwie transportowej dodawane są pola adresu i sumy kontrolnej. Całość stanowi pełną ramkę protokołu (zwaną ADU, ang. *Application Data Unit*). Ramka zawiera pakiety danych PDU (ang. *Protocol Data Unit*), niezależne od warstw komunikacji. Pole kodu funkcji ma wartości z przedziału od 1 do 255, które określają funkcję, jaką należy wykonać na podstawie danych. Pole danych jest przesyłane od klienta do serwera i zawiera dodatkowe informacje, których serwer używa do wykonywania określonych działań. Daną może być adres rejestru, liczba elementów, wartość jakiegoś licznika itp. Pole danych może zostać pominięte, wówczas przesyłany jest kod funkcji, jaką ma podjąć serwer. Funkcja nie wymaga przesłania dodatkowych danych.

### Rysunek 12.17.

Podstawowa ramka  
Modbus



W protokole Modbus urządzenia mają przypisany unikalny adres. Adresacja umożliwia umieszczenie do 247 urządzeń w magistrali. W zależności od zastosowanego typu protokołu Modbus urządzenia działają na zasadzie master-slave lub peer-to-peer (jeśli korzystamy z implementacji standardu Modbus poprzez sieć Ethernet). Tylko urządzenie master może zainicjować transakcję i wysłać polecenie do urządzenia slave (odbiornika). Przykładami typowych poleceń są zmiany ustawień układu PLC lub RTU, odczyt lub zapis danych w rejestrze, odczyt wartości w czasie rzeczywistym z portu wejścia-wyjścia.



Aby zapoznać się szczegółowo ze standardem Modbus, warto odwiedzić witrynę [www.modbus.org/specs.php](http://www.modbus.org/specs.php).

W protokole Modbus (a także w innych protokołach) możemy skorzystać z następujących typów danych:

- ♦ liczba zmiennoprzecinkowa,
- ♦ wartość logiczna,
- ♦ dane w formacie 8-bitowym lub 32-bitowym (tryb 32-bitowy jest rozszerzeniem standardu Modbus),
- ♦ 32-bitowa liczba całkowita,
- ♦ liczba wykładnicza,
- ♦ dane mieszane,
- ♦ słowo 16-bitowe,
- ♦ obiekty BLOB (dostępne w innych protokołach).

Gdybyśmy mieli przełącznik, który może być włączony lub wyłączony, to jego aktualny stan moglibyśmy przechować w rejestrze za pomocą stanów 1 lub 0. Aby zmienić stan, za pośrednictwem urządzenia master możemy wydać polecenie przełączenia odpowiednio na wartość 0 lub 1. Wartość ta będzie następnie generować określone działania, na przykład zmianę napięcia, która powoduje przełączenie stanu.

## Protokoły BACnet i LonTalk

Protokół BACnet (ang. *Building Automation and Control Networks*) jest alternatywą dla protokołu Modbus. BACnet jest otwartym protokołem komunikacji, umożliwiającym współdziałanie systemów sterowania i monitorowania, pochodzącym od różnych producentów. Protokół jest wspierany przez organizacje ANSI, ASHRAE oraz ISO. Standard BACnet pojawił się wcześniej niż standard Modbus, a kiedy został wydany w 1996 r., przyjęło go wielu producentów branży automatyki budynków.

BACnet został zaprojektowany jako protokół obiektowy, w którym wbudowano mechanizm wykrywania atrybutów i zdefiniowano obiekty, do których należą: Analog Output and Value; Binary Input, Output, and Values; Event Enrollment Command; Device; File; Multistate Input and Output; Notification Class; Program; and Schedule. Ramki BACnet mogą być transportowane w sieciach ARCNET, IP, Ethernet, punkt-punkt (P2P na RS 232), Token Ring (Master-Slave przez RS 485), LonTalk. BACnet jest dostawcą niezależnym i nie wymaga specjalnej obsługi sprzętu.

Protokół LonTalk został utworzony przed standardami Modbus i BACnet. Na początku był standardem firmowanym przez Echelon Corporation, teraz jest standardem ANSI. Jest często wymieniany jako alternatywa dla obydwu wspomnianych protokołów i ma zastosowanie w przemyśle, w domu, transporcie i automatyce budynków. Nazwa pochodzi od Local Operating Network (sieci lokalne). Obecnie istnieje wiele procesorów wspierających protokół LonTalk.

## OPC

Technologia OLE firmy Microsoft jest podstawą standardu OPC, przeznaczonego dla szeroko pojętej automatyki. Standardy OPC zostały utworzone w wyniku zapotrzebowania na zintegrowanie serwerów Windows z urządzeniami automatyki, wykorzystywanymi w procesach sterowania produkcją. Standardy OPC są opracowywane przez grupę OPC Foundation ([www.opcfoundation.org](http://www.opcfoundation.org)). Zdefiniowano w nich zestaw metod (interfejsów i protokołów) dostępu do danych z urządzeń znajdujących się w sieci. OPC to otwarty, oparty w dużej mierze na rozwiązaniach firmy Microsoft standard umożliwiający połączenie źródeł danych, takich jak sterowniki PLC, inne sterowniki, porty wejścia-wyjścia, bazy danych z aplikacjami interfejsu HMI.

Podczas gdy Microsoft dokonał rozwoju technologii COM do jej wersji rozproszonej (DCOM), standard OPC również ewoluował. Aplikacje z wykorzystaniem OPC zostały wydane w postaci zestawu kontrolerek ActiveX, które można dodawać do obiektu kontenera. Dzisiaj OPC znajduje się w .NET Framework w wersji OPC-UA, która jest rozwijana.

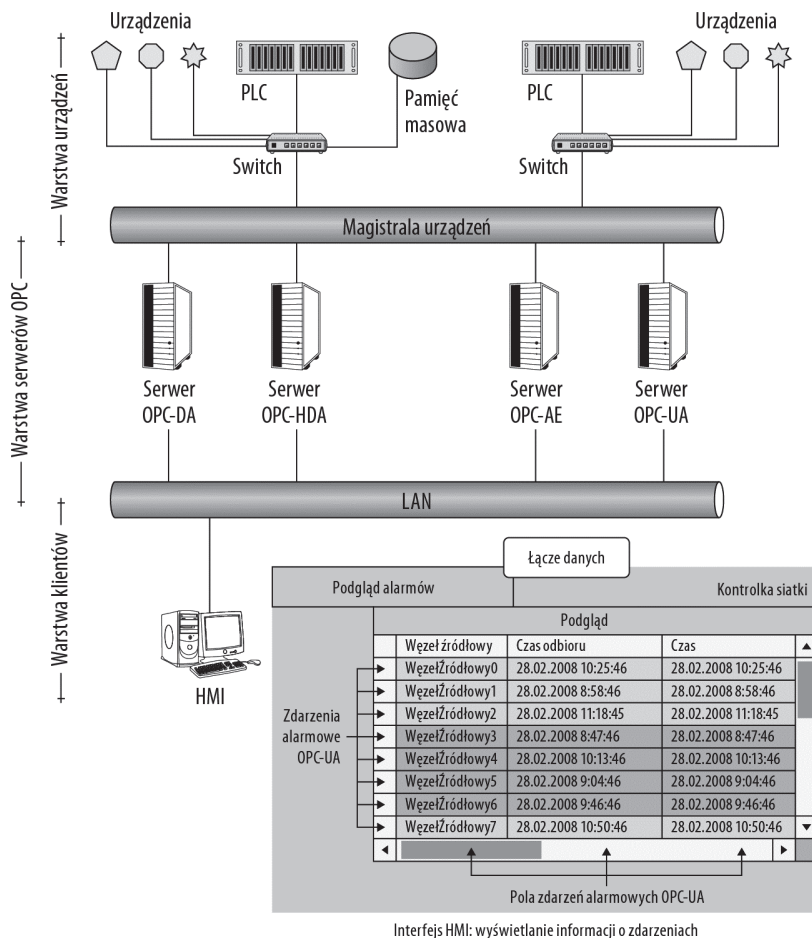
Obecnie istnieją następujące wersje OPC:

- ♦ OPC Data Access (OPC-DA), wykorzystywana do odczytu danych czasu rzeczywistego z urządzeń,
- ♦ OPC Alarm & Events (OPC-AE), umożliwia przetwarzanie zdarzeń,
- ♦ OPC Historical Data Access (OPC-HDA), umożliwia logowanie zdarzeń,
- ♦ OPC Batch, używany do przetwarzania plików wsadowych,
- ♦ OPC Data eXchange, wykorzystywany do komunikacji serwer-serwer, monitoring, zarządzania konfiguracją,
- ♦ OPC Commands, wykorzystywany do przesyłania poleceń sterujących do urządzeń,
- ♦ OPC XML-DA, definiujący sposób reprezentacji danych za pomocą XML,
- ♦ OPC Security, wykorzystywany do zapewniania bezpieczeństwa danych,
- ♦ OPC Complex Data, obsługujący dane binarne i w formacie XML.
- ♦ OPC Unified Architecture, stanowi najnowszą technologię zbudowaną na podstawie .NET Framework.

Najważniejsze z wymienionych wariantów to OPC-DA, OPC-AE i OPC-HDA.

OPC stanowi interfejs pomiędzy klientem a aplikacjami serwera, zapewniający powszechnie znany i dobrze udokumentowany mechanizm przeznaczony do przekazywania danych ze źródła do dowolnej aplikacji klienckiej. Standard określa metody przekazywania danych, a także zapewnia szczegółowe informacje na temat innych atrybutów w celu uzupełnienia danych, takie jak zakres informacji, typ danych, status określonych flag. Serwery OPC gromadzą dane pochodzące z urządzeń, które są zebrane przez układy PLC i udostępniają dane dla klientów znajdujących się w sieci. Rysunek 12.18 przedstawia sieć OPC.

**Rysunek 12.18.**  
Sieć OPC



Na rysunku 12.18 pokazano trójwarstwową sieć OPC. Topologia jest podobna do tej, którą przedstawia rysunek 12.15. Obydwa rysunki różnią się definicją trzech poziomów. W dolnej części znajduje się warstwa klienta z konsolą HMI. W prawym dolnym rogu widać okno z podglądem zdarzeń alarmowych wyświetlanym na monitorze. Klient wysyła dane związane ze zdarzeniami poprzez sieć LAN do serwerów OPC, które reprezentują warstwę pośrednią (ang. *Middleware*). W warstwie serwerów OPC znajdują się cztery najważniejsze typy serwerów (OPC DA, OPC HDA, OPC AE, OPC UA). Te serwery pobierają dane z warstwy urządzeń lub wysyłają odpowiednie polecenia pomiędzy warstwami klientów i urządzeń.

W trakcie rozwoju standardu OPC-UA włączono do niego specyfikacje elementów OPC-AE, OPC-DA, OPC-HDA. OPC-UA to adaptacja architektury SOA do odpowiedniego modelu aplikacji, przestrzeni nazw i systemu bezpieczeństwa zbudowanego w oparciu o architekturę Windows .NET Framework Architecture. OPC-UA posiada następujące funkcjonalności:

- ♦ Buforowanie danych z zapewnieniem dostarczenia poprzez mechanizm potwierdzeń.
- ♦ Redundancja danych, z definicją alternatywnych ścieżek transmisji, przełączania do systemu zapasowego i z wykorzystaniem innych technologii.

- ♦ Sygnał Heartbeat, zapewniający odpowiedni stan połączenia i inne funkcje zależne od czasu.
- ♦ Model zabezpieczeń, który określa mechanizm dostępu do danych OPC na podstawie uwierzytelniania i autoryzacji, gdzie wykorzystuje się szyfrowanie i dostęp poprzez certyfikat i podpis.
- ♦ Adresowanie, które umożliwia powiązanie źródeł danych z wartościami.
- ♦ Kompatybilność dostępu do danych, alarmów i innych serwerów.
- ♦ Usług umożliwiające zarządzanie źródłami danych poprzez sieć lub usługi sieciowe. Komunikacja jest zapewniona za pomocą API standardu OPC-UA (.NET, Java itd.), co umożliwia aplikacjom dostęp do usług.

## Podsumowanie

W tym rozdziale przedstawiono różne rodzaje lokalnych sieci komputerowych i ich technologie. Opisano Ethernet, Token Ring, FDDI, X10 i inne standardy automatyki przemysłowej, a także wszystkie standardy IEEE 802.x. Ethernet to sieć wykorzystująca transmisję ramek w trybie rozgłoszeniowym. W rozdziale wyjaśniono, do czego służą ramki i jak są zbudowane.

Sieci Token Ring wykorzystują specjalne ramki tokenów, dzięki którym zapewniono kontrolę dostępu węzłów do sieci. FDDI to sieci zbudowane w oparciu o pierścienie z zastosowaniem łączy światłowodowych, używane do tworzenia łączy dużej prędkości.

W rozdziale tym przedstawiono też różne standardy automatyki przemysłowej. Standard X10 umożliwia automatyzację domu, w przemyśle wykorzystuje się przeróżne technologie wspomagające monitorowanie urządzeń produkcyjnych i sterowanie nimi. Sieci umożliwiają transmisję danych z czujników, siłowników, przełączników, zaworów i innych urządzeń i sprawiają, że zebrane dane są dostępne dla komputerów z oprogramowaniem zapewniającym monitoring i sterowanie.

W następnym rozdziale omówiono rozległe sieci komputerowe WAN. WAN to zbiór inter-sieci lub sieci z łączami umożliwiającymi transmisje na duże odległości.



# Rozdział 13.

## Sieci szkieletowe i rozległe WAN

### W tym rozdziale:

- ♦ Sieci rozległe WAN
- ♦ Sieci z komutacją obwodów
- ♦ Sieci ISDN i DSL
- ♦ Łączenie sieci WAN za pomocą łączy dużych prędkości i SDH/SONET
- ♦ Sieci z komutacją pakietów
- ♦ Protokoły sieci pakietowych — X.25, ATM, Frame Relay
- ♦ Infrastruktura sieci Internet i Internet2

Sieci WAN (ang. *Wide Area Network* — rozległa sieć komputerowa) to zbiór sieci połączonych ze sobą za pośrednictwem ogólnodostępnych łączy publicznych, zwykle zapewniających pokrycie dużego obszaru geograficznego. Aby zbudować sieć WAN, trzeba zastosować odpowiednie technologie i urządzenia zapewniające routing, przełączanie pakietów i wyznaczanie tras pomiędzy węzłami transmisji. Istnieją cztery rodzaje sieci WAN: sieci z komutacją obwodów, sieci z komutacją pakietów, sieci z komutacją komórek oraz łącza dzierżawione.

Sieć PSTN (ang. *Public Switched Telephone Network* — publiczna sieć telefoniczna) jest przykładem sieci z komutacją obwodów. PSTN to sieć zbudowana hierarchicznie, umożliwia kilka metod łączności w celu transmisji danych; metody te zostaną przedstawione w dalszej części rozdziału. Warto zwrócić uwagę na dwie najpopularniejsze technologie transmisji danych, DSL i ISDN, które będą opisane bardziej szczegółowo. W sieciach szkieletowych wykorzystuje się łącza T i E. W tych sieciach można wyróżnić wiele technologii i standardów umożliwiających transmisję danych z różnymi prędkościami. Najszybsze sieci są budowane w oparciu o kable światłowodowe. Najpopularniejszym protokołem transmisji danych, wykorzystywanym w sieciach szkieletowych, jest SDH/SONET. W sieciach SDH/SONET dane mogą być przesyłane w formie asynchronicznej z zastosowaniem protokołu ATM lub techniki Packet over SONET/SDH (PoS).

W sieciach z komutacją pakietów definiuje się punkty końcowe transmisji (węzeł źródłowy, węzeł docelowy), ale nie ma definicji routingu danego pakietu. Najlepszym przykładem sieci z komutacją pakietów jest Internet. W niniejszym rozdziale zostaną przedstawione protokoły powszechnie wykorzystywane w sieciach pakietowych: X.25, Frame Relay, ATM.

Internet jest zbiorem sieci, w którym głównie występuje ruch TCP/IP. W sieci Internet znajdują się punkty wymiany ruchu internetowego — IXP (ang. *Internet eXchange Point*). Sieć Internet2 to Internet drugiej generacji, działający w oparciu o sieć szkieletową wysokiej prędkości (10 Gb/s). Podstawowe funkcjonalności oferowane przez tę sieć zostaną omówione w dalszej części rozdziału.

## Sieci rozległe WAN

Rozległa sieć komputerowa WAN jest siecią złożoną z mniejszych sieci i ma szeroki zasięg geograficzny. WAN łączy sieci lokalne LAN za pomocą łączy obsługiwanych przez operatorów publicznych. Gdy sieć WAN ma ograniczony zasięg do niewielkiego obszaru geograficznego, na przykład parku przemysłowego lub kampusu uczelni, jest czasem określana jako kampusowa sieć komputerowa CAN (ang. *Campus Area Network*). Sieci WAN obejmujące zasięgiem obszar miasta nazywane są miejskimi sieciami komputerowymi — MAN (ang. *Metropolitan Area Network*). Nazwa WAN jest często stosowana zamiennie z terminami MAN i CAN, aby podkreślić aspekt łączenia wielu sieci. Systemy telefonii stacjonarnej są sieciami WAN, tak samo jak sieć Internet, która jest najlepszym przykładem sieci rozległej.

Istnieją dwa zasadnicze aspekty technologii WAN. Pierwszym z nich jest sposób, w jaki są połączone sieci LAN, i metoda transmisji danych, czyli typ połączenia. Gdy mamy do czynienia z wydajnym połączeniem o wysokiej przepustowości, mówimy o sieci szkieletowej. Często termin *sieć szkieletowa* jest stosowany również w odniesieniu do sieci lokalnych, zapewniających bardzo dużą przepustowość. Drugim istotnym aspektem jest sposób przełączania i routingu. Routery są stosowane w całej sieci, ale te znajdujące się na styku sieci są kluczowe dla określenia właściwości danej sieci WAN. Ten rozdział opisuje różne protokoły sieciowe warstwy drugiej i trzeciej modelu ISO/OSI (warstwa łączy danych i warstwa sieci).

Łączy sieci WAN można zrealizować w oparciu o różne media transmisyjne (nośniki) i przy użyciu różnych protokołów sieciowych. Jeśli w sieci są zdefiniowane łącza z mechanizmem przełączającym „ścieżki transmisji” w razie potrzeby, to mamy do czynienia z *sieciami z komutacją obwodów*.

Alternatywnie można skorzystać z mechanizmu polegającego na definiowaniu węzłów końcowych transmisji, bez sztynnego przypisywania łącza transmisyjnego. W tym przypadku w sieci trzeba zdefiniować dodatkowo funkcjonalność inteligentnego routingu. Tego typu rozwiązanie WAN nosi miano *sieci z komutacją pakietów* lub w uproszczeniu — *sieci pakietowej*, gdzie pakiet jest formą „ujednoliczonego kontenera” różnych typów transmitowanych danych. Podobną technologią do przełączania pakietów jest przełączanie komórek. W tym przypadku dane są umieszczane w swego rodzaju komórkach o stałym rozmiarze, które są przesyłane poprzez określone łącze.

Sieci WAN można podzielić na cztery kategorie:

- ♦ **Sieć z komutacją obwodów.** Ten typ jest wykorzystywany przez operatorów telekomunikacyjnych. Operator używa dedykowanych kanałów pomiędzy punktami końcowymi transmisji. W tym przypadku w protokołach transmisji znajduje się informacja nadmiarowa, służąca do obsługi połączenia. Przykładem protokołu stosowanego w tych sieciach jest PPP.
- ♦ **Sieć z komutacją pakietów.** W sieciach pakietowych WAN tworzy się wirtualne łącza w celu przesłania pakietów pomiędzy węzłami końcowymi. To rozwiązanie pozwala na współdzielenie jednego łącza fizycznego przez wiele systemów. Transmisja jest realizowana w trybie punkt-punkt (unicast) lub multimediami („jeden do wielu”, multicast). Protokoły sieci pakietowych to przede wszystkim X.25, Frame Relay, PoS.
- ♦ **Sieć z komutacją komórek.** Sieci zbudowane w oparciu o komórki<sup>1</sup> danych działają podobnie jak sieci pakietowe. Różnicą jest logiczna jednostka przesyłana w łączu, którą jest w tym przypadku komórka o stałej długości. Technologie komutacji komórek działają z wykorzystaniem technik synchronizacyjnych, wymagających przesyłania informacji nadmiarowych, co w konsekwencji sprawia, że transmisja jest realizowana wolniej. Protokołem związanym z tą technologią jest ATM.
- ♦ **Sieć oparta na łączach dzierżawionych.** Łącze dzierżawione jest dedykowanym połączeniem zestawionym pomiędzy punktami końcowymi transmisji. Ze względu na to, że w tym przypadku wszystkie pakiety trafiają z jednoznacznie określonego punktu źródłowego do punktu docelowego, takie łącze jest bardzo bezpieczne, z reguły szybkie i na ogół kosztowne. Do sterowania transmisją używa się tu protokołów warstwy łącza danych.

Nie można zdefiniować jednego, dominującego typu sieci WAN. W trakcie budowy sieci często wybór wykorzystywanych technologii jest kompromisem kosztu, wymaganej odległości, potrzebnej niezawodności i złożoności. W rezultacie powstało mnóstwo technologii wdrożonych w celu umożliwienia transmisji w sieciach WAN. Wiele z nich było przeznaczonych najpierw dla operatorów telekomunikacyjnych do realizacji usług głosowych, a następnie dostosowanych do świadczenia usług transmisji danych. Niektóre technologie zdefiniowano od razu w celu umożliwienia budowy szybkich sieci. Powstały również rozwiązania, których celem było dostarczenie nowych usług przy zachowaniu wstecznej kompatybilności ze starszymi standardami.

## Sieci z komutacją obwodów

Sieci z komutacją obwodów (komutacją kanałów, łączy) stanowią rozwiązanie, które najwcześniej było stosowane w sieciach WAN. Powstały one z analogowych sieci wykorzystywanych do zapewnienia usług głosowych, które cechowały się niską przepływnością łącza. Systemy telekomunikacyjne są najlepszym przykładem tego rozwiązania,

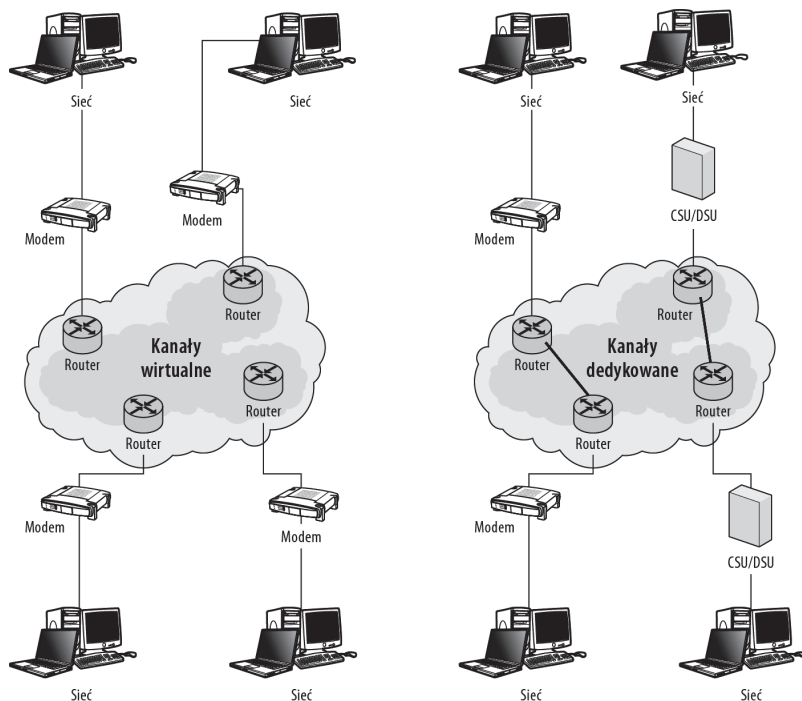
---

<sup>1</sup> Takie sieci można nazwać sieciami komórkowymi, ale ten termin jest zarezerwowany dla telekomunikacyjnych sieci bezprzewodowych i nie będzie tu stosowany — *przyp. tłum.*

ale jeszcze wcześniejszą odmianą tego typu komunikacji były systemy telegraficzne. Za pośrednictwem sieci z komutacją obwodów przesyła się obecnie dane zarówno w formie analogowej, jak i cyfrowej. W sieci można zdefiniować przypisanie danego łącza do określonej trasy transmisji. Taka sieć nosi miano *dedykowanej sieci z komutacją obwodów*, której przykład przedstawia prawa część rysunku 13.1. Istnieją rozwiązania umożliwiające zastosowanie jednego fizycznego łącza z dostępnej puli tylko na czas transmisji danych i tworzenie w ten sposób *połączenia wirtualnego*, którego przykład pokazano w lewej części rysunku 13.1. Łącze dedykowane jest przydzielone na stałe do danej trasy, natomiast łącza wirtualne są tworzone na bieżąco, w zależności od potrzeb. Po dokonaniu transmisji danych połączenie zostaje zerwane, a obwód (kanał, łącze) — zwolniony.

### Rysunek 13.1.

*Kanały wirtualne i dedykowane w sieci z przełączaniem obwodów*



Rysunek 13.1 przedstawia różnice pomiędzy wspomnianymi dwoma rodzajami sieci. Użytkownicy sieci lokalnych mogą łączyć się z dostawcą usług z wykorzystaniem modemów, multiplekserów, jednostek CSU lub DSU. CSU i DSU to interfejsy do sieci rozległej WAN.

W sieci z wykorzystaniem komutacji obwodów przed rozpoczęciem przesyłania danych należy zestawiać łącze transmisyjne. Taki system można traktować jak architekturę chmury, gdzie trasa połączenia jest zestawiana z dostępnych łączy transmisyjnych w systemie. Wyznaczoną trasą są przesyłane dane. Ta trasa jest fachowo nazywana *obwodem transmisyjnym* lub — potocznie — *obwodem*. Sieci z komutacją obwodów nie są efektywne w porównaniu z innymi rozwiązaniami. Pomimo wielu stacji podłączonych do sieci, które współdzielą zestaw dostępnych obwodów, część łączy zawsze jest nieużywana i pozostaje dostępna w puli. Z drugiej strony przypisanie łącza na czas transmisji zapewni odpowiednią gwarancję usługi połączenia, bez konieczności stosowania dodatkowych protokołów warstw wyższych.

Niektóre sieci komutacji pakietów, omówione w dalszej części tego rozdziału, mogą zachowywać się tak, jakby były sieciami z komutacją obwodów.

W sieciach z komutacją obwodów występują pewne opóźnienia, spowodowane czasem potrzebnym na zestawienie połączenia. Z tego powodu większość sieci z komutacją obwodów o wysokiej prędkości transmisji korzysta z dedykowanego kanału sygnalizacyjnego, który służy do zarządzania ruchem w sieci. Dedykowany kanał sygnalizacyjny nie jest wymogiem technologicznym, ale może znacznie usprawnić funkcjonowanie sieci. W sieciach o niskich prędkościach (np. zbudowanych w oparciu o POTS) nie stosuje się dedykowanych kanałów sygnalizacyjnych.

## Sieć telekomunikacyjna PSTN

Sieci cyfrowe umożliwiają współpracę sieci z komutacją obwodów (takich jak POTS) z sieciami pakietowymi, np. TCP/IP. Obie sieci mogą być wykorzystywane do świadczenia usług transmisji głosu, ale ich wymagania są różne.

Sieć PSTN to *publiczna sieć telefoniczna z komutacją obwodów*. PSTN jest regulowana przez standard ITU-T — plan jednolitej numeracji telefonów jest zdefiniowany przez standard ITU-E.164.

W USA sieć telefoniczna była kontrolowana przez firmę AT&T aż do początku lat osiemdziesiątych. Firma AT&T zbudowała w USA sieć telefoniczną, tworząc hierarchiczną strukturę, która zawierała pięć poziomów (lub klas). Odpowiednią centralę obszarową reprezentował trzycyfrowy prefiks, po którym podawano siedmiocyfrowy numer telefonu obsługiwany przez biura klasy 5. W tamtych czasach istniało około 20 000 ośrodków zarządzania połączeniami numerów tej klasy. Łączy klasy 5. były agregowane w centralach biur rozliczeń klasy 4., a te z kolei były łączone w ośrodkach klasy 3. (gdzie zarządzano kodami obszaru). Klasę 2. stanowiły centrale regionalne, połączone z ośrodkiem centralnym (klasa 1.). Centrale klasy 1. były połączone z centralą międzynarodową. Tę hierarchię sieci ilustruje rysunek 13.2.

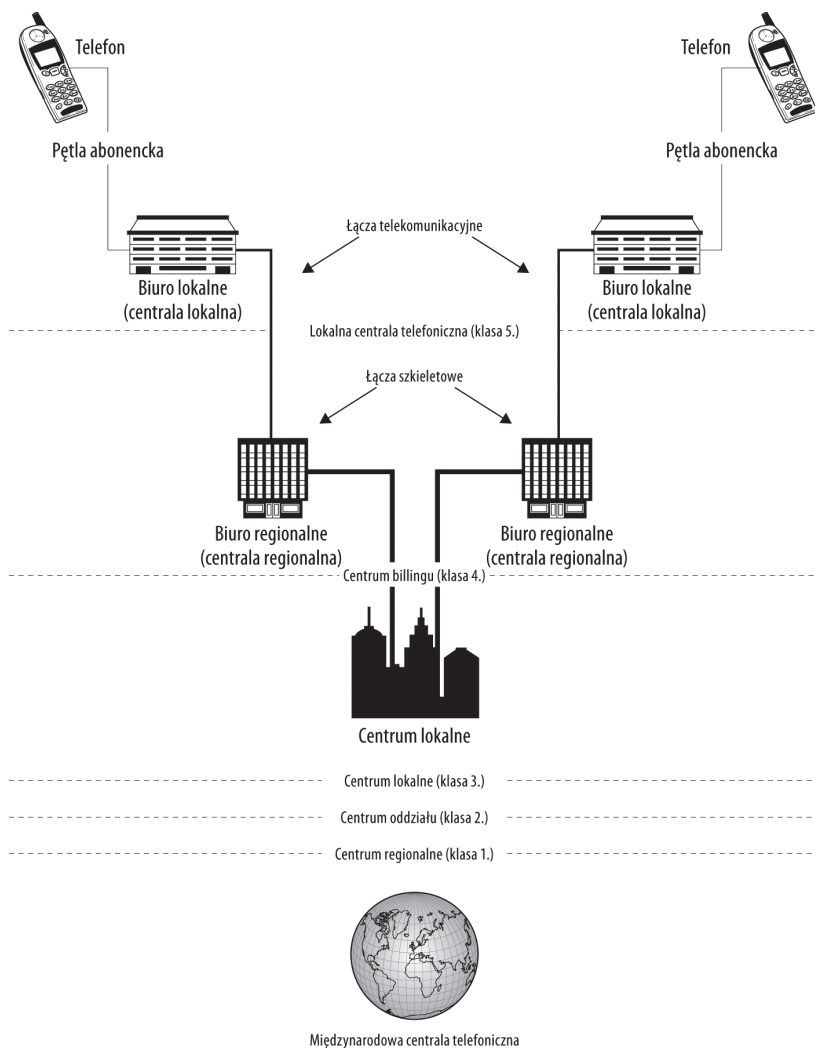
1 stycznia 1984 r. koncern AT&T został podzielony tak, aby utworzyć grupę siedmiu niezależnych firm regionalnych, zwaną RBOC:

- ♦ Ameritech
- ♦ Bell Atlantic
- ♦ BellSouth
- ♦ NYNEX
- ♦ Pacific Telesis
- ♦ Southwestern Bell
- ♦ US West

Były jeszcze dwa dodatkowe ośrodki, które nie należały do grupy RBOC: Cincinnati Bell i SNET; koncern AT&T posiadał w nich udziały mniejszościowe.

**Rysunek 13.2.**

Pierwotna  
hierarchiczna  
struktura sieci AT&T



Rozpad korporacji spowodował, że w hierarchii straciły znaczenie ośrodki klas 1. – 3. Klasy 4. i 5. nadal są w użyciu. Po rozpadzie firmy grupy RBOC wspólnie przygotowywały szereg nowych protokołów sieciowych, które można było wykorzystywać w ich obrębie. Wiele z nich zostało opracowanych przez Bellcore.



Więcej informacji związanych z procesem rozwoju spółek grupy RBOC można znaleźć w witrynie: [http://en.wikipedia.org/wiki/Bell\\_System\\_divestiture](http://en.wikipedia.org/wiki/Bell_System_divestiture).

Firmy telekomunikacyjne w USA zostały poddane znacznej konsolidacji, obecnie istnieją następujące:

- ♦ **AT&T** — pierwotnie Southwestern Bell, który nabył AT&T i przejął tę nazwę. Firma nabyła również spółkę BellSouth.

- ♦ **Qwest** — US West został przejęty przez Qwest.
- ♦ **SBC** — Southwestern Bell zmienił nazwę na SBC i nabył Ameritech i Pacific Telesis.
- ♦ **Verizon** — pierwotnie spółka o nazwie Bell Atlantic. To konsorcjum nabyło GTE i NYNEX.

W sieciach z komutacją obwodów łącze jest ustanowione pomiędzy komputerami końcowymi na czas przesyłania danych. W zależności od warunków panujących w sieci łącze może być zestawiane w inny sposób, ale pozostanie zestawione na czas trwania transmisji. Sieci z komutacją obwodów są sieciami z określonym stanem, co sprawia, że ich pojemność jest ograniczona przez liczbę dostępnych łączy. Każde łącze fizyczne może obsłużyć wiele połączeń, ale jest ograniczone.

W sieciach z komutacją pakietów dane są dzielone na odpowiednie bloki i umieszczane w pakietach, które są przesyłane poprzez wirtualne połączenia pomiędzy komputerami końcowymi. Ścieżka pomiędzy punktami transmisji pakietu nie jest istotna. Każdy z pakietów przesyłany pomiędzy dwoma określonymi punktami może mieć inną ścieżkę transmisji. W tym przypadku najważniejsze jest poprawne złożenie pakietów w miejscu docelowym. Sieć pakietowa jest bezstanowa, a jej pojemność ogranicza szybkość transmisji danych i efektywność użytych metod kodowania danych.

W kolejnych podrozdziałach opisano powszechnie stosowaną technologię sieci komutowanych: sieć cyfrową z integracją usług (ang. *Integrated Services Digital Network* — ISDN), oraz technologię wykorzystującą infrastrukturę PSTN — pary przewodów miedzianych: cyfrową linię abonencką (ang. *Digital Subscriber Line* — DSL).

## ISDN

Sieć cyfrowa z integracją usług ISDN to technologia umożliwiająca transmisję danych cyfrowych w sieci z komutacją obwodów. ISDN pozwala firmom świadczącym usługi telekomunikacyjne na realizację usług zarówno łączności głosowej, jak i transmisji danych za pośrednictwem jednej linii. Użytkownicy ISDN mogą wykupić usługi transmisji danych o prędkości wynoszącej zwykle 128 kb/s. Łącza ISDN są tworzone z wykorzystaniem kanałów o szerokości 64 kb/s.

Urządzenia zgodne z normami ISDN są włączane do PSTN za pośrednictwem zakończenia sieciowego (NT1 lub NT1 i NT2). Aby podłączyć urządzenia niezgodne (telefon analogowy, modem analogowy), należy za NT1 zainstalować TA (ang. *terminal adapter*). Dostęp do Internetu poprzez ISDN jest realizowany jako usługa wdzwaniana (dial-up). Aby uzyskać dostęp do sieci, modem ISDN wybiera numer usługi i łączy się ze zdalnym routerem.

ISDN jest jedną z pierwszych form połączeń szerokopasmowych dostępnych dla gospodarstw domowych, położonych w odległości mniejszej niż 5,5 km od centrali telefonicznej. W przypadku gospodarstw znajdujących się dalej należy zastosować odpowiednie urządzenia wzmacniające, co podnosi koszt realizacji usługi.

W sieciach ISDN są zdefiniowane trzy następujące rodzaje dostępu:

- ♦ **Podstawowy BRI (ang. *Basic Rate Interface*)**, o przepustowości 144 kb/s, składający się z dwóch cyfrowych kanałów transmisyjnych: B (ang. *Bearer Channel*), o przepustowości 64 kb/s każdy, i cyfrowego kanału sygnalizacyjnego: D (ang. *Delta Channel*), o przepustowości 16 kb/s. W tym dostępie wykorzystuje się dwu- lub czteroprzewodowe kable. Interfejs jest stosowany jako łącze szeregowe z modemem lub pomiędzy urządzeniem a TA.
- ♦ **Pierwotny PRI (ang. *Primary Rate Interface*)**, o przepustowości 2048 kb/s (30 kanałów B, kanał D i kanał synchronizacji po 64 kb/s) lub 1544 kb/s (23 kanały B i kanał D po 64 kb/s plus 8 kb/s, synchronizacja), czyli składający się z traktu E1 (lub T1 w USA). Dostęp PRI jest używany na całym świecie, głównie do podłączania systemów PBX do sieci telefonicznej.
- ♦ **Dostęp przez sieć B-ISDN (ang. *Broadband ISDN*)**, która jest rozwinięciem klasycznej sieci ISDN, opracowanym w 1980 roku w celu umożliwienia wysyłania treści multimedialnych, takich jak wideo na żądanie czy telewizja, oraz usług szybkiej transmisji danych, przeznaczonych głównie dla firm i organizacji naukowych, takich jak uniwersytety i laboratoria badawcze. Sieci B-ISDN nie odniosły dużego sukcesu na rynku, obecnie można rzadko je spotkać.

W sieciach ISDN można łączyć kanały B w tak zwane *kanały H*, w następujący sposób:

- ♦ H0 to 6 połączonych kanałów B o przepustowości łącznej 384 kb/s
- ♦ H10 to 23 połączone kanały B o przepustowości łącznej 1472 kb/s
- ♦ H11 to 24 połączone kanały B o przepustowości łącznej 1536 kb/s
- ♦ H12 to 30 połączone kanały B o przepustowości łącznej 1920 kb/s

Kanał H12 jest dostępny tylko w sieci E1, głównie w Europie.

Kiedy ISDN został wprowadzony w 1990 roku, przemysł telekomunikacyjny spodziewał się rozwoju rynku połączeń z Internetem. Standard odniósł średni sukces w USA, lepsze wyniki odnotowano w Europie, ale oczekiwania operatorów nie zostały spełnione. Interfejs PRI jest powszechnie stosowany w połączeniach telefonicznych, ale łączy BRI, które zoptymalizowano pod kątem przesyłania danych, są droższe i mniej popularne niż DSL.

Omówiliśmy pokrótce wariant szerokopasmowej sieci ISDN — B-ISDN. Warianty ISDN, wymienione wcześniej w niniejszym rozdziale, są klasyfikowane jako ISDN wąskopasmowy (N-ISDN).

## DSL

Cyfrowa linia abonencka DSL (ang. *Digital Subscriber Line*) jest jedną z najpopularniejszych metod stosowanych dzisiaj do zapewnienia łączności z Internetem za pośrednictwem linii telefonicznej. Jej jedyną rywalką jest metoda dostępu do sieci za pośrednictwem telewizji kablowej. Być może w przyszłości technologia WiMAX (802.16) wyprze tę technologię. DSL został wprowadzony w 1998 r.

Najbardziej rozpowszechnioną wersją DSL jest *asymetryczne DSL (ADSL)*, sporadycznie spotyka się wariant symetryczny SDSL omawianego rozwiązania. ADSL działa z prędkością od 512 kb/s do 20 Mb/s (pobieranie danych) i 256 kb/s do 1 Mb/s (wysyłanie danych), gdzie dana prędkość jest związana z wymaganym stopniem jakości usług zamówionym od dostawcy oraz ze stanem technicznym linii telefonicznej. Asymetryczność łączy wynika z faktu, że przez większość czasu użytkownicy pobierają dane. Dzięki temu usługodawca może lepiej wykorzystać infrastrukturę sieciową i poprawić jakość realizowanych usług, co zapewnia zadowolenie klientów.

W DSL niezwykle ważnym czynnikiem jest odległość. DSL wymaga, aby abonent znajdował się w odległości maksymalnie 3,4 km lub 5,5 km od centrali. Wymóg ten dotyczy także systemu ISDN. Odległość ta może zostać przedłużona przez operatora poprzez zastosowanie łącza światłowodowego pomiędzy centralą a pętlą abonencką. Instalacja odpowiednich regeneratorów może również zwiększyć zasięg DSL. Innym ważnym czynnikiem jest jakość drutu miedzianego. Lepsze kable zapewniają lepsze parametry, takie jak tłumienność czy odległość sygnału do szumu.

W sieci ADSL prędkość pobierania jest większa od prędkości wysyłania, podczas gdy w SDSL prędkość transmisji jest taka sama w obu kierunkach. Technologię DSL na początku wdrażano w oparciu o ISDN i ta wersja nosi nazwę IDSL (ISDN DSL). ADSL można uruchomić z wykorzystaniem nie tylko zwykłej linii telefonicznej, ale również układów ISDN BRI.

ADSL wykorzystuje pętlę abonencką, znaną z systemu podstawowej telefonii POTS, z zastosowaniem kanału o wyższej częstotliwości. Użycie pasma wyższej częstotliwości powoduje, że sygnały standardowej usługi głosowej i ADSL nie doznają interferencji. Modem ADSL jest w rzeczywistości jednostką transmisyjną ATU-R (ang. *ADSL Terminal Unit-Remote*), którą można podłączyć z firewallem, routerem, gatewayem lub komputerem, korzystając ze złącza Ethernet lub USB. W większości przypadków ludzie decydują się na połączenia Ethernet.

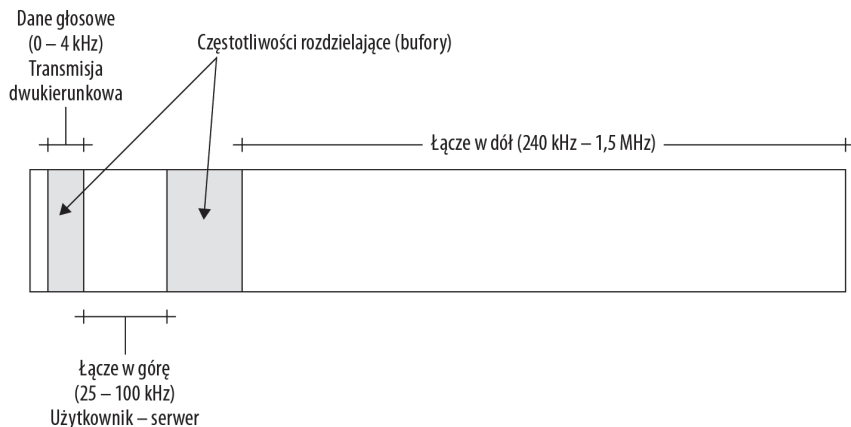
Zazwyczaj usługi głosowe są przesyłane w paśmie poniżej 4 kHz, a usługi danych w paśmie powyżej 24 kHz. W celu zapewnienia poprawnej transmisji obydwu sygnałów instaluje się po stronie abonenta filtr dolnoprzepustowy, który jest umieszczany między linią telefoniczną a aparatem telefonicznym. Ten filtr tłumi wszystkie sygnały powyżej 4 kHz (górnej granicy pasma usług głosowych).

Niektóre typy DSL wymagają instalacji rozdzielacza sygnałów (tzw. splittera). Terminy ADSL Lite, G. Lite i Universal ADSL odnoszą się do tych technologii ADSL, które nie wymagają użycia rozdzielacza. W systemach wymagających rozdzielacza stosuje się jedną z dwóch metod. Pierwszą z nich jest wykorzystanie amplitudowo-fazowej modulacji bez fali nośnej<sup>2</sup>, którą przedstawiono na rysunku 13.3. W tej metodzie sygnał dzieli się na trzy pasma:

---

<sup>2</sup> Amplitudowo-fazowa modulacja bez fali nośnej (znana również jako modulacja CAP) jest odmianą kwadraturowej modulacji amplitudy (QAM). Różne implementacje modulacji CAP umożliwiają zmianę zarówno głębokości modulacji, jak i prędkości transmisji w celu dostosowania się do warunków panujących w linii telefonicznej (medium transmisyjnym). Modulacja CAP jest wypierana przez modulację wielotonową DMT (ang. *discrete multitone modulation*), znacznie częściej stosowaną w liniach telefonicznych z usługą ADSL — *przyp. tłum.*

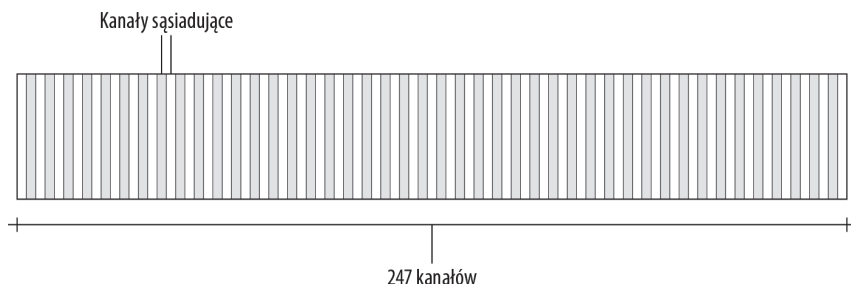
**Rysunek 13.3.**  
Modulacja CAP



- ♦ Usługi telefoniczne (głosowe) są przenoszone w paśmie od 0 do 4 kHz (podobnie jak POTS).
- ♦ Kanał łączności w górę (od użytkownika do serwera) jest przenoszony w paśmie od 25 do 160 kHz.
- ♦ Kanał łączności w dół (od serwera do użytkownika) zaczyna się od częstotliwości 240 kHz. Górna częstotliwość kanału jest zmienna i zależy od warunków panujących w linii (długość linii, zaszumienie, liczba użytkowników korzystających z centrali) z maksymalną wartością około 1,5 MHz.

Alternatywą dla modulacji CAP jest *modulacja wielotonowa* DMT. Tę modulację przedstawiono na rysunku 13.4. W DMT podzielono pasmo na 247 równych kanałów o szerokości 4 kHz. Każdy z kanałów jest monitorowany w celu zapewnienia dobrych parametrów sygnału. W trakcie pogorszenia warunków transmisji w danym kanale następuje przeniesienie sygnału do innego kanału, aby zapewnić odpowiednią przepustowość i jakość transmisji. Niższe częstotliwości (około 8 kHz) są używane do zapewnienia transmisji dwukierunkowej. Modulacja CAP wymaga dużego nakładu na przetwarzanie sygnałów, ale jest efektywniejsza niż DMT, jeśli chodzi o wykorzystanie przepustowości łącza. Większość dostawców ADSL używa systemów działających w oparciu o DMT.

**Rysunek 13.4.**  
Modulacja wielotonowa DMT



W tabeli 13.1 podsumowano różne warianty DSL, które są dostępne na całym świecie, wraz z ich prędkościami, wymaganiami i ograniczeniami.

**Tabela 13.1.** Rodzaje i charakterystyka usług DSL

Typ DSL	Opis	Prędkość transmisji (pobieranie; wysyłanie)	Maksymalna odległość	Zastosowanie
ADSL <sup>1</sup>	DSL asymetryczny	do 8 Mb/s; do 1 Mb/s	1,5 Mb/s – 5,5 km, 2 Mb/s – 4,9 km, 6 Mb/s – 3,6 km, 8 Mb/s – 2,7 km	Używane do zapewnienia dostępu do Internetu, transmisji video, usług VOD, zdalny dostęp do sieci lokalnych.
ADSL Lite (G.Lite) <sup>1</sup>	DSL asymetryczny, bez splittera	od 1,5 Mb/s do 6 MB/s	5,5 km	Standardowa usługa ADSL; zmniejszona przepustowość kosztem braku rozdzielacza.
ADSL2 <sup>1</sup>	DSL asymetryczny	do 12 Mb/s; do 1 Mb/s, do 3,5 Mb/s dla Annex J	2 Mb/s – 4,5 km 6 Mb/s – 3,3 km 10 Mb/s – 2,1 km 12 Mb/s – 1,3 km	Używane do zapewnienia dostępu do Internetu, transmisji video, usług VOD, zdalny dostęp do sieci lokalnych.
ADSL2+ <sup>1</sup>	DSL asymetryczny	do 24 Mb/s; do 1 Mb/s, do 3,5 Mb/s dla Annex M	2 Mb/s – 4,5 km 8 Mb/s – 3,1 km 18 Mb/s – 1,9 km 24 Mb/s – 0,9 km	Używane do zapewnienia dostępu do Internetu, transmisji video, usług VOD, zdalny dostęp do sieci lokalnych.
HDSL <sup>2</sup>	DSL głównie wykorzystywany do dostarczania linii E1/T1	2 Mb/s na jednej parze lub dwóch parach przewodów miedzianych (trzech parach w starszych implementacjach)	5,5 km	Dostarczanie E1/T1 dla ISDN-PRA, do abonenckich central telefonicznych lub łącza WAN do firm.
IDSL <sup>2</sup>	Łącza DSL oparte na technologiach ISDN	128 Kb/s	5,5 km	Podobnie jak usługa ISDN BRI, ale tylko transmisja danych (bez usług głosowych).
SDSL <sup>2</sup>	Symetryczny DSL	2,3 Mb/s w obu kierunkach	3 km	Używana do tworzenia sieci WAN.
VDSL <sup>2</sup>	Bardzo szybki DSL (ang. <i>Very High Speed DSL</i> )	12,9 – 52,8 Mb/s; 1,5 – 2,8 Mb/s	1,3 km – 12,96 Mb/s; 900 m – 25,82 Mb/s; 300 m – 52,85 Mb/s	Sieci ATM, połączenie światłowodowe bardzo szybkie, ale na niewielkich odległościach.
VDSL2 <sup>2</sup>	Bardzo szybki DSL 2 (ang. <i>Very High Speed DSL 2</i> )	do 200 Mb/s w obu kierunkach	300 m – 200 Mb/s, 500 m – do 100 Mb/s, 1 km – do 50 Mb/s	Triple play — jednocześnie dostarczanie Internetu, telewizji wysokiej rozdzielczości i usług telefonicznych.

<sup>1)</sup> Usługa może być realizowana na tej samej parze przewodów miedzianych z usługami głosowymi.

<sup>2)</sup> Usługa musi być realizowana na dedykowanej parze przewodów miedzianych.

Wraz z rozpowszechnieniem się telefonii komórkowej coraz więcej ludzi w Europie decyduje się na posiadanie tylko telefonów komórkowych, rezygnując z telefonów stacjonarnych. Konsekwencją tego stanu rzeczy jest uchwała Parlamentu Europejskiego nakazująca firmom telekomunikacyjnym oferowanie usług transmisji danych bez konieczności wykupu usługi telefonii stacjonarnej. W Polsce odpowiednie zalecenia nałożył na operatorów Urząd Komunikacji Elektronicznej.

Abonenci korzystający z dostępu DSL za pośrednictwem zwykłych linii abonenckich są podłączeni do sieci szkieletowych za pośrednictwem multipleksera DSLAM. Urządzenie to jest zwykle umieszczane w centralach telefonicznych i realizuje multipleksację danych, pochodzących od wielu użytkowników, w ramach protokołu ATM, Frame Relay. Niektóre urządzenia DSLAM umożliwiają multipleksację na różne sposoby.

## Sieć telewizji kablowej

Dostęp do sieci za pośrednictwem telewizji kablowej jest porównywalny z dostępem realizowanym z zastosowaniem DSL. Dostawcy usług telewizji kablowej obecnie tworzą sieci hybrydowe HFC (ang. *Hybrid fibre-coaxial* — hybrydowe sieci oparte na kablach światłowodowych i koncentrycznych). Magistrała doprowadzająca sygnał na dany obszar jest realizowana z wykorzystaniem kabli światłowodowych, następnie sygnał jest konwertowany na postać elektryczną i dostarczany do abonenta kablami koncentrycznymi. W nowszych rozwiązaniach sygnał jest przekazywany kablem światłowodowym bliżej odbiorcy usługi, np. do budynku, w którym następuje konwersja sygnału i dostarczenie go do abonenta. Modemy kablowe spełniają wymagania standardu DOCSIS (ang. *Data Over Cable Service Interface Specification* — standard transmisji danych w hybrydowych sieciach kablowych) głównie w USA; w Europie jest to standard EuroDOCSIS, ale konkretne implementacje zależą od usługodawców.

Sieci kablowe są sieciami współdzielonych obwodów, co oznacza, że wszystkie dane są transmitowane z wykorzystaniem danego obwodu. W tych sieciach istotnym problemem jest zabezpieczenie transmisji, bo dane przesyłane w jednej, wspólnej sieci są potencjalnie dostępne dla innych użytkowników sieci. Modemy kablowe umożliwiają bardzo szybką transmisję danych; najnowsza specyfikacja EuroDOCSIS 3.0 pozwala na osiągnięcie przepływności 120 Mb/s w kierunku do użytkownika i 10 Mb/s w kierunku do sieci. Funkcjonalności sieci rozległych WAN w sieciach kablowych są realizowane z zastosowaniem innych technologii, przedstawionych w niniejszym rozdziale.

## Łacza T i E

Zarówno w sieciach z komutacją obwodów, jak i w sieciach z komutacją pakietów wykorzystuje się koncepcję kanałów w celu zwiększenia przepustowości sieci. Kanał jest swego rodzaju ścieżką przez medium transmisyjne, utworzoną przez fizyczną separację z zastosowaniem wieloprzewodowego kabla albo przez separację elektryczną, z użyciem na przykład zwielokrotnienia (multipleksacji) kanału z podziałem czasu TDM lub zwielokrotnienia kanału z podziałem częstotliwości FDM. Zwielokrotnienie FDM zrealizowane w kablu światłowodowym jest nazywane zwielokrotnieniem optycznym lub zwielokrotnieniem długości fali (odpowiednio ODM lub WDM).

W technice FDM całe pasmo częstotliwości jest podzielone na przedziały, które nazywa się kanałami logicznymi. Przykładem użycia techniki FDM jest radio FM, gdzie każda stacja ma przydzieloną odpowiednią częstotliwość. Podczas korzystania z okularów stereoskopowych, które umożliwiają oglądanie filmów 3D, na ekranie wyświetla się naprzemiennie klatki obrazu przeznaczonego dla prawego i lewego oka. Stereoskopia jest dobrym przykładem zastosowania techniki TDM w praktyce.

Międzykontynentalny system połączeniowy, zbudowany w połowie XX wieku, umożliwia transmisję tysięcy multipleksowanych połączeń głosowych na duże odległości z wykorzystaniem techniki FDM. Innym przykładem zastosowania tej techniki jest system zbudowany przez firmę Bell, umożliwiający 12 połączeń (z modulacją dwuwstęgową) lub 24 połączenia (z modulacją jednowstęgową) za pośrednictwem czterech przewodów. W celu zapewnienia odpowiedniej jakości transmisji trzeba było wzmacniać sygnał co 10 km. Jeszcze innym przykładem zastosowania FDM jest modulacja wielotonowa DMT, wykorzystywana w technologii DSL.

W nowoczesnych sieciach telefonicznych wykorzystuje się zwielokrotnienie TDM. TDM to metoda stosowana w systemach z modulacją impulsowo-kodową PCM, której użyto do tworzenia systemów plezjochronicznych PDH. Modulacja PCM jest stosowana w większości sieci cyfrowych.

Łącze E1 pracuje na dwóch oddzielnych zestawach kabli z wykorzystaniem skrętki. Sygnał w postaci analogowej jest zamieniany na postać cyfrową za pośrednictwem odpowiedniego kodeka. Pojedyncza ramka danych na łączu E1 jest podzielona na 32 przedziały czasowe, zwane szczelinami lub kanałami, które są oznaczane jako TS0 – TS31. W telekomunikacji używa się przeróżnych kodeków w celu konwersji sygnału na postać cyfrową, w tym przypadku najistotniejszy jest proces konwersji i umieszczenia sygnału źródłowego w jednym z kanałów. Zestaw kanałów tworzy ramkę, której transmisja trwa 125  $\mu$ s. W każdej szczelinie czasowej przesyła się 8 bitów informacji, przepustowość pojedynczego kanału wynosi 64 kb/s, a przepustowość całego łącza to 2048 kb/s. W USA i Kanadzie mają zastosowanie łącza T1, gdzie przesyła się 24 kanały (przepustowość łącza wynosi 1,54 Mbit/s).

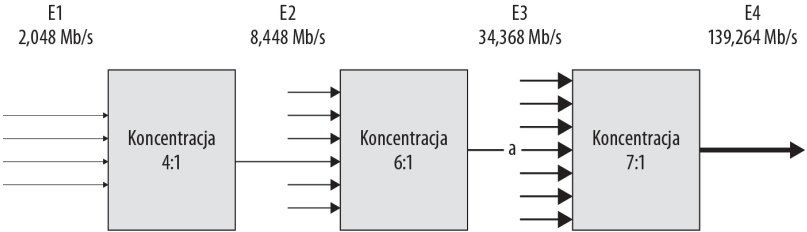
Aby zapewnić dostateczne pokrycie sieci telefonicznych oraz efektywne wykorzystanie łączy, zdefiniowano plezjochroniczną hierarchię cyfrową PDH, określającą sposób zwielokrotnienia kanałów cyfrowych. W Europie wygląda to następująco:

- ♦ cztery trakty E1 o przepływności 2,048 Mb/s są agregowane do kanału E2 o przepływności 8,448 Mb/s;
- ♦ cztery kanały E2 tworzą kanał E3 o przepływności 34,368 Mb/s;
- ♦ cztery kanały E3 tworzą kanał E4 o przepływności 139,264 Mb/s.

Rysunek 13.5 przedstawia zwielokrotnienie kanałów systemu europejskiego.

W USA odpowiednikiem europejskiego łącza E jest trakt T. Łącze T zostało ustandaryzowane przez ITU-T, podobnie jak trakt E został zatwierdzony przez europejski urząd CEPT. W tabeli 13.2 porównano łącza E z łączami T. W USA najczęściej wykorzystuje się łącza T1 i T3.

**Rysunek 13.5.**  
Sposób łączenia  
kanałów



**Tabela 13.2.** Prędkości transmisji w standardach T i E

Standard T	Standard E	DS	Przepływność	Liczba kanałów głosowych
FT1	E0	DS0	64 kb/s	1
T1		DS1	1,54 Mb/s	24
	E1		2,05 Mb/s	30
T2		DS2	6,31 Mb/s	96
	E2		8,45 Mb/s	120
	E3		34,37 Mb/s	480
T3		DS3	44,38 Mb/s	672
	E4		139,27 Mb/s	1 920
T4		DS4	274,18 Mb/s	4 032
	E5		565,15 Mb/s	7 680

Łącza E są używane w Europie, a łącza T — w USA i Kanadzie.

W przypadku cyfrowej sieci telefonii standard PCM jest używany do przekazywania kilku połączeń w kablu dwu- lub czteroprzewodowym (trakty E lub T) lub światłowodzie. W sieciach SONET i SDH stosuje się czasową technikę wielodostępu do medium — TDM. Sieci SDH/SONET są wykorzystywane jako magistrale ruchu internetowego, ponieważ umożliwiają przesyłanie danych kilku dostawców usług w jednym światłowodzie. System bezprzewodowy telefonii GSM używa również technologii TDM.

## Sieci SONET/SDH

Sieci SONET (ang. *Synchronous Optical Network* — synchroniczna sieć optyczna) są oparte na wielodostępie czasowym TDM i są często używane w telekomunikacji. Standard SONET polega na przesyłaniu danych w kablach światłowodowych. Dane cyfrowe są wprowadzane do medium poprzez lasery impulsowe lub diody elektroluminescencyjne (LED). Sieci SONET są stosowane w sieciach telefonicznych jako magistrale internetowe.

Standard SONET powstał w wyniku badań przeprowadzonych przez instytut Bellcore Baby w 1985 roku. Kilka lat później w Komitecie CCITT dodano kilka rozszerzeń i opracowano odmianę SONET, która stała się technologią SDH (ang. *Synchronous Digital Hierarchy* — synchroniczna hierarchia cyfrowa). Czysta forma standardu SONET jest wykorzystywana w Ameryce Północnej, a technologia SDH jest stosowana na całym świecie. Warto wspomnieć, że obydwie technologie mogą być wykorzystane w tej samej sieci fizycznej.

Standard SONET/SDH określa również normy związane z medium fizycznym, między innymi prędkość transmisji, stopień maksymalnego rozszynchronizowania, parametry izolacji kabla i korekcji sygnału, jak również zestaw protokołów zarządzania siecią, na przykład język TL1. Urządzenia sieci SONET/SDH są zarządzane za pomocą aplikacji używającej SNMP lub innego protokołu zarządzania.



Frame Relay, ATM i PoS opisano szczegółowo w kolejnych podrozdziałach.

SONET/SDH został zaprojektowany do przesyłania danych głosowych, które całkowicie wypełniają segment 64 kb/s. Dane o zmiennej wielkości, takie jak pakiety, są przesyłane w szczelinach czasowych, gdzie dowolne dane dopełniają pozostałe wolne miejsca w szczelinach czasowych, gdy sieć nie jest wykorzystywana w 100 procentach. To prowadzi do nieefektywności. Rozwiązaniem tego problemu było opracowanie technologii Frame Relay, w której łączenie danych i wypełnianie segmentów SONET jest realizowane z zastosowaniem multipleksowania statystycznego.

Frame Relay nie daje zadowalającej jakości usług QoS i nie może obsługiwać transmisji wymagających większych przepustowości. Problemy Frame Relay rozwiązuje protokół ATM, w którym zaimplementowano odpowiedni mechanizm zapewniający QoS w celu zabezpieczenia jakości połączenia w sieciach światłowodowych. ATM jest obecnie używany w większości sieci SONET/SDH i spełnia wymagania sieci optycznych o średnich prędkościach transmisji. W szybszych sieciach ATM wykazuje problemy związane z narzutem w komórkach transportowych, powstałym z translacji innych protokołów, takich jak Ethernet. Jeśli ramka z danymi nie wypełni komórki transportowej, pozostałe miejsce będzie wypełnione innymi bitami, nieprzenoszącymi żadnej informacji. To sprawia, że przy bardzo dużych prędkościach transmisji ATM jest nieefektywny.

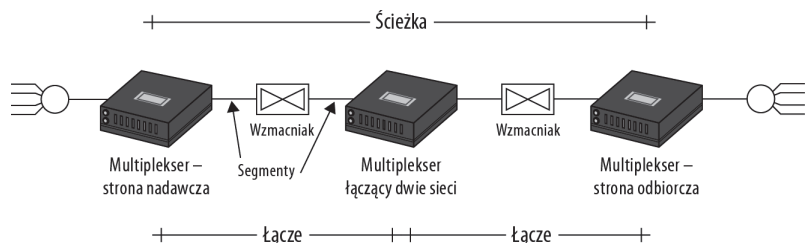
W sieciach optycznych wyższych prędkości, które będą przyszłością sieci szkieletowych WAN, częściej będzie się wykorzystywać protokół PoS. ATM i PoS mogą działać w tej samej sieci SONET/SDH, ponieważ nie wykluczają się wzajemnie.

## Architektura SONET/SDH

Sieci SONET/SDH są realizowane w strukturze pierścieniowej. Połączenie SONET/SDH nazywa się *ścieżką*, a każda część połączenia to *sekcja*. W celu utrzymania odpowiednio wysokiej mocy sygnału w całej długości ścieżki transmisji wykorzystuje się wzmacniaki. System opiera się na multipleksach, stawianych co najmniej w punkcie początkowym i końcowym transmisji. Każde połączenie między multipleksami nazywa się *łączeniem*. Rysunek 13.6 przedstawia diagram toru.

**Rysunek 13.6.**

*Ścieżka, łącze i sekcja w sieci SONET/SDH*



SONET/SDH korzysta z trzech różnych topologii sieci (rysunek 13.7):

- ♦ **Topologia LAPS** z zastosowaniem protokołu automatycznego przełączania. Składa się z czterech światłowodów jednokierunkowych: dwóch działających w każdym kierunku transmisji oraz dwóch światłowodów ochronnych. Przełączanie jest realizowane łącznie za łączem (po kolei), na zasadzie negocjacji.

Na rysunku 13.7 strzałki wskazują kierunek transmisji. Ścieżka główna to czarna strzałka, ścieżkę zapasową przedstawiono jako linię przerywaną z białą strzałką. W rozwiązaniu tym są dwa przełączniki, dzięki czemu transmisja jest zachowana nawet w przypadku awarii jednego z nich.

- ♦ **Topologia UPSR** — składa się z dwóch ścieżek, formujących strukturę pierścienia. Podczas gdy ścieżka robocza pierścienia jest w użyciu, druga odgrywa rolę medium zapasowego, aktywowanego w razie awarii. W sieciach SDH ten typ architektury nosi nazwę łącza zapasowego SNCP, ale w przypadku SDH mamy do czynienia z topologią kraty, a nie pierścienia.
- ♦ **Topologia BLSR**. Jest to dwu- lub czterokablowa sieć światłowodowa dwukierunkowa, zbudowana w formie pierścienia. W konfiguracji dwukablowej każdy z pierścieni odgrywa rolę zarówno pierścienia roboczego, jak i pierścienia zapasowego. W topologiach jednokierunkowych tylko jeden pierścień pełni funkcję ścieżki roboczej, a w topologii BLSR — obydwie pierścienie.

## Ramkowanie

Sieci SONET/SDH realizują transmisję danych ze stałą prędkością, która jest wielokrotnością 64 kb/s. Segment 64 kb/s odnosi się do łącza *DS0* (*E0* w Europie) i jest to standardowa przepustowość usługi telefonii głosowej.

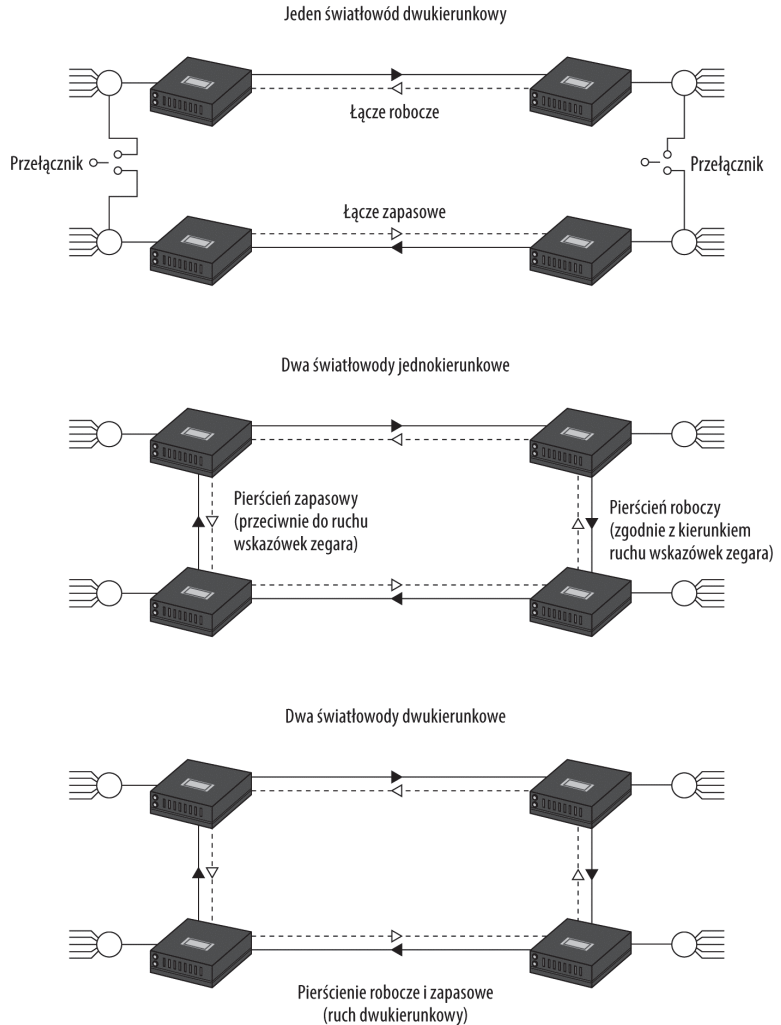
Funkcja synchronizacji w SONET/SDH jest utrzymywana dzięki zegarom atomowym, rozmieszczonym w całym systemie. Dane są przesyłane przez sieć SONET/SDH w formie ramek, w których są enkapsulowane protokoły, takie jak ATM lub PoS. Ramki różnią się nieznacznie w dwóch wspomnianych standardach.

W sieciach SONET dane są multipleksowane w ten sposób, że w tak zwanym wirtualnym kontenerze można umieszczać różne rodzaje ramek jednocześnie. Wyróżniamy kilka typów transmisji sieci SONET. SONET STS-1 pozwala na transmisję z prędkością 51,84 Mb/s, a norma równoważnego standardu SDH STM-1 umożliwia transmisję z prędkością trzy razy większą, 155,52 Mb/s. Główna różnica pomiędzy łączami w sieciach SONET i E1 – E4 jest taka, że w tych pierwszych mamy do czynienia z niewielkim opóźnieniem. Dla E1 opóźnienie wynosi 125  $\mu$ s, podczas gdy dla sieci SONET/SDH opóźnienie wynosi zaledwie 32  $\mu$ s. W przypadku transmisji danych przez światłowodową sieć SONET/SDH używamy określenia OC-1 zamiast STS-1. Pojęciem OC-N określamy sygnał optyczny. OC-3 przenosi na przykład trzy strumienie STS-1 (lub jeden STM-1).

Oktet to równoważnik ośmiu bitów. Jeden bajt składa się często z ośmiu bitów, ale nie zawsze. Nierzadko obydwa terminy są używane zamiennie.



**Rysunek 13.7.**  
Topologie SONET

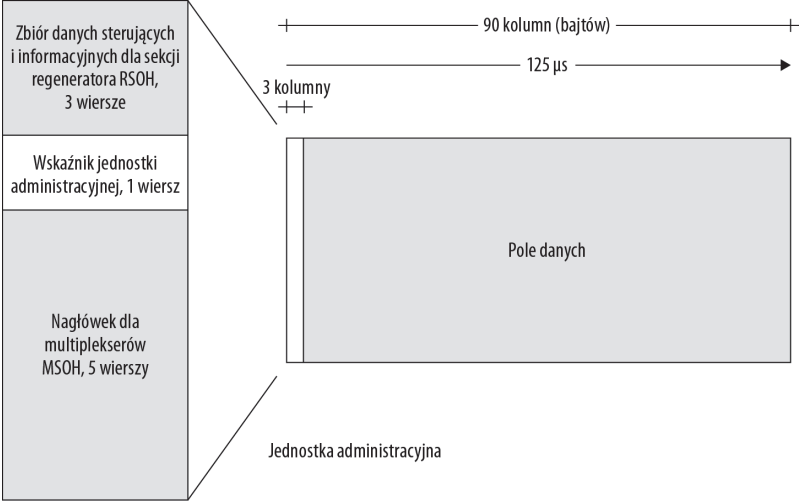


W rozdziale 17. omówiono strukturę pakietów TCP, gdzie pakiet składa się z części nagłówkowej, zawierającej kilka sekcji, po której następuje część danych TCP. Ramki SONET mają inną konstrukcję, w której dane i bity dodatkowe są umieszczane w tej samej sekcji. Struktura ramki różni się nieco w sieciach SONET i SDH. SONET STS-1 składa się z 810 oktetów: 9 rzędów pól danych po 87 oktetów i 3 oktetów nagłówka. W przypadku STM-3 elementy struktury są trzy razy większe. Rysunek 13.8 przedstawia ramkę SONET.

Synchronizacja działa w ten sposób, że co 125  $\mu$ s ramka przechodzi przez specjalny punkt w sieci, a 8 bit/125  $\mu$ s stanowi przepływność 64 kb/s, czyli standard DS0. Ponieważ w obu standardach stosuje się ten sam zegar, sygnały z SONET i SDH mogą być przesyłane jednocześnie. Tabela 13.3 przedstawia różne prędkości SONET/SDH, które uzyskuje się poprzez zwielokrotnienie strumieni:

1. Trzy łącza STS-1 są multipleksowane 3:1, łączem wyjściowym jest STS-3.
2. Cztery łącza STS-3 są multipleksowane 4:1, łączem wyjściowym jest STS-12.

**Rysunek 13.8.**  
*Ramka SONET*  
(810 oktetów)



**Tabela 13.3.** *Zwielokrotnienie łączy SONET/SDH*

Nośnik optyczny OC	Ramka SONET	Ramka SDH	Pasmo (kb/s)	Przepływność (kb/s)
OC-1	STS-1	STM-0	50 112	51 840
OC-3	STS-3	STM-1	150 336	155 520
OC-12	STS-12	STM-4	601 344	622 080
OC-24	STS-24	STM-8	1 202 688	1 244 160
OC-48	STS-48	STM-16	2 405 376	2 488 320
OC-192	STS-192	STM-64	9 621 504	9 953 280
OC-768	STS-768	STM-256	38 486 016	39 813 120
OC-3072	STS-3072	STM-1024	153 944 064	159 252 480

- 3. Jedno łącze STS-12 przesyła się przez skrambler (rejestr przesuwany, połączony z wejściem).
- 4. Wyjście skramblera jest połączone z konwerterem optycznym.
- 5. Optyczny sygnał OC-12 jest wprowadzany w medium transmisyjne (światłowód).

Obecnie najwyższy transfer z powszechnie dostępnych tego typu rozwiązań jest na poziomie OC-192 lub STM-64, który może osiągnąć szybkość transmisji do 10 Gb/s. Jest to porównywalne z Gigabit Ethernet. STM-256, o prędkości 40 Gb/s, jest dopiero wprowadzany. W celu osiągnięcia wyższych prędkości dane SONET można wprowadzać do medium, korzystając z różnych długości fal, przy użyciu technologii o nazwie WDM (ang. *Wavelength Division Multiplexing* — zwielokrotnianie w dziedzinie długości fali). Kabel podmorski, położony w latach dziewięćdziesiątych, umożliwia zastosowanie zwielokrotnienia DWDM, które jest odmianą WDM.

## Protokół PoS (Packet over SONET/SDH)

Protokół PoS to protokół przesyłania pakietów, który wykorzystuje połączenia typu punkt-punkt (PPP). Przewiduje się, że PoS stanie się dominującym standardem transportu w szybkich sieciach światłowodowych SONET/SDH. Norma ta została opracowana przez Cisco Systems, jest zaimplementowana w części sprzętowej i obsługiwana przez szybkie routery. Znaczna część ruchu PoS działa na poziomie OC-192 pierścieni SONET/SDH.

PoS jest protokołem łącza danych (warstwa 2. modelu ISO/OSI). Pakiety PoS są umieszczane w ramach SONET/SDH; omawiana technologia definiuje poziomy alarmowe, monitoring wydajności, niezawodności przełączania i synchronizacji. Pakiet w formacie PoS znacznie ułatwia integrację ruchu Ethernet IP w ramach PoS przy zachowaniu mniejszego nagłówka.

Systemy z protokołem PoS mogą działać w sieciach SONET/SDH równocześnie z realizacją usług głosowych TDM i obsługą ATM, pod warunkiem że korzystają z różnych przedziałów czasowych i nie będzie problemów z konfliktem dostępu. Niezależność ta ma kilka zalet. Na przykład ramki ATM mogą być wykorzystywane do świadczenia usług DSL oraz innych usług, które można zrealizować w oparciu o DSL (usługi transmisji danych, PVC, SVC itp.). Wszystkie tego typu usługi można zagregować w ATM, a następnie transmitować do routerów PoS, które przekazują ruch do sieci światłowodowej. Przykładem routera umożliwiającego translację ATM — PoS jest Cisco 12000. Rysunek 13.9 przedstawia proces agregacji.

Na rysunku 13.9 należy zwrócić uwagę na łącza POP pomiędzy routerami PoS i przełącznikami ATM, które są wykonane w formie redundantnej matrycy. POP jako technologia transmisji punkt-punkt może ulec awarii i z tego powodu potrzebuje redundancji, aby zapewnić niezawodność ruchu w sieci, co w sieci szkieletowej jest sprawą krytyczną.

Routery PoS mogą być podłączone do sieci szkieletowych w następujący sposób:

- ♦ przez multiplekser SONET/SDH,
- ♦ przez DWDM,
- ♦ bezpośrednio do sieci światłowodowej (do ciemnych włókien, ang. *dark fiber*).

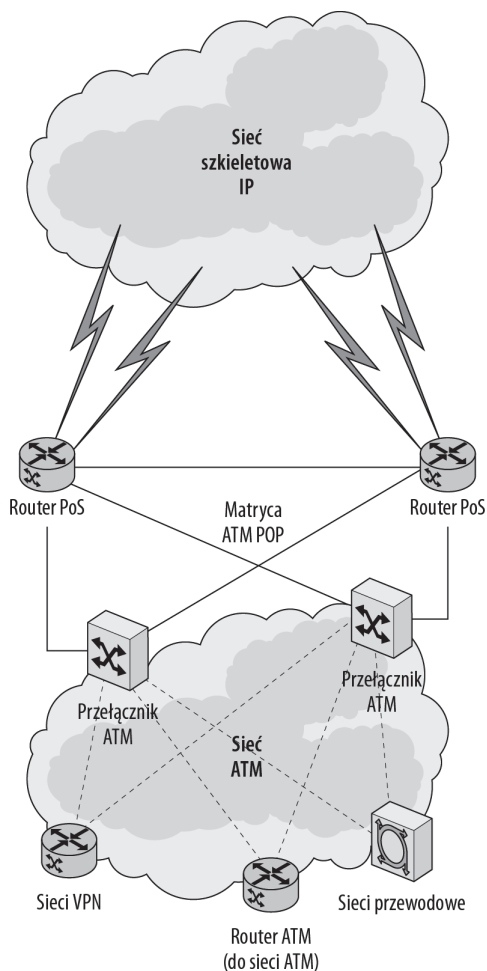
Gdy stosuje się ciemny światłowód, po stronie nadawczej trzeba wykorzystać laser lub LED, a w odbiorniku należy zainstalować fotodiode. Jeśli tor jest odpowiednio długi, trzeba zastosować w łączy regenerator SONET. Przykładem optycznego regeneratora SONET dla torów poziomu OC-48 jest Cisco 15104. Opisana procedura nazywa się „oświetleniem światłowodowym”.

Ramki PoS mają pewne specyficzne wymagania:

- ♦ **Zabezpieczenie porządku transmisji.** Ramki PoS muszą być odpowiednio umieszczone w ramach transportowych SONET/SDH.
- ♦ **Wyrównanie do oktetu.** Granice oktetu danych muszą być wyrównane z granicami oktetu STS/STM.
- ♦ **Skrambling pola danych.** Informacja znajdująca się w polu danych musi zostać poddana operacji skramblingu, aby zapewnić synchronizację i możliwość odtworzenia informacji zegarowych.

**Rysunek 13.9.**

*Agregacja ruchu ATM  
w routerach PoS*



Proces zapewnienia porządku transmisji realizuje następujące zadania:

- ♦ umieszcza datagram IP w ramce PPP,
- ♦ umieszcza ramki PPP w ramce HDLC,
- ♦ umieszcza ramki HDLC w ramce SONET/SDH.

## Sieci pakietowe

Sieci pakietowe działają w oparciu o podział transmitowanych danych na pakiety. *Pakiety* są elementami zmiennej długości, zawierającymi dodatkowe pola adresowania i formowania w tak zwanym nagłówku. W sieciach pakietowych definiuje się punkty końcowe transmisji (stacje nadawcze i odbiorcze), ale w niektórych standardach nie definiuje się jednoznacznie toru transmisji pomiędzy tymi punktami.



Wykaz sieci pakietowych znajduje się pod adresem  
[http://en.wikipedia.org/wiki/Packet\\_switched\\_network](http://en.wikipedia.org/wiki/Packet_switched_network).

Ethernet i IP są protokołami bezpołączeniowymi, w których trasa pakietów jest bez znaczenia. Niektóre protokoły pakietowe wykorzystują technologie wirtualnych obwodów, podczas gdy w innych można znaleźć stałe obwody wirtualne. Przykładem protokołów połączeniowych są TCP (opisany w rozdziale 17.), X.25, ATM i MPLS; wszystkie są opisane w kolejnych punktach rozdziału.

Pakiety są tworzone w określonej kolejności lub sekwencji po stronie nadawczej i muszą zostać ponownie złożone w tej samej sekwencji. Aby zapewnić prawidłowe złożenie pakietów, w protokołach stosuje się kilka różnych mechanizmów. Każdy pakiet posiada identyfikator, a protokoły zawierają odpowiedni system komunikacji o potrzebie retransmisji błędnie odebranego lub zagubionego pakietu. Poprawność pakietów jest określona dzięki mechanizmom kontroli błędów, stosowanym na końcu każdego odcinka trasy i (lub) w punkcie końcowym transmisji, gdzie pakiety są ponownie scalane.

W sieciach pakietowych mogą znaleźć się dodatkowe elementy przenoszenia danych, tak zwane *datagramy*. Datagramy są częścią pakietu, zbioru pakietów lub innej kombinacji danych, umieszczanej w swego rodzaju kopercie wykorzystywanej do wysyłania i kontroli transmisji. Przykładem technologii, w której używa się datagramów, jest MPLS.

Sieci z przełączaniem pakietów mają przewagę nad sieciami z komutacją kanałów, bo w tych pierwszych można w pełni wykorzystać fizyczną przepustowość łączy. Pakiety mogą być kierowane przez zestaw segmentów wyznaczony na podstawie aktualnych warunków panujących w całej sieci. Małe opóźnienia związane z krótkotrwałymi połączeniami sprawiają, że sieci z przełączaniem pakietów szybciej inicjują transmisję w porównaniu z sieciami z przełączaniem kanałów.

## Sieci X.25

X.25 jest cyfrową odmianą protokołu pakietowego opracowanego w latach siedemdziesiątych, przed powstaniem sieci Internet, jako standard organizacji ITU-T. X.25 został wdrożony w sieciach telefonicznych jeszcze przed pojawieniem się szybkich łączy na początku lat dziewięćdziesiątych, dzięki którym można było wykorzystywać ISDN, ATM, ADSL i PoS. To stare rozwiązanie zastąpiono w późniejszych czasach protokołem IP. W modelu OSI X.25 świadczy usługi w warstwach od 1. do 3. (fizyczna, łączy danych i sieci). Standard warstwy fizycznej X.25 jest zdefiniowany jako X.21.

Dzisiaj X.25 jest używany w sieciach krajów rozwijających się, w Europie w niektórych systemach PoS, w systemach śledzenia GPS, a także w sieciach bezprzewodowego radia pakietowego, takiego jak standard AX.25. X.25 jest zatem w dużej mierze standardem o znaczeniu historycznym. Sieci takie jak CompuServe, Telnet, Euronet i Tymnet zostały zbudowane w oparciu o X.25.

Architektura X.25 tworzy wirtualne połączenia, które łączą urządzenia końcowe abonenta (DTE) z urządzeniem komunikacyjnym transmisji danych DCE w sieci X.25. DTE to zwykle terminal lub komputer, a DCE może być modemem podłączonym do sieci. Dla użytkownika połączenie w sieci X.25 wygląda jako połączenie punkt-punkt. X.25 definiuje możliwość segmentacji sieci transmisyjnej za pomocą połączeń wirtualnych trwałych typu PVC lub przełączanych SVC.



DCE jest nazywany urządzeniem łączy danych lub urządzeniem komunikacyjnym transmisji danych. Zwykle jest to komputer lub urządzenie realizujące konwersję sygnału, kodowanie i synchronizację.

Sieci X.25 można podłączyć do asynchronicznych urządzeń, takich jak modemy, terminale i drukarki, poprzez urządzenie konwersji pakietowej PAD. Protokół używany przez urządzenia PAD został zdefiniowany jako standard X.3, a pomiędzy terminalem a urządzeniem PAD używa się protokołu X.28. Aby połączyć urządzenie PAD z inną siecią, trzeba skorzystać ze standardu X.29. Urządzenia PAD są zatem bardzo uniwersalnymi jednostkami, zapewniającymi współpracę sieci X.25 z innymi sieciami. Urządzenia PAD znajdują się we wszystkich sieciach komutacji pakietów, gdzie trzeba dokonać konwersji prędkości pomiędzy węzłem nadawczym i odbiorczym. Konwertery PAD muszą się znaleźć na obu końcach połączenia.

X.25 powstał w celu zapewnienia niezawodnego połączenia i transmisji danych. W protokole zaimplementowano różne mechanizmy zapewniające prawidłowy odbiór pakietów w miejscu przeznaczenia. Zawiera on funkcje, które przejęły sieci IP: korekcję błędów, kontrolę przepływu oraz wysyłanie wiadomości. X.25 to wolne sieci — z ograniczeniem prędkości do tylko 64 kb/s.

## Technologia SMDS

SMDS (ang. *Switched Multimegabit Data Service*) należy do rodziny technologii szybkich sieci pakietowych. Standard SMDS został opracowany przez Bellcore na początku lat dziewięćdziesiątych jako technologia łącząca sieci LAN i MAN.

SMDS poprzedza rozwój protokołu ATM. Ta technologia bezpołączeniowa, zapewniająca usługi pakietowe, umieszcza datagramy w komórkach i wysyła je poprzez sieci pierścieniowe SONET/SDH. Dzięki temu sieci MAN mogą mieć promień około 50 km. Technologia ta była częścią standardu IEEE 802.6, definiującego rozwiązanie Distributed Queue Dual Bus (DQDB).

W USA sieci SMDS były wdrażane przez kilka lat, ale technologia ta nie stała się tam wszechobecna. W Europie SMDS miał więcej sukcesów; był sprzedawany na rynkach europejskich jako CBDS i stał się popularny w krajach z wielkimi metropoliami. Jednakże w połowie lat dziewięćdziesiątych SMDS został zastąpiony przez Frame Relay oraz szybsze sieci zbudowane w oparciu o protokół Ethernet, których przykładem jest PoE. Instytut IEEE określił standard 802.6 jako format przestarzały i SMDS ma w dużej mierze znaczenie historyczne.

## Technologia ATM

ATM (ang. *Asynchronous Transfer Mode*) to technologia szerokopasmowej komunikacji, zapewniająca średnią prędkość transmisji danych w trybie połączeniowym. Protokół ten działa w warstwie łącza danych (warstwa 2.), gdzie określa format przesyłania danych o nazwie *komórka*. W warstwie fizycznej (warstwa 1.) określa cyfrową technologię przełączania, która łączy punkty końcowe z wykorzystaniem wirtualnego obwodu. ATM początkowo miał umożliwiać transmisję w sieciach z komutacją kanałów i komutacją pakietów.

ATM jest zazwyczaj implementowany sprzętowo w przełącznikach i kartach sieciowych. Technologia ta jest kluczowa dla SONET/SDH, szkieletowej sieci telefonicznej, przedstawionej wcześniej w rozdziale. ATM jest technologią używaną w szerokopasmowych sieciach cyfrowych z integracją usług (B-ISDN) i w sieciach ADSL. Koszt technologii i złożona budowa ATM uniemożliwia stosowanie tego protokołu w sieciach lokalnych LAN.

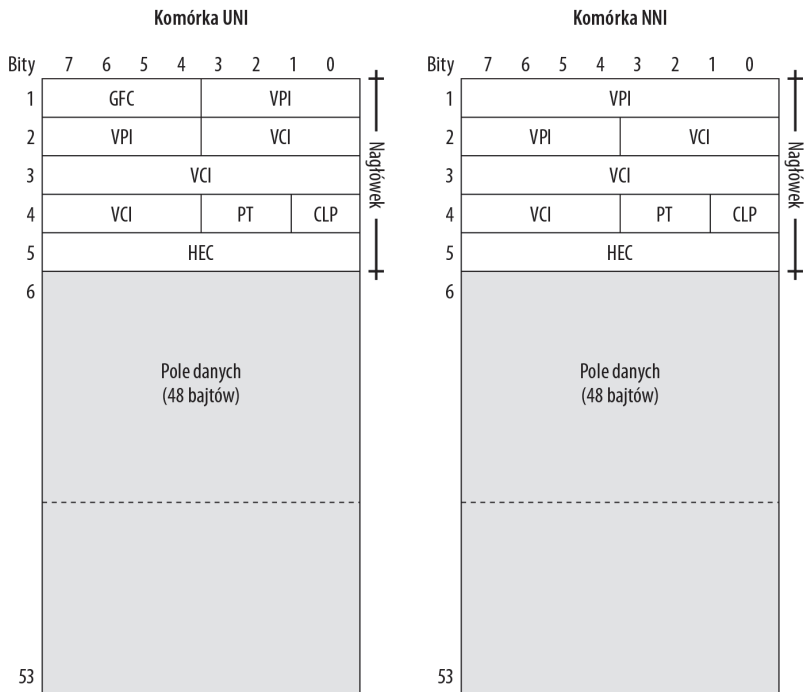
ATM został zaprojektowany do przetwarzania danych przesyłanych w czasie rzeczywistym, takich jak głos i video. Komórki transportowe w sieci ATM mają rozmiar 53 bajtów. Ten niewielki rozmiar umożliwia równomierne rozmieszczenie strumienia danych o dużej prędkości i dostarczenie go do kodeka, który konwertuje analogowy sygnał audio na postać cyfrową (lub na odwrót). Wszystkie datagramy, niezależnie od ich rozmiarów początkowych, są w ATM dzielone na fragmenty 48-bajtowe, do których dołącza się 5-bajtowy nagłówek routingu ATM w trakcie konstruowania komórek.

Jeśli komórka zostanie zagubiona w trakcie transmisji lub dotrze z opóźnieniem, kodeki wykorzystywane do przetwarzania w czasie rzeczywistym i segmentacji generują ciszę (w przypadku sprzętu audio) lub wyświetlają poprzednio zdekodowaną ramkę obrazu albo stosują jeszcze inną metodę w celu uzupełnienia brakujących danych. Niewielki rozmiar komórki oznacza, że brak jednej w pełnym przekazie jest mało dostrzegalny dla odbiorcy; brak danych tej komórki może być nawet niezauważalny dla człowieka. Dzięki zastosowaniu ATM jest możliwe obniżenie jittera (krótkotrwałych odchyleń parametrów transmisji od założonych wartości) do wartości mniejszych niż 5 procent w porównaniu z innymi standardami sieci pakietowych (porównywane są standardy, które powstały w tym samym czasie co ATM).

Protokół ATM do realizacji połączenia używa kanałów wirtualnych. Definiuje się dodatkowo pole VPI (o wielkości 8 lub 12 bitów) oraz pole VCI o wielkości 16 bitów. Obydwa pola znajdują się w nagłówku komórki. Wspomniane identyfikatory są zmieniane w każdym z węzłów pośrednich, znajdujących się w torze transmisji. W przeciwieństwie do TCP/IP, gdzie trasa pakietu nie ma znaczenia i tylko punkty końcowe transmisji są jasno określone, komórki ATM poruszają się po tej samej trasie, dlatego wymagają mniejszego narzutu informacji nadmiarowych.

Twórcy ATM zdefiniowali dwa podstawowe rodzaje styków: UNI (styk użytkownik — sieć, ang. *User to Network Interface*) i NNI (styk międzywęzłowy, ang. *Network to Network Interface*). Każdy styk ma własny, nieco inny format nagłówka komórki. Rysunek 13.10 przedstawia obydwa formaty komórek.

**Rysunek 13.10.**  
Struktura komórki ATM



Objaśnienie: GFC (ang. *Generic Flow Control*) — sterowanie przepływem ogólnym; VPI (ang. *Virtual Path Identifier*) — identyfikator wirtualnej ścieżki; VCI (ang. *Virtual Channel Identifier*) — identyfikator wirtualnego kanału; PT (ang. *Payload Type*) — typ danych; CLP (ang. *Cell Loss Priority*) — bit priorytetu; HEC (ang. *Header Error Control*) — pole kontrolne.

Mimo że w ATM jest niższy narzut protokołu, ma on mechanizmy kontroli ruchu sieciowego. ATM posiada cztery typy usług wymuszające odpowiedni poziom transferu: CBR (ang. *Constant Bit Rate* — stała szybkość bitowa), VBR (ang. *Variable Bit Rate* — zmienna szybkość bitowa), ABR (ang. *Available Bit Rate* — dostępna szybkość bitowa) i UBR (ang. *Unspecified Bit Rate* — nieokreślona szybkość bitowa). Parametry jakości usługi QoS (ang. *Quality of Service*) wiążą się z zawartym kontraktem ruchowym (ang. *traffic contract*). Mechanizmy kontroli w ATM sprawdzają zgodność strumienia komórek z kontraktem ruchowym; wiąże się to z takimi pojęciami, jak kształtowanie ruchu (ang. *traffic shaping*) i polityka ruchu (ang. *traffic policing*).

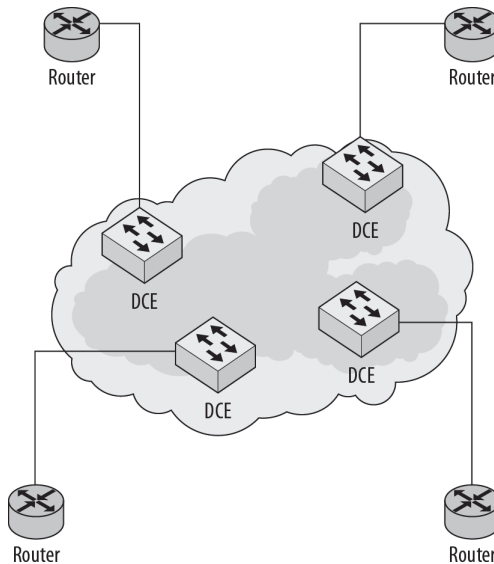
Minęło już 20 lat od opracowania standardu ATM przez ATM Forum i ITU. Od tamtego czasu nastąpiło wiele zmian w technologiach sieciowych. W chwili obecnej prędkości osiągnane przez technologie takie jak 10 Gigabit Ethernet z wykorzystaniem światłowodów, transmisja pakietów, nawet pełnej wielkości (1600 bajtów), są bardzo szybkie, rzędu 1,3 ms. To sprawia, że ATM staje się coraz mniej opłacalnym rozwiązaniem. Szybkie sieci szkieletowe działają z prędkościami większymi niż zdefiniowany poziom OC-3. Mimo że ATM będzie jeszcze używany przez wiele lat, oczywiste jest, że inne, nowoczesne technologie zastąpią w przyszłości ten standard w szybkich łączach sieci szkieletowych.

## Frame Relay

Sieć Frame Relay (rysunek 13.11) poprzez fizyczne połączenia multipleksuje wiele wirtualnych łączy (obwodów). Frame Relay jest protokołem warstwy fizycznej i łączy danych modelu ISO/OSI (warstwa 1. i 2.). W sieci Frame Relay ramki są kierowane pomiędzy węzłami z wykorzystaniem logiki przełączników i routerów. Sieci Frame Relay są popularnymi systemami przesyłania głosu i danych między poszczególnymi sieciami LAN połączonymi siecią WAN.

**Rysunek 13.11.**

*Sieć Frame Relay*



DCE (ang. *Data Circuit-terminating Equipment*) to urządzenia służące do synchronizacji sieci, przełączania usług pomiędzy DTE (ang. *Data Terminal Equipment*); głównie są to przełączniki Frame Relay. DTE to urządzenia dostępne do sieci FR, takie jak: FRAD (Frame Relay Access Devices), terminale, routery, multipleksery.

Ramki w standardzie Frame Relay mają zmienną długość, pole danych może mieć do 16 kB. Obwody wirtualne są identyfikowane przez 10-bitowy numer DLCI (ang. *Data Link Connection Identifier*); identyfikatory DLCI mają znaczenie lokalne (są modyfikowane w węzłach tranzytowych FR). Rodzaj dzierżawy, umowa o świadczenie usług i fizyczne parametry łącza stanowią główne ograniczenie prędkości maksymalnej w sieciach Frame Relay. Wydajność łącza Frame Relay sięga ATM-owego STM-4 (STS-12).

W każdym fizycznym łączy FR możemy umieścić wiele łączy wirtualnych. Dla każdego obwodu wirtualnego są negocjowane z operatorem dwa parametry, CIR (ang. *Committed Information Rate*) i EIR (ang. *Excess Information Rate*). Parametr CIR określa minimalną, gwarantowaną przez operatora przepływność, a EIR jest niegwarantowaną przepływnością maksymalną. Koszt wirtualnego łącza dzierżawionego stanowi zwykle ułamek tego, co trzeba zapłacić za normalne łącze dzierżawione w danej relacji. Sieci Frame Relay mają na celu poprawę stopnia wykorzystania sieci fizycznej dla dostawców usług, co działa pod warunkiem, że usługodawca nie przeciąża systemu zbyt dużą liczbą abonentów.

Ramka Frame Relay ma niewiele pól z informacjami nadmiarowymi — w tym protokole nie ma kontroli przepływu czy mechanizmu potwierdzania wiadomości. W sieciach Frame Relay zapewniono mechanizmy sterowania przeciążeniami. Węzły DCE ostrzegają DTE o przeciążeniu, ustawiając w nagłówku ramki bit FECN w przypadku odbiorcy lub bit BECN w przypadku nadawcy. Urządzenie DTE zmniejsza wtedy szybkość transmisji. Jeśli to nie nastąpi, w pierwszej kolejności DCE zacznie kasować ramki z DE = 1 (z niższym priorytetem), a następnie BCE będzie zmniejszało priorytet wszystkich ramek.

W przeciwieństwie do starszego protokołu X.25, który służył do zapewnienia transmisji danych analogowych i stanowił podwaliny systemu Frame Relay, omawiany standard używa technologii szybkiej transmisji pakietowej bez korekcji błędów. Ramka zaklasyfikowana jako błędna zostanie natychmiast odrzucona. Ewentualną retransmisję zajmują się protokoły warstw wyższych.

Usługi sieci Frame Relay nie są zwykle wykorzystywane w sieciach rozległych; używa się ich raczej w łączach dedykowanych z zastosowaniem np. DSL lub modemów kablowych.

## Protokół MPLS

Protokół MPLS (ang. *Multi Protocol Label Switching*) stanowi alternatywną metodę zarządzania pakietami, ramkami i komórkami w wielu różnych typach sieci. Protokół działa w warstwie 2. i 3. modelu ISO/OSI (tj. w warstwie łącza danych i sieci) i może być używany w sieciach z komutacją kanałów i komutacją pakietów. MPLS jest standardem IETF zapewniającym odpowiednią jakość usług QoS (ang. *Quality of Service*).

Etykiety MPLS są dodawane do pakietów w routerach brzegowych sieci MPLS — LER (ang. *Label Edge Router*). Etykieta składa się m.in. z pola ID, identyfikującego etykietę MPLS, i pola TTL, informującego, ile routerów pakiet przeszedł. Informacje te są wprowadzane po sprawdzeniu tablicy etykiet LIB (ang. *Label Information Base*) węzła LER. Na podstawie tych informacji router LER wysyła pakiet do następnego routera w sieci MPLS — LSR (ang. *Label Switched Router*). LSR zamienia etykietę na nową zgodnie z danymi w tablicy LIB i transmituje pakiet dalej. Jeśli następny router nie obsługuje protokołu, MPLS usuwa etykietę.

MPLS będzie logicznym zamiennikiem protokołu ATM i zastąpi jego komórki wraz z nagłówkami, a także zapewni synchronizację odpowiednią dla szybkich sieci optycznych. Jako protokół warstwy 2. i 3. MPLS oferuje usługi datagramów i może być używany do transmisji pakietów IP, a także ramek Ethernet, ATM i SONET. Działanie MPLS opiera się na wykorzystaniu bardzo szybkich przełączników. Jednym z głównych twórców tej technologii jest Cisco Systems.

MPLS znajduje zastosowanie w dużych sieciach, działających w oparciu o protokół IP i wymagających zapewnienia usług zgodnych z odpowiednim poziomem QoS. Protokół obsługuje IPv4 i IPv6 i może być wykorzystany w połączeniach ATM, Frame Relay, T1. Przewaga prędkości działania MPLS w porównaniu z innymi protokołami nie jest jego główną zaletą, bo prędkość sieci nie ma już obecnie takiego znaczenia jak zachowanie odpowiedniego poziomu usług QoS. Obsługa danych wymagających wysokiej klasy QoS, takich jak VoIP, wymaga wysokiej sprawności sieci (małe opóźnienia), co zapewnia protokół MPLS.

## Sieci Internet i Internet2

Internet to sieć WAN składająca się z wielu połączonych sieci rozległych. Można powiedzieć, że jest to intersieć intersieci. Około 95% ruchu stanowi stos TCP/IP. Obydwa protokoły zostały opisane w niniejszej książce. Internet jest bardzo ciekawą siecią rozległą, bo stanowi połączenie wielu różnych węzłów WAN. Poniżej przedstawiono szczegółowo aspekty punktów wymiany ruchu IXP (ang. *Internet eXchange Point*).

Gdy Internet stawał się coraz bardziej komercyjny, otwarty i zatłoczony, jego pierwotne przeznaczenie jako sieci wspierającej badania i rozwój, realizowane na uniwersytetach i w laboratoriach, stało się utrudnione. Utworzono wiele nowych sieci, które zostały opracowane jako Internet nowej generacji, znany również pod nazwą Internet2. Jednym z projektów takiej sieci jest Janet, realizowany w Wielkiej Brytanii. W Europie realizuje się dużo innych projektów Internetu nowej generacji. Internet2 umożliwia wykorzystanie zaawansowanych aplikacji i technologii i obecnie służy jako poligon doświadczalny dla przyszłego rozwoju publicznej sieci Internet nowej generacji.

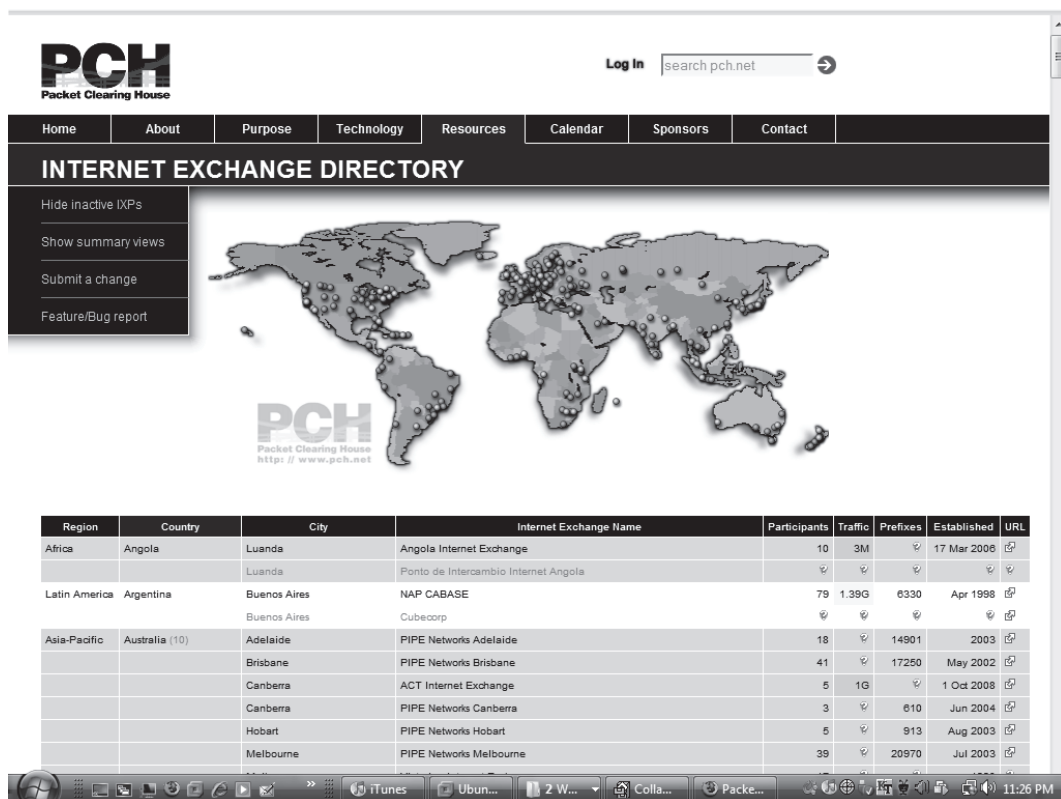
### Punkty wymiany ruchu internetowego

Punkty wymiany ruchu w przypadku dużych sieci w Internecie w USA były nazywane punktami dostępu do sieci NAP (ang. *Network Access Point*). Pierwszy punkt był utrzymywany przez fundację National Science Foundation (NSF), która zajmowała się również rozbudową systemu. W trakcie rozwoju sieci dodano trzy dodatkowe systemy, zarządzane przez Sprint, Ameritech i Pacific Bell. Systemy znajdowały się w Waszyngtonie, Chicago, Kalifornii i New Jersey. Wraz ze wzrostem liczby punktów dostępu w niektórych miastach dostawcy utworzyli obszarowe punkty dostępu MAE (ang. *Metropolitan Area Exchanges*).

W trakcie rozwoju systemu powstawało coraz więcej połączeń sieciowych, łączących poszczególne sieci ze sobą. Obecnie punkty wymiany ruchu między dostawcami usług i sieciami nazywają się punktami IXP lub IX (od angielskiego terminu *Internet Exchange Points*). Terminy NAP i MAE są coraz rzadziej stosowane. Punkt IXP jest punktem przejścia od infrastruktury zarządzanej przez dostawcę usług do infrastruktury zewnętrznej. Wymiana ruchu jest realizowana w oparciu o odpowiednie umowy, regulujące warunki i opłaty korzystania z sieci szkieletowych. Ruch transferowy pomiędzy punktami IXP jest zwykle zwolniony z dodatkowych opłat, natomiast przesyłanie danych do sieci docelowej jest płatne. Opłata zależy od poziomu usługi i ilości przesłanych danych.

Punkty wymiany ruchu IXP realizują routing pomiędzy sieciami, zapewniając wysoką wydajność i bezawaryjność. IXP posiadają niezależne łącza. Połączenia międzykontynentalne są realizowane za pośrednictwem kabli światłowodowych, ułożonych na dnie oceanów. Rysunek 13.12 przedstawia witrynę Packet Clearing House Web z wykazem punktów wymiany IXP wraz ze statystykami (<https://prefix.pch.net/applications/ixpdir/>).

Punkty wymiany ruchu IXP pełnią funkcję przełączania. Wszelkie kształtowanie ruchu, filtrowanie lub sterowanie routingiem jest nadzorowane przez dostawców usług internetowych, którzy uczestniczą w wymianie danych. Relacje między dwoma dostawcami usług



**Rysunek 13.12.** Wykaz punktów wymiany ruchu IXP na podstawie Packet Clearing House

internetowych biorących udział w wymianie danych są definiowane przez BGP (protokół bramy brzegowej, ang. *Border Gateway Protocol*), który służy do tworzenia tabeli routów, punktów dostępu do różnych sieci IP. Sieci dostępne przez ten system są określane mianem systemów autonomicznych AS (ang. *Autonomous Systems*), a ścieżki dostępu do nich nazywają się wektorami ścieżki (ang. *path vectors*). System AS to zbiór prefiksów IP, kontrolowanych przez danego operatora.

Nie cały ruch w Internecie jest transmitowany przez punkty IXP. Wielu dostawców usług internetowych ma łącza bezpośrednie. W tych przypadkach ruch jest kierowany przez zewnętrzne punkty wymiany wyłącznie w razie awarii. Dla tych dostawców usług internetowych, którzy nie mają umów bezpośrednich między sobą, wymiana danych przez punkty IXP jest jedynym dostępnym rozwiązaniem.

W październiku 2008 r. w pierwszej dziesiątce znajdowały się punkty wymiany ruchu internetowego przedstawione w tabeli 13.4 (na podstawie dostępnych źródeł). Najwyżej oceniany punkt IXP z USA nie jest widoczny. Jest nim New York International Internet eXchange (NYIIX), który został sklasyfikowany na dwunastej pozycji. NYIIX miał 98 członków, maksymalną przepustowość 23 Gb/s, a średnia wydajność to 15 Gb/s. Ta lista podlega sezonowym zmianom. Należy również zauważyć, że w informacjach o punktach IXP w USA często nie ujawnia się natężenia ruchu.

**Tabela 13.4.** *Dziesięć najaktywniejszych punktów wymiany*

Nazwa	Położenie geograficzne	Liczba członków	Maksymalne obciążenie (Gbits/s)	Średnie obciążenie (Gbits/s)
Amsterdam Internet Exchange (AMS-IX)	Amsterdam, Holandia	300	419	280
Deutscher Commercial Internet Exchange (DE-CIX)	Frankfurt nad Menem, Niemcy	250	428	210
London Internet Exchange (LINX)	Londyn, Wielka Brytania	221	256	157
Japan Network Access Point (JPNNAP)	Tokio, Japonia	88	183	129
Netnod Internet Exchange in Sweden (Netnod)	Sztokholm, Szwecja	53	103	104
Japan Internet Exchange (JPIX)	Tokio, Japonia	107	73	55
Spain Internet Exchange	Madryt, Hiszpania	43	72	61
Hong Kong Internet eXchange (HKIX)	Hongkong, Chiny	76	47	34
Budapest Internet Exchange (BIX)	Budapeszt, Węgry	52	35	26
Polish Internet eXchange	Warszawa, Polska	76	35	18

Według witryny *InternetWorldStats.com* (czerwiec 2008 r.) 1,46 mld ludzi ma dostęp do Internetu, co stanowi około 21,9 proc. całej ludności świata (6,68 mld). Ostatnie dane szacunkowe opublikowane przez Discovery Institute przewidują cały ruch internetowy w 2015 r. na poziomie zetabajta, tj. 1000 eksabajtów. W 2006 r. ruch wynosił około 26 eksabajtów.

## Internet2

Internet2 Network to konsorcjum uczelni, przedsiębiorstw, organizacji badawczych i agencji rządowych, biorących udział w użytkowaniu i rozwoju zaawansowanych technologii sieciowych dla Internetu. Celem projektu jest stworzenie systemu wsparcia dla najnowocześniejszych badań, umożliwiających powstanie technologii nowej generacji i jej transfer do publicznej sieci Internet. Wśród obecnych technologii w sieci Internet2 są mechanizmy obsługi bibliotek multimediów, videokonferencji, zaawansowane oprogramowanie warstwy pośredniej, wirtualne laboratoria, zdalne aplikacje do badania stanu zdrowia, aplikacje naukowe i wiele innych.

Internet2 jest zastrzeżonym znakiem towarowym organizacji, która stworzyła pierwszą wersję zaawansowanych sieci szkieletowych, Abilene Network. Abilene Network łączy wszystkie stany USA łączem o przepustowości 10 Gb/s. Kolejny projekt w tej grupie, National LambdaRail (NLR), polegał na realizacji szkieletowej sieci optycznej o poziomie OC-192. Większość artykułów związanych z Internet2 napisano na temat Abilene Network. Obecnie sieć Internet2 ma nazwę „Internet2 Network”, zgodnie z wolą Abilene

Network. Rysunek 13.13 przedstawia aktualny zasięg sieci Internet2 (stan z maja 2009 roku). Należy pamiętać, że Internet2 jest usługą szkieletową, która nie obejmuje całych Stanów Zjednoczonych.



**Rysunek 13.13.** Sieć Internet2

## Podsumowanie

W tym rozdziale omówiono sieci rozległe WAN i ich cechy. Przedstawiono protokoły i technologie wykorzystywane do zapewnienia routingu i przełączania.

PSTN, sieć z komutacją kanałów, może obsługiwać zarówno usługi głosowe, jak i transmisje danych. Najczęstsze typy połączeń, ISDN i DSL, zostały opisane szczegółowo.

W sieciach szkieletowych stosuje się łącza T i E. Najpopularniejszym protokołem transmisji danych w tych sieciach jest SONET/SDH. Transmisja danych w sieciach SONET/SDH najczęściej wykorzystuje technologie ATM lub Packet over SONET/SDH.

Sieci z przełączaniem pakietów są używane do transmisji ruchu TCP/IP. W sieciach tych stosuje się protokoły takie jak X.25, Frame Relay i ATM. Ważnym elementem w sieciach rozległych są punkty wymiany IXP. Dodatkowo omówiono pokrótce standard sieci nowej generacji Internet2.

Kolejny rozdział dotyczy tworzenia sieci bezprzewodowych.

# Rozdział 14.

## Sieci bezprzewodowe

### W tym rozdziale:

- ♦ Sieci bezprzewodowe
- ♦ Grupa standardów 802.11
- ♦ Tworzenie łącz i sieci bezprzewodowych
- ♦ Dostępne urządzenia bezprzewodowe

Grupa standardów sieci bezprzewodowych IEEE 802.11x, znana jako standardy sieci Wi-Fi, wywołała rewolucję w sieciach komputerowych w ostatnim dziesięcioleciu. W tym rozdziale przedstawiono różne standardy sieci bezprzewodowych, własności takich sieci i sposób tworzenia sieci lub połączeń sieciowych w technologii bezprzewodowej. Sieci bezprzewodowe obsługują dwa różne typy architektury: ad hoc i infrastrukturalny.

Powszechnie stosowane standardy sieci bezprzewodowych są oparte na łączach radiowych w publicznie dostępnych pasmach o częstotliwości 2,4 GHz lub 5 GHz. W technologii Wi-Fi pasmo jest dzielone na kanały, a następnie wykorzystuje jedną z technik transmisji: albo z wykorzystaniem rozpraszania widma, albo z wykorzystaniem tak zwanego skakania po częstotliwościach. W niniejszym rozdziale przedstawiono szczegółowo zarówno technikę rozpraszania widma w systemach szerokopasmowych za pomocą ciągów kodowych DSSS (ang. *Direct-Sequence Spread Spectrum*), jak i metodę rozpraszania widma poprzez skakanie sygnału po częstotliwościach w kolejnych odstępach czasu, w dostępnym paśmie FHSS (ang. *Frequency-Hopping Spread Spectrum*). Zanim sygnały zostaną wysłane w eter, podlegają kodowaniu i odpowiedniej modulacji. Najczęściej wykorzystywaną techniką jest modulacja z kluczowaniem fazy PSK (ang. *Phase Shift Keying*).

Ramki standardów 802.11x, które będą przedstawione w dalszej części rozdziału, są podobne do ramek Ethernet. Główną metodą w transmisji radiowej jest wielodostęp do łącza ze śledzeniem stanu nośnika i unikaniem kolizji CSMA/CA. W niniejszym rozdziale zostaną przedstawione metody uzgadniania transmisji (*handshaking*), sterowania ruchem i zarządzania łączem.

Punkty dostępu, bramki, routery to urządzenia bezprzewodowe, które są wykorzystywane przez klienty bezprzewodowe w celu podłączenia do sieci. Właściwości tych różniących się między sobą urządzeń zostaną przedstawione w dalszych punktach rozdziału. Opisano tu również metody rozszerzenia sieci, w tym zastosowanie regeneratorów systemów dystrybucji oraz specjalnych anten (takich jak anteny inteligentne).

Oprogramowanie, którego można użyć do wykrycia urządzeń bezprzewodowych w sieci i do zbadania ruchu bezprzewodowego, jest również przedmiotem tego rozdziału. Przedstawiono tu także powszechnie stosowane różne formy zabezpieczeń sieci bezprzewodowych.

## Sieci bezprzewodowe

W sieciach bezprzewodowej transmisji radiowej wykorzystuje się głównie systemy działające w pasmach 2,4 GHz lub 5 GHz. Pasma te zostały wybrane, ponieważ są publicznie dostępne oraz umożliwiają zbudowanie sieci ad hoc bez wprowadzania zakłóceń do innych systemów radiowych. Można stwierdzić, że pojawienie się rodziny standardów 802.11x w świecie internetu jest tak rewolucyjnym skokiem technologicznym, jak pojawienie się standardów telefonii komórkowej w telekomunikacji. Istnieją cztery główne standardy sieci bezprzewodowych z grupy 802.11: 802.11a, 802.11b, 802.11g oraz 802.11n. Produkty tworzone na podstawie standardu 802.11n ostatnio zyskują na popularności po stosunkowo długim okresie zatwierdzania standardu, kiedy to były budowane z wykorzystaniem projektu wspomnianej normy.

Sieci bezprzewodowe, tworzone za pomocą bezpośrednich połączeń pomiędzy dwiema stacjami (ang. *Station*, STA — w terminologii IEEE 802.11 jest to każde urządzenie kompatybilne ze standardami z grupy 802.11), połączenia punkt-punkt, nazywa się sieciami ad hoc, w których implementuje się zestaw niezależnych, podstawowych usług sieciowych IBSS (ang. *Independent Basic Service Set*). Sieci ad hoc mogą być tworzone z zestawu połączeń pomiędzy stacjami. Tryb ad hoc jest czasami określany jako peer-to-peer. Sieć, w której stacje łączą się z urządzeniem nadawczo-odbiorczym, zwanym punktem dostępu AP (ang. *Access Point*), jest określana jako sieć infrastrukturalna i realizuje szereg usług podstawowych BSS (ang. *Basic Service Set*). W sieciach tych wykorzystuje się identyfikator SSID. Rysunek 14.1 przedstawia elementy sieci bezprzewodowej.

Zarówno sieci ad hoc, jak i infrastrukturalne wykorzystują identyfikator SSID (ang. *Service Set Identifier*), zapewniający podstawowe bezpieczeństwo dostępu do sieci. SSID jest nazwą sieci bezprzewodowej. Można powiedzieć, że identyfikatory SSID są stosowane w taki sam sposób jak nazwy domen w sieci przewodowej. Podczas inicjalizacji pierwszej stacji w sieci ad hoc wymagane będzie nazwanie sieci. Podobnie podczas konfigurowania punktu dostępowego AP lub routera bezprzewodowego czy bramy pojawi się prośba o utworzenie nowego identyfikatora SSID.

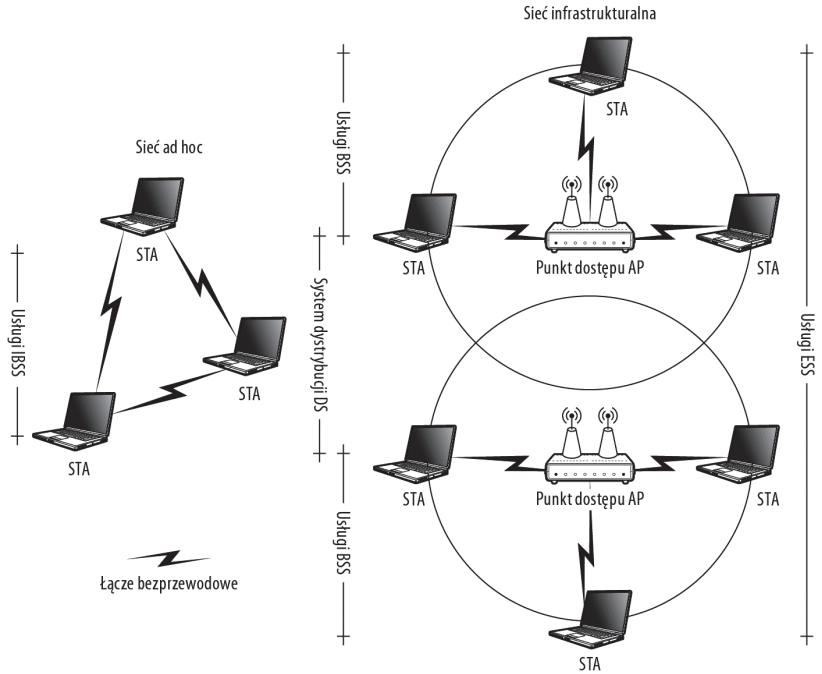
Pierwsza stacja sieci ad hoc lub punkt dostępu AP tworzy tzw. ramkę 802.11 beacon, której zadaniem jest rozgłoszenie informacji o sieci dla potencjalnych klientów bezprzewodowych. Podczas próby połączenia klienty są proszone o podanie hasła potrzebnego do uzyskania dostępu do sieci bezprzewodowej. W sieciach, gdzie nie utworzono hasła, istnieje zagrożenie spowodowane tym, że każdy klient może uzyskać połączenie, przez co nie mamy kontroli nad potencjalnymi użytkownikami sieci.

Jeśli połączymy co najmniej dwie sieci bezprzewodowe w ten sposób, że ich punkty dostępu AP będą mieć nakładające się obszary pokrycia, utworzymy system dystrybucji DS (ang. *Distribution System*<sup>1</sup>). System DS charakteryzuje zdolność do przenoszenia danych

---

<sup>1</sup> Obecnie takie systemy są częściej nazywane bezprzewodowymi systemami dystrybucji WDS (ang. *Wireless Distribution System*) — *przyp. tłum.*

**Rysunek 14.1.**  
Sieci bezprzewodowe  
ad hoc  
i infrastrukturalne



pochodzących od jednej stacji, podłączonej do określonego punktu AP, do klienta znajdującego się w obszarze pokrycia innego punktu dostępu. W tym przypadku potrzebne jest zestawienie łączy pomiędzy punktami dostępowymi AP (zwanego mostem AP-AP), bo poszczególne stacje nie mogą się komunikować bezpośrednio.

Po zainstalowaniu co najmniej dwóch punktów dostępu bezprzewodowego, które komunikują się ze sobą i są częścią tej samej sieci lub podsieci, mamy do czynienia z realizacją rozszerzonego zestawu usług ESS (ang. *Extended Services Set*), rozpoznawanego pod identyfikatorem ESSID. Na rysunku 14.1 przedstawiono system dystrybucyjny z wykorzystaniem mostu AP-AP, ale częściej w systemach sieci bezprzewodowych poszczególne punkty dostępu komunikują się za pomocą sieci przewodowej. W tym przypadku usługi ESS są dostępne tylko bezprzewodowej części systemu. W przypadku systemu złożonego z urządzeń o tym samym ESSID klienci mogą być przenoszone pomiędzy obszarami pojedynczych podsystemów bez konieczności zmiany konfiguracji.

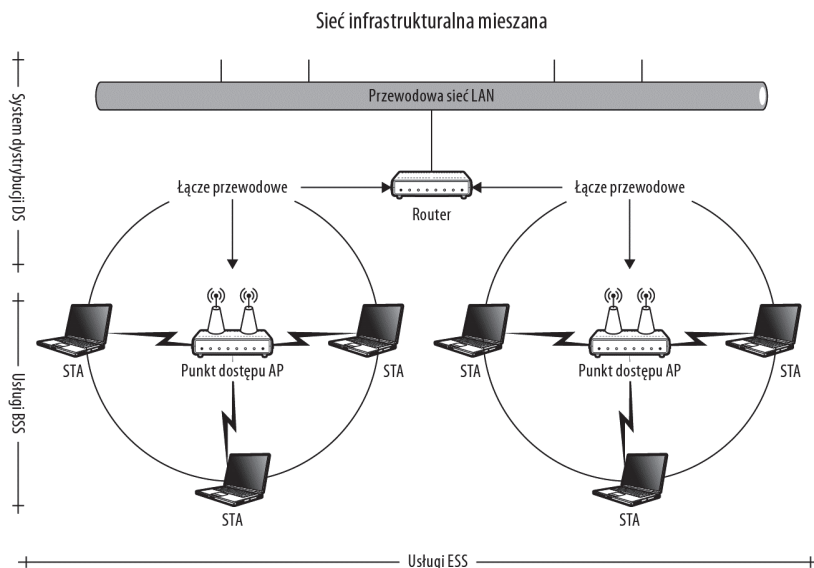
Rysunek 14.2 przedstawia budowę sieci opartej na częściach przewodowej i bezprzewodowej.

## Sieci Wi-Fi

*Wi-Fi* jest znakiem towarowym stowarzyszenia Wi-Fi i stanowi nazwę wszystkich technologii utworzonych na podstawie standardów IEEE 802.11x. Nazwa Wi-Fi jest rozwijana jako skrót od *Wireless fidelity*, podobnie jak norma jakości dźwięku Hi-Fi to *High fidelity*; została wymyślona przez Interbrand Corporation w 1999 roku, aby zastąpić skomplikowaną nazwę IEEE 802.11b Direct Sequence, i obecnie jest marką bez rzeczywistego związku z tą technologią. Logo Wi-Fi przypomina yin-yang, co podkreśla, że projekt ma na celu wskazanie interoperacyjności standardów.

**Rysunek 14.2.**

*Sieć oparta  
na częściach  
przewodowej  
i bezprzewodowej*



Wi-Fi jest głównym zestawem standardów komputerowych sieci bezprzewodowych, który wprowadzony przez organizację IEEE stał się niemal wszechobecny na rynku. Kupując bezprzewodowy laptop, drukarkę, serwer multimedialny lub jakiegokolwiek inne urządzenie bezprzewodowe, możemy mieć pewność, że znajduje się w nim kilka wersji implementacji 802.11, co daje stosunkowo dużą szansę, że urządzenie będzie współpracować z innymi bezprzewodowymi urządzeniami sieciowymi, które już posiadamy. Istnieje kilka kwestii związanych z interoperacyjnością, które zostaną omówione w tym rozdziale.

Wi-Fi nie jest jedyną bezprzewodową technologią powszechnie stosowaną w urządzeniach domowych. Istnieją inne technologie bezprzewodowe, w które na przykład są wyposażone telefony komórkowe, gry video, piloty i inne urządzenia. Te technologie to Bluetooth, łącze podczerwieni oraz inne technologie radiowe. W większości są one zorientowane połączeniowo, dlatego w tym rozdziale omówiono szczegółowo sieci 802.11. Jedynym wyjątkiem jest Bluetooth, opisany w rozdziale 11., gdzie przedstawiono osobiste sieci WLAN (tzw. pWLAN).

## Standardy grupy IEEE 802.11x

Każdy ze standardów grupy 802.11x określa inny system modulacji i odpowiednią szerokość pasma pracy. W każdym standardzie stosuje się koncepcję kanału w celu oddzielenia poszczególnych połączeń. Na przykład pasmo 2,4 GHz (znane również jako ISM-S<sup>2</sup>), wykorzystywane w standardzie 802.11b/g, obejmuje zakres od 2,400 do 2,4835 GHz i jest podzielone na 13 kanałów. Każdy kanał ma szerokość 22 MHz, kanały nakładają się na siebie i są w stosunku do sąsiednich kanałów przesunięte o 5 MHz. Poszczególne kanały są numerowane od 1. (2,400 do 2,423 GHz) do 13. (2,461 do 2,483 GHz). Najmocniejszy

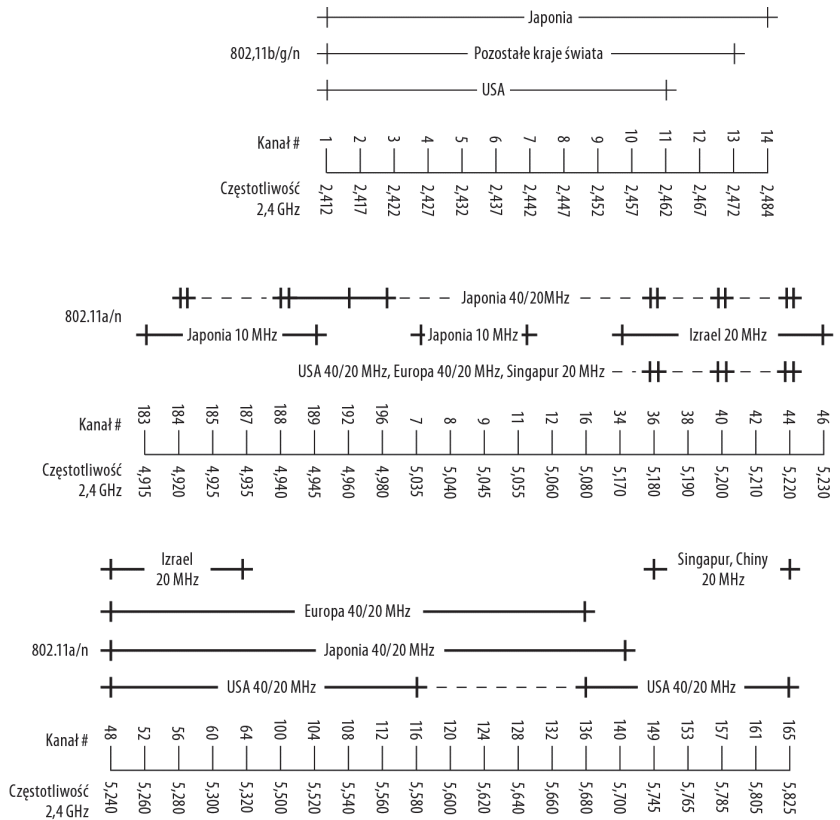
<sup>2</sup> ISM (ang. *Industrial, Scientific, Medical*) to pasmo częstotliwości radiowych przeznaczone do zastosowań przemysłowych, naukowych i medycznych. ISM jest pasmem nielicencjonowanym, udostępnianym publicznie. Pasma ISM dzieli się na ISM-S (2,4 GHz) i ISM-C (5 GHz) — *przyp. tłum.*

sygnał jest w punkcie środkowym każdego kanału; w przypadku kanału 1. najmocniejszy sygnał znajdzie się na częstotliwości 2,411 GHz, a dla kanału 13. — na częstotliwości 2,472 GHz.

Istnieją pewne różnice w udostępnianych częstotliwościach kanałów ogólnodostępnych w poszczególnych krajach świata. Stany Zjednoczone pozwalają na wykorzystanie kanałów od 1. do 11. w paśmie 2,4 GHz, natomiast zakazują stosowania kanałów 12. i 13. oraz czasem definiowanego kanału 14. na częstotliwości 2,473 GHz (górny kanał z zakresu 2,4 GHz). Japonia zezwala na wykorzystywanie wszystkich 14 kanałów, ale większość pozostałych krajów świata zezwala na stosowanie tylko 13 kanałów.

W paśmie 5 GHz (ISM-C), w którym działają 802.11a oraz opcjonalnie 802.11n, znajdują się 42 kanały. Rysunek 14.3 podsumowuje bieżące wykorzystanie różnych kanałów w niektórych krajach. Należy pamiętać, że pasma i kanały dozwolone w danych krajach mogą ulec zmianie.

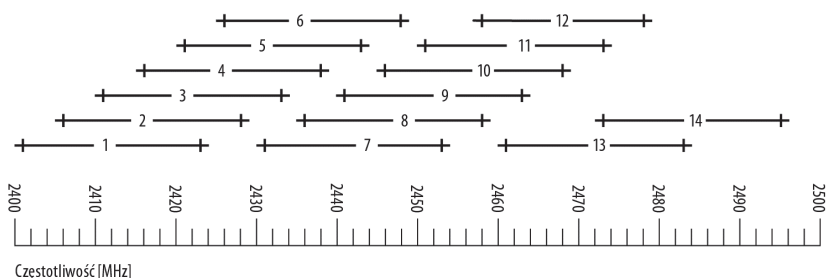
**Rysunek 14.3.**  
Wykorzystanie  
kanałów standardu  
802.11 w różnych  
krajach świata



Rozmiar kanałów z zakresu 2,4 GHz wynika z rozkładu energii każdego z kanałów w widmie. Maksymalny sygnał w częstotliwości środkowej musi być wytłumiony o 50 dB przy krawędzi kanału (22 MHz z każdej strony pasma). Pomiedzy poszczególnymi kanałami stosuje się przesunięcie o szerokości 5 MHz, co oznacza, że widmo każdego kanału nakłada się częściowo z widmem czterech sąsiednich kanałów. Rysunek 14.4 ilustruje zjawisko nakładania się kanałów w paśmie 2,4 GHz.

**Rysunek 14.4.**

Podział pasma 2,4 GHz na kanały



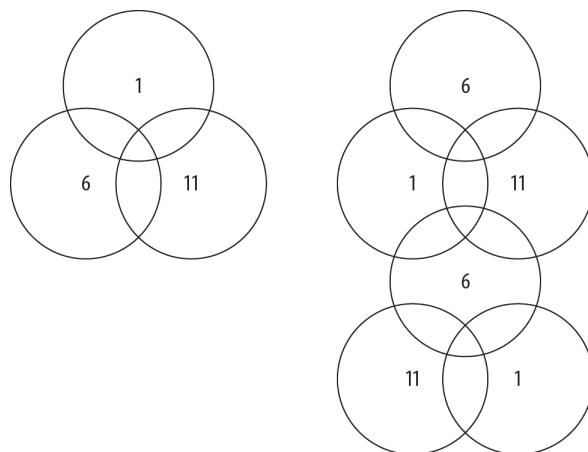
To w praktyce oznacza, że z 13 kanałów w paśmie 2,4 GHz tylko 3 kanały można przypisać do sąsiadujących sieci bezprzewodowych, których zasięg częściowo się pokrywa. Te kanały to zazwyczaj 1., 6. i 11 lub 1, 7 i 13.

Wraz z oddalaniem się nadajników od siebie ich zdolność do oddziaływania na odbiornik znajdujący się w przylegającym kanale maleje. Zatem jeśli kanały 1., 6. i 11. działają w jednym pomieszczeniu bez problemów, nadajnik działający na kanale 1. z jednej strony budynku nie ma wpływu na inny, korzystający z kanału 4. z drugiej strony budynku.

System przedstawiony na rysunku 14.5 pokazuje, jak można rozmieścić punkty dostępowe, aby kanały o tych samych numerach się nie nakładały. Przy użyciu tej metody możliwe jest rozszerzenie zasięgu całej sieci bez niepotrzebnej interferencji międzykanałowej.

**Rysunek 14.5.**

Rozmieszczanie punktów dostępowych w sieci

**Standard 802.11**

Standard 802.11 został opublikowany po raz pierwszy w 1997 roku. Zdefiniowano w nim trzy typy połączeń bezprzewodowych:

- ♦ **Wykorzystanie fal elektromagnetycznych (optycznych)** z zakresu podczerwieni — DFIR (ang. *Diffuse Infrared*) — umożliwiające transfer z prędkością do 1 Mb/s.
- ♦ **Wykorzystanie fal elektromagnetycznych (radiowych, z zakresu 2,4 GHz)** z rozpraszaniem widma metodą przeskoków częstotliwości — FHSS (ang. *Frequency Hopping Spread Spectrum*) — umożliwiające transfer z prędkością 1 lub 2 Mb/s.

- ♦ **Wykorzystanie fal elektromagnetycznych (radiowych, z zakresu 2,4 GHz)** z rozpraszaniem widma metodą bezpośredniego modulowania nośnej sekwencji kodową — DSSS (ang. *Direct Sequence Spread Spectrum*) — umożliwiające transfer z prędkością 1 lub 2 Mb/s.

Urządzenia oparte na 802.11 stały się przestarzałe wraz z nadejściem standardu 802.11b.



W celu transmisji sygnału o częstotliwości radiowej trzeba zastosować odpowiednią technologię modulacji, co omówiono szczegółowo w rozdziale 5.

W standardach 802.11b 802.11g wykorzystano modulację DSSS w paśmie o częstotliwości 2,4 GHz (ISM-S). To pasmo jest używane również przez inne urządzenia bezprzewodowe, na przykład kuchenki mikrofalowe, telefony, zabawki, elektroniczne nianie, walkie-talkie. Na tej częstotliwości urządzenia pracujące w standardzie 802.11b/g mogą zatem być zakłócanne. Inne technologie łączności bezprzewodowej wykorzystują takie metody modulacji, które wykluczają zakłócenia. Bluetooth i inne technologie działające w paśmie 2,4 GHz, w których używa się modulacji FHSS, nie kolidują z innymi systemami wykorzystującymi pasmo ISM-S, ale mogą zakłócać (w niewielkim stopniu) urządzenia zgodne z 802.11b/g.

Ze względu na to, że w paśmie 2,4 GHz działa wiele technologii i ta częstotliwość może być zatłoczona, standard 802.11a został opracowany w celu wykorzystania pasma o częstotliwości 5 GHz (ISM-C). Dzięki temu, że w tym przypadku urządzenia działają na wyższych częstotliwościach, 802.11a zapewnia większą przepustowość, ale ma mniejszy zasięg w porównaniu z 802.11b/g. Dodatkowo fale o częstotliwości 5 GHz słabiej przenikają przez ściany w porównaniu z falami o częstotliwości 2,4 GHz. W terenie zabudowanym zakres standardu 802.11a zapewnia o połowę mniejszy zasięg w porównaniu z 802.11b.

Produkty zgodne ze standardem 802.11a pojawiły się na rynku po wprowadzeniu urządzeń opartych na normie 802.11b. Była to druga generacja Wi-Fi. Standard 802.11g stanowi trzecią, 802.11n — czwartą generację urządzeń bezprzewodowych Wi-Fi. Urządzenia działające na częstotliwościach zgodnych ze standardem 802.11a nie są w stanie współpracować z 802.11b/g ze względu na różnicę wykorzystywanego pasma radiowego. W przypadku, gdy urządzenie pracujące w standardzie 802.11g wykryje urządzenia działające zgodnie z 802.11b, prędkość sieci jest zmniejszana, aby zachować kompatybilność ze standardem 802.11b.

Na rynku jest dostępnych wiele urządzeń, które mają zaimplementowaną obsługę dwóch lub trzech różnych standardów. Najwcześniej pojawiły się urządzenia działające w dwóch pasmach, najczęściej można spotkać produkty zgodne z 802.11a/802.11b. Gdy tylko wprowadzono urządzenia zgodne z 802.11g, na rynku pojawiły się produkty oferujące wszystkie trzy wersje (a, b oraz g).

Do standardu 802.11n poza innymi funkcjonalnościami dodano technologię wieloantenuowej transmisji radiowej MIMO (ang. *Multiple Input Multiple Output*). MIMO jest technologią anten inteligentnych, przedstawioną w dalszej części rozdziału. Standard 802.11n oferuje możliwość współdziałania z 802.11b/g, ponieważ funkcjonalności nowego standardu stanowią rozszerzenie wcześniejszych norm.

W tabeli 14.1 znajduje się wykaz wariantów standardu 802.11 i ich właściwości.

**Tabela 14.1.** Właściwości standardów grupy 802.11

Standard	Pasmo (GHz)	Modulacja <sup>1</sup>	Przepustowość (Mbit/s)	Zasięg (w budynku/na zewnątrz, w metrach)
802.11	2,4	IR/FHSS/DSSS	2	20/100
802.11a	5,0	OFDM	54	35/120
802.11b	2,4	DSSS	11	38/140
802.11g	2,4	OFDM, DSSS	54	38/140
802.11n	2,4 lub 5,0	OFDM	600	70/250
802.11y	3,7	OFDM	54	-/5000

<sup>1)</sup> IR (ang. *infrared*, podczerwień), FHSS (skakanie po częstotliwościach w odstępach czasu, w dostępnym widmie), DSSS (bezpośrednie modulowanie nośnej sekwencją kodową) i OSDM (multipleksowanie z ortogonalnym podziałem częstotliwości).

## Standard 802.11y

Standard 802.11y zatwierdzono we wrześniu 2008 r. Definiuje on wysoką moc sygnału (maksymalnie 20 W) dla częstotliwości 3,7 GHz (od 3650 do 3760 MHz), umożliwiając realizację połączeń radiowych na odległość do 5 km. To pasmo częściowo pokrywa się z niektórymi częstotliwościami wykorzystywanymi w radiowej łączności naziemnej lub satelitarnej, stąd możliwość jego stosowania jest ograniczona. W celu wykorzystania urządzeń pracujących zgodnie z normą 802.11y w Stanach Zjednoczonych należy uzyskać pozwolenie. Każda licencja jest wydawana dla określonej stacji bazowej, a nie dla konkretnej lokalizacji. Urządzenia klienckie standardu 802.11y nie wymagają pozwolenia, ale przed rozpoczęciem transmisji wymagany jest sygnał zezwolenia na nadawanie od licencjonowanej stacji bazowej. Dzięki licencji i kontroli transmisji można łatwo wyłapać urządzenia zakłócające licencjonowane urządzenia.

Aby umożliwić realizację wielu połączeń zgodnie ze standardem 802.11y w tym samym obszarze geograficznym, trzeba było zastosować protokół CBP (ang. *Contention-based protocol*). Protokół ten umożliwia jednoczesne nadawanie przez kilku użytkowników na jednym kanale.

Inną nową funkcją standardu 802.11y jest możliwość wykrywania kanałów przez stacje bazowe na podstawie pomiaru poziomu szumu i dostępnej przepustowości, a także dynamicznego przełączania kanałów. W celu obsługi połączeń z klientami powstał nowy schemat komunikatów ECSA (ang. *Extended channel switch announcement*), umożliwiający klientom sygnalizowanie zmian w kanale i jednocześnie realizujący przełączanie kanałów.

Wszystkie nielicencjonowane urządzenia 802.11y są określane mianem STA. Standard 802.11y wymaga od stacji bazowej lub punktu dostępowego nie tylko nawiązania połączenia z klientem, ale również możliwości zastosowania ograniczenia dostępu. Mechanizm, który służy do zarządzania połączeniem, to DSE (ang. *Dependent Station Enablement*).

Ta metoda dostępu jest określana mianem „lekkiej licencji” i może być stosowana również w odniesieniu do innych pasm standardu 802.11y. Poza pasmami 4,9 GHz i 5,0 GHz analizowana jest grupa innych częstotliwości, należących do grupy IMT-Advanced: 450 – 862 MHz,

2300 – 2400 MHz, 2700 – 2900 MHz, 3400 – 4200 MHz i 4400 – 5000 MHz. Przewiduje się, że kiedy urządzenia te w końcu będą dostępne na rynku, umożliwią osiągnięcie prędkości transmisji na poziomie około 100 Mbit/s dla aplikacji mobilnych i 1 Gb/s dla łączy stacjonarnych.

Wymienione pasma stanowią przypisane częstotliwości (np. dla odpowiednich służb), które często nie są w rzeczywistości użytkowane, nawet w gęsto zabudowanych obszarach. Dostępność łączy w tych pasmach jest zależna od czasu i położenia geograficznego, gdzie odbywa się transmisja danych. Na przykład na niektórych obszarach znajdują się wolne kanały pasma przeznaczonego dla analogowej telewizji naziemnej (tzw. *white spaces*). Chodzi o to, aby korzystając z różnych technologii zapewnienia wielodostępu do łączy radiowego, udostępnić te częstotliwości dla usług transmisji danych.

## Modulacja

W standardzie 802.11b, który został wprowadzony w 1999 r., zastosowano modulację CCK (ang. *Complementary Code Keying*), polegającą na tzw. kluczowaniu kodem komplementarnym. Kody komplementarne to zestaw sekwencji o takiej samej długości, utworzony tak, że liczba par stanów o tych samych własnościach jest równa liczbie par o własnościach przeciwnych. Dzięki tej modulacji można łatwiej rozpoznać zakodowany sygnał; łatwiej niż z zastosowaniem kodów Barkera, wykorzystanych pierwotnie w standardzie 802.11.

Modulacja polegająca na kluczowaniu fazy PSK (ang. *Phase Shift Keying*) lub jeden z jej wariantów jest cyfrową modulacją sygnału, wykorzystywaną niemal we wszystkich normach grupy 802.11x (z wyjątkiem 802.11b i pierwotnej postaci 802.11). W tej modulacji sygnały są kodowane przez zmianę fazy fali nośnej, gdzie każda faza reprezentuje określone dane binarne. W tej modulacji znany jest kod odwzorowujący zmianę fazy sygnału na określone symbole (znaki), dzięki czemu można zdemodulować sygnał po stronie odbiorczej na podstawie tablic odwzorowania przechowywanych w odbiorniku. Jeśli system dokonuje porównania odebranego sygnału z zestawem sygnałów referencyjnych, mówimy o technologii CPSK (ang. *Coherent Phase Shift Keying*).



Sygnał cyfrowy może być zmodulowany przy użyciu modulacji należącej do grupy technologii utworzonych z wykorzystaniem modulacji amplitudy (ASK) lub modulacji fazy (PSK).

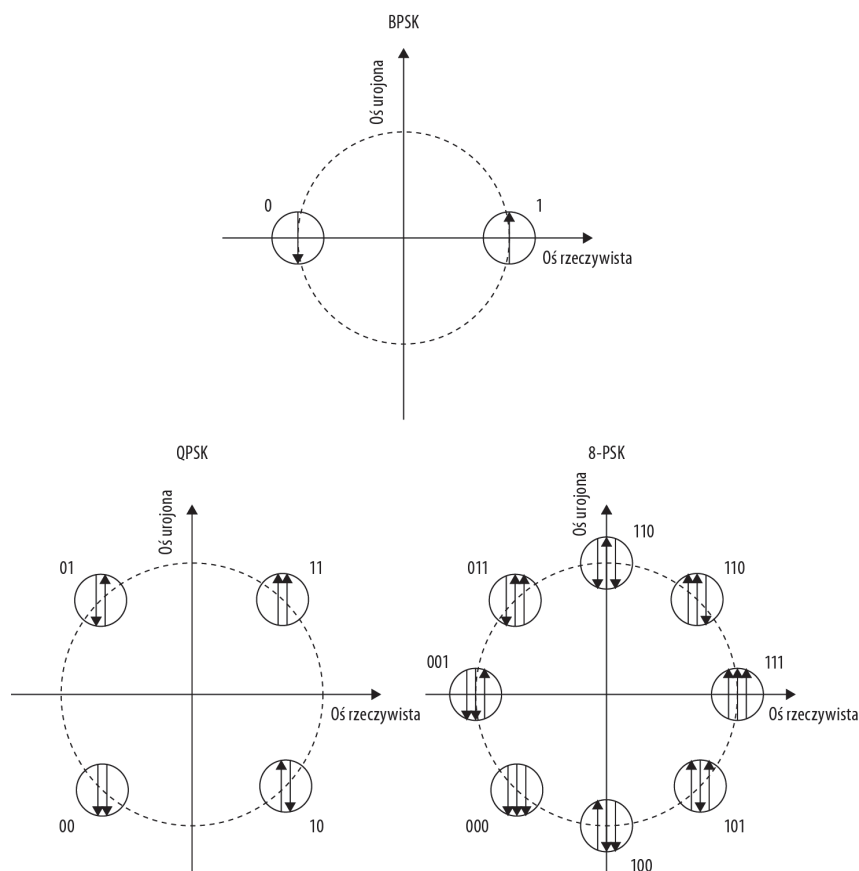
Istnieje wiele odmian modulacji PSK. Jedną z nich jest DPSK (ang. *Differential Phase Shift Keying* — różnicowa modulacja fazy). W tej modulacji wartość binarna określana jest przez stopień przesunięcia fazy względem bieżącej wartości (bieżącego znaku, bitu). Dzięki temu mamy prosty algorytm modulacji i nie musimy korzystać z jakichkolwiek tablic odwzorowania. To sprawia, że w DPSK kodowanie i dekodowanie sygnału jest łatwiejsze i szybsze w porównaniu z CPSK. Wadą jest wprowadzenie większej liczby błędów w trakcie demodulacji.

Modulację PSK można przedstawić za pomocą specjalnego wykresu, tak zwanego diagramu konstelacji. Diagram jest wykresem zespolonym, gdzie konkretne liczby zespolone są reprezentowane przez część rzeczywistą osi  $x$  (w fazie osi) i część urojoną w osi  $y$  (oś kwadratury). Wykres jest dwuwymiarowy w płaszczyźnie zespolonej (zwanej czasem płaszczyzną

Arganda). Płaszczyzna umożliwia reprezentację funkcji zmiennych w czasie w postaci punktów na okręgu. Górny fragment rysunku 14.6 przedstawia modulację z binarnym kluczowaniem fazy BPSK (ang. *Binary Phase Shift Keying*), najprostszej odmiany modulacji fazy.

### Rysunek 14.6.

Diagramy konstelacji modulacji BPSK, QPSK i 8-PSK



W tej modulacji wykorzystuje się dwa stany, reprezentowane przez przesunięcie fazowe o 180 stopni. Fakt, że oba stany są nakreślone na osi rzeczywistej, nie ma znaczenia; stany można zaznaczyć w dowolnym miejscu na okręgu, pod warunkiem że będą przesunięte o 180 stopni.

Spośród wszystkich dostępnych systemów modulacji ten zapewnia najniższą stopę błędów dzięki znaczącej różnicy między stanami, która jest w tym przypadku największa w porównaniu z innymi modulacjami PSK. Wadą modulacji BPSK jest to, że jej system kodowania umożliwia przesłanie pojedynczego bitu. Zatem jest to stosunkowo wolna modulacja i z tego powodu często jest zastępowana szybszymi odmianami PSK.

Na rysunku 14.6 przedstawiono obok BPSK również modulacje wyższego rzędu. Wspomniany rysunek pokazuje reprezentację tych modulacji na diagramie konstelacji. Jedną z nich jest kwadraturowa modulacja fazy QPSK (ang. *Quadrature Phase Shift Keying*), znana też jako 4-QAM lub 4-PSK. Ten system umożliwia kodowanie czterech stanów, a każdy z nich reprezentuje dwa bity. Łatwo zauważyć, że symbole między sobą różnią się tylko jednym bitem. Taki schemat kodowania nazywa się kodem Graya.

Z matematycznego punktu widzenia modulację QPSK można przedstawić jako dwie nośne będące w kwadraturze, czyli złożenie dwóch niezależnych modulacji BPSK. W ten sposób można dowiedzieć, że wskaźnik błędu w QPSK jest taki sam jak w przypadku modulacji BPSK. Modulacja QPSK umożliwia przesyłanie danych z dwukrotnie większą szybkością w porównaniu z BPSK (dzięki dwukrotnie większej efektywności wykorzystania widma), przy użyciu tego samego pasma. Dzięki temu QPSK umożliwia lepsze spożytkowanie dostępnego łącza radiowego. Przepustowość gwarantowaną przez zastosowanie BPSK możemy uzyskać, stosując jedynie połowę pasma przy użyciu modulacji QPSK.

Łatwo można sobie wyobrazić utworzenie wyższego rzędu modulacji poprzez podwojenie liczby stanów modulacji QPSK, co w diagramie konstelacji oznaczmy ośmioma dostępnymi stanami. Ta modulacja jest określana mianem 8-PSK, a każdy stan koduje aż trzy bity kodu Graya. Diagram konstelacji dla 8-PSK jest przedstawiony w prawym fragmencie rysunku 14.6. Praktycznie rzecz biorąc, 8-PSK jest najwyższym poziomem modulacji typu PSK ze stosowanych obecnie. Wyższe poziomy nie są w użyciu ze względu na dużą ilość błędów. Aby jeszcze efektywniej spożytkować pasmo, trzeba skorzystać z innych metod modulacji, na przykład z modulacji amplitudy, której reprezentantem jest kwadraturowa modulacja amplitudowo-fazowa QAM (ang. *Quadrature Amplitude Modulation*).

QPSK stanowi podstawę wielu innych technik modulacji. Można na przykład rozdzielić cztery przesunięcia na dwie pary przesunień i każdą z nich zmodulować przy użyciu innej techniki, zapewniając przesunięcie w czasie. Jedną z nich będzie sinusoida, a drugą — cosinusoida, dzięki czemu otrzymamy dwa niezależne sygnały przesunięte o 180 stopni w fazie.

Techniką wywodzącą się z QPSK jest OQPSK (przesunięta modulacja QPSK), polegająca na przesunięciu w czasie bitów parzystych i nieparzystych o znak jednego bitu. W ten sposób w trakcie przesyłania kolejnych symboli sygnał zmieni się maksymalnie w fazie o 90 stopni. Modulacja OQPSK jest wydajniejsza przy zastosowaniu filtra dolnoprzepustowego, w który zwykle wyposaża się nadajniki.  $\Pi/4$ -QPSK to kolejna odmiana modulacji z przesunięciem 45 stopni (lub  $\pi/4$ ).

W standardzie łączności bezprzewodowej 802.11a zaplanowano 52 fale nośne w kanale, w przedziale częstotliwości 4915-5825 GHz, oraz przesunięcie kanałów wynoszące 20 MHz. W normie 802.11a wykorzystano modulacje BPSK, QPSK, 16QAM, 64QAM i wiele schematów kodowania. Wynika to z wymagań przepustowości: systemy 802.11a powinny zapewnić do 54 Mb/s, z czasem 3,2  $\mu$ secs na symbol.

Po zapoznaniu się z formowaniem sygnałów nośnych warto poznać metody multipleksacji sygnałów. Obecnie stosuje się dwa rodzaje technologii rozproszonego widma z wykorzystaniem skakania po częstotliwościach i — coraz częściej — metody multipleksacji ortogonalnej z podziałem częstotliwości.

## Modulacja DSSS

Modulacja DSSS została wprowadzona w standardach 802.11 (podstawowy) i 802.11b. Widmo rozproszone odnosi się do sposobu, w jaki szerokie pasmo o niskiej, stałej gęstości mocy jest podzielone na kanały radiowe. Zastosowanie widma rozproszonego wymaga użycia znacznie szerszego pasma łącza niż szerokość pasma informacji, a pasmo transmisji może być określone niezależnie od informacji, którą przesyła.

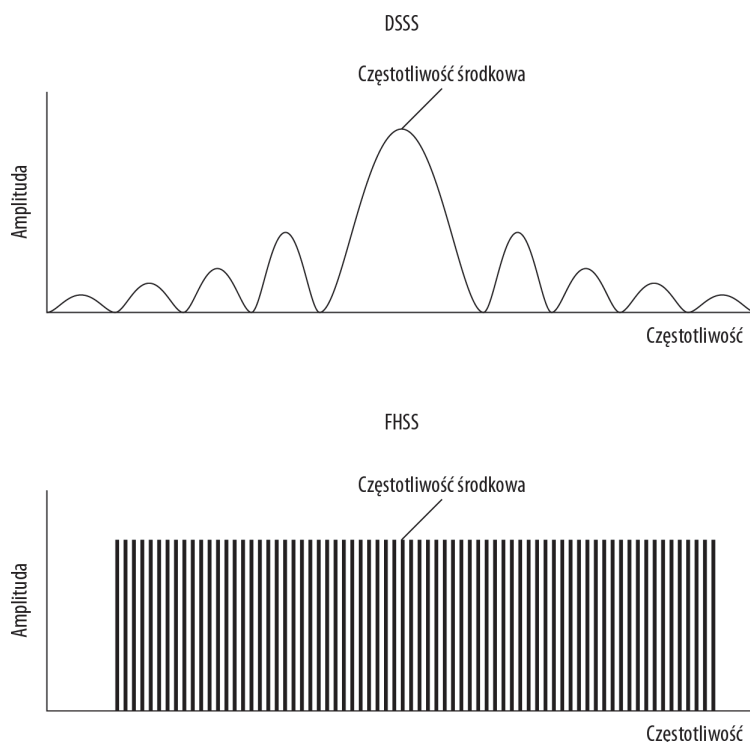


Podstawy multipleksacji zostały przedstawione w rozdziale 5.

Na rysunku 14.7 pokazano widmo częstotliwościowe<sup>3</sup> sygnału DSSS, które można uzyskać przy zastosowaniu analizatora widma. Na wykresie znajduje się amplituda sygnału (oś  $y$ ) w odniesieniu do częstotliwości na osi  $x$ . Wykres w górnej części rysunku ilustruje widmo DSSS, natomiast w dolnej części przedstawiono widmo sygnału FHSS. Warto porównać te wykresy. Technologia FHSS (zwana potocznie skakaniem po częstotliwościach) jest powszechnie używana w telefonii komórkowej i zostanie szczegółowo omówiona w kolejnym podrozdziale.

### Rysunek 14.7.

Widmo sygnału  
zmodulowanego  
DSSS i FHSS



Trzeba zauważyć, że widmo sygnału jest 20 razy większe od widma sygnału niosącego informację. Ogólnie współczynnik szerokości pasma sygnału zmodulowanego do sygnału pierwotnego wynosi 20 – 250:1. Można spotkać także systemy, gdzie ten współczynnik wynosi 1000. Połączenie szerokiego spektrum z sygnałem o niskiej mocy sprawia, że informacje zmodulowane omawianą techniką są bardzo trudne do przechwycenia (charakterystyką są zbliżone do szumu), co powoduje, że ta technologia od dłuższego czasu jest bardzo popularna w zastosowaniach militarnych.

<sup>3</sup> Widmo częstotliwościowe — rozkład mocy składowych harmonicznych sygnału w funkcji częstotliwości. Widmo częstotliwościowe pozwala na analizę zjawisk fizycznych związanych z falami elektromagnetycznymi, takich jak: fale akustyczne, przebiegi napięć zmiennych w obwodach elektrycznych itp. Widmo częstotliwościowe otrzymuje się w wyniku przekształcenia matematycznego, znanego jako transformata Fouriera — *przyp. tłum.*

Systemy modulacji bezpośredniej, opartej na sekwencjach kodowych, czyli rozpraszające ciągi pseudolosowe, polegają na modulacji fali sinusoidalnej odpowiednio dobranym ciągiem pseudolosowym. Szybkość rozpraszającego strumienia pseudolosowego jest dużo wyższa od prędkości sygnału informacyjnego. Ciąg pseudolosowy złożony z tzw. bitów rozpraszających (nazywanych również chipami) jest generowany przez specjalny układ szyfrujący. W odbiorniku znajduje się układ deszyfrujący, w którym zastosowano ten sam kod pseudolosowy. Dzięki temu odbiornik ma możliwość rozpoznania i zdekodowania informacji pochodzącej z nadajnika.

Bez znajomości ciągu pseudolosowego sygnał rozproszony, złożony z „szybkich” sekwencji wartości 1 i  $-1$ , przypomina biały szum<sup>4</sup>, którego energia jest równomiernie rozłożona w całym widmie. Rekonstrukcja sygnału widma rozproszonego polega na przemnożeniu odebranego sygnału przez zsynchronizowany ciąg pseudolosowy, dzięki czemu można otrzymać pierwotne dane, wysłane przez nadajnik. Aby dokonać synchronizacji, należy przesłać odpowiednie dane udostępniające tabelę sekwencji kanałów. Po zsynchronizowaniu nadajnika z odbiornikiem wspomniane dane umożliwiają kontrolę bieżącej pozycji w tabeli sekwencji kanałów.

Zmodulowany sygnał DSSS można poprawić przez zwiększenie sekwencji pseudolosowych i wykorzystanie szybszych ciągów kodowych, dzięki czemu można zwiększyć stosunek mocy sygnału do szumu. Trzeba jednak pamiętać o ograniczeniach technologii wynikających z zysku przetwarzania<sup>5</sup>.

Modulacja z kluczowaniem bezpośrednim umożliwia nakładanie się częstotliwości kanałów dzięki zastosowaniu w każdym z nich niezależnego pseudolosowego ciągu rozpraszającego. Ta własność jest podstawą metody kodowego wielodostępu CDMA (ang. *Code Division Multiple Access*), gdzie w jednym kanale przy zastosowaniu różnych ciągów rozpraszających można przesłać niezależne informacje i zdekodować je w odbiornikach.

Transmisja w widmie rozproszonym ma kilka pożądaných właściwości:

- ♦ Niska moc sygnałów, co także pomaga utrzymać niski stosunek mocy sygnału do mocy szumu.
- ♦ Odporność na inne sygnały radiowe i zakłócenia wąskopasmowe.
- ♦ Redundancja możliwych dróg transmisji.
- ♦ Pojemność wielu strumieni danych, dostępnych z każdego kanału dla wielu użytkowników.
- ♦ Mechanizm zabezpieczeń oparty na zmieniających się przypisanych pasmach.
- ♦ Mała ilość zaników i zjawisk związanych z wielodrogowością.

<sup>4</sup> Biały szum to zbiór sygnałów o przypadkowo zmieniających się w czasie parametrach, w tym sygnałów elektromagnetycznych o całkowicie płaskim widmie. Nazwa pochodzi od światła białego, które jest mieszaniną wszystkich barw (czyli fal elektromagnetycznych o różnej długości w zakresie widzialnym) o płaskim widmie — *przyp. tłum.*

<sup>5</sup> Zysk przetwarzania (zwany również zyskiem kodowym) określa stopień poprawy stosunku mocy sygnału do mocy szumu na wyjściu układu w porównaniu ze stosunkiem mocy sygnału do mocy szumu na wejściu układu. Wartość tego parametru zależy od stosunku pasma częstotliwości sygnału przesyłanego w kanale radiowym do szerokości pasma sygnału modulującego — *przyp. tłum.*

Funkcje te pozwalają na zastosowanie systemów Wi-Fi bez licencji w publicznie dostępnych pasmach częstotliwości. Systemy, w których wykorzystano modulację DSSS, to obok zgodnych ze standardem 802.11b systemów łączności bezprzewodowej również telefonia komórkowa CDMA, telefonia bezprzewodowa (900 MHz, 2,4 GHz i 5,8 GHz), systemy nawigacji satelitarnej Galileo (oraz jej amerykańskiego odpowiednika — GPS-u), systemy łączności bezprzewodowej ZigBee, oparte na standardzie 802.15. 4-2006, oraz systemy automatycznego, bezprzewodowego odczytu danych (tzw. smart metering).

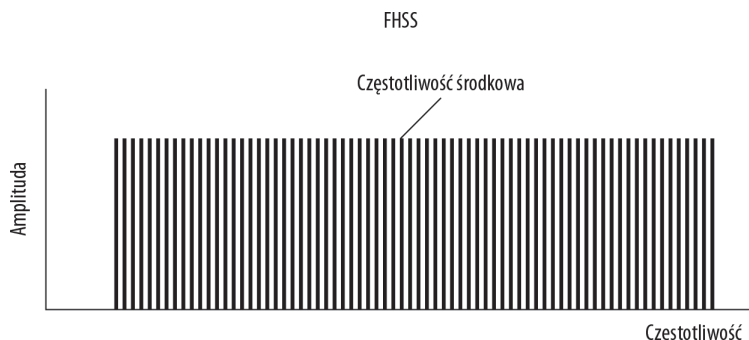
## Modulacja FHSS

Metoda FHSS (skakanie po częstotliwościach w odstępach czasu, w dostępnym widmie, ang. *Frequency Hopping Spread Spectrum*) była wykorzystywana w pierwotnej wersji standardu 802.11. W innych standardach Wi-Fi nie stosowano już tej metody modulacji. Jest ona wykorzystywana w systemach telekomunikacyjnych. Podobnie jak DSSS, FHSS polega na metodzie rozproszenia sygnału. Główną różnicą w porównaniu z DSSS jest to, że FHSS działa na bazie szybkiego przełączania częstotliwości z wykorzystaniem pseudolosowych sekwencji (podobnie jak w DSSS).

Rysunek 14.8 przedstawia widmo sygnału FHSS, które można zaobserwować, korzystając z analizatora widma. Kształt fali jest zupełnie inny niż w DSSS (gdzie mieliśmy do czynienia z sygnałem  $[(\sin x) / x]^2$ ). W modulacji FHSS wykorzystuje się wąskie pasma. Energia sygnału może być równomiernie rozmieszczona, co przedstawiono na rysunku 14.8. Można też pominąć niektóre z częstotliwości dostępnego pasma. Za pośrednictwem systemów FHSS można dokonać transmisji danych analogowych lub cyfrowych.

### Rysunek 14.8.

Pasma  
z wykorzystaniem  
modulacji FHSS



Sygnał transmitowany z wykorzystaniem modulacji FHSS jest trudny do wykrycia i przechwycenia. Dzięki zastosowaniu metody rozpraszającej z użyciem ciągu pseudolosowego dla odbiorcy nieposiadającego odpowiednich kodów deszyfrujących sygnał przypomina szum. W celu odtworzenia sygnału informacyjnego należy skorzystać w odbiorniku z sekwencji pseudolosowej, zastosowanej w nadajniku. To sprawia, że przechwycenie informacji jest utrudnione. FHSS, podobnie jak DSSS, umożliwia wykorzystanie pasm częstotliwości używanych również w innych systemach radiowych.

Technologia FHSS jest zastosowana w systemie Bluetooth, gdzie użyto adaptacyjnego skakania po częstotliwościach — AFH (ang. *Adaptive Frequency Hopping*). W AFH używa się częstotliwości najsilniejszych, unikając tych, które zostały w danym momencie uznane za pasma niskiej jakości lub w których występują zbyt duże zakłócenia.

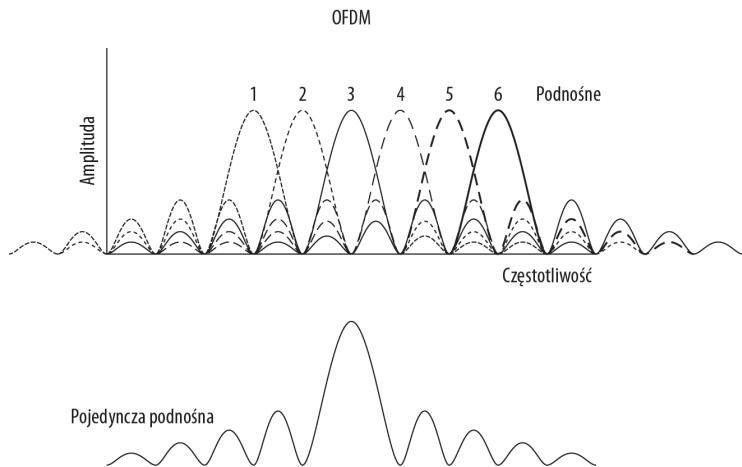
## Modulacja OFDM

Modulacja OFDM (ang. *Orthogonal Frequency Division Multiplexing*) to metoda polegająca na jednoczesnej transmisji wielu strumieni danych z wykorzystaniem ortogonalnych częstotliwości nośnych. Technologia ta została zastosowana w standardach 802.11a/g/n/y. Fale podnośne są w niej nakładane na siebie tak, aby amplitudy maksymalne występowały w tej samej częstotliwości. Aby wykorzystać możliwie wiele podnośnych, trzeba zastosować odpowiednią funkcję multipleksacji. Aby zapewnić efektywność dostępnego pasma częstotliwości, wykorzystuje się szybką transformatę Fouriera FFT<sup>6</sup> (ang. *Fast Fourier Transform*).

Aby zrozumieć zasadę działania OFDM, najlepiej zacząć od budowy fali nośnej. Rysunek 14.9 przedstawia podnośną podstawową, na którą nałożono pięć dodatkowych podnośnych. W górnej części rysunku widać główną podnośną wraz z nałożonymi, dodatkowymi falami, a w dolnej części — obwiednię widma pojedynczej podnośnej.

### Rysunek 14.9.

Złożenie  
ortogonalnych  
podnośnych w nośną  
OFDM



Modulacja OFDM jest powszechnie używana z następujących powodów:

- ♦ Umożliwia niezwykle szybką transmisję danych, sięgającą teoretycznego limitu Nyquista<sup>7</sup>, zapewniając efektywne wykorzystanie dostępnego pasma.
- ♦ Odporność na zakłócenia wąskopasmowe, zaniki i efekty wielodrogowości<sup>8</sup>.

<sup>6</sup> Szybka transformata Fouriera (FFT, ang. *Fast Fourier Transform*) to algorytm liczenia dyskretnej transformaty Fouriera oraz transformaty do niej odwrotnej. FFT ma wiele zastosowań komercyjnych. Tę technikę wykorzystuje się w telekomunikacji do kodowania danych, a także w kodowaniu MP3, obróbce sygnałów transmisji obrazu itp. — *przyp. tłum.*

<sup>7</sup> Dowolny ciągły sygnał, który jest odbierany w skończonym paśmie częstotliwości, może zostać w pełni odtworzony, jeżeli częstotliwość próbkowania jest co najmniej dwukrotnie większa od częstotliwości sygnału. Jest to tzw. częstotliwość Nyquista, a wspomniana reguła to twierdzenie Nyquista, w którym możemy wyróżnić: krok próbkowania jako  $ts = 1/f_{max}$ , gdzie  $f_{max}$  to częstotliwość maksymalna — *przyp. tłum.*

<sup>8</sup> Zjawisko wielodrogowości polega na tym, że do odbiornika dociera sygnał bezpośredni i zbiór sygnałów odbitych. Sygnały odbite pokonują większą drogę, zatem docierają do odbiornika z przesunięciem czasowym. W efekcie w odbiorniku pojawia się kilka kopii sygnału informacyjnego, przesuniętych w czasie. Odbiornik zatem dekoduje kilka bitów jednocześnie zamiast spodziewanego jednego bitu. Ten problem w dużej mierze rozwiązuje stosowanie OFDM — *przyp. tłum.*

- ♦ Odporność na błędy synchronizacji czasu (OFDM jest wrażliwa na błędy synchronizacji częstotliwości).
- ♦ Umożliwia efektywne wykorzystanie FFT do przetwarzania sygnałów.

Transmisja danych powoduje wprowadzenie zniekształceń i obniżenie mocy sygnału wraz ze wzrostem odległości pomiędzy nadajnikiem a odbiornikiem. *Zniekształcenia* są powodowane przez opór w przewodach linii transmisyjnych, a w łączach radiowych — przez zjawisko wielodrogowości, zakłócenia częstotliwościowe itp. Wielodrogowość oznacza odbiór sygnału informacyjnego w postaci fali bezpośredniej i co najmniej jednej, dodatkowej fali odbitej. Wielodrogowość nakłada ograniczenia na liczbę podnośnych, których można użyć w danym systemie transmisji, a czasami wymaga zastosowania pustej podnośnej, zwanej pasmem ochronnym, zapewniającym dodatkowy czas na buforowanie i przetwarzanie sygnałów odbitych. Zakłócenia związane z zagęszczeniem wielu sygnałów informacyjnych są określane mianem interferencji międzysymbolowych ISI (ang. *InterSymbol Interference*). Zastosowanie pasma ochronnego także przyczynia się do zmniejszenia problemów wynikających z niedoskonałych ortogonalności sygnałów, co prowadzi do zakłóceń między nośnymi ICI (ang. *InterCarrier Interference*). Wykorzystanie dodatkowych technik wraz z OFDM umożliwia zachowanie odpowiednich poziomów tolerancji na różne zakłócenia, ale interferencje ISI i ICI to główne problemy technologii OFDM.

Dodatkową, istotną wadą OFDM jest wymaganie większej mocy sygnałów w porównaniu z innymi technologiami.

Każda z podnośnych jest wykorzystywana do przesyłania danych, które są zakodowane przy użyciu różnych metod modulacji, takich jak PSK czy QAM. Sygnał danych jest zatem nałożony na falę nośną przy stosunkowo niskiej szybkości transmisji bitów (zwaną także prędkością symbolową). Dzięki zastosowaniu wielu podnośnych, z których każda transmituje część strumienia danych, przepustowość systemu jest równa lub wyższa w porównaniu z innymi technologiami, działającymi na bazie jednej nośnej.

OFDM jest obecnie dominującą formą multipleksowania, wykorzystywaną w cyfrowej komunikacji szerokopasmowej. Ta technologia jest obecna w systemach przewodowych, takich jak ADSL, oraz bezprzewodowych, takich jak Wi-Fi, cyfrowe radio i telewizja cyfrowa, telefonia komórkowa trzeciej generacji. OFDM jest tak popularną technologią, bo umożliwia wykorzystanie nowych technik modulacji bez konieczności wymiany infrastruktury.

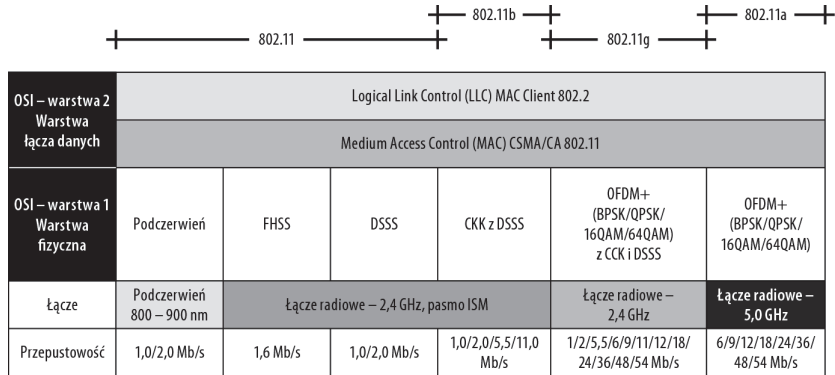
## Protokół 802.11

Protokół 802.11 definiuje ramki i sposób ich transmisji w warstwie fizycznej i MAC (podwarstwie łącza danych) z wykorzystaniem protokołu CSMA/CA. Standardy grupy 802.11x, przedstawione w kilku poprzednich punktach, określają mechanizm dostępu do sieci i definiują porty komunikacyjne, używane przez urządzenia bezprzewodowe do podłączenia z siecią Ethernet. Rysunek 14.10 pokazuje rozmieszczenie poszczególnych standardów 802.11 w odniesieniu do modelu OSI.

W modelu OSI warstwa MAC obsługuje synchronizację, zarządzanie energią, usługi przenoszenia (roaming) oraz usługi zarządzania sprzętem w sieci. Warstwa fizyczna zawiera protokół PLCP (ang. *Physical Layer Convergence Protocol*) i podwarstwy zależne od nośnika

**Rysunek 14.10.**

Protokół 802.11  
i odniesienie  
do modelu ISO/OSI



PMD (ang. *Physical Medium Dependent*). PLCP jest warstwą, która obsługuje wykrywanie nośnej (część protokołu CSMA/CA). Podwarstwa PMD jest odpowiedzialna za modulację i kodowanie sygnału. Z rysunku 14.10 wynika, że w warstwie fizycznej wykorzystuje się kilka różnych systemów modulacji. Należą do nich IR, CCK, FHSS, DSSS oraz OFDM, które zostały opisane wcześniej w niniejszym rozdziale. Modulację CCK opisano w części dotyczącej modulacji.

## Unikanie kolizji

Istnieją dwa główne systemy unikania kolizji, które są stosowane w połączeniach bezprzewodowych zgodnych ze standardem 802.11. Jedną z nich jest mechanizm DCF (ang. *Distributed Coordination Function*), zwany także metodą PCSM (ang. *Physical Carrier Sense Method*), a drugą — mechanizm PCF (ang. *Point Coordination Function*). Mechanizm DCF polega na tym, że przed wysłaniem danych stacja nasłuchuje medium i rozpoczyna transmisję ramek dopiero wtedy, gdy medium jest wolne. Krótkie okresy pomiędzy transmisją kolejnych ramek pojawiają się w sposób losowy. Mechanizm DCF wymusza na stacji nadawczej zatrzymanie transmisji kolejnych ramek i retransmisję poprzedniej (ARQ), jeśli nie otrzyma od stacji odbiorczej potwierdzenia jej otrzymania (ACK) bądź otrzyma potwierdzenie negatywne (NAK). Inne stacje, które chcą się włączyć do „rozmowy”, są ograniczone przez fakt, że czas oczekiwania pomiędzy ARQ i ACK/NAK jest znacznie krótszy niż okres nasłuchu dostępu do medium.

Druga technologia unikania kolizji to PCF. Gdy odległość pomiędzy nadajnikiem i odbiornikiem jest znaczna, odstęp czasu pomiędzy ARQ i ACK/NAK może być zbyt długi, aby uniknąć zakłóceń w transmisji danych. W przypadku znaczących opóźnień inne stacje mogą nadawać swoje paczki danych po wykryciu ciszy w kanale transmisyjnym. W ten sposób wystąpi kolizja w punkcie zbiorczym transmisji danych, którym jest zwykle punkt dostępu AP. Zjawisko to nosi nazwę ukrytego węzła; dwa komputery w sieci bezprzewodowej, znajdujące się w dużej odległości, nie rozpoznają siebie.

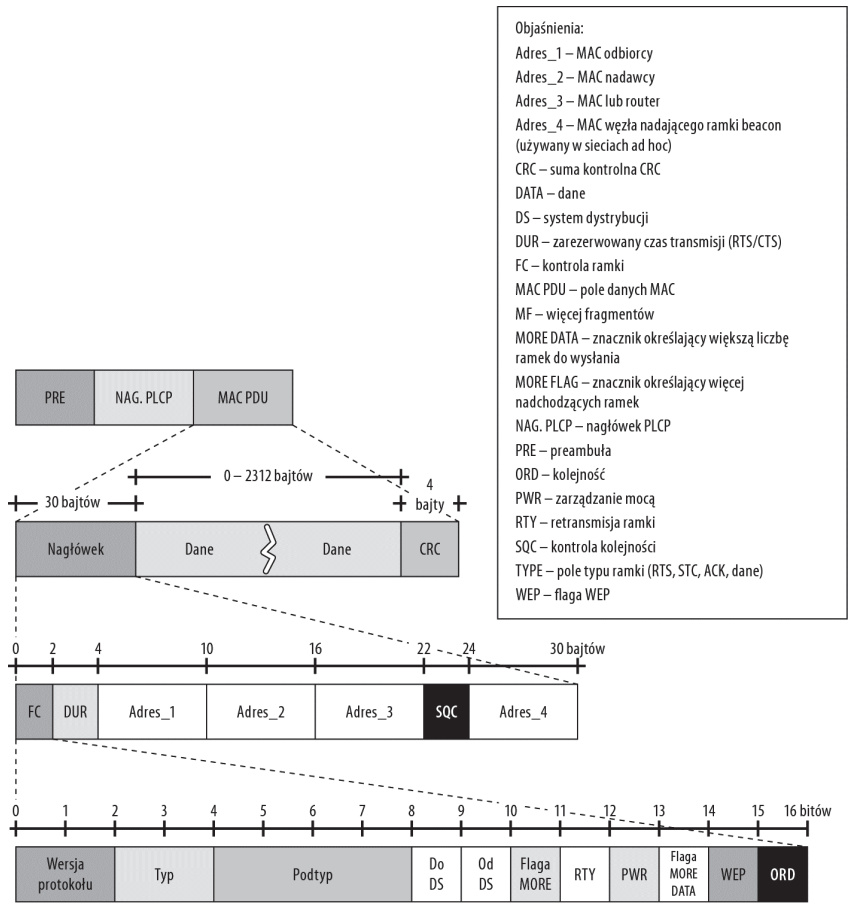
W sieci Ethernet, przedstawionej w rozdziale 11., używa się protokołu CSMA/CD, w którym zamiast mechanizmu unikania zaimplementowano mechanizm detekcji kolizji. W sieciach bezprzewodowych wykrywanie kolizji jest niezwykle trudne. W Wi-Fi zaimplementowano mechanizmy unikania kolizji, powodujące niestety zwiększenie transmisji koniecznych informacji nadmiarowych i zmniejszenie przepustowości łącza.

Potencjalnym rozwiązaniem problemu ukrytego węzła jest utworzenie odpowiednika współdzielonego obwodu zarządzanego w punkcie dostępu. Mechanizm PCF wymaga od stacji nadawczych wysyłania żądania o nadawanie RTS (ang. *Request To Send*) do punktu dostępu. RTS jest następnie przekazywany do innych węzłów sieci bezprzewodowej, a po pewnym czasie, jeśli punkt dostępu nie wykrywa transmisji pochodzącej z innego węzła, wysyła zezwolenie na nadawanie pakietów CTS (ang. *Clear To Send*) do węzła, który nadał RTS, a następnie blokuje obwód w celu realizacji konkretnej transmisji danych.

### Struktura ramki 802.11

Rysunek 14.11 przedstawia ramkę MAC zdefiniowaną w standardzie 802.11. Jest ona podobna do struktury ramek Ethernet, opisanej szczegółowo w rozdziale 13. Ramka składa się z trzech części: preambuły, nagłówka PLCP i właściwego pola MAC PDU, które zawiera wszystkie dane, i pola protokołu 802.11. MAC PDU składa się z trzech części: nagłówka, pola danych oraz pola sumy kontrolnej CRC32, używanego do sprawdzania poprawności ramki. Pole danych jest polem o zmiennej długości, pochodzi z warstw wyższych protokołu, a mechanizm sum kontrolnych CRC jest algorytmem standardowym, zatem warto przyrzeć się bliżej jedynie strukturze nagłówka ramki MAC. Na rysunku 14.11 linią przerywaną wskazano pole, którego szczegóły przedstawiono poniżej.

**Rysunek 14.11.**  
Struktura ramki  
802.11



Kontynuując podróż do wnętrza ramki standardu 802.11, spójrzmy najpierw na pole nagłówka. To pole zawiera wszystkie dane warstwy sesji. Niezwykłość nagłówka polega na tym, że zawiera aż cztery pola adresowe, podczas gdy w ramce Ethernet mieliśmy do czynienia z dwoma polami adresowymi: nadawcy i odbiorcy. Ramka standardu 802.11 musi zawierać nie tylko adresy nadawcy i odbiorcy, ale również adres MAC punktu dostępu, przez który dana ramka zostanie przesłana. Jeśli mamy do czynienia z siecią typu peer-to-peer lub ad hoc, czwarte pole adresowe zawiera adres inicjatora, który wysyła ramki beacon. Dzięki temu inne klienty mają informację, jak łączyć się z tą siecią. Pole adresu zawiera:

- ♦ Adres\_1 to adres odbiorcy, przeznaczenia (RA, ang. *Receiver Address*).
- ♦ Adres\_2 to adres nadawcy (TA, ang. *Transmitter Address*).
- ♦ Adres\_3 to adres docelowy ramki (DA, ang. *Destination Address*).
- ♦ Adres\_4 to adres źródłowy (SA, ang. *Source Address*), czyli adres MAC węzła, w którym powstała ramka.

Pole DUR służy do definiowania czasu aktywności ramki. Czas ten określa, czy ramka ma być dalej przesyłana, czy też powinna zostać odrzucona przez system. Pole FC zapewnia mechanizm, dzięki któremu można rozróżnić poszczególne rodzaje ramek 802.11. Aby móc ustawić sekwencję ramek, umieszczono pole SQC, które zawiera 12-bitowy identyfikator sekwencji i 4-bitowy numer fragmentu ramki, określający jej miejsce w sekwencji. Pole sekwencji jest licznikiem, którego wartość rozpoczyna się od 0 i jest zwiększana aż do 4095, po czym następuje zerowanie licznika. Pole określające fragment jest również licznikiem. Jego wartość w zależności od wartości granicznej ramki jest zwiększana do 16 lub 24.

Pole FC jest ostatnim polem przedstawionym na rysunku 14.11. To 16-bitowe pole zawiera następujące elementy:

- ♦ **Wersja protokołu.** To pole zawiera wersję protokołu 802.11, służy do tworzenia ramki. Każda stacja odbiorcza może ustalić na podstawie wartości tego pola sposób jej obsługi.
- ♦ **Typ.** Pole to zawiera wartość, która określa, czy ramka jest ramką sterowania, danych, czy zarządzania. Na przykład 00 to ramka zarządzania, a niektóre z jej podtypów to Probe Req 0100, Probe Resp 0101, beacon 1000 i tak dalej.
- ♦ **Podtyp.** Niektóre typy ramek są związane z zestawem podtypów wykorzystywanych do wykonywania określonych działań. Ramka sterowania może mieć jeden z podtypów: RTS, CTS i ACK. Ramka danych nie ma podtypów. Ramka zarządzania zawiera beacon, Probe Request/Response, Association Request/Response, Reassociation Request/Response, Disassociation, Authentication i Deauthentication.
- ♦ **Do DS i Od DS.** Te dwa pola określają, czy ramka będzie transmitowana do/od centrum dystrybucyjnego między komórkami w sieci komórkowej, czy do/z routera w sieci rozproszonej.
- ♦ **Flaga MORE.** Ta wartość pola wskazuje, czy istnieje więcej fragmentów do przesłania.
- ♦ **Flaga RTY.** Oznacza, że ramka została już wysłana.
- ♦ **Flaga PWR.** Określa tryb pracy (aktywny lub oszczędzania energii).

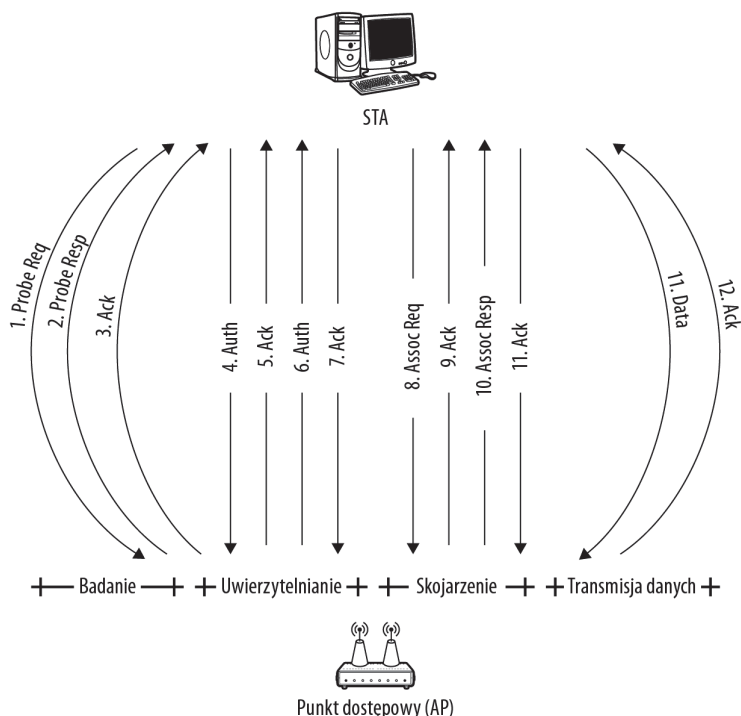
- ♦ **Flaga MORE DATA.** Flaga informująca o nadawaniu większej liczby ramek, przydatna dla stacji pracujących w trybie oszczędzania energii. Jeśli tę ramkę otrzyma punkt dostępu AP, to znaczy, że przesyłane są ramki w trybie rozgłoszeniowym lub do wielu odbiorców (multicast).
- ♦ **Pole WEP.** To pole wskazuje, czy wykorzystano protokół Wireless Encryption Protocol (WEP).
- ♦ **Pole ORD.** To pole informuje odbiorcę, że dana sekwencja powinna być przetwarzana po kolei.

## Przykład połączenia

Przyjrzyjmy się pokrótce procesowi połączenia klienta infrastrukturalnej sieci bezprzewodowej z punktem dostępowym. Połączenie można podzielić na trzy części: skanowanie, uwierzytelnianie i skojarzenie. Skojarzenie oznacza nawiązanie połączenia z punktem dostępowym. Po skojarzeniu klient jest połączony z punktem dostępowym, co logicznie odpowiada połączeniu jak w sieci przewodowej. Rysunek 14.12 przedstawia opisaną wymianę informacji.

### Rysunek 14.12.

*Wymiana informacji podczas procedury powiązania stacji STA z punktem dostępowym AP*



Istnieją dwa rodzaje skanowania sieci: aktywne i pasywne. Podczas aktywnego skanowania stacja wysyła żądanie w postaci ramki Probe Req i oczekuje na odpowiedź od punktu dostępowego AP w postaci ramki Probe Resp. W trybie pasywnym stacja pracuje w trybie nasłuchu i czeka na pojawienie się ramki beacon. Wspomniane ramki w zależności od typu zawierają określone informacje w polu danych.

Fragment *Uwierzytelnianie* jest zależny od użytej metody szyfrowania: otwarte połączenie, połączenie szyfrowane WEP lub WPA. Najprostsze jest otwarte połączenie. W tym przypadku stacja wysyła ramkę do AP, który odpowiada ramką uwierzytelniania i autoryzacji.

Aby utworzyć skojarzenie na podstawie klucza współdzielonego i WEP, szyfrowanie WEP musi być włączone w obu punktach połączenia. Stacja wysyła ramkę uwierzytelniania, a w odpowiedzi od punktu AP otrzymuje niezaszyfrowaną ramkę uwierzytelniania. STA w odpowiedzi przesyła zaszyfrowaną ramkę Authentication. Punkt dostępowy AP deszyfruje odpowiedź i porównuje ją z oryginalną ramką. Jeśli informacja się zgadza, stacja STA otrzymuje informację o pomyślnie przeprowadzonej procedurze skojarzenia.

## Punkty dostępu i bramy

Bezprzewodowy punkt dostępowy (AP lub WAP) to urządzenie nadawczo-odbiorcze, które jest węzłem w sieci bezprzewodowej. Punkt AP stanowi połączenie sieci przewodowej z siecią bezprzewodową. Można powiedzieć, że punkt dostępowy AP jest swego rodzaju mostem pomiędzy siecią przewodową a siecią bezprzewodową. Punkt AP może również być mostem między dwoma sieciami przewodowymi; wówczas mamy do czynienia z połączeniem AP – AP. W trakcie wizyty w kawiarni z bezprzewodowym dostępem do sieci najprawdopodobniej skorzystamy z usługi realizowanej za pośrednictwem punktu dostępowego.

Większość punktów dostępowych AP ma ograniczenie pojemności do jednej podsieci, zawierającej 255 klientów. W praktyce liczba jednocześnie realizowanych połączeń jest jeszcze mniejsza. Na rynku można kupić punkty dostępowe AP działające w standardzie 802.11a (rzadko), 802.11b (często), 802.11g (często), 802.11n (nowe rozwiązania) albo działające w kombinacji dwóch lub trzech z wymienionych standardów. Najczęściej spotyka się kombinację 802.11b/g, 802.11a/g jest rzadziej spotykana, a 802.11a/b/g jest najrzadziej spotykaną kombinacją. Urządzenia działające w standardzie 802.11n zwykle nie obsługują innych standardów.

Większość gospodarstw domowych, które mają dostęp do internetu, korzysta z bramki zainstalowanej na styku łącza szerokopasmowego i sieci domowej. Niektóre z tych bram stanowią most pomiędzy siecią WAN a przewodową lub bezprzewodową siecią LAN. Różnica pomiędzy bramą a punktem dostępu polega na zestawie realizowanych usług. Większość bramek ma wbudowane serwery DHCP i DNS, niektóre z rozwiązań są wyposażone w obsługę prostych funkcji dodatkowych, takich jak firewall, translacja NAT, routing. Większość produktów wymaga niewielkich zabiegów konfiguracyjnych — są to urządzenia typu Universal Plug and Play (UPnP). Bramy bezprzewodowe świadczą te same usługi co routery bezprzewodowe, ale te drugie są odporniejsze na wystąpienie błędów transmisji (routing i trasowanie). W celu odróżnienia pozostałych urządzeń od prawdziwych bram używa się określonych nazw, na przykład: brama domowa, brama zintegrowana itp.

Bramy świadczą następujące usługi:

- ♦ łączności bezprzewodowej, opartej na standardach 802.11,
- ♦ kojarzenia, instalacji i konfiguracji urządzeń bezprzewodowych,
- ♦ funkcji routera zgodnego ze standardem 802.3 i trawersacji NAT,

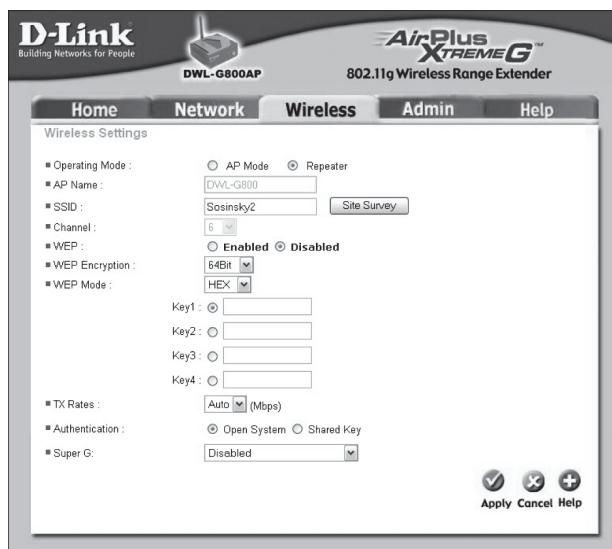
- ♦ DHCP, DNS, IPv6,
- ♦ bezpieczeństwa (WEP i WPA),
- ♦ wykrywania urządzeń i UPnP,
- ♦ diagnostyki.

W następnej części przedstawiono urządzenia, których zadaniem jest rozszerzanie sieci — czyli regeneratory i mosty. Podczas gdy bramy służą do ograniczania zasięgu sieci, regeneratory i mosty służą do jej rozszerzania.

## Regeneratory i mosty

Regenerator jest urządzeniem, które otrzymuje sygnał i retransmituje go z większą mocą. Regeneratory korzystają z tych samych ustawień sieci, nie są elementami powodującymi większą złożoność całej sieci. Umieszczając regenerator w pobliżu granicy zasięgu punktu dostępu, zwiększamy zasięg tego punktu. Większość urządzeń AP może pracować w trybie regeneratora. Na rysunku 14.13 przedstawiono przykładową stronę konfiguratora ustawień urządzenia D-Link 802.11g Wireless Range Extender. Regenerator może wzmocnić sygnał o 50 procent lub więcej, w zależności od wykorzystywanego protokołu, zastosowanych urządzeń i anten.

**Rysunek 14.13.**  
*Ustawienie urządzenia AP na tryb wzmacniaka*



Jeśli jest to możliwe, należy używać regeneratorów i innych urządzeń sieci bezprzewodowej pochodzących od tego samego producenta. W ten sposób unika się problemów związanych z konfiguracją urządzeń różnych producentów.

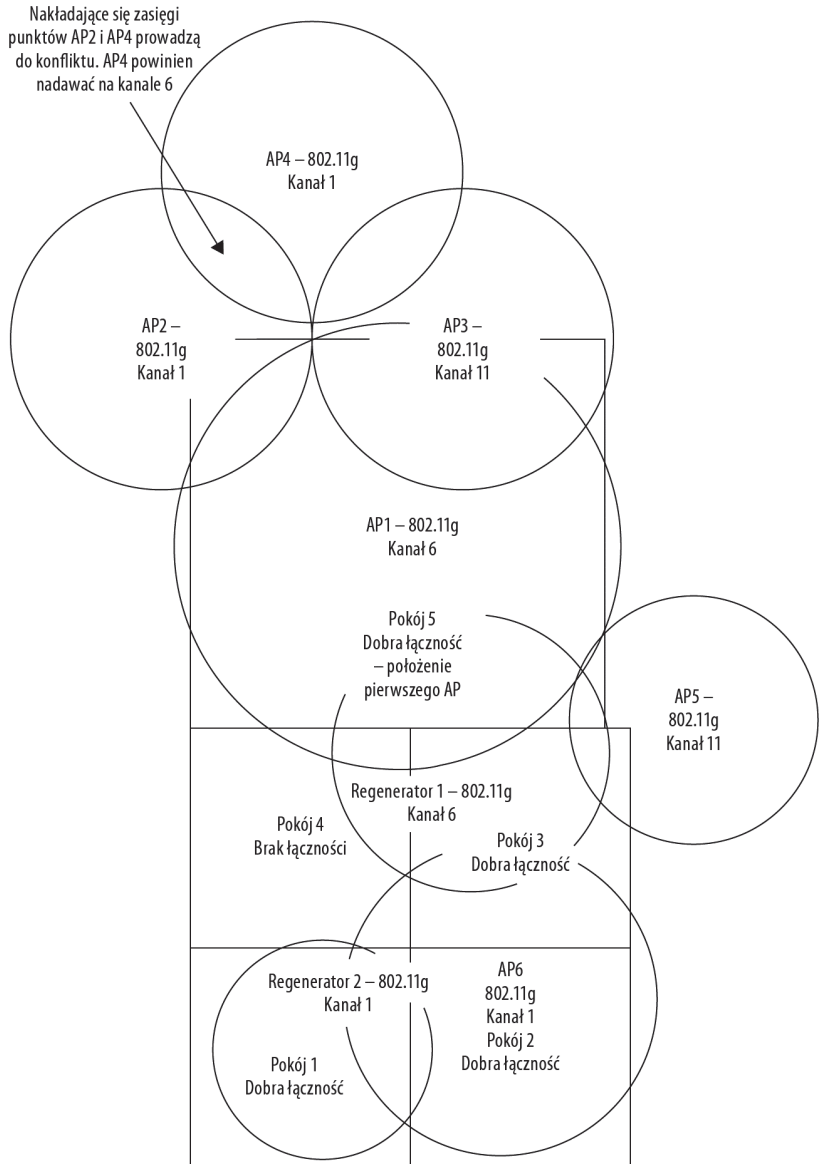
Punkt dostępowy może odbierać sygnał z innego punktu dostępowego za pośrednictwem określonego kanału. Jeśli urządzenie pracuje w trybie regeneratora, trzeba w nim ustawić ten sam kanał i SSID co w urządzeniu źródłowym. Użycie regeneratorów w sieci prowadzi do zmniejszenia ich wydajności, co ogranicza możliwość zastosowania regeneratorów

w większych sieciach lub środowiskach o dużym natężeniu ruchu. Regeneratory muszą przetworzyć dwukrotnie większą liczbę ramek w porównaniu z punktem dostępu. W zastosowaniach domowych lub w małych biurach to rozwiązanie jest wystarczające.

Dobrym sposobem na określenie liczby urządzeń bezprzewodowych potrzebnych w tworzonej sieci jest sporządzenie planu piętra i nakreślenie na nim zasięgu przewidzianych urządzeń. Tego typu rysunek jest cenny przy ustalaniu miejsc, gdzie wymagane są nowe urządzenia, decydowaniu, które stacje będą współpracować z danym punktem dostępu itp. Przykład planu bezprzewodowej sieci lokalnej przedstawiono na rysunku 14.14.

**Rysunek 14.14.**

*Planowanie dostępu do sieci bezprzewodowej z wykorzystaniem schematu piętra*



Nie wszystkie punkty dostępne oferują tryb mostowania. Wiele z tych, które mają taką funkcję, nie realizuje jej efektywnie. Mostowanie dużo lepiej działa w urządzeniach bezprzewodowych skierowanych do rynku przedsiębiorstw niż tych przeznaczonych dla rozwiązań domowych. Budując most pomiędzy dwoma urządzeniami, warto zaopatrzyć się w nie u tego samego dostawcy, a najlepszym rozwiązaniem jest posiadanie dwóch identycznych urządzeń. Aby stworzyć most, należy wykonać następujące czynności:

1. Otworzyć konfigurator pierwszego urządzenia (AP\_1) i ustawić tryb pracy na punkt-punkt (point-to-point) lub most bezprzewodowy (Wireless Bridge).
2. Wpisać adres MAC drugiego punktu dostępowego (AP\_2) do odpowiedniej tabeli (oznaczonej zwykle Bridge).
3. Ustawić SSID i kanał (Channel) w urządzeniu AP\_1.
4. Powtórzyć kroki 1. do 3. dla urządzenia AP\_2, wprowadzając adres MAC AP\_1 do tego urządzenia w tabeli Bridge.
5. Skierować odpowiednio anteny urządzeń i przetestować połączenie.

Może się okazać, że producenci mają różne nazwy dla funkcji mostowania: tryb punktu dostępowego, tryb grupy roboczej w trybie bridge, punkt-punkt, dodatkowy punkt-punkt, punkt-wielopunkt itd. Najczęściej wykorzystywane są topologie:

- ♦ **Punkt-punkt**, topologia „jeden do jednego”.
- ♦ **Punkt-wielopunkt**, topologia „jeden do wielu”. W tym przypadku jeden punkt dostępowy pełni funkcję mostu głównego, pozostałe są zwykłymi mostami. Most główny jest odpowiedzialny za uwierzytelnianie i skojarzenia z resztą urządzeń. Most główny powinien być umieszczony w centralnym punkcie w celu zmaksymalizowania wydajności i zasięgu całej sieci. W połączeniu typu punkt-punkt, gdzie nie ma mostu głównego, zwykły most przejmuje rolę mostu głównego i realizuje jego zadania.
- ♦ **Wielopunktowa, redundantna**. W tej topologii stosuje się duplikat pary końcowych punktów dostępowych, dzięki czemu w przypadku problemu z łącznością za pomocą jednego punktu sieć może skorzystać z drugiego łącza między sieciami.

## Tryb Wireless Distribution System

Tryb Wireless Distribution System (WDS) umożliwia utworzenie mostu pomiędzy dwoma sieciami LAN za pośrednictwem dwóch punktów dostępowych. Punkty dostępowe mogą być podłączone lokalnie do sieci LAN, poprzez regeneratory albo za pośrednictwem innego łącza (tzw. stacji zdalnej). Zadaniem regeneratora jest przekazanie wzmocnionego sygnału pomiędzy dwoma punktami dostępowymi. Funkcja WDS powoduje obniżenie przepustowości łącza o połowę ze względu na przekazywanie całego ruchu pomiędzy routerem a klientem bezprzewodowym.

WDS oferuje dwa tryby pracy:

- ♦ **Most bezprzewodowy pomiędzy dwoma punktami dostępowymi** (połączenie AP – AP).
- ♦ **Regenerator bezprzewodowy**. W tym trybie punkt dostępu wzmacnia sygnał, przesyła go do innego punktu dostępowego, który następnie transmituje informację do odbiorcy końcowego.

Tryb WDS nie jest zdefiniowany w standardzie Wi-Fi. Przy wdrażaniu tego systemu należy w miarę możliwości korzystać z urządzeń pochodzących od jednego producenta.



Akronim WDS jest stosowany również przez Cisco i odnosi się do usługi Wireless Domain Service (usługa domeny bezprzewodowej). Usługa ta jest częścią rozwiązania Cisco o nazwie Structured Wireless Aware Network (SWAN), które jest używane do roamingu obsługi klienta, wdrażania i zarządzania sieciami WLAN.

Klienty wysyłające pakiety za pośrednictwem WDS nie dokonują zmian adresów MAC; dane te w urządzeniach pośrednich nie ulegają modyfikacji. Poszczególne pakiety są automatycznie przekazywane do odbiorców końcowych.

Każdy komponent w WDS ma przypisany identyfikator SSI (ang. *Service Set Identifier*). W systemie znajduje się tabela zawierająca adresy MAC wszystkich punktów dostępowych. W zależności od dostawcy urządzeń usługa WDS może mieć narzucony limit uczestników. Usługa WDS musi być skonfigurowana tak, aby wszystkie urządzenia nadawały na tym samym kanale i były skonfigurowane na podstawie jednego wybranego protokołu zabezpieczeń (WEP lub WPA, z określonym kluczem). W obecnych systemach WDS nie ma mechanizmu automatycznej zmiany kluczy w trakcie sesji. Oznacza to, że WDS działa z szyfrowaniem WEP i WPA-PSK, ale nie obsługuje WPA2.

Aby zestawić połączenie WDS, należy:

1. W konfiguratorze sieci wybrać dwa pierwsze punkty dostępowe, które mają działać w systemie WDS.
2. Znaleźć opcję włączenia WDS i uruchomić ją w pierwszym AP, wprowadzając adres MAC drugiego AP do tabeli WDS.
3. Wybrać kanał pierwszego AP.
4. Otworzyć ustawienia zarządzania drugim AP, włączyć opcję WDS i wpisać adres MAC pierwszego AP do tabeli WDS.
5. Ustawić kanał na drugim AP (ten sam, który skonfigurowano w pierwszym AP).
6. W razie potrzeby dodać kolejne punkty dostępowe.



Błędna konfiguracja WDS może spowodować utworzenie pętli.

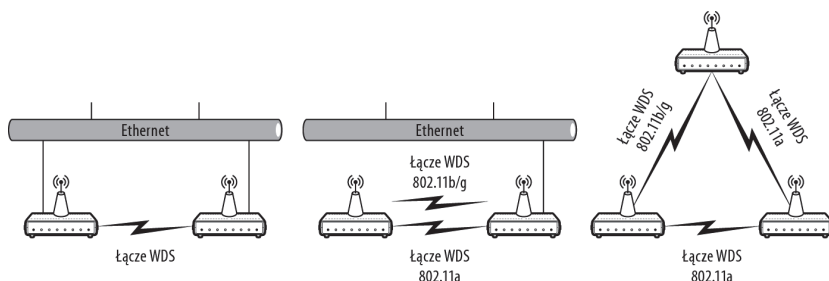
Konfigurując system WDS, można łatwo utworzyć pętlę. Po utworzeniu takiej pętli ruch krążących pakietów doprowadzi do awarii sieci. Aby uniknąć tego problemu, trzeba się upewnić, że unikamy następujących scenariuszy:

- ♦ **Dwa punkty AP w systemie WDS** są podłączone do tego samego łącza Ethernet.
- ♦ **Dwa punkty AP są podłączone do dwóch systemów WDS**, gdzie jeden z nich jest oparty na standardzie 802.11a, a drugi — na 802.11b/g.
- ♦ **Trzy punkty AP są podłączone do trzech niezależnych łączy**, zrealizowanych na podstawie standardów 802.11b/g, 802.11a oraz dwóch łączy w pętli.

Rysunek 14.15 przedstawia sytuacje prowadzące do wystąpienia niepożądanego pętli.

**Rysunek 14.15.**

*Przykłady  
nieprawidłowej  
konfiguracji WDS,  
prowadzącej  
do zatrzymania  
pracy sieci*



W sprzedaży dostępne są następujące produkty wspierające WDS:

- ♦ 3COM Wireless 7760 11a/b/g PoE access point
- ♦ Alcatel Speed Touch (716 i 780)
- ♦ Apple Time Capsule, Airport Extreme i Airport Express
- ♦ Asus WL-500g/gc/gU
- ♦ Belkin FD57230-4
- ♦ Cisco Wireless AP (Aironet)
- ♦ D-Link (DGL-4300, DWL-2100AP, DAP-1160)
- ♦ Motorola WR850G/GS
- ♦ Netgear ProSafe access point (WG102, WAG102, WG302, WAG302 i WG602v2/3)
- ♦ PLANET Wireless AP i router (WAP-4000A, WAP-4033, WAP-4035, WAP-4036, WAP-4060PE, WRT-414, WRT-416 oraz WNRT-620)
- ♦ SMC EZ Connect g Wireless access point (SMCWEBT-G) SMC7988VoWBRA, SMC Barricade SMCWBR14T-G/G2
- ♦ USRobotics Professional access point (5453), MAXg (5432, 5441, 5451, 5455, 5461, 5465 i 9108) oraz Ndx (5454, 5464 i 9113)
- ♦ Zoom X6

Wymieniono jedynie przykłady urządzeń dostępnych obecnie na rynku.

## Routerzy i bramy bezprzewodowe

W rozdziale 9. powiedziano, że routery są urządzeniami łączącymi dwie lub więcej sieci. W routerach wbudowano odpowiednie mechanizmy służące do sterowania ruchem pakietów — są to tabele routingu i algorytmy wyznaczające preferowane trasy. Routery są bramami warstwy trzeciej; w modelu ISO/OSI znajdują się w warstwie sieci.

Bezprzewodowy router realizuje te same funkcjonalności co router przewodowy, ale dodatkowo posiada interfejs bezprzewodowy i może odgrywać rolę punktu dostępowego. Większość niewielkich routerów, przeznaczonych do użytku domowego lub małych biur,

posiada cztery porty Ethernet, wbudowaną funkcję punktu dostępowego z zaimplementowanymi protokołami 802.11 oraz port równoległy lub port USB, dzięki któremu można udostępnić dowolne urządzenie peryferyjne, np. drukarkę. Router Linksys WRT54GL (802.11b/g), przedstawiony na rysunku 14.16, jest klasycznym przykładem urządzenia do zastosowań domowych.

### Rysunek 14.16.

*Router Linksys  
WRT54GL: tani,  
oparty na systemie  
Linux, łatwy  
w konfiguracji*



Największą różnicą pomiędzy routerem a punktem dostępowym jest to, że klient AP ma dostęp tylko do jednej sieci, a router umożliwia połączenie klienta z wieloma sieciami. Routery również mają funkcję badania pakietów i przekazywania ich odpowiednią drogą do miejsca przeznaczenia. Punkty dostępu nie badają pakietów i przekazują wszystkie otrzymane pakiety do sieci.

Z routera należy skorzystać w wymienionych sytuacjach:

- ♦ Mamy tylko jeden dostępny zewnętrzny adres IP. Routery zapewniają też usługi DNS i DHCP, a także współdzielenie adresu IP poprzez NAT.
- ♦ Trzeba podłączyć się do wielu sieci.
- ♦ Znacznie obciążona sieć bezprzewodowa wymaga większej przepustowości niż oferowana przez AP.
- ♦ Potrzeba lepszego zarządzania siecią, bardziej zaawansowanych narzędzi diagnostycznych i możliwości zarządzania poprzez interfejs WWW.
- ♦ Potrzebujemy lepszej ochrony, filtrowania opartego na adresach MAC, adresach IP, nazwach domen, porach dnia; konieczne są inne funkcjonalności, które są często oferowane przez firewalles. Niektóre routery mają obsługę wielu sesji IPsec, VPN, szyfrowania WEP i innych opcji bezpieczeństwa.

## Konfiguracja routera

Większość routerów bezprzewodowych można skonfigurować za pomocą narzędzi uruchamianych w przeglądarce internetowej. W tym celu wystarczy wprowadzić adres IP routera i zalogować się do narzędzia za pomocą identyfikatora i hasła. Zazwyczaj router można skonfigurować ręcznie albo skorzystać z kreatora konfiguracji. Aby skonfigurować router, na ogół trzeba wprowadzić następujące informacje w odpowiednie pola kreatora lub formularza:

- ♦ Adres IP serwera i domeny dla sieci szerokopasmowej lub WAN. W wielu przypadkach ten interfejs sieciowy jest realizowany przez DHCP dostawcy usług, wystarczy go tylko wprowadzić w odpowiednie pole bądź zaakceptować konfigurację automatyczną.
- ♦ Pula adresów IP dla interfejsu sieci bezprzewodowej. Po włączeniu DHCP router może klientom przypisać adres dynamiczny lub statyczny z danej podsieci.
- ♦ Przypisany identyfikator SSID i numer kanału.
- ♦ Typ zabezpieczeń, które chcemy zastosować, oraz nowe dane autoryzacji administratora. Można wprowadzić skorzystać z ustawień domyślnych konta administratora, ale te są powszechnie znane przez hakerów, którzy mogą użyć ich do ataku na system.
- ♦ Wszystkie typy filtrów, które mają być zastosowane w sieci, takie jak filtr adresów MAC.

## Aktualizacja routera

Istnieje dużo oprogramowania dla routerów na licencji freeware lub shareware. Dzięki tym rozwiązaniom router kupiony za około 200 złotych oferuje zaawansowane funkcjonalności, spotykane zwykle w droższych produktach. Przykładem przydatnego oprogramowania jest DD-WRT (autor: Brain Slayer), którego gotowe aktualizacje można pobrać z witryny [www.dd-wrt.com/wiki/index.php/Main\\_Page](http://www.dd-wrt.com/wiki/index.php/Main_Page). Na stronie znajdziemy listę funkcji, która jest zbyt długa, aby ją tu szczegółowo przedstawić. Spośród najważniejszych można wymienić OpenVPN, QoS, Samba, Site Survey, WDS, filtrowanie MAC, WPA na WDS i inne.

Tomato z [polarcloud.com](http://polarcloud.com) ([www.polarcloud.com/tomato](http://www.polarcloud.com/tomato)) to kolejny przykład oprogramowania przygotowanego dla routerów. Wielu dostawców sprzętu załącza również to oprogramowanie do sprzedawanego sprzętu. Narzędzie ma przyjazne dla użytkownika GUI i posiada dużo zaawansowanych funkcji, takich jak monitor przepustowości, QoS, kontrola dostępu, zarządzanie połączeniem (P2P), CIFS (Samba), WDS, Telnet obsługa skryptów.

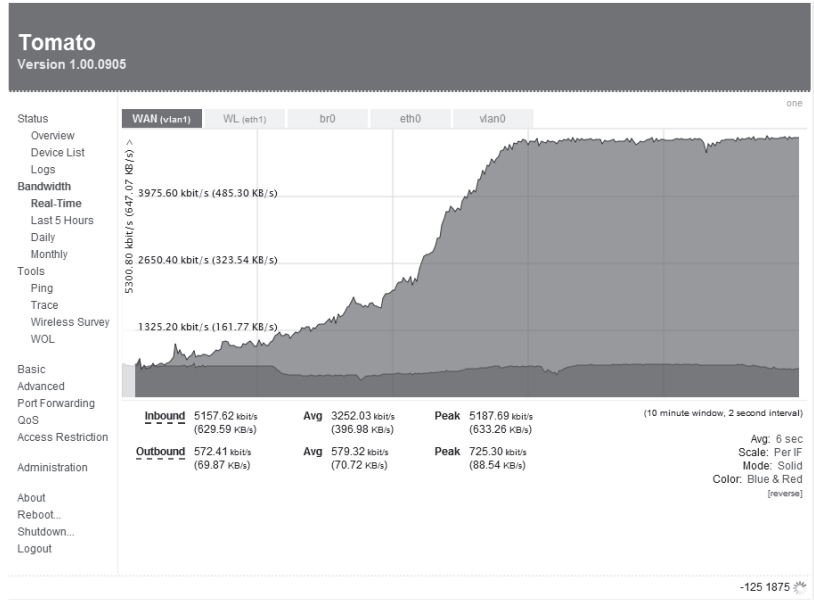
Tomato obsługuje przeglądarki internetowe takie jak Firefox lub Internet Explorer. Rysunek 14.17 przedstawia ekran Bandwidth Usage (wykorzystanie dostępnej przepustowości). Aplikacja Tomato jest szczególnie pomocna w generowaniu raportów. Można na przykład tworzyć wykresy rozkładu połączeń na podstawie reguł QoS.

Tomato jest dostępny dla urządzeń zbudowanych na bazie chipsetu Broadcom, między innymi:

- ♦ Linksys WRT54G v1-v4, WRT54GS v1-v4, WRT54GL 1.x, WRTSL54GS (bez obsługi USB);
- ♦ Buffalo WHR-G54S, WHR-HP-G54, WZR-G54, G54-WBR2;
- ♦ Asus WL500g Premium (bez obsługi USB);
- ♦ SparkLAN WX-6615GT.

**Rysunek 14.17.**

Jedną z ciekawych funkcji aplikacji Tomato jest monitorowanie wykorzystania łącza



Aplikacja Tomato jest bardzo popularna wśród użytkowników routera Linksys WRT54GL („L” w nazwie oznacza, że router korzysta z systemu Linux). Jedną z ciekawszych funkcji oferowanych przez Tomato jest *Signal boosting*, polegający na wzmocnieniu emisji sygnału. WRT54GL domyślnie transmituje z mocą 42 mW. Poprzez odpowiednie ustawienia konfiguracyjne można podnieść wartość mocy emitowanej aż do 251 mW, przy czym 70 mW uważa się za wartość bezpieczną. Ustawienie tej wartości w praktyce podwaja zasięg routera.

Narzędzie Tomato nie jest tak funkcjonalne, jak DD-WRT, ale zapewnia podstawowe funkcje, które można łatwo konfigurować. Oba produkty znacznie poprawiają użyteczność routera bezprzewodowego, pod warunkiem że dany model można zaktualizować tym oprogramowaniem.

## Sieć bezprzewodowa laptopów XO

W projekcie *One Laptop Per Child* (OLPC; [www.laptop.org](http://www.laptop.org)), czyli „laptop dla każdego dziecka”, skorzystano z sieci bezprzewodowej typu ad hoc, która jest niezależna od topologii i samonaprawialna. Każdy laptop może zlokalizować inne dostępne laptopy i utworzyć z nimi sieć, umożliwiającą współdzielenie zasobów. Pierwszy model laptopa o nazwie XO posiada szereg funkcji. Jedną z nich, o której warto tu wspomnieć, jest obsługa sieci kratowej WMN (ang. *Wireless Mesh Network*).

Sieć bezprzewodowa, która samodzielnie się konfiguruje i naprawia, jest określana mianem bezprzewodowej sieci kratowej lub MANET (ang. *Mobile Wireless Ad Hoc Mesh Network*). W przypadku systemów ruchomych, instalowanych w pojazdach, mamy do czynienia z siecią VANET (ang. *Vehicular Wireless Ad Hoc Mesh Network*).

Układ scalony odpowiedzialny za komunikację w bezprzewodowej sieci kratowej, znajdujący się w laptopie XO, uruchamia oprogramowanie, które jest zgodne ze standardami projektu sieci kratowej IEEE 802.11s. Oprogramowanie umożliwia komunikację z innymi urządzeniami bez konieczności konfigurowania jakichkolwiek ustawień. 802.11s wprowadza rozszerzenie do standardu 802.11 MAC, które zapewnia obsługę transmisji w trybie zwykłym, rozgłoszeniowym i multimediami. W sieci 802.11s każdy węzeł jest określany mianem węzła kraty MP (ang. *Mesh Point*). Takimi węzłami mogą być również punkty dostępowe AP, zdefiniowane w standardzie 802.11. Rysunek 14.18 przedstawia laptop XO z widokiem dostępnych węzłów w sieci.

#### Rysunek 14.18.

Laptop XO z widokiem dostępnych węzłów sieci kratowej. Każda ikona przedstawia dostępne urządzenie



802.11s definiuje protokół routingu o nazwie *Hybrid Wireless Mesh Protocol*, w skrócie HWMP. Protokół jest obowiązkowym elementem systemu, zgodnie z zapisem w standardzie. Protokół HWMP umożliwia tworzenie urządzeń przez różnych producentów, dzięki czemu każde urządzenie zgodne z 802.11s może się znaleźć w sieci MANET.

Protokół routingu HWMP bazuje na elementach protokołu AODV (ang. *Ad Hoc On Demand Distance Vector*) i algorytmie przeszukiwania drzewa. AODV korzysta z algorytmu wektora odległości. Protokół jest opisany w projekcie standardu dostępnym w witrynie <http://tools.ietf.org/html/rfc3561>. AODV utworzono na podstawie innego protokołu, DSDV (ang. *Destination-Sequence Distance Vector*), który działał z wykorzystaniem dynamicznych tabel przeskoku. Protokół jest odpowiedni dla sieci z niewielką liczbą węzłów, bo w większych sieciach może wprowadzać problemy wydajnościowe, związane z wyznaczaniem dużej liczby możliwych tras. W AODV poprawiono tę wadę DSDV przy użyciu algorytmu do obliczania metryk trasy, biorącego pod uwagę zarówno liczbę przeskoku, jak i zysk wydajności z przeskoku. Odpowiednie pomiary są dokonywane poprzez wysyłanie pakietu RouteRequest i analizie odpowiedzi RouteReady. W ten sposób system samodzielnie uczy się różnych możliwych tras i wybiera najkorzystniejszą.

Standard 802.11s pozwala na zastosowanie w sieci serwera. W projekcie OLPC zdefiniowano możliwość wykorzystania serwera o nazwie OLPC XS. Ten serwer obsługuje klienty XO, umożliwiając połączenie do 100 laptopów. Laptopy OLPC i serwery OLPC XS są obecnie jedynymi produktami działającymi zgodnie ze standardem 802.11s. Protokoły zdefiniowane w standardzie 802.11s będą zintegrowane z warstwą mac80211 jądra systemu operacyjnego Linux, począwszy od wersji 2.2.26.

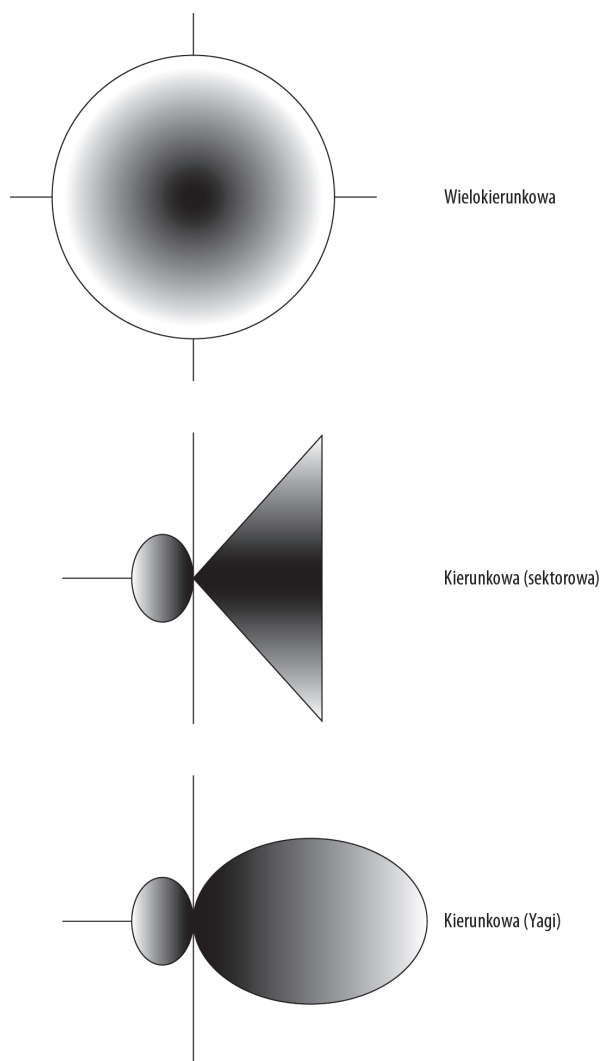
# Anteny

Anteny odgrywają znaczącą rolę w zdolności urządzeń bezprzewodowych do przesyłania lub odbierania sygnałów. Zazwyczaj wykorzystuje się anteny wielokierunkowe, ale czasem używa się również anten kierunkowych. Charakterystyka anteny wynika z jej fizycznej konstrukcji.

Rysunek 14.19 przedstawia trzy rodzaje charakterystyk anten. U góry znajduje się charakterystyka anteny wielokierunkowej. Budowa takich anten zwykle oparta jest na sferze. W środkowej części rysunku pokazano charakterystykę anteny kierunkowej. Najlepszym przykładem takiej anteny jest antena sektorowa, stosowana często w sieciach komórkowych. Innym przykładem anteny kierunkowej jest antena Yagi. Trzy typy anten widać na rysunku 14.19.

## Rysunek 14.19.

*Charakterystyka anten*



## Charakterystyka anteny

Skuteczność anteny określamy mianem zysku anteny, który jest wyrażony w decybelach (dB). Zysk to stosunek mocy sygnału wyjściowego wzmacniacza do mocy sygnału na wejściu układu. Zysk jest zwykle wyrażony w decybelach w odniesieniu do anteny izotropowej i podawany jest w jednostkach dBi. Antena izotropowa to teoretyczna antena, która emituje sygnał równomiernie (izotropowo) we wszystkich kierunkach. Zysk anteny jest parametrem wykorzystywanym w opisie jej nadawczej i odbiorczej funkcji. Jeśli w systemie zastosujemy lepsze anteny, poprawimy jakość sygnału (moc) zarówno po stronie nadawczej, jak i odbiorczej układu.

Anteny są od razu dopasowane do konkretnej częstotliwości (wynika to z ich konstrukcji) albo są to specjalne układy o skomplikowanej budowie, które można regulować. Anteny zaprojektowane dla sygnałów stosowanych w standardzie 802.11b nie będą działać poprawnie w wyższych częstotliwościach (standard 802.11a). Można natomiast wykorzystać anteny zaprojektowane dla 802.11a do transmisji w częstotliwościach zdefiniowanych przez 802.11b.

Fale radiowe ulegają wielu zakłóceniom. W wyniku licznych odbić powstaje efekt wielodrogowości. Klienci, które chcą się podłączyć do sieci bezprzewodowej, wyszukują najmocniejszego sygnału, ale w niektórych miejscach, gdzie teoretycznie powinien być zasięg, tworzą się martwe punkty w wyniku niefortunnej superpozycji sygnałów. Z tego powodu przesunięcie anteny lub obrócenie jej czaszy może mieć duży wpływ na wydajność łącza.

Fale radiowe tracą swą moc wraz ze zwiększaniem się odległości od anteny nadawczej. Utrata mocy ma związek z propagacją w wolnej przestrzeni. Utrata mocy jest wprost proporcjonalna do kwadratu odległości pomiędzy anteną nadawczą i odbiorczą. Wewnątrz budynku propagacja fal zależy między innymi od materiałów wykorzystanych w konstrukcji domu. Beton obniża moc sygnału w większym stopniu niż drewno. Ilość materiału w ścianie rozdzielającej jest również ważna. Na przykład sygnał odbierany na piętrze ma większą moc niż sygnał, który przechodzi przez mocno zabudowany narożnik domu. Niektóre urządzenia bezprzewodowe pozwalają na zmianę mocy nadawania, tym samym zwiększając ich zasięg i moc wypromieniowywaną przez antenę połączoną z urządzeniem.

Antena wielokierunkowa promieniuje we wszystkich kierunkach i zwykle ma postać długiego, cienkiego pręta. Istnieje dużo rodzajów anten kierunkowych, których kąt wiązki głównej wynosi z reguły od 80 do 120 stopni. Anteny kierunkowe są często stosowane w narożnikach pomieszczeń i promieniają do wszystkich stron pomieszczenia; często mają czaszę paraboliczną lub panel, którego zadaniem jest skupianie padających fal radiowych. Do budowy anten kierunkowych można użyć też innych elementów, które ułożone w określony sposób poprawiają kierunkowość. Klasycznym przykładem anteny kierunkowej jest antena Yagi, znana z naziemnych, analogowych systemów telewizyjnych i radiowych. Niektóre anteny kierunkowe umożliwiają zestawienie połączenia nawet w odległości kilkunastu kilometrów, ale takie łącza są bardzo wrażliwe na przeszkody.

Poziom promieniowania wstecznego określa charakter kierunkowy anteny. Parametr ten określa stosunek mocy wypromieniowanej w listku głównym do mocy wypromieniowanej przez listki wsteczne. Poziom promieniowania oznacza się jako F/B (ang. *Front-to-Back*). Parametr F/B idealnej anteny o promieniowaniu dookołnym ma wartość 1,0, anteny wielokierunkowe cechują się wartością bliską 1. W antenach kierunkowych omawiany współczynnik

może przyjmować duże wartości — dla anten typu Yagi jest to nawet 5 lub 6. Rysunek 14.20 przedstawia cztery różne typy anten bezprzewodowych: a) Hawking HAI7SIP Hi-Gain 7 dBi, antena wielokierunkowa; b) Hawking HAI8DD Hi-Gain 8 dBi, antena kierunkowa; c) Hawking HAI15SC Hi-Gain 15 dBi, antena sektorowa; d) Wade J250-915-10 900 MHz 13 dB, antena Yagi.

**Rysunek 14.20.***Przykład anten*

Wykres promieniowania anteny kierunkowej przedstawia jej charakterystykę. Charakterystyka promieniowania anteny jest wykresem trójwymiarowym, zatem przekrój poziomy może znacznie różnić się od przekroju pionowego. Ta różnica w charakterystyce promieniowania jest istotna dla każdej sieci WLAN, która obejmuje swoim zasięgiem cały budynek. Wzrost mocy sygnału nadawanego może zmniejszyć pokrycie w pionie lub w poziomie albo w obydwu płaszczyznach. Anteny promieniają dookoła, poziomo lub pionowo.

Położenie anteny wpływa na jej polaryzację. Pola magnetyczne i elektryczne są względem siebie prostopadłe. O polaryzacji poziomej anteny mówimy wtedy, gdy płaszczyzna pola elektrycznego jest równoległa do podłoża. W polaryzacji pionowej anteny płaszczyzna pola elektrycznego jest prostopadła do płaszczyzny ziemi. Wszystkie anteny systemu sieci bezprzewodowej muszą mieć tę samą polaryzację.

Antena, która nadaje równomiernie we wszystkich kierunkach, to antena izotropowa; jej zysk wynosi 1 dB lub 0 dB. Wzrost parametru o 2 dB lub 3 dB stanowi podwojenie mocy sygnału. Aby utworzyć efektywny system transmisji bezprzewodowej, należy skorzystać z anten o wysokim zysku. Maksymalna moc nadawania sygnału jest ustalana prawnie. W Stanach Zjednoczonych można emitować sygnał o mocy 1000 mW, limit w Japonii to

10 mW/MHz, a w Europie — 100 mW. Limity odpowiadają efektywnej mocy wypromieniowanej izotropowo — EIRP (ang. *Effective Isotropical Radiated Power*). Współczynnik zysku może być różny w zależności od tego, czy antena nadaje, czy odbiera fale.

Szerokość wiązki anteny jest miarą kąta wiązki promieniowania. Kąt mierzy się pomiędzy punktami, w których moc sygnału wynosi połowę mocy maksymalnej anteny, promieniowanej w środku wiązki głównej. Anteny z wąską wiązką główną mają większy zasięg.

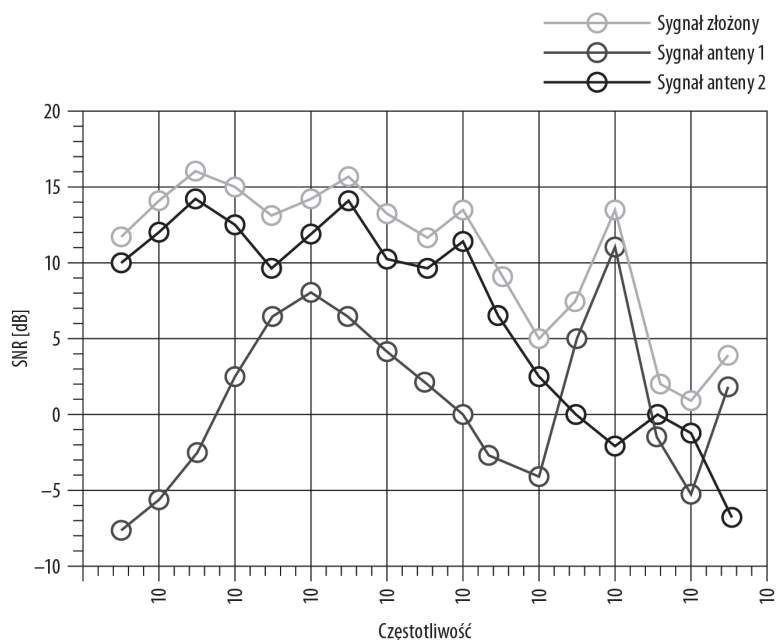
## Anteny inteligentne

Anteny inteligentne, zwane również antenami MIMO (ang. *Multiple-Input Multiple-Output*), są w rzeczywistości układami antenowymi, umożliwiającymi transmisję wieloantenową zarówno po stronie nadawczej, jak i po stronie odbiorczej. Technologia systemów wieloantenowych zwiększa wydajność transmisji bezprzewodowej, zmieniając możliwości systemów przedstawionych w standardach 802.11x. Anteny inteligentne MIMO są opisane w specyfikacji 802.11n, 802.16e WIMAX, a także zostaną wyspecyfikowane w standardach sieci czwartej generacji.

MIMO wykorzystuje strumienie danych, które są nadawane jednocześnie w tym samym paśmie przy użyciu różnych anten, z zastosowaniem multipleksacji przestrzennej, dzięki czemu można podwoić lub nawet potroić przepustowość łącza. Strumienie mogą być nadawane różnymi drogami od nadajnika do odbiornika (można wykorzystywać efekty odbicia sygnału). Po odpowiednim przetworzeniu odebranych sygnałów dane są składane w jeden strumień. Zastosowanie anten inteligentnych poprawia odbiór, zmniejsza ryzyko wielodrogowości i zaników sygnału. Rysunek 14.21 przedstawia superpozycję dwóch sygnałów z anteny MIMO w postaci parametru SNR (stosunek mocy sygnału do mocy szumu) w funkcji częstotliwości.

### Rysunek 14.21.

Złożenie sygnałów odebranych przez inteligentną antenę MIMO



Zastosowanie anten inteligentnych ma następujące zalety:

- ♦ zwiększona odporność systemu na zaniki,
- ♦ większy zasięg, większa pojemność oraz zwiększenie przepustowości łącza,
- ♦ lepsza efektywność widmowa,
- ♦ mniejsze zużycie energii,
- ♦ obniżenie kosztów sieci.

Liczne dostępne na rynku urządzenia bezprzewodowe obsługują systemy wieloantenowe, dzięki czemu wykorzystuje się w pewnym stopniu wspomniany efekt superpozycji. Na przykład w wieloprotokołowym punkcie dostępowym 802.11b/g mogą znajdować się dwie osobne anteny: jedna do obsługi transmisji 802.11b, a druga — 802.11g. Anteny inteligentne są wyposażone w cyfrowy procesor sygnału (DSP), którego zadaniem jest podział strumienia na podstrumienie i przekazanie ich do odpowiednich anten. W punkcie odbioru antena odbiera wszystkie sygnały i przekazuje je do DSP w celu złożenia. Dzięki zastosowaniu anten inteligentnych można transmitować sygnał o większej mocy, z dokładnie uformowaną wiązką. Na rysunku 14.22 przedstawiono kartę Linksys Wireless-N PCI z anteną inteligentną.

### Rysunek 14.22.

*Karta sieciowa  
Linksys Wireless-N  
PCI z zastosowaniem  
anten inteligentnej*



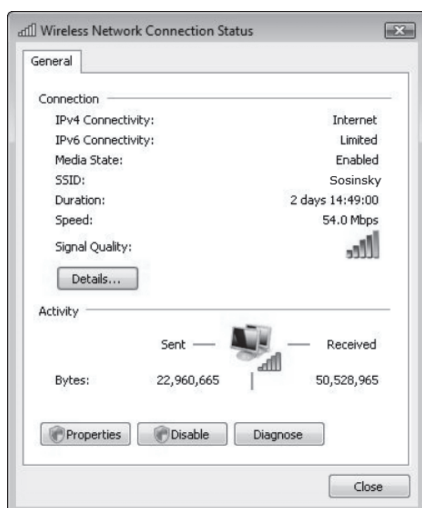
## Oprogramowanie wspierające sieci bezprzewodowe

Większość urządzeń Wi-Fi może być zarządzana bezpośrednio z poziomu systemu operacyjnego lub za pośrednictwem odpowiedniego oprogramowania, dostarczanego przez producenta wraz z urządzeniem. W większości systemów operacyjnych znajdują się wbudowane aplikacje, których zadaniem jest skanowanie sieci bezprzewodowych. Włączając skanowanie sieci w systemie Windows, w rzeczywistości używamy specjalnej aplikacji, której zadaniem jest wyszukanie wszystkich dostępnych sieci bezprzewodowych.

Wyniki wyszukiwania w systemie Windows XP i Vista są przedstawione za pomocą piktogramu z pięcioma paskami, odpowiadającymi mocy sygnału. W zależności od mocy sygnału (bardzo słaba, słaba, dobra, bardzo dobra, znakomita) kolejne paski piktogramu przybierają kolor zielony. Rysunek 14.23 pokazuje okno dialogowe *Wireless Network Connection Status* (Stan: Połączenie sieci bezprzewodowej) systemu Vista. Wymienione w oknie informacje są przydatne i umożliwiają podjęcie decyzji, którą z sieci bezprzewodowych wybrać. Te informacje niestety nie są wystarczające do monitorowania sieci bezprzewodowej. Aby mieć wystarczającą ilość danych do monitorowania sieci, trzeba zaopatrzyć się w odpowiednie oprogramowanie, na ogół powszechnie dostępne w internecie. Wiele programów zostało opracowanych przez miłośników łączności bezprzewodowej i komputerów, którzy oferują je bezpłatnie lub za przystępną cenę.

### Rysunek 14.23.

Okno *Wireless Network Connection Status* (Stan: Połączenie sieci bezprzewodowej) w systemie Vista



Jednym z najstarszych skanerów sieciowych jest *Network Stumbler* (<http://stumbler.net>), znany jako *NetStumbler*, dostępny obecnie w wersji 0.4.0, wydany w 2004 roku. Ta wersja wykrywa sygnały 802.11a/b/g, pod warunkiem że karta Wi-Fi zainstalowana w komputerze obsługuje te standardy. Mimo że wspomniana wersja programu nie doczekała się wersji dla Visty lub Windows 7, z powodzeniem działa z systemem Windows XP, 2000 i 9x. Wersja programu *NetStumbler* dla urządzeń przenośnych i telefonów komórkowych, działająca w systemie operacyjnym Windows CE, została wydana pod nazwą *MiniStumbler*.

Termin *wardriving* oznacza proces wyszukiwania sieci bezprzewodowych na wybranym terenie. W procesie tym często wykorzystuje się samochód oraz notebook lub palmtop wyposażony w bezprzewodową kartę sieciową, dodatkową antenę, specjalne oprogramowanie, a często również odbiornik GPS, umożliwiający precyzyjne lokalizowanie sieci na mapie. Nazwa *wardriving* pojawiła się w 1983 roku w filmie *Gry wojenne*, w którym zautomatyzowane oprogramowanie automatycznie wybierało określone numery dostępne, aby skontaktować się z innymi systemami.

Skanery sieciowe są przydatne do następujących celów:

- ♦ sprawdzania konfiguracji sieci bezprzewodowej,
- ♦ określania, czy istnieją nieznane punkty dostępowe,

- ♦ optymalizacji połączeń sieciowych,
- ♦ pomiaru siły sygnału w różnych miejscach,
- ♦ poszukiwania źródła zakłóceń,
- ♦ pomiaru sygnału GPS,
- ♦ oraz oczywiście do wardrivingu.

NetStumbler nie jest wyłącznie „biernym obserwatorem” sieci. Gromadzi parametry sieci za pomocą technologii Active Scanning. To oznacza, że każde urządzenie nasłuchujące może wykryć stosowanie oprogramowania NetStumbler, zwłaszcza jeśli w okolicy znajduje się wiele sieci Wi-Fi. NetStumbler bada odpowiedzi na zapytania sondujące, wykrywa punkty dostępu, ale nie jest w stanie określić standardu obsługiwanego przez dany węzeł lub stację.

Obok programu NetStumbler istnieje wiele innych aplikacji, między innymi:

- ♦ **inSSIDer 2** ([www.metageek.net/products/inssider](http://www.metageek.net/products/inssider)). Jest to program na licencji open source, współpracujący z Windows API Wi-Fi w celu badania sieci bezprzewodowych. inSSIDer jest dostarczany przez firmę MetaGeek, która oferuje również inne produkty, w tym Wi-Spy (analyzer widma) i Chanalyzer. Rysunek 14.24 przedstawia okno programu inSSIDer.

**Rysunek 14.24.**  
inSSIDer — przykład  
skanowania sieci



- ♦ **iStumbler** (<http://istumbler.net>). Program jest przeznaczony dla Mac OS X, AirPort, Bluetooth i Bonjour.
- ♦ **Kismet** (<http://kismetwireless.net>). Jest to skaner, sniffer (bada ramki 802.11) oraz pakiet oprogramowania do wykrywania włamań (pasywne skanowanie). Kismet działa w systemach Windows i Mac OS X.
- ♦ **Polecenie netsh (Windows Vista, 7)**. Polecenie to może być używane do wykrywania punktów dostępu. Format polecenia jest następujący: netsh wlan show networks mode = BSSID.

- ♦ **Vistumbler** (<http://vistumbler.net>). Jest to skrypt AutoIt, który przedstawia graficznie wyjście polecenia netsh. Jest zgodny z systemami Windows Vista i 7.

Wymieniona lista przedstawia przykłady skanerów sieciowych, dostępnych na licencji free-ware lub shareware. Wielu innych dostawców oprogramowania ma w swojej ofercie tego typu aplikacje. Niektóre z nich, dostępne komercyjnie, mogą być dość drogie. Listę dostępnego oprogramowania Wi-Fi można znaleźć na stronach [www.tech-faq.com/wi-fi-software-tools.shtml](http://www.tech-faq.com/wi-fi-software-tools.shtml).

## Bezpieczeństwo

Część definicji protokołu 802.11x obejmuje metody uwierzytelniania połączenia, stosowane w celu zapewnienia dostępu do portu i sieci. Port LAN, wykorzystany do zapewnienia dostępu do sieci, nazywa się Port Access Entity (PAE). PAE nie musi być fizycznym portem; jest to element logiczny powiązany z portem fizycznym. Element PAE może żądać dostępu, zapewniać dostęp albo realizować obydwie wspomniane funkcje.

W sieci bezprzewodowej znajduje się serwer uwierzytelniania, który przechowuje dane potrzebne do autoryzacji i odpowiada na żądania uwierzytelniania. Na podstawie przesłanych przez klienta informacji serwer podejmuje decyzję o świadczeniu bezprzewodowego dostępu do usług sieciowych lub o odmowie dostępu. Serwer uwierzytelniania znajduje się w punkcie dostępowym AP albo w innym miejscu sieci; wówczas żądania o dostęp są przekazywane do odpowiedniej maszyny. Uwierzytelnianie najczęściej jest realizowane z wykorzystaniem protokołu RADIUS.

Serwer uwierzytelniania rozróżnia dwa rodzaje portów. Pierwszym z nich jest port o niekontrolowanym dostępie, który umożliwia komunikację między elementem uwierzytelniającym (zwykle bezprzewodowym AP) i przewodową siecią LAN. Ramki wysyłane przez klienty nigdy nie są przekazywane za pośrednictwem niekontrolowanego portu. Port niekontrolowany wymaga, aby ramki pochodziły z AP. Drugim rodzajem jest port kontrolowany. Port kontrolowany umożliwia klientom wymianę ramek z pozostałymi węzłami sieci tylko wówczas, gdy klienty pomyślnie przejdą proces uwierzytelniania i autoryzacji 802.1x. Port kontrolowany jest zabezpieczony, co uniemożliwia komunikację klienta z siecią przed pomyślnie zakończonym procesem autoryzacji. Aby uchronić dostęp do portu, serwer uwierzytelniania tworzy unikatowy klucz sesji dla każdego klienta. Bez klucza sesji ramki są odrzucane.

## Szyfrowanie WEP

Szyfrowanie WEP (ang. *Wired Equivalent Privacy*) polega na formowaniu ramek z wykorzystaniem 40- lub 104-bitowych kluczy algorytmu RC4. Jeśli ramka jest zaszyfrowana, w polu FC nagłówka ramki 802.11 ustawiony jest bit WEP. W omawianym systemie stosuje się metodę klucza współdzielonego. Polega ona na tym, że w procesie uwierzytelniania biorą udział dwa klucze, przy czym każda ze stron połączenia posiada tylko jeden z nich. WEP określa klucz globalny, wykorzystywany w sesjach broadcast lub multicast. Osobny klucz jest definiowany dla sesji typu punkt-punkt.



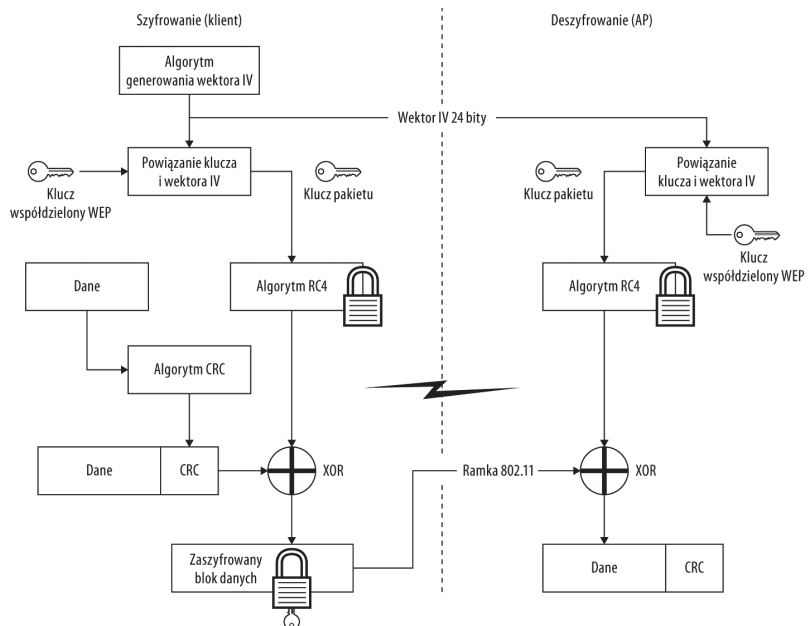
WEP jest uważany za stosunkowo słaby system zabezpieczeń, łatwy do złamania. Aby umożliwić lepsze zabezpieczenie, trzeba skorzystać z szyfrowania WPA.

Szyfrowanie WEP działa w następujący sposób:

1. Najpierw tworzona jest suma kontrolna CRC na podstawie pola danych ramki 802.11. Suma kontrolna służy do weryfikacji danych po zdeszyfrowaniu.
2. Tuż za polem danych zostaje umieszczone pole CRC.
3. Następnie jest wyliczany 24-bitowy wektor inicjujący IV.
4. Wektor IV jest dołączany do klucza WEP.
5. Wartość „IV + klucz WEP” jest następnie podawana do generatora liczb pseudolosowych, aby utworzyć odpowiedni strumień kluczy o rozmiarze takim samym jak „IV + klucz WEP”.
6. Strumień klucza jest następnie poddany operacji XOR z sekwencją „dane + wektor IV”, powstaje zaszyfrowany strumień danych.
7. Na koniec tworzona jest ramka 802.11, w której przed zaszyfrowanym polem danych umieszcza się wektor IV.

Rysunek 14.25 przedstawia proces szyfrowania i deszyfrowania WEP.

**Rysunek 14.25.**  
Proces szyfrowania  
i deszyfrowania WEP



Deszyfrowanie jest procesem odwrotnym do szyfrowania:

1. Wektor IV pochodzący z zaszyfrowanej ramki jest dołączany do klucza WEP. Wektor ten jest polem znajdującym się tuż przed zaszyfrowanym blokiem danych.

2. Sekwencja „IV + WEP” zostaje podana na wejście generatora pseudolosowego, dzięki czemu otrzymamy strumień kluczy — ten sam, który był wykorzystany w procesie szyfrowania bloku danych.
3. Strumień kluczy i zaszyfrowany blok danych jest przekazywany do bramki XOR, w wyniku czego otrzymujemy blok danych z polem CRC.
4. Suma kontrolna jest następnie wykorzystywana do obliczenia wektora IV, porównywanego z wektorem wyznaczonym lokalnie. Jeśli obydwa wektory są takie same, proces deszyfrowania uznaje się za pomyślny.

WEP był pierwszym systemem zabezpieczeń wprowadzonym komercyjnie do urządzeń realizujących transmisję bezprzewodową. Obecnie ten system jest bardzo powszechny. Trzeba jednak zwrócić uwagę na związane z nim wady i problemy. Głównym problemem jest to, że klucze szyfrowania WEP należy przysyłać w bezpieczny sposób poprzez łącze bezprzewodowe. Klucze są umieszczone w czystym tekście, dzięki czemu łatwo je przechwycić za pośrednictwem sniffera. Dodatkowo klucze WEP zwykle nie są często zmieniane, bo modyfikacja klucza wymaga naszego zaangażowania. Jeśli haker uzyskuje dostęp do klucza WEP, może z niego korzystać aż do momentu zmiany dokonanej przez administratora łącza. Nie ma również mechanizmu zarządzania grupą kluczy, co sprawia, że wraz z rozwojem sieci coraz trudniej zarządzać bezpieczeństwem całej sieci bezprzewodowej.

## Szyfrowanie WPA

Szyfrowanie WPA i WPA2 jest obecnie stosowane w sieciach bezprzewodowych standardu IEEE 802.11. Ta metoda szyfrowania wprowadza protokół generacji kluczy tymczasowych TKIP (ang. *Temporary Key Integrity Protocol*), który rozwiązuje wybrane problemy obecne w technice WEP. TKIP generuje klucze dla każdego wysyłanego pakietu. W tym celu wykorzystuje 48-bitowy wektor inicjujący i 128-bitowy klucz szyfrowania. Zastosowanie TKIP stanowi zasadniczą różnicę pomiędzy WEP i WPA: podczas gdy w WEP używa się tego samego klucza do transmisji wszystkich pakietów, w WPA wykorzystywane klucze są często zmieniane. Dłuższy klucz główny i zastosowanie różnych metod szyfrowania uniemożliwiają dostęp snifferom. Podobnie jak w przypadku WEP, WPA zapewnia szyfrowanie globalne i dla transmisji punkt-punkt.

W WPA obydwa węzły połączenia dysponują kluczem PSK. Dzięki temu klucz PSK nie może zostać przechwycony, zatem WPA jest systemem bezpieczniejszym, nadającym się do małych sieci bezprzewodowych. WPA jest zaimplementowany w punktach dostępowych wyprodukowanych po 2003 r. W starszych urządzeniach zwykle można zaktualizować oprogramowanie, które posiada tę funkcjonalność. Standard WPA jest prowadzony przez stowarzyszenie Wi-Fi, a produkty przechodzą procedury certyfikacji zgodności, dzięki czemu mogą być opatrzone logo Wi-Fi.

WPA2 jest techniką szyfrowania wdrożoną w standardzie 802.11i, ratyfikowanym w 2004 roku. Każde urządzenie obsługujące szyfrowanie WPA2 musi przejść procedury certyfikacji Wi-Fi i posiadać logo stowarzyszenia. W WPA2 zastosowano protokół szyfrujący CCMP, wykorzystujący zaawansowany algorytm szyfrowania AES (ang. *Advanced Encryption Standard*). Nie wszystkie starsze urządzenia mogą obsługiwać WPA2, bo część z nich nie ma zaimplementowanych protokołów TKIP (z WPA) i AES (z WPA2). Zatem zaletą WPA2 jest bezpieczeństwo transmisji, ale wadą brak kompatybilności wstecznej. Rysunek 14.26 przedstawia ustawienia zabezpieczeń routera Netgear RangeMax (Model WNR834B).

**Rysunek 14.26.**

Ustawienia  
zabezpieczeń routera  
Netgear WNR834B

**NETGEAR SMARTWIZARD** router manager  
RangeMax™ NEXT Wireless Router model WNR834B

**Setup Wizard**

- Setup
  - Basic Settings
  - Wireless Settings**
  - Content Filtering
  - Logs
  - Block Sites
  - Block Services
  - Schedule
  - E-mail
- Maintenance
  - Router Status
  - Attached Devices
  - Backup Settings
  - Set Password
  - Router Upgrade
- Advanced
  - Wireless Settings**
  - Port Forwarding

**Wireless Settings**

Wireless Network

Name (SSID):

Region:

Channel:

Mode:

Security Options

☐ None

☐ WEP

☒ WPA-PSK (TKIP)

☐ WPA2-PSK (AES)

☐ WPA-PSK (TKIP) + WPA2-PSK (AES)

Security Encryption (WPA-PSK)

Passphrase:  (8 ~ 63 characters)

Key Update:  (0 no update or 30 ~ 86400 seconds)

WPA ma dwa wbudowane poziomy bezpieczeństwa: WPA Personal (WPA-PSK) i WPA Enterprise. W pierwszym z nich, przeznaczonym dla użytkowników domowych i małych firm, używa się klucza PSK. Dzięki temu nie trzeba wyposażać sieci w serwer uwierzytelniania. Aby uzyskać dostęp do sieci zabezpieczonej WPA-PSK, należy wpisać hasło w postaci znaków ASCII (od 8 do 63) lub 64 cyfry szesnastkowe (256 bitów). Ze znaków ASCII i nazwy sieci (identyfikator SSID) tworzy się 256-bitowy ciąg, wykorzystywany w procesie szyfrowania. Technika WPA-PSK jest narażona na ataki hakerów metodami słownikowymi i brutalnymi, dlatego tak ważne jest tworzenie silnych haseł. Zaleca się hasła mieszane, zawierające znaki alfanumeryczne i specjalne, o długości 13 znaków.

Tabela 14.2 przedstawia wykaz wybranych urządzeń, w których zastosowano określone metody zabezpieczeń transmisji bezprzewodowej.

**Tabela 14.2.** Metody zabezpieczeń w wybranych urządzeniach domowych

Nazwa urządzenia	WEP	WPA-PSK	WPA2-PSK
ASUS Eee PC	X	X	X (zabezpieczenie sprzętowe)
iPhone	X	X	X
Nintendo DS.	X	–	–
Nokia N800/N810	X	X	X
PlayStation3	X	X	X
PlayStation Portable	X	X	–
Wii	X	X	X
Xbox 360 Wi-Fi	X	X	–

W metodzie WPA Enterprise trzeba zaopatrzyć sieć w serwer RADIUS, którego zadaniem jest uwierzytelnianie dostępu do sieci. W tym przypadku punkt dostępowy AP przekazuje żądania do serwera RADIUS, który następnie uwierzytelnia lub odrzuca żądanie na podstawie danych znajdujących się w serwerze. Jeśli serwer nie jest w stanie podjąć decyzji o statusie żądania, może wymagać podania dodatkowych informacji lub drugiego hasła.

WPA jest dużo bezpieczniejszym systemem szyfrowania niż WEP, szczególnie w przypadku zastosowania mocnych haseł. Protokoły AES i WPA2 są jeszcze bezpieczniejsze niż TKIP i WPA, dlatego właśnie zamiast szyfrowania WEP zalecane są te metody.

## Podsumowanie

W tym rozdziale wyjaśniono, jak tworzyć połączenia bezprzewodowe oparte na standardzie IEEE 802.11 Wi-Fi i jak nimi zarządzać. Sieci bezprzewodowe mogą być sklasyfikowane jako ad hoc lub infrastrukturalne.

Sieci bezprzewodowe korzystają z częstotliwości radiowych w paśmie 2,4 GHz lub 5 GHz. W pasmach tworzy się kanały, a dane są przesyłane za pośrednictwem fal radiowych z użyciem technik transmisji w widmie rozproszonym. Sygnały są kodowane za pomocą odpowiednich technik modulacji. Ramki 802.11x są podobne w budowie do ramek Ethernet. Ramki są przesyłane zgodnie z protokołem CSMA/CA. W niniejszym rozdziale opisano metody uzgadniania transmisji (handshakingu) połączeń bezprzewodowych, metody kontroli ruchu w tych połączeniach i zarządzanie tymi połączeniami.

Klienty sieci bezprzewodowych korzystają z punktów dostępu, bramek, routerów i innych urządzeń bezprzewodowych. W rozdziale omówiono pokrótce najważniejsze z nich, a także oprogramowanie do obsługi urządzeń i sieci bezprzewodowych oraz różne powszechnie używane formy zabezpieczeń takich sieci.

W następnym rozdziale przedstawiono sieci pamięci masowej i sposoby włączania ich do sieci danych w celu udoskonalenia dostępu do danych i poprawienia parametrów wydajnościowych.

# Rozdział 15.

## Sieć pamięci masowej

### W tym rozdziale:

- ♦ Potrzeba utworzenia sieci pamięci masowej
- ♦ Różne typy sieci SAN
- ♦ Modele współdzielonej sieci masowej
- ♦ Usługi i urządzenia pamięci masowej
- ♦ Sieci Fibre Channel
- ♦ Technologie pamięci masowej z zastosowaniem IP

Sieci pamięci masowej wykorzystują kolekcję technologii pozwalających na współdzielenie poprzez sieć zasobów pamięci masowej. Operacje wejścia-wyjścia pamięci masowej mogą oznaczać ogromną ilość danych przesyłanych przez sieć, a więc istnieje silna motywacja do odizolowania tego ruchu i umieszczenia go w dedykowanej sieci. W ten sposób powstała sieć typu SAN (ang. *Storage Area Network* — sieć pamięci masowej). Huby, przełączniki sieciowe, routery, serwery, macierze dyskowe, biblioteki taśmowe oraz biblioteki dysków magnetoptycznych to jedne z wielu urządzeń, które można znaleźć w sieci SAN. Topologią sieci pamięci masowej może być połączenie punkt-punkt, pętla z arbitrażem oraz pełna sieć (ang. *Fabric*).

Model stanowi opis, który kategoryzuje architekturę współdzielonej sieci pamięci masowej. Ten model w naturalny sposób rozróżnia serwery pamięci masowej na rozwiązania zorientowane pod kątem bloków (SAN) i rozwiązania zorientowane pod kątem plików (NAS — ang. *Network Attached Storage*). Model został rozszerzony o urządzenia taśmowe. Będzie on wykorzystany do pokazania, jak różne sieciowe rozwiązania służące do tworzenia kopii zapasowej zostały dostosowane przez model, oraz przedstawienia konfiguracji urządzeń w tych różnych rozwiązaniach.

Omówione zostaną koncepcje stojące za oddzieleniem dysków fizycznych od adresów logicznych. Tego rodzaju separacja pozwala na łatwą wirtualizację pamięci masowej. W celu ponownego połączenia danych przechowywanych na dysku w postać plików i informacji, które mogą być używane przez aplikacje, stosowana jest agregacja.

Fibre Channel w sieciach SAN jest technologią dominującą. W rozdziale będzie omówiony protokół, architektura oraz komponenty sieci Fibre Channel. Sieci typu Fibre Channel były początkowo skonfigurowane za pomocą topologii FC-AL (ang. *Fibre Channel Arbitrated Loop*), ale obecnie większość rozwiązań jest opierana na topologii FC-SW (ang. *Fibre Channel Switched fabric*). Poruszone będzie zagadnienie używania przełączników sieciowych i routerów Fibre Channel oraz ich różne typy portów. Elementy sieci SAN, takie jak poszczególne interfejsy sieciowe i dyski twarde, mają swoje adresy, a elementy mogą być grupowane i izolowane za pomocą technik strefowania, które zostaną przedstawione w rozdziale.

Kilka technologii wspiera przesyłanie danych z sieci SAN poprzez sieci IP.

W rozdziale zostaną omówione iSCSI (ang. *Internet Small Computer System Interface*), FCIP (ang. *Fibre Channel over IP*) oraz iFCP (ang. *Internet Fibre Channel Protocol*).

## Potrzeba utworzenia sieci pamięci masowej

W wielu firmach ponad połowa budżetu przeznaczonego na technologię jest wykorzystywana do zakupu pamięci masowej. Zapytania do baz danych, operacje tworzenia kopii zapasowej i odzyskiwania danych, replikacja i tworzenie kopii lustrzanych oraz dziesiątki innych zastosowań wymagających dostępu do danych prowadzą do sytuacji, w której ogromna część ruchu sieciowego jest powiązana z przechowywaniem danych. Aby zmniejszyć obciążenie sieci, ruch sieciowy związany z przesyłaniem danych bardzo często jest odseparowany w oddzielnej sieci o nazwie SAN (ang. *Storage Area Network* — sieć pamięci masowej). Termin SAN może być stosowany względem dowolnej sieci, w której ruch związany z przesyłaniem danych został odizolowany od pozostałego ruchu sieciowego, niezależnie od stosowanej technologii, topologii oraz protokołów.



Firma IBM używa akronimu SAN dla pojęcia „System Area Network”, ale ten termin wypadł z łask i jest stosowany sporadycznie.

Potrzebę tworzenia sieci pamięci masowej można podsumować za pomocą następującego faktu. Jeżeli przyjąć założenie, że serwery pamięci masowej klasy przemysłowej, na przykład EMC Symmetrix DMX-4, mogą przechowywać do 2400 dysków twardych o pojemności 1 TB (czyli łącznie 2,4 petabajta przestrzeni dyskowej), to każdy z takich w pełni wyposażonych systemów najczęściej kosztuje więcej niż budynek, w którym został zainstalowany. Nie można się więc dziwić istnieniu silnej motywacji do efektywnego współdzielenia tego rodzaju zasobów.

Niektóre z urządzeń w sieci SAN to:

- ♦ huby, przełączniki sieciowe i routery;
- ♦ serwery pamięci masowej i macierze dyskowe;
- ♦ biblioteki taśm;
- ♦ optyczne zmienne automatyczne;
- ♦ urządzenia wirtualizujące.

Sieci SAN są najczęściej budowane z użyciem hubów i przełączników sieciowych Fibre Channel i łączone za pomocą połączeń optycznych lub elektrycznych. Słowo „fibre” jest tutaj poprawne. Po zmodyfikowaniu technologii, tak aby były dostępne także połączenia miedziane, zmieniono nazwę technologii z Fiber Channel na Fibre Channel. Zabieg ten pozwolił zachować podobieństwo nazwy i odejść od jednoznacznego kojarzenia się Fibre Channel z technologią światłowodową. Sieć SAN implementuje architekturę Fabric, która pozwala zasobom pamięci masowej na łączenie się z innymi zasobami za pomocą wielu ścieżek. Technologia Fibre Channel ma własny zestaw protokołów, adresowania, słownictwo oraz konstrukcję odbiegającą od innych standardów sieciowych, które Czytelnik dotąd poznał, na przykład TCP/IP. Zasoby pamięci masowej są dostępne dla stacji roboczych i serwerów w sieci lokalnej (LAN, ang. *Local Area Networks*) za pomocą powszechnie stosowanych interfejsów urządzeń.

Sieci pamięci masowej to bardzo dynamiczny obszar technologii, w którym zawsze występuje coś zupełnie nowego. Dane z sieci Fibre Channel mogą być enkapsulowane w pakiety TCP, a następnie transmitowane poprzez sieci WAN (ang. *Wide Area Network*). Alternatywnym rozwiązaniem rozbudowy pamięci masowych jest wykorzystanie enkapsulowania poprzez TCP protokołu SCSI. W ten sposób protokół iSCSI staje się bardzo cenną metodą współdzielenia pamięci masowej w sieciach.

W rozdziale będą przedstawione najważniejsze pojęcia i koncepcje z zakresu sieci pamięci masowej oraz sposoby ich stosowania we własnych sieciach.

## Różne typy sieci pamięci masowej

Sieć pamięci masowej może być wdrożona na wiele różnych sposobów. Każdy typ oferuje możliwość współdzielenia zasobu pamięci masowej wraz z innymi komputerami w danej sieci.

Najprostszą postacią pamięci masowej jest podłączenie bezpośrednio do komputera dysków lub macierzy. Pamięć masowa wewnętrznie połączona z komputerem jest w przemyśle określana jako bezpośrednio połączona przestrzeń dyskowa (DAS, ang. *Direct Attached Storage*). SCSI jest najczęściej wykorzystywanym, wysoko wydajnym standardem podłączenia dysków.

W chwili obecnej do połączenia dodatkowej pamięci masowej z komputerami biurkowymi stosowane są powszechnie dostępne interfejsy USB (ang. *Universal Serial Bus*), FireWire oraz zewnętrzny SATA (eSATA). Stacje robocze wymagające wysokiej wydajności oraz małe serwery z reguły wykorzystują SCSI bądź inne szyny zapewniające wysoką wydajność. W zastosowaniach, gdzie pojemność i cena przestrzeni pamięci masowej mają większe znaczenia niż wydajność, interfejs SCSI jest zastępowany przez SATA (Serial ATA) na wszystkich poziomach wdrożenia, od komputerów aż do serwerów pamięci masowej klasy przemysłowej. W przypadku małych podsystemów pamięci masowej, takich jak zewnętrzne macierze RAID, są one połączone z komputerem za pomocą topologii bezpośredniego połączenia punkt-punkt (ang. *point-to-point connection*). Fibre Channel Point-to-Point (FC-P2P) to pojedyncze połączenie między dwoma urządzeniami.

Do zbudowania sieci łączącej urządzenia SCSI potrzebujemy odpowiedniego protokołu transportu danych. Najczęściej stosowanym protokołem transportowym jest FCP (ang. *Fibre Channel Protocol*), który zostanie szczegółowo omówiony w dalszej części rozdziału.

Topologie zarówno DAS, jak i FC-P2P współdzielią swoje zasoby przestrzeni dyskowej przez utworzenie dysku bądź pliku współdzielonego w ramach systemu operacyjnego komputera. Ograniczeniem wydajności jest połączenie sieciowe, przepustowość szyny oraz możliwości komputera w zakresie przetwarzania żądań dostępu do pamięci masowej z innych systemów w danej sieci. Topologie DAS i FC-P2P są architekturami szyny i nie będą klasyfikowane jako sieć.

Kiedy w komputerze zainstalowano wiele kart interfejsu sieciowego (NIC, ang. *Network Interface Card*) lub karty sieciowe Fibre Channel z dwoma fizycznymi połączeniami, wówczas można utworzyć topologię pętli. Jest to rodzaj architektury używany przez firmę IBM w jej sieciach Token Ring. Kontrolery Fibre Channel (HBA, ang. *Host Bus Adapters*) pozwalają na utworzenie pętli obejmującej do 126 urządzeń logicznych, nazywanej siecią FC z pętlą arbitrażową (ang. *Fibre Channel Arbitrated Loop*). FC-AL, dominująca kiedyś topologia sieci pamięci masowej, jest teraz przeznaczona do obsługi połączeń w macierzach dyskowych.

Ostatnia topologia powszechnie wykorzystywana w sieciach pamięci masowych nosi nazwę switched fabric. Tego rodzaju sieć jest utworzona za pomocą Fibre Channel i oferuje sieciom LAN i WAN wiele zalet architektury komutowanej. Główną zaletą jest inteligentna metoda kierowania ruchem i filtrowania pakietów, ale inne cenne zalety to między innymi nadmiarowe ścieżki, wymienne części oraz inne czynniki, które będą dokładnie omówione w dalszej części rozdziału. Większość sieci SAN jest konstruowana z użyciem topologii FC-SW (ang. *Fibre Channel Switched fabric*).

## SAN kontra NAS

Sieci SAN zostały opracowane przede wszystkim w celu wsparcia określonych zastosowań, takich jak magazynowanie danych w kilku zasobach pamięci masowych zorganizowanych w grupę. Te wczesne sieci SAN były określane mianem „wysp SAN”. Kiedy pojawiła się potrzeba połączenia ze sobą wymienionych wysp SAN, sieci Storage Area Network przekształcono na postać systemów federacyjnych. Wiele standardów omówionych w rozdziale zostało opracowanych w grupach przemysłowych, takich jak SNIA (Storage Networking Industry Association, <http://www.snia.org>) i FCIA (Fibre Channel Industry Association, <http://www.fibrechannel.org>).

Najprostsza postać sieci SAN to przełącznik sieciowy, dwa lub więcej urządzeń HBA oraz okablowanie niezbędne do połączenia serwera z urządzeniami pamięci masowej. Wiele firm, między innymi QLogic i Hewlett-Packard, oferuje zestawy nazywane „SAN w pudełku”, składające się z wymienionych komponentów oraz oprogramowania do zarządzania siecią SAN.

Jeden z systemów przechowywania danych, który w normalnych warunkach nie jest uznawany za SAN, to NAS (ang. *Network Attached Storage*). Najlepsze określenie NAS to serwer plików podłączony do sieci lokalnej LAN za pomocą TCP/IP. Sieć NAS stosuje protokoły plików, takie jak NFS i SMB/CIFS, transportowane poprzez TCP/IP. Natomiast sieci SAN wykorzystują protokoły bazujące na blokach. To jest podstawowa różnica pomiędzy sieciami NAS i SAN. Jednak niektórzy producenci utworzyli systemy hybrydowe łączące SAN i NAS (w rzadkich przypadkach DAS). Istnieją więc systemy bram NAS dla sieci SAN — przykładem może być tutaj EMC Celerra — i czasami trudno powiedzieć, do której kategorii zalicza się dane urządzenie. Serwer plików pozbawiony części serwerowej (pamięć masowa) nosi nazwę *NAS Head*. On również może być podłączony do sieci SAN, co zostanie przedstawione w dalszej części rozdziału.

## Koncepcja Business Continence Volumes

Istnieją zastosowania, w których sieci Storage Area Network wyróżniają się i pozostają niezastąpione. Tworzenie kopii zapasowej i replikacja to dwa najczęściej przychodzące do głowy zastosowania. Sieć SAN pozwala organizacjom nie tylko na współdzielenie zasobów pamięci masowej, ale gwarantuje również bardzo efektywny sposób zapewnienia danym wysokiej odporności na uszkodzenia. Jeżeli w organizacji są procesy o znaczeniu krytycznym, co w erze internetu dostępnego przez 24 godziny na dobę jest dość powszechnie spotykane, należy zwiększyć odporność na uszkodzenia poprzez zapewnienie systemu zapasowego wykorzystywanego w momencie awarii.

Rozważmy na przykład koncepcję Business Continence Volumes (BCV) opracowaną przez EMC. Koncepcja BCV zakłada utworzenie kopii aktywnego systemu pamięci masowej, która będzie przedstawiała stan w danym momencie czasu. W przypadku pracy z posiadanymi danymi, gdy system nie ma znaczenia krytycznego, można utworzyć kopię BCV, a następnie odłączyć ją od systemu podstawowego. Kopia BCV znajduje się więc offline; może być podłączona do innego serwera, który nie ma znaczenia krytycznego, i wykorzystana w celu:

- ♦ utworzenia kopii zapasowej bez wpływania na system produkcyjny bądź sieć;
- ♦ przeanalizowania przez aplikację taką jak analizator magazynu danych bez wpływu na serwer podstawowy;
- ♦ zoptymalizowania celem zmniejszenia stopnia powtarzania się danych lub usunięcia niepotrzebnych danych i tym samym zmniejszenia zbioru danych;
- ♦ zastosowania w charakterze szybko dostępnego, drugiego systemu danych, używanego, gdy system podstawowy ulegnie awarii. Szybkość dostępu jest uzależniona od ilości czasu potrzebnego na odłączenie podstawowej pamięci masowej i ponowne jej przyłączenie do BCV.

BCV można wykorzystać na wiele innych sposobów, ale możliwość zmniejszenia obciążenia sieci powoduje, że ta technologia jest bardzo atrakcyjna. EMC rozróżnia dwa odmienne rodzaje BCV. Pierwszy to klon BCV powstały w wyniku utworzenia odbicia lustrzanego. Natomiast drugi to migawka BCV powstała w wyniku użycia algorytmu kopiowania podczas zapisu w celu przyrostowego przekazywania zmian w systemie produkcyjnym.

Migawki są bardzo cenne podczas tworzenia historii zmian w pliku, ale są ograniczone przez wielkość zasobu pamięci masowej, która je przechowuje.

## Wirtualizacja pamięci masowej

Podstawową koncepcją w sieci pamięci masowej jest wirtualizacja pamięci masowej, czyli oddzielenie fizycznej pamięci masowej od logicznej przez utworzenie technologii mapowania. Wspomniane mapowanie na poziomie bloku może być przeprowadzone przez utworzenie indeksu głównego, podczas gdy w systemie plików bądź bazie danych może być osiągnięte na poziomie indeksu, pliku lub rekordu. Po wykonaniu mapowania w osprzęcie bądź oprogramowaniu pamięć masowa zawsze jest wirtualizowana.

Wirtualizacja pamięci masowej powoduje oddzielenie identyfikacji od miejsca. Można to potraktować jako rodzaj przekierowania. W serwerze zorientowanym blokowo zestaw bloków może być przypisany identyfikatorowi jednostki logicznej (ang. *Logical Unit Identifier*, LUN). Każdy poszczególny blok otrzymuje wartość przesunięcia, która identyfikuje ten blok w ramach LUN. Ta wartość przesunięcia nosi nazwę adresu bloku logicznego (ang. *Logical Block Address*, LBA). Wartość przesunięcia wskazuje punkt w sekwencji bloków w ramach jednostki LUN, w którym znajduje się dany blok. Kompletna mapa przestrzeni masowej definiuje przestrzeń nazw, która w urządzeniach blokowych nosi nazwę dysku wirtualnego (ang. *virtual disk*, *vdisk*).

Każda jednostka LUN jest montowana i obecna w sieci pamięci masowej dzięki kontrolerowi pamięci masowej. Wymienionym kontrolerem pamięci masowej może być urządzenie sprzętowe znajdujące się w HBA (ang. *Host Bus Adapter*) bądź oprogramowanie zainstalowane na górze stosu sieci. Wspomniane HBA to urządzenie interfejsu sieciowego, które łączy komputer z siecią albo urządzeniem pamięci masowej. Powszechnie spotykane są urządzenia HBA dla SCSI, Fibre Channel oraz eSATA. Zdecydowanie rzadziej urządzenia HBA są stosowane w przypadku interfejsów USB, FireWire, IDE, a nawet Ethernet. Sama jednostka LUN może być wynikiem operacji mapowania, a tym samym pozwala wtedy na jeszcze większą elastyczność. Wirtualizację dysku można przeprowadzić programowo, na poziomie systemu operacyjnego lub sprzętowo. W przypadku rozwiązania sprzętowego tabela mapowania przechowuje niezbędne metadane potrzebne do przeprowadzania przekierowania operacji wejścia-wyjścia pamięci masowej.

Wirtualizacja jest funkcją, która może zaoferować potężne możliwości i pozwala na jeszcze bardziej centralne zarządzanie pamięcią masową za pomocą mniejszej liczby konsol. W całkowicie zaimplementowanej, heterogenicznej wirtualizacji współdzielonej sieci pamięci masowej możliwe jest przeprowadzanie migracji danych pamięci masowej z jednego serwera do innego w trakcie ich działania. Podczas tego procesu sieć będzie w pełni obsługiwała żądania dostępu do danych przychodzące z różnych komputerów. Taka możliwość może być nieoceniona w takich sytuacjach, jak:

- ♦ dynamiczna zmiana wielkości woluminów;
- ♦ optymalizacja aplikacji sieciowej;
- ♦ replikacja;
- ♦ tworzenie kopii lustrzanej (synchroniczne i asynchroniczne);

- ♦ tworzenie kopii migawkowych w danej chwili;
- ♦ odzyskiwanie danych po awarii;
- ♦ zarządzanie pojemnością;
- ♦ dostrajanie wydajności działania, które obejmuje przeniesienie części używanych danych do szybszej pamięci masowej oraz poprawienie stopnia wykorzystania dysku.

Wirtualizacja udostępnia technologię nazywaną „thin provisioning”. Dzięki niej pamięć masowa staje się zasobem dostępnym na żądanie i kiedy zachodzi taka potrzeba, może być dostarczana w małych ilościach. Wirtualizacja ułatwia również wdrożenie polityki zarządzania cyklem życia informacji (ang. *Information Lifecycle Management*, ILM), w której określamy reguły biznesowe w stosunku do danych. Wada wirtualizacji pamięci masowej to bardzo często trudny proces jej implementacji, gdyż jest to rozwiązanie przeznaczone dla wielu platform, dostarczane przez wielu producentów, a tym samym trudne do instalacji i skomplikowane w zarządzaniu.

Oprogramowanie wirtualizacji pamięci masowej najczęściej znajduje się w:

- ♦ **Komputerach.** Oprogramowanie może znajdować się w systemie operacyjnym w postaci menedżera woluminów wraz ze sterownikiem urządzenia na poziomie jądra, w postaci systemu plików (CIFS/NFS) lub jako rezultat automatycznego montowania systemów plików, m.in. AUTOFS. Przykładami w tej kategorii mogą być Menedżer dysków logicznych Windows, LVM w systemach Unix i Linux, Symantec VERITAS Storage Foundation (dla systemu Windows i Solaris), NetApp MultiStore/FlexVol oraz IpStor NSS VA firmy FalconStor Software.
- ♦ **Urządzeniach pamięci masowej.** Kontroler pamięci masowej dostarcza macierz RAID i buforowanie, przechowuje metadane, a także migruje i replikuje dane oraz przeprowadza wirtualizację HBA na komputerach, do których jest podłączony.
- ♦ **Usługach sieciowych.** Specjalizowane serwery sieciowe mogą zapewnić wirtualizację przez przeprowadzanie przekierowania komunikacji na niskim poziomie lub za pomocą funkcji wyznaczania tras. Serwery te znajdują się pomiędzy pamięcią masową i komputerami na poziomie sieci, a cała komunikacja pamięci masowej odbywa się poprzez serwer. Aplikacja działająca na serwerze spełnia funkcję mapowania. Przykładami takiego rodzaju technologii są Coraid VS21 EtherDrive VirtualStorage, EMC Invista, LSI StorAge SVM oraz IPStor NSS firmy FalconStor Software.
- ♦ **Przełącznikach lub urządzeniach sieciowych.** Urządzenia te zawierają oprogramowanie agregujące pamięć masową jako część ich mechanizmu przekierowania.

Urządzenia wirtualizacji mogą być wewnętrzne (względem sieci), czyli symetryczne — wówczas znajdują się na ścieżce danych między komputerem a urządzeniem pamięci masowej. Zwykle oznacza to, że urządzenie to stanowi część (wprawdzie brzegową, ale jednak) sieci pamięci masowej. Ponieważ urządzenia wewnętrzne znajdują się w ścieżce danych, bardzo często oferują możliwość buforowania, co pozwala na zwiększenie wydajności działania.

Urządzenia wirtualizacyjne mogą być również zewnętrzne (względem sieci), czyli asymetryczne — wówczas nie znajdują się na ścieżce danych. Urządzenia zewnętrzne są używane do przeprowadzania bezpośrednich operacji wejścia-wyjścia pamięci masowej w sieci SAN. Są umieszczone w sieci Ethernet komputera macierzystego i zwykle oferują znacznie mniejszą wydajność niż rozwiązania bazujące na urządzeniach wewnętrznych. W przypadku wirtualizacji zewnętrznej nie można zastosować buforowania.

W swoich przełącznikach sieciowych Fibre Channel firma Cisco wbudowała funkcję o nazwie VSAN (ang. *Virtual Storage Area Network*), która obecnie jest standardem ANSI. Technologia ta pozwala na połączenie zbioru portów w wielu przełącznikach sieciowych w celu utworzenia wirtualnej architektury fabric. Różne porty przełącznika sieciowego mogą być przypisane różnym sieciom VSAN. Ewentualnie wiele przełączników sieciowych może być dołączonych do jednego bądź wielu portów w celu zdefiniowania unikalnych sieci VSAN. Sieć VSAN opracowano na podobieństwo architektury Virtual LAN używanej w sieciach Ethernet.

VSAN nie określa używanego protokołu sieciowego, to należy do warstwy sieciowej. Możliwe jest utworzenie sieci VSAN wykorzystującej protokół FCP (ang. *Fibre Channel Protocol*), FCIP (ang. *Fibre Channel over IP*), FICON (ang. *Fibre Connectivity*) opracowanego przez IBM oraz iSCSI Transport. Urządzenia zapewniają separację ruchu na poziomie poszczególnych sieci VSAN. Sieć VSAN zawiera różne usługi zarządzania łącznie ze strefami (zostanie to omówione w dalszej części rozdziału), bilingowaniem urządzeń, polityką bezpieczeństwa oraz usługą WWN (ang. *World Wide Name*). Jedną ze szczególnie użytecznych funkcji VSAN jest możliwość zmiany wielkości sieci VSAN przez dodanie albo usunięcie portów zamiast konieczności fizycznego dodawania bądź usuwania przełączników sieciowych w sieci Fibre Channel.

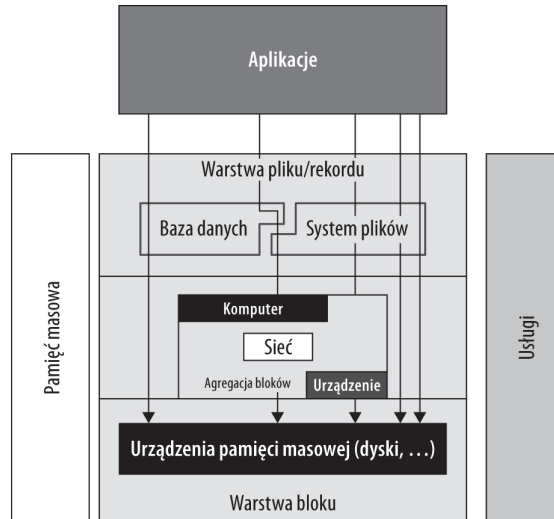
## Model współdzielonej sieci pamięci masowej

Wskazane jest posiadanie struktury, w ramach której będą przedstawione sposoby konstrukcji sieci pamięci masowej, odpowiednie kategorie różnych komponentów, protokołów, osprzętu oraz oprogramowania. W tym celu organizacja SNIA (Storage Networking Industry Association, <http://www.snia.org>) zdefiniowała ujednolicony, teoretyczny model sieci pamięci masowej na wzór siedmiowarstwowego modelu ISO/OSI lub alternatywnego modelu TCP/IP. Model ten został utworzony w latach 2000 – 2003 przez Wayna Rickarda, Johna Wilkesa, Davida Blacka oraz Haralda Skadała. Swój wkład w budowę modelu mieli również inni członkowie SNIA. Opracowany model nosi nazwę modelu współdzielonej architektury sieci pamięci masowej. Na rysunku 15.1 pokazano ostatnią opublikowaną wersję modelu SNIA.

Model SNIA współdzielonej pamięci masowej definiuje usługi, warstwy i, co najważniejsze, interfejsy, które urządzenia muszą posiadać, aby mogły działać. W celu obsłużenia pełnego żądania pamięci masowej żądanie z aplikacji musi przemierzyć jedną z pięciu różnych ścieżek, które zostały pokazane na rysunku 15.1. Pokazany model można wykorzystać do opisanego sposobu działania urządzeń oraz określenia typu urządzenia na podstawie wybranej ścieżki.

**Rysunek 15.1.**

Model współdzielonej  
architektury sieci  
pamięci masowej



## Współdzielone taśmy

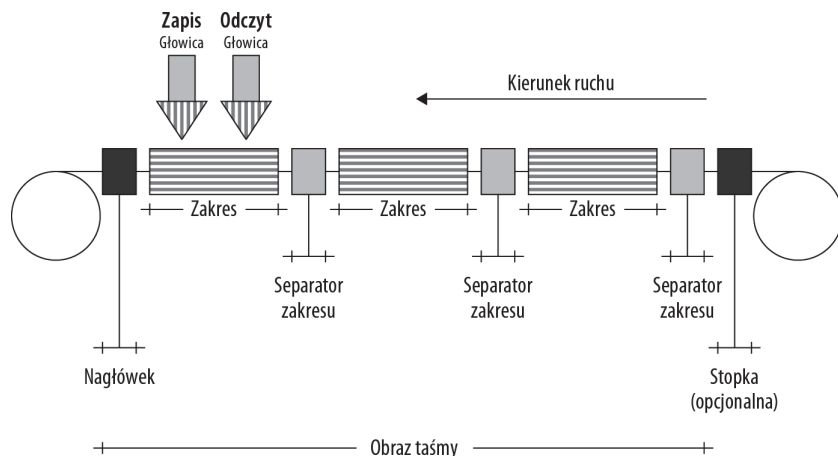
Znacząca część danych współdzielonych w sieci znajduje się w zautomatyzowanych urządzeniach zarządzających taśmami (urządzenia te są również nazywane bibliotekami taśmowymi). Bardzo często służą do tworzenia kopii zapasowych lub archiwizacji danych w różnorodnych organizacjach, na przykład w Internal Revenue Service, systemach rezerwacji w liniach lotniczych, magazynach danych kart kredytowych oraz innych ogromnych magazynach danych. Tego rodzaju biblioteki mogą zawierać setki urządzeń taśmowych (streamerów) mających dostęp do tysięcy taśm przechowujących petabajty danych. Niski koszt przechowywania danych na taśmie stanowi pewny rodzaj rekompensaty niższej wydajności oferowanej przez taki system.

Taśma to nośnik szeregowy, w którym dostęp do danych musi odbywać się po kolei. Z tego powodu operacje swobodnego dostępu są powolne. Jednak gdy dane są transmitowane w kolejności, przepustowość taśmy będzie wysoka.

Zawartość taśmy jest opisywana w kategoriach jednostki nazywanej „obrazem taśmy” (ang. *tape image*). Pojedyncza taśma może przechowywać jeden obraz taśmy, zaczynający się nagłówkiem. Podobnie jak w przypadku dysków twardych, aby taśma mogła być prawidłowo odczytana przez głowicę, w pierwszej kolejności musi być sformatowana. Istnieje wiele sposobów zapisu danych na taśmie: liniowe, liniowe i kręte, wiele jest wielościeżkowych, niektóre są spiralne, ale większość pozostaje rozwiązaniami własnościowymi. Wszystkie wspomniane metody współdzielą powszechnie stosowaną strukturę organizacyjną, która została zilustrowana na rysunku 15.2.

Na rysunku 15.2 taśma jest nawinięta na szpuli po prawej stronie, przesuwa się w lewą stronę i jest nawijana na szpulę znajdującą się po lewej stronie. Kiedy taśma znajduje się pod głowicami magnetycznymi, jedna głowica odczytuje dane, natomiast druga zapisuje dane. Obrazy taśmy są dzielone na sekwencję bloków taśmy nazywanych zakresami.

**Rysunek 15.2.**  
Struktura logiczna  
taśmy



Na taśmie niemal zawsze zapisywany jest nagłówek, a czasem nawet stopka jako część operacji formatowania i przechowywania rekordów. Zakresy są od siebie oddzielone tak zwanym *separatorom zakresu*. Kiedy zachodzi potrzeba odczytania fragmentu obrazu taśmy, głowica odpowiedzialna za odczyt powoduje odczytanie spisu treści w nagłówku, a następnie przechodzi do położenia na taśmie, w którym rozpoczynają się żądane dane. Kiedy dane trzeba zapisać na taśmie, zostają umieszczone na końcu taśmy. Następnie taśma jest cofnięta do nagłówka, w którym są umieszczane informacje o wprowadzonych zmianach.

Taśma jest szeregowym urządzeniem przechowującym dane. Odczyt danych z taśmy jest bardzo wolny, ponieważ zachodzi konieczność mechanicznego przesunięcia taśmy do miejsca, w którym znajdują się żądane dane. Jednak zapis może być bardzo szybki. Zaletą taśmy jest niewielki koszt przechowywania ogromnych ilości danych.

W modelu współdzielonej pamięci masowej systemy taśmowe rozciągają się na wszystkie jego poziomy, począwszy od najwyższego w warstwie aplikacji, jak pokazano na rysunku 15.1. Dość częstym zastosowaniem jest tworzenie kopii zapasowych. Wiele programów klasy przemysłowej do tworzenia kopii zapasowej — na przykład CommValut Systems Galaxy, Computer Associates ARCserve Backup, EMC Legato Networker, HP OpenView Storage Data Protector and Archive Backup System (ABS), IBM Tivoli Storage Manager (TSM) oraz Symantec NetBackup (wcześniej VERITAS NetBackup) — obsługuje urządzenia taśmowe (głównie mniejsze jednostki) albo producenci odpłatnie dostarczają dodatkowe moduły oferujące obsługę systemów taśmowych klasy przemysłowej.

System formatu taśmy rozciąga się na warstwach modelu od aplikacji aż do komputera macierzystego (rysunek 15.3). Operacja formatowania jest odpowiedzialna za umieszczanie plików bądź rekordów w zakresach taśmy, które z kolei są następnie umieszczone w obrazach taśmy. Rozwiązanie otwarte charakteryzuje się tym, że operacje formatowania taśmy oraz inne funkcje są wykonywane przez oprogramowanie obsługujące taśmę.

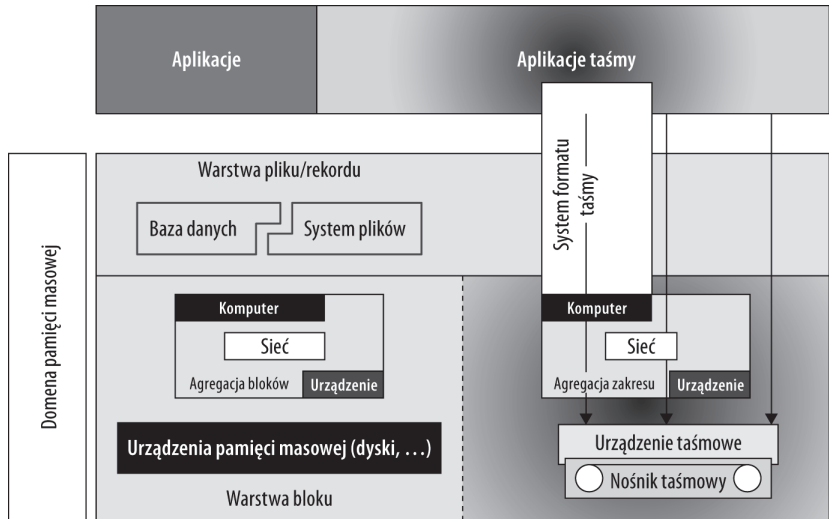
Taśma nie jest dyskiem. Nie istnieje więc żadna bezpośrednia korelacja pomiędzy woluminem na dysku a obrazem na płycie. Taśma jest urządzeniem sekwencyjnym, jednostką agregacji jest zakres, a nie blok. W modelu taśmy agregacja zachodzi w warstwach komputera macierzystego (sieci, urządzenia). Warto również zwrócić uwagę na fakt, że w tym

modelu następuje oddzielenie urządzenia od nośników. Jest to konieczne, ponieważ taśma jest nośnikiem wymiennym. Ten model został zastosowany w bibliotekach dysków magnetycznych, wykorzystując wymienne nośniki CD lub DVD.

Na rysunku 15.3 różne rodzaje operacji na taśmie są zaznaczone w modelu taśmy za pomocą strzałek. W sekcji taśmy strzałka po lewej stronie przechodzi przez system formatowania taśmy, komputer oraz agregację zakresu i odpowiada operacji zapisu danych pliku na taśmie. Typowym programem używającym tej ścieżki będzie polecenie `tar`, które odczytuje dane z dysku. `tar` to polecenie systemu Unix odpowiedzialne za archiwizację na taśmie. Ta sama lewa strzałka w sekcji taśmy obsługuje ścieżkę `write` dla polecenia `dump`, powodującego odczytanie plików w systemie plików, które zostały zapisane na taśmie. Model koncentruje się na zadaniach do wykonania, a nie na urządzeniach.

### Rysunek 15.3.

*Model współdzielonej pamięci masowej w postaci taśmy*



W ostatnim scenariuszu polecenie `tar` powoduje utworzenie na taśmie wirtualnej kopii zapasowej plików przez (w pierwszej kolejności) odczyt danych z dysku twardego, a następnie przekazanie ich oprogramowaniu tworzącemu kopię zapasową. Wspomniane oprogramowanie umieszcza dane na taśmie. Proces ten obejmuje skonwertowanie danych na format taśmy i przekazanie komputerowi sekwencyjnych danych, który z kolei zapisuje taśmę wirtualną na dysku.

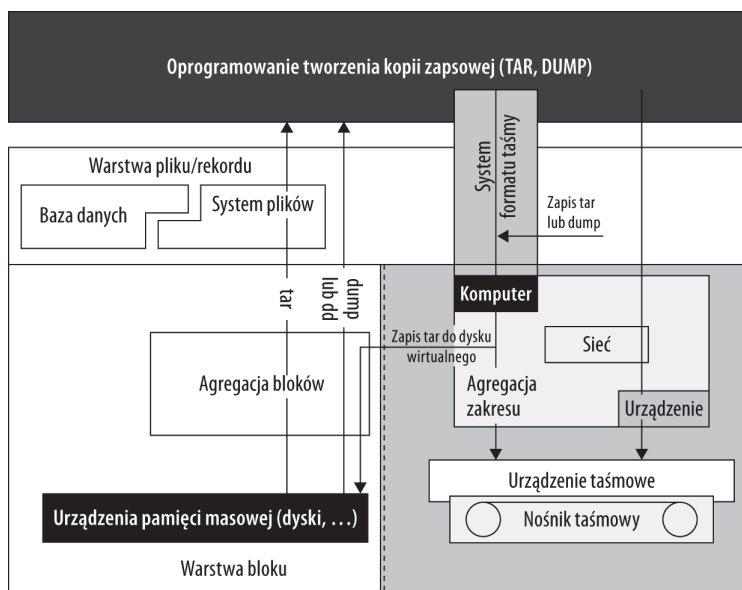
Środkowa strzałka rozciągająca się od oprogramowania tworzącego kopię zapasową, poprzez sieć, aż do urządzenia taśmowego symbolizuje operację zapisu, która jako dane wejściowe pobiera polecenie `dd`. Wymienione polecenie `dd` przeprowadza operację odczytu, która kopiuje wolumin i umieszcza go na taśmie.

Te różne operacje tworzenia kopii zapasowej zostały pokazane na rysunku 15.4.

Po poznaniu sposobu przetwarzania poleceń sieciowych tworzących kopię zapasową na taśmie warto pokrótce zobaczyć, jak ten model używa urządzeń. Na rysunku 15.5 pokazano sześć różnych technologii tworzenia kopii zapasowej na taśmie. Widniejące na rysunku przykłady zostały objaśnione w kolejności od przykładu w lewym górnym rogu.

**Rysunek 15.4.**

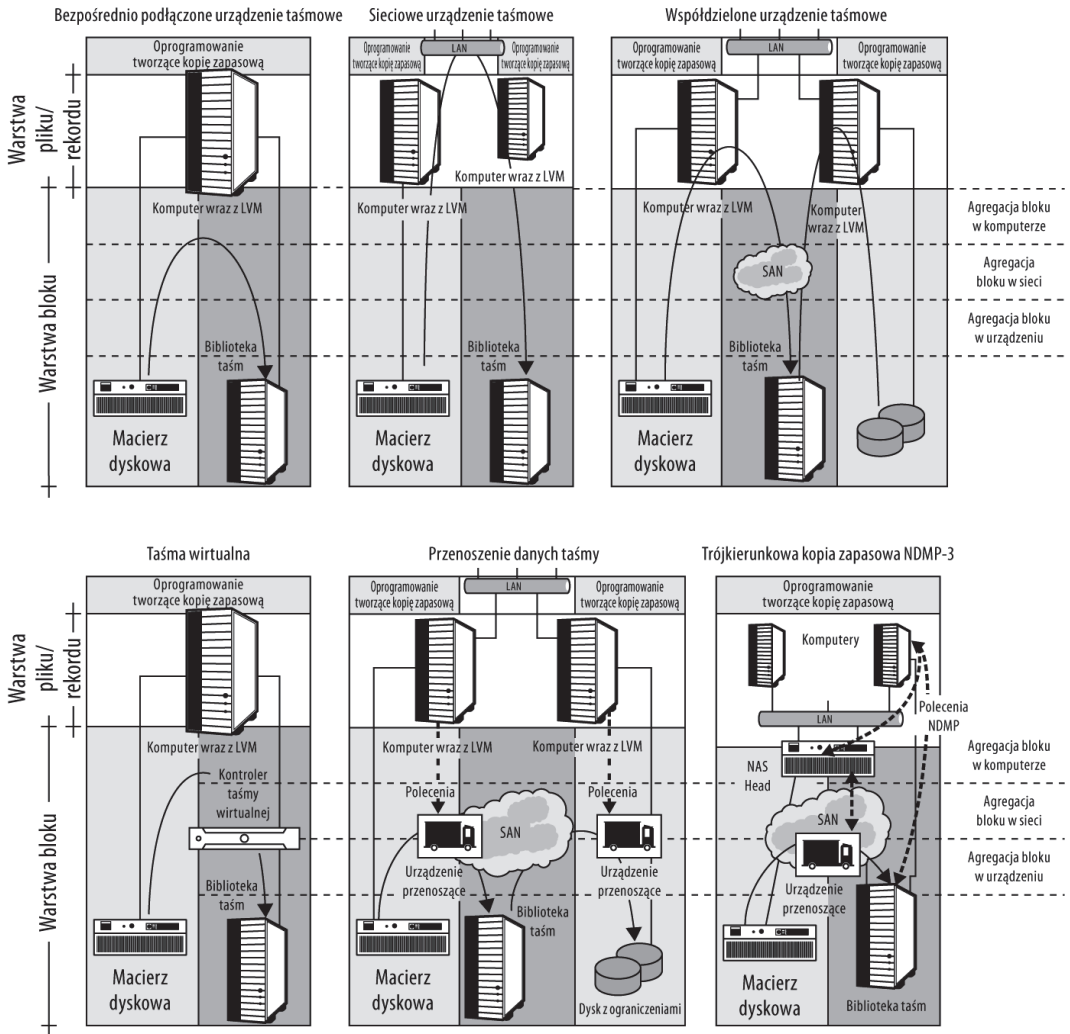
Różne polecenia tworzenia kopii zapasowej pokazane w modelu współdzielonej taśmy



Najprostszym przykładem jest tworzenie kopii zapasowej do bezpośrednio podłączonego urządzenia taśmowego. W takim przypadku dane są kopiowane z dysku na taśmę poprzez szynę systemową. Zarówno to rozwiązanie, jak i pokazane na kolejnym przykładzie rozwiązanie wykorzystujące napęd taśmowy podłączony do sieci (w którym dysk i napęd taśmowy są umieszczone w sieci) to rozwiązania, gdzie szyna lub sieć rozciąga się na wszystkich warstwach modelu taśmowego. Ta sama szyna systemowa komputera macierzystego jest stosowana zarówno dla poleceń, jak i przekazywania danych z macierzy dyskowej do biblioteki taśmowej. W obu przykładach agregacja jest przeprowadzana w komputerze macierzystym przy użyciu systemu plików komputera macierzystego.

Najprostsze i prawdopodobnie najważniejsze rozwiązanie tworzenia kopii zapasowej za pomocą SAN zostało pokazane w prawym górnym rogu rysunku 15.5 (zatytułowane „Współdzielone urządzenie taśmowe”). Ta architektura pozwala na utworzenie kopii zapasowej bez używania sieci LAN. Polecenia są przekazywane z komputera macierzystego do różnych urządzeń, ale ruch sieciowy związany z tworzeniem kopii zapasowej odbywa się jedynie poprzez sieć pamięci masowej, a nie sieć lokalną LAN. W tym przykładzie biblioteka taśmowa jest pokazana jako pojedyncze urządzenia. Wiele wdrożeń tego rodzaju spowoduje podział biblioteki taśm na partycje, co pozwoli na jednoczesne tworzenie wielu kopii zapasowych. Oprogramowanie odpowiedzialne za tworzenie kopii zapasowej na różnych komputerach kontroluje różne automatyczne urządzenia wybierające taśmy i napędy.

Wirtualizację taśmy można przeprowadzić za pomocą emulacji i przekierowania. W takim przypadku, pokazanym w lewym dolnym rogu na rysunku 15.5 (przykład zatytułowany „Taśma wirtualna”), urządzenie taśmy wirtualnej jest wdrażane w ścieżce danych. Z punktu widzenia komputera to urządzenie jest widziane jako zwykłe urządzenie taśmowe. Abstrakcja pozwala komputerowi na utworzenie kopii zapasowej, a następnie przekazanie jej urządzeniu w celu dalszego przetworzenia. Przewagą takiego rozwiązania nad bezpośrednio podłączonym urządzeniem taśmowym jest pozbycie się przez komputer macierzysty obciążenia związanego z przetworzeniem kopii zapasowej. Operacja przetworzenia jest



**Rysunek 15.5.** Sześć technologii tworzenia kopii zapasowej na taśmie

przeprowadzana przez urządzenie, a komputer może w tym czasie zajmować się innymi zadaniami. Kiedy komputer „wypada” z operacji przetwarzania kopii zapasowej, jak ma to miejsce w omawianym przypadku, wtedy określamy to mianem tworzenia kopii zapasowej bez udziału serwera (ang. *Server-Free Backup*).

Piąte rozwiązanie nosi nazwę „Przenoszenie danych taśmy” i zostało pokazane na rysunku 15.5 jako środkowy przykład w dolnej linii. Dane są przechowywane w macierzy dyskowej, ale aplikacja wymaga ich przeniesienia na dysk z ograniczeniami. W rozwiązaniu pojawiają się więc urządzenia przenoszące, po jednym w każdej ścieżce danych. Przerywana strzałka wskazuje, że komputer macierzysty wydaje polecenia, natomiast urządzenie przenoszące wykonuje pozostałą część pracy. Pierwsze zadanie używa ścieżki danych pobierającej dane z miejsca ich przechowywania w macierzy dyskowej i przenosi je poprzez pierwsze urządzenie przenoszące do wewnętrznego położenia na taśmie w bibliotece taśm. Drugie zadanie

za pomocą drugiego urządzenia przenoszącego kopiuje dane z biblioteki taśm do wskazanego miejsca docelowego, którym jest dysk. Rozwiązanie „Przenoszenie danych taśmami” ma taką samą ogromną zaletę jak „Współdzielone urządzenie taśmowe”, czyli wykonuje swoje zadanie bez używania sieci lokalnej. Dodatkową zaletą jest przeniesienie do urządzeń przenoszących obciążenia związanego z przetwarzaniem kopii zapasowej.

Ostatnie rozwiązanie pokazane na rysunku 15.5, w prawym dolnym rogu, ilustruje architekturę tworzenia kopii zapasowej z wykorzystaniem serwera plików i przenoszenia danych. Technologia wykorzystana do kontroli nad tworzeniem kopii zapasowej nosi nazwę „trójkierunkowa kopia zapasowa NDMP”. NDMP to skrót od *Network Data Management Protocol* i oznacza technologię używaną przez NetApp i Legato (obecnie własność EMC) do bezpośredniego przenoszenia danych do urządzenia tworzącego kopię zapasową; kontrolerem jest serwer plików bądź NAS. Polecenia NDMP są obsługiwane przez niemal wszystkie programy klasy przemysłowej służące do tworzenia kopii zapasowej. Agregacja jest przeprowadzana w urządzeniu NAS, które otrzymuje polecenia NDMP od komputera macierzystego. Biała, podwójna strzałka między urządzeniem przenoszącym i NAS symbolizuje polecenia służące do pracy z blokami w macierzy dyskowej.

## Domena pamięci masowej

W modelu sieci współdzielonej pamięci masowej domena pamięci masowej to kontener pozwalający na organizację informacji w postaci plików. Wspomniane pliki są wskaźnikami do informacji znajdujących się na dysku, zorganizowanych przez wykorzystanie pól, rekordów i metadanych, które dostarczają kontekstu wystarczającego do zrozumienia przeznaczenia danych i sposobu ich używania. Metadane mogą zawierać typ danych, aplikacja powiązana z danymi musi mieć możliwość wyświetlania i edytowania danych, układania ich w sekwencje oraz inne właściwości, które pozwalają na przekształcenia danych na postać użytecznych informacji.

Na górze domeny pamięci masowej warstwa pliku (rekordu) dostarcza logikę wymaganą do pakowania informacji, tak aby mogły być przechowywane w użyteczny sposób. W wielu przypadkach ilość danych jest większa niż fizyczne jednostki alokowane w pamięci masowej, na dysku pamięć masowa jest alokowana w blokach. System plików bądź baza danych musi mieć możliwość segmentowania informacji na możliwe do przechowywania fragmenty, które można pobierać i umieszczać w sekwencji, gdy jest to konieczne. Bardzo często systemy plików i bazy danych są połączone w pojedynczą strukturę. System plików bądź baza danych używa przestrzeni nazw lub hierarchii obiektu, który pozwala na przeprowadzanie operacji wyszukiwania i pobierania danych.

W modelu nie został pokazany obiekt lub plik bufora, który jest wykorzystywany w celu zwiększenia wydajności systemu przez przechowywanie w pamięci ostatnio używanych elementów. Wszystkie systemy pamięci masowej używają różnych poziomów buforowania, aby zwiększyć wydajność działania. Zastosowanie bufora pociąga za sobą konieczność, by system pamięci masowej zawierał logikę określającą, czy dane przenoszone z bądź do pamięci masowej są przekazywane prawidłowo oraz czy spełnione są reguły zaimplementowane w celu zapewnienia spójności danych. Te reguły logiki są nazywane koherencją systemu. Ponieważ buforowane informacje mogą być nowsze bądź starsze niż przechowywane na dysku, absolutnie niezbędne jest, aby logika koherencji była solidna i niezawodna.

Rozróżnienie pomiędzy informacjami w postaci plików i rekordów oraz danymi w postaci bloków jest ważne podczas definiowania koncepcji w modelu współdzielonej pamięci masowej.

Dane są przechowywane na najniższym poziomie, w warstwie bloku. Blok zawiera dane, ale nie ma żadnego kontekstu opisującego te dane. Bloki są po prostu adresami miejsc w urządzeniu pamięci masowej, na przykład na dysku twardym, dysku typu SSD (ang. *Solid State Disk*), dysku optycznym lub na taśmie. Bloki mogą być zapisywane, nadpisywane, usuwane i przenoszone. Ich kolejność nie ma żadnego związku z tym, co użytkownik bądź program komputerowy uznaje za użyteczne. Aby móc wykorzystać dane przechowywane w blokach, konieczne jest zastosowanie metody agregującej bloki. Agregacja danych dostarcza niezmiernie ważnej tabeli wyszukiwań, zawierającej wskaźniki mapujące bloki na schemat organizacyjny.

## Agregacja

System plików bądź baza danych może wykorzystywać informacje znajdujące się w blokach, ponieważ przechowują informacje o plikach lub rekordach odpowiadających wskaźnikom w urządzeniu blokowym oraz ich kolejności. W ten sposób zapewnione są wszystkie wymagania w celu pobrania informacji. Z punktu widzenia systemu plików lub bazy danych miejsce fizycznego przechowywania danych nie pociąga za sobą żadnych konsekwencji. System mapowania z pliku do wskaźnika w pamięci masowej pozwala na przekierowanie odniesienia wskaźnika do innego bloku lub zupełnie innego urządzenia pamięci masowej.

Ta abstrakcja dostarczana przez agregację jest sercem zbioru technologii wirtualizacji pamięci masowej, które mają znaczenie krytyczne w dostarczaniu elastyczności niezbędnej do tego, aby sieć pamięci masowej była praktyczna. Macierz RAID, jednostki logiczne i woluminy, a także oprogramowanie zarządzające woluminami — wszystkie wymienione elementy mogą funkcjonować dzięki mapowaniu.

Nie wszystkie operacje pamięci masowej wymagają, aby dane były przedstawiane w formie użytecznych informacji. W rzeczywistości większość operacji wymaga jedynie, aby dane były obsługiwane bez modyfikacji. Podczas tworzenia kopii zapasowej jednego dysku na drugim lub jednego woluminu na drugim wiedza o tym, który blok jest używany przez określony plik (i na odwrót), stanowi zbędne obciążenie i jest ignorowana. Przemysłowe technologie kopii zapasowej i replikacji ignorują struktury plików i przeprowadzają te operacje na poziomie bloków, kopiując dane z jednego miejsca do drugiego sektor po sektorze, blok po bloku. Techniki sprawdzania błędów określają, czy operacja została przeprowadzona prawidłowo, ale w większości sytuacji serwer bądź komputer używający tych danych nie musi być zaangażowany w wymienione operacje. Większość operacji na poziomie bloków jest implementowana przez same systemy pamięci masowej.

Konkluzja jest następująca: jeżeli wymagane jest, aby operacje na danych były przeprowadzane szybko, to trzeba zainwestować w technologię bazującą na blokach. Gdy wymagana jest możliwość zarządzania informacjami, trzeba zastosować systemy bazujące na plikach.

## Modele urządzeń

Przedstawiony na rysunku 15.1 model współdzielonej pamięci masowej pokazuje pięć różnych ścieżek żądania danych z pamięci masowej do warstwy aplikacji. W rzeczywistości istnieje możliwość zdefiniowania ośmiu ścieżek przez cztery różne interfejsy tworzone przez model. Pokazane na rysunku są tymi najbardziej użytecznymi, biorąc pod uwagę klasy urządzeń, które można zakupić i zainstalować.

Cztery interfejsy w modelu to:

- ♦ **Warstwa aplikacji/systemu operacyjnego.** Ta warstwa jest zwykle zdefiniowana przez API niezbędne do nawiązania połączenia z usługami znajdującymi się w obu warstwach.
- ♦ **Warstwa systemu operacyjnego/pliku i rekordu.** Inny zestaw API jest stosowany do powiązania systemu operacyjnego z informacjami.
- ♦ **Warstwa pliku/bloku.** Ten interfejs definiuje miejsce, w którym używane są protokoły sieciowe.
- ♦ **Warstwa bloku/urządzenia pamięci masowej.** Ten interfejs używa poleceń szyny niskiego poziomu, na przykład SCSI do zarządzania danymi.

Interfejsy są bardzo ważne, niezależnie od technologii oraz tego, jak nazywa je producent. Kiedy używany jest otwarty standard dla API interfejsu, zapewniany jest pewny rodzaj niezależności od dostawcy, którego nie ma podczas używania własnościowego API dostawcy pamięci masowej.

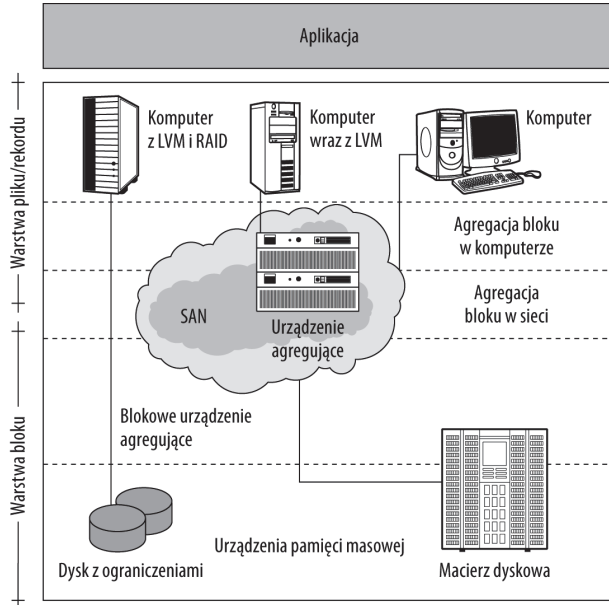
Blokowe urządzenia pamięci masowej z reguły charakteryzują się klasycznymi koncepcjami występującymi w modelu Storage Area Network i mogą zajmować trzy najniższe warstwy modelu. Urządzenia pamięci masowej w warstwie bloku wykonują większość pracy podczas operacji pamięci masowej. Urządzenia pamięci masowej pobierają polecenia z komputera, a następnie niezależnie wykonują te operacje. Wśród operacji, które może wykonać serwer zorientowany blokowo, są bezpośrednie transfery blokowe z urządzenia do urządzenia podczas tworzenia kopii zapasowej i kopiowania, replikacja, tworzenie kopii lustrzanych oraz inne operacje wejścia-wyjścia wymagane przez aplikację od pamięci masowej. Logika wbudowana w serwery pamięci masowej zwiększa wydajność działania poprzez buforowanie zawartości, skanowanie dysków oraz przeprowadzanie operacji konserwacyjnych w pamięci masowej.

Na rysunku 15.6 pokazano, jak zorientowane blokowo serwery pamięci masowej wpasowały się w architektoniczny model sieci pamięci masowej.

Zorientowane blokowo systemy pamięci masowej działają doskonale, kiedy aplikacja przekazuje urządzeniu polecenie w rodzaju „skopiuj ten wolumin”, „wykonaj kopię zapasową” lub nawet „wprowadź tę małą zmianę w tym ogromnym pliku”. Każda operacja niewymagająca zrozumienia sposobu przechowywania danych na dysku, powiązana z plikami bądź informacjami będzie obsługiwana znacznie wydajniej jako operacja blokowa. W przypadku wprowadzania drobnej zmiany w bazie danych, gdzie zmiana obejmuje dane w pojedynczym sektorze, operacja blokowa będzie musiała zmodyfikować tylko dany sektor. Jednak kiedy filer lub serwer zorientowany plikowo zmienia plik, wówczas konieczne jest nadpisanie całego pliku. Istnieją sytuacje, w których wydajność filerów znacznie przewyższa wydajność oferowaną przez serwery blokowe pamięci masowej.

**Rysunek 15.6.**

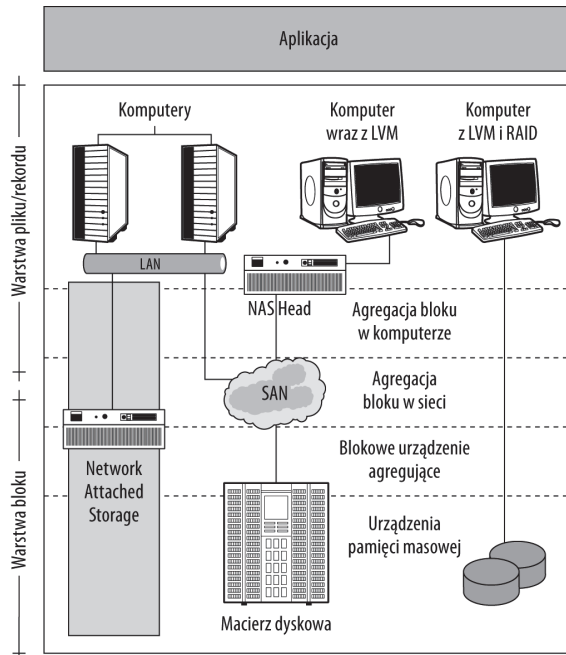
Różne zorientowane  
blokowo urządzenia  
pamięci masowej



Serwery zorientowane plikowo mogą być budowane w modelu współdzielonej pamięci masowej jako kompletne serwery plików NAS, NAS Head i macierz dyskowa lub jako urządzenie komputera, w którym system plików (baza danych) opiera się na urządzeniu agregującym, pośredniczącym w operacjach na danych pamięci masowej. Te trzy różne rodzaje urządzeń, czyli Network Attached Storage, macierze dyskowe i bezpośrednio podłączone dyski, zostały pokazane na rysunku 15.7.

**Rysunek 15.7.**

Różne urządzenia  
pamięci masowej,  
które są zorientowane  
plikowo (od lewej  
do prawej): Network  
Attached Storage,  
macierze dyskowe  
i bezpośrednio podłączone  
dyski



W zorientowanym plikowo systemie pamięci masowej istnieje funkcja mapowania, która łączy woluminy, bloki i sektory z plikami lub tabelami, rekordami i krotkami. Z punktu widzenia sieciowego systemu pamięci masowej schemat organizacyjny systemu plików, bazy danych lub ich zorientowana obiektowo wersja pozostają bez znaczenia, ważna jest funkcja mapowania. Urządzenia NAS (ang. *Network Attached Storage*), takie jak filer NetApp, działają pod kontrolą specjalizowanego systemu operacyjnego WAFL (ang. *Write Anywhere File Layout*), Windows Storage Server 2003 R2, działa pod kontrolą Windows Server 2003 R2, a nawet urządzenia bazodanowe, takie jak nieoferowany już Oracle 8i Appliance lub bieżący Netezza Data Warehouse Appliance, działają równie dobrze jako serwery zorientowane plikowo. NAS rozciąga się na wszystkie warstwy modelu współdzielonej pamięci masowej, od sieci komputera macierzystego aż do dysku z ograniczeniami.

Inne rodzaje zorientowanych plikowo serwerów pamięci zostały utworzone poprzez wydzielenie funkcjonalności z NAS. Jeżeli urządzenie pamięci masowej zostanie usunięte z NAS, to pozostałość nosi nazwę NAS Head. Wymienione urządzenie NAS Head ma zorientowany plikowo system operacyjny, aplikacje do zarządzania woluminami i macierzą RAID oraz obsługę funkcji wejścia-wyjścia niezbędnych do wysyłania poleceń i odbierania danych z urządzenia pamięci masowej. Jednak NAS Head nie wykonuje podstawowych operacji pamięci masowej. Ta funkcja została wydzielona przez połączenie serwera pamięci masowej do tej samej sieci SAN, do której jest podłączone urządzenie NAS Head. Z punktu widzenia aplikacji bądź komputera macierzystego NAS Head jest identyczny z samodzielnym serwerem NAS. NAS Head to znacznie bardziej elastyczne urządzenie. Może być podłączone do komputera macierzystego za pomocą sieci LAN lub bezpośrednio za pomocą oprogramowania LVM (ang. *Logical Volume Manager*).

Kolejna operacja wydzielenia powoduje usunięcie z NAS zorientowanego plikowo specjalizowanego systemu operacyjnego. Komputer macierzysty musi więc współpracować z urządzeniami pamięci masowej bezpośrednio, z dyskiem z ograniczeniami, albo za pośrednictwem sieci pamięci masowej prowadzącej do macierzy dyskowej. W przypadku filera DAS (ang. *Direct Attached Storage*) komputer macierzysty musi mieć możliwość tworzenia woluminów logicznych przy użyciu oprogramowania nazywanego LVM oraz prawdopodobnie obsługiwać tworzenie macierzy RAID. Zastosowanie oprogramowania RAID — niezależnie od tego, czy wbudowanego w system operacyjny, czy dostarczanego przez firmę trzecią, na przykład VERITAS Volume Manager — może nie być konieczne, ponieważ wiele urządzeń HBA jest sprzedawanych wraz z kontrolerem RAID wbudowanym bezpośrednio na płycie głównej. Wszystkie macierze dyskowe są dostarczane wraz ze sprzętowym kontrolerem RAID. Tak więc kiedy komputer zostaje połączony z macierzą dyskową, potrzebuje jedynie LVM do celu przeprowadzenia operacji względem zorientowanego plikowo pamięci masowej.

Zorientowane plikowo serwery pamięci masowej działają doskonale, kiedy aplikacja przekazuje urządzeniu pamięci masowej zestaw poleceń, takich jak „odczytaj ten zestaw plików”, „ponownie indeksuj ten system plików” lub „wykonaj przyrostową kopię migawkową bądź kopię zapasową tego woluminu”. Każda operacja, gdzie informacja izoluje położenie pamięci masowej i sekwencje danych na podstawie plików, wiąże się z efektywnością, której blokowe urządzenia pamięci masowej nie mogą się równać.

Klasycznym przykładem efektywnej aplikacji zorientowanej plikowo pamięci masowej jest strumieniowanie danych — im większych tym lepiej. Jeżeli aplikacja wykonuje żądanie pojedynczego, ogromnego, strumieniowanego pliku, to urządzeniu pamięci masowej prze-

kazuje sekwencję lokalizacji na dysku, które następnie wywołują operacje odczytu niezbędne, aby żądany plik był dostępny dla aplikacji w komputerze.

Zorientowany blokowo system pamięci masowej nie wiedziałby, w jaki sposób przetworzyć strumieniowany plik. Otrzymałby informację w jednym bloku, a następnie zażądał położenia kolejnego bloku z indeksu głównego, który mapuje pliki, używając zestawu wskaźników, każdy do kolejnego położenia. Kiedy dane w sekwencji bloków są ponownie łączone wówczas mamy strumień poleceń do wskaźników przedstawiających kolejny segment. To wiąże się z ogromnym obciążeniem i spadkiem wydajności działania strumieniowania w urządzeniach blokowych, zwłaszcza gdy jednocześnie korzysta z niego wielu użytkowników.

Jednak im mniejsza wielkość żądanych plików i większa ich liczba, tym mniejsza różnica w wydajności pomiędzy systemami pamięci masowej zorientowanymi plikowo i blokowo. Pod względem stopnia skomplikowania operacje mapowania stają się podobne, a jedyna różnica polega na tym, że mapowanie jest przeprowadzane przez filer bądź macierz pamięci masowej. Opóźnienie powodowane przez sieć będzie mniejsze w przypadku przekazywania wskaźników lub lokalizacji w pamięci masowej niż w trakcie transferu do aplikacji rzeczywistych plików poprzez sieć pamięci masowej bądź LAN.

## Sieci Fibre Channel

Fibre Channel (FC) to bardzo szybkie połączenie, które pierwotnie zostało wprowadzone w superkomputerach jako HPPI (ang. *High Performance Parallel Interface*). Od tamtej pory interfejs HPPI został zaadaptowany, rozbudowany i stał się interfejsem FC, który został dominującym standardem w sieciach pamięci masowej. Interfejs FC jest zdefiniowany przez zbiór standardów ANSI, które określają nie tylko rodzaj okablowania i połączeń używanych w warstwie fizycznej sieci, ale również protokół FCP (ang. *Fibre Channel Protocol*) jako protokół transportowy. Protokół FCP został zaprojektowany w celu hermetyzacji poleceń i danych w różnych formatach, takich jak SCSI (większość), ATM i IP. Połączenia Fibre Channel mogą być miedziane albo światłowodowe (składające się zarówno z pojedynczego włókna, jak i wielu włókien).

Sieci Fibre Channel czasami są opisywane w kategoriach poziomów klas. Wspomniane poziomy klas opisują rodzaje używanych topologii i połączeń. W użyciu mamy sześć klas sieci Fibre Channel:

- ♦ **Klasa 1.** oznacza połączenia od końca do końca wraz z weryfikacją ramki. Klasa 1. nie używa negocjacji. Każde urządzenie w połączeniu dwupunktowym kontroluje przepływ danych między punktami. Klasa 1. nie jest siecią współdzielonej pamięci masowej, to system zamknięty.
- ♦ **Klasa 2.** jest połączeniem frame-switched, używanym we współdzielonych połączeniach światłowodowych. Doręczana ramka jest weryfikowana, ale ramki nie muszą być dostarczane w kolejności. Brak zagwarantowania kolejności oznacza, że sieć FC klasy 2. nie może komunikować się przy użyciu danych SCSI, które wymagają przekazywania sekwencyjnego. Rozwiązanie zapewnia protokół iSCSI, oferujący wysyłanie SCSI przez Fibre Channel. Tym samym producenci przełączników sieciowych nie muszą dostarczać własnych rozwiązań dla tej klasy, jak to było kiedyś.

- ♦ **Klasa 3.** oferuje przełączanie ramek, ale bez potwierdzenia odbioru w przełączniku sieciowym. W tej klasie potwierdzanie ramki jest funkcją komputera macierzystego. Klasa 3. używa mechanizmu kontroli przepływu bufora. Klasa 3. FC również nie obsługuje zachowania kolejności ramek, ale zawiera funkcję pozwalającą na jednoczesne wysyłanie danych do więcej niż tylko jednego urządzenia.
- ♦ **Klasa 4.** zapewnia częściową alokację pasma — kanał wirtualny. Klasa 4. ma możliwość współdzielenia połączeń.
- ♦ **Klasa 5.** proponuje synchroniczną (w tym samym czasie) usługę just-in-time (dokładnie na czas).
- ♦ **Klasa 6.** to usługa wieloemisyjna, która oferuje dedykowane połączenia światłowodowe.

## Standardy sieci Fibre Channel

Niektórzy będą utrzymywać, że ponieważ standard wymaga jedynie tego, aby porty mogły wzajemnie się komunikować, a połączenie miało strukturę szyny szeregowej, to Fibre Channel tak naprawdę nie stanowi prawdziwej sieci. Jednak na potrzeby niniejszej książki oraz biorąc pod uwagę liczbę różnych urządzeń, które mogą być podłączone do FC, wydaje się rozsądne, aby zbiór urządzeń podłączonych do FC potraktować jako sieć.

W tabeli 15.1 zostały wymienione różne standardy Fibre Channel, które wprowadzono od chwili zdefiniowania pierwszego standardu ANSI w roku 1994. Produkty bazujące na standardzie 8 gigabitów na sekundę są zgodne z pozostałymi. Nowsze standardy 10 i 20 gigabitów na sekundę nie są zgodne wstecz. Producenci, którzy zajmują się produkcją Fibre Channel HBA, to między innymi ATTO, Brocade, Emulex, LSI Logic i QLogic. Urządzenia HBA wymienionych producentów są czasami sprzedawane na podstawie umów OEM, a następnie oferowane klientom pod marką dostawców sprzętu.

**Tabela 15.1.** Standardy sieci Fibre Channel

Standard	Szybkość (Gbod/s)	Przepustowość (Mb/s)
20GFC	21,04	2550
10GFC Parallel	12,75	
10GFC Serial	10,52	1275
8GFC	8,5	800
4GFC	4,25	400
2GFC	2,125	200
1GFC	1,0625	100

Okablowanie, połączenia i złącza Fibre Channel są urządzeniami pasywnymi. Sygnał jest wysyłany i odbierany przez nadajnik (odbiornik). Każde połączenie (złącze) posiada dwa nadajniki (odbiorniki), a dane przesyłane są dwoma żyłami (kanałami) w przeciwnych kierunkach. Taki system eliminuje problemy występujące w sieciach, w których sygnał jest przesyłany za pomocą tej samej żyły. Przykładem takiej sieci może być Ethernet, w której

można zauważyć utratę danych z powodu zakłóceń i rywalizacji sygnału, co wynika z ruchu dwukierunkowego. Dodatkowe obciążenie z tym związane występuje w systemie, gdzie trzeba podjąć środki w celu rozwiązania takiego problemu. W przypadku Fibre Channel istnieje duża odporność na wymienione problemy, co wiąże się z zastosowaniem topologii pętli. Z tego powodu większość urządzeń HBA Fibre Channel ma dwa fizyczne porty.

## Oznaczenia portów

W sieci Fibre Channel port jest dowolną jednostką logiczną, która może być przypisana adresowi sieciowemu oraz pozwala na przepływ danych w obie strony. Obejmuje to nie tylko HBA, ale także fizyczne oraz logiczne urządzenia pamięci masowej, komputery, przełączniki sieciowe oraz huby. W tabeli 15.2 wymieniono różne rodzaje używanych portów Fibre Channel.

**Tabela 15.2.** *Porty sieci Fibre Channel*

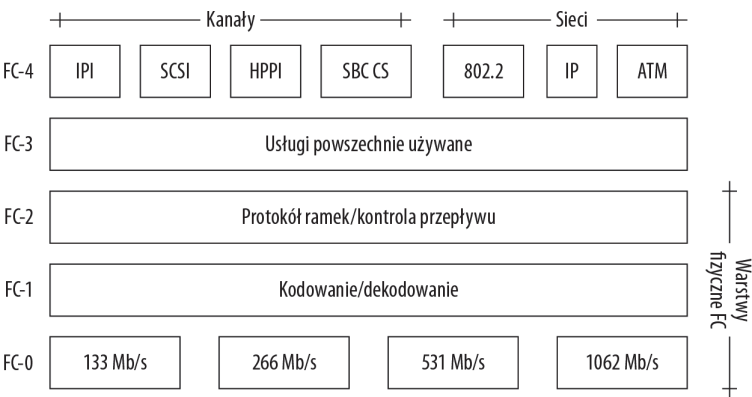
Identyfikator portu	Nazwa	Typ	Przeznaczenie
E_port	Extender Port	Przełącznik sieciowy	Łączy przełączniki sieciowe w kaskadę.
EX_port	Expansion Port (port rozszerzający)	Przełącznik sieciowy (router)	Łączy router FC z przełącznikiem sieciowym FC. W routerze emulowany jest port E_port, natomiast w przełączniku sieciowym jest to port EX_port.
F_port	Fabric Port (port komutowany)	Przełącznik sieciowy	Łączy port komutowany z węzłem.
FL_port	Fabric + Loop Port (port komutowany + pętla)	Przełącznik sieciowy	Łączy port przełącznika sieciowego zarówno w pętlę, jak i przełącznik sieciowy.
Fx_port	Autosensing Port (port automatycznego wykrywania)	Przełącznik sieciowy	Po połączeniu z N_port może stać się portem F_port, natomiast po połączeniu z NL_port może stać się portem FL_port.
G_port	General Port (port ogólny)	Przełącznik sieciowy	Może być użyty do emulacji innego dowolnego portu, zwykle portu E_port lub F_port.
L_port	Loop Port (port pętli)	Węzeł	Łączy węzeł z pętlą FC jako portem NL_port lub FL_port.
N_port	Network Port (port sieciowy)	Węzeł	Łączy węzeł z przełącznikiem sieciowym.
NL	Network + Loop Port (port sieci + pętli)	Węzeł	Łączy węzeł zarówno z pętlą, jak i przełącznikiem sieciowym.
TE_port	Trunking Expansion Port <sup>1</sup>	Przełącznik sieciowy	Standard Cisco VLAN dla połączeń „przełącznik sieciowy do przełącznika sieciowego”, które emulują port E_port.
U_port	Universal Port (port uniwersalny)	Węzeł	Pojęcie stosowane względem dowolnego portu.

<sup>1)</sup> W zależności od producenta i urządzenia ten port może również nosić nazwę Port Channel lub EISL.

# Protokół Fibre Channel Protocol

Protokół Fibre Channel Protocol używa architektury pięciowarstwowej, która zawiera niskiego poziomu warstwę sygnałową oraz wysokiego poziomu warstwy usług, jak pokazano na rysunku 15.8. Warstwy od FC-0 do FC-2 są nazywane warstwami fizycznymi i zawierają protokoły zarówno mediów, jak i połączenia. Różne urządzenia mogą rozpościerać się na odmienne warstwy w tym modelu. Hub FC operuje jedynie na warstwie FC-0. Natomiast przełączniki sieciowe obejmują warstwy od FC-0 do FC-2. Z kolei inteligentne routery FC operują na warstwach od FC-0 do nawet FC-4, ponieważ wiele routerów FC działa również w charakterze routerów SCSI.

**Rysunek 15.8.**  
Architektura  
protokołu Fibre  
Channel Protocol



Poszczególne warstwy protokołu FC mają następujące przeznaczenie:

- ♦ **FC-0.** Warstwa fizyczna (FC-0) obejmuje okablowanie światłowodowe, miedziane, złącza oraz specyfikację elektryczną i parametry optyczne, które są wymagane przez osprzęt. Kiedy używane jest włókno światłowodowe, warstwa FC-0 wykorzystuje system OFC (ang. *Open Fibre Control*) do obniżenia mocy używanego lasera, tak aby nie zniszczyć wykorzystywanych portów FC.
- ♦ **FC-1.** Warstwa łączy danych (FC-1) jest odpowiedzialna za kodowanie i dekodowanie poleceń oraz danych w szeregowym formacie ośmiobitowym na dziesięciobitowy znak transmisyjny. Mniejsze rozmiary ułatwiają wysyłanie i odbieranie szeregowych strumieni bitowych w przypadku wystąpienia błędu.
- ♦ **FC-2.** Warstwa sieciowa (FC-2) jest warstwą zarządzającą transmisją danych w sieci FC. Nadzoruje ona proces tworzenia i zarządzania ramkami, uporządkowanymi zbiorami, sekwencjami, wymianą oraz protokołami Fibre Channel. Protokoły obejmują Primitive Sequence, Fabric Login, N\_Port Login, Data Transfer oraz N\_Port Logout.

W celu zarządzania ruchem sieciowym ramek warstwa FC-2 używa mechanizmu kontroli przepływu bazującego na dostępnej przestrzeni bufora. Dla różnych rodzajów ruchu sieciowego można zdefiniować odmienne klasy usług.

- ♦ **FC-3.** Warstwa powszechnie używanych usług (FC-3) zawiera mechanizm służący do zarządzania maskowaniem portu N-port. Pozwala to wielu portom na równoległą transmisję danych jako pojedynczej jednostki informacji przez wiele połączeń. Obsługiwana jest także funkcja nosząca nazwę „hunt groups”, dzięki której więcej

niż tylko jeden port może odpowiadać na pojedynczy alias adresu. Wymieniona funkcja poprawia wydajność przez umożliwienie dostępu do urządzenia pamięci masowej, które może być zajęte bądź zablokowane na innym porcie. Trzecią technologią implementowaną przez FC-3 jest multitemisja, która w FC przedstawia ideę wysyłania danych do więcej niż tylko jednego portu w danym czasie. Można więc na przykład wysyłać dane do wszystkich lub dowolnego portu N\_port.

- ♦ **FC-4.** Warstwa mapowania protokołu (FC-4) jest warstwą interfejsu aplikacji, która mapuje protokoły sieciowe do warstw FC niższych niż FC-4. Obsługiwana sieć i struktura szyny to Small Computer System Interface (SCSI), Intelligent Peripheral Interface (IPI), High Performance Parallel Interface (HIPPI) Framing Protocol, Internet Protocol (IP), ATM Adaptation Layer for computer data (AAL5), Link Encapsulation (FC-LE), Single Byte Command Code Set Mapping (SBCCS) oraz IEEE 802.2.

## Zarządzanie ruchem sieciowym Fibre Channel

Protokół Fibre Channel Protocol stosuje formę zarządzania ruchem sieciowym na podstawie kredytów bufora. Każdemu portowi w sieci jest przypisany budżet ruchu sieciowego do wykorzystania. Po wykorzystaniu dostępnego budżetu ruch sieciowy danych jest przekierowywany do kolejnego portu w sekwencji. Kredyty bufora są zdefiniowane dla kontroli przepływu od końca do końca, gdzie porty N\_port, L\_port lub NL\_port służą w charakterze punktów końcowych. Porty potwierdzają otrzymanie ramki, a następnie dodatkowy kredyt jest przydzielany portowi wysyłającemu, który zostaje umieszczony w kolejce ruchu sieciowego. Drugi rodzaj kontroli przepływu nosi nazwę kontroli od bufora do bufora i zarządza dostępnym kredytem między dwoma sąsiadującymi portami. Kontrola ruchu sieciowego od bufora do bufora opiera się na tym, że port otrzymujący dane wysyła do portu wysyłającego sygnał gotowości do odbioru danych.

Sieć FC-SW (ang. *Fibre Channel Switched fabric*) używa odmiennego mechanizmu kontroli przepływu. Węzły i procesy wysyłają swój status różnym portom jako część rytuału logowania. Kiedy każdy węzeł loguje się do sieci FC-SW, port inicjujący i docelowy uwierzytelniają logowanie węzła i negocjują właściwości połączenia, między innymi typ używanych protokołów oraz szybkość transmisji. Sieć FC-SW używa protokołu FCP-SCSI. Wymieniony proces uwierzytelniania logowania i negocjacji właściwości występuje w każdym rodzaju połączenia FC-SW, nawet w tym, które wykorzystuje bezpośrednio dołączone urządzenie Fibre Channel.

## Kontrola przepływu w sieci Fibre Channel

Ramki Fibre Channel mają znaczniki początkowe i końcowe. Nagłówek definiuje ramkę oraz zawiera adres, dane, korekcję błędów, zbiór weryfikujący dane, który przeprowadza operację potwierdzenia, jak również odzyskiwanie danych. Ramki hermetyzują dane w innych protokołach, tak więc ramka Fibre Channel przeprowadza mapowanie do innych protokołów na wyższym poziomie, takich jak SCSI, IP, HIPPI, FICON, ESCON, 802.2 oraz Virtual Interface Architecture (VIA). Na rysunku 15.9 pokazano strukturę ramki FC.



Schemat arbitrażu używany przez sieć FC-AL bazuje na schemacie arbitrażu szyny SCSI. W sieci FC-AL port o najwyższym priorytecie uzyskuje dostęp do przewodu w celu wysyłania i odbierania ramek. Szyna SCSI wykorzystuje priorytet bazujący na charakterystyce elektrycznej szyny, natomiast w sieciach FC-AL priorytet jest określany w oprogramowaniu jako polecenia. W ten sposób sieć FC-AL działa zarówno na przewodzie miedzianym, jak i światłowodzie.

Port `L_port` lub `NL_port` w sieci FC-AL rozpoczyna komunikację przez wydanie w pierwszej kolejności polecenia oznaczającego gotowość do wysyłania danych. Kiedy polecenie przechodzi przez pętlę, każdy węzeł po kolei porównuje priorytet z węzłem, który chce uzyskać dostęp do pętli. Następnie ten węzeł pobiera albo przekazuje polecenie kontrolne. Kiedy pętla będzie dostępna dla dowolnego portu, następuje wymiana danych i zmiana priorytetów. Węzeł o kolejnym priorytecie w kolejności ponownie rozpoczyna sekwencję „gotowy do wysyłania danych” i przyjmuje polecenie pętli. Następuje wymiana ramek z użyciem sekwencji transmisji ramek, przy czym wielkość ramki zazwyczaj mieści się w dwóch kilobajtach. Mała wielkość ramki oznacza możliwość szybkiego odzyskania wszelkich utraconych ramek, ponieważ proces ponownego ich transferu będzie krótki. To ma zasadnicze znaczenie w przypadku szeregowej komunikacji danych.

Pętle arbitrażowe mogą być konstruowane w postaci pierścienia albo huba (pasywna gwiazda). Postać pierścienia jest prostsza do zaimplementowania, ale ma taką wadę, że awaria dowolnego urządzenia w pierścieniu oznacza awarię całego pierścienia. Z kolei hub nadal funkcjonuje po awarii urządzenia, ponieważ po podłączeniu do huba za pomocą topologii gwiazdy każde urządzenie nadal jest logicznym pierścieniem.

FC-AL używa podzbioru różnych typów dostępnych portów logicznych. Porty `NL_port` i `FL_port` lub `L_port` są portami, które mogą być używane w komunikacji arbitrażowej. Porty `NL_port` muszą mieć możliwość zalogowania do sieci fabric i uwierzytelnienia się. Rejestracja nazw wykorzystuje protokół FLOGI (ang. *Fabric Login*). Port `NL_port` będzie inicjatorem wszelkiej komunikacji do innych węzłów w sieci fabric. Pętla arbitrażowa połączona przez port `FL_port` jest uznawana za pętlę publiczną, podczas gdy każdy port `NL_port`, który nie jest podłączony do sieci fabric, jest uznawany za pętlę prywatną. Z punktu widzenia protokołów FC-AL połączenie do huba nie jest uznawane za port.

## Sieć Fibre Channel Switched fabrics

Sieć Fibre Channel Switched fabric (FC-SW) to sieć, w której różne urządzenia sieciowe są połączone z innymi za pomocą pośrednich, inteligentnych przełączników sieciowych Fibre Channel. Jak zostanie powiedziane w rozdziale 17., w którym przedstawiono sieć fabric InfiniBand oraz systemy zestawu komputerów, topologie sieci fabric mają wiele zalet. Sieci fabric zapewniają skalowalność, są odporne na uszkodzenia i bardzo elastyczne.

W celu implementacji sieci FC-SW będzie potrzebny przełącznik sieciowy FC, który jeszcze przed rokiem 2003 należał do bardzo kosztownych elementów. Dostępność znacznie tańszych przełączników FC, jak również spadek kosztu jednostkowego za pojedynczy port w większych przełącznikach (nazywanych Fibre Channel Directors) spowodowały, że sieci FC-SW stały się dominującą architekturą sieci pamięci masowej. Brocade, Cisco oraz QLogic to doskonale znani producenci przełączników sieciowych Fibre Channel, choć nie są jedyne. Przełącznik sieciowy klasy Fibre Channel Directors zawiera co najmniej 128 portów.

## Adresowanie Fibre Channel

Sieć FC-SW ma przestrzeń adresową wraz z  $2^{24}$  adresami logicznymi (16 777 216). Kiedy w tej samej sieci są używane co najmniej dwa przełączniki sieciowe, to mogą być skonfigurowane w taki sposób, aby utworzyły sieć kratową (ang. *mesh network*). W sieciach FC-SW stosowane są trzy różne schematy adresowania *World Wide Name* (WWN), adresy portów oraz *Arbitrated Loop Physical Addresses* (AL-PA).

Schemat WWN, czasami określany jako WWID, został przypisany urządzeniom pamięci masowej zarówno Fibre Channel, jak i Serial Attached SCSI. Schemat WWN pełni w sieci FC-AL taką samą funkcję jak adres Ethernet MAC w sieci TCP/IP. W schemacie WWN stosowane są dwie konwencje nazw. Pierwsza — WWNN — to węzeł WWN i ma zastosowanie względem wszystkich portów w urządzeniu HBA. Druga to port WWN (WWPN) i jest unikalnym identyfikatorem portu.

Schemat WWN używa adresu przypisanego w trakcie produkcji urządzenia. Wspomniany adres składa się z szesnastkowego prefiksu 10:00 lub prefiksu producenta 2#:##, do którego zostają dodane trzybitowy identyfikator producenta i trzybajtowy numer seryjny. Prefiks producenta nosi nazwę OUI (ang. *Organizationally Unique Identifier*). W nowszej konwencji nazw WWN początkowe pół bajta to szesnastkowe 5 lub 6, do których dodany jest trzybitowy identyfikator producenta oraz 4,5-bajtowy numer seryjny.

Przykłady identyfikatorów firm: 00:60:69 dla Brocade; 00:1B:32 dla urządzeń HBA firmy QLogic; 00:C0:DD dla przełączników sieciowych FC firmy QLogic; 00:60:48 dla EMC Symmetrix; 00:60:16 dla EMC CLARiiON, 00:A0:98 dla NetApp; 00:50:76 dla IBM.

Adresy portów są unikalnymi, 24-bitowymi adresami przypisanymi portom. Jest to podobne do przypisywania adresów IP kontrolerowi sieciowemu w sieci TCP/IP. Przypisanie numerów adresów portów należy do osoby bądź organizacji, która konfiguruje sieć FC SAN.

Adresy fizyczne pętli arbitrażowej (ang. *Arbitrated Loop Physical Address*, AL-PA) są używane w topologiach pętli do zdefiniowania adresowalnego i unikalnego adresu. Pętle FC mają małą liczbę węzłów i dlatego wystarczający będzie 8-bitowy identyfikator wraz z 126 adresami.

## Podział na strefy

W sieci pamięci masowej FC-AL istnieje możliwość zaimplementowania funkcji o nazwie **podział na strefy** (ang. *zoning*), która powoduje podział zasobów pamięci masowej w sposób podobny do utworzenia podsieci w sieci Ethernet. Sieć FC-AL obsługuje cztery odmienne rodzaje stref:

- ♦ **Miękki podział na strefy.** Kiedy tworzona jest strefa z miękkim podziałem na strefy, każdy komputer połączony z siecią fabric będzie mógł przeglądać jedynie nazwy urządzeń pamięci masowej, do których dostęp ma ten komputer. Miękki podział na strefy wpływa jedynie na funkcję przeglądania. Każdy komputer nadal może połączyć się z dowolnym urządzeniem, o ile podany będzie adres tego urządzenia. Tak więc miękki podział na strefy nie jest bezpieczną metodą ograniczania dostępu do pamięci masowej.



Podział na strefy to funkcja sieci FC-AL i nie została zaimplementowana w innych rodzajach sieci Fibre Channel.

- ♦ **Twardy podział na strefy.** Twardy podział na strefy to funkcja, która nie tylko ogranicza przeglądanie urządzeń pamięci masowej, ale również blokuje ruch sieciowy z komputera macierzystego do urządzenia pamięci masowej, jeśli dany komputer macierzysty nie ma uprawnień do łączenia się z określonym urządzeniem pamięci masowej. Twardy podział na strefy to bezpieczna metoda kontrolowania dostępu do pamięci masowej. W tej metodzie wykorzystywany jest mechanizm filtrowania ramek w celu ustalenia systemu wysyłającego i odbierającego dane. Twardy podział na strefy jest funkcją przełącznika sieciowego Fibre Channel i nie wszystkie przełączniki sieciowe oferują tę funkcję.
- ♦ **Podział na strefy nazw.** Każdemu urządzeniu w sieci FC-AL jest przypisany unikalny, 8-bajtowy World Wide Name (WWN). Podział na strefy nazw jest stosunkowo bezpieczny, ale pozwala na podszycie się.
- ♦ **Podział na strefy portów.** Strefy mogą być tworzone na poziomie portów przełącznika sieciowego Fibre Channel. W ten sposób port w jednym przełączniku sieciowym ma dostęp lub nie ma dostępu do portów w innym przełączniku sieciowym. Funkcja ta wymaga obsługi ze strony przełącznika sieciowego i zazwyczaj oba używane przełączniki sieciowe pochodzą od tego samego producenta.

Najlepsza metoda bezpieczeństwa opiera się na połączeniu metod podziału na strefy w celu zabezpieczenia dostępu do zasobów sieci pamięci masowej.

## Technologie pamięci masowej z zastosowaniem IP

Wykorzystanie infrastruktury sieci IP dla sieci pamięci masowej wiąże się z dużym wysiłkiem. Do pewnego stopnia sieć IP pamięci masowej może zastąpić pewną część sieci pamięci masowej Fibre Channel, szczególnie w łączach WAN, małych sieciach LAN oraz aplikacjach LAN o małej wydajności. W tym podrozdziale zostaną przedstawione trzy różne technologie stosowania pamięci masowej z użyciem IP:

- ♦ **iSCSI.** iSCSI używa zbioru poleceń SCSI oraz formatu danych w celu wysyłania pakietów za pomocą sieci IP. Ogólnie rzecz biorąc, IP rozszerza SCSI na bardzo duże odległości, pozwalając komputerom macierzystym wraz z DAS na pojawianie się innym węzłom w sieci, tak jakby były współdzielonymi urządzeniami sieciowymi.
- ♦ **Fibre Channel over IP (FCIP lub FC/IP).** FCIP to protokół tunelowania, który enkapsuluje ramki Fibre Channel w ramach pakietów IP. FCIP to technologia dwupunktowa. Urządzenie inicjujące i docelowe enkapsulują i dekapują pakiety w celu otrzymania ramek FC.
- ♦ **iFCP.** iFCP dodaje polecenia i dane Fibre Channel do pakietów IP, a następnie wysyła dane pamięci masowej poprzez IP. To jest koncepcja bardzo podobna do iSCSI pod tym względem, że polecenia iFCP i iSCSI są opakowane przez TCP

do ich transmisji poprzez sieć IP. Jednak technologia FCIP może być stosowana jedynie w sieciach Fibre Channel. Pakiety IP są wysyłane z bramki iFCP do innej bramki iFCP i pozwalają na routing, podczas gdy dane FCIP są wysyłane za pomocą mechanizmu tunelowania.

Sieci pamięci masowej oraz IP są zbudowane na podstawie dwóch odmiennych zestawów wymagań. Sieci pamięci masowej są projektowane w celu zapewnienia maksymalnej przepustowości oraz niezawodności dostarczania danych. Z kolei sieci IP są odporne na uszkodzenia, ale nie były projektowane w celu osiągnięcia maksymalnej szybkości. Wymienione różnice wpływają na sposób stosowania wcześniej wspomnianych protokołów przekazywania pamięci masowej poprzez IP. Każda aplikacja wrażliwa na naturalne opóźnienia sieci IP nie jest dobrą kandydatką do zastosowania standardu pamięci masowej z wykorzystaniem IP.

Dane przesyłane z pokoju do pokoju mogą przechodzić przez jeden router bądź przełącznik sieciowy wraz z występującym w tym czasie jednym „przeskokiem”. Każdy taki „przeskok” powoduje zwiększenie opóźnienia występującego w sieciach TCP/IP. Tak więc połączenie z jednym „przeskokiem” prawdopodobnie będzie sprawdzało się satysfakcjonująco w przypadku połączenia o wysokiej wydajności, przy założeniu, że przepustowość połączenia będzie wystarczająca. Jednak gdy dane są przesyłane przez miasto, województwo bądź kraj, gdzie trzeba uwzględnić opóźnienie wynikające z wielu „przeskoków”, to protokołu FCIP nie będzie można uznać za satysfakcjonujące rozwiązanie podczas łączenia się z bazą danych OLTP bądź pamięcią masową dostępną w sieci.

Bez przeprowadzenia testów nie można powiedzieć, jaka jest przepustowość. Jest ona w dużym stopniu uzależniona od warunków sieciowych. Istnieje jednak możliwość poznania przybliżonej wartości opóźnienia. Wystarczy wysłać niewielkie pakiety zamierzoną trasą przez połączenie FCIP. W tym celu trzeba wykonać kilka operacji traceroute w różnych porach dnia (i tygodnia), a następnie przeanalizować zgłoszone opóźnienie. traceroute to dostępna w systemie Unix wersja polecenia tracert w Windows oraz tracepath w systemie Linux. Na rysunku 15.11 pokazano polecenie tracert wydane z przykładowej stacji roboczej do serwera DNS Verizon. Wartość „przeskoku” w sieci LAN to ogólnie 2 ms (milisekundy), podczas gdy pozostałe wartości opóźnienia to 372 ms (czyli 0,32 s). Jeżeli ruch odbywa się w obie strony, to obliczenia te trzeba podwoić.

**Rysunek 15.11.**  
Wynik obliczenia  
opóźnienia na trasie  
Boston — Nowy Jork

```

C:\Windows\System32\cmd.exe
C:\>tracert 4.2.2.1
Tracing route to vnsc-pri.sys.gtei.net [4.2.2.1]
over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  0.0.0.0
  1  1 ms  <1 ms  <1 ms  192.168.1.1
  2  1 ms  1 ms  1 ms  dslrouter [192.168.1.1]
  3  28 ms  26 ms  27 ms  10.9.45.1
  4  27 ms  28 ms  28 ms  so-0-3-3-0.CORE-RTR1.BOS.verizon-gni.net [130.81.4.65]
  5  29 ms  28 ms  29 ms  so-0-2-0-0.BB-RTR1.BOS.verizon-gni.net [130.81.20.84]
  6  37 ms  36 ms  38 ms  so-6-2-0-0.BB-RTR2.NY325.verizon-gni.net [130.81.19.70]
  7  37 ms  37 ms  37 ms  0.ge-1-1-0.XL3.NYC4.ALTER.NET [152.63.1.45]
  8  35 ms  35 ms  35 ms  0.ge-6-1-0.BR3.NYC4.ALTER.NET [152.63.3.166]
  9  37 ms  36 ms  36 ms  xe-10-2-0.edge2.NewYork2.level3.net [4.68.110.23]
 10  40 ms  34 ms  35 ms  vlan79.csw2.NewYork1.Level3.net [4.68.16.126]
 11  36 ms  35 ms  35 ms  ge-2-0.core1.NewYork1.Level3.net [4.68.97.8]
 12  36 ms  37 ms  35 ms  vnsc-pri.sys.gtei.net [4.2.2.1]

Trace complete.
C:\>

```

## Protokół iSCSI

Protokół iSCSI umieszcza polecenia SCSI wewnątrz pakietów TCP w celu ich transmisji poprzez sieci IP. iSCSI to stosunkowo nowa technologia, która pozwala komputerowi macierzystemu na współpracę z pamięcią masową tak, jakby była podłączona bezpośrednio do komputera. Pamięć masowa jest jednak obecna w sieci IP jako zasób współdzielony. iSCSI oferuje wiele bardzo ważnych zalet względem sieci SAN i Fibre Channel. Ponieważ dane są przesyłane przez sieci IP, to wdrożenie iSCSI jest znacznie tańsze i pozwala na wykorzystanie istniejących sieci. Występujące w Fibre Channel ograniczenie dotyczące odległości nie występuje w iSCSI, więc łącza WAN są praktyczniejsze.

Protokół iSCSI jest udostępniany sprzętowo w urządzeniu HBA albo jako oprogramowanie, w postaci specjalnych sterowników do formatowania pakietów. Wykorzystanie pamięci masowej poprzez IP jako sieci pamięci masowej powoduje, że użycie protokołu iSCSI jest bardzo atrakcyjne we wdrożeniach LAN, oddziałach, grupach roboczych oraz innych rozwiązaniach, w których sieć już istnieje.

Klienty iSCSI są nazywane inicjatorami, polecenia mają format CDB (ang. *Command Descriptor Block*) i są wysyłane do urządzenia docelowego. W celu rozróżniania poszczególnych inicjatorów i urządzeń docelowych iSCSI używa unikalnych identyfikatorów. Istnieją trzy różne i oddzielne konwencje nazw:

- ♦ IQN — *iSCSI Qualified Name*;
- ♦ EUJ — *Extended Unique Identifier*;
- ♦ NAA — *T11 Network Address Authority*.

IQN to najbardziej rozpowszechniony z trzech wymienionych formatów. Przybiera on formę *iqn.yyyy.mm {odwrotna nazwa domeny}*. Przykładem może być *iqn.2009-06.20.com.nazwadomeny:nazwaurzadzenia.typ.polozenie*.

Bardzo ważna jest ochrona ruchu sieciowego iSCSI, ponieważ polecenia są zazwyczaj wysyłane niezaszyfrowane, w postaci zwykłego tekstu. Do nawiązania sesji między inicjatorem i urządzeniem docelowym iSCSI używa różnych metod uwierzytelniania. Najprostszą metodą jest użycie CHAP (ang. *Challenge and Response Protocol*). Bezpieczniejszą metodą uwierzytelnienia może być użycie IPsec jako protokołu sieciowego. Inny sposób używany do zabezpieczenia ruchu sieciowego iSCSI to umieszczenie tego ruchu sieciowego w dedykowanym mu połączeniu wymuszonym na poziomie portu przełącznika sieciowego lub VLAN. iSCSI można również skonfigurować w taki sposób, że połączenie będzie wymagało uwierzytelnienia określonego numeru jednostki logicznej (LUN).

Inicjator iSCSI jest jednym z punktów końcowych sesji SCSI. Wysyła polecenia SCSI do urządzenia docelowego, ale nie określa położenia danych lub wartości LUN danych. Inicjator w systemie komputera macierzystego to najczęściej sterownik urządzenia emulującego iSCSI HBA. Do wysyłania i otrzymywania poleceń iSCSI sterownik urządzenia wykorzystuje stos sieciowy komputera macierzystego. Wymienione sterowniki urządzeń mogą być dostarczane przez producenta systemu operacyjnego lub producenta HBA jako część oprogramowania dołączonego do urządzenia.



Na witrynie Microsoft, pod adresem <http://www.microsoft.com/WindowsServer2003/technologies/storage/iscsi/default.msp>, znajduje się strona poświęcona technologii iSCSI w systemie Windows.

Inicjatory są również zawarte w urządzeniach HBA. Funkcja inicjatora jest osadzona w oprogramowaniu (firmware) urządzenia HBA i zwykle dodaje pewny rodzaj silnika przetwarzającego TCP bez użycia procesora komputera. iSCSI to protokół, który wymaga rozwiązań o wysokiej wydajności oraz funkcji przerzucającej dużą część operacji przetwarzania i ruchu sieciowego danych na urządzenie HBA. iSCSI HBA są obecnie obsługiwane przez 10-gigabitowy bądź 1-gigabitowy Ethernet.

Urządzenie docelowe iSCSI jest punktem końcowym sesji SCSI. Oczekuje na polecenia wysyłane przez inicjator i odpowiada na nie. Urządzenie docelowe pobiera miejsce położenia danych, najczęściej w postaci wartości LUN, i przekazuje je inicjatorowi, tak aby możliwe było pobranie żądanych danych. Urządzenie docelowe iSCSI to najczęściej pewnego rodzaju logiczna jednostka dyskowa znajdująca się w systemie pamięci masowej, choć równie dobrze może to być system taśm bądź optyczny zmieniacz nośników. Urządzenie docelowe może obejmować także zasoby wirtualne, na przykład wirtualne dyski twarde, wirtualne taśmy oraz inne wirtualne media, do których dostęp ma oprogramowanie iSCSI przez użycie kontrolerów wewnętrznych względem urządzeń zawierających wirtualne komponenty.

Oprogramowanie działające w charakterze urządzenia docelowego to sterownik urządzenia na poziomie jądra, który jest dostępny w większości systemów operacyjnych bądź jest dostarczany przez producenta HBA. Niektórzy producenci umieszczają iSCSI wewnątrz oferowanych macierzy dyskowych jako zestaw urządzeń docelowych iSCSI, które mogą komunikować się z wieloma komputerami macierzystymi.

LUN to pozwalająca na adresowanie jednostka pamięci masowej na szynie SCSI. Może to być pojedynczy dysk twardy, macierz RAID lub częściej wolumin, który został zdefiniowany z fragmentu jednego z dwóch pierwszych fizycznych zasobów pamięci masowej. iSCSI traktuje LUN tak jak oddzielny napęd dyskowy; formatuje i montuje system plików w LUN oraz zarządza nim. W celu zamontowania iSCSI LUN jednostka musi być sformatowana przez system iSCSI, wtedy jej system plików staje się częścią definicji iSCSI LUN.

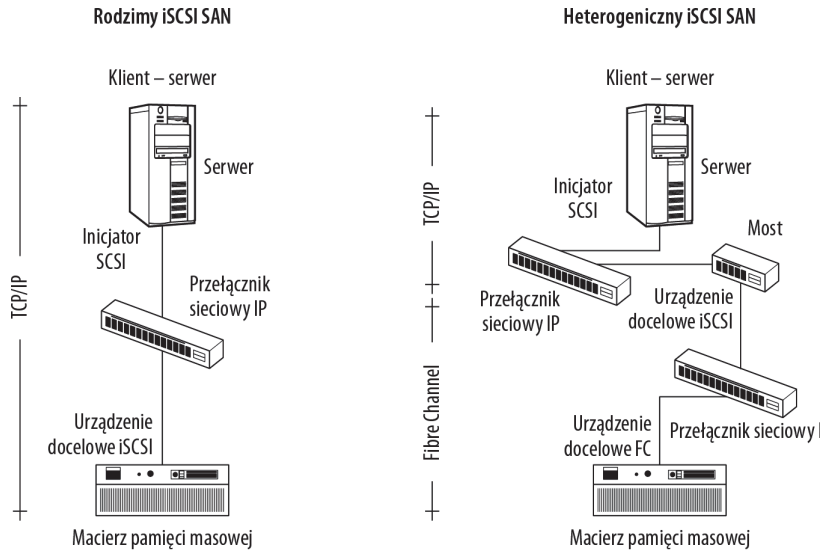
iSCSI to najpopularniejszy z wielu protokołów sieciowych pamięci masowej, który enkapsuluje polecenia pamięci masowej. iFCP współdzieli wiele cech charakterystycznych z opisanym w tym podrozdziale protokołem iSCSI. Na rysunku 15.12 zostały pokazane dwie odmienne topologie iSCSI. Po lewej stronie znajduje się topologia używającego jedynie rodzimego iSCSI. Natomiast po prawej stronie rysunku znajduje się topologia łącząca iSCSI i Fibre Channel za pomocą pośredniego mostka, oznaczonego jako heterogeniczny iSCSI SAN.

## Fibre Channel over IP

Sieci Fibre Channel są niepraktyczne na dłuższych odległościach oraz wymagają kosztownej infrastruktury i specjalistycznej wiedzy w celu ich implementacji. Istnieje ogromna rzesza inżynierów sieciowych znających sieci TCP/IP i ogromna infrastruktura dostępna dla tego protokołu sieciowego. Z tego powodu *Fibre Channel over IP* (FCIP) ma licznych zwolenników.

**Rysunek 15.12.**

Rodzima oraz heterogeniczna implementacja iSCSI SAN



W chwili obecnej sieć FCIP jest używana do łączenia „wysp SAN” za pomocą łączy WAN. Na każdym końcu łącza znajduje się bramka FCIP. Z punktu widzenia sieci miejsce położenia urządzeń bramki nie ma żadnego znaczenia. Największe zmartwienie dotyczy tego, czy możliwe będzie przesłanie wymaganego ruchu sieciowego przez połączenie, wykorzystując dostępną przepustowość łącza.

Wiele sieci Fibre Channel SAN zostało zbudowanych w celu dostarczenia obsługi pamięci masowej dla bardzo szybkich systemów transakcyjnych baz danych. System transakcyjny może wydłużyć czas oczekiwania na dane do sekundy bądź dwóch, ale dłuższy okres oczekiwania skutkuje poważnym zmniejszeniem wydajności działania systemu. Odległość, jaką pakiet FCIP musi pokonać, ma zasadnicze znaczenie, czy sieci FCIP można użyć w systemie transakcyjnym.

Istnieją procesy tolerujące opóźnienie. Tworzenie kopii zapasowej i replikacja to przykłady aplikacji, w których można zastosować FCIP. W procesie tworzenia kopii zapasowej dane są kopiowane z jednego miejsca do drugiego. Jeżeli wystąpi opóźnienie, to po prostu zmniejszy się szybkość przesyłania danych. O ile się zmniejszy? Przy obecnych szybkościach dane są przesyłane przez połączenie OC-3 IP około sześciokrotnie wolniej niż przez FC SAN. Przyrostowe tworzenie kopii zapasowej, często nazywane *data vault*, nadaje się do stosowania FCIP — przykładem może tutaj być popularna aplikacja komercyjna o nazwie Carbonite. Użytkownik definiuje kopię zapasową, a system rozpoczyna powolne kopiowanie wszystkich danych. Kiedy zbiór danych zostanie skopiowany w całości (co może zająć nawet dni), wprowadzane zmiany są kopiowane jedynie z niewielkim opóźnieniem.

Proces *data vaulting* jest szczególnie ważny, kiedy chronione dane są cenne. Produkty przeprowadzające *data vaulting* funkcjonujących systemów transakcyjnych muszą stosować specjalne techniki w celu skopiowania danych, które są zablokowane przez system operacyjny, ponieważ są aktualnie używane. Do rozwiązania tego rodzaju problemów programy te zwykle używają wielu własnościowych technik. Uchwalona w USA ustawa Sarbanes-Oxley (2002), definiująca warunki korporacyjnego przechowywania rekordów, spowodowała, że proces *data vaulting* stał się jeszcze popularniejszy.

## Protokół Internet Fibre Channel Protocol

Protokół iFCP (ang. *Internet Fibre Channel Protocol*) to protokół tunelowania, pozwalający danym Fibre Channel na przepływ z jednej bramki iFCP do innej. Protokół ten został opracowany w celu umożliwienia tworzenia szybkich połączeń dwupunktowych i łączenia sieci SAN przez łącza IP. Enkapsulowane dane wewnątrz iSCSI mogą zawierać polecenia SCSI lub dane sformatowane w FCIP (ang. *Fibre Channel over IP*) i są umieszczane wewnątrz pakietów IP.

W przypadku połączenia iFCP większość pracy jest wykonywana przez TCP/IP, łącznie z wyznaczaniem trasy (*routingiem*) i przełączaniem, wykrywaniem błędów, kontrolą przepływu i odzyskiwaniem danych. Formowanie pakietu następuje w bramce iFCP, podobnie jak wyodrębnianie ramek z otrzymanych pakietów.

## Zarządzanie siecią Storage Area Network

Sieć SAN (ang. *Storage Area Network*) zawiera setki, jeśli nie tysiące elementów, którymi trzeba zarządzać, aby sieć pamięci masowej działała optymalnie. Wspomniane elementy obejmują ruch sieciowy portów, przypisanie portów, aktywność dyskową, monitorowanie połączeń, charakterystyki wydajności komputera oraz wiele innych czynników. Niemal wszystkie komponenty zainstalowane w sieci SAN spełniają standardy przemysłowe, takie jak SNMP, co pozwala na ich wyszukanie i zarządzanie nimi. Większość oprogramowania przeznaczonego do zarządzania siecią SAN to struktury szkieletowe, używające SNMP dla poleceń oraz funkcji kontrolnych wydawanych z poziomu konsoli (komputer).

Większość oprogramowania do zarządzania siecią SAN to aplikacje dla systemu Windows bądź Solaris, wiele z nich bazuje na przeglądarce internetowej, więc są niezależne od platformy sprzętowej. Kiedy używany jest system Windows, do zarządzania urządzeniem aplikacja bardzo często stosuje interfejs WMI (ang. *Windows Management Instrumentation*).

WMI to rozszerzenie WEBM (ang. *Web-Based Enterprise Management*) oraz modelu CIM (ang. *Common Information Model*), który został opracowany przez zespół DMTF (ang. *Distributed Management Task Force*) w celu standaryzacji komponentów. W poprzednim zdaniu użyto wielu skrótów, ale WMI jest stosowane wymiennie z SNMP i pozwala komputerom z systemem Windows na używanie interfejsu wiersza poleceń (WMIC), opracowanego przez firmę Microsoft w celu uzyskiwania łatwego dostępu do urządzeń. Narzędzia graficzne to po prostu nakładki na te polecenia.

Oprogramowanie zarządzające siecią SAN może być zaimplementowane wewnętrznie w postaci urządzenia lub serwera na krawędzi sieci SAN bądź w samej sieci SAN jako część ścieżki danych. Może być również zaimplementowane jako jedno z wymienionych urządzeń, ale w postaci rozwiązania zewnętrznego, które znajduje się w sieci lokalnej (LAN), nie w ścieżce danych wejścia-wyjścia pamięci masowej. Aplikacje te mogą przeprowadzać operacje wykrywania i mapowania, monitorowania użycia przepustowości oraz wprowadzać zmiany w środowisku. Przykłady pakietów zarządzających siecią SAN są Onaro SANscreen (teraz własność NetApp), EMC ControlCenter SAN Manager oraz System Storage SAN Volume Controller (SVC) firmy IBM. Oprogramowanie tej kategorii jest bardzo drogie, ale przynosi ogromne korzyści pod względem efektywności.

Pokrewnym rodzajem oprogramowania używanego w zarządzaniu sieciami jest oprogramowanie SRM (ang. *Storage Resource Management*). Oprogramowanie SRM można zaimplementować w sieciach dowolnego rodzaju (LAN, SAN itd.) i monitorować zasoby pamięci masowej aż do najniższego poziomu. Wczesne wersje SRM pozwalały na zarządzanie limitami dyskowymi, ale w obecnej generacji oprogramowania SRM możliwe jest ustalenie dysków, które są niemal zapełnione, określenie najczęściej używanych plików, liczby egzemplarzy poszczególnych fragmentów danych itd. Oprogramowanie SRM jest nieocenione w przedsiębiorstwach oraz sieciach pamięci masowej, ale jego cena powoduje, że to stosunkowo mało liczna kategoria. System Windows Server 2008 jest dostarczany wraz z podstawową aplikacją SRM, która pozwala użytkownikowi na samodzielne przetestowanie tego obszaru technologii. W przyszłości oprogramowanie SRM prawdopodobnie stanie się standardowym modulem we wszystkich sieciowych systemach operacyjnych.

## Protokół Internet Storage Name Service

Protokół iSNS (ang. *Internet Storage Name Service*) to proponowany standard IETF, który ma na celu ujednolicenie metod używanych do zarządzania urządzeniami iSCSI i FCIP w sieci IP. Spora liczba producentów oferuje serwery iSNS, między innymi OpenSolaris Project, Microsoft iSNS Server 3.0 oraz Linux isns for iscsi. Usługi iSNS dostarczają następujących możliwości:

- ♦ rejestrowanie nazw;
- ♦ wykrywanie domen (DD, ang. *Discovery Domain*);
- ♦ uwierzytelnianie logowania;
- ♦ wykrywanie zasobów pamięci masowej;
- ♦ informowanie o zmianie stanu (SCN, ang. *State Change Notification*);
- ♦ zarządzanie połączeniem Fibre Channel i iSCSI.

Podczas gdy w każdej implementacji część Fibre Channel w iSNS jest wymagana, to część iSCSI jest opcjonalna. Protokół tworzy zestaw usług zarządzania, które emulują sieć Storage Area Network Switched fabric. Istnieją cztery części sieci iSNS:

- ♦ **Serwer (serwery).** Serwer iSNS może obsługiwać ruch sieciowy zarówno iSCSI, jak i FCIP.
- ♦ **Klient (klienci).** Klient to dowolne urządzenie obsługujące iSNS.
- ♦ **Baza (bazy) danych.** Baza danych iSNS obsługuje informacje o klientach w jej DD oraz zdarzeniach.
- ♦ **Protokół iSNS (iSNSP).** Protokół jest wykorzystywany do komunikacji pomiędzy klientem, serwerem, przełącznikami sieciowymi i innymi urządzeniami docelowymi.

Ustanowienie systemu zarządzającego iSNS pozwala urządzeniom docelowym na rejestrację w DD oraz na to, by mogły być zarządzane za pomocą jednostek logicznych, takich jak grupy pamięci masowej. Przechowywane dane uwierzytelniające mogą być stosowane względem zbioru jednostek pamięci masowej, które pozwalają sieci pamięci masowej na zarządzanie ogromną ilością zasobów. Kontrola nad poszczególnymi fragmentami struktury zarządzającej może być delegowana.

## Podsumowanie

W tym rozdziale zostały przedstawione technologie sieci pamięci masowej oraz powody, dla których są takie ważne. Niektóre z obecnie największych używanych sieci to Storage Area Network (SAN). Sieci pamięci masowej mogą być opisane w kategoriach ich topologii oraz wykorzystywanych technologii. Jednym z ważniejszych tematów poruszonych w rozdziale były sieci Fibre Channel. Topologie sieci pamięci masowej mogą być oparte na: połączeniu bezpośrednim, połączeniu dwupunktowym, pętli arbitrażowej oraz fabrics.

Zaprezentowany został model współdzielonej sieci pamięci masowej, co pozwoliło Czytelnikowi na poznanie słownictwa stosowanego do opisanie różnych aplikacji, urządzeń oraz technologii. Urządzenia pamięci masowej mogą być w szerokim ujęciu podzielone na rozwiązania zorientowane blokowo lub plikowo. Model współdzielonej pamięci masowej został rozszerzony o urządzenia taśmowe.

Koncepcje takie jak dyski fizyczne kontra logiczne, wirtualizacja pamięci masowej, agregacja i przekierowanie powodują, że sieci pamięci masowej są łatwe w adaptowaniu i użytkowaniu.

W kolejnym rozdziale zostaną przedstawione kolejne technologie sieci o wysokiej wydajności.

# Rozdział 16.

## Łączy o dużej szybkości

### W tym rozdziale:

- ♦ Różne standardy sieci o dużej szybkości
- ♦ Techniki służące do zmniejszania obciążenia sieciowego
- ♦ Komputery sieciowe o wysokiej wydajności
- ♦ Grid, mesh, edge i cloud computing

Wydajne systemy obliczeniowe do swojego funkcjonowania wymagają sieci. To mogą być systemy o potężnych możliwościach używające sieci o wysokiej wydajności lub systemy rozproszone, które składają się z wielu elementów składowych i mogą używać sieci o małej szybkości. W tym rozdziale przedstawione będą oba rodzaje rozwiązań.

Ethernet to dominujący standard sieci. Przetwarzające obecnie systemy oparte na technologii Ethernet używają 10-gigabitowego Ethernetu (10GbE). Standard ten został opisany w tym rozdziale, podobnie jak przyszłe formy Ethernetu, nad którymi trwają prace.

W chwili obecnej sieci mogą przekazywać większą ilość ruchu sieciowego, niż może być przetworzona przez przeważającą część komputerów. Aby komputery stały się efektywniejsze, na rynek wprowadzono kilka nowych technologii; np. TOE (ang. *TCP Offload Engine*) pozwalają na przesunięcie przetwarzania stosu TCP do karty sieciowej, odciażając procesor komputera.

Inny zbiór technologii podobnych do TOE nosi nazwę *zero copy network*. Polega on na utworzeniu wirtualnego interfejsu sieciowego, który również przyczynia się do redukcji obciążenia związanego z przetwarzaniem sieciowym. Architektura VIA (ang. *Virtual Interface Architecture*) oraz szyna urządzenia InfiniBand to przykłady analizowanych sieci typu zero copy network. Pięć z dziesięciu najpotężniejszych komputerów na świecie zostało zbudowanych na bazie tej szyny o wysokiej szybkości.

Przeanalizowane tu będą różne typy klastrów sieciowych. Obejmują one systemy odporne na awarie zapewniające poprawną pracę mimo usterek, rozwiązania równoważące obciążenia pomagające w osiągnięciu lepszego poziomu wykorzystania zespołu serwerów oraz wszechobecnych narzędzi obliczeniowych, gdzie systemy rozproszone są połączone razem w sieć i tworzą wirtualny superkomputer.

Przetwarzanie sieciowe (*grid* lub *mesh computing*) jest bardzo ważnym i zyskującym coraz większą popularność obszarem sieci komputerowych. Największe zbudowane dotąd projekty komputerowe są właśnie tego rodzaju. Przykładem może być *Folding@home* lub *SETI@home*. Systemy przetwarzania sieciowego są rozwijane w celu umożliwienia „przetwarzania w chmurze” (ang. *cloud computing*) oraz z uwzględnieniem przyszłego tworzenia służących temu narzędzi komputerowych.

## Wydajne systemy obliczeniowe

*Wydajne systemy obliczeniowe* (ang. *High-performance computing*, HPC) to pojęcie używane w stosunku do systemów charakteryzujących się wysoką wydajnością lub wysoką szybkością generowania danych wyjściowych. Zaczęto nim określać komputery typu mainframe, superkomputery, klastry komputerów, a ostatnio rozproszone systemy przetwarzania sieciowego, znajdujące się w „chmurach”. Aby możliwe było dostarczenie usług niezbędnych do funkcjonowania architektury systemów HPC, większość ich opiera się na swojej sieci.

W niektórych przypadkach sieć musi używać zaawansowanego osprzętu sieciowego, takiego jak Ethernet 10 gigabitów na sekundę (i więcej), łączy o wysokiej wydajności, takich jak InfiniBand, oraz specjalnych funkcji adapterów sieciowych, na przykład TOE i Virtual Interface Architecture. W rozdziale zostaną przedstawione wymienione technologie, jak również powody, dla których są tak ważne, oraz miejsca, gdzie są obecnie używane.

Jeżeli skala projektu jest odpowiednio duża, to wysoką wydajność można także osiągnąć, używając wolnych i mniej niezawodnych połączeń, na przykład internetu dostępnego na komputerach o małej mocy obliczeniowej, lub wykorzystując ułamek zasobów komputera o dużej wydajności. Największe utworzone dotąd projekty obliczeniowe, przeprowadzające najwięcej obliczeń, to systemy rozproszone, które działają na komputerach wolontariuszy rozsianych na całym świecie. Ogólnie rzecz biorąc, systemy tego rodzaju to w znacznym stopniu superkomputery przetwarzania równoległego. Chociaż nie są bezpłatne (ktoś musi płacić za energię elektryczną), to jednak są systemami o niskich kosztach, ponieważ systemy te są współdzielone i używane do różnych celów. Pozwalają na realizowanie kosztownych projektów, których przeprowadzenie w innym przypadku byłoby niemożliwe.

Istnieje duże zainteresowanie, z naciskiem na sieci komputerowe jako narzędzia i na oprogramowanie jako usługę, systemami komputerowymi tworzącymi „chmurę” umożliwiającą powstanie zjawiska określanego mianem *przetwarzanie bez granic*. Oznacza to dostępność sieci w każdym miejscu. Przemysł przesuwają się w kierunku tego typu systemu zarówno w dziedzinie oprogramowania i systemów operacyjnych, jak również zdalnych aplikacji przez używanie technologii wirtualizacji. Systemy przetwarzania sieciowego i sieci rozproszone zyskują więc jeszcze większą popularność.

Jeżeli Czytelnik siedzi przed ekranem swojego komputera PC, to może rozsądnie zadawać sobie pytanie, co ten rozdział ma wspólnego z siecią. Odpowiedzią jest oczywiście to, że tego rodzaju technologie stają się z czasem coraz tańsze i są wykorzystywane w kolejnej generacji sprzętu komputerowego. Z dużym prawdopodobieństwem można oczekiwać, że w nadchodzących pięciu latach technologie omówione w tym rozdziale zostaną szeroko wprowadzone w wielordzeniowych komputerach domowych, działających pod kontrolą systemów operacyjnych pozwalających na przetwarzanie równoległe.

Jeżeli Czytelnik jest ciekawy, to warto wspomnieć, że projekt Top500.org (<http://top500.org>) dwukrotnie w ciągu roku zbiera dane statystyczne dotyczące najpotężniejszych komputerów na świecie. Zebrane informacje są przechowywane na witrynie internetowej projektu w formie pozwalającej na poznanie producentów, technologii, krajów i instalacji, które osiągnęły określony poziom wydajności. Liczby podawane na witrynie projektu Top500 bazują na danych statystycznych LINPACK, dostarczanych przez osoby pracujące z danymi systemami albo z nimi powiązane. W tabeli 16.1 wymieniono dziesięć najlepszych komputerów, które znalazły się na liście w listopadzie 2010 roku.

## Poza gigabitowy Ethernet

Gigabitowy Ethernet (GbE lub czasem GigE) to obecny standard dla sieci typu Ethernet. Oznacza to możliwość zakupu przełączników sieciowych GbE, routerów i hubów w rozsądnych cenach, dzięki którym ten osprzęt sieciowy staje się praktycznym wyborem dla sieci w małych firmach oraz domach.

Ethernet jest tak wszechobecnym standardem, że w tym rozdziale wykroczymy w przyszłość, aby poznać mapę drogową rozwoju Ethernetu pod kątem sieci o wysokiej wydajności.

Standardy Ethernetu przechodziły przez progresję, gdzie szybkość wzrastała dziesięciokrotnie wraz z wprowadzeniem każdej nowej generacji. Jak dotąd, dostępne są następujące generacje Ethernetu:

- ♦ 10 Mb/s Ethernet;
- ♦ 100 Mb/s Ethernet;
- ♦ 1 Gb/s Ethernet, 1 GbE;
- ♦ 10 Gb/s Ethernet, 10 GbE;
- ♦ 40 Gb/s Ethernet, 40 GbE;
- ♦ 100 Gb/s Ethernet, 100 GbE.

Standardy 40 Gigabit Ethernet i 100 Giga Ethernet (IEEE 802.3ba) pojawiły się w roku 2010 i obecnie są to najszybsze zdefiniowane standardy Ethernetu na rynku. W przypadku 40 GbE i 100 GbE są dostępne interfejsy dla kabli światłowodowych jedno- i wielomodowych, standard opisuje również rozwiązanie dla kabli miedzianych na niewielkie odległości (10 m), jednak na rynku jeszcze nie ma dostępnych takich rozwiązań. Wersje 10 GbE są dostępne dla kabli światłowodowych i miedzianych oraz miedzianych twin-ax (InfiniBand). Standard definiuje połączenia z pełnym duplexem (dwukierunkowy ruch sieciowy) oraz nie obsługuje półduplexu CSMA/CD. Obecny rynek dla technologii 10 GbE to ponad milion portów rocznie sprzedawanych w pamięci masowej, sieciach fabric oraz na rynku wirtualizacji.

W przypadku 10 GbE warto zwrócić uwagę na fakt dostępności kilku różnych rodzajów połączeń 10GBase-T. W przypadku włókna światłowodowego dostępne są następujące wersje połączeń 10GBase: R (standard Range), SR (*Short Range*), LR (*Long Range*), LRM (*Long Range Multimode*), ER (*Extended Range*), ZR oraz LX4. W przypadku przewodów

**Tabela 16.1.** *Dziesięć najlepszych komputerów na świecie*

Pozycja	$R_{\max}$ (TFLOPS)	$R_{\text{szczytowe}}^*$ (TFLOPS)	Nazwa kodowa	Opis	Producent	Lokalizacja
1	2566	4701	Tianhe	NUDT TH MPP, X5670 2,93 GHz 6C, NVIDIA GPU, FT-1000 8C	NUDT	National Supercomputing Center in Tianjin, Chiny, 2010
2	1759	2331	Jaguar	Cray XT5-HE Opteron 6-core 2,6 GHz	Cray	Oak Ridge National Laboratory, USA, 2009
3	1271	2984	Nebulae	Dawning TC3600 Blade, Intel X5650, NVidia Tesla C2050 GPU	Dawning	National Supercomputing Centre in Shenzhen (NSCS), Chiny, 2010
4	1192	2288	TSUBAME 2.0	HP ProLiant SL390s G7 Xeon 6C X5670, Nvidia GPU	NEC/HP	GSIC Center, Tokyo Institute of Technology, Japonia, 2010
5	1054	1289	Hopper	Cray XE6 12-core 2,1 GHz	Cray	National Energy Research Scientific Computing Center, USA, 2010
6	1050	1255	Tera-100	Bull bullx super-node S6010/S6030	Bull SA	Commissariat a l'Energie Atomique (CEA), Francja, 2010
7	1042	1376	Roadrunner	BladeCenter QS22/LS21 Cluster, PowerXCell 8i 3,2 Ghz/Opteron DC 1,8 GHz, Voltaire Infiniband	IBM	Los Alamos National Laboratory, USA, 2009
8	832	1029	Kraken XT5	Cray XT5-HE Opteron 6-core 2,6 GHz	Cray	National Institute for Computational Sciences, University of Tennessee, USA, 2009
9	825	1003	Jugene	Blue Gene/P Solution	IBM	Forschungszentrum m Juelich (FZJ), Niemcy, 2009
10	817	1029	Cielo	Cray XE6 8-core 2,4 GHz	Cray	Los Alamos National Laboratory, USA, 2010

\*  $R_{\max}$  oznacza najwyższy wynik LINPACK, natomiast  $R_{\text{szczytowe}}$  oznacza teoretyczny, maksymalny wynik wyrażony w teraflopach.

miedzianych standardy połączeń dla 10GBase to T: (802.an-2006), CX4 (802.ak), SFP+ Direct Attach, KX4 oraz KR. KX4 i KR to standardy 802.3ap używane na płytach montażowych jako routery, przełączniki sieciowe oraz serwery blades. Analogiczne oznaczenia są stosowane w standardach dla 40 GbE i 100 GbE.

## 10GBase-T

10GBase-T to najpopularniejszy rodzaj połączenia, który może być używany wraz ze skrętką przewodów miedzianych na odległość do 100 metrów, ale to nie jest najszybszy rodzaj połączenia. Typ 10GBase-T jest zgodny wstecz z 1GBase-T, a jego porty mogą automatycznie negocjować szybkość portu. Ten standard używa wtyczek RJ-45 oraz okablowania kategorii 6., najlepiej przewodów Cat6a. Dodatkowe partycjonowanie w przewodzie pozwala na redukcję wzajemnego przenikania.

Moduły połączeń dla kabli 10GbE są nazywane PHY i łączą warstwę połączenia urządzenia (MAC) z kablem miedzianym bądź światłowodem. PHY to układ włączający warstwę fizyczną połączenia z kablem 10GbE i jest umieszczony wraz z mikrokontrolerem w module, który można umieścić na płycie montażowej przełącznika sieciowego lub routera 10GbE. Układy PHY istnieją zarówno dla modułów 10GbE LAN, jak i WAN, ale WAN PHY, choć są wolniejsze, to współdzielił ten sam typ optyki. Układ koduje i dekoduje dane podczas transmisji i ma dwa oddzielne podsystemy: PCS (ang. *Physical Coding Sublayer*) oraz PMDL (ang. *Physical Medium Dependent Layer*). Inne technologie używające układów PHY to między innymi USB, SATA, IrDA (czasami) oraz wiele innych systemów osadzonych.

Karty interfejsów sieciowych (ang. *Network Interface Cards*, NIC) 10GbE można zakupić u wielu producentów, takich jak np. Intel, Chelsio, NetXen, Silicom, HP, Neterion, LeWiz, Tehuti Networks oraz Myricom. Jeden z producentów — NetEffect — został ostatnio wykupiony przez firmę Intel. Karty NIC używają szyny PCI-X lub PCI i są połączone za pomocą różnych rodzajów modułów PHY. Bieżącym zaleceniem jest kupowanie standardowych miedzianych CX4 dla połączeń 10GbE o długości do 15 metrów oraz stosowanie światłowodu na większych odległościach.

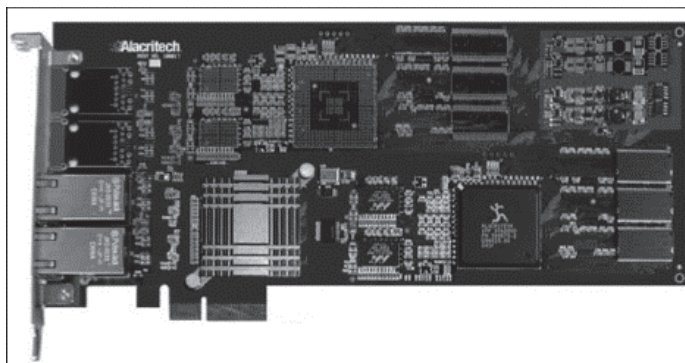
## Przetwarzanie stosu TCP bez użycia procesora

*Technologia TOE* (ang. *TCP Offload Engine*) to specjalny rodzaj interfejsu sieciowego, zawierającego dedykowany stos TCP/IP oraz własny układ ASIC, przeznaczony i zoptymalizowany do przetwarzania sieciowych operacji wejścia-wyjścia. Istniejące obecnie rozwiązania TOE koncentrują się na kartach interfejsu sieciowego 10 Gigabit Ethernet, gdyż ta technologia jest najpopularniejsza.

Już w roku 1990 firma Auspex opracowała technologię TOE, która była znana pod nazwą *Functional Multiprocessing* (FMP). Firma Alacritech założona przez Larry'ego Bouchera oraz innych inżynierów Auspex była pierwszą firmą oferującą karty TOE w 2001 roku. Na rysunku 16.1 pokazano aktualnie oferowaną przez Alacritech kartę TOE SEN2102ET 10 GbE. Technologia Chimney Offload firmy Microsoft (wcześniej Partial TCP Offload Architecture) powstała na bazie technologii Alacritech, jak również TCP Chimney Offload firmy Broadcom.

**Rysunek 16.1.**

Karta TOE 10 GbE  
Alacritech PCI-e 1 X.  
Układ ASIC to duży,  
czarny układ z symbolem  
biegnącego człowieka,  
znajdujący się w prawym  
dolnym rogu karty.  
Zdjęcie przedstawiające  
kartę pochodzi z firmy  
Alacritech, Inc.



Technologia TOE jest implementowana na następujące sposoby:

- ♦ **iSCSI HBA.** Te urządzenia TOE HBA to kontrolery dysków po stronie komputera oraz inicjatory iSCSI po stronie sieci. Rozwiązanie to stanowi kompletną technologię TOE.
- ♦ **TCP Chimney Offload.** Technologia TCP Chimney Offload w postaci zaimplementowanej przez firmy Microsoft i Broadcom to tylko częściowy system konwersji TCP bez użycia procesora. System TOE w technologii Chimney zajmuje się przetwarzaniem TCP, ale pozostawia procesorowi kontrolę nad połączeniem między punktami końcowymi TCP. Takie podejście oddala większość zarzutów formułowanych pod adresem technologii TOE. Jej krytycy twierdzili, że z tego powodu system stawał się mniej bezpieczny, ponieważ nie wiedział o połączeniu oraz istniało potencjalne niebezpieczeństwo manipulowania połączeniem na zewnątrz.
- ♦ **Parallel Stack Offload.** W technologii Parallel Stack Offload cały stos TCP/IP jest powielony. Takie podejście nosi nazwę *Full Offload*. Jeden stos działa w procesorze CPU komputera, natomiast drugi w układzie TOE. Drugi stos TCP jest nazywany *vampire trap* — przechwytuje i przekierowuje do głównego stosu TCP ruch TCP generowany przez aplikacje.



Szczegółowe omówienie TCP znajduje się w rozdziale 17.

TCP to warstwa transportowa (OSI Level 3) protokołu IP (Internet Protocol). Zadania warstwy TCP są następujące:

- ♦ tworzenie i usuwanie punktów końcowych połączenia IP;
- ♦ dostarczanie protokołu wymiany informacji;
- ♦ tworzenie sekwencji pakietów;
- ♦ dostarczanie mechanizmu sprawdzania, czy wystąpiły błędy;
- ♦ dostarczanie mechanizmów sterowania przepływem;
- ♦ potwierdzanie otrzymania pakietów.

Swoje zadania TCP wykonuje przez dodanie nagłówka do danych i utworzenie pakietu. Do takiego pakietu protokół IP dodaje adresowanie, które definiuje system źródłowy oraz adres, potrzebny, aby pakiet dotarł do punktu końcowego połączenia. W celu obsługi pakietów TCP wymaga wykonania dużej ilości operacji. W sieciach GbE systemy przeprowadzające ogromną ilość sieciowych operacji wejścia-wyjścia stają się ograniczone pod względem procesorów. Tego rodzaju systemy obejmują serwery WWW, serwery terminali, serwery plików, serwery kopii zapasowej itp.



Proces dodawania nagłówka nosi nazwę enkapsulacji, natomiast usuwanie nagłówka to dekapulacja. W dziedzinie sieci pojęcia używane do określenia nawiązywania i zrywania połączenia logicznego przez kanał wirtualny to odpowiednio „ustanawianie” i „zrywanie”.

Jeżeli sprawdzić ilość czasu zużytego na wysyłanie danych przez jedną aplikację sieciową do innej w sieci pozbawionej technik redukujących obciążenie, okaże się, że ilość czasu przeznaczona na przetwarzanie transferu danych niemal dziesięciokrotnie przekracza ilość czasu potrzebną na przesył tych danych. Zasoby procesora są więc odrywane od faktycznych operacji, które ma przeprowadzać dany system. Po zastosowaniu technik redukujących obciążenie, takich jak TOE, poziom wykorzystania procesora jednordzeniowego spada z 85 – 95% do zaledwie 10 – 15%. Technologia TOE staje się szczególnie wartościowa w aplikacjach multimedialnych przesyłających dane strumieniowo.

Technologia TOE łączy funkcję przetwarzania z pełni funkcjonalnym stosem TCP. Subsystem TOE odczytuje i zapisuje nagłówki pakietów IP, wysyła i odczytuje dane TCP oraz przeprowadza ustanowienie i zerwanie połączenia bez wykorzystywania procesora (procesorów) CPU komputera. TOE stosuje również pewne formy DMA (ang. *Direct Memory Access*) w celu odczytu i zapisu bufora pamięci bez wykorzystania procesora. Co więcej, w komputerze z aktywną technologią TOE aplikacja generująca żądanie do ruchu sieciowego TCP wymaga procesora jedynie w celu wysłania żądania transferu danych do systemu TOE, a system TOE zajmuje się całą resztą.

Z technologią TOE wiąże się jeszcze jedna bardzo ważna zaleta dotycząca wydajności. Ponieważ TOE znajduje się na karcie sieciowej PCIe, większość obciążenia związanego z przetwarzaniem i transferem danych nie przechodzi przez szynę interfejsu PCI. Szyna PCI nie jest w stanie obsłużyć ogromnej ilości małych komunikatów tak sprawnie, jak obsługuje ogromną ilość danych zawartych w małej liczbie komunikatów. Dzięki pozbyciu się ruchu komunikatów z szyny PCI opóźnienie w ruchu sieciowym wprowadzane przez PCI może być znacznie ograniczone.

Podczas gdy w obecnej technologii sieci komputerowych system TOE zapewnia istotne korzyści związane z wydajnością, z powodu braku równowagi pomiędzy dużymi i małymi możliwościami w zakresie przetwarzania technologia TOE wiąże się z pewnymi wadami. Prawdopodobnie przedmiot największej krytyki został już wymieniony — bezpieczeństwo. TOE przejmuje od systemu operacyjnego odpowiedzialność za podstawowe funkcje sieciowe. Dlatego też w przypadku zagrożeń sieciowych, w kwestii ochrony podsystemu sieciowego, trzeba zdać się na dostawcę technologii TOE. Ponieważ TOE nie dostarcza komputerowi macierzystemu informacji o połączeniu, ma to wpływ na możliwości systemu w zakresie zarządzania cechami charakterystycznymi sesji, na przykład filtrowaniem pakietów i parametrami QoS (ang. *Quality of Service*).

Karty TOE są drogie i nie są jeszcze powszechnie wykorzystywanymi produktami. Tak więc są przeznaczone do zastosowań w serwerach oraz bywają dostępne w postaci układów na niektórych serwerowych płytach głównych firmy Intel. Istnieje duże prawdopodobieństwo, że w nadchodzących latach ta technologia stanie się tańsza i wszechobecna, ale w chwili obecnej systemy TOE są sprzedawane przez niewielkich producentów jako systemy własnościowe.

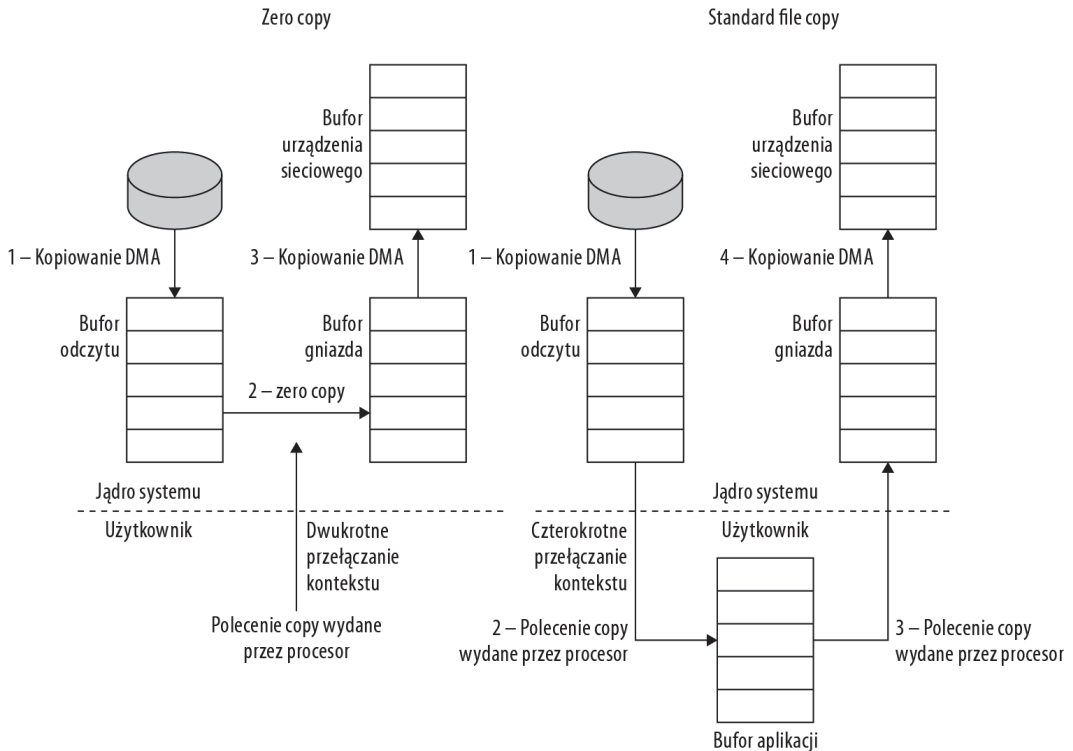
Ponieważ architektura VIA (ang. *Virtual Interface Architecture*) wykorzystuje TOE, w dalszej części rozdziału powrócimy do tematu TOE, w podrozdziale poświęconym VIA.

## Sieci Zero Copy Network

Sieci typu Zero Copy Networks używają technologii redukcji obciążenia procesora w celu przekazywania informacji w specjalnie dedykowanej pamięci z jednego komputera do drugiego. W ten sposób zasoby procesora mogą być wykorzystywane do wykonywania innych operacji obliczeniowych, co powoduje, że komputer jest używany nieco wydajniej. Sieciowe operacje wejścia-wyjścia także zostają usprawnione, ponieważ aplikacje poziomu klienta mogą poinstruować jądro systemu, aby dane były przekazywane bezpośrednio, bez ich odsyłania z powrotem do aplikacji. Dane są pobierane za pomocą pewnej formy DMA, bez konieczności interwencji ze strony jądra systemu poza wysłaniem samego polecenia. Opóźnienie wprowadzane przez przełączanie kontekstu jądro systemu/poziom użytkownika, które jest wymagane podczas przechodzenia między różnymi stanami procesora w trakcie przekazywania danych, zostaje więc wyeliminowane.

W celu włączenia systemu zero copy komputer musi być wyposażony w inteligentne karty wraz z własnymi stosami protokołu sieciowego. Układy ASIC na kartach pozwalają na kontrolowanie karty za pomocą specjalnych sterowników urządzeń, używanie rozszerzeń systemu plików, a także używanie metod DMA. Dzięki tym ostatnim jednostka MMU (ang. *Memory Management Unit*) kopiuje i mapuje dane z pamięci do karty sieciowej podczas przysyłania ich przez sieć. Większość producentów sprzedających systemy sieciowe tego rodzaju dostarcza zarówno sprzęt, jak i oprogramowanie. Jednak w sieciowych systemach operacyjnych operacje typu zero copy zyskują coraz większą popularność. API Linuksa `sendfile` i `sendfile64` obsługują zero copy, podobnie jak biblioteki klas Javy w systemach Unix i Linux dzięki metodzie `transferTo()`, dostępnej w `java.nio.channels.FileChannel`.

Na rysunku 16.2 pokazano schemat transferu plików za pomocą operacji zarówno zero copy, jak i standardowej operacji kopiowania. W operacji kopiowania typu zero copy następuje dwukrotne przełączenie kontekstu, natomiast w standardowej operacji kopiowania czterokrotne. W rozwiązaniu zero copy dane są odczytywane z dysku, a ich przeniesienie z bufora odczytu do bufora gniazda, gdzie mogą być odczytane przez kartę sieciową, wymaga pojedynczego polecenia na poziomie użytkownika. W standardowej procedurze kopiowania pliku dane są odczytywane z bufora odczytu, a następnie kopiowane do bufora gniazda za pomocą dwóch poleceń na poziomie użytkownika. Za każdym razem, gdy następuje wydanie polecenia na poziomie użytkownika, mamy do czynienia z przełączaniem kontekstu, które dwukrotnie zmienia stan procesora. Przełączanie kontekstu przerywa kolejną przetwarzania i powoduje dodanie znacznego obciążenia do każdej operacji. Z tego powodu operacja typu zero copy jest wydajniejsza i nie narzuca dodatkowego obciążenia.



**Rysunek 16.2.** Kopiowanie plików za pomocą operacji zero copy oraz standardowego kopiowania

Technologia RDMA (ang. *Remote Direct Memory Access*) w tych systemach pozwala, aby dane aplikacji były wysyłane do pamięci komputera docelowego bez użycia systemu operacyjnego komputerów zaangażowanych w tę operację. RDMA wymaga specjalnego zaprogramowania sposobu dostępu do pamięci oraz wypełnienia pamięci danymi, które mają być przekazane.

Technologia zero copy pokazuje pełnię swoich możliwości w rozproszonych systemach przetwarzania równoległego, w których szybkość sieci pozostawiła daleko w tyle możliwości komputera w zakresie przetwarzania danych wyjściowych.

## Virtual Interface Architecture

*Virtual Interface Architecture* (VIA) to standard sieciowego klastra wysokiej szybkości, który został utworzony w końcu 1997 roku przez konsorcjum zrzeszające firmy między innymi Intel, Microsoft i Compaq (obecnie część HP). Klastry komputerów stały się popularnym zamiennikiem dla komputerów typu mainframe i superkomputerów, a VIA pozwala na ich znacznie efektywniejsze skalowanie. Celem utworzenia VIA było opracowanie otwartego, wymiennego standardu, który mógłby zastąpić stosowane dotąd własnościowe rozwiązania w zakresie klastrów sieciowych.

Architektura VIA jest stosowana w następujących rozwiązaniach:

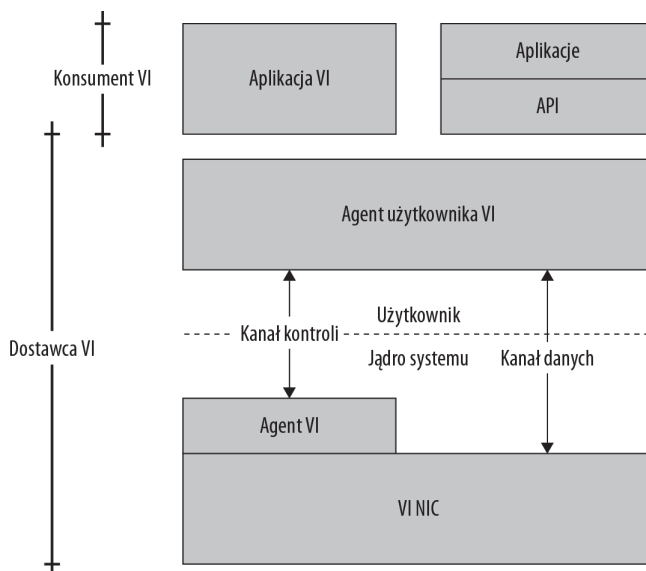
- ♦ **InfiniBand.** Architektura sieciowa typu switched fabric.
- ♦ **Internet Wide Area RDMA Protocol (iWARP).** Rozszerzona wersja VIA dla sieci IP.
- ♦ **Emulex (poprzednio GigaLAN) cLAN.**

Wąskim gardłem w sieciach komputerowych o wysokiej wydajności jest opóźnienie powstałe na skutek ogromnego stopnia wykorzystania procesora, co wiąże się z koniecznością obsługi całego ruchu wejścia-wyjścia między systemami. W klastrach sieciowych o wysokiej wydajności, bez żadnej formy redukcji obciążenia procesora, sieci zużywają tak duże zasoby procesora, że powoduje to dramatyczny spadek wydajności systemu.

Na rysunku 16.3 pokazano schemat wirtualnego interfejsu sieciowego, utworzonego przez VIA. Architektura VI może być opisana przez konsumenta usługi VI, którym jest funkcja warstwy aplikacji współdziałająca z dostawcą tej usługi. Dostawca ten zawiera agenta użytkownika wykorzystującego własne funkcje na poziomie jądra systemu. Polecenia wysyłane z aplikacji do dostawcy VI są obsługiwane przez agenta VI, podczas gdy dane są bezpośrednio przekazywane z aplikacji VI do wirtualnego urządzenia NIC w celu ich przetworzenia. Dwóch wymienionych agentów wykonują zadania w sposób podobny do zarządzania kolejką i ustalania priorytetów. Zadania intensywnie wykorzystujące procesor, na przykład adresowanie i tworzenie pakietów, są wykonywane na poziomie VI NIC. Warto zwrócić uwagę, że kanał danych prowadzi bezpośrednio z poziomu użytkownika do VI NIC bez konieczności przetwarzania danych przez funkcje na poziomie jądra systemu.

**Rysunek 16.3.**

*Komponenty systemu VIA*



Kopiowanie danych i transfer plików podąża za tym, co nazwano regułą 80/80:

- ♦ 80% operacji kopiowania powoduje kopiowanie danych o wielkości 256 bajtów lub mniej, służących do celów kontrolnych i synchronizacji;
- ♦ 80% żądanych danych znajduje się w danych o wielkości 8K bądź więcej.

Wymienione czynniki powodują wprowadzenie ogromnego obciążenia podczas operacji kopiowania i sieciowego transferu plików. Tego rodzaju problemy są rozwiązywane przez architekturę VIA.



Sieci VIA są nazywane *System Area Network* (SAN); sposób ich użycia poprzedza sieci *Storage Area Network* (skrót to również SAN). W celu uniknięcia pomyłek w tej książce podczas omawiania technologii VIA będzie stosowane pojęcie sieci VIA. Ponadto VIA to także nazwa tajwańskiego producenta układów scalonych, używających energooszczędnych procesorów X86, stosowanych w wielu laptopach.

VIA to protokół sieciowy typu zero copy, który omija tryb jądra systemu i przeprowadza wirtualizację interfejsu sieciowego. Aplikacje poziomu użytkownika mogą kontrolować i używać interfejsu sieciowego bez wykorzystywania procesora, a tym samym znacznie obniżać obciążenie procesora. Interfejs wirtualny jest nazywany *dostawcą*, natomiast aplikacja uzyskująca dostęp do interfejsu nosi nazwę *konsumenta*. Ścieżka kontrolna jest używana w celu nawiązania i przerywania połączenia. Ścieżka danych wysyła i otrzymuje komunikaty *Send/Receive* i *Remote DMA READ/WRITE*. Dostęp VIA jest zapewniany przez użycie VIPL (ang. *Virtual Interface Provider Library*).

Protokół *Internet Wide Area RDMA Protocol* (iWARP) to standard IETF, który jest kolejnym superzbiorem VIA, tym używanym w sieciach TCP/IP. Kontroler interfejsu sieciowego dla iWARP to technologia TOE na bazie Ethernetu, używająca protokołu DDP (ang. *Direct Data Protocol*) w celu inicjalizacji operacji typu zero copy. TCP to protokół transportowy używany przez iWARP. iWARP używa interfejsu posiłkowego (takiego jak InfiniBand). Inne protokoły, które mogą używać iWARP, zostały zdefiniowane przez zespół OpenFabrics Alliance for Linux oraz Winsock Direct firmy Microsoft.

## InfiniBand

Architektura Infiniband wywodzi się z inicjatywy przemysłowej, zawiązanej przez kilka grup przemysłowych, której celem było utworzenie następnej generacji zamiennika dla szyny PCI. Stowarzyszenie The InfiniBand Trade Association (<http://www.infinibandta.org>) powstało w 1999 roku i miało za zadanie utworzenie nowego, zapewniającego wysoką wydajność urządzenia dla serwerów oraz szyny dla sieci switched fabrics. Początkowo opracowane technologie nosiły nazwy Next Generation I/O (NGIO) oraz Future I/O (FIO), które następnie zostały połączone w jedną o nazwie System I/O. W wyniku tego powstała architektura InfiniBand.

Architektura InfiniBand to nadzbiór VIA, implementujący połączenia między systemami komputerowymi, systemami pamięci o wysokiej wydajności oraz innymi urządzeniami. Standard InfiniBand został zdefiniowany w taki sposób, aby umożliwić zwiększenie jego szybkości działania. W momencie wydania dostępne były trzy szybkości działania: 1X (od 2 do 8 Gb/s), 4X (od 8 do 32 Gb/s) oraz 12X (24Gb/s), wraz z zakresami zdefiniowanymi przez użycie pojedynczej, podwójnej i poczwórnej szybkości przesyłania danych w pamięci (odpowiednio SDR, DDR i QDR).

InfiniBand nie implementuje API, które mogłoby być programowane przez producentów. Zamiast tego standard definiuje zestaw operacji i działań, które muszą być zaimplementowane. Następnie producent urządzenia używa wybranego języka programowania w celu utworzenia systemu kontroli i wysyłania danych.

Połączenie InfiniBand to dwukierunkowe łącze posiadające dziesięciobitowy kanał, w którym osiem bitów jest przeznaczonych dla danych, natomiast dwa dla dedykowanych sygnałów kontrolnych. Większe szybkości to łącza zagregowane jako wielokrotność (4 i 12) pojedynczych łączy. Łącze jest definiowane jako połączenie między urządzeniami kanału, które w architekturze InfiniBand odgrywają taką samą rolę jak urządzenia NIC w sieci Ethernet. Urządzenia HCA (ang. *Host Channel Adapter*) i TCA (ang. *Target Channel Adapter*) po stronie komputera i urządzenia dodatkowego negocjują protokoły bezpieczeństwa, a także definiują parametry QoS dla połączenia. Producenci dostarczający urządzenia Channel to między innymi Cisco, Mellanox i QLogic. Przełączniki InfiniBand są produkowane przez Cisco, HP, Mellanox, QLogic i Voltaire.

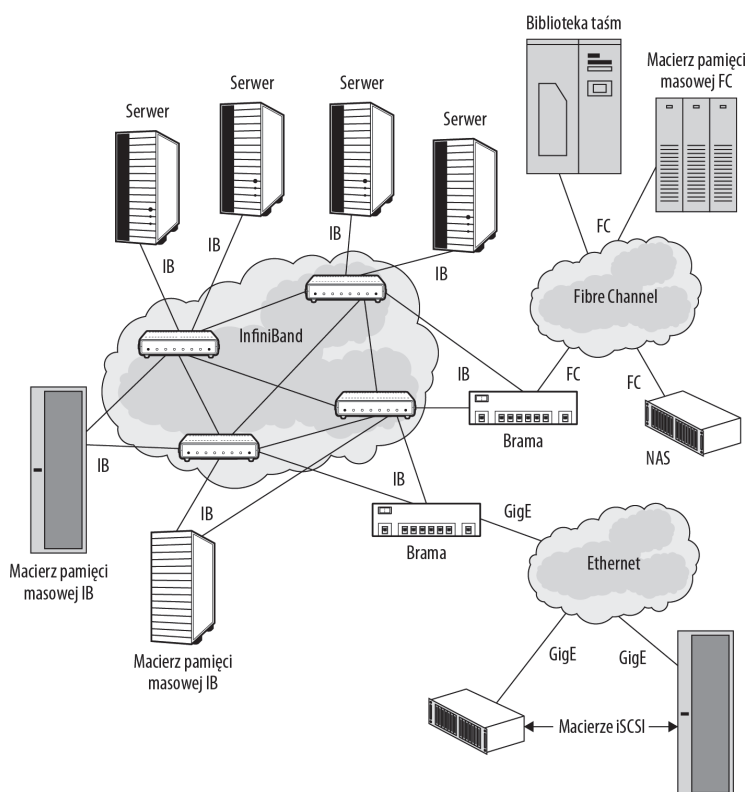
Architektura InfiniBand stała się często wybieranym sposobem łączenia klastrów systemów komputerowych o wysokiej wydajności.

Jednak architektura InfiniBand bardzo wolno przyjmuje się w przemyśle. Pewne opory w jej przyjęciu wiążą się z oczekiwaniem na standardy Ethernetu o wysokiej wydajności, które są obecnie opracowywane. Fibre Channel również jest trudny do wyparcia w sieciach pamięci masowej switched fabric. Producenci pracują nad technologią *Fibre Channel over InfiniBand* (FCoIB) i mają nadzieję, że architektura InfiniBand stanie się popularniejsza na rynku Storage Area Network.

Na rysunku 16.4 pokazano hipotetyczne rozwiązanie InfiniBand WAN z naciskiem na połączenia z urządzeniami pamięci masowej.

#### Rysunek 16.4.

*InfiniBand może funkcjonować jako wysokiej wydajności i wysoce redundancyjny komponent WAN*



## Klasy sieciowe

Klasy komputerowe to obszar, na którym standardy szybkich sieci odgrywają ważną, o ile nie decydującą rolę. Klaster może być utworzony za pomocą dwóch komputerów współdzielących tę samą szynę dla urządzeń peryferyjnych. Jednak gdy wiele komputerów jest połączonych ze sobą i są rozdzielone na zespoły serwerów lub rozproszone w architekturę przetwarzania sieciowego, szyny urządzeń peryferyjnych są zastępowane przez sieci. W kolejnych podrozdziałach zostaną przedstawione dwa rodzaje odmiennych klastrów sieciowych. Jedne mają potężne możliwości i wymagają szybkich połączeń, natomiast drugie mają równie potężne możliwości, ale działają na dużej liczbie komputerów i używają standardowej sieci.

Klasy sieciowe są tworzone w następujących celach:

- ♦ **Odporność na uszkodzenia.** Aplikacje o znaczeniu krytycznym nie mogą przestać funkcjonować lub przerwa w działaniu musi być bliska zeru. W tabeli 16.2 wymieniono różne poziomy odporności na uszkodzenia.

**Tabela 16.2.** Wymagania na polu odporności na uszkodzenia

Procentowy czas działania	Okres przestoju w ciągu roku	Platforma	Implementacja
90 (jedna dziewiątka)	36 dni, 12 godzin i 36 minut	Standardowy komputer PC/serwer	Nie jest wymagana odporność na uszkodzenia
99 (dwie dziewiątki)	87 godzin i 46 minut	Serwer ministerialny	Przywrócenie z obrazu
99,9 (trzy dziewiątki)	8 godzin i 46 minut	Wysoka dostępność	Podczas przerwy przekierowanie na serwer lustrzany bądź zapasowy
99,95	4 godziny i 23 minuty	Wysoka dostępność	Podczas przerwy przekierowanie na serwer lustrzany bądź zapasowy
99,99 (cztery dziewiątki)	52 minuty i 33 sekundy	Aplikacje o znaczeniu krytycznym	Uszkodzony klaster powoduje przekierowanie do innego węzła
99,999 (pięć dziewiątek)	5 minut i 35 sekund	Odporność na uszkodzenia	Cały komputer jest powielony w celu szybkiego przełączenia w przypadku awarii
99,9999 (sześć dziewiątek)	31 i pół sekundy	Praca ciągła	Systemy Stratus FT i kilka innych

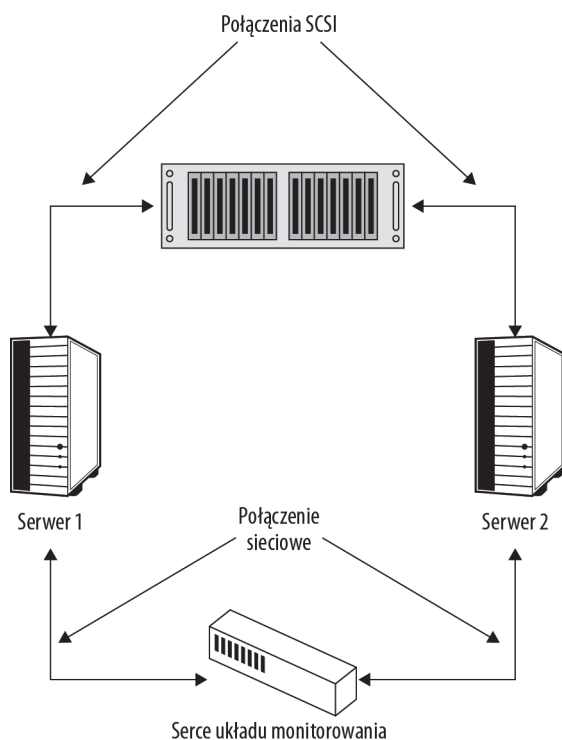
- ♦ **Poziom wykorzystania.** Zespoły serwerów działają w taki sposób, że zawierają system przeprowadzający rozkład obciążenia, który kładzie nacisk na poziom wykorzystania komputerów.
- ♦ **Wszechobecne narzędzia.** Rozproszone przeprowadzanie obliczeń, których pożądanym wynikiem jest utworzenie komputera narzędziowego, mogącego obsługiwać aplikacje przeprowadzające obliczenia.

Odporność na uszkodzenia w klastrach jest tworzona przez implementację systemu pozwalającego na pracę mimo awarii. Ten system może być prosty i obejmować układ, który nieustannie monitoruje i sprawdza, czy węzeł klastra nadal działa. Tego rodzaju układ wysyła w stałych odstępach czasu wiadomości sprawdzające, czy system działa. Układ czeka ustaloną ilość czasu, zanim ponowi komunikat lub uruchomi system zapasowy w klastrze.

Najwcześniejsze klastry firmy Microsoft składały się z dwóch węzłów wraz ze współdzielonym rozwiązaniem pamięci masowej, jak pokazano na rysunku 16.5. Dwa komputery pozostawały w związku „komputer nadrzędny-podległy”. Jeżeli jeden z nich uległ awarii, to w ciągu kilku sekund klaster przekazywał zadania do drugiego. Współdzielona pamięć masowa była rozwiązaniem w postaci macierzy RAID, która sporadycznie ulegała awarii. Ten rodzaj klastrów był system typu „współdziel coś”, „współdziel wszystko” bądź „nie współdziel niczego”. Aktualnie niemal wszyscy producenci sprzętu serwerowego i sieciowych systemów operacyjnych dostarczają rozwiązania bazujące na klastrach.

### Rysunek 16.5.

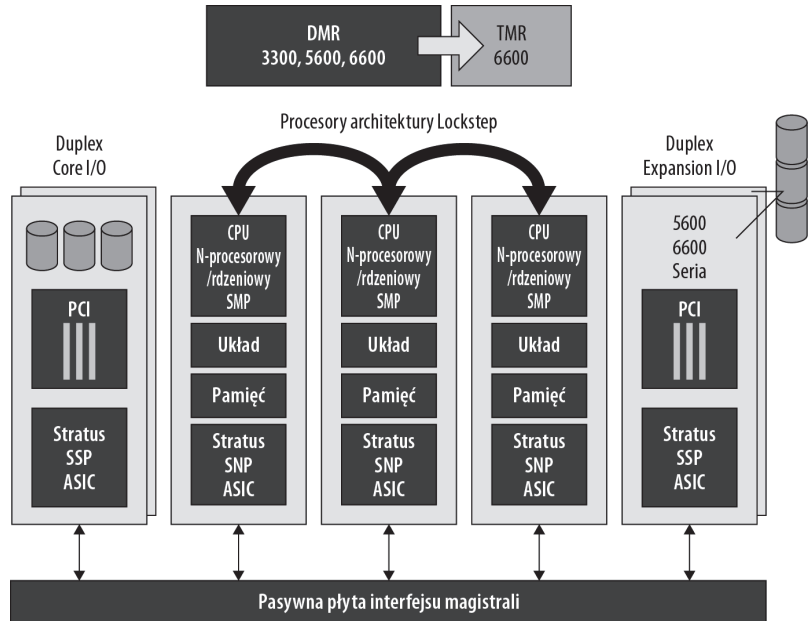
*Prosty klaster składający się z dwóch węzłów, zapewniający możliwość pracy pomimo wystąpienia awarii*



Klastry działające mimo awarii i komputery odporne na uszkodzenia mogą być skomplikowanymi rozwiązaniami, składającymi się z wielu redundancyjnych systemów komputerowych, które nieustannie uaktualniają wszystkie węzły. Przykładem systemu typu „współdziel wszystko” jest seria Stratus FT, stosowana w aplikacjach o znaczeniu krytycznym, gdzie awarie nie są tolerowane. Architektura ich systemu Lockstep wraz z pełnym systemem redundancyjnym została pokazana na rysunku 16.6. Ten system ma niezawodność *sześciu dziesiątek* (99,9999 procent), a czas przestoju jest nie większy niż 31 i pół sekundy rocznie.

**Rysunek 16.6.**

Architektura Stratus Lockstep ma wiele systemów redundancyjnych, które są nieustannie uaktualniane



Na rysunku 16.6 można zobaczyć, że dane są zapisywane jednocześnie do trzech oddzielnych, symetrycznych wieloprocessorowych systemów (SMP), zawierających N procesorów (wątków). W architekturze Stratus systemy zawierają własnościowe układy ASIC (ang. *Application Specific Integrated Circuits*): Stratus North PCI (SNP) i Stratus South PCI (SSP), które obsługują transakcyjną spójność podczas przetwarzania danych. Układy SNP i SSP mają możliwość jednoczesnej komunikacji z pasywną płytą interfejsu magistrali, która jest interfejsem wejścia-wyjścia, komunikującym się z urządzeniami peryferyjnymi lub z innymi systemami za pomocą sieci.

Sieciowe klastry komputerów znajdują się wśród komputerów o najwyższej wydajności. Dla przykładu 7. na liście Top500.org (tabela 16.1) monolityczny komputer Roadrunner, znajdujący się w laboratorium Los Alamos Laboratory (Nowy Meksyk), zbudowany jest przez IBM na podstawie klastrów BladeCenter QS22 połączonych siecią Voltaire InfiniBand. W czerwcu 2008 roku Roadrunner został ogłoszony pierwszym komputerem, którego wydajność jest wyrażana w PFLOPS (P = peta) na sekundę.

FLOPS to skrót od *Float Point Operations Per Second* — liczba operacji zmiennoprzecinkowych na sekundę, mierzona za pomocą aplikacji takich jak LINPACK. Kalkulator kieszonkowy działa z szybkością około 10 FLOPS, procesor Intel Quad-core QX9775 z szybkością 51 GFLOPS. Dla porównania PFLOPS to 1015 TFLOPS (T — tera) i milion GFLOPS. Systemy komputerowe o największej wydajności wyrażanej w FLOPS to rozproszona sieć obliczeniowa Folding@Home, która osiągnęła wydajność 5.5 PFLOPS.

## Równoważenie obciążenia

Zespoły serwerów stosują pewną formę klastrów, nazywaną *równoważeniem obciążenia*. Równoważenie obciążenia jest użyteczne, kiedy system jest ograniczony pod kątem operacji wejścia-wyjścia i gdy zachodzi potrzeba skalowania serwerów typu out (więcej serwerów)

zamiast typu up (więcej serwerów o potężnych możliwościach). Serwery mogą być dodawane i usuwane na żądanie. Klastrowanie wraz z równoważeniem obciążenia nie ma żadnych dodatkowych wymagań dotyczących szybkości sieci dla połączeń przychodzących i wychodzących ani też nie wymaga, aby obciążenie było rozkładane równo.

W takim systemie serwer, router lub główny przełącznik sieciowy wraz z oprogramowaniem pośrednim kieruje ruchem sieciowym IP w taki sposób, aby zadania były rozkładane na grupę serwerów. Jeżeli serwer przejdzie do trybu offline, to zostaje usunięty z puli dostępnych serwerów, a zadania będą przekazywane do innych komputerów. Takie rozwiązania bardzo często wykorzystują buforowanie w celu buforowania przychodzącego ruchu sieciowego w godzinach szczytu.

Systemy równoważenia obciążenia mogą mieć architekturę następujących typów:

- ♦ **Szeregowanie cykliczne.** Tabela kolejno używanych adresów IP.
- ♦ **Równoważenie obciążenia w mostku.** To rozwiązanie jest przeprowadzane w urządzeniach warstwy drugiej za pomocą wirtualnych adresów IP w sieci LAN. Ruch do sieci LAN jest wysyłany do adresu wirtualnego, a następnie przekazywany do serwerów, które mogą przetworzyć żądanie.

**Równoważenie obciążenia w routerze.** Ta forma równoważenia obciążenia dodaje inteligencję do sposobu, w jaki obciążane są serwery. Zwykle opiera się na wykorzystaniu urządzeń warstwy trzeciej, które działają jako zapory sieciowe lub serwery proxy obejmujące dwie podsieci.

Przykłady rozwiązań sprzętowych do równoważenia obciążenia w routerze to:

- ♦ BIG-IP firmy F5 (<http://www.f5.com>);
- ♦ Citrix NetScaler MX (<http://www.citrix.com/english/ps2/products/product.asp?contentID=21679>);
- ♦ Coyote Point Systems Equalizer (<http://www.coyotepoint.com>).

Przykładami równoważenia obciążenia przeprowadzanego przez oprogramowanie mogą być moduły równoważenia obciążenia wbudowane w systemach Windows Server 2003 i 2008. Niemal każdy sieciowy system operacyjny wspomniany w tym rozdziale jest dostarczany z modułami równoważenia obciążenia. Przykładami oprogramowania równoważającego obciążenie są:

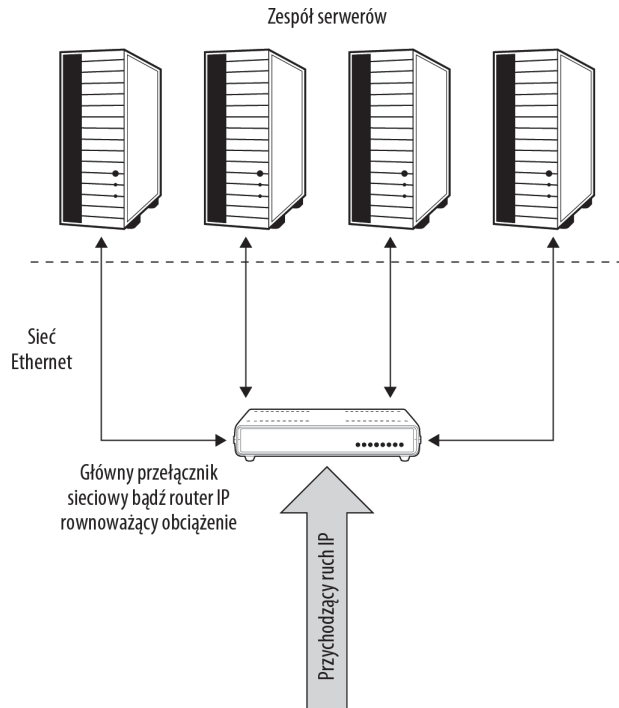
- ♦ Balance (<http://www.inlab.de/balance.html>);
- ♦ Queue (<http://www.gnu.org/software/gnu-queue/>);
- ♦ Linux Virtual Server (<http://www.linuxvirtualserver.org>).

Każda usługa sieciowa nadaje się do równoważenia obciążenia. To obejmuje między innymi serwery DNS, DHCP, FTP, NNTP i inne. Serwery WWW są przykładem aplikacji używanych w programach zespołu serwerów ze zrównoważonym obciążeniem. Równoważenie obciążenia w sieciach IP działa na zasadzie nasłuchiwania portów pod kątem tego rodzaju ruchu sieciowego, który później ma być poddawany równoważeniu. Następnie

żądania są przekazywane do serwera. Ogólnie rzecz biorąc, działają jak inteligentne routery i pozostają niewidoczne dla przechodzącego przez nie ruchu sieciowego. Na rysunku 16.7 pokazano rozwiązanie równoważące obciążenie.

### Rysunek 16.7.

*Klasy, w których zrównoważono obciążenie, optymalizują poziom wykorzystania serwera przez rozłożenie zadań na zespół serwerów, wykorzystując do tego sieć*



Przetwarzanie z maksymalną wydajnością to forma rozproszonego równoważenia obciążenia, które jest przeprowadzane przez przekazywanie danych do geograficznie rozproszonych miejsc. Rozproszone serwery danych kierują dane do bliskich pod względem geograficznym serwerów w internecie. Bardzo często serwery te są skonfigurowane jako witryny lustrzane oryginalnych witryn. Firma Akamai (<http://www.akamai.com>) jest pionierem w tej kategorii usług sieciowych i oferuje klientom swoje serwery lustrzane, aby dostarczały odpowiednich danych użytkownikom. Serwery brzegowe zazwyczaj nie sprawdzają się dobrze podczas dostarczania zawartości dynamicznej, ponieważ koordynacja i replikacja stają się zbyt trudne. Producenci zwykle oferują usługi QoS i gwarancję wydajności. Usługi te są na tyle dojrzałe, że zapewnią efektywność firmie każdej wielkości. W zależności od producenta i jego topologii sieci systemy przetwarzania z maksymalną wydajnością mogą być również systemami przetwarzania sieciowego.

## Systemy przetwarzania sieciowego

Systemy przetwarzania sieciowego to rozproszone systemy połączonych siecią komputerów, pomiędzy które rozkładane jest obciążenie. W tego rodzaju przetwarzaniu siecią może być internet, połączenie może być wolne, a protokołami mogą być standardowe protokoły sieciowe. Systemy te są nazywane systemami *przetwarzania sieciowego*, ponieważ zostały zaprojektowane do funkcjonowania na zasadzie narzędzia i dostarczają mocy obliczeniowej

na żądanie. Są nazywane także *sieciami mesh*. W zależności od zaimplementowanego oprogramowania przetwarzanie sieciowe może wykorzystywać model klient-serwer, model n-warstwowy lub model „równy z równym”.

Przetwarzanie sieciowe ma następujące zalety:

- ♦ poprawia poziom wykorzystania sprzętu oraz zmniejsza potrzebę budowania i utrzymywania rzadko używanych zasobów dodatkowych;
- ♦ pozwala na utworzenie odpowiednika superkomputera za ułamek jego ceny;
- ♦ może służyć zainteresowanym społecznościom;
- ♦ może stanowić podstawę przeprowadzania obliczeń, gdzie usługi są zawsze i wszędzie dostępne.

Jeżeli w systemie będzie zgromadzona odpowiednia liczba komputerów, to nawet jeśli tylko część tych komputerów będzie pracować w danej chwili nad projektem, ich łączna moc będzie odpowiadać mocy dostępnych dzisiaj największych superkomputerów. Istotnie, wśród dzisiejszych systemów o największej wydajności kilka z nich to systemy przetwarzania sieciowego. Folding@Home to system o wydajności 5,5 PFLOPS, zorganizowany przez Uniwersytet w Stanford, który jest ponad dwukrotnie wydajniejszy niż najszybszy superkomputer, jaki został dotąd zbudowany. System ten jest wykorzystywany do analizowania struktur białek.

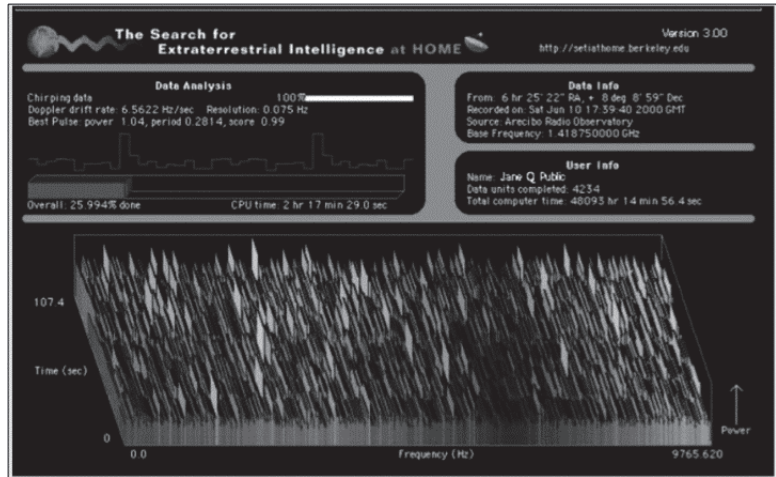
Nazywanie systemu przetwarzania sieciowego komputerem jest niewłaściwe. Tak naprawdę to systemy komputerów wirtualnych, a ich praca jest nadzorowana przez serwer bądź serwery, w zależności od liczby systemów składowych. Systemy przetwarzania sieciowego przeprowadziły wiele ważnych obliczeń w biochemii, ekonomii, astronomii oraz w wielu innych dziedzinach.

Wiele systemów przetwarzania sieciowego oferuje aplikacje klienckie na kilku platformach, a ich oprogramowanie działa tylko wtedy, gdy komputer klienta pozostaje bezczynny. Użycie cykli bezczynnego komputera określa się wyrażeniami *wygrzebywanie cykli*, *wygrzebywanie CPU* lub stosuje się inne, równie znaczne nazwy.

SETI@home to inna społeczność wolontariuszy udostępniających komputery laboratorium Space Sciences Laboratory na uniwersytecie w Berkeley. SETI to skrót od *Search for Extra Terrestrial Intelligence*, a systemy przetwarzania sieciowego pomagają w szukaniu małych, zielonych ludków w kosmosie. Oprogramowanie klienckie jest używane na 2,4 miliona komputerów (278 000 aktywnych klientów w 234 krajach) i działa jako wygaszacz ekranu (zob. rysunek 16.8). Agregujący dwa miliony lat czasu komputerowego SETI@home to według Księgi rekordów Guinnessa największy projekt obliczeniowy w historii. Projekt SETI utworzył BOINC (ang. *Berkeley Open Infrastructure for Network Computing*), czyli jeden z największych używanych systemów przetwarzania sieciowego zbudowanych przez wolontariuszy.

Systemy przetwarzania sieciowego są przedmiotem zainteresowania i wysiłków producentów, którzy przekształcają aplikacje biurowe na postać oprogramowania działającego „w chmurach”. Istnieje mała różnica między systemem „działania w chmurach” i przetwarzaniem sieciowym — oba pojęcia oznaczają zdaną usługę na żądanie. Narodowe systemy

**Rysunek 16.8.**  
Wygaszacz ekranu  
SETI@home



przetwarzania sieciowego są obecnie tworzone i jeszcze znajdują się na etapie prototypów. Unia Europejska sponсорuje systemy przetwarzania sieciowego budowane na potrzeby badań fizycznych, biologicznych oraz innych projektów naukowych. W USA budowany jest system A National Technology Grid, służący do testowania koncepcji publicznego narzędzia obliczeń na żądanie.

Obliczenia „w chmurach” są udostępniane przez wielu różnych producentów sieciowych systemów operacyjnych w ramach takich inicjatyw, jak SaaS (ang. *Software as a Service*), SOA (ang. *Service Oriented Architecture*), platforma .NET firmy Microsoft oraz aplikacje Web 2.0.

Firma Sun<sup>1</sup> oferuje oprogramowanie o nazwie SGE, czyli Sun Grid Engine (<http://www.oracle.com/us/products/tools/oracle-grid-engine-075549.html>), które jest systemem typu open source przetwarzania wsadowego, implementowanego w klastrach bądź zespołach serwerów. Implementacje tego rodzaju mają dużo wspólnego z rozwiązaniami równoważenia oprogramowania. Narzędziowy system komputerowy Sun Grid został zbudowany na bazie SGE. Sun oferuje także produkt komercyjny o nazwie Sun N1 Grid Engine (N1GE), który opisuje tę technologię jako *Distributed Resource Management* (DRM).

## Podsumowanie

W tym rozdziale przedstawiono sieciowe systemy komputerowe o dużej wydajności. Potężne systemy używają sieci o dużej szybkości, podczas gdy systemy rozproszone korzystają ze standardowych rodzajów sieci.

Ethernet jest używany powszechnie — jego nowy standard prawdopodobnie będzie równie popularny. Dostępny obecnie standard 10 GbE jest wykorzystywany w przełącznikach sieciowych i serwerach o wysokiej szybkości działania. Pojawiły się nowe standardy dla Ethernetu: 40 GbE i 100 GbE.

<sup>1</sup> Firma Sun obecnie należy do Oracle — *przyp. tłum.*

Aby rozwiązać problemy z obciążeniem procesora, opracowano wiele technik odciążania procesora od obsługi ruchu sieciowego. W rozdziale omówiono technologie TOE (ang. *TCP Offload Engine*) oraz sieci typu zero copy — architektury VIA (ang. *Virtual Interface Architecture*) i szynę urządzeń Infiniband.

Przedstawiono także klastry komputerów połączone w sieci. Używane są trzy rodzaje klastrów: rozwiązania zapewniające możliwość działania po wystąpieniu awarii, rozwiązania pozwalające na zrównoważenie obciążenia oraz rozwiązania umożliwiające obliczenia narzędziowe. Pokrótce wspomniano również o przetwarzaniu sieciowym oraz obliczeniach „w chmurach”.

Kolejny rozdział rozpoczyna się podrozdziałem dotyczącym sieci TCP/IP. Czytelnik pozna w nim protokół transportowy TCP.

# Część IV

# Sieci TCP/IP

## **W tej części:**

**Rozdział 17.** Internetowy protokół transportowy

**Rozdział 18.** Protokoły internetowe

**Rozdział 19.** Usługi określania nazw



# Rozdział 17.

# Internetowy protokół transportowy

## W tym rozdziale:

- ♦ W jaki sposób dane są transportowane przez internet?
- ♦ Czynniki wpływające na wydajność działania sieci IP
- ♦ Co się znajduje w pakiecie IP?
- ♦ W jaki sposób zarządza się przepływem danych?
- ♦ Połączenia i porty

*Transmission Control Protocol* (TCP) i *Internet Protocol* (IP) to dwa protokoły składające się na akronim TCP/IP. TCP/IP to zestaw protokołów, czyli uzgodnionych standardów, które są używane do wysyłania pakietów przez sieć i zarządzania komunikacją w sieci. TCP to technologia nawiązująca wirtualne połączenie między systemami, zarządzająca transmisją danych oraz gwarantująca, że dane zostaną niezawodnie dostarczone. Dane znajdujące się w pakiecie to dane TCP, natomiast mechanizm wykorzystywany w celu dostarczenia pakietów do miejsca ich przeznaczenia to IP. Sposób działania TCP wpływa na większość komunikacji internetowej, jak również na sposoby tworzenia aplikacji oraz na wydajność sieci. Protokół IP, który zostanie omówiony w rozdziale 18., jest metodą używaną do wysyłania pakietów przez routery. Zawiera metody przeznaczone nie tylko dla danych pakietów, ale również odpowiedzialne za adresowanie.

TCP rozwiązuje problem zapewnienia niezawodnej komunikacji, kiedy nośnik wykorzystywany do transmisji z natury jest zawodny. Pakiety mogą wybierać różne trasy prowadzące do miejsca docelowego, wypadać z sekwencji bądź zupełnie ginać po drodze. TCP gromadzi dane przez wysyłanie pakietów w kolejności, zapewnia poprawność wszystkich pakietów i żąda ponownego przesłania pakietu, jeśli zaginął bądź został uszkodzony w trakcie transmisji.

Urządzenia podłączone do sieci TCP/IP mogą mieć zupełnie odmienne możliwości. Przykładowo urządzenie PDA (ang. *Personal Data Assistant*) może być wolne, podczas gdy komputer może być szybki. TCP implementuje funkcje takie jak kontrola przepływu w celu zróżnicowania szybkości transmisji danych oraz zapewnia multipleksowanie, które jednocześnie uruchamia wiele procesów w celu zwiększenia wydajności. Może również wpływać na wielkość pakietów.

Nie cała komunikacja wymaga obciążenia związanego z niezawodną transmisją danych. W trakcie wysyłania szybko zmieniających się danych, na przykład dźwięku bądź obrazu wideo, zagubienie ramki nie ma istotnego wpływu na jakość. W przypadku tego rodzaju aplikacji stosowany jest protokół UDP (ang. *User Datagram Protocol*), omówiony w tym rozdziale i porównany z TCP.

## Transmission Control Protocol

Protokół TCP (ang. *Transmission Control Protocol*) to obecnie najczęściej używany protokół transportowy w sieciach komputerowych. TCP zapewnia mechanizm kontroli zarządzający danymi znajdującymi się w wiadomości. Gwarantuje więc wysyłanie danych w łatwych do zarządzania fragmentach, które będą dostarczone w niezmienionej postaci. Dane mogą być przesyłane w określonej kolejności; po ich złożeniu powstaje wierna kopia wysłanego materiału. Protokół TCP zawiera pewny zbiór poleceń kontrolnych, pozwalających na zróżnicowanie ilości danych transferowanych w poszczególnych pakietach, jak również na określanie szybkości, z jaką pakiety będą wysyłane. Wśród aplikacji polegających na protokole TCP mamy przeglądarki internetowe, serwery WWW, klientów poczty elektronicznej oraz programy pozwalające na transfer plików.

Protokół TCP został opracowany w celu rozwiązania problemu niezawodnej komunikacji za pomocą sieci, która z natury nie zapewnia niezawodności. Kiedy dane muszą być podzielone na pakiety IP i transmitowane jako zestaw żądań IP, istnieje potrzeba zastosowania mechanizmu nadzorującego przepływ tych danych. TCP pozwala, aby program wydał pojedyncze polecenie wysłania danych, następnie protokół TCP zajmuje się obsługą wszystkich szczegółów związanych z transferem danych.

Pakiet IP składa się z porcji danych zbudowanych z sekcji nagłówka, po której znajduje się sekcja główna. W nagłówku zakodowane są informacje szczegółowe, określające między innymi miejsce docelowe pakietu, wszelkie preferencje dotyczące trasy, którą pakiet powinien obrać, wielkość danych znajdujących się w sekcji głównej pakietu, sumę kontrolną, gwarantującą poprawność pakietu, oraz pozycję w sekwencji, gdzie powinny być umieszczone dane pakietu. Nagłówek i powiązaną z nim treść IP można potraktować jako metadane opisujące dane TCP zawarte w części głównej pakietu.

Internet został zaprojektowany jako wysoce redundancyjna struktura, która powinna przetrwać wszelkie utraty znaczących fragmentów sieci i nadal funkcjonować pomimo tych strat. Kiedy dane są wysyłane z jednego systemu do drugiego, nie ma gwarancji, że pakiety będą wysyłane tą samą trasą, przybędą w jakiejś uporządkowanej kolejności i że wszystkie zostaną dostarczone prawidłowo. Prawdę mówiąc, pakiety mogą korzystać z wielu różnych tras, podróżując do miejsca przeznaczenia, przybywać poza kolejnością, a nawet gubić się w trakcie transmisji.

Protokół TCP ma język kontroli, który tworzy połączenia między dwoma systemami, wysyła wiadomości wskazujące kolejny wymagany pakiet w sekwencji, żąda ponownej transmisji pakietu, kiedy jest to wymagane, i potwierdza złożenie w całość otrzymanych danych. Po stronie wysyłającego wewnętrzny licznik czasu ponownie wysyła ostatnio żądane dane, jeśli w określonym czasie nie nadeszło polecenie potwierdzające ich przyjęcie przez odbierającego. Wszystkie wysłane dodatkowo pakiety to oczywiście obciążenie dla systemu TCP i powód znacznego zmniejszenia jego wydajności.



Protokół TCP został zdefiniowany w dokumencie RFC 793 „Transmission Control Protocol”. Natomiast dokument RFC 768 „User Datagram Protocol” definiuje użycie protokołu UDP. Dodatkowy protokół, omówiony w dokumencie RFC 1122, zatytułowanym „Requirements for Internet Hosts — Communication Layers”, zawiera informacje szczegółowe, które szkicują funkcję transportową obu wymienionych protokołów.

Protokół TCP zaprojektowano w celu niezawodnego dostarczania danych, ale nie został on zoptymalizowany pod względem wydajności. Kiedy jest używany, bardzo często występują opóźnienia związane z ponownym wysyłaniem pakietów i mogą one wynosić nawet kilka sekund lub więcej. Czas, w jakim pakiet pokonuje trasę, można sprawdzić za pomocą polecenia `tracert` wydanego systemowi, który wysyła dane. `tracert` (tracert w systemie Windows) to polecenie wysyłające pakiety do systemu docelowego; pokazuje ono wszystkie węzły pośrednie oraz trasę pakietu i ilość czasu, którego potrzebuje on na podróż ze źródła do węzła.

TCP jest implementowany w każdym systemie operacyjnym, który musi działać w sieci TCP/IP. W obecnych czasach oznacza to niemal każdy system operacyjny, który można znaleźć w komputerach biurkowych, jak również wszystkie podłączone do sieci serwery. Routery, bramy oraz zapory sieciowe również implementują TCP, o czym świadczy ich możliwość odpowiadania na polecenia `ping` oraz zarządzanie wymienionymi urządzeniami (i inwentaryzowanie ich) przez aplikacje SNMP (ang. *Simple Network Management Protocols*). Ponadto, gdy konsola zarządzania urządzeniem może być wyświetlona w przeglądarce internetowej, urządzenie obsługuje również protokół HTTP.

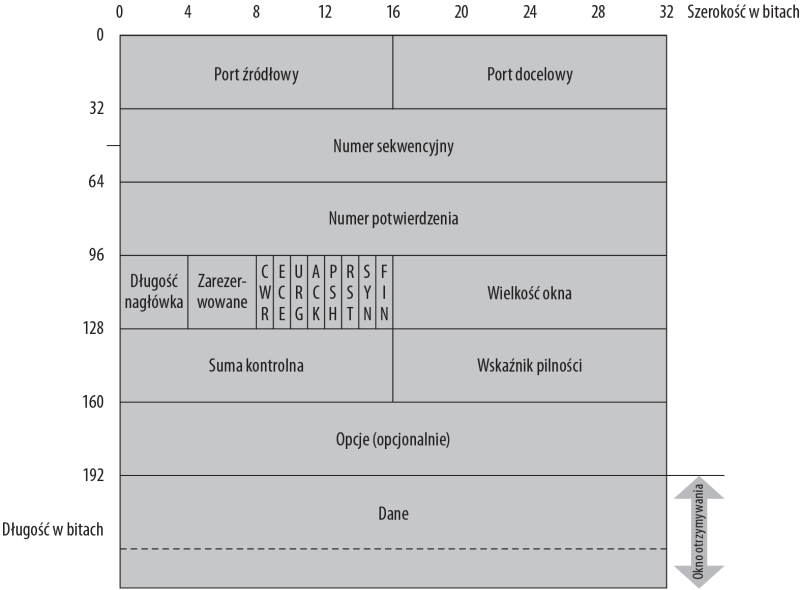
Protokół TCP w znacznym stopniu obciąża procesor. Dlatego też w systemach z dużą ilością wykonywanych operacji wejścia-wyjścia, na przykład serwerach WWW i terminalach, operacje te mogą być wąskim gardłem wydajności. W ostatnich latach podjęto wysiłek w celu opracowania specjalizowanych kart sieciowych zawierających układy ASIC wraz z wbudowanym w nie silnikiem TCP. Technologię TOE omówiono w rozdziale 16. tej książki.

Nie wszystkie operacje transmisji danych wymagają niezawodności. Niektóre aplikacje działają doskonale, jeśli otrzymują większą część danych. Tego rodzaju aplikacje funkcjonują najlepiej, kiedy szybkość transmisji danych jest wysoka. Przykładem może być strumieniowanie wideo. W aplikacji wideo utrata jednej ramki ma niewielkie znaczenie, gdyż w ciągu sekundy wyświetlanych jest 30 ramek lub więcej. Jednak gdy szybkość przekazywania danych jest wysoka, wówczas film można odtworzyć w większej rozdzielczości, co ma znaczenie dla oglądającego. Dlatego też aplikacje zajmujące się operacjami takimi jak strumieniowanie obrazu wideo lub *Voice over IP* (VoIP) z reguły używają specjalnych protokołów strumieniowania oraz protokołu UDP zamiast TCP. Protokół UDP zostanie omówiony w dalszej części rozdziału.

## Struktura pakietu

Pakiet TCP składa się z nagłówka z wieloma sekcjami oraz części głównej (dane TCP — *Okno otrzymywania*) o zmiennej wielkości, określanej przez wartość pola *Wielkość okna*. Na rysunku 17.1 pokazano schemat pakietu TCP. Wielkość okna to wartość negocjowana, która jest używana w celu niedopuszczenia do przepełnienia bufora pamięci TCP w systemie otrzymującym pakiety. System po prostu sygnalizuje wysyłającemu, kiedy wysyłać dane bądź opóźniać ich wysyłanie. Taka forma zarządzania ruchem zostanie szczegółowo omówiona w dalszej części rozdziału.

**Rysunek 17.1.**  
*Struktura pakietu TCP, w którym pokazano wszystkie nagłówki*



## Pola nagłówka

Pierwsze cztery pola w nagłówku to port źródłowy, port docelowy, numer sekwencyjny oraz numer potwierdzenia. Porty są podobne do kanałów telewizyjnych pod tym względem, że przedstawiają rodzaj wysyłanych bądź odbieranych danych. Port jest opisany jako transmitujący dane wychodzące lub oczekujący na dane przychodzące. Kiedy dane docierają do portu 8080, są rozpoznawane jako dane dla serwera proxy, takiego jak Microsoft Internet Security and Acceleration (ISA), a następnie układane w kolejności i wysyłane do aplikacji. Port 8080 to alternatywa dla HTTP. Jeżeli dane docierają do portu 110, to są rozpoznawane jako dane POP3 (ang. *Post Office Protocol 3*), a następnie układane w kolejności i wysyłane do programu pocztowego. Porty zostaną omówione w podrozdziale „Porty”, znajdującym się na końcu rozdziału.

*Numer sekwencyjny* i *Numer potwierdzenia* to pola używane do kontroli ruchu. Jeżeli flaga SYN (*Synchronize*) ma wartość 1 (włączona), to wartość pola *Numer sekwencyjny* jest początkowym (wyznaczanym losowo) numerem sekwencyjnym. Od tej wartości będą liczone bajty danych przekazywanych do odbiorcy. Kiedy flaga SYN ma wartość 0 (wyłączona), wartość pola *Numer sekwencyjny* określa początkowy bajt danych przekazywanych w tym segmencie w tej sesji TCP.

Jeśli flaga ACK (*Acknowledgement*) ma wartość 1 (włączona), wartość pola *Numer potwierdzenia* wskazuje numer bajta w sesji TCP, na jaki czeka system zdalny.

## Flagi

Pole 8-bitowe, rozpoczynające się od 104. bitu nagłówka, zawiera flagi, które są używane w celu określenia stanu innych pól oraz przeznaczenia danych. Wartość pola *Długość nagłówka* wskazuje, ile słów 32-bitowych ma nagłówek. Ze względu na opcjonalne pole

Opcje nagłówek TCP może mieć różną długość. Pole *Zarezerwowane* nie zostało zdefiniowane i powinno mieć wartość 0. Następnie mamy zestaw ośmiu jednobitowych pól nazwanych *Flagami* lub *Bitami kontrolnymi*. Przeznaczenie flag jest następujące:

- ♦ **CWR.** Flaga CWR (ang. *Congestion Window Reduced*) ma wartość 1 (włączona), kiedy system wysyłający otrzymuje dane TCP wraz z opcją ECE o wartości 1.
- ♦ **ECE.** Flaga Echo (ewentualnie ECN) ma ustawioną wartość 1 (włączona), kiedy system może wykonać operację echo w momencie nawiązywania połączenia (*three-way handshake*).
- ♦ **URG.** Flaga Urgent ma ustawioną wartość 1 (włączona) w momencie, kiedy segment zawiera informacje określone przez nadawcę jako pilne; wartość pola *Wskaźnik pilności* wskazuje ostatni bajt tych danych.
- ♦ **ACK.** Flaga ACK (*Acknowledgement*) ma ustawioną wartość 1 (włączona), kiedy wartość pola potwierdzenia jest znacząca. Segment z włączonym ACK posiada potwierdzenie prawidłowo odebranego segmentu.
- ♦ **PSH.** Flaga Push nakazuje protokołowi TCP natychmiastowe wysłanie danych z tej wiadomości do warstwy aplikacji.
- ♦ **RST.** Flaga Reset wartość 1 (włączona) resetuje połączenie.
- ♦ **SYN.** Flaga Synchronize wskazuje, że protokół dokonuje synchronizacji numerów sekwencyjnych.
- ♦ **FIN.** Flaga Final ma ustawioną wartość 1 (włączona), protokół jest w trakcie kończenia sesji.

## Pole sumy kontrolnej

Pole sumy kontrolnej zawiera wartość używaną do określenia, czy cały pakiet prawidłowo dotarł do miejsca przeznaczenia. Pole to zawiera mechanizm sprawdzający zarówno nagłówek, jak i same dane. Wartość sumy kontrolnej zmienia się w zależności od tego, czy pakiet jest transmitowany przez protokół IP w wersji 4., czy wersji 6. Jednak format nagłówka TCP pozostaje taki sam dla obu wersji.

W celu pobrania sumy kontrolnej wyszukane zostają wszystkie 16-bitowe słowa w pakiecie, a następnie dodane. Jeżeli pakiet ma nieparzystą liczbę oktetów (słów), to ostatni jest dopełniany zerami. Na otrzymanej liczbie jest przeprowadzana operacja dopełnienia do jedności. W ten sposób uzyskujemy pełne, 16-bitowe słowo sumy kontrolnej.

W ogólnych rozważaniach przedstawionych w tym rozdziale dokładne informacje dotyczące sum kontrolnych nie są bardzo istotne. Jeżeli Czytelnik jest zainteresowany tymi szczegółami, to może je znaleźć w dokumentach RFC 793 (dla IP w wersji 4.) i RFC 2460 (dla IP w wersji 6.). Jednak warto wspomnieć, że te dwie używane metody obliczania sum kontrolnych są bardzo słabe w porównaniu z metodami takimi jak CRC (ang. *Cyclic Redundancy Check*), stosowanymi na poziomie aplikacji. Tak naprawdę w większości aplikacji stosowane są bardziej zaawansowane sposoby sprawdzania poprawności danych.

## Pola kontrolne

Jako fragment części odpowiedzialnej za kontrolę ruchu pole *Wielkość okna* określa wielkość okna otrzymywania. Wielkość transferowanego bloku danych nie jest sztywno ustalana przez TCP. Blok ten może być bardzo mały i mieć wielkość jednego bajta, być bardzo duży i mieć wielkość jednego kilobajta lub wielkość z wymienionego przedziału. Jeżeli wiadomość ma wielkość 2048 KB, to można użyć dowolnej kombinacji wielkości bloku danych, aż do osiągnięcia tych 2048 KB. System otrzymujący dane może ustalić wielkość okna na podstawie ilości miejsca pozostałego w buforze pamięci TCP. Górną granicę wielkości dla pojedynczego pakietu określa MTU (ang. *Maximum Transmission Unit*).

Pole wskaźnika pilności jest używane, gdy opcja Urgent (URG) ma ustawioną wartość 1. Wymienione pole podaje wartość przesunięcia względem numeru sekwencji dla ostatniego ważnego bajta danych w sekwencji Urgent.

Blok opcji zawiera pewną liczbę odmiennych wartości, które można ustawić w zakresie od 0 do 8. Są one następujące:

0. Koniec listy opcji.
1. Brak operacji.
2. Skalowanie okna.
3. SACK — selektywne potwierdzanie (ang. *Selective Acknowledgement*).
4. Długość danych (jeżeli wymagane).
5. Długość danych (jeżeli wymagane).
6. Długość danych (jeżeli wymagane).
7. Długość danych (jeżeli wymagane).
8. Znacznik czasu.

## Pole danych

Ostatni blok to blok danych. W tym miejscu znajduje się porcja danych TCP pakietu; dane są w postaci protokołu warstwy aplikacji. W polu danych można zastosować dowolny format danych, który może być wysłany przez TCP, na przykład HTTP, FTP, POP3, SMTP i wiele innych. Jednak dane w pakiecie mogą być wysyłane tylko w jednym formacie, a ponadto muszą być wysyłane do portu, który oczekuje tego typu danych.

Wielkość pola danych nie jest ustawioną wartością. Może być bardzo mała (na przykład jeden bajt) lub bardzo duża, aż do maksymalnej wielkości okna. Protokół TCP ma wbudowany mechanizm pozwalający na ustawienie wielkości pola danych w zależności od warunków. To jest część mechanizmu kontroli TCP.

## Operacje protokołu

TCP działa przez utworzenie połączenia między dwoma systemami. Połączenie pozostaje wirtualne, ponieważ choć oba punkty końcowe połączenia są znane, to ścieżki do nich prowadzące już nie. Punkt końcowy jest definiowany za pomocą dwóch parametrów: adresu IP i numeru portu.

W celu utworzenia połączenia TCP wykorzystuje mechanizm 3-etapowego procesu negocjacji (ang. *three-way handshake*):

1. Komputer nadawcy wysyła żądanie SYN do komputera odbiorcy z początkowym, wyznaczanym losowo numerem sekwencyjnym. Flaga SYN ustawiona na 1, ACK na 0.
2. Komputer odbiorcy potwierdza otrzymanie wiadomości — zwraca nadawcy odpowiedź SYN-ACK. W polu *Numer sekwencyjny* umieszcza początkową, losową wartość, a w polu *Numer potwierdzenia* numer sekwencyjny, otrzymany w pakiecie od nadawcy, zwiększony o jeden. Flagi SYN i ACK ustawione na 1.
3. Komputer nadawcy wysyła wiadomość ACK w celu wskazania, że połączenie zostało nawiązane. Flaga SYN ustawiona na 0, flaga ACK na 1. Pole *Numer sekwencyjny* jest zwiększone o jeden w stosunku do wysłanego w kroku pierwszym, a pole *Numer potwierdzenia* ma wartość zwiększoną o jeden, przesłaną przez odbiorcę w kroku drugim, w polu *Numer sekwencyjny*.

Po nawiązaniu połączenia można przystąpić do transferu danych. Połączenie jest definiowane przez cztery parametry: adres IP i numer portu nadawcy, adres IP i numer portu odbiorcy. Ponieważ protokół TCP obsługuje multipleksowanie, pełny opis połączenia będzie zawierał protokół transportowy użyty do utworzenia połączenia dwukierunkowego:

(TCP, IP-nadawcy, Port-nadawcy, IP-odbiorcy, Port-odbiorcy)

Połączenia mogą być również opisane jako jednokierunkowe:

(TCP, IP-nadawcy, Port-nadawcy)

oraz w kierunku przeciwnym:

(TCP IP-odbiorcy, Port-odbiorcy)

Koncepcja połączeń jednokierunkowych jest tak naprawdę przydatna tylko wtedy, gdy są stosowane różne protokoły. Jeżeli użytkownik na przykład kliknie w przeglądarce internetowej łącze do pobrania pliku za pomocą FTP, to połączenie wychodzące HTTP będzie wysłane przez port 80, podczas gdy plik przychodzący będzie wysłany przez FTP do portu 21.

Aktywny transfer danych jest charakteryzowany przez następujące działania:

1. System nadawcy rozpoczyna od wysłania pakietów IP w wielkości oraz z szybkością, które zostały wynegocjowane podczas nawiązywania połączenia (*three-way handshake*).
2. System odbiorcy zbiera pakiety w pamięci bufora i rozpoczyna ich ponowne łączenie w całość. Pole sumy kontrolnej każdego pakietu jest używane w celu określenia, czy otrzymany pakiet jest prawidłowy.

3. Jeżeli pakiet zaginął, to system odbiorcy żąda ponownej transmisji.
4. W regularnych odstępach czasu system odbiorcy wysyła polecenie ACK wraz z pozycją następnego oczekiwanego pakietu (pole *Numer potwierdzenia* wskazuje, że wszystkie pakiety o mniejszym numerze sekwencyjnym zostały odebrane). Taki mechanizm nosi nazwę *potwierdzenia skumulowanego*; schemat ten czasami jest nazywany *schematem PAR* (ang. *Positive Acknowledgement with Retransmission*). Każde polecenie ACK może ustawić flagę zmieniającą szybkość transmisji, jak również wielkość danych znajdujących się w każdym pakiecie.
5. Jeżeli system nadawcy nie otrzyma polecenia ACK wraz z informacją potwierdzającą dostarczenie pakietu, po określonym czasie rozpoczyna ponowne wysyłanie pakietu.
6. Kiedy system odbiorcy otrzyma wiadomość ACK od systemu nadawcy, potwierdzającą dostarczenie ostatniego wysyłanego pakietu, wówczas wysyłający będzie kontynuował wysyłanie pakietów dodatkowych od wskazanego miejsca w sekwencji.
7. Kiedy system odbiorcy dostanie ostatni pakiet w sekwencji, przeprowadzi sprawdzenie danych, a następnie wyśle wiadomość LAST-ACK.

Wraz z ostatnim pakietem TCP nie wysyła znacznika końca wiadomości. Wiadomość będzie kompletna, kiedy komputer odbierający przekaże wszystkie połączone dane aplikacji, która z nich korzysta. Nie ma struktury dla strumieniowania danych TCP, protokół TCP nie posiada wiedzy na temat zawartości znajdującej się w danych. Nie może więc umieścić określonego rekordu danych przed innym bądź wysłać określonego pliku przed innym. Wszelkie operacje umieszczania danych w kolejności i ich obsługa są przeprowadzane przez aplikację. Dlatego też to do aplikacji należy wysłanie sygnału informującego, że połączenie nie jest dłużej wymagane. Brak sygnału ze strony aplikacji to powód, dla którego połączenia są pozostawione otwarte, chociaż nie są dłużej wymagane.

Połączenie zostaje zerwane za pomocą innego procesu typu *handshake*. Każdy punkt końcowy niezależnie od drugiego zamyka połączenie.

W celu zamknięcia połączenia trzeba wykonać następujące kroki:

1. Punkt końcowy 1 wysyła pakiet FIN do punktu końcowego 2.
2. Punkt końcowy 2 odsyła potwierdzenie (ACK) do punktu końcowego 1. Następnie punkt końcowy 1 zamyka połączenie ze swojej strony, połączenie pozostaje w stanie półotwartym.
3. Punkt końcowy 2 wysyła pakiet FIN do punktu końcowego 1.
4. Punkt końcowy 1 odsyła potwierdzenie (ACK) do punktu końcowego 2. Następnie punkt końcowy 2 zamyka połączenie ze swojej strony, tym samym całkowicie zamykając połączenie.

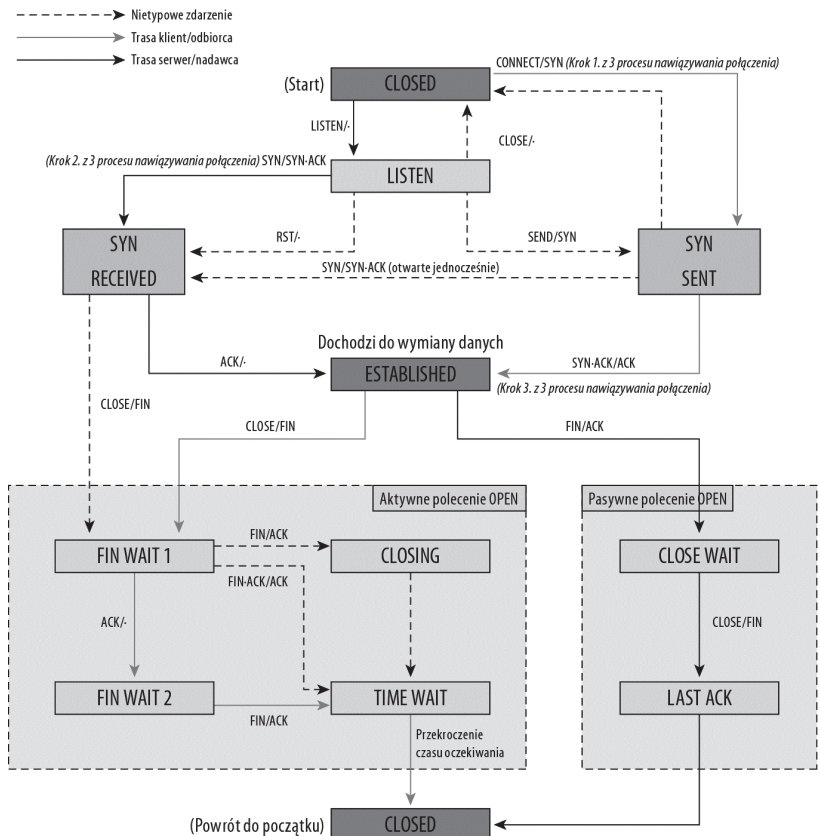
Powyższy opis pokazuje czteroetapową operację, która wymaga przeprowadzenia czterech różnych transmisji. Większość połączeń jest zamykanych za pomocą operacji trzyetapowej przez połączenie kroków 2. i 3. w pojedyncze polecenie FIN & ACK.

Podsumowując, punkty końcowe mogą znajdować się w jednym z poniższych stanów:

1. LISTEN
2. SYN-SENT
3. SYN-RECEIVED
4. ESTABLISHED
5. FIN-WAIT-1
6. FIN-WAIT-2
7. CLOSE-WAIT
8. CLOSING
9. LAST-ACK
10. TIME-WAIT
11. CLOSED

Na rysunku 17.2 zilustrowano różne stany połączeń TCP wraz z metodami używanymi do poruszania się pomiędzy tymi stanami. Wskazano kroki niezbędne do nawiązania połączenia, jak również związek pomiędzy stanami Active Open i Passive Open.

**Rysunek 17.2.**  
Wykres pokazujący  
stany w systemie TCP



## Połączenia

Środowisko TCP dla wielu systemów operacyjnych jest postrzegane przez programistów jak następny system plików. Ma to miejsce w przypadku własnościowego interfejsu Winsock firmy Microsoft, jak również interfejsu BSD Sockets, powszechnie używanego w wielu systemach, na przykład Unix, Mac OS, BSD, czyli Berkeley Software Distribution albo system operacyjny Berkeley Unix. TCP komunikuje się za pomocą modułu IP, który do komunikacji z siecią wymaga sterownika urządzenia.

Programy, które chcą użyć TCP do transferu danych, mają do dyspozycji zorientowane połączeniowo klasy wywołań systemowych:

- ♦ OPEN
- ♦ CLEAN
- ♦ SEND
- ♦ RECEIVE
- ♦ STATUS

Wraz z poleceniami są przekazywane parametry połączeń jednokierunkowych, które dostarczają adres oraz port systemu docelowego. Inne parametry będące częścią tych poleceń są używane do zapewnienia bezpieczeństwa oraz innych zadań.

Połączenia są odpowiedzią na wywołanie polecenia OPEN modułu TCP stosu sieciowego systemu operacyjnego nadawcy. Ten moduł następnie komunikuje się z modulem TCP systemu odbiorcy, oba wykorzystują swoje moduły IP do przesłania danych. Podczas tworzenia połączenia wywołanie zwrotne do aplikacji przekazuje uchwyt połączenia z powrotem do niej, dzięki któremu możliwa jest identyfikacja połączenia. Wymieniony uchwyt to mała liczba całkowita, która wraz z innymi parametrami połączenia jest przechowywana przez program w TCB (ang. *Transmission Control Block*).

Programy wykonują dwa rodzaje wywołań OPEN: aktywne albo pasywne. Aktywne polecenie OPEN powoduje, że moduł TCP wysyła systemowi odbiorcy wiadomość o otwieraniu połączenia. Jeżeli system odbiorcy zwróci aktywne polecenie OPEN, to połączenie zostaje nawiązane i można przystąpić do transferu danych.

Pasywne polecenie OPEN powoduje, że moduł TCP systemu odbiorcy przechodzi w stan, w którym jest przygotowany do przyjmowania pakietów od systemu nadawcy. Pasywnemu poleceniu OPEN można przekazać parametr w postaci punktu końcowego systemu odbiorcy; w punkcie tym program TCP oczekuje na określone pakiety. Pasywne polecenie OPEN ewentualnie może nie zawierać punktów końcowych. W takim przypadku moduł TCP akceptuje wszystkie dane po otrzymaniu żądania połączenia (SYN) od systemu nadawczego. Przychodzące żądanie SYN jest początkiem transmisji wskutek wydania polecenia OPEN w systemie nadawczym.

Aplikacja wydająca pasywne polecenie OPEN przełącza się w stan oczekiwania. Następnie TCP informuje ją o nawiązaniu połączenia przez przekazanie do niej aktywnego polecenia OPEN z systemu nadawcy. Na tym etapie pasywny stan OPEN w systemie odbiorcy zostaje zmieniony na aktywny stan OPEN i rozpoczyna się transfer danych.

## Kontrola przepływu

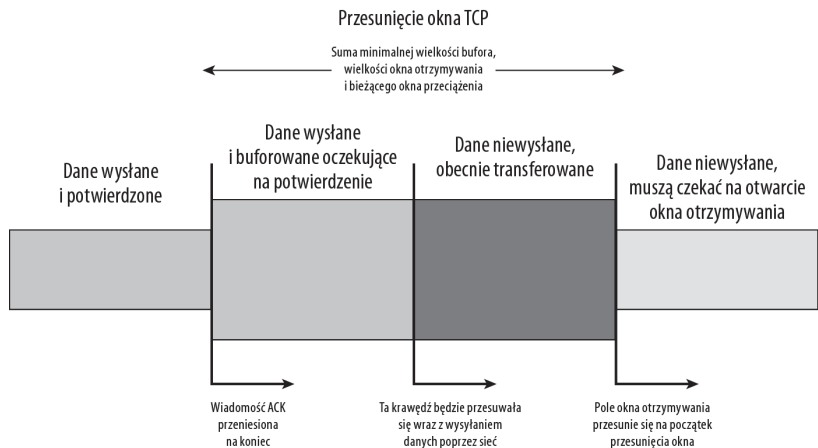
Mechanizm kontroli przepływu danych TCP działa w następujący sposób: na początku określana jest szybkość transmisji i wielkość pakietu, a następnie parametry te są modyfikowane zgodnie z potrzebami w trakcie transferu danych. Wielkość nagłówka pakietu nie ulega zmianie, ale ilość danych TCP znajdujących się w części głównej pakietu może być zmieniona. Parametr MSS (ang. *Maximum Segment Size*), czyli maksymalna wielkość segmentu, określa wielkość pojedynczego segmentu, który może być używany. Wartość ta jest ustalana podczas nawiązywania połączenia i jest powiązana z wielkością MTU (ang. *Maximum Transmission Unit*), dozwoloną przez warstwę Data Link sieci.

### Przesuwające się okna

Używany protokół kontroli przepływu jest określany mianem *przesuwanego okna*. Rozmiar okna jest podawany przez odbiorcę i określa ilość danych, jakie może on przyjąć bez przepełnienia bufora. Pakiet potwierdzenia ACK, jaki otrzymuje nadawca, powoduje przesunięcie początku okna. Początek znajduje się zawsze za ostatnimi potwierdzonymi danymi, których ciągłość jest zachowana. Nadawca wysyła dane aż do wypełnienia okna. Działanie przesuwającego się okna odbiorcy zostało pokazane na rysunku 17.3.

#### Rysunek 17.3.

*Przesuwające się okno odbiorcy pozwala na efektywny transfer danych bez przepełniania bufora*



Okno TCP może mieć wielkość od 2 do 65 535 bajtów. W niektórych systemach wykorzystywana jest technika o nazwie *skalowanie okna*, negocjowana w trakcie nawiązywania połączenia TCP. Ta opcja umożliwia zwiększenie maksymalnej wielkości okna aż do 1 GB. Skalowanie okna powoduje problemy w wielu routerach i zaporach sieciowych, a także komputerach działających pod kontrolą systemów Vista i Linux.

### Kontrola przeciążenia sieci

Odbiorca ma możliwość zatrzymania przepływu danych. W tym celu wystarczy ustawić zerową wielkość okna. Kiedy system nadawcy wykryje znak zatrzymania, wówczas włączy wewnętrzny licznik czasu, nadzorujący limit czasu oczekiwania podczas wysyłania danych. Gdy wspomniany licznik osiągnie zdefiniowaną wartość, system nadawcy wyśle mały

pakiet, którego celem będzie wydanie polecenia ACK ze strony odbiorcy wraz z nową wielkością okna. Taka metoda gwarantuje, że transfer danych nie będzie zatrzymany na stałe, jeżeli wiadomość ACK od systemu odbiorcy ulegnie zagubieniu.

Innym sposobem przerywania strumienia danych TCP jest wysłanie dodatkowych danych oznaczonych jako pilne. Kiedy pakiet przybywa z takim oznaczeniem, TCP zatrzymuje przetwarzanie danych w bieżącym strumieniu i przechodzi do przetwarzania pakietu oznaczonego jako pilny. Następnie powraca do przetwarzania strumienia przetwarzanego przed przybyciem pakietu oznaczonego jako pilny. Pakiety pilne są nazywane danymi OOB (ang. *out-of-band*). Przykładem procesu OOB będzie wysłanie sygnału przerywania z programu działającego w systemie nadawcy.

TCP pozwala na stosowanie wiadomości SACK (ang. *Selective Acknowledgement*) jako rodzaju optymalizacji. Odbiorca może wysłać tę wiadomość w dowolnym momencie po otrzymaniu bloku pakietów, które mogą być połączone w całość, ale wymagają wcześniejszych pakietów, by zachować prawidłową sekwencję. Wiadomość SACK ma taką samą strukturę jak ACK, ale zawiera otrzymany początkowy i końcowy numer sekwencyjny. Jeżeli na przykład otrzymane zostały bajty od 0 do 2044, a blok SACK ma numery sekwencyjne od 2088 do 9696 dla otrzymanego zakresu, to system nadawcy ponownie wyśle pakiety o numerach sekwencyjnych od 2045 do 4087. Wiadomość SACK jest opcjonalna, ale często wykorzystywana.

Kontrola przepływu danych zawiera także mechanizm pozwalający na zmianę szybkości transmisji jako funkcję wydajności działania sieci. W systemie nadawcy na podstawie częstotliwości otrzymywania wiadomości ACK od odbiorcy istnieje możliwość oszacowania wydajności działania sieci. Większe odstępy czasu pomiędzy wiadomościami ACK wskazują na przeciążenie sieci i stanowią bazę dla czasu ponownej transmisji, pozwalającą na oszacowanie czasu przesyłu danych. Każda wiadomość TCP zawiera znacznik czasu. Protokół TCP jest zaopatrzony w zestaw algorytmów — powolny start, unikanie przeciążenia, szybką ponowną transmisję i szybkie odzyskiwanie — które zostały opracowane w celu umożliwienia kontrolowania szybkości transferu.

## Multipleksowanie

Multipleksowanie to funkcja pozwalająca, aby strumień danych był wysyłany za pomocą kilku oddzielnych procesów. TCP oferuje multipleksowanie jako opcję. Kiedy aplikacja obsługuje multipleksowanie, może być ono użyte do przyspieszenia i zoptymalizowania transferu danych TCP. Z przykładem multipleksowania można się spotkać, gdy przeglądarka internetowa pobiera stronę internetową, używając protokołu HTTP, lub gdy narzędzie do transferu plików transferuje plik za pomocą wielu połączeń. TCP ma możliwość połączenia w jedną całość danych pochodzących z różnych strumieni.

Aplikacje wysyłają dane przez porty przypisane na stałe albo przez zarejestrowany port. Program iTunes firmy Apple używa portu 3689 do otrzymywania danych za pomocą protokołu DAAP (ang. *Digital Audio Access Protocol*). Podczas odświeżania listy podcastów (zbioru wiadomości RSS) otwiera się wiele połączeń używających tego samego numeru portu. Gdy pobierany jest większy plik wideo, na przykład NBC Nightly News lub Meet the Press, i nie są pobierane w tym czasie inne podcasty, to program iTunes tworzy trzy

strumienie przeznaczone do pobrania pliku wideo. W przypadku pobierania kilku podcastów każdy ze wspomnianych trzech strumieni jest używany do pobierania innego. Na rysunku 17.4 pokazano multipleksowanie w postaci trzech współbieżnych strumieni TCP.



**Rysunek 17.4.** Przykład multipleksowania trzech niezależnych strumieni za pomocą tego samego protokołu i portu

TCP nie ma żadnych szczegółowych informacji o tym, które strumienie są używane do pobierania poszczególnych podcastów. Do zadań programu iTunes należy pobieranie danych i poprawne umieszczanie plików podcastów w odpowiednich katalogach, tak aby stały się dostępne dla aplikacji. Ponadto to program iTunes ustala, które pliki będą pobierane oraz w jakiej kolejności. Użytkownik może zmodyfikować kolejność pobierania plików przez przenoszenie ich na liście plików do pobrania, wstrzymywanie pobierania lub całkowite usunięcie wybranych plików z listy.

## Protokół User Datagram Protocol

Protokół *User Datagram Protocol* (UDP) to protokół internetowy tworzący bezstanowe połączenia między dwoma komputerami w sieci IP. UDP tworzy krótki format transferu danych nazywany *datagramem* oraz połączenie nazywane *gniazdem do przesyłania datagramów* między dwoma punktami końcowymi. Tworzone połączenie wirtualne używa tej samej koncepcji portu do wysyłania danych różnego rodzaju pomiędzy komputerami. Pojęcie *bezzstanowy* odnosi się do mechanizmu transferu, który nie próbuje zagwarantować poprawności wysyłanych danych. System odbiorcy odtwarza dane z otrzymanych datagramów niezależnie od tego, czy znajdują się we właściwej kolejności i czy sekwencja jest poprawna.

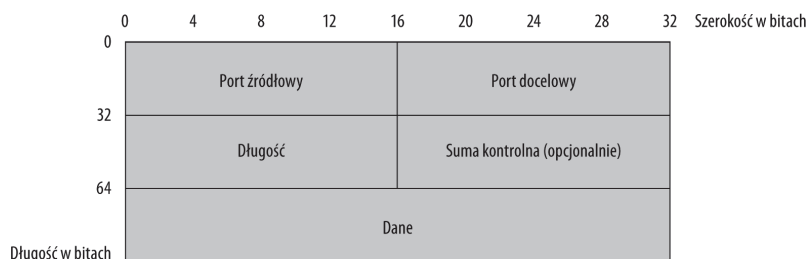


Skrót UDP czasami bywa rozwijany jako *Universal Datagram Protocol* (uniwersalny protokół datagramów) lub ironicznie jako *Unreliable Datagram Protocol* (zawodny protokół datagramów). Jednak zgodnie z dokumentem RFC 768 oficjalną nazwą jest *User Datagram Protocol*.

Fakt, że UDP nie powoduje takiej nadmiarowości jak w przypadku protokołu TCP, oznacza możliwość osiągania większych transferów za pomocą UDP niż przy użyciu TCP. Z tego powodu protokół UDP będzie lepszym rozwiązaniem w sytuacjach, gdy nie jest wymagane niezawodne dostarczanie danych — na przykład w przypadku wysyłania krótkich wiadomości, dużej ilości danych redundancyjnych lub wysyłania danych opcjonalnych. Usługi rozpoznawania nazw, jak omówiony w rozdziale 19. DNS (ang. *Domain Name System*), używają UDP, ponieważ ich wiadomości są krótkie, a system zgłaszający ponownie przekazuje zapytania, jeśli odpowiedź nie nadejdzie. Aplikacje obsługujące głos, muzykę i wideo stosują protokół UDP, ponieważ zgubienie ramki filmu bądź ułamka sekundy połączenia VoIP (ang. *Voice over IP*) nie spowoduje znacznego obniżenia jakości materiału. Niemal wszystkie aplikacje używane do strumieniowania mediów używają UDP jako protokołu transferu w sieciach IP.

Datagramy UDP mają bardzo prosty format, który został pokazany na rysunku 17.5. Jedyne funkcje znajdujące się w datagramie to suma kontrolna używana do określenia jego poprawności oraz możliwość multipleksowania datagramów. To zapewnia możliwość transmisji wielu strumieni danych w aplikacjach, które obsługują taką funkcję. Obie wymienione funkcje są opcjonalne, jeśli w specyfikacji portu źródłowego użyto IP w wersji 4. W przypadku użycia IP w wersji 6. wymagana jest suma kontrolna.

**Rysunek 17.5.**  
Struktura datagramu  
UDP



O ile sieć nie używa dużej liczby aplikacji multimedialnych, protokół UDP będzie po mniejszym, choć ważnym komponentem ruchu w tej sieci. Jednak pewne istotne protokoły wykorzystują UDP — nie tylko wspomniany już DNS, ale również DHCP (ang. *Dynamic Host Configuration Protocol*), dostarczający adresy IP klientom, RIP (ang. *Routing Information Protocol*), stosowany w celu dostarczenia dynamicznego trasowania w sieciach, oraz SNMP (ang. *Simple Network Management Protocol*), wykorzystywany w większości pakietów zarządzania siecią. Z tego powodu UDP staje się protokołem o znaczeniu krytycznym wśród protokołów internetowych.

W sieciach, w których używana jest duża liczba aplikacji multimedialnych, UDP może wyprzeć ruch sieciowy TCP. Kiedy TCP wykrywa przeciążenie sieci, jego mechanizmy powodują zmniejszenie produkcji pakietów, walcząc w ten sposób z przeciążeniem. To powoduje, że UDP zużywa jeszcze większą przepustowość sieci, co prowadzi do wyparcia ruchu o znaczeniu krytycznym dla usług sieciowych. Aplikacje TCP, takie jak dostęp do bazy danych, wymagające do prawidłowego działania niezawodnego transferu danych TCP,

mogą zostać spowolnione lub nawet zatrzymane aż do unormowania się sytuacji. Ten problem doprowadził do tego, że w wielu sieciach usługi strumieniowania zostały w ogóle zakazane albo znacznie ograniczone.

## Porty

Do komunikacji pomiędzy punktami końcowymi protokoły zarówno TCP, jak i UDP używają portów. Kiedy pakiet danych dociera do miejsca przeznaczenia, następuje sprawdzenie jego adresu źródłowego, numeru portu źródłowego, adresu docelowego oraz numeru portu docelowego. Numer portu jest przypisany określonej typowi danych. Lista portów i obsługiwanych przez nie typów danych jest ustalana przez organizację IANA (*Internet Assigned Numbers Authority*, <http://www.iana.org/assignments/port-numbers>).

Każdy komputer niezależnie zarządza swoimi portami. Proces rejestru zdarzeń lub proces superdemona w systemach Linux (Unix) monitoruje numery portów, szczególnie portów doskonale znanych, w celu określenia, kiedy otrzymywany jest ruch sieciowy.

Poniżej wymieniono trzy różne zakresy portów:

- ♦ **Porty przypisane na stałe.** Te porty są używane przez powszechnie stosowane protokoły; numery tych portów znajdują się w zakresie od 0 do 1023 i są administrowane przez organizację IANA. Niektóre z portów przypisanych na stałe zostały wymienione w tabeli 17.1.
- ♦ **Porty zarejestrowane.** To są porty wysyłające lub otrzymujące ruch sieciowy przez określone aplikacje i zostały zarejestrowane przez producentów, handlowe grupy przemysłowe oraz przez pojedyncze osoby i organizacje. Numery portów zarejestrowanych znajdują się w zakresie od 1024 do 49 151. Porty zarejestrowane nie są kontrolowane przez organizację IANA, ale są wymienione w jej rejestrach.
- ♦ **Porty dynamiczne i (lub) prywatne.** Te porty nie są przypisane, pozostają do dowolnego użytku. W celu zwiększenia poziomu bezpieczeństwa w niektórych aplikacjach porty są wybierane losowo w trakcie nawiązywania połączenia. Są one nazywane *portami ulotnymi* i tracą swoje znaczenie po zamknięciu połączenia. Zakres numerów portów dynamicznych i prywatnych to od 49 152 do 65 535.

**Tabela 17.1.** Doskonale znane porty (od 0 do 1023)

Port	Opis
0 — T, U	Zarezerwowany
1 — T, U	TCP Port Service Multiplexer — multiplexer obsługi portów TCP
2 — T, U	Narzędzia zarządzania
3 — T, U	Proces kompresji
5 — T, U	Remote Job Entry — zgłoszenie zdalnej pracy
7 — T, U	Echo
13 — T, U	Daytime (dokument RFC 867) — czas dzienny

**Tabela 17.1.** Doskonale znane porty (od 0 do 1023) — ciąg dalszy

Port	Opis
17 — T, U	Cytat dnia
18 — T, U	Message Send Protocol
19 — T, U	Generator znaków
20 — T, U	FTP — transfer plików: dane
21 — T, U	FTP — transfer plików: sterowanie
22 — T, U	SSH Remote Login Protocol
23 — T, U	Telnet
25 — T, U	SMTP (Simple Mail Transfer Protocol)
33 — T, U	Display Support Protocol — protokół obsługi wyświetlania
37 — T, U	TIME Protocol — czas
38 — T, U	Route Access Protocol
39 — T, U	Resource Location Protocol — protokół lokalizacji zasobów
41 — T, U	Graphics — grafika
42 — T, U	Host Name Server Protocol — serwer nazw komputerów
42 — T, U	WINF (nieoficjalnie)
43 — T, U	Protokół WHOIS — program identyfikujący
48 — T, U	Digital Audit Daemon
49 — T, U	TACACS Login Host Protocol
50 — T, U	Remote Mail Checking Protocol
53 — T, U	DNS (Domain Name System)
63 — T, U	whois++
65 — T, U	TACACS — Database Service
66 — T, U	Oracle SQL*NET
67 — T, U	BOOTP (Bootstrap Protocol) — serwer protokołu inicjalizacji
68 — T, U	BOOTP (Bootstrap Protocol) — klient protokołu inicjalizacji
69 — T, U	TFTP (Trivial File Transfer Protocol) — uproszczony protokół transferu plików
70 — T, U	Gopher
79 — T, U	Finger
80 — T, U	HTTP (HyperText Transfer Protocol) — połączenie z serwerem WWW
82 — T, U	XFER Utility
88 — T, U	Kerberos

**Tabela 17.1.** Doskonale znane porty (od 0 do 1023) — ciąg dalszy

Port	Opis
92 — T, U	Network Printing Protocol
105 — T, U	Mailbox Name Nameserver
107 — T, U	Remote Telnet Service Protocol
109 — T, U	Post Office Protocol 2 (POP2) — protokół pocztowy POP wersja 2.
110 — T, U	Post Office Protocol 3 (POP3) — protokół pocztowy POP wersja 3.
113 — T, U	Authentication Service — usługa uwierzytelniania
115 — T, U	SFTP (Simple File Transfer Protocol)
118 — T, U	SQL Services
119 — T, U	NNTP (Network News Transfer Protocol)
123 — T, U	NTP (Network Time Protocol)
129 — T, U	Password Generator Protocol
137 — T, U	NetBIOS Name Service — obsługa nazw NetBIOS
138 — T, U	NetBIOS Datagram Service
139 — T, U	NetBIOS Session Service — obsługa sesji NetBIOS
143 — T, U	IMAP (Internet Message Access Protocol)
152 — T, U	BFTP (Background File Transfer Program)
153 — T, U	SGMP (Simple Gateway Monitoring Protocol)
156 — T, U	SQL Service — obsługa SQL
161 — T, U	SNMP (Simple Network Management Protocol)
162 — T, U	SNMP TRAP (Simple Network Management Protocol Trap)
170 — T	Print-srv, Network PostScript
177 — T, U	XDMCP (X Display Manager Control Protocol)
179 — T	BGP (Border Gateway Protocol)
194 — T	IRC (Internet Relay Chat)
201 — T, U	AppleTalk Routing Maintenance
213 — T, U	IPX
218 — T, U	MPP (Message Posting Protocol)
220 — T, U	IMAP (Interactive Mail Access Protocol), wersja 3.
389 — T, U	LDAP (Lightweight Directory Access Protocol)
401 — T, U	UPS (Uninterruptible Power Supply)
427 — T, U	SLP (Service Location Protocol)

**Tabela 17.1.** Doskonale znane porty (od 0 do 1023) — ciąg dalszy

Port	Opis
443 — T	HTTPS (HyperText Transfer Protocol over TLS/SSL)
444 — T, U	SNPP (Simple Network Paging Protocol), dokument RFC 1568
445 — T	Microsoft-DS Active Directory, udział Windows
445 — U	Microsoft-DS SMB — współdzielenie plików
464 — T, U	Zmiana/ustawienie hasła Kerberos
500 — U	ISAKMP (Internet Security Association and Key Management Protocol)
513 — T	Login
513 — U	Who
514 — T	Shell
514 — U	Syslog
515 — T	LPD (Line Printer Daemon)
520 — U	RIP — protokół routingu
524 — T, U	NCP (NetWare Core Protocol)
525 — U	Timed, Timeserver
530 — T, U	RPC
531 — T, U	AOL Instant Messenger (IRC) (Nieoficjalnie)
540 — T	UUCP (Unix-to-Unix Copy Protocol)
546 — T, U	DHCPv6 klient
547 — T, U	DHCPv6 serwer
548 — T	AFP (Apple Filing Protocol) przez TCP
554 — T, U	RTSP (Real Time Streaming Protocol)
631 — T, U	IPP (Internet Printing Protocol)
660 — T	Mac OS X Server Admin — administracja systemem
666 — U	Wyłączony z użytku
691 — T	MS Exchange Routing
860 — T	iSCSI (dokument RFC 3720)
953 — T, U	RDNS Domain Name System (DNS)
993 — T	IMAPS (Internet Message Access Protocol over SSL)
995 — T	POP3S (Post Office Protocol 3 over TLS/SSL)



Porty o numerach większych niż 1023 mogą być przypisywane w locie. Te rodzaje portów noszą nazwę portów tymczasowych i są charakterystyczne dla określonego modułu TCP, który jest używany.

## Problemy z TCP

Komunikacja TCP jest narażona na różnego rodzaju ataki. W przypadku ataku DoS (ang. *Denial of Service*) atakujący wysyła dużą liczbę pakietów SYN pochodzących z fałszywego adresu IP. Taki atak, nazywany powodzią SYN, wymusza na systemie odbiorcy (zwykle serwerze) udzielania odpowiedzi na te żądania i tym samym zużycie posiadanych zasobów na obsługę nieprawdziwych połączeń.

Inny problem związany z ruchem TCP polega na tym, że nagłówek nie jest szyfrowany, a więc może być odczytany przez skanery pakietów monitorujące dane. Istnieje możliwość przejścia połączenia przez poznanie numeru sekwencyjnego, a następnie utworzenie pakietu o poprawnym numerze sekwencyjnym. Sam pakiet nie musi być skomplikowany, musi zawierać jedynie ilość informacji wystarczającą do przerwania synchronizacji między systemami. Kiedy połączenie zostanie zerwane, haker przejmuje kontrolę nad trasą pakietów, tak aby jego system stał się fałszywym punktem końcowym. Implementacja losowo wybieranych ISN powoduje, że przejście połączenia staje się znacznie trudniejszym zadaniem. Opisana forma ataku nosi nazwę „człowiek pośrodku” (ang. *Man-in-the-Middle*).

Jak już wcześniej wspomniano, ruch TCP może być zakłócony, kiedy inny rodzaj ruchu sieciowego, na przykład UDP, stanie się większą częścią ogólnego ruchu sieciowego. Wiąże się to z faktem, że TCP implementuje mechanizm kontroli przeciążenia sieci, który zmniejsza wielkość okna otrzymywania w celu zmniejszenia szybkości transmisji. W pewnym momencie ruch sieciowy TCP może spaść do poziomu zamrożenia, określanego mianem *zapaści z powodu przeciążenia*. Wprawdzie istnieją rozwiązania tego problemu, ale niektóre z nich same są problematyczne.

Pierwszym rozwiązaniem jest ograniczenie użycia strumieniowania mediów w sieci. W przypadku biura używającego aplikacji biurowych i niewymagającego dużej ilości treści multimedialnych ograniczenie multimediów nie stanowi kłopotu. Jeżeli jednak wykonywana praca wymaga ogromnej ilości strumieniowanych mediów, to trzeba zaimplementować inne metody kontroli. Jednym z potencjalnych rozwiązań pozostaje zastosowanie wysokiej jakości aplikacji QoS (ang. *Quality of Service*) w celu utrzymania przepływu ruchu na określonym poziomie. W wielu sieciowych systemach operacyjnych rozpoczęto implementację usług QoS jako funkcji podstawowych systemu. Aby uzyskać zaawansowany QoS, wiele firm zainwestowało środki w skomplikowane routery.

Inny problem pojawiający się w sytuacjach, w których mamy do czynienia z dużym ruchem sieciowym, występuje wtedy, gdy ogromne strumienie danych i systemy odbiorców odsyłają wiadomości ACK do nadawcy wraz z bardzo małą wielkością okna odbioru. Nadawca rozpoczyna więc wysyłanie bardzo małych pakietów zawierających jedynie po kilka bajtów. Takie zachowanie jest wysoce nieefektywne i nosi nazwę SWS (ang. *Silly Window Syndrome*), czyli „syndrom głupiego okna”. Aby walczyć z tym zjawiskiem, nowsze implementacje TCP zawierają logikę po stronie nadawcy, nazywaną algorytmem Nagle’a, która wykrywa omówiony stan i próbuje go naprawić.

Algorytm Nagle’a, opisany w dokumencie RFC 896 („Congestion Control in IP/TCP Internetworks”), jest używany do rozwiązywania problemu przeciążenia spowodowanego wysyłaniem w tym samym czasie zbyt wielu małych pakietów. Wiele procesów, np. naciśnięcia klawiszy w systemach Telnet, powoduje wysyłanie danych we fragmentach o wielkości jednego bajta. Ponieważ wszystkie nagłówki TCP/IP mają co najmniej 40 bajtów (20 bajtów dla TCP i 20 bajtów dla IPv4), nadmiarowość protokołów związana z wysyłaniem tego typu danych może być ogromna. Zadaniem algorytmu Nagle’a jest połączenie wielu małych wiadomości wychodzących i wysłanie ich w postaci pojedynczego pakietu, przy założeniu, że system odbiorcy nie udziela odpowiedzi na już wysłane wiadomości.

Algorytm Nagle’a ma następującą postać:

```
IF są nowe dane do wysłania
  IF wielkość okna >= MSS AND dostępne dane są >= MSS
    SEND teraz pełny segment MSS
  ELSE
    IF w potoku wciąż znajdują się niepotwierdzone dane
      umieszczaj dane w buforze aż do chwili otrzymania potwierdzenia
    ELSE
      SEND dane natychmiast
    END IF
  END IF
END IF
```

Algorytm Nagle’a ma jedną zasadniczą wadę — daje złe wyniki, kiedy używane są opóźnione wiadomości ACK, tak zwane ACK delay. Wiele implementacji TCP nie używa algorytmu Nagle’a lub wyłącza go, ponieważ powszechnie stosowane ustawienie opóźnienia na 500 milisekund (pół sekundy) może prowadzić do wielu operacji zapisu w aplikacji. Opóźnienia mogą być wyłączane za pomocą polecenia TCP\_NODELAY. Jednak większość rozwiązań problemu buforuje polecenia w aplikacji celem uniknięcia przeciążenia sieci z powodu wysyłania ogromnej ilości małych pakietów.

Zjawisko polegające na tym, że okno otrzymywania wysyła ogromną ilość drobnych pakietów i tym samym brakuje danych potrzebnych do działania aplikacji, nazywa się „syndromem tinygram” — jest to przeciwieństwo „syndromu głupiego okna”, w którym okno otrzymywania zostaje całkowicie zapełnione i nie ma możliwości otrzymywania kolejnych informacji.

## Podsumowanie

W rozdziale zostały omówione dwa najważniejsze protokoły transportowe używane w sieciach TCP/IP, czyli TCP (ang. *Transmission Control Protocol*) oraz UDP (ang. *User Datagram Protocol*). Protokół TCP jest używany wtedy, gdy dane muszą zostać dostarczone w całości, z zachowaniem kolejności. Z kolei protokół UDP jest wykorzystywany przez aplikacje, które tolerują utratę części danych.

Oba wymienione protokoły tworzą połączenia wirtualne i używają koncepcji portów do wysyłania danych różnego typu z systemu nadawcy do systemu odbiorcy. Połączenia są tworzone między dwoma komputerami i mają niezależne trasy, którymi dane są przekazywane między nimi.

Protokół TCP jest wyposażony w mechanizmy gwarantujące prawidłowe dostarczanie danych. Do łączenia danych dla warstwy wyższej wykorzystywany jest schemat zachowania kolejności. Protokół wysyła potwierdzenia po otrzymaniu danych lub kiedy dane są wymagane. W rozdziale przedstawiono różne sposoby kontroli przepływu danych oraz kontroli przeciążenia sieci, które są stosowane w celu zachowania jakości.

Protokół UDP jest bardzo ważny dla aplikacji strumieniujących media. Powoduje on znacznie mniejszą nadmiarowość niż TCP i jest stosowany w przypadku aplikacji używających małych wiadomości lub aplikacji strumieniujących.

W kolejnym rozdziale będzie przedstawiony protokół IP (Internet Protocol), kontrolujący schemat adresowania używany do wysyłania pakietów przez sieć TCP/IP. Omówione zostaną wersje zarówno 4., jak i 6. protokołu IP. Będzie także w pełni zaprezentowana koncepcja sieci i podsieci.



# Rozdział 18.

## Protokoły internetowe

### W tym rozdziale:

- ♦ W jaki sposób protokół Internet Protocol jest używany do wysyłania pakietów?
- ♦ W jaki sposób są tworzone i przypisywane adresy?
- ♦ Różne wielkości sieci oraz sposoby tworzenia podsieci
- ♦ Tworzenie i używanie sieci opartych na IPv6

Protokół IP (ang. *Internet Protocol*) to podstawowy protokół używany w celu całościowego dostarczania pakietów poprzez sieć TCP/IP. Istnieją dwie wersje protokołu IP: powszechnie używana wersja IPv4 oraz wersja IPv6, która jest stopniowo wprowadzana. W rozdziale zostaną szczegółowo omówione obie wersje.

IP to protokół niezależny od transportu, który działa w różnego rodzaju sieciach. Został zaprojektowany jako bezpołączeniowy, odporny na uszkodzenia oraz pozwalający na wyznaczanie tras (ang. *routing*). Dostępne są cztery rodzaje routingu: emisja pojedyncza (ang. *unicast*), rozgłaszanie (ang. *broadcast*), rozgłaszanie kierunkowe (ang. *directed broadcast*) i multiemisja (ang. *multicast*). W wersji IPv6 rozbudowano multiemisję, wyeliminowano rozgłaszanie oraz dodano funkcję routingu *anycast*.

Przestrzeń adresowa w wersjach IPv4 i IPv6 są całkiem odmienne. IPv4 wykorzystuje 32-bitową przestrzeń adresową, w której adresy są zwykle zapisane w formacie dziesiętnym wraz z kropkami: `###.###.###.###`. Dzięki zastosowaniu techniki maskowania przestrzeń adresowa może być podzielona na bloki o różnej wielkości. Bloki mogą tworzyć podsieci, a inne techniki, takie jak NAT, są stosowane w celu rozszerzenia przestrzeni adresowej. Przypisywanie adresów za pomocą DHCP zostanie omówione w dalszej części rozdziału.

Wersja IPv6 to 128-bitowa przestrzeń adresowa, a adresy są zwykle zapisane w formacie szesnastkowym. Adres tworzy osiem bloków w formacie `nnnn:nnnn:nnnn:nnnn:hhhh:hhhh:hhhh:hhhh`, gdzie `n` oznacza identyfikator sieci, natomiast `h` to identyfikator urządzenia sieciowego. Istnieją różne sposoby przedstawiania adresów IPv6. Wersja IPv6 jest konfigurowana automatycznie i pozwala na stosowanie wielu adresów dla każdego interfejsu sieciowego. Adresy są umieszczane w zakresach i należą do poszczególnych stref.

Zmniejszona wielkość nagłówka IPv6 oraz funkcje dodatkowe wbudowane do protokołów IPv6 i ICMPv6 powodują, że protokół IPv6 jest łatwiejszy do implementacji w sieciach. Funkcja określania dostępności sąsiednich węzłów (ang. *Neighbor Discovery*) powoduje, że szczególnie wygodne stało się tworzenie sieci ad hoc, przeglądanie ich oraz optymalizowanie routera.

Adresy dostępne w protokole IPv4 najprawdopodobniej wyczerpią się w roku 2011, więc zaadaptowanie protokołu IPv6 jest nieuniknione.

## Ogólny opis protokołu IP

Protokół IP to protokół warstwy sieciowej odpowiedzialny za utrzymanie i obsługę punktów końcowych połączenia internetowego. IP definiuje schemat adresowania, hermetyzuje dane w formacie datagramu, który jest transportowany poprzez sieć. Protokół IP jest protokołem bezpołączeniowym. Oznacza to, że chociaż punkty końcowe połączenia są znane i mogą być rzeczywiste bądź wirtualne, to trasy między tymi punktami końcowymi pozostają niezdefiniowane.

Ponieważ protokół IP nie ma żadnych żądań dotyczących połączenia poza tym, aby pakiety zostały dostarczone bez błędów, to ruch IP może przepływać przez różne rodzaje sieci oraz dostosowywać się do warunków sieciowych, zmieniając trasę, gdy będzie to konieczne. Protokół IP został zaprojektowany do działania w sieciach rozległych, operujących na pakietach opartych na Ethernetie, ATM, FDDI, sieciach bezprzewodowych 802.11x i w różnych systemach autonomicznych (AS). Protokół może przetrwać atak nuklearny, po którym ogromny odsetek sieci będzie nieużyteczny. Istnieją trzy zdefiniowane rodzaje systemów autonomicznych:

- ♦ **Multihomed.** System autonomiczny ma co najmniej dwa niezależne połączenia z innymi systemami autonomicznymi, ale nie przesyła ruchu pomiędzy nimi.
- ♦ **Stub.** System autonomiczny ma jedno połączenie z innym systemem autonomicznym.
- ♦ **Transit.** System autonomiczny ma co najmniej dwa niezależne połączenia z dwoma różnymi systemami autonomicznymi i przesyła ruch pomiędzy nimi.

Zgodnie z pierwotnymi wyobrażeniami internet miał za zadanie połączyć pewną liczbę różnych sieci w grupę routingu, każda z tych sieci miała mieć unikalny prefiks. Każdy prefiks routingu oraz zdefiniowane przez niego drzewo hierarchii miały być zarządzane przez dostawców usług internetowych (ISP, ang. *Internet Service Provider*) lub inną jednostkę wyposażoną w wiele niezależnych połączeń z siecią złożoną i zarejestrowany numer ASN (ang. *Autonomous System Number*) w bazie IANA ASN (dla Europy funkcje przydzielania i utrzymywania ASN sprawuje RIPE, <http://ripe.net>). Protokół BGP (ang. *Border Gateway Protocol*) wykorzystuje 16-bitową przestrzeń adresową dla numerów ASN. Daje to 65 535 numerów ASN używanych do kierowania ruchu do każdej sieci w internecie. Dla ASN zakłada się następujące przypisanie:

- ♦ **0.** Zarezerwowane dla sieci nieroutowalnych albo do użytku lokalnego.
- ♦ **1 – 54271.** Te wartości są przyznawane przez odpowiednie instytucje.
- ♦ **54272 – 64511.** Wartości zarezerwowane dla IANA i nie mogą być routowane.

Zostały rozdzielone już wszystkie adresy, więc w celu dalszego wzrostu potrzebna jest większa przestrzeń adresowa. Zaadaptowano 32-bitową przestrzeń adresową, w której na początku oryginalnej przestrzeni adresowej umieszczane jest 16-bitowe słowo w postaci `nowy.stary`. W nowym schemacie, zaadaptowanym w roku 2007, stare przypisanie 12345 ma postać 0.12345. Rozszerzona 32-bitowa przestrzeń nazw rezerwuje numery ASN 1.stary i 65535..65535. Wszystkie pozostałe są dostępne.

Sieci IP są routowalne i wykorzystują protokoły routingu: IGP (ang. *Interior Gateway Protocol*) lub EGP (ang. *Exterior Gateway Protocol*). Decyzja o kierunku przekazania pakietów jest podejmowana na poziomie każdego routera i potencjalnie każdego urządzenia bądź komputera w sieci.



Szczegółowe omówienie routingu IP znajduje się w rozdziale 9.

W zależności od wybranego adresu docelowego ruch sieciowy IPv4 może mieć postać emisji pojedynczej, rozgłaszania lub multemisji. Ich przeznaczenie jest następujące:

- ♦ **Emisja pojedyncza.** Pakiet emisji pojedynczej to taki, który zawiera pojedynczy adres docelowy, na przykład 4.2.2.1. To może być żądanie DNS do serwera, na przykład Verizon.net DNS, używanego przez daną sieć.
- ♦ **Multemisja.** Pakiety multemisji są powielane w routerze i wysyłane do różnych miejsc docelowych. Zakres adresów IPv4 zarezerwowanych dla multemisji to od 224.0.0.0 do 239.255.255.255.
- ♦ Zakres od 224.0.0.0 do 224.0.0.255 został zarezerwowany dla multemisji adresów lokalnych dla łącza — to znaczy adresów, które są połączone z protokołami warstwy danych, ale nie są poddawane routingu. Zazwyczaj adresy lokalne dla łącza są automatycznie konfigurowane i znajdują się w tej samej podsieci.
- ♦ **Rozgłaszanie.** Czasami zachodzi potrzeba rozgłoszenia pakietu do każdego komputera w sieci (w rzeczywistości w lokalnej podsieci). W tym celu należy wysłać wiadomość do adresu 255.255.255.255. Rozgłaszanie jest przeprowadzane w trakcie operacji zapytywania, żądania usługi oraz innych.
- ♦ **Rozgłaszanie kierunkowe.** Jeżeli zachodzi potrzeba przeprowadzenia rozgłaszania do określonej podsieci, która jest inna niż wysyłający komputer macierzysty, to wiadomość należy wysłać na adres `###.###.###.255`.

Cztery omówione powyżej formy routingu IPv4 zostały pokazane na rysunku 18.1.

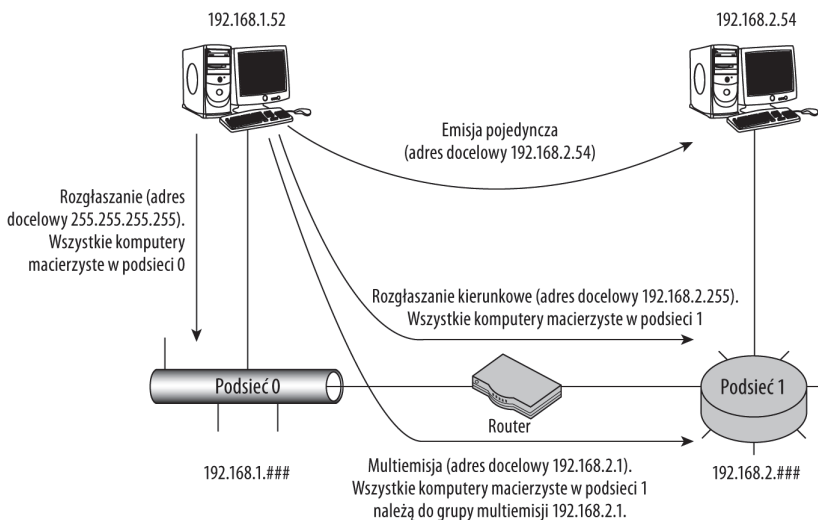
## Protokół Internet Protocol Version 4 (IPv4)

Pierwsza wersja protokołu Internet Protocol (IPv4) jest dominującym standardem. Protokół ten można rozpoznać po użyciu adresów składających się z czterech oktetów `###.###.###.###`, co czasami jest nazywane zapisem dziesiętnym z kropkami.

Warto zapoznać się z prostym przykładem pokazującym sposób adresowania w IPv4. Po wydaniu polecenia `ping` witrynie [www.nytimes.com](http://www.nytimes.com) adres serwera WWW witryny New York Times zostanie określony jako 199.239.136.200. Po uruchomieniu przeglądarki internetowej,

**Rysunek 18.1.**

Cztery rodzaje routingu IPv4



na przykład Microsoft Internet Explorer, i wprowadzeniu podanego adresu zostanie wyświetlona witryna internetowa New York Times. Adresy IP w formacie zapisu dziesiętnego z kropkami można skonwertować na inne formaty, na przykład szesnastkowy z kropkami, ósemkowy z kropkami, szesnastkowy, dziesiętny i ósemkowy. Wartość w notacji dziesiętnej odpowiadająca witrynie *nytimes.com* to 3354364104. Po wprowadzeniu podanej wartości w pasku adresu przeglądarki internetowej nastąpi wyświetlenie witryny internetowej New York Times. Większość przeglądarek internetowych prawidłowo interpretuje adresy IP podane w wymienionych formatach alternatywnych.

## Adresowanie IPv4

Schemat adresowania oktetów w IPv4 definiuje 32-bitową przestrzeń adresową. Każda z czterech liczb adresu może mieć wartość od 0 do 255 ( $2^8$ ), co oznacza ograniczenie do 4 294 967 296 unikalnych adresów przestrzeni adresowej. Kiedy projektanci opracowywali protokół IP, nawet nie przypuszczali, jaką popularność może on zdobyć. Dostępność niemal czterech miliardów adresów wydawała się wystarczająca. W chwili ustanowienia protokołu IPv4, w roku 1980, wielkość populacji na świecie wynosiła około 4,5 miliarda osób. Standard pozwalał więc, aby każda osoba na świecie miała swój adres IPv4. W erze, kiedy lodówka, toster, sensor i niemal wszystko, o czym można pomyśleć, ma możliwość pobrania adresu IP, dni protokołu IP wersji IPv4 są policzone (jeśli można tak powiedzieć). Problem ten nosi nazwę wyczerpania puli adresów IP. Dla porównania protokół IPv6 dysponuje 128-bitową przestrzenią adresową, która definiuje  $3,4 \times 10^{38}$  unikalnych numerów.

Protokół IPv4 został zdefiniowany w dokumentach IETF RFC 791 i MIL-STD-1777.



Aby rozwiązać problem wyczerpywania puli adresów IPv4, wprowadzono trzy różne rozszerzenia adresowania IP:

- ♦ CIDR (ang. *Classless Inter-Domain Routing*);
- ♦ VLSM (ang. *Variable Length Subnet Masks*);

- ♦ maskowanie podsieci.

Wymienione technologie są omówione w rozdziale.

## Podział przestrzeni nazw

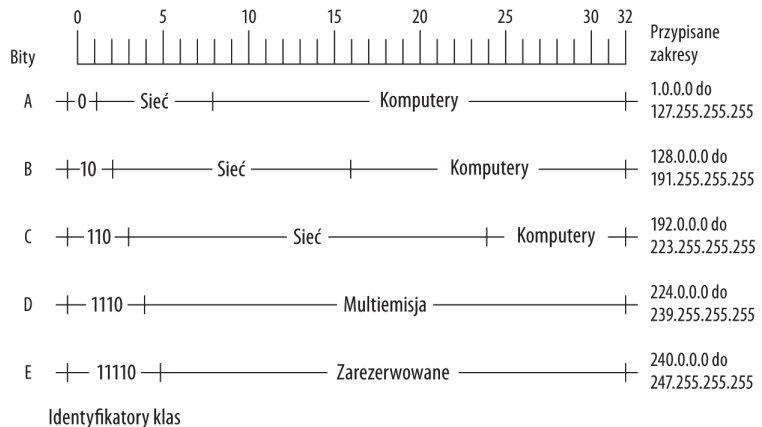
We wczesnych latach osiemdziesiątych, kiedy protokół IP był opracowywany, oryginalna przestrzeń nazw składała się z identyfikatora sieci, którym był pierwszy oktet adresu. Następnie znajdował się identyfikator komputera w postaci trzech kolejnych oktetów, łącznie były więc cztery oktety. Oryginalny schemat pozwalał na utworzenie sieci o numerach od 0 do 255, czyli łącznie 256 sieci.

## Klasy

Wraz z zaistnieniem konieczności utworzenia większej liczby sieci projektanci IP zdali sobie sprawę, że choć niektóre sieci mogą być ogromne, to większość będzie mała, natomiast tylko część będzie średniej wielkości. Schemat adresowania został zmieniony w taki sposób, aby liczba oktetów definiujących identyfikator sieci mogła wahać się od jednego do trzech, natomiast liczba oktetów przypisanych identyfikatorom komputerów wynosiła od trzech do jednego. Sieć wymagająca tylko jednego oktetu dla identyfikatora sieci pozwala na użycie  $2^{24}$  (16 777 216) adresów. Sieć z dwoma oktetami dla identyfikatora sieci pozwala na użycie  $2^{16}$  (65 536) adresów, a małe sieci, w których do zdefiniowania identyfikatora sieci używane są trzy oktety, pozwalają na wykorzystanie jedynie  $2^8$  (256) adresów. To jest źródło, z którego wywodzi się notacja klas sieciowych. Początkowe przypisania klas od A do E zostały pokazane na rysunku 18.2.

**Rysunek 18.2.**

*Początkowe przypisania klas sieciowych w IPv4*



Zadaniem klas była alokacja bloków adresów dla organizacji na podstawie ich wielkości oraz rodzaju ruchu przechodzącego przez sieć (emisja pojedyncza albo multiemisja). Tak więc zestaw kolejnych adresów sieciowych mógł zostać rozdzielony między organizacje takie jak AOL, podczas gdy mniejsze zestawy adresów sieciowych mogły zostać rozdzielone między firmy XYZ. Wymienione klasy nie są obecnie używane, ale często pojawiają się w podręcznikach i książkach poświęconych sieciom ze względu na ich historyczne znaczenie. W niektórych przypadkach klasy są używane do opisanie pewnej liczby adresów w podsieci, na co pozwala maska sieciowa; będzie to omówione w dalszej części rozdziału. W tabeli 18.1 wymieniono różne typy klas zdefiniowane w dokumencie RFC 791.

**Tabela 18.1.** *Typy klas sieci*

Klasa	Bity początkowe	Adres początkowy	Adres końcowy (blok routingu CIDR)	Domyślna maska podsieci
Klasa A	0	0.0.0.0	127.255.255.255 (/8)	255.0.0.0
Klasa B	10	128.0.0.0	191.255.255.255 (/16)	255.255.0.0
Klasa C	110	192.0.0.0	233.255.255.255 (/24)	255.255.255.0
Klasa D (multiemisja)	1110	224.0.0.0	239.255.255.255 (/4)	N/D
Klasa E (zarezerwowana)	11 110	240.0.0.0	255.255.255.255 (/4)	N/D

Źródło: <http://tools.ietf.org/html/rfc791>.

## CIDR (Classless Inter-Domain Routing)

Klasy straciły na znaczeniu, kiedy internet stał się narzędziem publicznym, a przestrzeń adresowa musiała zostać pofragmentowana i podzielona na miliony kawałków. Ostatecznie klasy oddały pola temu, co obecnie nazywamy CIDR (ang. *Classless Inter-Domain Routing*), i blokom adresów rozdzielonych między organizacje oraz dostawców internetu (ISP) różnych wielkości. W opublikowanym przez IETF w roku 1993 (dokument RFC 1518) schemacie routingu CIDR adresy IP są przypisane w strukturze hierarchicznej, która pozwala na ich przekierowanie do poprawnej sieci. Ponadto nastąpi przejście do odpowiedniego komputera, jeżeli adres pozwala na routing.

Technologia CIDR znosi ściśle ograniczenie wprowadzone przez klasy; sieci mogą być segregowane na podstawie systemu oktetów, co znacznie ułatwia kierowanie ruchem w internecie. Powstały w ten sposób system nosi nazwę VLSM (ang. *Variable Length Subnet Mask*) i pozwala, aby ciągle podsieci były agregowane na postać nadsieci. Agregacja powoduje, że dostępne adresy są wykorzystywane w sposób bardziej optymalny. Ponadto, co jest równie ważne, zmniejsza liczbę wpisów routera przez ukrycie wszystkich podsieci w ramach nadsieci VLSM w pojedynczym wpisie w tabeli routingu.

Schemat CIDR dzieli przestrzeń adresową IPv4 na bloki, które mogą być rozdzielane, i je reprezentuje. Każdy blok jest zdefiniowany przez dołączenie do adresu IP binarnej reprezentacji maski w postaci ###.###.###.###/N, gdzie N jest liczbą od 0 do 32 (w przypadku protokołu IPv6 zakres numerów to od 0 do 128). Liczba ta przedstawia ilość bitów w adresie IP reprezentujących podsieć, pozostałe bity określają ilość adresów w bloku (danej podsieci). Im ta liczba jest większa, tym mniejszy zakres adresów znajduje się w bloku.

W celu ustalenia ilości adresów w bloku (podsieci) należy użyć następującego wzoru:  $2^{32-N}$ , dla N równego 24 otrzymujemy  $2^8$ , czyli 256 adresów, dla N równego 18 otrzymujemy  $2^{14}$ , czyli 16 384 adresy w bloku. Po wprowadzeniu adresu 199.239.136.200/24 blok CIDR będzie zawierał wszystkie adresy od 199.239.136.0 do 199.239.136.255. Z kolei adres 199.239.136.200/28 jest adresem w bloku o adresach od 199.239.136.192 do 199.239.136.207; dowolny adres spoza tego bloku, np. 199.239.136.217, znajduje się poza blokiem (podsiecią).

W tabeli 18.2 przedstawiono konwersję klas na prefiksy bloków CIDR. Czytelnik może się więc samodzielnie przekonać, jak przypisanie VSLM pozwala na zastosowanie efektywnych przypisań w bloku każdego rodzaju.

**Tabela 18.2.** *Wielkości bloków CIDR*

Prefiks bloku CIDR	Odpowiednik klasy	Unikalne węzły
/32	1/256 klasy C	1
/31	1/128 klasy C	2
/30	1/64 klasy C	4
/29	1/32 klasy C	8
/28	1/16 klasy C	16
/27	1/8 klasy C	32
/26	1/4 klasy C	64
/25	1/2 klasy C	128
/24	Klasa C	256
/23	2 klasy C	512
/22	4 klasy C	1024
/21	8 klas C	2048
/20	16 klas C	4096
/19	32 klasy C	8192
/18	64 klasy C	16 384
/17	128 klas C	32 768
/16	256 klas C lub 1 klasa B	65 536
/15	512 klas C lub 2 klasy B	131 072
/14	1024 klasy C lub 4 klasy B	262 144
/13	2048 klas C lub 8 klas B	524 288
/12	4096 klas C lub 16 klas B	1 048 576

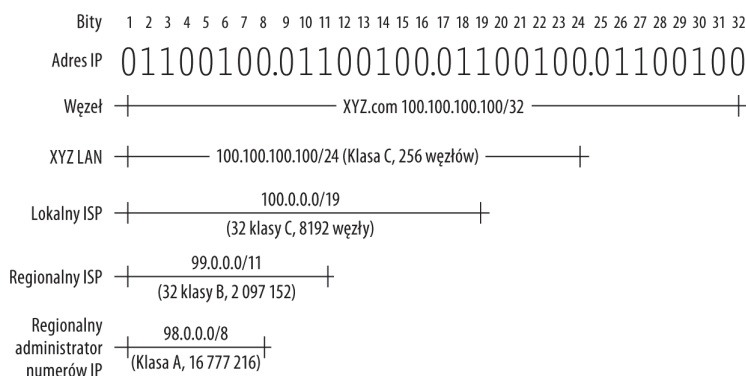
Bloki mniejsze niż /27 zwykle nie są przypisywane przez ISP. Bloki większe niż /13 są zarezerwowane dla regionalnych administratorów numerów IP.

Wraz z przypisaniami bloku CIDR nie jest już konieczne przechowywanie tras do poszczególnych komputerów w routerach internetowych. Przy wykorzystaniu mechanizmu agregacji trasy są sumowane do pojedynczych wpisów. W przypadku posiadania czterech kolejnych tras do podsieci /26 (zawartych w jednej sieci /24), które w danej tablicy routingu wskazują ten sam interfejs wyjściowy, możemy dokonać agregacji i pozostawić jedną trasę /24.

Jeżeli chodzi o większe sieci, rozważymy adres `###.###.0.0/16`, który używa maski podsieci w postaci `255.255.0.0`. Zapis `/16` oznacza, że sieć jest odpowiednikiem 256 ciągłych klas C lub jednej klasy B i definiuje przestrzeń adresową wraz z 65 536 komputerami. Pojedynczy wpis routera `200.100.0.0/16` jest wystarczający do przedstawienia wszystkich wspomnianych komputerów. Bardzo łatwo można dostrzec, jaką elastyczność i ekonomiczność oferuje ten system. Taka agregacja zmniejszyła wielkość światowych tabel routingu do około 35 000 wpisów. Na rysunku 18.3 pokazano hipotetyczny schemat agregacji adresów IPv4.

### Rysunek 18.3.

Agregacja nazw IP  
za pomocą schematu  
CIDR



## Regionalni administratorzy numerów IP

Internet jest podzielony na kilka regionów geograficznych; każdy ma własne duże zakresy, które następnie są dzielone na mniejsze. Taka hierarchia wycofuje większość wpisów, które by istniały w przypadku niezdefiniowania nadsieci. Pozwala również na bardzo efektywny routing na podstawie zarówno adresu, jak i położenia geograficznego.

Adresy IP są kontrolowane przez organizację IANA (ang. *Internet Assigned Numbers Authority*), a poszczególne zakresy adresów są zarządzane przez organizacje regionalne (zob. rysunek 18.4). Regionalni administratorzy (ang. *Regional Internet Registries*, RIR) przyznają adresy IP dostawcom internetu, instytucjom i organizacjom na terenie swojej działalności. Utrzymują także listę przypisań adresów powiązaną z numerami systemów autonomicznych (ASN); uzupełnieniem jest baza `whois`, pozwalająca na określenie, komu został przypisany dany adres IP. Do usług oferowanych przez RIR zaliczamy między innymi:

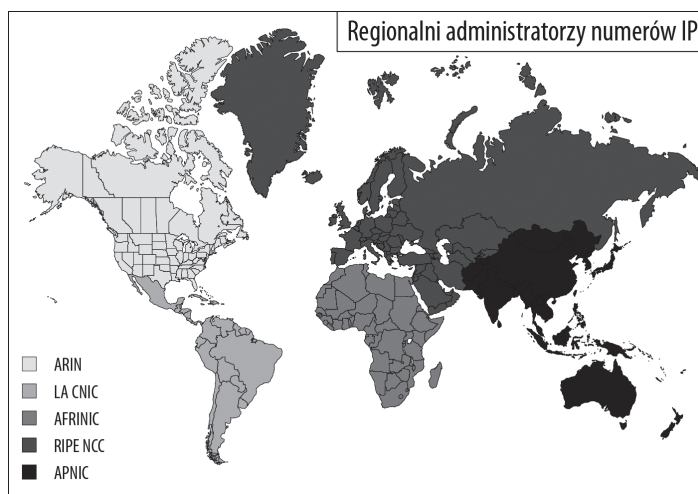
- ♦ alokację adresów IPv4 i IPv6;
- ♦ utrzymanie i rozwijanie bazy danych `whois`;
- ♦ przydział numerów ASN;
- ♦ utrzymanie i rozwój baz trasowania;
- ♦ utrzymanie głównych serwerów DNS.

Skróty użyte na rysunku 18.4 oznaczają:

- ♦ **ARIN** — American Registry for Internet Numbers (Ameryka Północna);
- ♦ **LA CNIC** — Latin American and Caribbean Internet Address Registry (Ameryka Łacińska i Karaiby);
- ♦ **AFRINIC** — African Network Information Centre (Afryka);

**Rysunek 18.4.**

Obecny podział  
regionalnych  
administratorów  
adresów IP



- ♦ **RIPE NCC** — Ripe Network Coordination Centre (Europa, Bliski Wschód oraz centralna Azja);
- ♦ **APNIC** — Asia-Pacific Network Information Centre (Azja i Pacyfik).



Przypisanie adresów IP w RIR są odrębne od nazw domen, które są rejestrowane przez ICANN.

## Adresy zarezerwowane

Nie wszystkie adresy IPv4 są dostępne do użycia w sieci rozległej. Pewne zakresy są przeznaczone do stosowania w sieciach prywatnych, podczas gdy inne pozostają zarezerwowane dla sieci multiemisyjnych. Różne adresy zarezerwowane przyjmują następujące formy:

- ♦ **(<ID\_sieci>, 0)**. Adres zarezerwowany dla nazwy sieci.
- ♦ **(<ID\_sieci>, -1)**. Wartość -1 oznacza, że wszystkie bity są zastępowane przez jedyńki. Adres rozgłoszeniowy w sieci.
- ♦ **(-1, -1)**. Adres zawierający same jedyńki jest adresem rozgłoszeniowym w sieci lokalnej.
- ♦ **(0, 0)**. Taki adres wskazuje, że system jest zarówno siecią lokalną, jak i systemem lokalnym — w szczególności jest to „ten komputer”. Adres jest napotykan, kiedy system wysyła żądania do serwera BOOTP w celu pobrania poprawnego adresu sieciowego. Jest również spotykany jako wpis w routerze, prowadzący do trasy domyślnej (nazywanej także bramą domyślną).
- ♦ **(0, <ID\_komputera>)**. Taki adres odnosi się do komputera, który jest przypisany do identyfikatora komputera w sieci lokalnej.
- ♦ **(127, <wszystko>)**. Taki adres przedstawia komputer lokalny; komunikacja z adresami z tego zakresu jest komunikacją w ramach jednego komputera.

Zgodnie z definicją w dokumencie RFC 1918 sieć prywatna nie może być używana w internecie i nie podlega routingu. Każdy pakiet pochodzący z urządzenia, którego adres mieści się w zakresie sieci prywatnej, będzie odrzucony przez router w internecie.

Większość sieci LAN w domach i biurach używa zakresu prywatnych adresów IP, zdefiniowanych dla IPv4 albo IPv6. Ruch sieciowy przychodzący do sieci prywatnej musi przejść przez bramkę lub serwer proxy, a przekazanie pakietów do właściwych adresów wymaga mechanizmu takiego jak NAT (Network Address Translation). Wykorzystanie NAT zmniejszyło, ale tylko na chwilę, presję przejścia na IPv6. Wraz z zapewnianiem przestrzeni adresów IPv4 sieci IP będą powoli przechodziły na drugą wersję protokołu, czyli IPv6.



Należy zachować szczególną ostrożność, kiedy dwie sieci (lub więcej) używają tej samej podsieci prywatnej, aby nie dochodziło do konfliktów.

Nazwa *localhost* określa interfejs sieciowy loopback w komputerze lokalnym. Zakres adresów karty loopback jest zakresem prywatnym. Nazwa *localhost* odwołuje się do adresu przypisanego urządzeniu, a dokładniej interfejsowi sieciowemu. Kiedy pakiety są kierowane (polecenie ping) do *localhost*, są zwracane wraz z adresem przychodzącym, który jest taki sam jak pakiety wychodzące, jakby podróżowały po sieci wirtualnej. Z tego powodu *localhost* odnosi się do interfejsu loopback w urządzeniu. Karta loopback jest wykorzystywana w celu sprawdzania działania interfejsu sieciowego. Najczęściej stosowany sposób sprawdzenia karty loopback polega na wydaniu polecenia ping 127.0.0.1. Organizacja IANA określiła także numery innych bloków, które są zarezerwowane do użytku prywatnego bądź do innych celów. Niektóre z zarezerwowanych bloków wymieniono w tabeli 18.3.

**Tabela 18.3.** Adresy zarezerwowane IANA

Blok adresu	Wielkość bloku (adresy)	Przeznaczenie	RFC
0.0.0.0/8	24 (16 777 216)	Sieć lokalna (używana lokalnie)	1700
10.0.0.0/8	24 (16 777 216)	Prywatne	1918
14.0.0.0/8	24 (16 777 216)	Publiczne (prywatne przed lutym 2008 roku)	1700
127.0.0.0/8	24 (16 777 216)	Loopback	3330
128.0.0.0/16	16 (65 536)	Zarezerwowane przez IANA	3330
169.254.0.0/16	16 (65 536)	Łącze lokalne	3927
172.16.0.0/16	16 (65 536)	Prywatne	1918
191.255.0.0/16	16 (65 536)	Zarezerwowane przez IANA	3330
192.0.0.0/24	8 (256)	Zarezerwowane przez IANA	3330
192.0.2.0/24	8 (256)	Dokumentacja i przykładowy kod	3330
192.88.99.0/24	8 (256)	Przekazywanie IPv6 – IPv4	3068
192.168.0.0/16	16 (65 536)	Prywatne	1918
198.18.0.0/15	17 (131 072)	Testowanie sieci	2544
223.255.255.0/24	8 (256)	Zarezerwowane przez IANA	3330
224.0.0.0/4	28 (268 435 456)	Multicast (klasa D)	3171
240.0.0.0/4	28 (268 435 456)	Zarezerwowane (klasa E)	1700
255.255.255.255	0 (1)	Rozgłaszanie	

Źródło: <http://www.iana.org>.

W przypadku starych klas sieciowych adres kończący się zerem był przypisany jako identyfikator sieci, podczas gdy adres kończący się liczbą 255 był zarezerwowany jako adres rozgłoszeniowy podsieci. Nie można było na przykład przypisywać adresów 192.168.0.0 i 192.168.0.255 dla bloku klasy C zdefiniowanego przez ten zakres.

Wraz z nadejściem schematu CIDR sytuacja uległa zmianie i tylko sieci posiadające maski między /24 (255.255.255.0) i /32 (255.255.255.255) powodują zarezerwowanie tych adresów. W podsieci definiującej ogromny blok muszą być zarezerwowane tylko pierwszy i ostatni adres. Dlatego też w przypadku bloku 100.100.0.0/16 maską podsieci będzie 255.255.0.0, a liczba dozwolonych adresów to 65 535 w zakresie od 100.100.0.0 do 100.100.255.255. W wymienionym zakresie adresy 100.100.0.0 i 100.100.255.255 muszą być zarezerwowane, ale wszystkie inne kończące się na zero lub 255 mogą być wykorzystane. Przykłady adresów dozwolonych w tym zakresie to 100.100.1.0 i 100.100.254.255.

## Adresowanie zero configuration

Adresy lokalne względem łącza są używane w sieciach lokalnych i nie podlegają routingu. Jeżeli stosowane jest dynamiczne przypisywanie IP z serwera DHCP, gdy serwer pozostaje niedostępny bądź nie może przypisać adresu, to pojawiają się adresy z zakresu od 169.254.0.0 do 169.254.255.255. W protokole IPv4 zakres adresów lokalnych względem łącza 169.254.0.0/16 jest przypisywany za pomocą mechanizmu o nazwie IPv4LL (ang. *IPv4 Link-Local*), który został zdefiniowany w dokumencie RFC 3927.

Powszechne jest posiadanie adresów lokalnych względem łącza, przeznaczonych do użytku lokalnego i przypisanych przez automatyczną usługę przypisywania za pomocą technologii, którą czasami nazywa się *Zero Configuration Networking*. Zeroconfig lub Zeroconf to usługa dostarczająca adresy IP w sieci bez konieczności używania jakiegokolwiek serwera, takiego jak DHCP lub BOOTP. Włączony Zeroconfig jest odpowiedzialny za następujące usługi:

- ♦ przypisanie urządzeniom sieciowym adresów lokalnych względem łącza;
- ♦ przeprowadzanie rozpoznawania nazw;
- ♦ oferowanie funkcji przeglądania sieci;
- ♦ automatyczne wykrywanie dostępnych usług sieciowych takich jak drukowanie.

Oferowana przez firmę Microsoft technologia wykrywania usług nosi nazwę *Simple Service Discovery Protocol* i stanowi część protokołu UPnP (ang. *Universal Plug and Play*). Natomiast technologia wykrywania usług oferowana przez firmę Apple to mDNS (*Multicast DNS/DNS-SD*). Ten obszar technologii nie został jeszcze ustandaryzowany, choć organizacja IETF zaproponowała standard o nazwie SLP (ang. *Service Location Protocol*), który pojawił się w systemach Linux i Solaris. Firmy Microsoft i Apple nadal korzystają z własnych technologii.

Czytelnik prawdopodobnie zna nazwy tych technologii. Wersja Zeroconfig oferowana przez Apple to Bonjour (poprzednio Apple Rendezvous). Z kolei schemat adresowania oferowany przez Microsoft nosi nazwę APIPA (ang. *Automatic Private IP Address*) lub IPAC (ang. *Internet Protocol Automatic Configuration*). W systemach Linux i BSD można zaimplementować Avahi, wersję technologii Bonjour.

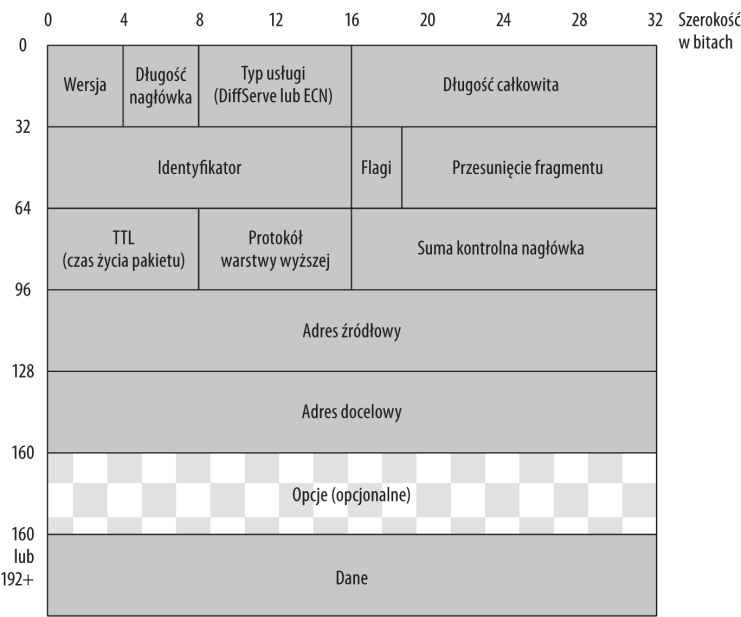
W ostatnim czasie stało się praktyką, że niektóre systemy adaptują do użytku prywatnego zakresy zarezerwowane przez IANA. Na przykład usługa Hamachi VPN dla swoich węzłów używa zakresu sieciowego 5.0.0.0/8. Ponieważ VPN to ruch hermetyzowany, adresy sieciowe są ukrywane w ramach pakietów poddawanych routingowi, a więc nie są ujawniane oraz odrzucane w internecie. Przy założeniu, że dwie sieci prywatne nie współdzielą tego samego zakresu adresów, nie powoduje to żadnych problemów, chociaż używanie adresów prywatnych IANA nie jest zalecane.

**Datagramy IP**

Nagłówek IP jest umieszczany na początku danych TCP i składa się z pewnej liczby standardowych pól identyfikujących źródło, przeznaczenie oraz format wykorzystanego protokołu IP. Wymagane jest użycie wszystkich trzynastu pól poza opcjonalnymi. Zgodnie z konwencją protokół IP zapisuje dane w formacie big endian. Wspomniany big endian to format używany przez procesory Sun SPARC oraz procesory firmy Motorola stosowane w starszych wersjach komputerów Macintosh. Architektura Intel X86 stosuje format little endian. Oznacza to, że kiedy dane protokołu IP są wysyłane bądź odbierane w systemie pracującym pod kontrolą procesora Intel, muszą zostać skonwertowane z big endian na little endian.

W formacie big endian najważniejszy bajt jest zapisywany jako pierwszy, więc liczby big endian mają kolejność bajtów od najwyższego.

**Rysunek 18.5.**  
*Struktura nagłówka IP*



Pola nagłówka IP są wykorzystywane w następujących celach:

- ♦ **Wersja.** To jest 4-bitowa wartość numeru wersji protokołu IP: 4 lub 6.
- ♦ **Długość nagłówka.** To pole uwzględnia użycie lub brak pola opcji i ustawia odpowiednią, całkowitą długość nagłówka. W połączeniu z polem „Przesunięcie fragmentu” pozwala na niezawodny odczyt porcji danych.

- ♦ **Typ usługi (DiffServe lub ECN).** To pole ma za zadanie wskazać typ metody *Quality of Service*. Aktualny sposób użycia pola TOS to przypisanie wartości DiffServe (ang. *Differentiated Services*) lub ECN (ang. *Explicit Congestion Notification*), która przydzieli priorytety IP w usługach strumieniowania mediów.

To 8-bitowe pole pozwala na określenie pierwszeństwa, opóźnień, przepustowości i niezawodności. Podczas wysyłania strumieniowanych danych zwiększa się znaczenie przepustowości, natomiast zmniejsza się niezawodność. W przypadku transferu plików można zastosować odwrotne ustawienia.

- ♦ **Długość całkowita.** Definiuje długość całego datagramu aż do wielkości  $2^{16}$  bajtów (65 535). Minimalna długość pakietu to 20 bajtów; jeśli pakiet wymaga więcej niż  $2^{16}$  bajtów, datagramy są dzielone na fragmenty.
- ♦ **Identyfikator.** Pole identyfikatora służy do ustalenia kolejności fragmentów podzielonego datagramu IP.
- ♦ **Flagi.** Istnieją trzy jednobitowe pola, które są ustawieniami flag. Pierwsze zawsze ma wartość zero, natomiast dwa kolejne wskazują możliwość podziału datagramu na mniejsze części (ang. *Don't Fragment*, czyli DF) i istnienie dodatkowych fragmentów (ang. *More Fragments*, czyli MF). Pole DF pomaga w routingu bądź wycofywaniu pakietów podzielonych na fragmenty. Kiedy dane są podzielone na fragmenty, wszystkie pakiety poza ostatnim muszą mieć wartość 1 w opcji MF.
- ♦ **Przesunięcie fragmentu.** To pole określa przesunięcie danych w stosunku do oryginalnej zawartości datagramu przed fragmentacją. W przypadku każdego podziału na fragmenty pierwszy pakiet ma w tym polu wartość zero. Pole pozwala na użycie trzynastu bitów 8-bitowych jednostek, czyli do 65 528 bajtów. Oznacza to 8192 fragmenty na datagram.
- ♦ **TTL (Time To Live).** To 8-bitowe pole TTL jest ograniczeniem informującym komputer bądź router, czy przekazywanie pakietu ma być kontynuowane. Początkowo to ustawienie odnosiło się do sekund, ale później zmieniono je na liczbę „skoków”, które może wykonać pakiet. Każde przejście pakietu przez router powoduje zmniejszenie wartości tego pola o jeden. Po osiągnięciu wartości zero pakiet jest porzucany przez router. Wygaśnięcie TTL powoduje, że ostatni komputer bądź router wysyła wiadomość ICMP, informującą o przekroczeniu wartości TTL przez pakiet.
- ♦ **Protokół.** IP może przenosić pewną liczbę odmiennych protokołów. To 8-bitowe pole zawiera numer protokołu zdefiniowany przez IANA. Niektóre z najczęściej stosowanych wartości to 0, IPv6 hop-by-hop; 1, ICMP (ang. *Internet Control Message Protocol*); 2, IGMP (ang. *Internet Group Management Protocol*); 6, TCP (ang. *Transmission Control Protocol*); 17, UDP (ang. *User Datagram Protocol*); 27, RDP (ang. *Reliable Datagram Protocol*); 89, OSPF (ang. *Open Shortest Path First*); 129, SMP (ang. *Simple Message Protocol*); i 133, FC (ang. *Fibre Channel*).
- ♦ **Suma kontrolna nagłówka.** To 16-bitowe pole zawiera sumę kontrolną, która jest dopasowywana podczas każdego przeskoku w trasie (ze względu na zmianę wartości w polu TTL nagłówka). Kiedy komputer bądź router odkryje, że suma kontrolna nie odpowiada obliczonej na podstawie zawartości nagłówka, to pakiet zostanie porzucony.

Algorytm sumy kontrolnej sprawdza każde 16-bitowe słowo w nagłówku, po pół słowa za jednym razem, pobiera resztę i sumuje całość w celu otrzymania wyniku. Otrzymany wynik jest następnie dopełniany i używany w sumie kontrolnej. Dopełnienie oznacza zamianę 1 na 0 i na odwrót.

- ♦ **Adres źródłowy.** To jest adres IPv4 zapisany w kodzie dwójkowym.

Konwersja adresu przebiega następująco: dla adresu 192.168.1.1 mamy cztery oktety dwójkowe 11000000.10101000.00000001.00000001, które wypełnią to 32-bitowe pole ciągiem tekstowym 1100000010101000000000000100000001.



Adres w polu adresu źródłowego to adres wysyłającego. Ten adres może być zmieniony przez mechanizm NAT (ang. *Network Address Translation*) na adres urządzenia dostarczającego NAT. Adres źródłowy można sfalszować także na wiele innych sposobów.

- ♦ **Adres docelowy.** Adres docelowy jest takim samym typem 32-bitowego adresu dwójkowego jak wprowadzony w polu adresu źródłowego.
- ♦ **Opcje.** W polu opcji można dodać do pakietu informacje dodatkowe. Pole to zostało dołączone w celu umożliwienia zmian i wprowadzania dodatków do protokołu IP. Może ono pozostać puste albo zawierać różne opcje. Każda opcja rozpoczyna się pojedynczym bajtem oznaczającym typ opcji, a następnie znajdują się dane opcji. Pole kończy się wartością 0x00, przedstawiającą EOL (ang. *End of Options List*). Wartość EOL jest wymagana tylko wtedy, kiedy pole opcji nie wypełnia nagłówka. Wynika to z faktu, że pole opcji musi być wielokrotnością czterech bajtów. W tabeli 18.4 wymieniono opcje. Wszystkie opcje, które nie są obsługiwane przez router bądź komputer, zostaną zignorowane.

Alternatywnym sposobem użycia pola opcji jest dołączenie zestawu opcji, które ustawiają poziom bezpieczeństwa, wskazują pełną ścieżkę (Strict Source Routing) lub wymagany zestaw routerów (Loose Source Routing), mają routery dodane do adresów w nagłówku (Record Route) i dodają znacznik czasu (Timestamp) do każdego dołączonego adresu routera. Te pola nie są już zalecane. Wymogi bezpieczeństwa w wielu nowoczesnych routerach powodują odrzucenie pakietów zawierających przestarzałe opcje.

- ♦ **Dane.** Są to dane datagramu przekazywane przez pakiet. Znajdują się w formie wskazywanej przez pole protokołu, najczęściej jako dane TCP lub UDP.

**Tabela 18.4.** *Opcje protokołu IP*

Pole	Bity	Przeznaczenie
Skopiowany	1	Wartość 1 oznacza, że pole opcji musi być umieszczone we wszystkich fragmentach pakietu.
Klasa opcji	2	Wartość 0 wskazuje opcję kontrolną, wartość 2 oznacza usuwanie błędów i pomiary, natomiast wartości 1 i 3 są zarezerwowane.
Numer opcji	5	Wskazuje opcję.
Długość opcji	8	Wielkość opcji wraz z polem długości. To pole nie zawsze jest używane.
Dane opcji	Zmienne	Dane opcji. To pole nie zawsze jest używane.

Pola Skopiowane, Klasa opcji oraz Numer opcji mogą być połączone w jedno ośmiobitowe pole o nazwie Typy opcji.

Różne obsługiwane typy protokołów zostały wymienione w tabeli 18.5.

**Tabela 18.5.** Numery protokołów zdefiniowane przez IANA

Dziesiątne	Słowo kluczowe	Protokół
0	HOPOPT	Opcja IPv6 Hop-by-Hop
1	ICMP	Internet Control Message Protocol
2	IGMP	Internet Group Management Protocol
3	GGP	Gateway-to-Gateway Protocol
4	IP	IP w IP (enkapsulacja)
5	ST	Internet Stream Protocol
6	TCP	Transmission Control Protocol
7	CBT	Core-based trees
8	EGP	Exterior Gateway Protocol
9	IGP	Interior Gateway Protocol (każdy, także prywatny — Cisco IGRP)
10	BBN-RCC-MON	BBN RCC Monitoring
11	NVP-II	Network Voice Protocol
12	PUP	PUP (PARC Universal Packet)
13	ARGUS	ARGUS
14	EMCON	EMCON
15	XNET	Cross Net Debugger
16	CHAOS	Chaos
17	UDP	User Datagram Protocol
18	MUX	Multipleksowanie
19	DCN-MEAS	Podsystemy pomiaru DCN
20	HMP	Host Monitoring Protocol
21	PRM	Packet Radio Measurement
22	XNS-IDP	XEROX NS IDP
23	TRUNK-1	Trunk-1
24	TRUNK-2	Trunk-2
25	LEAF-1	Leaf-1
26	LEAF-2	Leaf-2
27	RDP	Reliable Data Protocol
28	IRTP	Internet Reliable Transaction Protocol
29	ISO-TP4	ISO Transport Protocol Class 4

**Tabela 18.5.** Numery protokołów zdefiniowane przez IANA — ciąg dalszy

Dziesiętnie	Słowo kluczowe	Protokół
30	NETBLT	Bulk Data Transfer Protocol
31	MFE-NSP	MFE Network Services Protocol
32	MERIT-INP	MERIT Interodal Protocol
33	DCCP	Datagram Congestion Control Protocol
34	3PC	Third Party Connect Protocol
35	IDPR	Inter-Domain Policy Routing Protocol
36	XTP	Xpress Transport Protocol
37	DDP	Datagram Delivery Protocol
38	IDPR-CMTP	IDPR Control Message Transport Protocol
39	TP++	TP++ Transport Protocol
40	IL	IL Transport Protocol
41	IPv6	IPv6 (enkapsulacja)
42	SDRP	Source Demand Routing Protocol
43	IPv6-Route	Nagłówek Routing dla IPv6
44	IPv6-Frag	Nagłówek Fragment dla IPv6
45	IDRP	Inter-Domain Routing Protocol
46	RSVP	Resource Reservation Protocol
47	GRE	General Routing Encapsulation
48	DSR	Dynamic Source Routing
49	BNA	BNA
50	ESP	Encapsulating Security Payload
51	AH	Authentication Header
52	I-NLSP	Integrated Net Layer Security Protocol — TUBA
53	SWIPE	IP wraz z szyfrowaniem
54	NARP	NBMA Address Resolution Protocol
55	MOBILE	IP Mobility
56	TLSP	Transport Layer Security Protocol używający zarządzania kluczem Kryptonet
57	SKIP	Simple Key-Management for Internet Protocol
58	IPv6-ICMP	ICMP dla IPv6
59	IPv6-NoNxt	Nagłówek No Next dla IPv6

**Tabela 18.5.** Numery protokołów zdefiniowane przez IANA — ciąg dalszy

Dziesiątne	Słowo kluczowe	Protokół
60	IPvOpts	Opcje dotyczące przeznaczenia dla IPv6
61		Dowolny protokół wewnętrzny komputera
62	CFTP	CFTP
63		Dowolna sieć lokalna
64	SAT-EXPAK	SATNET i Backroom EXPAK
65	KRYPTOLAN	Kryptolan
66	RVD	MIT Remote Virtual Disk Protocol
67	IPPC	Internet Pluribus Packet Core
68		Dowolny rozproszony system plików
69	SAT-MON	SATNET Monitoring
70	VISA	VISA Protocol
71	IPCV	Internet Packet Core Utility
72	CPNX	Computer Protocol Network Executive
73	CPHB	Computer Protocol Heart Beat
74	WSN	Wang Span Network
75	PVP	Packet Video Protocol
76	BR-SAT-MON	Backroom SATNET Monitoring
77	SUN-ND	SUN ND PROTOCOL — tymczasowy
78	WB-MON	WIDEBAND Monitoring
79	WB-EXPAK	WIDEBANK EXPAK
80	ISO-IP	ISO Internet Protocol
81	VMTP	Versatile Message Transaction Protocol
82	SECURE-VMTP	SECURE-Versatile Message Transaction Protocol
83	VINES	VINES
84	TTP	TTP
85	NSFNET-IGP	NSFNET-IGP
86	DGP	Dissimilar Gateway Protocol
87	TCF	TCF
88	EIGRP	EIGRP
89	OSPFIGP	Open Shortest Path First

**Tabela 18.5.** Numery protokołów zdefiniowane przez IANA — ciąg dalszy

Dziesiętnie	Słowo kluczowe	Protokół
90	Sprite-RPC	Sprite RPC Protocol
91	LARP	Locus Address Resolution Protocol
92	MTP	Multicast Transport Protocol
93	AX.25	AX.25
94	IPIP	IP-within-IP Encapsulation Protocol
95	MICP	Mobile Internetworking Control Protocol
96	SCC-SP	Semaphore Communications Sec. Protocol
97	ETHERIP	Ethernet-within-IP Encapsulation Protocol
98	ENCAP	Encapsulation Header
99		Dowolny prywatny schemat szyfrowania
100	GMTP	GMTP
101	IFMP	Ipsilon Flow Management Protocol
102	PNNI	PNNI poprzez IP
103	PIM	Protocol Independent Multicast
104	ARIS	Aggregate Route IP Switching Protocol
105	SCPS	Space Communication Protocol Standards
106	QNX	QNX
107	A/N	Active Networks
108	IPComp	IP Payload Compression Protocol
109	SNP	Sitara Networks Protocol
110	Compaq-Peer	Compaq Peer Protocol
111	IPX-in-IP	IPX w IP
112	VRRP	Virtual Router Redundancy Protocol
113	PGM	PGM Reliable Transport Protocol
114		Dowolny protokół „0-hop”
115	L2TP	Layer Two Tunneling Protocol
116	DDX	D-II Data Exchange (DDX)
117	IATP	Interactive Agent Transfer Protocol
118	STP	Schedule Transfer Protocol
119	SRP	SpectraLink Radio Protocol
120	UTI	UTI

**Tabela 18.5.** Numery protokołów zdefiniowane przez IANA — ciąg dalszy

Dziesiętnie	Słowo kluczowe	Protokół
121	SMP	Simple Message Protocol
122	SM	SM
123	PTP	Performance Transparency Protocol
124	ISIS over IPv4	IS-IS przez IPv4
125	FIRE	
126	CRTP	Combat Radio Transport Protocol
127	CRUDP	Combat Radio User Datagram
128	SSCOPMCE	
129	IPLT	
130	SPS	Secure Packet Shield
131	PIPE	Enkapsulacja prywatnego IP w ramach IP
132	SCTP	Stream Control Transmission Protocol
133	FC	Fibre Channel
134	RSVP-E2E-IGNORE	
135	Mobility Header	
136	UDPLite	UDP Lite
137	MPLS-in-IP	MPLS przez IP
138	manet	MANET Protocol
139	HIP	Host Identity Protocol
140	Shim6	Site Multihoming za pośrednictwem IPv6
141 – 252		Nieprzypisane
253		Używany do eksperymentów oraz podczas testowania
254		Używany do eksperymentów oraz podczas testowania
255	Zarezerwowany	

W trakcie transportu pakietów IPv4 poprzez sieć nagłówki pakietów są weryfikowane za pomocą sumy kontrolnej. Jeżeli nagłówek nie przejdzie weryfikacji, pakiet będzie odrzucony. W większości przypadków nic więcej się nie zdarzy, a nadawca ponownie wyśle pakiet po otrzymaniu od odbiorcy wiadomości o niedotarciu poprzedniego pakietu (funkcja warstwy transportowej). Gdy stosowane są metody *Quality of Service*, istnieje możliwość użycia protokołu ICMP (ang. *Internet Control Message Protocol*) w celu zasygnalizowania odrzucenia pakietu.

## Tworzenie podsieci

Kiedy firma XYZ otrzyma blok adresów IPv4, adresy te staną się logicznymi jednostkami, przede wszystkim wskaźnikami do komputerów, które zostały przypisane do otrzymanych adresów. Problem związany z takim podejściem polega na tym, że wiele sieci składa się z różnych części, fizycznie znajdujących się w oddzielnych sieciach, ze względu na położenie geograficzne, na połączenia o niskiej przepustowości czy zróżnicowaną politykę bezpieczeństwa dla odrębnych grup użytkowników. Wszystkie wymienione czynniki są powodami stosowania podziału sieci.

Wydzielona część sieci nosi nazwę podsieci. Podsieci są tworzone przez zastosowanie „masek podsieci” względem bloku adresów. Maskę podsieci pozwala wyodrębnić z adresu IP część określającą adres sieci, stałą dla danej podsieci, i część zmienną w ramach podsieci, określającą adresy urządzeń. To prosty i elegancki system podziału sieci.

Przeanalizujemy teraz powszechnie spotykany przykład, który prawdopodobnie jest znany Czytelnikowi. Dotyczy bloku adresów, który kiedyś został nazwany klasą C sieci, składającego się z 256 ciągłych adresów sieciowych. Większość sieci prywatnych jest skonfigurowana dla tej wielkości sieci. W sieci prywatnej o zakresie od 192.168.1.0 do 192.168.1.255, która w technologii CIDR jest określana jako 192.168.1.0/24, maska podsieci ma wartość 255.255.255.0. Maskę pozwala na użycie dla komputera dowolnej z 256 wartości dostępnych dla ostatniego oktetu. Przyjmijmy założenie, że zadanie polega na utworzeniu w podanym zakresie dwóch oddzielnych podsieci o takiej samej wielkości. W tym celu w systemach można zastosować maskę podsieci 255.255.255.128. Każdy adres znajdujący się w zakresie od 0 do 127 będzie należał do podsieci 1., natomiast każdy adres w zakresie od 128 do 255 będzie zaliczał się do podsieci 2. Można to zweryfikować przez wprowadzenie odpowiednich informacji na witrynie <http://subnet-calculator.com>.



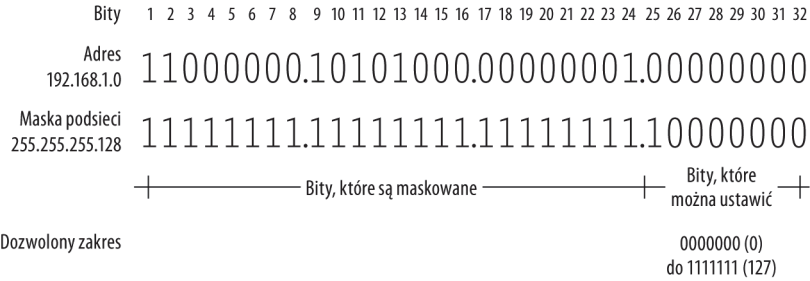
Dostępny na witrynie <http://subnet-calculator.com> kalkulator podsieci może być używany do obliczania masek podsieci, bitów, komputerów oraz innych czynników bądź do sprawdzania poprawności własnych obliczeń. Podana witryna oferuje także kalkulator CIDR.

Systemy w każdej podsieci pozostają niewidoczne dla pozostałych podsieci. Jednak wszystkie systemy są widoczne na zewnątrz sieci, niezależnie od zdefiniowanych podsieci. Z tego powodu tworzenie podsieci nie wymaga modyfikacji ustawień interfejsu sieciowego lub zmian rejestracyjnych w bazach danych adresów znajdujących się na zewnątrz względem danej sieci.

Zagadnienie tworzenia podsieci jest znacznie łatwiejsze, niż się wydaje na początku, o ile rozważy się adres zapisany binarnie. Na rysunku 18.6 pokazano omawiany przykład, zapisany w systemie dwójkowym. Warto zwrócić uwagę, że maska podsieci zmniejsza zakres adresów w ostatnim okciecie.

Jeżeli zachodzi potrzeba podziału sieci /24 na większą liczbę podsieci, można do tego celu zastosować wartości masek podsieci wymienione w tabeli 18.2. Każdy bit maskowany poza częścią adresu odpowiedzialną za identyfikację sieci jest określany mianem identyfikatora podsieci. Na rysunku 18.6 wartość identyfikatora podsieci wynosi 1. Z tabeli 18.6 wynika, że wartość identyfikatora dla maski podsieci 255.255.255.240 wynosi 4.

**Rysunek 18.6.**  
*Podział sieci /24  
na dwie identyczne  
podsieci*



**Tabela 18.6.** *Tworzenie podsieci sieci /24*

Ostatni oktet (dziesiętnie)	Ostatni oktet (dwójkowo)	Liczba unikalnych adresów <sup>1</sup>	Liczba możliwych podsieci	Efektywny CIDR
255	11111111	1	256	/32
254	11111110	2	128	/31
252	11111100	4	64	/30
248	11111000	8	32	/29
240	11110000	16	16	/28
224	11100000	32	8	/27
192	11000000	64	4	/26
128	10000000	128	2	/25
0	00000000	256	1	/24

<sup>1</sup> Liczba unikalnych adresów w przypadku podsieci musi być zredukowana o 2 adresy. Pierwszy adres jest zarezerwowany dla adresu sieci (adres identyfikujący tę podsieć), a ostatni jako adres rozgłoszeniowy tej podsieci. W tabeli podano pełną, niezredukowaną liczbę unikalnych adresów danej podsieci.

Podsieci są numerowane na podstawie długości maski podsieci i inkrementowane na podstawie liczby utworzonych podsieci. Kiedy nie ma zdefiniowanego identyfikatora sieci, sieć pozostaje nienaruszona i mamy wówczas do czynienia z siecią bazową. W klasie sieciowej C wraz ze zdefiniowanymi ośmioma podsieciami podsieci są oznaczone cyframi od 0 do 7, jak pokazano na rysunku 18.7.

Podczas tworzenia podsieci następuje modyfikacja tabeli routingu w celu uzupełnienia informacji o zmianach. W pakietach przychodzących adres docelowy jest porównywany z zawartością tabeli routingu. Wpisy w tabeli zawierają adresy sieci z maskami, do których są przypisane trasy wyjściowe. Dopasowanie najbliższe adresowi docelowemu powoduje skierowanie pakietu w odpowiednim kierunku.

## Ustawianie adresu IP

Bardzo ważna jest możliwość odnalezienia konfiguracji IP interfejsu sieciowego i jej zmiana, gdy znajdzie taka konieczność. Istnieje pięć podstawowych metod zmiany adresu IP urządzenia:

**Rysunek 18.7.**

*Schemat numerowania podsieci dla klasy C składającej się z ośmiu podsieci*

Adres bazowy	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	
(Podsieć 0) 192.168.1.0–31	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
(Podsieć 1) 192.168.1.32–63	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0
(Podsieć 2) 192.168.1.64–95	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
(Podsieć 3) 192.168.1.96–127	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0
(Podsieć 4) 192.168.1.128–159	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
(Podsieć 5) 192.168.1.160–191	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0
(Podsieć 6) 192.168.1.192–223	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0
(Podsieć 7) 192.168.1.224–255	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0

- ♦ **Interfejs wiersza poleceń.** Zmiana z poziomu interfejsu wiersza poleceń za pomocą polecenia takiego jak `ipconfig` w systemie Windows lub `ifconfig` w systemach Linux, Unix, Solaris i Macintosh.

W systemie Windows użycie opcji `/all` powoduje wyświetlenie pełnej informacji o adresach. Można użyć także innych opcji, na przykład `/release` lub `/renew`, które powodują zmianę dynamicznie przypisywanego adresu sieciowego. Więcej informacji o opcjach poleceń w systemie Windows można znaleźć w pomocy lub stosując opcję `/?`; w pozostałych systemach powinniśmy skorzystać z opcji `--help` lub pomocy na stronach `man` (`man ifconfig`).



Różne narzędzia wiersza poleceń rzadko pokazują informacje o strefach adresu IPv6, o ile takie strefy zostały zdefiniowane.

- ♦ **Narzędzie graficznego interfejsu użytkownika.** Zwykle będzie to panel kontrolny, dostępny w niemal każdym graficznym systemie operacyjnym.
- ♦ **Menu lub systemy bazujące na przeglądarce internetowej.** Urządzenia takie jak routery, przełączniki sieciowe i urządzenia sieciowe korzystają z tego rodzaju systemów.
- ♦ **Usługa sieci dynamicznej, na przykład DHCP (wersja 4. lub 6.) albo BOOTP.** Wszystkie sieciowe urządzenia mają możliwość bycia klientami DHCP. Obsługa BOOTP jest zastrzeżona dla komputerów, w których ją włączono.
- ♦ **Protokół NDP (Neighbor Discovery Protocol) dla IPv6.** Ten protokół warstwy łączy wyszukuje inne węzły i połączenia IPv6 oraz określa adresy używane przez sąsiednie węzły. Ponadto ustala router i trasę, które najlepiej wykorzystać podczas komunikacji z nimi.

W dwóch kolejnych podrozdziałach zostaną omówione statyczne oraz dynamiczne adresowanie IP. Statyczny adres IP to taki, który wymaga ręcznej konfiguracji. Styczne adresy IP są wymagane przez określone rodzaje serwerów i mogą być stosowane w małych sieciach. Dynamiczne adresy IP są przypisywane przez odpowiednie protokoły, oferują dużą elastyczność i szerokie możliwości konfiguracji. Dynamiczne adresy IP są stosowane w sieciach, w których konieczne jest używanie puli adresów IP, w urządzeniach mobilnych oraz wielu innych przypadkach.

## Adresowanie statyczne

Styczny adres IP wymaga skonfigurowania go na urządzeniu. Pozostaje taki sam aż do ponownej konfiguracji. Pewne urządzenia sieciowe do prawidłowej pracy wymagają statycznego adresu IP. Do takich urządzeń zaliczamy między innymi serwery DHCP i DNS, bramy sieciowe, routery, serwery WWW oraz serwery domen. Wymienione systemy wymagają, aby urządzenia były zawsze dostępne pod tym samym adresem. Z punktu widzenia komputerów oraz innych urządzeń, które nie dostarczają usług, używanie adresowania statycznego nie przynosi istotnych korzyści.

W przypadku małych sieci z niewielką liczbą komputerów i urządzeń statyczna adresacja nie jest problematyczna. Nie występują żadne istotne przeciwwskazania do stosowania statycznych adresów IP.

W sieci domowej autora ustawione są następujące statyczne adresy IP:

- ♦ **ID komputera = 1.** Adres przypisany bramie sieciowej.
- ♦ **ID komputera = 2.** Adres przypisany do serwera DNS, gdy taki jest używany.
- ♦ **ID komputera = 3.** Adres przypisany do serwera domen, gdy taki jest używany.
- ♦ **ID komputera = 4 – 20.** Adresy przypisane do wszystkich pozostałych urządzeń.
- ♦ **ID komputera = 21 – 80.** Adresy przypisane klientom.
- ♦ **ID komputera = 81 – 99.** Adresy statyczne zarezerwowane dla urządzeń bezprzewodowych, takich jak punkty dostępowe.
- ♦ **ID komputera = 100 – 110.** Adresy przypisane interfejsowi sieciowemu TiVo.
- ♦ **ID komputera = 150 – 200.** Adresy z puli dynamicznych adresów IP, których może używać serwer DHCP.

Patrząc na przedstawiony schemat, można zauważyć, że chociaż statyczne adresy IP są wykorzystywane znacznie częściej, to autor jednak nie przydziela obsesyjnie wszystkim urządzeniom sieciowym takich adresów, a nawet do tego nie dąży. W sytuacjach, w których podłączamy do sieci nowe urządzenie lub z jakiegoś powodu istniejące utraci adres IP (na przykład podczas instalacji systemu operacyjnego), serwer DHCP zapewnia przypisanie adresu IP z dostępnej puli. Przedstawiony schemat sprawdza się u autora, ponieważ sieć jest mała. Jeżeli wystąpiłaby konieczność przypisywania 16 – 20 adresów sieciowych, to autor znacznie intensywniej wykorzystywałby serwer DHCP. Natomiast w ogromnych sieciach większość systemów ma przypisywane dynamiczne adresy IP.

Podsumowując, statyczne adresy IP są potrzebne:

- ♦ dla urządzeń wymagających niezmiennego adresu IP, takich jak routery;
- ♦ dla urządzeń sieciowych, które muszą być dostępne na zewnątrz danej sieci: serwerów WWW, serwerów poczty elektronicznej, serwerów FTP oraz innych aplikacji serwerowych;
- ♦ dla niektórych aplikacji usług w terminalu;
- ♦ w pewnych schematach licencjonowania, gdzie licencja jest powiązana z określonym adresem IP (bardzo rzadko);
- ♦ dla usług strumieniowania, w których punkty końcowe połączenia muszą być ustawione na stałe.

## Adresowanie dynamiczne

Nie trzeba używać statycznych adresów IP w przypadku komputerów, urządzeń sieciowych nieudostępniających usług w sieci, tzw. klientów, korzystających z usług takich jak przeglądanie zasobów internetu, wysyłanie i odbieranie wiadomości e-mail, używanie komunikatorów internetowych, pobieranie lub wysyłanie plików oraz podobne zadania. Dynamiczne adresowanie IP oferuje zaletę w postaci automatycznej konfiguracji adresu, która może być bardzo czasochłonnym procesem w większych sieciach. Uwalnia także administratora od konieczności pamiętania o zmianie konfiguracji podczas przenoszenia systemu z jednej podsieci do innej.

Wygoda wiąże się jednak z pewnymi wymaganiami. Usługa dynamicznego przydzielania adresów (DHCP) i usługa określania nazw (na przykład DNS) muszą działać przez cały czas, aby sieć funkcjonowała prawidłowo. Urządzenie otrzymuje adres IP na ściśle określony przez administratora DHCP czas dzierżawy.

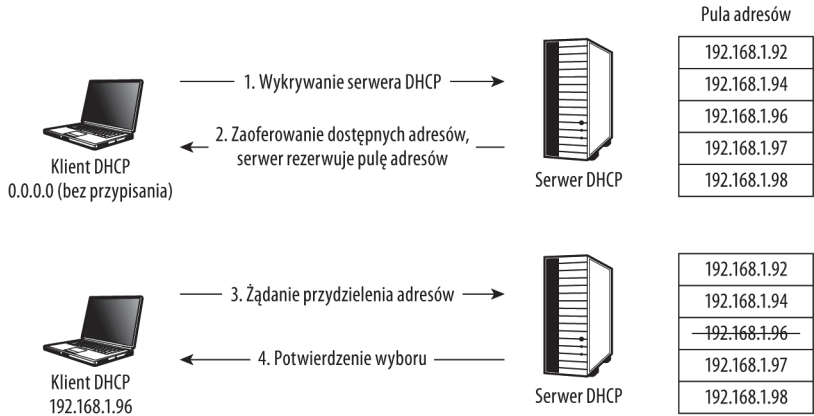
## Dynamic Host Configuration Protocol

DHCP (ang. *Dynamic Host Configuration Protocol*) to usługa, która przypisuje dynamiczne adresy IP klientom DHCP i zarządza nimi. Serwery DHCP znajdują się w przełącznikach sieciowych, routerach, urządzeniach sieciowych oraz wszystkich sieciowych systemach operacyjnych, które działają w serwerach bądź stacjach roboczych. Domyślnie usługa ta jest zwykle wyłączona, więc sieci nie mają problemów związanych z wieloma działającymi jednocześnie serwerami DHCP. W wielu przypadkach zachodzi także potrzeba włączenia DHCP po stronie klienta.

Po podłączeniu do sieci klient DHCP wysyła pakiet rozgłoszeniowy do sieci lokalnej. Adresatami są wszyscy użytkownicy danej sieci. Komunikat taki jest określany jako wykrywanie serwera DHCP. Na taki pakiet odpowiada tylko urządzenie z działającą usługą DHCP. W odpowiedzi serwer wysyła tzw. ofertę, na którą klient odpowiada następnym komunikatem z żądaniem. W ostatnim komunikacie (potwierdzeniu) serwer zatwierdza parametry. Od tego momentu klient może korzystać z adresów. Proces przyznawania adresu został zilustrowany na rysunku 18.8. Przypisany klientowi adres zostaje usunięty z puli adresów, co pokazuje przekreślony tekst na liście adresów znajdujących się w lewej dolnej części rysunku.

**Rysunek 18.8.**

Proces przyznawania adresu przez serwer DHCP



Konfiguracja DHCP dostarcza następujące informacje:

- ♦ adres IP;
- ♦ maska podsieci;
- ♦ nazwa domeny;
- ♦ adres serwera (serwerów) DNS;
- ♦ brama domyślna (router zewnętrzny, serwer proxy itd.).

## Konfiguracja

Jednym z parametrów konfigurowanych w serwerze DHCP jest okres ważności przydzielonego adresu. Okres dzierżawy może być długi — 30 dni to typowy okres w przedsiębiorstwach — lub krótki, często 48 godzin, podczas przypisywania adresu DHCP przez ISP klientowi zdalnemu przez połączenie szerokopasmowe, połączenie PPP (ang. *Point-to-Point Protocol*), komutowane bądź ISDN. W podanych odstępach czasu serwer pyta klienty o ich ustawienia DHCP lub klient zapytuje serwer w celu sprawdzenia, czy ustawienia nadal pozostają ważne. Jeżeli dzierżawa wygasła, serwer odświeża adres bądź oferuje klientowi inny.

Różne implementacje DHCP w odmienny sposób obsługują omówiony mechanizm. Dostawcy usług internetowych (ISP) obsługujący wielu zdalnych odbiorców wiążą ważność dzierżawy adresu z mechanizmem cyklicznie sprawdzającym, czy klient nadal jest aktywny.

Niektóre serwery DHCP obsługują funkcję nazywaną *alokacją statyczną*. W takim wypadku adresowi MAC klienta jest na stałe przydzielony adres IP. Klient taki zawsze podczas procedury pozyskiwania adresu z serwera DHCP otrzymuje ten sam adres IP. Pewne systemy robią tak automatycznie, inne wymagają ręcznego podania adresu MAC przez administratora. Alokacja statyczna nie jest funkcją standardową. Funkcja alokacji statycznej jest różnie określana przez różnych producentów, na przykład:

- ♦ Cisco (i teraz Linksys) nazywają ją Static DHCP;
- ♦ MAC/IP binding;
- ♦ Reserved IP Address (zob. rysunek 18.9) lub IP reservation.

**Rysunek 18.9.**

Strona  
konfiguracyjna DHCP  
w routerze/zaporze  
sieciowej Netgear  
FV318

**NETGEAR FV318 ProSafe VPN Firewall**

**settings**

- Setup Wizard
- VPN Wizard

**Setup**

- Basic Settings
- VPN Settings

**Security**

- Security Logs
- Block Sites
- Block Service
- Add Service
- Schedule
- E-mail

**Maintenance**

- Router Status
- Attached Devices
- Set Password
- Settings Backup
- Diagnostics
- Router Upgrade

**Advanced**

- Ports
- Dynamic DNS
- LAN IP Setup
- Static Routes
- Remote Management

**LAN IP Setup**

☐ Enable UPnP

**LAN TCP/IP Setup**

IP Address: 192 . 168 . 3 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: None

RIP Version: RIP-2B

MTU Size: ☒ Default ☐ Custom 1468

☒ Use router as DHCP server

Starting IP Address: 192 . 168 . 3 . 160

Ending IP Address: 192 . 168 . 3 . 199

WINS Server: 0 . 0 . 0 . 0

Lease Time: 72 /hours

**Reserved IP Addresses**

#	IP Address	MAC Address	Description
1	192.168.3.52	00:50:8D:B6:87:76	Barrie's workstation

Add Edit Delete

Apply Cancel

## Zabezpieczanie DHCP

Jak można zobaczyć na rysunku 18.9, wiele zapór sieciowych i routerów posiada funkcjonalność serwera DHCP. Serwery DHCP do komunikacji wykorzystują protokół UDP. Jeżeli zaporę sieciową bądź router mają świadczyć usługi dynamicznego przydzielania adresów, musimy pamiętać, aby była możliwość komunikacji z wykorzystaniem UDP dla portów:

- ♦ pakiety wysyłane przez serwer — port źródłowy 67, port docelowy 68,
- ♦ pakiety wysyłane przez klienta — port źródłowy 68, port docelowy 67.

Ten sam protokół warstwy transportowej i porty są używane przez protokół BOOTP.

## Protokół Bootstrap

Protokół BOOTP (ang. *Bootstrap Protocol*) jest poprzednikiem DHCP i działa na podobnych zasadach. BOOTP jest zgodny z DHCP i nadal pozostaje w użyciu. BOOTP przydziela adresy IP na żądanie podczas rozruchu systemu. DHCP najpierw wczytuje

system operacyjny, a następnie wysyła zapytanie o adres IP. Rozgłaszanie BOOTP następuje przez wysyłanie instrukcji z pamięci ROM (ang. *Read Only Memory*) interfejsu karty sieciowej (NIC) lub przez instrukcje z BIOS-u płyty głównej.

BOOTP jest znacznie łatwiejszy w obsłudze i wymaga niewielkiej (o ile w ogóle) konfiguracji w celu jego implementacji. W przeciwieństwie do usługi DHCP, pozwalającej na ponowną konfigurację po uruchomieniu systemu, BOOTP działa jedynie w trakcie fazy uruchamiania. Jest stosowany przede wszystkim w cienkich klientach serwerów terminali, gdzie klient jest pozbawioną dysku stacją roboczą, a system operacyjny jest wczytywany jako część procesu uruchamiania po otrzymaniu adresu.

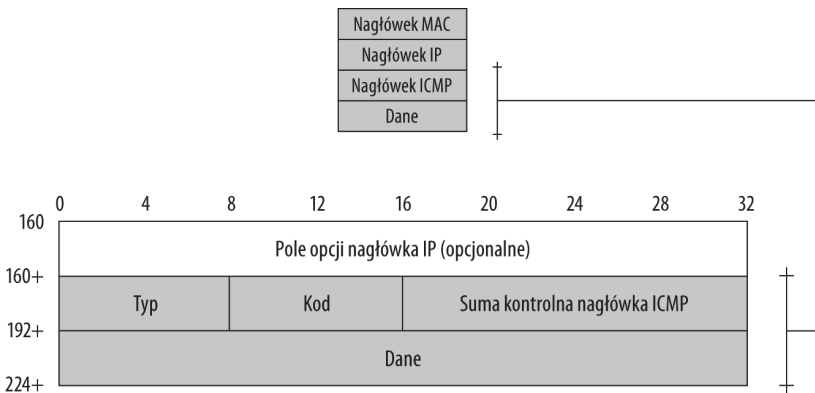
# Protokół Internet Control Message Protocol

Protokół ICMP (ang. *Internet Control Message Protocol*) obsługuje system wiadomości używanych do potwierdzania bądź żądania akcji i zdarzeń powiązanych z transferem danych IP. Jest bardzo ważny podczas kontrolowania ruchu i przeciążenia, sygnalizowania, czy pakiet dotarł prawidłowo, czy wymagane jest jego ponowne wysłanie oraz do kontrolowania routingu. Wygaśnięcie parametru TTL (ang. *Time To Live*) to jedno ze zdarzeń, które generuje wiadomość błędu ICMP.

Protokół ICMP jest wymagany do prawidłowego funkcjonowania protokołu IP. Nie zaleca się całkowitego blokowania protokołu ICMP. Istnieją dwie wersje tego protokołu, jedna dla IPv4 i druga dla IPv6. Wersja dla IPv6 zostanie przedstawiona pod koniec tego rozdziału.

Wiadomości ICMP są generowane z datagramów IP wymagających akcji ICMP. IP enkapsuluje nagłówek ICMP zawierający błąd i dodaje odpowiednie miejsce docelowe do pola wiadomości w nagłówku. ICMP jest protokołem zawodnym, nie gwarantuje dostarczania wiadomości. Typ wiadomości jest wskazywany przez pole umieszczone w nagłówku IP za bitem 160. bądź późniejszym, jeśli wypełnione zostało pole opcji nagłówka IP. Strukturę nagłówka ICMP pokazano na rysunku 18.10.

**Rysunek 18.10.**  
Struktura nagłówka ICMP



Podstawowe pola definiujące wiadomość ICMP to pola typu i kodu. Wymienione pola zostały ustandaryzowane przez organizację IANA i są wymienione w tabeli 18.7.

**Tabela 18.7.** Typy ICMP

Typ	Kod	Opis
0 — odpowiedź Echo (ang. <i>Echo Reply</i> )	0	Zwrot Echa (używany przez ping).
1 — miejsce docelowe jest nieosiągalne (ang. <i>Destination Unreachable</i> )		Miejsce docelowe jest nieosiągalne (ICMPv6).
2 — pakiet jest zbyt duży (ang. <i>Packet Too Big</i> )		Pakiet jest zbyt duży (ICMPv6).
3 — przekroczenie limitu czasu (ang. <i>Time Exceeded</i> )		Przekroczenie limitu czasu (ICMPv6).
3 — miejsce docelowe jest nieosiągalne (ang. <i>Destination Unreachable</i> )	0	Sieć docelowa jest nieosiągalna.
	1	Urządzenie docelowe jest nieosiągalne.
	2	Protokół docelowy jest nieosiągalny.
	3	Port docelowy jest nieosiągalny.
	4	Datagram jest za duży, wymagana jest fragmentacja, ale jest ustawiona flaga DF (ang. <i>Don't Fragment</i> ).
	5	Trasa docelowa jest nieosiągalna.
	6	Trasa do sieci docelowej jest nieznaną.
	7	Trasa do sieci docelowej jest nieznaną.
	8	Urządzenie źródłowe jest izolowane (przestarzałe).
	9	Sieć administracyjnie zablokowana.
	10	Urządzenie administracyjnie zablokowane.
	11	Sieć niedostępna, złe ustawienia TOS (ang. <i>Type of Service</i> ).
	12	Urządzenie niedostępne, złe ustawienia TOS.
	13	Komunikacja administracyjnie blokowana.
4 — tłumienie źródła (ang. <i>Source Quench</i> )	0	Tłumienie nadawcy, kontrola przeciążenia.
4 — problem z parametrem (ang. <i>Parameter Problem</i> )		Problem z parametrem (ICMPv6).
5 — komunikat przekserowania (ang. <i>Redirect Message</i> )	0	Przekierowanie ruchu do całej sieci.
	1	Przekierowanie ruchu do konkretnego urządzenia.
	2	Przekierowanie ruchu do całej sieci dla danych ustawień TOS.
	3	Przekierowanie ruchu do konkretnego urządzenia dla danych ustawień TOS.
6 — alternatywny adres urządzenia (ang. <i>Alternate Host Address</i> )		Alternatywny adres urządzenia.

**Tabela 18.7.** Typy ICMP — ciąg dalszy

Typ	Kod	Opis
7 — zarezerwowane		Zarezerwowany.
8 — żądanie Echa (ang. <i>Echo Request</i> )	0	Żądanie Echa (używane przez ping).
9 — informacje o routerze (ang. <i>Router Advertisement</i> )	0	Informacje o routerze.
10 — żądanie udzielenia informacji (ang. <i>Router Solicitation</i> )	0	Żądanie udzielenia informacji o routerze.
11 — przekroczenie limitu czasu (ang. <i>Time Exceeded</i> )	0	Czas życia pakietu (TTL) wygaśł po drodze.
	1	Czas życia pakietu (TTL) wygaśł podczas defragmentacji.
12 — błąd parametru: niewłaściwy nagłówek IP (ang. <i>Parameter Problem</i> )	0	Błąd wskaźnika.
	1	Brak wymaganej opcji.
	2	Niewłaściwa długość (błąd sumy kontrolnej).
13 — żądanie sygnatury czasowej (ang. <i>Timestamp</i> )	0	Żądanie sygnatury czasowej.
14 — zwrot sygnatury czasowej (ang. <i>Timestamp Reply</i> )	0	Zwrot sygnatury czasowej.
15 — żądanie informacji (ang. <i>Information Request</i> )	0	Żądanie informacji.
16 — zwrot informacji (ang. <i>Information Reply</i> )	0	Zwrot informacji.
17 — żądanie maski adresu (ang. <i>Address Mask Request</i> )	0	Żądanie maski adresu.
18 — zwrot maski adresu (ang. <i>Address Mask Reply</i> )	0	Zwrot maski adresu.
19 — zarezerwowane		Zarezerwowany ze względów bezpieczeństwa.
20 – 29 — zarezerwowane		Zarezerwowany do testowania odporności na awarie.
30 — traceroute (śledzenie trasy)	0	Śledzenie trasy.
31 — błąd konwersji datagramu. (ang. <i>Datagram Conversion Error</i> )		Błąd konwersji datagramu.
32 — zmiana adresu ruchomego urządzenia (ang. <i>Mobile Host Redirect</i> )		Zmiana adresu ruchomego urządzenia.
33 — Gdzie jesteś? (ang. <i>Where Are You?</i> )		Gdzie jesteś? (IPv6)
34 — Jestem tutaj! (ang. <i>Here I Am!</i> )		Jestem tutaj! (IPv6)

**Tabela 18.7.** Typy ICMP — ciąg dalszy

Typ	Kod	Opis
35 — żądanie rejestracji urządzenia ruchomego (ang. <i>Mobile Registration Request</i> )		Żądanie rejestracji urządzenia ruchomego
36 — zwrot na żądanie rejestracji urządzenia ruchomego (ang. <i>Mobile Registration Reply</i> )		Zwrot na żądanie rejestracji urządzenia ruchomego.
37 — żądanie nazwy domeny (ang. <i>Domain name Request</i> )		Żądanie nazwy domeny.
38 — zwrot nazwy domeny (ang. <i>Domain Name Reply</i> )		Zwrot nazwy domeny.
39		Algorytm SKIP Discovery Protocol (ang. <i>Simple Key Management for Internet Protocol</i> ).
40		Awaria związana z bezpieczeństwem.
41		Eksperymentalne protokoły mobilne.
42 – 99 — zarezerwowane		Zarezerwowane.
100		Nieprzeznaczone do ogólnego użytku.
101		Nieprzeznaczone do ogólnego użytku.
102 – 126 — zarezerwowane		Zarezerwowane.
127 — zarezerwowane		Zarezerwowane dla przyszłych komunikatów ICMPv6.
128 — żądanie Echa (ang. <i>Echo Request</i> )		Żądanie Echa (ICMPv6).
129 — zwrot Echa (ang. <i>Echo Reply</i> )		Zwrot Echa (ICMPv6).
130 – 199 — zarezerwowane		Zarezerwowane.
200		Nieprzeznaczone do ogólnego użytku.
201		Nieprzeznaczone do ogólnego użytku.
255 — zarezerwowane		Zarezerwowane dla przyszłych komunikatów ICMPv6.

Źródło: <http://www.iana.org/assignments/icmp-parameters>.

## IPv6 (Internet Protocol Version 6)

Druga wersja protokołu Internet Protocol (IPv6) jest następcą IPv4. Protokół IPv6 został opracowany w celu zapewnienia znacznie większej przestrzeni adresowej, wprowadzono autokonfigurację oraz usprawniono routing, a także poprawiono bezpieczeństwo. W większości protokoły internetowe działające z IPv4 również funkcjonują z IPv6. Niektóre protokoły warstwy aplikacji, na przykład FTP i NTPv3, enkapsulujące adresy IP, mogą nie działać bez przeróbek, co wynika z odmiennej struktury nagłówków IPv4 i IPv6.

Protokół IPv6 rozwiązuje wiele problemów, które powodowały, że sieć IPv4 sprawiała kłopoty w użytkowaniu. Nagłówki IPv6 są prostsze i mają wbudowany mechanizm QoS (ang. *Quality of Service*). Duża przestrzeń adresowa oznacza, że podsieci stają się abstrakcją, a nie koniecznością. Ponadto znika NAT (ang. *Network Address Translation*), odpowiedzialny za problemy z wykorzystaniem wielu protokołów. Eliminacja NAT powoduje usunięcie znacznej liczby sieciowych błędów konfiguracyjnych. Protokoły VoIP (ang. *Voice over IP*), BitTorrent, SIP (ang. *Session Initiation Protocol*) oraz strumieniowe i punkt-punkt miały problemy z NAT-em, ponieważ nie mogły zidentyfikować systemów docelowych.

W protokole IPv6 znacznie usprawniono routing, mechanizmy routingu multiemisji, anycastingu oraz emisji pojedynczej. W wielu przypadkach utworzenie sieci LAN nie wymaga nawet routera. Podsieci w IPv6 zawierają się w części adresu określającej sieć, dlatego ruch może być kierowany do właściwego komputera na podstawie adresu.

Protokół IPv6 Neighbor Discovery (ND) może wykrywać nie tylko sąsiednie komputery i urządzenia, ale także prefiksy sieciowe. Zawiera metody automatycznej konfiguracji adresu, określa kolejny przeskok, usuwa powtarzające się adresy oraz ustala, czy sąsiednie urządzenie jest dostępne, czy pozostaje w trybie offline. ND konsoliduje w pojedynczym protokole sieciowym wiele ważnych funkcji i może działać automatycznie w tle.

Ponieważ automatyczna konfiguracja adresów jest wbudowana w IPv6, serwer DHCP staje się w dużej mierze nieistotny, choć oczywiście istnieje wersja DHCPv6. Automatyczna konfiguracja adresów IPv6 jest przeprowadzana przez wysyłanie zapytania do routera. Istnieje możliwość konfiguracji adresu lokalnego dla łącza w taki sposób, aby był unikalny. Eliminuje to problem konfliktów w sieci, kiedy dwa komputery używają tego samego adresu IPv4.

W celu przesyłania pakietów IPv6 przez sieć IPv4 konieczna staje się enkapsulacja pakietów IPv6 wewnątrz IPv4. Proces ten nosi nazwę tunelowania i jego konfiguracja może być automatyczna lub predefiniowana. Jedną z metod wykorzystuje protokół ISATAP, polega na generowaniu adresu IPv6 z adresu IPv4. Technologia o nazwie Teredo stosuje automatyczne tunelowanie przez IPv4 UDP w celu transmisji pakietów IPv6 przez routery wykorzystujące technologię NAT. Teredo można spotkać w Windows XP SP2 IPv6, Windows Vista, Windows Server 2003 i 2008 oraz Mac OS X Leopard. Wymienione technologie pozwalają na płynne przejście z IPv4 na IPv6.



IPv5 został utworzony jako protokół strumieniowania dla ruchu audio oraz wideo i pozostaje niedostępny do używania jako protokół adresowania IP.

Okazało się, że protokół IPv6 jest wdrażany znacznie wolniej, niż którykolwiek z programistów pracujących nad nim mógł przypuszczać. Jest to związane z technologiami omówionymi w poprzednim podrozdziale — w szczególności NAT, CIDR i tworzeniem podsieci. Jednak tylko kwestią czasu pozostaje to, kiedy IPv6 stanie się dominującym protokołem adresowania IP. Organizacja IANA śledzi stopień wykorzystania IPv4 i przewiduje, że niezaalokowane adresy wyczerpią się około roku 2011. Jeżeli wszystkie przedstawione dotąd argumenty nie przekonały Czytelnika, że warto poświęcić czas na IPv6, należy pamiętać, iż w pewnym momencie po prostu nie będzie wyjścia i trzeba będzie zaakceptować IPv6.

## Adresowanie IPv6

IPv6 definiuje 128-bitową przestrzeń adresową, co jest niemal niewyobrażalną liczbą. Fragment adresu dotyczący urządzenia jest przypisany jako kolejny numer albo pobrany z adresu MAC interfejsu sieciowego. Fragment adresu identyfikujący sieć i fragment identyfikujący urządzenie mają po 64 bity długości. Dodanie w routerze wpisu z prefiksem identyfikującym sieć IPv6 pozwala zaadresować daną sieć. Oznacza to znaczne uproszczenie tabel routingu w porównaniu z IPv4, co prowadzi do lepszej wydajności routingu. Zmniejszenie poziomu skomplikowania nagłówka IPv6 to kolejny czynnik poprawiający wydajność routera.

W standardowym zapisie szesnastkowym adres IPv6 zostanie zapisany w postaci ośmiu czterocyfrowych grup; każda jest oddzielona dwukropkiem, jak przedstawiono poniżej:

```
2001:0db8:3c4d:0015:0000:0000:abcd:ef14
```

W powyższym przykładzie 2001:0db8:3c4d: jest globalnym prefiksem, 0015: to identyfikator podsieci, natomiast 0000:0000:abcd:ef14 to identyfikator interfejsu sieciowego.

Nie ma potrzeby określania identyfikatora sieci lub podsieci któregośkolwiek z routerów znajdujących się na trasie do tej sieci. Dodanie identyfikatora sieci powoduje zmianę routingu dla całego zbioru systemów w tej sieci IPv6.

Klasy sieciowe używane w IPv4 nie są dłużej stosowane w IPv6. Blok ciągłych adresów sieciowych definiujących pojedynczą sieć może być zdefiniowany przez wielkość prefiksu. Dwa poniższe adresy przedstawiają początek i koniec zakresu sieciowego:

```
2001:0db8:3c4d:0000:0000:0000:0000:0000  
2001:0db8:3c4d:ffff:ffff:ffff:ffff:ffff
```

Istnieje możliwość użycia notacji analogicznej do CIDR w celu wskazania wielkości prefiksu sieciowego, podobnie jak ma to miejsce w IPv4. W stosunku do powyższych adresów metoda ta pozwala na zapisanie bloku sieciowego w poniższej formie:

```
2001:0db8:3c4d::/48
```

Należy pamiętać, że IPv6 to 128-bitowa przestrzeń adresowa i każde osiem bloków w adresie przedstawia 16-bitowe dane zapisane w formie czterech znaków notacji szesnastkowej. Trzy wymienione bloki prefiksu sieciowego wskazują, że wielkość prefiksu sieciowego wynosi 48. To nadal pozostawia  $2^{80}$ , czyli  $1,21 \times 10^{24}$  adresów, które można przypisać. Większe wartości prefiksu sieciowego zmniejszają liczbę unikalnych adresów możliwych do przypisania. Jednak możliwości IPv6 są tak ogromne, że nawet w pełni 64-bitowy prefiks sieci nadal pozostawia  $2^{64}$ , czyli  $1,84 \times 10^{19}$  unikalnych adresów — ponad trzy miliardy adresów dla każdego mieszkańca Ziemi.

Możliwość tworzenia podsieci nie zniknęła w sieciach IPv6, jednak ich przydatność do zadań innych niż porównawcze traci sens. Zazwyczaj sieci /48 są stosowane w ogromnych organizacjach pozwalających na używanie wspomnianej wcześniej 80-bitowej przestrzeni adresowej. Mniejsze sieci używają prefiksu /56, pozwalającego na stosowanie 72-bitowej przestrzeni adresowej. Sieć /48 umożliwia zdefiniowanie 65 536 ( $2^{16}$ ) podsieci, podczas gdy sieć /57 umożliwia zdefiniowanie 128 ( $2^7$ ) podsieci. Ponieważ automatyczna konfiguracja wymaga do przypisania pełnych 64 bitów w adresie, Czytelnik nigdy nie spotka się z tworzeniem w sieci IPv6 podsieci używającej więcej niż dozwolone 64 bity.

Wszystkie urządzenia IPv6 muszą posiadać następujące adresy:

- ♦ adres lokalny łącza (ang. *Link-local address*);
- ♦ adres grupowy (multiemisja) wszystkich węzłów;
- ♦ adresy unicastowe (emisja pojedyncza);
- ♦ adres grupowy Solicited-Node dla każdego adresu unicast i anycast urządzenia;
- ♦ adresy grupowe do wszystkich grup, do których należy urządzenie;
- ♦ adres loopback (::1).

## Notacja skompresowana IPv6

Jeżeli Czytelnik uważał, że adresy IPv6 są dziwaczne, warto spojrzeć na pełny adres stosowany dla urządzenia localhost:

```
0000:0000:0000:0000:0000:0000:0000:0001
```

Wpisywanie tych wszystkich zer byłoby uciążliwe, więc protokół IPv6 na szczęście nie wymaga tego — ma funkcję o nazwie notacja skompresowana. W przypadku notacji skompresowanej można pominąć ciągły blok zer w adresie i zamienić je na podwójny dwukropek. W ten sposób przedstawiony adres sieciowy zostaje skompresowany do ::1, co jest bardzo poręczne. Kompresowanie zer do podwójnego dwukropka jest ograniczone jedną zasadą, opisaną poniżej. Podobnie adresy IPv6/IPv4, pokazane w dalszej części rozdziału, również można sprowadzić do notacji skompresowanej ::192.168.1.52.

Notacja skompresowana pozwala także na pominięcie początkowych zer w grupach, gdzie specyficzny jest przypadek, gdy grupa składa się z samych zer, co powoduje pozostawienie jednego zera. Na przykład adres:

```
2001:0db8:3c4d:0015:0000:0000:abcd:ef14
```

można skompresować na postać:

```
2001:0db8:3c4d:15:0:0:abcd:ef14
```

i stosując jeszcze pierwszą zasadę notacji skompresowanej, doprowadzić do postaci:

```
2001:0db8:3c4d:15::abcd:ef14
```

Notacja skompresowana pozwala na zastąpienie podwójnym dwukropkiem tylko jednego bloku zer. Jest ku temu dobry powód. Rozważmy przedstawiony poniżej adres:

```
2001:0000:0000:0015:0000:0000:0000:ef14
```

Jeżeli zostałby skompresowany do postaci:

```
2001::15::ef14
```

to nie można by stwierdzić, czy adres pełny ma postać:

```
2001:0000:0000:0000:0000:0015:0000:ef14,
```

czy:

2001:0000:0000:0000:0015:0000:0000:ef14,

czy:

2001:0000:0000:0015:0000:0000:0000:ef14,

czy może:

2001:0000:0015:0000:0000:0000:0000:ef14.

Prawidłowe postacie skompresowane rozpatrywanego adresu to:

2001:0:0:15::ef14,

lub:

2001::15:0:0:0:ef14.

Po zrozumieniu tych kilku reguł notacji skompresowanej można dostrzec, że wszystkie przedstawione poniżej adresy są równoważne:

2001:0db8:0000:0000:0000:0000:abcd:ef14

2001:0db8:0000:0000:0000::abcd:ef14

2001:0db8:0:0:0:0:abcd:ef14

2001:0db8:0:0::abcd:ef14

2001:0db8::abcd:ef14

2001:db8::abcd:ef14

co na początku będzie bardzo mylące.

Notację skompresowaną można spotkać wraz z dołączonym prefiksem sieci, na przykład adres 2001:db8:abcd::ef14/48.

## Kalkulatory IPv6

W przestrzeni adresowej IPv6 można napotkać żyjące tam potwory. Ich cechą charakterystyczną jest osiem cyfr znajdujących się na ich dłoniach i stopach lub są to inne kombinacje składające się maksymalnie z 32 cyfr.

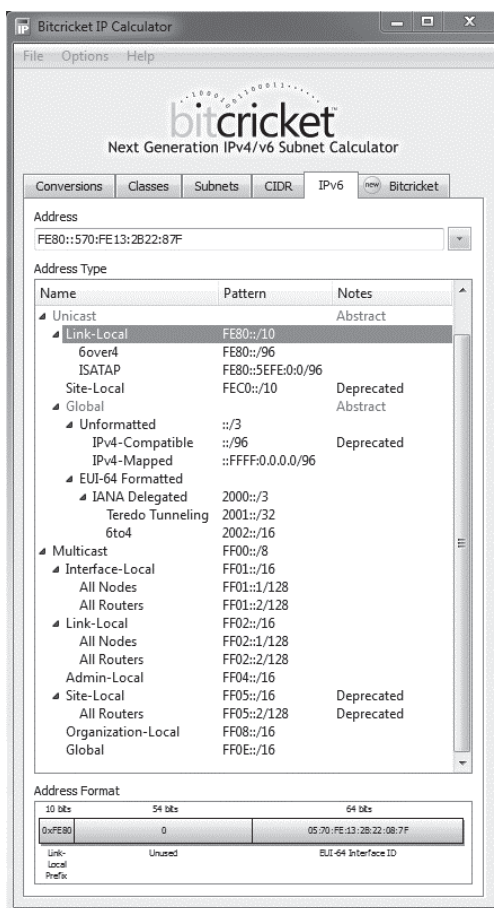
Ponieważ jakiś czas temu autor przestał nadażać za rosnącymi liczbami, woli polegać na wielu witrynach internetowych, narzędziach bądź tabelach, które istnieją w celu obsługi różnych form konwersji powiązanych z IP. Jednym z takich narzędzi jest Bitcricket (zob. rysunek 18.11), który może obliczać podsieci dla IPv4/IPv6, CIDR, jak również przeprowadzać konwersje pomiędzy liczbami zapisanymi w systemie dziesiętnym z kropkami, dziesiętnym, szesnastkowym z kropkami, dwójkowym z kropkami oraz dwójkowym. Program jest dostępny dla platform Windows i Macintosh, można go pobrać ze strony <http://www.bitcricket.com/ip-subnet-calculator.html>.

Na rysunku 18.11 pokazano stronę narzędzia Bitcricket wraz z wymienionymi różnymi zdefiniowanymi interfejsami.

Alternatywny kalkulator dla systemów Linux i Unix to IPv6Ccalc, który można pobrać ze strony <http://www.deepspace6.net/projects/ipv6calc.html>.

**Rysunek 18.11.**

Program Bitcricket  
może być używany do  
wylizania i konwersji  
IPv4/IPv6



## Adresy podwójnego stosu IPv6/IPv4

Przestrzeń adresowa IPv6 i IPv4 nie są zgodne. Chociaż na tym samym komputerze lub w tej samej sieci mogą funkcjonować oba protokoły, to jednak działają zupełnie niezależnie od siebie. Ponieważ większość świata używa adresów IPv4, protokół IPv6 byłby bezużyteczny, gdyby nie pozwalał na kodowanie adresów IPv4. W celu utworzenia adresu IPv4 w formacie adresu IPv6 trzeba adres zapisać w następującej postaci:

```
0000:0000:0000:0000:0000:0000:192.168.1.52
```

lub:

```
0000:0000:0000:0000:0000:ffff:192.168.1.52
```

Warto zwrócić uwagę na fakt, że powyższy adres ma zdefiniowane tylko siedem bloków rozdzielonych dwukropkami. Jednak wcześniej wspomniano, że adresy IPv6 wymagają ośmiu bloków. Powód, dla którego adres IPv6/IPv4 ma tylko siedem bloków, to fakt, że blok IPv4 jest zakodowany dla 32 bitów, a nie 16, jak ma to miejsce w blokach IPv6. Oznacza to, że fragment IPv4 adresu IPv6 jest blokiem podwójnym.

Protokół IPv6 ma możliwość używania tego, co ogólnie nazywamy adresami zgodnymi. W tego rodzaju adresie można połączyć sześć bardziej znaczących grup cyfr szesnastkowych wraz z czterema grupami cyfr dziesiętnych w mniej znaczących oktetach używanych przez IPv4. Stosując taki schemat, otrzymujemy adres w postaci:

h:h:h:h:h:h:d.d.d.d

gdzie h oznacza bardziej znaczące bajty, natomiast d mniej znaczące. Taka forma adresu pozwala na użycie poniższego zamiennika:

::ffff:192.168.2.52

który w adresie początkowym jest odpowiednikiem notacji:

::ffff:c0a8:0234.

Taka notacja dla adresów podwójnego stosu nie jest powszechnie obsługiwana, więc przed jej zastosowaniem należy się upewnić, że będzie prawidłowo obsługiwana.

## Strefy i zakresy adresów

Adres IPv6 jest zdefiniowany dla określonego zakresu. Jedną z metod opisanego zakresu adresów jest stwierdzenie, że przedstawia on punkty końcowe połączenia dla danego interfejsu sieciowego. Połączenie może obejmować region zdefiniowany jako połączenie lokalne, dane miejsce lub sieć globalną. Po przeanalizowaniu adresów IPv6 w systemie można odkryć, że w ramach tego samego interfejsu sieciowego znajdują się adresy połączenia lokalnego oraz adresy globalne. Chociaż interfejs sieciowy musi mieć przynajmniej jeden adres IPv6 emisji pojedynczej, w interfejsie można zdefiniować dowolną liczbę adresów IPv6.

Różne typy zdefiniowanych adresów to:

- ♦ **Adresy lokalne dla łącza** (ang. *Link Local Address*, LLA). Są to adresy sieci prywatnej, które nie podlegają routingowi i są ograniczone do pojedynczej sieci lub podsieci. Adresy te są konfigurowane automatycznie, przez połączenie prefiksu sieci FE80::/10 i adresu MAC interfejsu.
- ♦ **Adresy unikalne lokalnie** (ang. *Unique Local Address*, ULA). Adresy unikalne lokalnie są adresami sieci prywatnej, są routowalne tylko między sieciami prywatnymi, nie podlegają routingowi w sieci globalnej. Adresy ULA rozpoczynają się od FD, 40 następnych bitów to routing prywatny, potem 16 bitów to routing w ramach sieci LAN w danej lokalizacji, pozostałe 64 bity to adresy urządzeń.
- ♦ **Adresy Globalne** (ang. *Global Address*, GA). Są to adresy sieci publicznej, które podlegają routingowi w sieci globalnej. Adres GA zaczyna się od 3 bitów 001, następne 45 bitów to prefiks globalnego routingu, potem 16 bitów routingu prywatnego. Ostatnie 64 bity to adresy urządzeń.

Adres lokalny węzła (ang. *Site Local Address*) zdefiniowany w dokumencie RFC został wycofany w roku 2004 i nie jest używany.

Każdy interfejs sieciowy połączony z określonym zakresem adresów staje się częścią strefy zakresu. Strefy zakresów wymagają, aby każdy interfejs sieciowy miał unikalny adres w ramach danej strefy. Adresy nie muszą być unikalne w różnych strefach. Adres IPv6 wyświetlany przez polecenie `ipconfig /all` w systemie Windows ma następującą postać:

Adres IPv6 połączenia lokalnego . : fe80::e575:7878:cc94:ff7c%10(Preferowane)

Tytuł wskazuje, że adres należy do zakresu strefy połączenia lokalnego. Sam adres to ciąg tekstowy fe80::e575:7878:cc94:ff7c, natomiast %10 wskazuje, że numer indeksu strefy to 10. Definicja strefy znosi konieczność rozgłaszania sieci, natomiast prefiks fe80 to zakres lokalny. Adres lokalny dla łącza ma taki sam prefiks routingu fe80::/10.

Rozważmy przykład komputera macierzystego z dwoma fizycznymi połączeniami do sieci wraz z dwoma adresami lokalnymi względem łącza. Pierwszy adres to fe80::a/64, natomiast drugi to fe80::b/64. Oba wymienione interfejsy łączą się z siecią, w której jest urządzenie o adresie fe80::c/64. Komputer fe80::c/64 chce wysłać pakiety do komputera z dwoma fizycznymi połączeniami do sieci, używając adresu docelowego fe80::a/64. Ponieważ interfejs fe80::b/64 współdzieli ten sam adres lokalny względem połączenia, nie ma możliwości wskazania, do którego adresu (a/64 czy b/64) ten komputer fe80::c/64 powinien wysłać pakiety. Taki problem rozwiązuje zakres adresów. Istnieje możliwość zmiany adresów lokalnych względem połączenia w taki sposób, aby zawierały także strefę:

`<Adres_IPv6>%<Indeks_Strefy>`

Różne systemy operacyjne w odmienny sposób będą wskazywały indeks strefy. Microsoft Windows IPv6 używa liczb całkowitych, na przykład %1, podczas gdy systemy Linux i Unix używają nazwy interfejsu, na przykład %eth0.

Multiemisja, która jest wymaganym polem w nagłówku IPv6, może być używana do wysyłania pakietu do wszystkich urządzeń w strefie, na przykład do grupy multiemisji all-host połączenia lokalnego. Multiemisja w IPv6 zastępuje rozgłaszanie, które stanowiło część IPv4. Zadaniem multiemisji jest wysłanie pakietów do każdego interfejsu sieciowego będącego członkiem grupy multiemisji, które zostały zarejestrowane w routerze. Jeżeli w danym routerze nie zostali wymienieni żadni członkowie, to pakiety będą odrzucone. Multiemisja nie jest narażona na problemy związane z rozgłaszaniem, kiedy to niezamierzeni odbiorcy otrzymują to, co nazywamy burzą rozgłaszania.

Urządzenie IPv6 może wysłać pakiet na jeden adres przypisany wielu urządzeniom. Adresy te to adresy anycast, umożliwiające komunikację z najbliższym urządzeniem w grupie. Pakiet trafia do urządzenia, które router uzna za najbliższe. Pozwala to na poprawianie niezawodności i odporności na awarie. Adresy anycast mogą być tylko adresami docelowymi (nigdy źródłowymi).



Komunikacja anycast oraz inne technologie routingu IP zostały szczegółowo omówione w rozdziale 9. Wiele serwerów DNS w internecie używa komunikacji anycast do przeprowadzania replikacji.

W tabeli 18.8 wymieniono zarezerwowane zakresy adresów IPv6. Z zakresów wymienionych w poniższej tabeli tylko 0000::/8, 2000::/3, FC00/7, FE80::/10 i FF::/8 są dostępne publicznie jako adresy loopback albo jako zakres rozgłaszania.

**Tabela 18.8.** Zakresy adresów IPv6 IANA

Prefiks	Alokacja
0000::/8	Zarezerwowany przez IETF. Wyjątkiem są adresy IPv6 kompatybilne z IPv4: 0:0:0:0:0:a.b.c.d/96 lub ::a.b.c.d/96.
0100::/8	Zarezerwowany przez IETF.
0200::/7	Zarezerwowany przez IETF. Zakres 0200::/7 poprzednio był zdefiniowany jako tak zwany Network-Service-Access-Point (NSAP), obecnie uznany za przestarzały.
0400::/6	Zarezerwowany przez IETF.
0800::/5	Zarezerwowany przez IETF.
1000::/4	Zarezerwowany przez IETF.
2000::/3	Adresy globalne; jednoznaczne adresy, które są routowane przez sieć globalną. Przestrzeń IPv6 Unicast obejmuje cały zakres adresów IPv6 z wyjątkiem FF00::/8. Przypisane przez IANA adresy Unicast są obecnie ograniczone do zakresu adresów IPv6 Unicast 2000::/3. Przypisany zakres jest zarejestrowany w rejestrze IANA: <a href="http://iana-ipv6-unicast-address-assignments">iana-ipv6-unicast-address-assignments</a> .
2001:DB8::/32	Adres został zarezerwowany na potrzeby przykładów i dokumentacji.
3fff:ffff::/32	Adresy zarezerwowane na potrzeby przykładów i dokumentacji.
4000::/3	Zarezerwowany przez IETF.
6000::/3	Zarezerwowany przez IETF.
8000::/3	Zarezerwowany przez IETF.
A000::/3	Zarezerwowany przez IETF.
C000::/3	Zarezerwowany przez IETF.
E000::/4	Zarezerwowany przez IETF.
F000::/5	Zarezerwowany przez IETF.
F800::/6	Zarezerwowany przez IETF.
FC00::/7	Adresy lokalne Unicast można stosować w ramach sieci lokalnych, nieroutowalne do sieci globalnej.
FE00::/9	Zarezerwowany przez IETF.
FE80::/10	Adresy lokalne łączy, nieprzepuszczane przez urządzenia do sieci globalnej.
FEC0::/10	Zarezerwowany przez IETF. Zakres FEC0::/10 poprzednio był zdefiniowany jako prefiks zakresu adresów Site-Local. Ta definicja została jednak porzucona.
FF00::/8	Multicast.

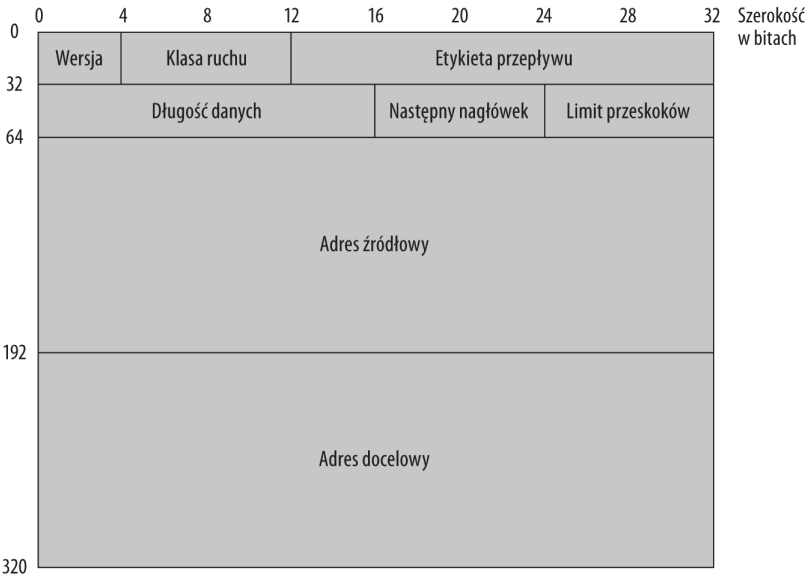
Źródło: <http://www.iana.org/assignments/ipv6-address-space>. Dokumenty RFC, w których zdefiniowano przestrzenie IPv6, to między innymi 1881, 1888m, 3879, 4048, 4147, 4193, 4291 oraz 4548.

W użyciu są dwie metody służące do automatycznej konfiguracji adresów w IPv6: bezstanowa SLAAC (ang. *Stateless Address Autoconfiguration*) oraz stanowa DHCPv6. System operacyjny obsługujący IPv6 konfiguruje automatycznie dla każdego interfejsu sieciowego adres lokalny łącza. Wykorzystuje w tym celu adres MAC interfejsu, odpowiednio go modyfikując. Aby uzyskać adres globalny, router znajdujący się w tej samej sieci cyklicznie wysyła w komunikatach ICMPv6 „informacje o routerze” (ang. *Router Advertisement*), w którym znajduje się ustalony na jego interfejsie prefiks sieci. System klienta uzupełnia swój adres o tę informację. DHCPv6 jest wykorzystywana, jeśli administrator sieci musi mieć większą kontrolę nad przydziałem adresów. Pozwala także na przekazywanie klientowi większej ilości informacji niż SLAAC. W większości przypadków w sieciach IPv6 wykorzystuje się SLAAC; serwer DHCPv6 jest stosowany rzadko.

Datagramy IPv6

Datagramy IPv6 są większe i prostsze niż ich odpowiedniki w IPv4. Nagłówek pakietu został pokazany na rysunku 18.12. Warto zwrócić uwagę na fakt, że IPv6 nie używa sumy kontrolnej nagłówka w celu sprawdzenia poprawności dostarczonego pakietu. Zamiast tego wykorzystuje do sprawdzania poprawności inne protokoły. Z tego powodu protokół IPv6 jest szybszy niż IPv4.

Rysunek 18.12.  
Struktura nagłówka  
IPv6



Poszczególne pola w nagłówku IPv6 mają następujące przeznaczenie:

- ♦ **Wersja.** Jest to czterobitowa reprezentacja cyfry 6 (0110).
- ♦ **Klasa ruchu.** Pole to zawiera zakres priorytetów używanych do kontrolowania ruchu pakietu. Pozwala na zapewnienie odpowiedniej jakości usług (QoS).
- ♦ **Etykieta przepływu.** Jest to 20-bitowe pole do oznaczania strumieni pakietów w celu ich rozróżnienia w warstwie sieci.

- ♦ **Długość danych.** Pole to wskazuje wyrażoną w bajtach wielkość danych pakietu. Jeżeli zawiera same zera, to oznacza, że pakiet to tak zwany „Jumbogram”, czyli pakiet o wielkości od 64 KB do 4 GB. Ramki Jumbo wymagają łączy o bardzo wysokim MTU (ang. *Maximum Transmission Unit*).
- ♦ **Następny nagłówek.** To odpowiednik pola protokołu w nagłówku IPv4. Może być również stosowany w celu dodania dodatkowego nagłówka do pakietu.
- ♦ **Limit przeskoków.** Pole to określa liczbę dozwolonych przeskoków sieciowych. Obecnie to zamiennik dla parametru TTL (ang. *Time-To-Live*) stosowanego w IPv4.
- ♦ **Adres źródłowy.** To 128-bitowy adres źródłowy IPv6.
- ♦ **Adres docelowy.** To 128-bitowy adres docelowy IPv6.

## Protokół IPv6 Neighbor Discovery

Protokół IPv6 Neighbor Discovery (ND) łączy w sobie dużą liczbę ważnych funkcji dostępnych w różnych protokołach IPv4, ma też kilka nowych funkcji. Nazwa protokołu wskazuje tylko na mały wycinek możliwości tej użytecznej technologii. Za pomocą ND można wykryć i skonfigurować pewną liczbę parametrów sieciowych. Ponadto obsługiwane są podstawowe funkcje protokołu IP.

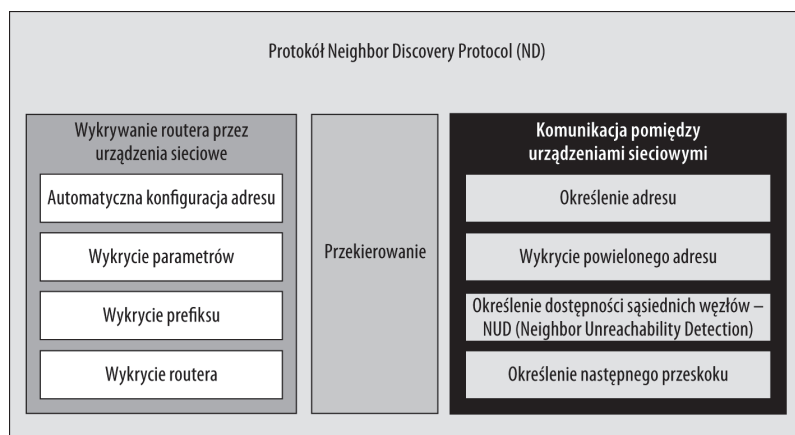
Protokół *Internet Protocol* to protokół warstwy sieciowej w modelu ISO/OSI oraz podstawowy protokół warstwy internetowej w zbiorze protokołów *Internet Protocol Suite*. IP jest odpowiedzialny za dostarczanie datagramów, adresowanie, routing oraz konfigurację interfejsu sieciowego. W IPv4 protokół ARP (ang. *Address Resolution Protocol*) zapewnia odnajdowanie adresu sprzętowego, gdy posiadamy adres warstwy sieciowej, natomiast ICMP (ang. *Internet Control Message Protocol*) zapewnia system wymiany informacji pomiędzy urządzeniami, które pozwalają na potwierdzanie i kontrolę ruchu sieciowego, wspiera QoS (ang. *Quality of Service*) i inne funkcje. Wiele z tych funkcji zostało skonsolidowanych w protokole ND, dostępnym w IPv6.

Jak pokazano na rysunku 18.13, protokół ND wykorzystywany jest do wykrywania routerów, adresów, prefiksów sieciowych i innych parametrów konfiguracyjnych. Do wykrywania elementów sieciowych protokół ND używa wiadomości ICMPv6, takich jak Router Advertisement i Router Solicitation, Echo Request i Echo Reply, Neighbor Advertisement i Neighbor Solicitation. Wymienione polecenia i dostarczane przez nie informacje współdziałają z komunikatami IPv6, takimi jak Redirect oraz Router Renumbering, co pozwala na budowanie zoptymalizowanych tabel routingu.

Najważniejsze funkcje oferowane przez ND to między innymi:

- ♦ **Określanie adresu.** Zapytanie o adres routera może zwrócić komputerowi poprawny identyfikator sieci w trakcie uruchamiania komputera bądź na żądanie. Do określenia adresu używana jest multiemisja, która jest znacznie efektywniejsza niż rozgłaszanie używane przez ARP w IPv4.
- ♦ **Automatyczna konfiguracja.** Protokół ND oferuje funkcje wiadomości, które pozwalają na wykonywanie zapytań dotyczących konfiguracji routera i mogą zwrócić parametry sieci.

**Rysunek 18.13.**  
Różne komponenty  
funkcjonalne  
w protokole ND  
(Network Discovery)  
w IPv6



- ♦ **Określenie następnego przeskoku.** Kiedy jeden komputer wysyła pakiety do innego, protokół ND analizuje nagłówek datagramu w celu ustalenia, czy wymagany jest router, czy komunikacja może być bezpośrednia. W zasięgu lokalnym komunikacja będzie bezpośrednia. Po określeniu, że adres docelowy nie znajduje się w sieci lokalnej, ND wybiera odpowiedni router, który będzie „kolejnym przeskakiem”. W większości przypadków pakiety używają udostępnianego przez komputer bufora lokalizacji docelowych i określają, gdzie datagramy powinny być wysłane. Po ustaleniu kolejnego przeskoku dla określonego datagramu bufor docelowy zostaje uaktualniony.
- ♦ **Przekierowanie.** Funkcja przekierowania w ND analizuje trasę przypisaną datagramom w celu ustalenia, czy została wybrana najlepsza. Jeżeli dostępna jest lepsza trasa, to ND tworzy wiadomość ICMPv6 Redirect, która zmienia routing dla wszystkich przyszłych datagramów dla połączenia zawierającego takie same punkty końcowe.
- ♦ **Wykrywanie i wybór routera.** Funkcja wiadomości w ND pozwala, aby protokół wykrywał routery w sieci i nieustannie uaktualniał informacje na ten temat. Dynamiczny wybór routerów i dostępne urządzenia, o których router wie, pozwalają ND na określenie aktywnych węzłów znajdujących się w trybie online oraz routerów używanych do przekierowania wiadomości na zewnątrz sieci.
- ♦ **Bezpieczeństwo.** ND działa w warstwie sieci i może być transportowany przez połączenie IPsec.

## ICMPv6

Protokół ICMPv6 oferuje pewne dodatkowe możliwości, które nie stanowiły części definicji ICMPv4. Jak można zobaczyć w tabeli 18.7, zdefiniowane zostały dodatkowe typy wiadomości dla wiadomości błędów (1, 2, 3, 4, 100, 101 i 127) oraz wiadomości informacyjnych (128, 129, 200, 201 i 255), które są charakterystyczne dla ICMPv6. Ponieważ IPv6 zawiera dodatkowe funkcje routingu, ICMPv6 ma pewne dodatkowe wymagania, które muszą być spełnione, między innymi:

- ♦ Wiadomość będąca wynikiem przesyłania pakietów przez sieć musi zostać wysłana do urządzenia, które ten pakiet wysłało.
- ♦ Jeżeli wiadomość jest odpowiedzią skierowaną na adres typu multicast, anycast lub unicast, który nie ma przypisanego trybu, to adres źródłowy takiej wiadomości musi być adresem unicast węzła generującego wiadomość.

Największa różnica pomiędzy ICMPv4 i ICMPv6 polega na dodatkowych kategoriach wiadomości dodanych w celu obsługi protokołu ND (zostały omówione w poprzednim podrozdziale). Wiadomości Neighbor Solicitation i Neighbor Advertisement zapewniają mechanizm wykrywania używany przez ND w celu zaoferowania przez ND funkcji przeglądania sieci. Wiadomości Neighbor Solicitation i Neighbor Advertisement obsługują funkcję przekierowania ND, co poprawia routing. Wiadomości przekierowania są wysyłane do urządzenia, które wysłało datagram inicjujący przekierowanie.

Funkcja Router Renumbering jest związana z obsługą prefiksów i automatyzacją routerów, pozwalającą na dystrybucję informacji o dostępnych trasach w ramach systemu autonomicznego. Funkcja ta obsługuje komunikaty Router Renumbering Command oraz Router Renumbering Result. Ponieważ pozwala na masową zmianę tras, wbudowano w nią mechanizmy, takie jak tryb testowy oraz Sequence Number Reset, które mają chronić przed nadużyciami tych funkcji optymalizujących.

## Podsumowanie

W tym rozdziale omówiono protokół Internet Protocol oraz jego znaczącą rolę, jaką odgrywa w sieciach TCP/IP. Protokół IP zapewnia dostarczanie pakietów z punktu do punktu, ale nie określa połączenia i metody transportu.

IPv4 używa 32-bitowego schematu adresowania. Czytelnik dowiedział się, w jaki sposób adresy określają sieci i interfejsy oraz jak można manipulować adresami w celu zdefiniowania sieci i podsieci. Omówione zostały także różne metody automatycznego przypisywania adresów w IPv4.

IPv6 to znacznie lepsza wersja protokołu IP. Dysponuje 128-bitową przestrzenią adresową, uproszczonym nagłówkiem oraz usprawnionymi funkcjami routingu. W rozdziale zostały omówione metody adresowania urządzeń w sieciach IPv6, tworzenia sieci i techniki pracy z nimi oraz działania w sieciach podwójnego stosu IPv4/IPv6.

W następnym rozdziale zostaną omówione usługi określania nazw, które tłumaczą adresy na nazwy przyjazne dla człowieka.

# Rozdział 19.

## Usługi określania nazw

### W tym rozdziale:

- ♦ Dlaczego mapowanie jest konieczne?
- ♦ Używanie pliku HOSTS w systemie lokalnym
- ♦ Używanie WINS podczas określania nazw NetBIOS
- ♦ Serwer DNS i jego ważne znaczenie w internecie
- ♦ Określanie nazw kontra usługi katalogowe

Serwery nazw to zbiór usług sieciowych, które tłumaczą adresy komputerowe bądź sieciowe na postać czytelną dla człowieka. Kiedy użytkownik otwiera katalog *Siec* w systemie operacyjnym, usługa nazw sprawdza dostępność urządzeń w sieci, a następnie wyświetla ich nazwy oraz inne informacje. Usługa nazw jest istotnym komponentem, wymaganym do poprawnego działania sieci. Bez funkcjonowania serwera nazw otrzymalibyśmy jedynie informacje czytelne dla komputera.

W użyciu pozostaje wiele różnych usług określania nazw. Przy tłumaczeniu adresów IP, na przykład 170.149.173.130 na nazwę *nytimes.com*, internet polega na protokole DNS (ang. *Domain Name System*).

Wprowadzie DNS to najczęściej używana usługa określania nazw, ale obecnie wykorzystywane są także inne usługi tego rodzaju. W rozdziale omówiono najprostszą i jednocześnie najstarszą metodę określania nazw — plik *hosts*. Za pomocą pliku *hosts* system może przeszukiwać listę znanych systemów, nawet jeśli zautomatyzowana usługa określania nazw ulegnie awarii.

Sieci Windows stosują WINS (ang. *Windows Internet Name Service*) do wyświetlania systemów używających protokołu NetBIOS. Systemy takie mogą zapewniać wysoką wydajność w sieciach Windows i są powszechnie wykorzystywane.

Serwer DNS można skonfigurować na potrzeby sieci LAN i dostarczania usługi określania nazw systemom w grupie roboczej lub częściej w ramach domeny. DNS przechowuje bazę rekordów zawierającą odwzorowania adresów IP na adresy symboliczne łatwiejsze do zapamiętania przez człowieka.

Usługi katalogowe rozszerzają ideę serwerów nazw o przechowywanie informacji dotyczących wielu innych aspektów obiektów sieciowych. Większość usług katalogowych opiera się na LDAP (ang. *Lightweight Directory Access Protocol*), który z kolei bazuje na znacznie bardziej skomplikowanej usłudze katalogowej X.500. LDAP to podstawa dla usług katalogowych używanych przez sieciowe systemy operacyjne.

## Plik HOSTS

Pierwszym systemem używanym do określania nazw w sieciach TCP/IP był plik *hosts*, przechowywany w sieci ARPAnet na komputerze SRI (ang. *Stanford Research Institute*). Plik *hosts* to zwykły plik tekstowy zawierający w jednej kolumnie adresy IP, natomiast w drugiej przypisane im nazwy symboliczne urządzeń. Taki system zapewnia wyszukiwanie na podstawie tej prostej bazy danych. Plik *hosts* jest interesujący głównie z powodów historycznych, ale nadal zachowuje pewną użyteczność, ponieważ jest przeszukiwany w trakcie każdej operacji określania nazw przed wykonaniem zapytania do serwera DNS. Jeżeli w pliku będzie znaleziony odpowiedni wpis, to zostanie użyty jako ostateczna odpowiedź dotycząca określenia nazwy.

Każdy komputerowy system operacyjny nadal tworzy plik *hosts*, który jest sprawdzany w trakcie operacji określania nazw. Ponieważ plik musi być obsługiwany ręcznie, większość użytkowników ma tendencję do jego ignorowania i polega na usługach automatycznych, takich jak DNS. W sieci o dowolnej wielkości zmiana wpisów na każdym komputerze to żmudne zadanie. Jeśli do przydzielania adresów wykorzystywane jest przypisywanie dynamiczne (jak w przypadku DHCP), to używanie tego rozwiązania jest ograniczone nawet w małej sieci. Ponieważ plik *hosts* jest jednak dostępny dla lokalnego administratora, to nadal istnieją pewne zastosowania, które można rozważyć.

W tabeli 19.1 wymieniono położenie pliku *hosts* w różnych sieciowych systemach operacyjnych.

**Tabela 19.1.** Położenie pliku *hosts* w różnych sieciowych systemach operacyjnych

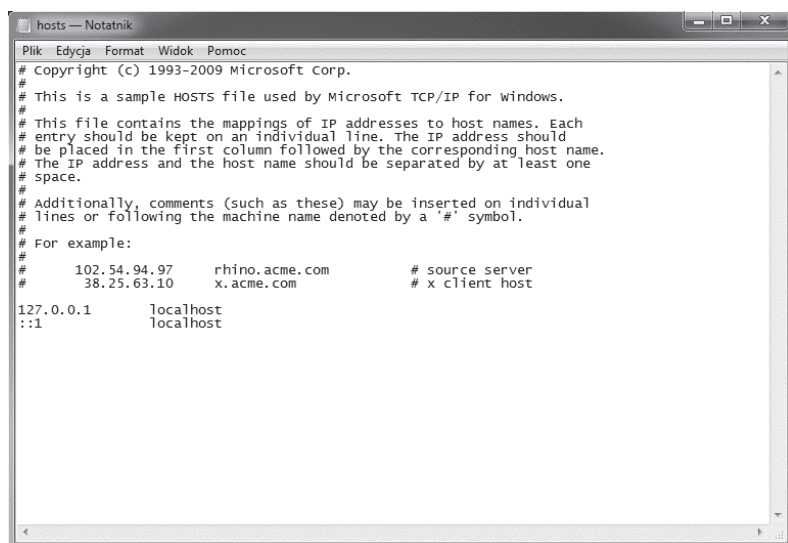
System operacyjny	Położenie	Uwagi
Linux (Unix)	<i>/etc/hosts</i>	
Mac OS X	<i>/private/etc/hosts</i>	
Mac OS 9 i wcześniejsze	<i>System Folder:Preferences</i>	W niektórych wersjach systemu plik <i>hosts</i> jest umieszczony w katalogu <i>System</i> .
OS/2	"Dysk startowy": <i>\MPTN\ETC\HOSTS</i>	
Windows NT — Vista	<i>%Katalog systemu Windows%\System32\drivers\etc\hosts</i>	Położenie tego pliku jest kontrolowane przez następujący klucz rejestru: \HKEY_LOCAL_MACHINE\SYSTEM\ ↳ CurrentControlSet\Services\ ↳ Tcpip\ Parameters\ DataBasePath
Windows ME/98/95	<i>%Katalog systemu Windows%\hosts</i>	

Aktualną zawartość pliku *hosts* można wyświetlić w edytorze tekstowym, oknie powłoki bądź wierszu poleceń.

W celu wyświetlenia zawartości pliku *hosts* w systemie Windows należy wykonać następujące kroki:

1. Wybrać opcję *Uruchom...* z menu *Start* bądź nacisnąć klawisze *Windows+R*.
2. Wpisać `%SystemRoot%\System32\drivers\etc\` i nacisnąć klawisz *Enter*.
3. W Eksploratorze Windows dwukrotnie kliknąć ikonę pliku *hosts*. Na ekranie zostanie wyświetlone okno dialogowe *Otwieranie za pomocą*.
4. W oknie dialogowym *Otwieranie za pomocą* należy wybrać program *Notatnik*, a następnie kliknąć przycisk *OK*. Na rysunku 19.1 pokazano zawartość domyślną pliku *hosts*.

**Rysunek 19.1.**  
*Domyślna zawartość  
pliku hosts dla  
systemu Windows Vista  
(wersja 64-bitowa)*



5. Teraz można wprowadzić w pliku wymagane zmiany.
6. Ostatni krok to wybranie opcji *Zapisz jako...* z menu *Plik* i zapisanie pliku pod nazwą "hosts" wraz z cudzysłowami w nazwie. Znaki cudzysłowu nakazują systemowi Windows zapis pliku bez rozszerzenia.

Jak Czytelnik zapewne pamięta z rozdziału 7., adresy 127.0.0.1 i ::1 są zarezerwowane dla urządzenia loopback w protokołach odpowiednio IPv4 i IPv6. Tworzenie nowych wpisów polega na utworzeniu nowego wiersza, wprowadzeniu adresu, a następnie jednej bądź więcej spacji i nazwy systemu. Poniżej przedstawiono kilka przykładów:

```
192.168.3.180 Maine # Stacja robocza Karoliny
192.168.3.183 Duet # Stacja robocza Alicji
# To jest komentarz, oba powyższe wpisy dotyczą lokalnych systemów komputerowych
64.233.169.104 www.Google.com
...
```

W pierwszej chwili użytkownik być może będzie chciał dodać do pliku *hosts* często odwiedzane witryny internetowe, co przyniesie skutek w postaci niewielkiej oszczędności czasu. Jednak związane z tym obciążenie administracyjne nie jest warte potencjalnych korzyści.

Plik *hosts* jest użyteczny przy blokowaniu witryn. Jeżeli zachodzi potrzeba zablokowania zdalnemu systemowi możliwości otrzymywania odpowiedzi z danego systemu, to ten system można przypisać do urządzenia loopback. Technikę tę stosuje się względem witryn reklamowych, lokalizacji rozsyłających spyware i malware, witryn rozpowszechniających treści erotyczne i pornograficzne itd. Na przykład w celu zablokowania witryny *GoogleAnalytics.com* należy dodać do pliku *hosts* następujący wiersz:

```
127.0.0.1 www.googleanalytics.com
```

Plik *hosts* nie pozwala na dopasowywanie wielu witryn internetowych poprzez używanie symboli wieloznacznych w nazwach adresów ani na blokowanie poszczególnych katalogów. Obsługiwane są jedynie nazwy domen.

Alternatywną techniką jest przekierowywanie usług reklamowych, takich jak *ad.Doubleclick.net*, do niepoprawnego adresu IP. W takim przypadku często stosuje się 0.0.0.0. Istnieje również możliwość przypisania blokowanej witryny do adresu, któremu w wewnętrznej sieci nic nie jest przypisane, i zarezerwowania tego adresu do tego celu. Taki rodzaj blokowania to tak naprawdę forma przekierowania. Przekierowanie może być używane w celu dostarczenia lokalizacji zastępczej do celów testowania oprogramowania sieciowego. Jednak złośliwe witryny internetowe czasami stosują tę technikę, aby przechwycić komputer.

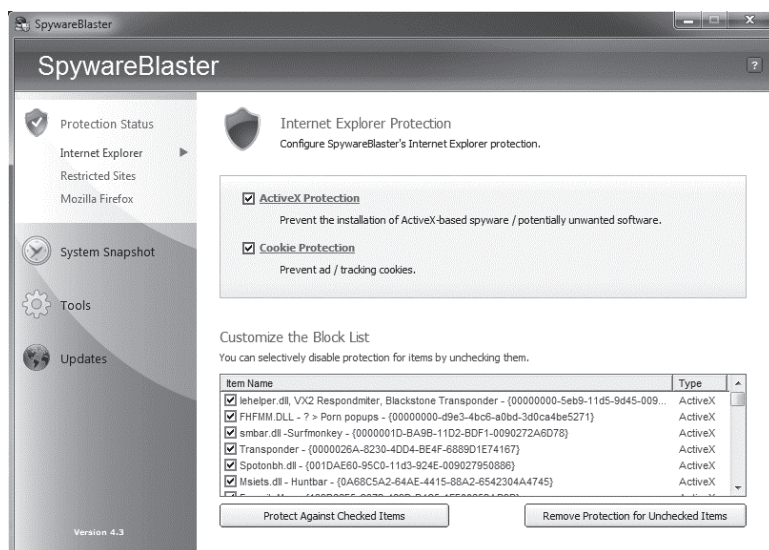
Można sobie wyobrazić, że plik *hosts* blokujący znane złe witryny internetowe to doskonały pomysł, ale tworzenie listy takich witryn i jej obsługa to zadanie herkulesowe. Istnieją inne rozwiązania warte wypróbowania. Jedną z możliwości jest pobranie pliku utworzonego przez innych, często społeczność osób współpracujących nad tworzeniem i obsługą rozbudowanych plików *hosts*.

Autor nie jest zwolennikiem używania plików *hosts* do innych celów niż wymienienie lokalnych systemów komputerowych w jego małej sieci. W celu blokowania witryn polega na zestawie innych narzędzi, łącznie z oprogramowaniem antywirusowym i antyspyware'owym. W szczególności bazuje na narzędziu SpywareBlaster firmy Javacool Software (zob. rysunek 19.2), które blokuje witryny internetowe za pomocą czarnej listy. SpywareBlaster nie zajmuje pamięci i obciąża system w niewielkim stopniu, kiedy przeglądarka Internet Explorer bądź Mozilla Firefox wykonuje żądania określania nazw. W przeglądarce Firefox autor instaluje rozszerzenie Adblock Plus, które również stosuje czarną listę w celu blokowania reklam. Poza tym autor używa rozszerzenia NoScript, uniemożliwiającego wykonywanie skryptów.

Innym poziomem ochrony jest włączenie w przeglądarkach internetowych funkcji zaufanych stref. Wprawdzie autor nie korzysta z tych funkcji, ale są one szczególnie użyteczne w sieciach korporacyjnych.

**Rysunek 19.2.**

*Narzędzie SpywareBlaster wykorzystuje subskrybowaną czarną listę w celu blokowania dostępu niechcianym treściom i witrynom internetowym*



## Protokół Address Resolution Protocol (ARP)

Ogólnie protokół odpowiada za wyszukiwanie adresu sprzętowego, gdy mamy adres warstwy sieci. W swoich rozważaniach skupimy się nad zastosowaniem ARP w zestawieniu z IP. ARP tworzy tabelę adresów IP oraz przypisanych im adresów fizycznych. Tabela ARP jest obsługiwana dynamicznie i przechowywana w pamięci, w buforze ARP. Dynamiczne wpisy wygasają na podstawie ustawienia czasu upływu ważności, podczas gdy statyczne wpisy są obsługiwane w buforze bez uwzględniania czasu, jaki upływa, o ile tabela w buforze ARP działa prawidłowo.

Dla każdego zarejestrowanego urządzenia tabela ARP składa się z następujących wierszy:

- ♦ adres IP;
- ♦ adres fizyczny;
- ♦ indeks IF (fizyczny port bądź interfejs);
- ♦ rodzaj wpisu: 3 — dynamiczny, 4 — statyczny, 2 — nieprawidłowy, 1 — brak przypisania.

ARP jest enkapsulowany w protokole warstwy łącza danych, co oznacza, że ARP nie podlega routinowi. Pozostaje użyteczny jedynie dla podsieci lokalnych.

## Żądania ARP

Podczas wykonywania zapytań do bufora ARP następuje wyszukanie adresu IP. Jeżeli dopasowanie zostanie znalezione, to będzie zwrócony adres fizyczny. W przypadku niezalezienia dopasowania ARP wysyła do wszystkich urządzeń w sieci wiadomość rozgłaszającą,

nazywaną żądaniem ARP. Wymienione żądanie ARP zawiera adres IP i kiedy odpowiednie urządzenie wykryje żądanie, udziela odpowiedzi, przekazując adres fizyczny. Następnie tabela ARP zostaje uaktualniona w celu zapisania tej wiadomości.

Pola w ramce ARP mogą przyjmować następujące wartości:

- ♦ **typ warstwy fizycznej (HTYPE):** 1 dla Ethernetu, 3 dla X.25, 6 dla IEEE 802.3, 18 dla Fibre Channel itd.;
- ♦ **typ protokołu warstwy wyższej (PTYPE):** 2048 dla protokołu IP, 2053 dla X.25 poziomu 3., 32 923 dla AppleTalk itd.;
- ♦ **długość adresu sprzętowego (HLEN) i długość adresu protokołu (PLEN):** długość sprzętowego adresu Ethernet to 4 bajty, długość adresu protokołu IP to również 4 bajty;
- ♦ **kod operacji (OPER):** kod operacji (czyli Opcode) wynosi 1 dla żądania ARP i 2 dla odpowiedzi ARP;
- ♦ **adres sprzętowy wysyłającego (SHA);**
- ♦ **adres IP wysyłającego (SPA);**
- ♦ **adres sprzętowy odbiorcy (THA);**
- ♦ **adres IP odbiorcy (TPA).**

W sieci tylko węzeł z odpowiednim adresem IP odbiorcy może udzielić odpowiedzi na żądanie ARP. Kiedy węzeł otrzyma żądanie, po kolei odczytuje informacje zawarte w tym żądaniu w celu określenia, czy może odpowiedzieć za pomocą sprzętu i protokołów wymienionych w żądaniu, a następnie udziela odpowiedzi. Tylko tabela bufora ARP zawierająca wpis dla adresu IP wysyłającego jest uaktualniana nowymi informacjami umieszczonymi w odpowiedzi. Jeżeli wpis dla danego węzła już istnieje, to zostanie uaktualniony.

## Protokół Reverse Address Resolution Protocol

Zdarzają się sytuacje, gdy urządzenie nie ma adresu IP i nie może utworzyć żądania ARP lub odpowiedzieć na takie żądanie. Najczęściej zdarza się to tzw. cienkim klientom (ang. *thin client*), próbującym nawiązać połączenie z serwerem terminali; w trakcie uruchamiania klienta nie następuje przypisanie adresu IP. Z tego rodzaju sytuacją można się również spotkać, gdy system traci dzierżawę DHCP. W przypadku takich systemów jedynym adresem posiadanym przez system jest adres MAC (adres fizyczny) interfejsu karty sieciowej (NIC). W celu rozwiązania problemu opracowano protokół RARP (ang. *Reverse Address Resolution Protocol*).

Żądanie RARP pochodzi od klienta RARP i rozgłasza adres fizyczny klienta serwerowi RARP. Żądanie i odpowiedź RARP muszą mieć format taki sam jak przedstawiony dla ARP. Różnica między nimi polega na wartościach w poszczególnych polach.

Wprawdzie RARP można skonfigurować tak, aby odpowiedź musiała nadchodzić od serwera RARP o określonym adresie IP, ale w większości przypadków system akceptuje od-

powieść pochodzącą od pierwszego serwera RARP, który mógł jej udzielić. Odpowiedź RARP nie jest rozgłaszana, ale wysyłana bezpośrednio do klienta RARP.

W sieci zazwyczaj znajduje się kilka serwerów RARP, ponieważ jeżeli serwer RARP ulegnie awarii, klient RARP będzie kontynuował rozgłaszanie żądań RARP aż do chwili otrzymania odpowiedzi. Jeżeli w sieci występuje duża liczba klientów rozgłaszających żądania, może to negatywnie wpłynąć na jej dostępność. Powstaje wówczas sytuacja nazywana *burzą żądań RARP*. Niepowodzenie w udzieleniu odpowiedzi na żądanie RARP oznacza, że klient pozostaje nieużyteczny, ponieważ nie może zostać uruchomiony.

Serwery RARP utrzymują tabele odwzorowań adresów IP dla określonych węzłów sieci. Każdy rekord w takiej tabeli ma klucz w postaci unikalnego identyfikatora przypisanego danemu klientowi RARP. Wspomniany unikalny identyfikator musi być wysłany serwerowi, aby możliwe było wygenerowanie odpowiedzi RARP. Ponieważ cienki klient nie ma możliwości przechowywania identyfikatora (gdyż nie można liczyć na to, że będzie posiadał pamięć masową), protokół odczytuje pewne parametry charakterystyczne dla sprzętu danego klienta.

## Przeglądanie bufora ARP

Większość wersji TCP/IP używa polecenia `arp`. Pozwala ono na przeglądanie bufora ARP z poziomu stacji roboczej Linux, Unix, Macintosh oraz Windows. Polecenie ARP używa kilku opcji bądź parametrów, które powodują modyfikację danych wyjściowych. Należy więc sprawdzić dokumentację systemu i ustalić poprawną wersję polecenia do wykorzystywania.

W systemie Windows całą zawartość bufora ARP można przejrzeć za pomocą opcji `-a`. Ponieważ rekordy zawierają informacje o sprzęcie, ARP staje się cennym narzędziem rozwiązywania problemów związanych z powielonymi adresami IP. Poza wymienionym przeznaczeniem polecenie ARP jest obecnie rzadko wykorzystywane. Na rysunku 19.3 pokazano wynik wykonania żądania ARP względem bufora lokalnego w systemie Windows. Dane wyjściowe wyświetlają różne interfejsy sieciowe zarówno fizyczne, jak i wirtualne.

### Rysunek 19.3.

Odpowiedź na wykonanie komendy ARP-a — polecenie pokazuje lokalny bufor ARP

```

C:\>arp -a

Interfejs: 192.168.1.3 --- 0x0
    Adres internetowy    Adres fizyczny    Typ
    192.168.1.1          00-1d-7e-fb-39-f8 dynamiczne
    192.168.1.2          00-0c-6e-d7-05-57 dynamiczne
    192.168.1.255        ff-ff-ff-ff-ff-ff statyczne
    224.0.0.22           01-00-5e-00-00-16 statyczne
    224.0.0.251          01-00-5e-00-00-fb statyczne
    224.0.0.252          01-00-5e-00-00-fc statyczne
    239.255.255.250      01-00-5e-7f-ff-fa statyczne
    255.255.255.255      ff-ff-ff-ff-ff-ff statyczne

Interfejs: 192.168.153.1 --- 0x0
    Adres internetowy    Adres fizyczny    Typ
    192.168.153.255      ff-ff-ff-ff-ff-ff statyczne
    224.0.0.22           01-00-5e-00-00-16 statyczne
    224.0.0.251          01-00-5e-00-00-fb statyczne
    224.0.0.252          01-00-5e-00-00-fc statyczne
    239.255.255.250      01-00-5e-7f-ff-fa statyczne

Interfejs: 192.168.209.1 --- 0x10
    Adres internetowy    Adres fizyczny    Typ
    192.168.209.255      ff-ff-ff-ff-ff-ff statyczne
    224.0.0.22           01-00-5e-00-00-16 statyczne
    224.0.0.251          01-00-5e-00-00-fb statyczne
    224.0.0.252          01-00-5e-00-00-fc statyczne
    239.255.255.250      01-00-5e-7f-ff-fa statyczne

C:\>
  
```

## Podstawowy system wejścia-wyjścia sieci

NetBIOS to usługa warstwy sesji (warstwa 5.) udostępniająca sieciowy interfejs programowania aplikacji (API), który pozwala starszym aplikacjom na komunikację z innymi w ramach sieci lokalnej (LAN). Skrót NetBIOS oznacza *Network Basic Input/Output System*. NetBIOS był wczesnym protokołem PC opracowanym przez firmę o nazwie Sytek dla komputerów IBM PC i został przedstawiony w roku 1983. Stał się standardem przemysłowym dla komputerów osobistych, nawet pomimo początkowego ograniczenia do obsługi jedynie osiemdziesięciu systemów.

Dopóki firma Microsoft w pełni nie zaadaptowała określania nazw za pomocą DNS, NetBIOS stanowił podstawową metodę określania nazw w sieciach Windows. NetBIOS jest wymagany przez wiele starszych aplikacji w sieciach Windows. Warto zwrócić uwagę, że NetBIOS to protokół nieroutowalny.

Ruch sieciowy NetBIOS jest transportowany za pomocą protokołów takich jak TCP/IP (NetBIOS poprzez TCP lub NBT), IPX/SPX (przestarzały, rodzimy format Novell Netware) lub NBF (NetBIOS poprzez IEEE 802.2); wszystkie wymienione są protokołami warstwy drugiej, czyli warstwy łącza danych.

Nazwy NetBIOS mogą być inne niż nazwy przypisane systemowi w TCP/IP, są ograniczone do piętnastu znaków i nie mogą zawierać spacji oraz poniższych znaków:

| ; " \* ? / \

Podczas instalacji systemu Windows podawana nazwa systemu staje się nazwą NetBIOS. Nazwę tę można zmienić za pomocą zakładki *Nazwa komputera* we właściwościach systemu (*Panel sterowania/System*). W większości przypadków nazwa komputera używana przez DNS powstaje przez dołączenie prefiksu w postaci nazwy NetBIOS do przyrostka podstawowego adresu DNS. Dlatego też jeżeli nazwa NetBIOS to *MójKomputer*, a przyrostek DNS to *MojaFirma.pl*, to nazwa komputera macierzystego używana przez DNS będzie miała postać *MójKomputer.MojaFirma.pl*.

Określanie nazwy za pomocą NetBIOS zostało porzucone na rzecz technologii DNS. Firma Microsoft nie zapewni obsługi określania nazw za pomocą NetBIOS w sieciach IPv6.

Określanie nazw przy zastosowaniu metody NetBIOS odbywa się za pomocą rozgłaszania, które sprawdza się doskonale w małych sieciach, lub za pomocą serwera WINS, zapewniającego określanie nazw NetBIOS w większych sieciach. Serwer WINS zostanie dokładniej omówiony w kolejnym podrozdziale. W zależności od konfiguracji systemu określanie nazw może być jedynie typu B (tylko rozgłaszanie), P (partnerskie lub tylko WINS), M (połączenie typów, najpierw rozgłaszanie, a później WINS) lub H (hybrydowe, najpierw WINS, a dopiero później rozgłaszanie).

Usługa NetBIOS wykonuje trzy zadania: rejestruje i określa nazwy, zarządza usługą sesji używaną podczas połączenia oraz wysyła datagramy (pakiety wysyłane poprzez zawodną sieć), które nie wymagają nazwanego połączenia.

Podczas określania nazw za pomocą NetBIOS system Windows używa także pliku wyszukiwania o nazwie *lmhosts*. Plik ten działa podobnie do pliku *hosts*, omówionego w poprzednim podrozdziale. W systemie Vista plik ten znajduje się w katalogu *C:\Windows\System32\drivers\etc* i ma rozszerzenie *.sam*. Można go otworzyć za pomocą Notatnika, jak pokazano na rysunku 19.4.

**Rysunek 19.4.**  
Plik *lmhosts*  
zapewnia metodzie  
NetBIOS możliwość  
wyszukiwania i ma  
pierwszeństwo przed  
wyszukiwaniem za  
pomocą serwera  
WINS



```
# Copyright (c) 1993-1999 Microsoft Corp.
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for windows.
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names. Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
# This file is compatible with Microsoft LAN Manager 2.x TCP/IP lmhosts
# files and offers the following extensions:
#
# #PRE
# #DOM:<domain>
# #INCLUDE <filename>
# #BEGIN_ALTERNATE
# #END_ALTERNATE
# \Oxnn (non-printing character support)
#
# Following any entry in the file with the characters "#PRE" will cause
# the entry to be preloaded into the name cache. By default, entries are
# not preloaded, but are parsed only after dynamic name resolution fails.
#
# Following an entry with the "#DOM:<domain>" tag will associate the
# entry with the domain specified by <domain>. This affects how the
# browser and logon services behave in TCP/IP environments. To preload
# the host name associated with #DOM entry, it is necessary to also add a
# #PRE to the line. The <domain> is always preloaded although it will not
# be shown when the name cache is viewed.
#
# Specifying "#INCLUDE <filename>" will force the RFC NetBIOS (NBT)
# software to seek the specified <filename> and parse it as if it were
# local. <filename> is generally a UNC-based name, allowing a
# centralized lmhosts file to be maintained on a server.
# It is ALWAYS necessary to provide a mapping for the IP address of the
# server prior to the #INCLUDE. This mapping must use the #PRE directive.
# In addition the share "public" in the example below must be in the
# LanManServer list of "NullSessionShares" in order for client machines to
# be able to read the lmhosts file successfully. This key is under
# \machine\system\currentcontrolset\services\lanmanserver\parameters\nullsessi
# in the registry. Simply add "public" to the list found there.
#
# The #BEGIN_ and #END_ALTERNATE keywords allow multiple #INCLUDE
# statements to be grouped together. Any single successful include
# will cause the group to succeed.
#
# Finally, non-printing characters can be embedded in mappings by
# first surrounding the NetBIOS name in quotations, then using the
# \Oxnn notation to specify a hex value for a non-printing character.
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97      rhino      #PRE #DOM:networking #net group's DC
# 102.54.94.102     "apname"  \Ox14  #special app server
# 102.54.94.123     popular   #PRE      #source server
# 102.54.94.117     localsrv  #PRE      #needed for the include
#
# #BEGIN_ALTERNATE
```

## Windows Internet Name Service

WINS (ang. *Windows Internet Name Service*) to technologia serwerowa firmy Microsoft służąca do określania nazw NetBIOS. WINS tłumaczy adresy sieciowe na nazwy NetBIOS, podobnie jak DNS tłumaczy adresy TCP/IP na w pełni kwalifikowane nazwy domen (FQDN). Dokładne omówienie DNS znajdzie się w kolejnym podrozdziale.

Technologia WINS została zaimplementowana jako baza danych w serwerze Windows wraz z interfejsem pozwalającym na zarządzanie. Kiedy klient WINS jest uruchamiany, wysłał do serwera WINS żądanie rejestracji nazwy, a nazwa i powiązany z nim adres zostają

zarejestrowane jako rekord bazy danych. Jeżeli inny klient będzie musiał komunikować się z tym pierwszym klientem, to wysyła do serwera zapytanie WINS wraz z nazwą pierwszego klienta. Serwer odpowiada na żądanie przez wysłanie adresu IP pierwszego klienta.

W dużych sieciach serwer WINS zmniejsza obciążenie związane z określaniem nazw NetBIOS przez dostarczanie znacznie efektywniejszego mechanizmu niż zapytania bazujące na rozgłaszaniu. Technologia WINS jest z reguły wykorzystywana w większych organizacjach w postaci wielu serwerów i zawiera usługę replikacji w celu dalszego przekazywania wprowadzonych zmian.

Usługa *Windows Computer Browser Service* wypełniająca informacjami katalog sieci w Windows może używać WINS w celu tworzenia list przeglądania. Wprawdzie NetBIOS nie pozwala na routing, ale wysyłanie list przeglądania — już tak.

Technologie określania nazw WINS i DNS mogą działać jednocześnie w tej samej sieci bez powodowania wzajemnych konfliktów. Obie przechowują nazwy w oddzielnych przestrzeniach nazw; DNS używa struktury hierarchicznej, podczas gdy WINS stosuje strukturę płaską. Technologia WINS jest istotna w sieciach, w których nadal funkcjonują systemy Windows 2000, XP lub Windows Server 2003. W sieciach używających jednocześnie nazw NetBIOS i nazw domen wymagana jest dostępność usług WINS i DNS.

## Domain Name System

DNS (ang. *Domain Name System*) to system używany do tłumaczenia adresów IP na nazwy przyjazne dla człowieka. Jest to usługa wykorzystywana w internecie i obecnie używana w niemal wszystkich sieciach LAN TCP/IP. DNS przechowuje również informacje dotyczące serwerów poczty. W końcu system może być zastosowany także do przechowywania wszelkiego rodzaju informacji, na przykład znaczników RFID (ang. *Radio-Frequency Identification*).

Pierwszą implementację systemu DNS opracowano w 1983 roku na podstawie dokumentów RFC. Obecnie powszechnie używana w internecie wersja oprogramowania DNS została napisana dla systemu Unix i pojawiła się w roku 1984 na uniwersytecie Berkeley. Na przestrzeni lat była oczywiście poprawiana i rozbudowywana. Ta wersja oprogramowania DNS, nazwana BIND (ang. *Berkeley Internet Name Domain*), to oprogramowanie typu open source, które intensywnie przetestowano i dopracowano w szczegółach. Wraz z wydaniem Windows NT oprogramowanie BIND zagościło w systemie Microsoft Windows. Oprogramowanie BIND jest utrzymywane przez konsorcjum Internet Systems Consortium (<http://www.isc.org/products/BIND/>).

DNS działa, przechowując rekordy w bazie danych znajdującej się na serwerze nazw, który jest odpowiedzialny za ich tłumaczenie dla określonej domeny. 13 serwerów DNS, tzw. root servers, obsługuje domeny najwyższego poziomu (TLD — ang. *top level domains*): *.com*, *.net*, *.gov*, *.edu*, *.us*, *.uk*, *.ch* itd., nadzór nad domenami TLD jest sprawowany przez ICANN. W celu zwiększenia wydajności systemu i jego odporności na awarie w sieci istnieje wiele kopii głównych serwerów, które są osiągalne pod tym samym adresem IP.



Domeny najwyższego poziomu (TLD, ang. *Top-Level Domains*) są zarządzane przez ICANN (ang. *Internet Corporation for Assigned Names and Numbers*), organizację typu non profit, mieszczącą się w Marina del Rey, w Kalifornii (<http://www.icann.org>).

Czytelnik prawdopodobnie zna podstawową strukturę domen. Domeny najwyższego poziomu (na przykład *.com*) są oddzielone od domen drugiego poziomu (*mojadomena*) kropką, jak w domenie *mojadomena.com*. Domeny przed dalszym podziałem bazują na dostarczanych usługach, tak więc *www.mojadomena.com* będzie jedną z subdomen, podobnie jak *ftp.mojadomena.com*. Trzeba pamiętać, że *mojadomena.com* i *www.mojadomena.com* nie są równorzędnymi odpowiednikami — ta druga jest subdomeną tej pierwszej, ale oba wymienione adresy mogą wskazywać na konkretne urządzenie. Specyfikacja DNS pozwala na użycie do 127 poziomów, do 63 znaków na poziom i do 255 znaków dla całej domeny.

## Żądania DNS

Żądanie DNS zainicjowane dla strony internetowej z poziomu określonej witryny nie przechodzi przez podstawowy bądź drugorzędny serwer nazw dla tej domeny. Zamiast tego przechodzi poziom po poziomie, aby mogło być zrealizowane za pomocą najbliższego źródła DNS. Przechodzi więc przez system lokalny i sprawdza, czy nazwa znajduje się w buforze DNS. Jeżeli zostanie znaleziona, to żądanie zwraca wynik. Normalnie lokalny bufor DNS nie przechowuje wielu rekordów. Nie wszystkie systemy operacyjne włączają lokalny bufor DNS; w dystrybucjach systemu Linux może wystąpić konieczność zainstalowania pakietu włączającego tę funkcję.

W systemie Windows zawartość bufora lokalnego można wyświetlić za pomocą polecenia `ipconfig /displaydns`. Na rysunku 19.5 pokazano przykładowe dane wyjściowe w 64-bitowym systemie Windows Vista. Dane wyjściowe tego polecenia zawierają nazwę rekordu w domenie, typ rekordu, wartości TTL (ang. *Time To Live*) oraz w ostatnim wierszu adres rekordu. Jeżeli zachodzi potrzeba wyczyszczenia zawartości bufora lokalnego, to można wydać polecenie `ipconfig /flushdns`.

### Rysunek 19.5.

W celu wyświetlenia bieżącej zawartości lokalnego bufora DNS w systemie Windows należy wydać polecenie `ipconfig /displaydns`

```
Wiersz polecenia
C:\Documents and Settings\Robert>ipconfig /displaydns

Konfiguracja IP systemu Windows

s4.hit.stat.pl
-----
Nazwa rekordu . . . . . : s4.hit.stat.pl
Typ rekordu . . . . . : 1
Czas wygaśnięcia (licznik TTL): 744
Długość danych . . . . . : 4
Sekcja . . . . . : Odpowiedź
Rekord (hosta). . . . . : 217.17.36.254

1.0.0.127.in-addr.arpa
-----
Nazwa rekordu . . . . . : 1.0.0.127.in-addr.arpa.
Typ rekordu . . . . . : 12
Czas wygaśnięcia (licznik TTL): 604610
Długość danych . . . . . : 4
Sekcja . . . . . : Odpowiedź
Rekord PTR . . . . . : localhost

www.google-analytics.com
-----
Nazwa rekordu . . . . . : www.google-analytics.com
Typ rekordu . . . . . : 5
Czas wygaśnięcia (licznik TTL): 191
Długość danych . . . . . : 4
Sekcja . . . . . : Odpowiedź
Rekord CNAME . . . . . : www-google-analytics.l.google.com
```

Lokalny bufor DNS nie przechowuje wielu rekordów (w zależności od jego konfiguracji). Jeżeli wymagany rekord nie znajduje się w buforze bądź jego ważność wygasła (wartość TTL, liczona w sekundach, spadła do zera), to żądanie jest przekazywane do lokalnego serwera DNS. W przypadku używania DNS w dużej sieci, gdzie wymagane jest rozwiązywanie nazw dla lokalnych zasobów, sieć prawdopodobnie ma własny serwer DNS. W przypadku małych sieci i używania DNS do określania nazw internetowych żądania DNS są przekazywane do serwerów DNS zdefiniowanych w opcjach konfiguracyjnych TCP/IP lub tych, które zostały przypisane automatycznie, o ile wybrano taką opcję.

Wiele zapór sieciowych i urządzeń internetowych jest dostarczanych wraz z serwerami DNS. Tak więc używanie ich jako podstawowych serwerów DNS dla danego połączenia z reguły będzie szybsze niż oczekiwanie na odpowiedź serwera DNS znajdującego się w internecie. Większość osób przyjmuje założenie, że DNS wymaga podania adresu DNS serwera dostawcy usług internetowych (ISP) w opcjach konfiguracyjnych TCP/IP. Jednak to nieprawda. Do tego celu można wykorzystać dostępne serwery DNS o dużej wydajności.

Przy założeniu, że żądanie DNS nie może być spełnione przez bufor lokalny bądź usługę DNS w sieci lokalnej, jest ono przekazywane do serwera DNS znajdującego się poza siecią lokalną. Serwer DNS sprawdza w buforze rekord powiązany z nazwą, której adres jest mu podawany. Jeżeli rekord nie zostanie znaleziony, żądanie jest kierowane do serwera nazw obsługującego domenę główną żądanej domeny, jeśli adres tego serwera jest znany. Ostatecznie żądanie może dotrzeć do głównego serwera nazw, ale to bardzo rzadka sytuacja. Funkcja replikacji DNS wypełnia serwery drugorzędne najważniejszymi adresami. Jeżeli Czytelnik kiedykolwiek zastanawiał się, dlaczego zmiana serwera DNS dla domeny zwykle trwa 24 do 36 godzin, to odpowiedzią jest właśnie proces replikacji.

DNS to architektura typu klient-serwer, a oprogramowanie klienta jest określane mianem *resolver*. Kiedy klient wykonuje zapytanie DNS, może być ono w jednym z dwóch dostępnych typów: rekurencyjnym bądź iteracyjnym. W zapytaniu rekurencyjnym, częściej stosowanym, serwer DNS musi zwrócić odpowiedź; w tym celu wykonuje zapytania do innych serwerów DNS lub zwraca informację o błędzie. W zapytaniu iteracyjnym serwer DNS może dostarczyć odpowiedź częściową, wskazując inny serwer DNS jako posiadający informacje bardziej szczegółowe lub błąd. Resolver może być skonfigurowany w celu używania dowolnego z wymienionych typów zapytań.

Warto przeanalizować zapytanie o adres IP dla przykładowego komputera o nazwie *www.mojadomena.com*. Zapytanie DNS zostaje wykonane i wysłane do głównego serwera nazw. Główny serwer nazw nie zawiera rekordu, więc odpowiedź jest wysłana do modułu o nazwie *DNS recursor* wraz z adresem następnego serwera nazw w łańcuchu. Wspomniany recursor wysłał żądanie do drugiego serwera nazw na niższym poziomie, który będzie miał odpowiedni rekord albo wyśle odpowiedź do recursora DNS wraz z nazwą kolejnego serwera nazw w łańcuchu. Proces jest powtarzany wielokrotnie, aż do znalezienia adresu IP.

Kiedy wykonanie zapytania zakończy się powodzeniem i nastąpi zwrócenie wyniku, rekord zasobu (RR, ang. *resource record*) dla danej odpowiedzi będzie przechowywany w buforze serwera DNS. Liczba zachowanych rekordów będzie wypadkową zarówno wielkości bufora, jak i wartości TTL rekordów. Nie wszystkie zapytania są wyszukiwaniami do przodu, to

znaczy, gdy zapytanie rozpoczyna się od nazwy domenowej, a wynik zwraca adres IP. Pewne zapytania DNS są zapytaniami odwrotnymi. Stosowane są, gdy posiadając adres IP, chcemy uzyskać odpowiadający mu adres domeny. Zapytania odwrotne są obsługiwane przez oprogramowanie firm trzecich.

W praktyce główne serwery nazw i wiele serwerów DNS górnego poziomu są buforowane w różnych miejscach i prawie nigdy bezpośrednio nie obsługują ządań DNS.

Technologia DNS nie jest pozbawiona wad. Jeśli serwer pytany o adres domeny zwraca nam w odpowiedzi adres serwera DNS, który jest adresem podrzędnym tej domeny, następuje zapętlenie. Na przykład pytając o domenę *helion.pl*, otrzymujemy w odpowiedzi adres serwera *dns.helion.pl*. W celu rozwiązania tego problemu serwer do swojej odpowiedzi dołącza tzw. *glue record*, który zawiera adres IP serwera niższego rzędu.

## Topologia DNS

DNS to hierarchiczna przestrzeń nazw, co oznacza, że ma strukturę odwróconego drzewa, podobną do struktury systemu plików na dysku twardym. Węzeł najwyższego poziomu w przestrzeni nazw jest zajmowany przez dobrze poinformowany serwer nazw, określany jako podstawowy bądź główny serwer nazw. Ten serwer zawiera to, co określone jest mianem *rekordów zasobów*, które łączą ten serwer nazw z innymi, zawierającymi rekordy zasobów do kolejnych serwerów nazw, podobnie jak w przypadku rozgałęzień drzewa.

Każde kolejne odgałęzienie drzewa jest zorganizowane w postaci *stref wpływów*, wszystkie połączone węzły (serwery DNS) odwołują się do najwyższego poziomu odgałęzienia jako ich podstawowego serwera nazw. W domenie *MojaFirma.com* strefa może składać się z serwera na poziomie *www.MojaFirma.com* i odpowiada za strefy znajdujące się poniżej. W żargonie DNS domena jest wskazywana przez rekord określany jako SOA (ang. *Start of Authority*, początek strefy wpływów) i ten rekord jest wówczas powiązany z głównym serwerem DNS tej domeny, czyli serwerem dostarczającym informacji autorytatywnych dla tej domeny.

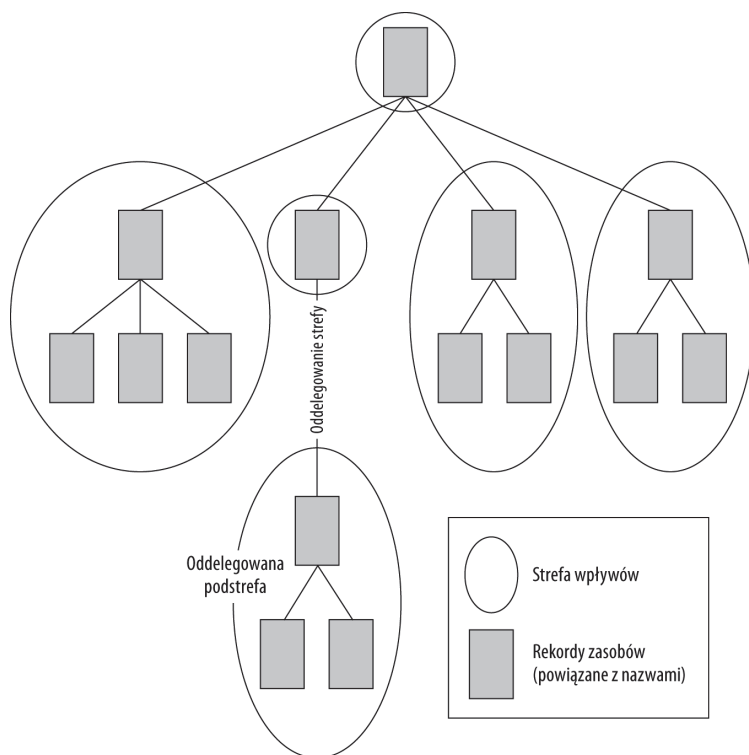
Jeżeli w subdomenie podstawowy serwer DNS to *MójSerwerDNS*, to jego adresem będzie *MójSerwerDNS.MojaFirma.com*. Ponieważ wpływy zostały oddelegowane do *www.MojaFirma.com*, ten serwer DNS stanie się podstawowym serwerem DNS dla strefy *MojaFirma.com*. Właścicielem serwera jest *root@MójSerwerDNS.MojaFirma.com*, natomiast adres znajdujący się w rekordzie SOA to *root.MójSerwerDNS.MojaFirma.com*.

Na rysunku 19.6 pokazano przestrzeń nazw DNS.

Na rysunku 19.6 strefa na górze funkcjonuje jako główny serwer DNS. To może być główny serwer *.com*, *.gov*, *.edu* bądź jakiegokolwiek inny. Wraz z podziałem drzewa DNS oddelegowuje wpływy do odpowiedzi na zapytania DNS do serwerów DNS stref. Dany serwer obsługuje wszystkie zapytania DNS dla danej strefy i stref znajdujących się poniżej, o ile zachodzi taka potrzeba. Serwer każdego poziomu strefy DNS oddelegowuje wpływy do podstref znajdujących się poniżej, tak więc wpływy są przekazywane z serwera DNS najwyższego poziomu do serwerów będących niżej w hierarchii. Celem hierarchii DNS jest obsłużenie zapytania DNS na możliwie najniższym poziomie drzewa.

**Rysunek 19.6.**

Przestrzeń nazw DNS



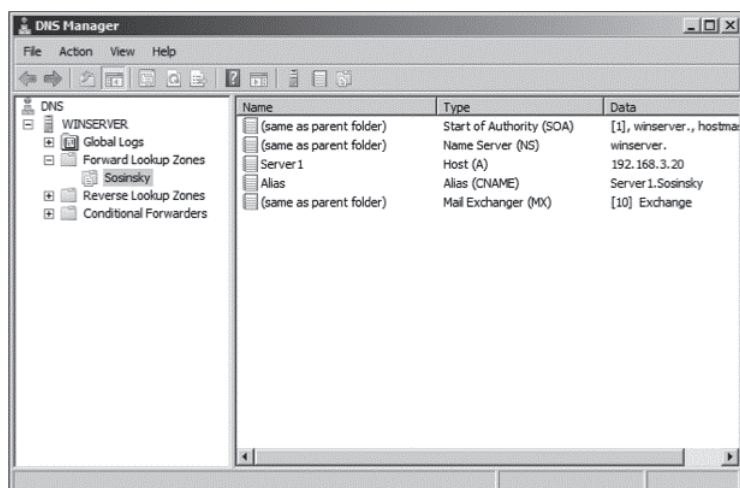
## Rekordy zasobów

Technologia DNS jest zaimplementowana w postaci systemu bazy danych, którą można zarządzać za pomocą zestawu poleceń w interfejsie wiersza poleceń (CLI, ang. *Command Line Interface*) albo narzędzi zarządzających graficznego interfejsu użytkownika (GUI, ang. *Graphical User Interface*). System pozwala na stosowanie pomocniczego serwera DNS, jak również systemów replikacji.

W Windows Server 2008 DNS jest rolą, którą można zainstalować na serwerze. Z powodów bezpieczeństwa Windows nie pozwala, aby usługa DNS została zainstalowana w kontrolerze domeny (choć może być uruchomiona w RODC (ang. *Read-Only Domain Controller*)), ale rola DNS współlistnieje z wieloma innymi rolami serwerowymi. W dużych domenach aktywność DNS to jedna z bardziej wymagających ról, która może angażować serwer. Powszechnie stosowaną praktyką jest używanie oddzielnego serwera dedykowanego dla usługi DNS.

Po zainstalowaniu DNS system Windows Server 2008 dodaje do listy narzędzi w katalogu *Narzędzia administracyjne* menedżera DNS. Menedżer DNS (podobnie jak inne narzędzia administracyjne) jest konsolą zarządzania (MMC, ang. *Microsoft Management Console*), która stanowi rodzaj struktury obsługującej różne zapytania do baz danych. Na rysunku 19.7 pokazano przykładową domenę w menedżerze DNS. Warto zwrócić uwagę na kilka różnego typu rekordów wypełniających węzeł *Forward Lookup Zones*, który został rozwinięty i pokazany na rysunku.

**Rysunek 19.7.**  
Menedżer DNS  
w systemie Windows  
Server 2008

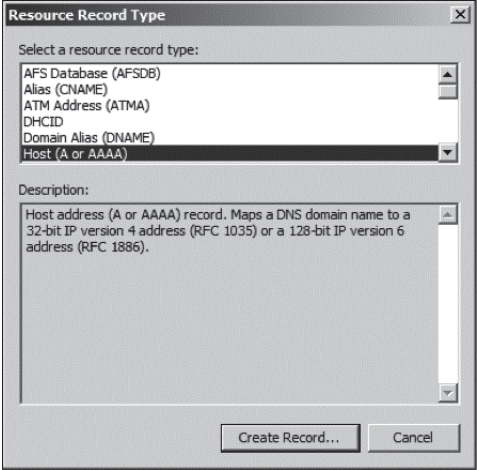


Na rysunku 19.7 pokazano kilka powszechnie stosowanych typów rekordów z wyjątkiem rekordów PTR, używanych przez DNS do realizacji zapytań odwrotnych. Możliwe do użycia rekordy obejmują między innymi:

- ♦ **Start of Authority (SOA).** Rekord SOA wskazuje serwer odpowiedzialny za daną strefę.
- ♦ **Name Server (NS).** Rekord NS jest używany przez DNS do wyświetlania adresu serwera nazw dla danej domeny. Dla każdej domeny musi istnieć co najmniej jeden wpis. Ponieważ niemal wszystkie domeny używają wielu serwerów nazw, co ma podnieść ich odporność na awarie, to bardzo często spotyka się dwa lub więcej wpisów rekordów NS.
- ♦ **Address (A).** Rekord A (lub rekord adresu) powinien przedstawiać zbiór rekordów w bazie danych DNS dla sieci dowolnego rodzaju. Rekord A zapewnia mapowanie nazw domen na adresy IP.
- ♦ **Canonical Name (CNAME).** Rekord CNAME jest aliasem nazwy domeny. Alias prowadzi do nazwy domeny wymienionej w pierwszym polu rekordu. W przypadku rekordu pokazanego na rysunku CNAME jest czwartym rekordem, a nazwa domeny to *AliasName*. Rekordy CNAME są czasami używane, kiedy zachodzi potrzeba ukrycia przed klientem prawdziwej nazwy systemu.
- ♦ **Mail Exchange (MX).** Rekord MX jest używany do wskazania serwera poczty elektronicznej w domenie.
- ♦ **Pointer (PTR).** Rekordy PTR (nie zostały pokazane na rysunku 19.7) są używane w celu mapowania adresów IP na przypisane im nazwy domenowe. Powodem tworzenia rekordów PTR jest obsługa zapytań odwrotnych. Z tego powodu zapytania odwrotne są czasami nazywane zapytaniami PTR. Podczas używania rekordów PTR ważne jest, aby upewnić się, że pozostają aktualne oraz zawierają takie same informacje jak te, które znajdują się w rekordach A.

Poniższa lista zawiera najczęściej spotykane rekordy zasobów DNS używane podczas określania nazw. Jak już wcześniej wspomniano, rekordy DNS mogą być tworzone dla wielu różnych zasobów. Pokazane na rysunku 19.8 okno dialogowe *Resource Record Type* wymienia

**Rysunek 19.8.**  
Okno dialogowe  
*Resource Record Type*



różne typy rekordów zasobów obecnie obsługiwanych przez Windows Server 2008. W tabeli 19.2 przedstawiono opisy typów rekordów wymienionych w oknie dialogowym *Resource Record Type*, pokazanym na rysunku 19.8.

**Tabela 19.2.** Typy rekordów zasobów

Typ rekordu zasobu	Opis
AFS Database (AFSDB)	Rekord serwera AFSDB (ang. <i>Andrew File System Database</i> ), który wskazuje położenie dowolnego z wymienionych poniżej standardowych podtypów serwera — położenie woluminu AFS lub serwer nazw uwierzytelniony przez DCE (ang. <i>Distributed Computing Environment</i> ). Ponadto obsługuje inne, zdefiniowane przez użytkownika podtypy serwerów używające formatu rekordu zasobów. (RFC 1183)
Alias (CNAME)	Rekord Alias — wskazuje alternatywę, czyli alias nazwy domeny DNS dla nazwy podanej w innych typach rekordu zasobów w danej strefie. Rekord ten jest znany jako rekord typu <i>Canonical Name</i> (CNAME). (RFC 1035)
ATM Address (ATMA)	Rekord ATM Address (ATMA) — mapuje nazwę domeny DNS na adres ATM.
Host Address (A lub AAAA)	Mapuje nazwę domeny DNS na 32-bitowy adres IPv4 (RF 1035) lub 128-bitowy adres IPv6. (RFC 1886)
Host Information (HINFO)	Rekord <i>Host Information</i> (HINFO) — wskazuje (RFC 1700) zarezerwowany ciąg tekstowy wartości dla typu procesora i systemu operacyjnego w celu mapowania do określonych nazw komputerów macierzystych DNS. Informacje te są używane przez protokoły aplikacji, takie jak FTP, które mogą używać specjalnych procedur podczas komunikacji między komputerami z takim samym typem procesora i systemu operacyjnego. (RFC 1035)
Integrated Services Digital Network (ISDN)	Mapuje nazwę domeny DNS na numer telefonu ISDN. Numery telefonów ISDN używane wraz z tym rekordem spełniają międzynarodowe standardy numerów telefonów CCITT E.163/E.164. (RFC 1183)
Mail Exchange (MX)	Wskazuje adresy serwerów poczty elektronicznej w domenie. Rekordy MX używają 16-bitowej liczby całkowitej w celu wskazania priorytetu serwera, wykorzystywanej w przypadku zastosowania wielu rekordów MX w domenie. Każdy serwer wskazany rekordem MX wymaga rekordu typu A z przypisanym adresem IP. (RFC 1035)

**Tabela 19.2.** Typy rekordów zasobów — ciąg dalszy

Typ rekordu zasobu	Opis
Mail Group (MG)	Dodaje skrzynki pocztowe domeny (każda określona przez rekord MB w bieżącej strefie) jako członków grupy dyskusyjnej domeny, która jest identyfikowana przez nazwę w tym rekordzie. (RFC 1035)
Mailbox (MB)	Mapuje określoną nazwę skrzynki pocztowej domeny do hosta, który będzie zajmował się obsługą tej skrzynki pocztowej. (RFC 1035)
Mailbox Information (MINFO)	Wskazuje nazwę skrzynki pocztowej domeny służącej do celów kontaktowych. Te informacje kontaktowe obsługują listę dyskusyjną bądź skrzynkę pocztową podaną w rekordzie. Ponadto rekord wskazuje skrzynkę pocztową przeznaczoną do otrzymywania komunikatów o błędach powiązanych z listą dyskusyjną lub skrzynką pocztową wymienioną w rekordzie MINFO. (RFC 1035)
Next (NXT)	Rekord zasobu NXT — wskazuje nieistniejącą nazwę w strefie przez utworzenie łańcucha wszystkich dosłownych nazw właściciela w tej strefie. Rekord ten wskazuje również typy rekordów zasobu dostępne dla istniejących nazw.
Pointer (PTR)	Wskazuje położenie w przestrzeni nazw domeny. Rekordy PTR są zwykle używane w domenach specjalnych w celu przeprowadzania zapytania odwrotnego (odzworowanie adresu IP na nazwę domeny). Kiedy używane są rekordy PTR, nie jest stosowane żadne dodatkowe przetwarzanie sekcji. (RFC 1035)
Public Key (KEY)	Rekord <i>Public Key</i> (KEY) — przechowuje klucz publiczny, który jest powiązany z nazwą domeny DNS. Klucz ten może być strefą, użytkownikiem, hostem bądź inną jednostką końcową. Rekord zasobu KEY jest uwierzytelniany za pomocą rekordu zasobu SIG. Klucz poziomu strefy musi podpisać rekordy typu KEY.
Rename Mailbox (MR)	Wskazuje nazwę skrzynki pocztowej domeny dla rekordu RP i mapuje tę nazwę do nazwy domeny, dla której istnieje rekord zasobu TXT. Kiedy w zapytaniach DNS są używane rekordy RP, kolejne zapytania mogą wymagać otrzymania rekordu TXT mapowanego za pomocą rekordu typu RP. (RFC 1183)
Responsible Person (RP)	Rekord <i>Responsible Person</i> (RP) — wskazuje nazwę skrzynki pocztowej osoby odpowiedzialnej i mapuje tę nazwę do nazwy domeny, dla której istnieje rekord TXT. Kiedy w zapytaniach DNS są używane rekordy RP, kolejne zapytania mogą wymagać otrzymania rekordu TXT mapowanego za pomocą rekordu typu RP. (RFC 1183)
Route Through (RT)	Rekord <i>Route Through</i> (RT) — podaje trasę pośrednią łączącą wewnętrzne komputery, które nie mają własnych bezpośrednich adresów WAN (ang. <i>Wide Area Network</i> ). W celu wskazania dwóch wymaganych pól rekord ten używa takiego samego formatu danych jak rekord typu MX: 16-bitowej liczby całkowitej przedstawiającej preferencje dla każdej trasy pośredniej oraz nazwę domeny DNS dla komputera macierzystego, przez który przechodzi trasa w postaci, w jakiej pojawia się w rekordach A, X25 i ISDN dla strefy. (RFC 1183)
Service Location (SRV)	Rekord <i>Service Location</i> (SRV) — pozwala administratorom na używanie kilku serwerów dla pojedynczej domeny DNS. Umożliwia to łatwe przeniesienie usługi TCP/IP z jednego serwera na inny oraz wyznaczenie pewnych serwerów jako podstawowych dla usługi, a innych jako ich kopii zapasowych. Klienci DNS używające zapytania typu SRV pytają o określoną usługę TCP/IP i protokół mapowany do danej domeny DNS oraz otrzymują nazwy wszystkich dostępnych serwerów. (RFC 2052)

**Tabela 19.2.** Typy rekordów zasobów — ciąg dalszy

Typ rekordu zasobu	Opis
Signature (SIG)	Rekord szyfrowanego podpisu (SIG) — uwierzytelnia zestaw rekordów zasobów określonego typu, klasy bądź nazwy i dołącza je z wewnętrznym przedziałem czasu oraz nazwą domeny DNS podpisującego. Wspomniane uwierzytelnianie oraz dołączanie jest przeprowadzane za pomocą technik kryptograficznych oraz klucza prywatnego podpisującego. Bardzo często podpisujący jest właścicielem stref, z której pochodzą podpisywane rekordy.
Text (TXT)	Rekord TXT — przechowuje ciąg tekstowy znaków służących w charakterze tekstu opisu powiązanego z określoną nazwą domeny DNS. Semantyka rzeczywistego tekstu opisującego, używanego jako data dla tego rekordu, zależy od domeny DNS, w której ten rekord jest umieszczony. (RFC 1035)
Well-Known Services (WKS)	Rekord <i>Well-Known Services</i> (WKS) — opisuje doskonale znane usługi TCP/IP obsługiwane przez określony protokół w danym adresie IP. Rekordy WKS dostarczają informacji o dostępności TCP i UDP dla serwerów TCP/IP. Jeżeli serwer obsługuje zarówno TCP, jak i UDP dla doskonale znanych usług lub jeśli serwer ma wiele adresów IP obsługujących usługę, to używa się wielu rekordów WKS. (RFC 1035)
X.25	Rekord X.25 — mapuje nazwę domeny DNS do adresu PSDN (ang. <i>Public Switched Data Network</i> ), takiego jak adresy X.121, które są zwykle używane w celu identyfikacji każdego punktu usługi mieszczącego się w publicznej sieci X.25. (RFC 1183)

Źródło: Microsoft Corporation, okno dialogowe *Record Resource Types* w systemie operacyjnym Windows Server 2008.

## Określanie nazw kontra usługi katalogowe

Usługi katalogowe są produktami, które w większości przypadków spełniają standard X.500 LDAP. Przykładami usług katalogowych są między innymi Windows Active Directory, Network Information Service, używane przez system Solaris oraz inne implementacje Unix i Linux, jak doskonały eDirectory firmy Novell. Podstawowym zadaniem usługi katalogowej jest bezpieczne przechowywanie danych identyfikacyjnych oraz właściwości dla obiektów sieciowych. Wspomniane obiekty sieciowe obejmują systemy, nazwy komputerów macierzystych i informacje o zasobach, a także obiekty takie jak konto i grupa użytkownika, charakterystyczne dla systemu operacyjnego struktury organizacyjne domeny, dane aplikacji oraz niemal wszystko inne, co producent systemu operacyjnego i firmy trzecie w nich umieszczają. Usługi katalogowe można rozszerzać i, co ważniejsze, pozostają bezpieczne i chronione. Chociaż określanie nazw jest jednym z podstawowych zadań usługi katalogowej, nie jest to jednak jej jedyne zadanie i tak naprawdę nie jest to podstawowa funkcja tych systemów.

Usługi określania nazw mają znacznie skromniejszą rolę. Koncentrują się na funkcji mapowania i mają kilka ograniczonych możliwości rozszerzenia. Efekt tych różnic można zaobserwować na przykładzie implementacji DNS. Wprawdzie technologia DNS jest stosowana do identyfikacji systemów w internecie oraz niemal powszechnie używana do identyfikacji systemów w sieciach LAN, ale nie są wykorzystywane jej wszystkie możliwości, wskazuje na to wiele nieużywanych typów rekordów, przedstawionych w poprzednim podrozdziale.

Użycie usług katalogowych powoduje zawieszenie stosowania DNS do innych celów w sieciowych systemach operacyjnych.

## Podsumowanie

W rozdziale wyjaśniono potrzebę mapowania, czyli tłumaczenia nazw przyjaznych dla człowieka na adresy sieciowe oraz na odwrót. Na przestrzeni lat opracowano wiele technologii służących do tego celu.

Pierwszą technologią był plik *hosts*, który chociaż wciąż istnieje, to ma bardzo ograniczone zastosowanie. Protokół NetBIOS dostarcza mechanizm pozwalający komputerom Windows na propagowanie nazw w sieci LAN. Serwery NetBIOS są nazywane serwerami WINS. W większości dużych sieci Windows technologia WINS jest używana jako usługa określania nazw z powodu dużej wydajności.

DNS (ang. *Domain Name System*) to usługa określania nazw, która przypisuje internetowym adresom IP nazwy przyjazne dla człowieka. W rozdziale przedstawiono konstrukcję sieci DNS oraz sposoby przeprowadzania zapytań do tej usługi w celu określenia nazw. DNS można stosować także w sieciach LAN. Technologia DNS jest cenna przy dostarczaniu zunanfikowanej usługi określania nazw, która może być wykorzystywana w sieciach TCP/IP.

Przedstawiono również różnice między usługami określania nazw, które to usługi tak naprawdę są funkcjami mapowania, czyli tłumaczenia adresów, oraz usługami katalogowymi. Usługi katalogowe to zabezpieczone bazy danych przechowujące wszystkie rodzaje informacji o obiektach sieci; usługi te można rozszerzać. Nowoczesne usługi katalogowe bazują przede wszystkim na protokole X.500 LDAP.

W kolejnym rozdziale będą przedstawione różne klasy sieciowych systemów operacyjnych (NOS, ang. *Network Operating System*), powszechne cechy charakterystyczne tych systemów, ich funkcje, a także czynniki, które je różnicują.



# Część V

# Aplikacje i usługi

## **W tej części:**

**Rozdział 20.** Sieciowe systemy operacyjne

**Rozdział 21.** Usługi domen i katalogowe

**Rozdział 22.** Usługi plików i buforowanie

**Rozdział 23.** Usługi sieciowe

**Rozdział 24.** Protokoły poczty elektronicznej

**Rozdział 25.** Strumieniowanie multimediów

**Rozdział 26.** Telefonia cyfrowa i VoIP



# Rozdział 20.

# Sieciowe systemy operacyjne

## W tym rozdziale:

- ♦ Protokoły i usługi sieciowych systemów operacyjnych
- ♦ Ważne funkcje sieciowych systemów operacyjnych
- ♦ Serwery Unix, Linux, Solaris, Novell NetWare oraz Windows

Sieciowy system operacyjny (ang. *Network Operating System*) to taki, który został zoptymalizowany w celu dostarczania usług sieciowych. Prace rozwojowe nad sieciami komputerowymi stanowiły katalizator rozwoju sieciowych systemów operacyjnych i na odwrót. Sieci i sieciowe systemy operacyjne są ze sobą powiązane.

Każdy sieciowy system operacyjny musi dostarczać system operacyjny obsługujący sprzęt komputerowy, obsługiwać protokoły i usługi oraz dostarczać te usługi oraz aplikacje systemom klientów. Poza wymienionymi usługami podstawowymi sieciowy system operacyjny może zaoferować narzędzia administracyjne i zarządzające, usługi katalogowe oraz nazw, serwery plików, wydruku, usługi sieciowe, tworzenie kopii zapasowej, zapewnienie bezpieczeństwa i routing sieciowy. Ponadto sieciowy system operacyjny musi działać jako system operacyjny, w którym można instalować i uruchamiać aplikacje sieciowe.

Sieciowy system operacyjny oferujący szeroką gamę możliwości zwykle jest określany mianem *platformy*. Przykładami platform są Unix, Linux i Microsoft Windows. Niektóre sieciowe systemy operacyjne zostały zoptymalizowane do celów specjalnych. Przykładem tego rodzaju systemu jest Cisco IOS, który działa w routerach i przełącznikach sieciowych firmy Cisco.

W rozdziale będą przedstawione różne sieciowe systemy operacyjne. Kilka popularnych i powszechnie używanych sieciowych systemów operacyjnych zostanie omówionych dokładnie. Będą to w szczególności te, które są instalowane na serwerach oraz w modelach klient-serwer oraz architekturze n-warstwowej.

System Unix stanowi prototyp sieciowego systemu operacyjnego i miał największy wpływ na wszystkie pozostałe systemy, które opracowano w późniejszym czasie. W rozdziale zostanie pokrótce przedstawiona historia systemu Unix oraz cele przyświecające programistom podczas jego tworzenia. Zaprezentowane będą również ważne cechy sieciowe systemu Unix, takie jak POSIX, SUS, gniazda i architektura STREAMS.

Szczegółowo omówione w rozdziale systemy operacyjne z rodziny Unix obejmują system Linux, jak również system operacyjny Solaris firmy Sun Microsystems<sup>1</sup>. Ponadto przedstawiony będzie Novell NetWare oraz jego wkład w opracowywanie sieciowych systemów operacyjnych, a także najnowsza wersja oprogramowania firmy Novell o nazwie Open Enterprise Server (OES).

Ostatnim omawianym systemem będzie Microsoft Windows Server. Każdy z trzech wymienionych systemów jest liderem w pewnych aspektach oprogramowania serwerowego. Czytelnik pozna ich mocne i słabe strony.

## Co to jest sieciowy system operacyjny?

Sieciowy system operacyjny to system operacyjny zoptymalizowany w celu dostarczania usług innym systemom w sieci. Niemal każdy komercyjny system operacyjny zbudowany w ostatnich pięćdziesięciu latach zawiera pewne komponenty sieciowe.

Sieciowe systemy operacyjne działające w sieciach rozproszonych stały się koniecznością wraz z wprowadzeniem pierwszej generacji klientów przenośnych. Przykładem wczesnego sieciowego systemu operacyjnego może być LANtastic firmy Artisoft (obecnie w wersji 8.0, <http://pcmicro.com/lantastic/>), który został opisany jako „równy z równym”. Oprogramowanie LANtastic pozwalało na połączenie w sieć klientów MS-DOS, Novell NetWare oraz OS/2 i zapewniało współdzielony dostęp do aplikacji, plików, drukarek i napędów optycznych. Przed wprowadzeniem Windows 95 produkt LANtastic odniósł duży sukces. Jednak kiedy producenci systemów operacyjnych zaczęli koncentrować swoje wysiłki nad sieciami dla komputerów osobistych, funkcje wbudowane w systemy operacyjne PC zepchnęły na drugi plan potrzebę tworzenia produktów takich jak LANtastic.

Na wczesnym etapie sieci komputerowych oprogramowanie NetWare firmy Novell było liderem na polu sprzętu komputerowego PC oraz pierwszym sieciowym systemem operacyjnym, który odniósł sukces komercyjny. Firma Novell zbudowała NetWare, opierając się na Xerox Network Services, i położyła nacisk na koncepcję współdzielenia plików. Pierwsza wersja oprogramowania NetWare pojawiła się w roku 1983 i osiągnęła sukces na rynku, gdy firma IBM użyła tego produktu w 1984 roku, wprowadzając IBM PC. Wczesne wersje NetWare działały w systemach MS-DOS jako programy TSR (ang. *Terminate and Stay Resident*) i miały możliwość mapowania woluminów do liter dysków lokalnych. Oprogramowanie NetWare zaprezentowało pełny zakres prawdziwego sieciowego systemu operacyjnego, pozwalało na ograniczanie dostępu na podstawie nazwy użytkownika oraz oferowało serwer wydruku. Komputer Macintosh firmy Apple, wprowadzony również w roku 1984, miał wbudowane funkcje sieciowe — protokół AppleTalk, który firma Apple rozwijała aż do momentu osiągnięcia dominacji przez sieci TCP/IP.

Do chwili wydania NetWare 4, w roku 1995, firma Novell była potęgą w przemyśle komputerów osobistych. Wydane przez firmę Microsoft pierwsza wersja Windows for Workgroups w roku 1993, a następnie Windows 95 zrobiły niewiele, aby zmniejszyć znaczenie rozwiązań firmy Novell. Dopiero wydanie Windows NT pozwoliło firmie Microsoft na dogonienie rywala.

---

<sup>1</sup> W roku 2010 firma Sun Microsystems została przejęta przez Oracle na mocy umowy podpisanej w roku 2009 — *przyj. tłum.*

Protokół IPX firmy Novell był szeroko wykorzystywany, ale sieci IPX zostały zarzucone na rzecz TCP/IP. Jeśliby wskazać jeden czynnik, który wstrząsnął rynkiem sieciowych systemów operacyjnych i oddzielił bieżące produkty od wczesnych systemów, to byłby nim rozwój internetu.

## Protokoły i usługi

Obecnie sieciowy system operacyjny oferuje szeroką gamę możliwości. Każdy system musi spełniać trzy poniższe warunki:

- ♦ dostarczać system operacyjny obsługujący sprzęt komputerowy;
- ♦ udostępniać różne protokoły sieciowe i usługi, takie jak adresowanie;
- ♦ uruchamiać aplikacje serwerowe, do których systemy klientów lub — w przypadku sieci równorzędnych — inne systemy będą miały dostęp.

Ponadto sieciowy system operacyjny może również dostarczać niektóre z wymienionych poniżej usług sieciowych:

- ♦ zarządzanie i administrowanie siecią;
- ♦ nazwy oraz inne usługi katalogowe;
- ♦ współdzielone pliki i drukarki, usługi sieciowe, tworzenie kopii zapasowych oraz usługi replikacji;
- ♦ usługi związane z bezpieczeństwem, kontrolą dostępu oraz logowaniem; sieciowy system operacyjny może działać jako serwer „potrójnego A”, tzn. oferując authentication, authorization i accounting (uwierzytelnianie, autoryzację i zliczanie, czyli rejestrację wykorzystania zasobów);
- ♦ przeprowadzanie routingu ruchu sieciowego i kontrolowanie dostępu do portów;
- ♦ opcje zapewniające wysoką dostępność, na przykład odporność na awarie, tworzenie klastrów, działanie po wystąpieniu awarii, oraz wysoką redundancję;
- ♦ możliwość dużej skalowalności systemu, na przykład równoważenie obciążenia lub obsługa systemów z dużą liczbą procesorów (SMP (ang. *Symmetric Multiprocessor*) albo NUMA (ang. *Non-Uniform Memory Access*)).

## Sieciowy system operacyjny — ogólny kontra specjalnego przeznaczenia

Część sieciowych systemów operacyjnych, na przykład Microsoft Windows, Novell NetWare, Sun Solaris, różne odmiany rodziny Linux itd., są od razu dostarczane z wyżej wymienionymi protokołami i usługami albo mają dodatki pozwalające na ich włączenie. Dlatego też systemy operacyjne tego rodzaju są określane mianem *platform* lub nieco rzadziej systemami sieciowymi ogólnego przeznaczenia. Nie wszystkie systemy muszą być tak szeroko zdefiniowane.

Przykładem systemu specjalnego przeznaczenia jest IOS (ang. *Internetwork Operating System*) firmy Cisco Systems. System IOS działa w niemal wszystkich routerach i przełącznikach sieciowych firmy Cisco, używających własnościowego systemu operacyjnego. Z drugiej strony oprogramowanie JUNOS firmy Juniper Networks, które firma ta określa jako system operacyjny routerów, działa na bazie implementacji FreeBSD. Tak więc chociaż wczesne routery internetowe bardzo często były zbudowane na bazie różnych wersji systemu Linux i SunOS, firma Cisco była w stanie zbudować routery oferujące jeszcze lepsze możliwości za niższą cenę. Stało się to możliwe dzięki opracowaniu specjalnego systemu IOS, dzięki czemu firma odniosła jeszcze większy sukces.

Prace nad sieciowym systemem ogólnego przeznaczenia przebiegały na różne sposoby. W większości przypadków platformy były implementowane w serwerach lub jako maszyny wirtualne. W ciągu ostatniej dekady tendencją było rozwijanie tego typu platform w oparciu o systemy operacyjne serwera i klienta na tym samym kodzie podstawowym. Firma Microsoft zapoczątkowała ten kierunek prac nad Windows 2000, a Windows 2003/XP oraz Windows 2008/Vista podążały tą ścieżką.

Ogólnie rzecz biorąc, wiele serwerowych systemów operacyjnych ma jądro systemu takie samo jak systemy klientów. Różnica między tymi dwoma rodzajami systemów sprowadza się do funkcji dodatkowych, wyłączenia pewnych funkcji bądź ich ograniczenia. Na przykład firma Microsoft wprowadziła dla klientów ograniczenie do dziesięciu połączeń podczas uzyskiwania dostępu do serwera WWW w stacji roboczej Windows. Jeżeli Czytelnik jest zainteresowany tym tematem, może zapoznać się z umieszczonym na stronie <http://www.msfn.org/win2k3/> artykułem przedstawiającym konwersję systemu Windows Server 2003 na stację roboczą Windows XP. Proces ten obejmuje dodanie DirectX, tematów, funkcji przywracania systemu, Javy oraz kilku innych usług do Windows Server 2003.

Kilka dystrybucji systemu Linux podąża tą samą ścieżką, ale to nie jest uniwersalny wzorzec. Na przykład firma Sun nie stosuje żadnego rozróżnienia między systemem Solaris działającym jako serwer a biurowym systemem operacyjnym.

Powszechnie używane systemy operacyjne zostały przedstawione w tabeli 20.1.

## Sieciowe systemy operacyjne i oprogramowanie

W poprzednim podrozdziale przedstawiono niektóre z ogólnych funkcji sieciowych systemów operacyjnych. Obecnie na rynku dostępne są dosłownie setki różnego rodzaju systemów sieciowych. Jednak ilość miejsca dostępnego w książce wyklucza możliwość pełnego omówienia każdego z nich. W kolejnych podrozdziałach zostaną więc bardziej szczegółowo przedstawione najpopularniejsze obecnie systemy sieciowe będące w użyciu, między innymi:

- ♦ Unix,
- ♦ Linux,
- ♦ Solaris,
- ♦ Novell NetWare i Open Enterprise Server,
- ♦ Windows Server.

**Tabela 20.1.** Powszechnie używane platformy sieciowych systemów operacyjnych

Nazwa systemu NOS	Właściciel	Wersja bieżąca	Obsługiwany sprzęt	Strona WWW
AIX	IBM	7.1	64-bitowe systemy RISC	<a href="http://www-03.ibm.com/systems/power/software/aix/index.html">http://www-03.ibm.com/systems/power/software/aix/index.html</a>
BSD	Projekt FreeBSD, NetBSD i OpenBSD	8.1, 5.1, 4.8	Alpha, ARM, x86, IA64, MIPS, PPC, SPARC64, SunOS4 oraz Xbox	<a href="http://www.freebsd.org">http://www.freebsd.org</a> <a href="http://www.netbsd.org">http://www.netbsd.org</a> <a href="http://www.openbsd.org">http://www.openbsd.org</a>
Digital Unix (TruUnix)	Hewlett-Packard (pomimo przejścia)	5.1B-5	Alpha (do 2012 roku)	<a href="http://www.hp.com">http://www.hp.com</a>
HP-UX	Hewlett-Packard	UNIX System V Release 4	IA64, PA-RISC (do 2012 roku)	<a href="http://www.hp.com">http://www.hp.com</a>
IOS	Cisco Systems	15	Routerzy i przełączniki sieciowe firmy Cisco	<a href="http://www.cisco.com/en/US/products/sw_iosswrel/products_ios_cisco_ios_software_category_home.html">http://www.cisco.com/en/US/products/sw_iosswrel/products_ios_cisco_ios_software_category_home.html</a>
IRIX	Silicon Graphics	6.5.30	Systemy SGI, procesory PowerPC	<a href="http://www.sgi.com/products/software/irix/">http://www.sgi.com/products/software/irix/</a>
Mac OS X	Apple Computer	10.6.6	x86, PowerPC oraz ARM v6	<a href="http://www.apple.com/macoss/">http://www.apple.com/macoss/</a>
NetWare (wyparty przez OES)	Novell	6.5 SP8 (odpowiednik OES 2)	x86	<a href="http://www.novell.com">http://www.novell.com</a>
Open Enterprise Server	Novell	OES 2 SP3	x86	<a href="http://www.novell.com">http://www.novell.com</a>
OpenVMS	Hewlett-Packard (pomimo przejścia)	8.4	Alpha, VAX, IA64 (Itanium)	<a href="http://www.hp.com">http://www.hp.com</a>
Red Hat Linux	Red Hat	6	x86, IA64	<a href="http://www.redhat.com/products/">http://www.redhat.com/products/</a>
SCO Open Server 6	The SCO Group	6	x86	<a href="http://www.sco.com/products/openserver6/">http://www.sco.com/products/openserver6/</a>
Solaris	Oracle	11	SPARC, x86, IA64	<a href="http://www.oracle.com/us/products/servers-storage/solaris/index.html">http://www.oracle.com/us/products/servers-storage/solaris/index.html</a>
Ubuntu	Canonical	10.10	x86, IA64	<a href="http://www.ubuntu.com">http://www.ubuntu.com</a>
Windows	Microsoft	2008 R2	x86, IA64	<a href="http://www.microsoft.com/windowsserver2008/en/us/default.aspx">http://www.microsoft.com/windowsserver2008/en/us/default.aspx</a>
z/OS (poprzednio MVS)	IBM	1.12	IBM zSeries (MVS działa na komputerach Mainframe System 360/390)	<a href="http://www-03.ibm.com/systems/z/os/zos/index.html">http://www-03.ibm.com/systems/z/os/zos/index.html</a>

## Unix

Unix jest określany jako wielozadaniowy, wieloużytkownikowy sieciowy system operacyjny z funkcją podziału czasu. Został zaprojektowany na bazie jądra, które w przeciwieństwie do wcześniejszych systemów operacyjnych można bardzo łatwo przenieść na inne architektury sprzętowe (rodziny procesorów); oddziela funkcje użytkownika od operacji jądra. Taka filozofia jest czasami określana mianem „filozofii Unix”. Sprawia ona, że sieciowy system operacyjny oraz jego komponenty są zarówno modułowe, jak i nadające się do ponownego używania.

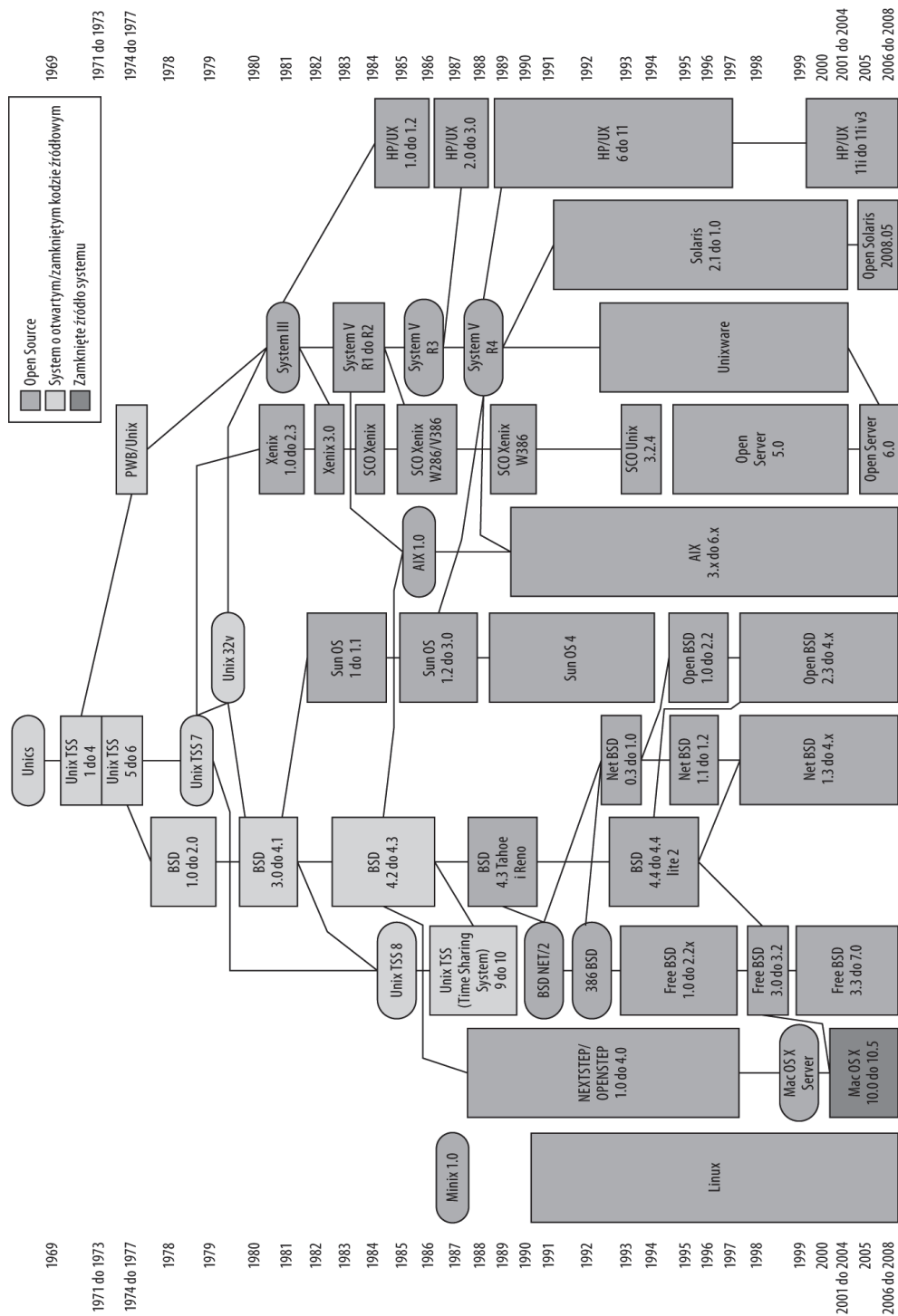
System Unix został opracowany w laboratoriach Bell Labs dla AT&T w późnych latach 60. Na jego potrzeby Dennis Ritchie opracował w 1972 roku język programowania C. Znak towarowy Unix, początkowo dostępny na licencji AT&T, jest obecnie własnością The Open Group, a sama nazwa UNIX lub Unix jest używana w odniesieniu do systemów operacyjnych zgodnie ze specyfikacją SUS (ang. *Single UNIX Specification*), która bardziej szczegółowo będzie omówiona w dalszej części rozdziału. Przykładami systemów operacyjnych Unix są AIX, HP-UX, Solaris oraz inne systemy bazujące na UNIX System V lub na ostatnim wydaniu AT&T o nazwie Seventh Edition UNIX, Version 7 Unix lub po prostu V7 Unix. Firma Caldera Systems przejęła prawa do V7 Unix i w roku 2002 wydała go jako własność publiczną. W porównaniu z innymi przemysłowymi systemami sieciowymi Unix jest uznawany za standard przemysłowy.



Używa się nazwy UNIX czy Unix? Można się spotkać z obydwojema wariantami pisowni. Nazwa UNIX pisana dużymi literami jest znakiem towarowym The Open Group oraz oficjalną nazwą nadawaną każdemu systemowi Unix, który jest zgodny ze specyfikacją SUS i jest licencjonowany. Gdy mamy na myśli ogólną klasę systemów operacyjnych, pisownia Unix jest według autora książki całkowicie akceptowalna.

Inne systemy operacyjne wywodzące się z koncepcji Unix, ale niezgodne ze specyfikacją SUS, są uznawane za systemy z rodziny Unix — dobrym przykładem są tutaj różne dystrybucje systemu Linux. Wpływ systemu Unix na systemy sieciowe powstałe znacznie później jest ogromny i nie można go pominąć. Patrząc na schemat pokazany na rysunku 20.1, można się przekonać, jak wiele z systemów sieciowych to systemy Unix albo powiązane z systemem Unix. Schemat został opracowany przez Erica Levenezę (<http://www.levenez.com/unix>).

Unix stał się standardem, ponieważ firma AT&T szeroko rozpowszechniła zarówno ten system, jak i język programowania C. Dostępność w systemie Unix rządowych i wojskowych aplikacji, jak również liberalna polityka dystrybucji systemu na uniwersytetach spowodowały, że system przeniesiono na wiele — znacznie więcej niż w przypadku innych systemów operacyjnych — platform sprzętowych. Unix stał się znany jako „system otwarty”, chociaż początkowo opłaty licencyjne dla użytkowników komercyjnych stanowiły pewną barierę w jego upowszechnianiu. Różne wersje systemu operacyjnego Unix zostały zainstalowane na uniwersytetach, zwłaszcza w Berkeley (Kalifornia), na którym opracowano BSD Unix, oraz Carnegie Mellon Institute w Pittsburghu, gdzie opracowano jądro MACH. Kiedy te otwarte wersje stały się głównymi wersjami systemu Unix, miały duży wpływ na decyzję firmy AT&T, aby Unix został szeroko udostępniony.

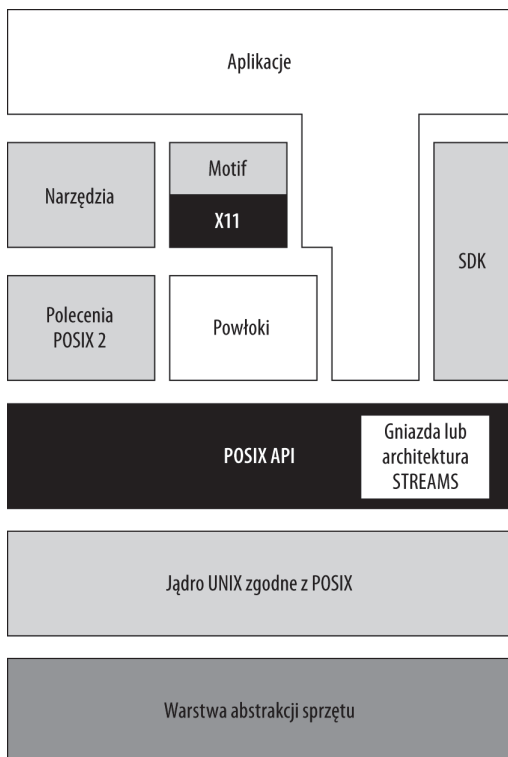


### Rysunek 20.1. Drzewo rodziny Unix

## POSIX

Interfejs systemu Unix oraz standaryzacja wokół języka C ostatecznie doprowadziły do powstania zestawu wskazówek projektowych i API, które stały się architekturą modelu sieciowego systemu operacyjnego. POSIX (ang. *Portable Operating System Interface for Unix*, <http://www.pasc.org>) to API (ang. *Application Programming Interface*) zdefiniowane przez standardy IEEE 1003 i ISO/IEC9945. POSIX zapewnia systemom sieciowym standaryzację interfejsów programistycznych, użytkownika i właściwości powłok systemów i dlatego został niemal powszechnie zaadaptowany. Na rysunku 20.2 pokazano niektóre ze standardowych komponentów architektury POSIX.

**Rysunek 20.2.**  
Architektura POSIX



Funkcje nowoczesnego systemu sieciowego — takie jak hierarchiczny system plików, przechowywanie zwykłego tekstu, interpreter wiersza poleceń, komunikacja między aplikacjami i komunikacja między procesami (ang. *Inter-Process Communication*, IPC), koncepcja pamięci współdzielonej, wiadomości i zapytań, semaforów, gniazd itp. — są wynalazkami wyrastającymi z systemu Unix, chociaż nie stanowiły części oryginalnego systemu Unix AT&T. Zostały dodane do niego w późniejszym okresie wraz z pojawieniem się konieczności obsługi asynchronicznych operacji wejścia-wyjścia. Zaufanie do pamięci masowej systemu, bazowanie na fragmentach pamięci masowej (bajty) zamiast na strukturze rekordu bazy danych również stały się standardem systemów sieciowych.

Z punktu widzenia usług sieciowych prawdopodobnie największym osiągnięciem jest przeniesienie tych usług i protokołów poza jądro systemu operacyjnego. W ten sposób progra-

miści mogą znacznie szybciej modernizować system operacyjny pod kątem szybko zmieniających się funkcji sieciowych. Duże możliwości modyfikacji funkcji sieciowych Unix pozwalają na długotrwały wpływ systemu na informatykę, a także przenoszenie jądra.

## Architektura STREAMS i gniazda

Architektura STREAMS i gniazda to dwie metody używane przez Unix do ustanowienia interfejsu sieciowego. Ponadto odgrywają one główną rolę w tworzeniu usług sieciowych.

Gniazdo to punkt końcowy połączenia sieciowego. Kiedy gniazdo pozwala na dwukierunkowy przepływ danych IP, jest określane mianem *gniazda internetowego*. Gdy gniazdo używa innych typów protokołów, nosi nazwę *gniazda sieciowego* lub jeszcze prościej — gniazda. Gniazda internetowe mają określone właściwości, takie jak używany protokół, przypisany adres IP, numer portu, numer usługi oraz (po nawiązaniu połączenia) zdalny adres IP i zdalny numer portu. Wymienione cechy charakterystyczne nadają gniazdom unikalną identyfikację.

Sieciowe systemy operacyjne wykorzystują koncepcję gniazda jako interfejsu między procesem aplikacji i stosem sieciowym, pozwalając na przepływ danych pomiędzy nimi. Gniazda są więc interfejsem między systemem i sieciowymi operacjami wejścia-wyjścia. Opracowanie architektury bazującej na gniazdach odegrało istotną rolę w ewolucji nowoczesnych systemów sieciowych i znacznie ułatwiło tworzenie spójnych modeli sterowników sieciowych. Umożliwiło także wzajemną współpracę różnych systemów.

Listę gniazd dostępnych w systemie Unix lub z rodziny Unix (na przykład w Linuksie) można wyświetlić za pomocą polecenia `netstat -an`. Alternatywna opcja — `netstat -b` — powoduje wyświetlenie gniazd ustanowionych przez różne aplikacje. Na rysunku 20.3 pokazano częściowe dane wyjściowe polecenia `netstat -an` wydane w systemie Windows Vista.

### Rysunek 20.3.

Polecenie `netstat -an` pozwala na wyświetlenie stanu gniazd i interfejsów sieciowych

Protokół	Adres lokalny	Obcy adres	Stan
TCP	0.0.0.0:135	0.0.0.0:0	NASEUCHIWANIE
TCP	0.0.0.0:445	0.0.0.0:0	NASEUCHIWANIE
TCP	0.0.0.0:554	0.0.0.0:0	NASEUCHIWANIE
TCP	0.0.0.0:2869	0.0.0.0:0	NASEUCHIWANIE
TCP	0.0.0.0:5357	0.0.0.0:0	NASEUCHIWANIE
TCP	0.0.0.0:10243	0.0.0.0:0	NASEUCHIWANIE
TCP	0.0.0.0:49152	0.0.0.0:0	NASEUCHIWANIE
TCP	0.0.0.0:49153	0.0.0.0:0	NASEUCHIWANIE
TCP	0.0.0.0:49154	0.0.0.0:0	NASEUCHIWANIE
TCP	0.0.0.0:49155	0.0.0.0:0	NASEUCHIWANIE
TCP	0.0.0.0:49156	0.0.0.0:0	NASEUCHIWANIE
TCP	127.0.0.1:31416	0.0.0.0:0	NASEUCHIWANIE
TCP	127.0.0.1:31416	127.0.0.1:49158	USTANOWIONO
TCP	127.0.0.1:31416	127.0.0.1:49193	USTANOWIONO
TCP	127.0.0.1:49158	127.0.0.1:31416	USTANOWIONO
TCP	127.0.0.1:49193	127.0.0.1:31416	USTANOWIONO
TCP	192.168.4.131:139	0.0.0.0:0	NASEUCHIWANIE
TCP	192.168.4.131:49207	209.85.135.99:80	USTANOWIONO
TCP	192.168.4.131:49208	209.85.135.99:80	USTANOWIONO
TCP	192.168.4.131:49231	209.85.135.106:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49232	209.85.135.147:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49233	209.85.135.147:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49234	209.85.135.147:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49235	209.85.135.147:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49236	209.85.135.147:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49237	209.85.135.147:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49239	209.85.135.100:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49240	209.85.135.101:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49241	95.100.141.15:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49242	193.219.28.105:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49243	193.219.28.105:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49244	193.219.28.105:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49245	193.219.28.105:80	OCEKIWANIE_ZAMKN
TCP	192.168.4.131:49246	193.219.28.105:80	OCEKIWANIE_ZAMKN

Prawdopodobnie najbardziej znaną architekturą gniazda sieciowego jest architektura Berkeley Sockets API, która została wprowadzona wraz z BSD UNIX v4.2. To API było chronione prawami autorskimi AT&T aż do chwili, gdy w 1989 roku uniwersytet Berkeley wydał system Unix, który był otwarty i pozwalał na publiczną adaptację na licencji Berkeley. Obecnie architektura Berkeley Sockets jest uznawana za standardowy model projektu gniazda sieciowego.

Architektura STREAMS jest alternatywą dla Berkeley Sockets. Po raz pierwszy pojawiła się w UNIX System V. STREAMS to architektura sieciowa używana w UNIX System V dla operacji wejścia-wyjścia w celu umożliwienia urządzeniu bądź plikowi specjalnemu systemu na komunikację z urządzeniem za pomocą sterownika tego urządzenia z użyciem standardowych systemowych wywołań wejścia-wyjścia. Architektura STREAMS ma konstrukcję modułową i pozwala na łączenie sterowników (które są modułami). Obciążenie powodowane przez architekturę STREAMS jest większe niż w przypadku gniazd. We wszystkich systemach operacyjnych używających architektury STREAMS dołączane jest również Sockets API. W początkowej specyfikacji *Single UNIX Specification* architektura STREAMS była komponentem obowiązkowym, natomiast w bieżącej specyfikacji SUS v3 stanowi komponent opcjonalny.

## Single UNIX specification

Kiedy jest mowa o Uniksie, większość osób zwykle ma na myśli wiele różnych wersji systemu Unix, które bazują na historycznym sieciowym systemie operacyjnym firmy AT&T. Wszystkie wymienione poniżej sieciowe systemy operacyjne są odmianami systemu Unix:

- ♦ IBM AIX 7.1;
- ♦ HP-UX 4;
- ♦ Mac OS X Server 10.6;
- ♦ SCO UnixWare 7.1.4 oraz SCO OpenServer 6;
- ♦ Sun Solaris 11;
- ♦ DEC Tru64 UNIX V5.1A (teraz jest własnością firmy Hewlett-Packard i przez nią jest obsługiwany);
- ♦ IBM z/OS 1.12.

Wymienione odmiany są aktualnie certyfikowane i zgodne ze specyfikacją SUS (ang. *Single UNIX Specification*). Linux oraz różne wersje BSD UNIX są uznawane za systemy operacyjne „z rodziny Unix”, niespełniające standardu SUS.



Aby dowiedzieć się więcej na temat specyfikacji SUS, warto zapoznać się z dokumentem SUS FAQ, dostępnym na stronie [http://opengroup.org/austin/papers/single\\_unix\\_faq.html](http://opengroup.org/austin/papers/single_unix_faq.html).

Specyfikacja SUS jest wynikiem wysiłków w celu utworzenia standardu systemu Unix, które zostały zapoczątkowane przez IEEE oraz The Open Group w latach osiemdziesiątych. Skutkiem tych działań był standard POSIX.1 (skrót od *Portable Operating System*

*Interface for Unix*), który wpłynął na prace prowadzone nad wieloma systemami sieciowymi w latach osiemdziesiątych i dziewięćdziesiątych w celu utworzenia zestawu standardów Unix. Okres ten był znany jako „wojny Unix” i doprowadził niektórych z głównych producentów systemu Unix do założenia COSE (ang. *Common Open Software Environment*). Największym osiągnięciem COSE było utworzenie środowiska CDE (ang. *Common Desktop Environment*), które łączyło środowisko X11 z interfejsem użytkownika OSF Motif oraz pakietem narzędziowym.

W rezultacie tych poczynąń powstała grupa *Austin Common Standards Revision Group* (<http://www.opengroup.org/austin/>) lub po prostu Austin Group. Specyfikacja SUS dostarczyła zestawu interfejsów użytkownika oraz oprogramowania, które stanowiły standard programowania w powłoce POSIX. Ponadto opracowana została pewna liczba systemowych narzędzi i usług, włączając w nie plik, terminal oraz usługi sieciowe. Wszystkie wymienione powyżej systemy operacyjne Unix są zgodne ze specyfikacją SUS.

## Linux

Linux jest systemem operacyjnym z rodziny Unix, używającym jądra Linux dostępnego jako open source. Wydaje się, że obecnie pod kontrolą systemu Linux działa największa liczba serwerów internetowych, jak wynika z danych statystycznych dotyczących wykorzystywania internetu. Organizacja Netcraft (<http://www.netcraft.com>), śledząca obecnie używane serwery WWW w internecie, ogłosiła, że połowa serwerów WWW działa pod kontrolą różnych wersji systemu Linux, FreeBSD to około 30%, natomiast pozostałe 20% należy do Windows Server. Inne badania, przeprowadzane na podstawie sprzedaży sprzętu i uwzględniające cały rynek serwerowy, wskazują, że Linux ma w nim około piętnastoprotentowy udział.

Wykorzystanie systemu Linux jako biurowego systemu operacyjnego jest znacznie bardziej ograniczone, chociaż dystrybucja Ubuntu na tym polu przejęła kilka procent. Linux stał się popularny na wschodzącym rynku „netbooków” i pojawia się w komputerach takich jak ASUS Eee oraz Acer Aspire One.

Różne wersje systemu Linux działają w urządzeniach o różnej wielkości, od małych urządzeń osadzonych aż po superkomputery. Wśród obsługiwanych platform są między innymi x86, SPARC, IA64, PowerPC, Motorola 68000 oraz IBM s390. Linux jest obsługiwany przez grupę głównych producentów sprzętu komputerowego. Firmy Dell, IBM, Hewlett-Packard, Sun Microsystems oraz Nokia sprzedają systemy działające pod kontrolą systemu operacyjnego Linux oraz wspierają wysiłki związane z rozwojem oprogramowania typu open source. Linux jest również zainstalowany na 91,8% najpotężniejszych superkomputerów, wymienionych na liście Top 500 Supercomputer Sites (<http://www.top500.org/stats/list/36/osfam>), co stanowi zaskoczenie dla większości osób, które po raz pierwszy stykają się z tymi danymi.

Przy użyciu systemów Linux zbudowana jest duża liczba ważnych witryn internetowych, łącznie z czterema największymi: Amazon, eBay, Google oraz Yahoo!. W niektórych krajach Linux stał się standardowym systemem operacyjnym dla rządów. Przykładami takich krajów są Brazylia, Rosja, Indie, Chiny, Niemcy oraz Francja.

## Dystrybucje

Obecnie dostępnych jest około stu dystrybucji systemu Linux, bazujących na dystrybucjach Debian, Gentoo, RPM oraz Slackware. Wśród najbardziej znanych znajdują się Linspire i Ubuntu (bazują na Debianie), Caldera Linux, Red Hat Linux oraz SUSE Linux (bazują na RPM). Klasy systemów Linux utworzono na podstawie następujących funkcji:

- ♦ Debian Linux używa formatu pakietów *.deb* i jest rozprowadzany z szeroką gamą oprogramowania, preferowanego przez systemy biurowe;
- ♦ Gentoo Linux używa formatu pakietów Portage i zwykle jest wysoce zoptymalizowany dla urządzeń oferujących mniejsze możliwości sprzętowe;
- ♦ Fedora Linux używa formatu pakietów RPM;
- ♦ Red Hat Enterprise Linux — inna wersja używająca formatu pakietów RPM, dostosowana do potrzeb serwerów.



Wikipedia zawiera długą listę dystrybucji systemu Linux wraz z odnośnikami do poświęconych im stron ([http://en.wikipedia.org/wiki/List\\_of\\_Linux\\_distributions](http://en.wikipedia.org/wiki/List_of_Linux_distributions)).

Pierwsza wersja jądra Linux została wydana przez jego twórcę, Linusa Torvaldsa, w roku 1991. Bieżąca wersja jądra (5 stycznia 2011 roku) to 2.6.37. Większość dodatkowych narzędzi oraz bibliotek pochodzi z systemu operacyjnego typu open source, projektu GNU, zapoczątkowanego w roku 1983 przez Richarda Stallmana i organizację Free Software Foundation w laboratoriach Media Labs Massachusetts Institute of Technology.

Projekt GNU obejmuje także powszechną licencję publiczną GNU (GPL), obecnie dostępną w wersji 3.0 (<http://www.gnu.org/licenses/gpl-3.0.txt>), na której podstawie jest rozpowszechniany Linux. Pojęcie *copyleft* (zrzeczenie się roszczeń z tytułu praw autorskich) ma czasami zastosowanie względem licencji GNU. Copyleft wymaga, aby program (na przykład Linux lub inne dzieło) i wszystkie zmodyfikowane i rozbudowane jego wersje były rozprowadzane bezpłatnie. Firmy takie jak Red Hat i Novell odpłatnie rozpowszechniają komercyjne wersje systemu Linux klasy przemysłowej, które nie spełniają wymogów licencji GNU GPL. Wymienione firmy pobierają opłatę za pomoc techniczną, jak również za wprowadzone modyfikacje. Aby spełnić wymagania standardów GPL, firmy sprzedające komercyjne systemy Linux wspierają wersje open source systemów Linux, które są zgodne z GPL.

## LAMP

Linux jest często instalowany na sprzęcie przemysłowym i pozwala na osiągnięcie dużej skalowalności przez skalowanie poziome. Wiele serwerów Linux ma zainstalowane oprogramowanie nazywane LAMP. Pakiet LAMP składa się z następujących komponentów:

- ♦ Linux — system operacyjny;
- ♦ Apache — serwer WWW;
- ♦ MySQL — serwer bazy danych;
- ♦ P — jeden z języków programowania lub języków skryptowych: PHP, Perl lub Python.

Linux został zaprojektowany do używania wielu reguł projektowych systemu Unix, które przedstawiono w poprzednim podrozdziale. Jądro systemu Linux jest monolityczne i zawiera moduły odpowiedzialne za zarządzanie procesami i pamięcią, sterowniki i operacje wejścia-wyjścia, pliki urządzeń, gniazda oraz system plików. Inne funkcje, takie jak interpretery poleceń (powłoki), narzędzia i graficzne interfejsy użytkownika (GUI), składają się na przestrzeń funkcji dostępnych dla użytkownika. Linux został zaprojektowany jako zgodny ze standardami POSIX, a większość dystrybucji zaadaptowało wiele reguł specyfikacji SUS, którą przedstawiono w poprzednim podrozdziale. Obecnie prowadzone są prace mające na celu utworzenie standardu systemu Linux — *Linux Standard Base* — które zostaną omówione w kolejnym podrozdziale.

Dla dystrybucji systemu Linux dostępnych jest wiele różnych graficznych interfejsów użytkownika (GUI), ale większość z nich bazuje na X Window System oraz interfejsie Motif. Najpopularniejsze GUI to KDE, Gnome oraz Xfce, a wiele dystrybucji pozwala na instalację więcej niż tylko jednego GUI, jeśli użytkownik sobie tego życzy. Wydajne serwery sieciowe zwykle są pozbawione GUI, polegają na CLI (ang. *Command Line Interface*) i działają w postaci określonej mianem „bezwjściowej” — to znaczy bez podłączonego monitora, klawiatury i myszy. Kontrola nad tego rodzaju serwerem odbywa się za pomocą sieci, często z poziomu sesji terminalu (emulator terminalu graficznego) bądź wiersza poleceń. Większość dystrybucji systemu Unix obsługuje tryb bezwjściowy, ponieważ stanowi on mniejsze obciążenie dla działających procesów. Firma Microsoft dodała ten tryb do Windows Server 2008.

## Linux Standard Base

LSB (ang. *Linux Standard Base*) to projekt zarządzany przez organizację Linux Foundation (<http://www.linuxfoundation.org/>), której celem jest utworzenie standardu funkcji systemu Linux, aby różne dystrybucje były w większym stopniu ze sobą zgodne. Podobnie jak przedstawiona wcześniej specyfikacja SUS, także LSB nadaje certyfikaty zgodności. LSB określa standardowe biblioteki, polecenia, narzędzia, komponenty systemu plików, funkcje podsystemu wydruku, POSIX oraz rozszerzenia X Window System. Ponadto LSB określa naturę formatu pakietów RPM używanych do instalacji systemu Linux. Ostatnia wydana w 2008 roku wersja LSB to 4.0.

## Solaris

System operacyjny Solaris firmy Oracle (dawniej Sun<sup>2</sup>) to obecnie najczęściej używany sieciowy system operacyjny Unix. Solaris został zaprezentowany w roku 1992 w celu zastąpienia systemu operacyjnego SunOS i wprowadził zaawansowany stos sieciowy obsługujący sieci TCP/IP. Solaris istnieje w dwóch wersjach: działającej w systemach komputerowych bazujących na procesorach SPARC firmy Oracle oraz w wersji x86 działającej na standardowej architekturze Intel. Firma Sun uznała Solaris za jeden z podstawowych sieciowych systemów operacyjnych dla dużych przedsiębiorstw, jak również za preferowaną platformę dla sieci pamięci masowej.

---

<sup>2</sup> Firma Sun 27 stycznia 2010 roku została przejęta przez firmę Oracle — *przypr.red*.

Najnowsza wersja Solarisa to 11. (SunOS 5.11). System operacyjny może być pobrany w dowolnej z jego dwóch architektur (SPARC x86 lub IA64) ze strony internetowej <http://www.oracle.com/us/products/servers-storage/solaris/index.html> i jest dostępny bezpłatnie do celów testowych i niekomercyjnych. Solaris można zainstalować w postaci serwera lub stacji roboczej. Istnieje możliwość instalacji wyłącznie podstawowych usług sieciowych, użytkownika, programisty bądź też instalacji całego pakietu, zawierającego oprogramowanie niezbędne do zarządzania siecią oraz narzędzia do zarządzania jej polityką.

Wprawdzie początkowe wersje Solarisa bazowały na kodzie własnościowym, ale firma Sun przekształciła ten system w model open source standardu przemysłowego. Większość kodu bazowego bieżącej wersji Solarisa została opublikowana jako open source pod nazwą OpenSolaris. Oferowana przez Oracle komercyjna wersja Solarisa posiada certyfikat zgodności z przedstawioną w poprzednim podrozdziale specyfikacją Single UNIX Specification.

Oryginalny stos sieciowy w systemie Solaris 1.x bazował na wersji BSD. Aby poprawić wydajność Solarisa, w wersji Solaris 2.x stos sieciowy przeniesiono na architekturę AT&T SVR4. Różne wersje 2.x kontynuowały przejście w kierunku stosu sieciowego STREAMS, który stał się podstawą dla funkcji sieciowych w UNIX System V. Architektura STREAMS jest znana zarówno ze względu na swoją modułową naturę, jak i możliwość przekazywania komunikatów między modułami. Tworzenie połączenia w architekturze STREAM wiąże się ze znaczącym obciążeniem, ale w przypadku długich sesji powiązanych z protokołami takimi jak FTP i NFS obciążenie to nie stanowi problemu.

Jednak wraz z przejściem sprzętu komputerowego firmy Sun na znacznie potężniejsze systemy wieloprocesorowe brak możliwości łatwego przeprowadzenia optymalizacji STREAM dla przetwarzania wieloprocesorowego stał się poważnym problemem. Pakiety są przetwarzane w architekturze STREAM, a wielowątkowość wraz z połączeniem więcej niż jednego procesora oznacza niemożliwe do uniknięcia wielokrotne przełączanie kontekstu (jądro — tryb użytkownika). Do późnych lat dziewięćdziesiątych serwery i stacje robocze Sun były najczęściej stosowaną platformą zarówno do routingu, jak i w przypadku aplikacji serwerowych, na których działało oprogramowanie serwerów WWW. Protokoły internetowe, w szczególności HTTP, są krótkotrwałymi połączeniami, a architektura STREAM pokazuje tutaj swoje wady. Podczas prac nad systemem Solaris 10 firma Sun dokonała przebudowania swojego stosu sieciowego.



Solaris od 2.0 do 2.6 odpowiada systemowi SunOS w wersjach od 5.0 do 5.6. Począwszy od systemu Solaris 7 (SunOS 5.7), firma Sun zaczęła numerować system Solaris, używając liczb całkowitych. Ostatnie wydanie to Solaris 11 (SunOS 5.11), wydane 31 stycznia 2005 roku. Wprawdzie Solaris jest następcą systemu SunOS, ale firma Sun zdecydowała się na pozostawienie schematu numerowania dla obu nazw.

Stos sieciowy w systemie operacyjnym Solaris 10 został przebudowany z użyciem architektury „FireEngine”, która połączyła wszystkie warstwy protokołów w pojedynczy moduł STREAM wraz z pełną obsługą wątkowania. Mechanizm określany jako *Vertical perimeters* pozwala na synchronizację per-procesor w module TCP/IP, co jest wdrożone przy użyciu *queue*. W Solarisie 10 architektura przekazywania komunikatów została zastąpiona przez inną, używającą interfejsu wywoływania funkcji BSD.

Solaris 10 i 11 obsługuje system plików NFS 4.0 i został zaprojektowany w celu obsługi sieci o przepustowości do 10 Gb/s. Używając funkcji o nazwie Solaris Zones, na tym samym komputerze można uruchomić wiele egzemplarzy systemu operacyjnego jako maszyny wirtualne.

Z kolei przy wykorzystaniu technologii Grid Container serwer może utworzyć partycję dyskową dla poszczególnych użytkowników i zapewnić im wrażenie, że działają w uruchomionym specjalnie dla nich systemie operacyjnym. Następuje więc zamiana serwera Sun na serwer terminalu.

Solaris ma również możliwość dołączania systemu plików ZFS (jego początkowa nazwa kodowa to *Zettabyte File System*), który oferuje kilka unikalnych funkcji przemysłowych. ZFS obsługuje bardzo duże wielkości woluminów oraz integruje system plików wraz z zarządzaniem woluminami. Oprócz wbudowanych funkcji tworzenia kopii migawkowych i pełnych system ZFS zawiera także schemat replikacji o nazwie RAID-Z. Technologia ta traktowana jako całość ma pewne unikalne możliwości w zakresie automatycznej naprawy. Firma Sun udostępniła ZFS jako oprogramowanie open source, które jest częścią projektu OpenSolaris (<http://www.opensolaris.org/os/community/zfs/>).

System Solaris jest dostarczany wraz z narzędziem o nazwie DTrace (ang. *Dynamic Tracing*), które diagnozuje wydajność aplikacji sieciowych oraz wykrywa miejsca występowania potencjalnych wąskich gardeł. Informacja ta może być przekazana do podsystemu zarządzającego awariami, odpowiedzialnego za usunięcie problemu, optymalizację i (lub) zgłoszenie administratorom systemu. DTrace był pierwszym komponentem systemu OpenSolaris wydanym jako oprogramowanie open source w ramach projektu OpenSolaris. OpenSolaris (<http://opensolaris.com/>) to wersja open source systemu operacyjnego Solaris.

## Novell NetWare oraz Open Enterprise Server

Oprogramowanie NetWare firmy Novell miało bardzo ważną pozycję w czasie opracowywania sieciowych systemów operacyjnych. Przez niemal dekadę NetWare był najważniejszym systemem sieciowym dla komputerów PC, w szczególności dla serwerów plików i wydruku oraz sieci heterogenicznych zawierających różne typy klientów. Kiedy Microsoft Windows Server i szczególnie serwery Linux stały się popularniejsze, NetWare jako platforma sieciowa stracił na znaczeniu. Firma Novell skoncentrowała swoje wysiłki programistyczne na narzędziach zarządzania siecią (ZenWorks), usługach katalogowych klasy przemysłowej (eDirectory) oraz innych produktach, które reprezentowały aktualny stan rozwoju w tej dziedzinie.

W konsekwencji tych czynników rynkowych Novell nadal pozostaje liderem w wymienionych obszarach, ale po kontynuacji prac nad NetWare do wersji 6.5 (wydana po raz pierwszy w sierpniu 2003 roku) firma przeniosła ofertę zarówno biurową, jak i serwerową do dystrybucji systemu Linux. Oprogramowanie NetWare 6.5 zostało zastąpione przez Open Enterprise Server (OES), które w wersji 2 SP1 bazuje na jądrze NetWare 6.5 SP8. System OES 1 pojawił się w marcu 2005 roku, natomiast wersja OES 2 SP3 została wydana w grudniu 2010 roku.

OES jest 64-bitowym sieciowym systemem operacyjnym, który może być uruchomiony jako maszyna wirtualna w monitorze maszyn wirtualnych Xen (ang. *Hypervisor XEN*) na bazie SUSE Linux Enterprise Server (SLES) 10. Firmy Xen i SUSE zostały przejęte przez Novell. SUSE Linux jest dostępny również dla użytkowników jako openSUSE, obecnie w wersji 11. (<http://www.opensuse.org>), a SUSE Linux Enterprise jako serwer w wersji open source. Natomiast SUSE Linux Enterprise Desktop (<http://www.novell.com/products/desktop/>) to komercyjna wersja klienta dla OES.

OES 2 to system sieciowy, który może działać na bazie jądra NetWare albo Linux. Novell umieścił OES jako rozwiązanie przemysłowe do obsługi serwera plików, serwera wydruku, usług katalogowych oraz aplikacji sieciowych. Jeśli działa na bazie jądra NetWare, produkt nosi nazwę OES-NetWare i umożliwia dodanie modułów NLM (ang. *NetWare Loadable Modules*). Dzięki modułom NLM możliwe jest dodawanie różnych aplikacji, przede wszystkim Apache, eDirectory, GroupWise, iPrint, NSS, OpenSSH, Tomcat oraz innych. Wspomniany NLM to moduł wykonawczy bądź dodatek rozszerzający jądro NetWare.

## Windows Server

Windows Server jest uznawany za serwer ogólnego przeznaczenia, który oferuje najlepszą i najszerszą obsługę aplikacji sieciowych ze wszystkich omówionych dotąd sieciowych systemów operacyjnych. Unikalną zaletą firmy Microsoft pozostaje fakt, że Windows kontroluje niemal 90% światowego rynku systemów operacyjnych dla komputerów biurowych, co skutkuje ogromną liczbą cennych funkcji, takich jak zautomatyzowana implementacja, zarządzanie polityką<sup>3</sup> (ang. *policy engine*) sieciowego systemu operacyjnego oraz inne dostępne funkcje.

Pod marką Microsoft Server firma Microsoft sprzedaje także rozbudowany zestaw aplikacji serwerowych. Przykłady produktów Microsoft Server to między innymi Biz Talk Server, Commerce Server, Exchange Server, Internet Information Server (dołączony do Windows Server), ISA Server, SQL Server, Windows Storage Server (w postaci oddzielnego wydania Windows) itp. Różne wersje Windows Server obejmują produkty od Windows Home Server, przez Windows Small Business Server, aż do Windows Datacenter Edition. Spośród wszystkich produktów wymienionych powyżej Microsoft Exchange osiągnął najwyższą pozycję na rynku poczty korporacyjnej, natomiast SQL Server to najlepiej sprzedający się komercyjny serwer bazy danych klasy przemysłowej.

Technologia serwerowa Microsoftu miała swój początek w pracach nad systemem operacyjnym OS/2 we współpracy z firmą IBM. Microsoft porzucił OS/2 i zapoczątkował projekt Windows NT, kierowany przez Davida Cutlera. Zaprezentowany w lipcu 1993 roku Windows NT był pierwszym komercyjnym 32-bitowym systemem i miał numer wersji 3.1, aby zachować zgodność z aktualnymi systemami biurowymi Microsoftu. Kolejne wersje serwerowego systemu operacyjnego nosiły nazwy Windows Server 2000, Windows Server 2003 oraz Windows Server 2008.

Początkowym celem opracowania NT było utworzenie systemu operacyjnego, który byłby bardziej przenośny i mógł działać na wielu różnych rodzajach procesorów. Hybrydowe jądro NT zostało wyodrębnione z architektury komputera przez HAL (ang. *Hardware Abstraction Layer*), a tryb jądra oddzielono od trybu użytkownika. Z początkowych architektur x86 (IA32), PowerPC, MIPS R3000/4000, DEC Alpha oraz IA64 (Itanium i AMD64) pozostały jedynie wersje x86 i IA64. Tryb użytkownika obsługuje wiele różnych systemowych API łącznie z Win32, OS/2 oraz POSIX. Początkowy stos sieciowy bazował na OS/2 LAN Manager, który ostatecznie przeprojektowano na bazujący na BSD Unix. Rodzimy system plików Windows Server to NTFS i jest on ciągle rozwijany wraz z systemem operacyjnym. System Microsoft Windows jest znany z doskonałej bazy sterowników obsługi-

<sup>3</sup> To termin stosowany przez Microsoft; firma Novell stosuje pojęcie „mechanizm reguł” — *przyp. tłum.*

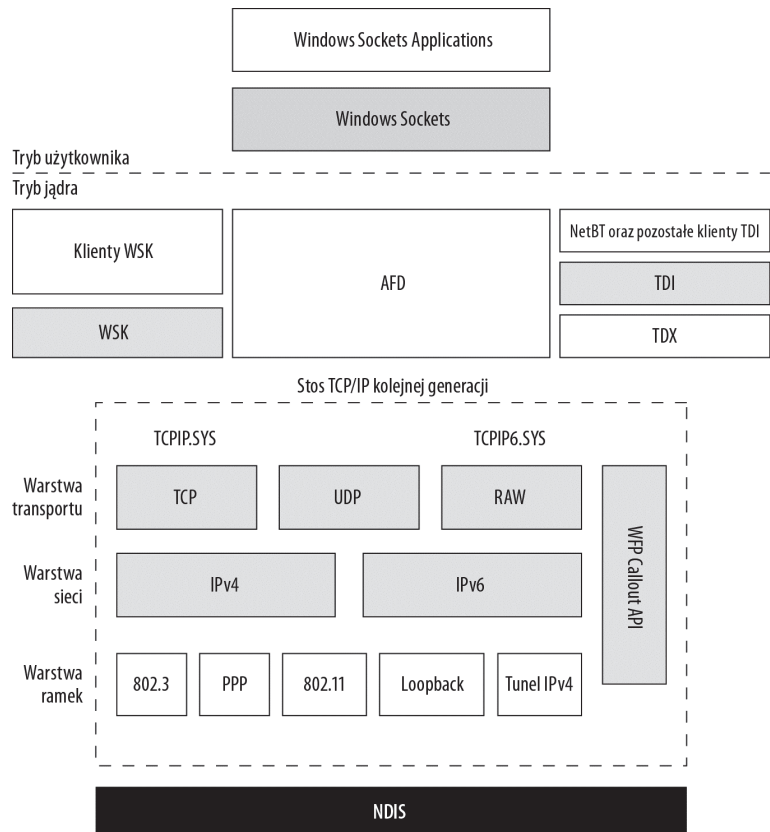
wanych za pomocą technologii Windows Driver Foundation (znanej również jako Model), które pozwalają na obsługę ogromnej ilości urządzeń dostępnych na rynku. Poza tym system Windows jest znany ze ścisłego przestrzegania zasady, aby kolejne wersje były maksymalnie zgodne z poprzednimi.

Każda nowa wersja systemu operacyjnego Windows Server wprowadza małą liczbę nowych, głównych podsystemów sieciowych oraz długą listę nowych funkcji. Istotna funkcja wprowadzona w Windows Server 2000 to technologia Active Directory, która została usprawniona w Windows Server 2003. Windows Server 2003 zaoferował także poważne usprawnienia w zakresie zarządzania politykami, stabilności oraz zarządzania systemem. Z kolei ważne funkcje Windows Server 2008 to obsługa dużej liczby technologii bazujących na sieci, które obsługują aplikacje rozproszone, powstałe na podstawie platformy .NET. Ponadto wprowadzono nowe procedury graficzne oraz technologię wirtualizacji Hyper-V.

W systemie operacyjnym Windows Server 2008 zupełnie przeprojektowano stos sieciowy TCP/IP na architekturę, którą pokazano na rysunku 20.4. NDIS znajduje się na dole i jest warstwą sterowników urządzeń Windows.

#### Rysunek 20.4.

*Kolejna generacja stosu sieciowego TCP/IP, wprowadzona w systemach operacyjnych Windows Server 2008 i Vista*



Gdy trwały prace nad książką, najnowszymi wersjami Windows były Windows Server 2008 R2 oraz Windows 7. System Windows 7 pojawił się w roku 2010 i jest zoptymalizowaną wersją systemu Vista, działającą na platformach x86 oraz IA64 (Itanium).

## Podsumowanie

Sieciowy system operacyjny (ang. *Network Operating System*) dostarcza klientom usługi sieciowe. Poznanie systemów sieciowych jest konieczne, aby zrozumieć sposób tworzenia sieci komputerowych.

Każdy sieciowy system operacyjny musi obsługiwać sprzęt, na którym jest uruchamiany, protokoły i usługi, a także dostarczać te usługi bądź aplikacje komputerom klientów. System sieciowy może również oferować dowolną liczbę innych usług; gdy ma szeroką gamę możliwości, nosi nazwę platformy. Unix, Linux, Solaris, NetWare i Microsoft Windows Server to przykłady platform sieciowych, które zostały omówione w rozdziale.

W kolejnym rozdziale będzie przedstawiona podstawowa funkcja systemu NOS, czyli usługi katalogowe. Usługi katalogowe przechowują informacje dotyczące obiektów sieciowych. Informacje te można wykorzystać w różnych kontekstach.

# Rozdział 21.

# Usługi domen i katalogowe

## **W tym rozdziale:**

- ♦ Co to jest usługa katalogowa?
- ♦ Jak informacje pozwalają na tworzenie inteligentnych aplikacji sieciowych?
- ♦ Jak usługi katalogowe organizują sieci w domeny?
- ♦ Co to jest Microsoft Active Directory?

Usługi katalogowe odgrywają ważną rolę w bieżącej architekturze klient-serwer sieciowych systemów operacyjnych. Zapewniają usługi nazw, przechowują informacje na temat obiektów w sieci oraz pozwalają na przekazywanie tych informacji dalej, do innych serwerów i aplikacji. Obecnie w użyciu jest wiele usług katalogowych, a nowoczesne sieci bardzo intensywnie z nich korzystają.

Najmniejszą podstawową jednostką w usłudze katalogowej jest domena. Domena to zbiór systemów współdzielących tę samą bazę danych bezpieczeństwa. Domeny mogą być różnych typów i zawierać takie elementy, jak jednostki organizacyjne, konta użytkowników i komputerów, a także inne obiekty, do których można uzyskać dostęp za pomocą unikalnej nazwy.

Większość nowoczesnych usług katalogowych bazuje na standardzie X.500. Wersja LDAP dla X.500 została utworzona dla sieci TCP/IP i jest używana w większości obecnie dostępnych produktów. W rozdziale zostaną omówione różne usługi katalogowe oraz ich cechy charakterystyczne. Wśród zaprezentowanych funkcji znajdują się między innymi zarządzanie polityką, replikacja i synchronizacja, jednokrotne logowanie, przestrzenie nazw, zarządzanie tożsamościami oraz kontrola dostępu na podstawie ról.

Microsoft Active Directory (AD) to najlepiej znana i najczęściej używana usługa katalogowa. Technologię AD zbudowano w celu przechowywania obiektów różnego typu z uwzględnieniem aspektów bezpieczeństwa. W rozdziale będą omówione różne klasy obiektów przechowywanych w AD oraz sposoby implementacji domen oraz ich wzajemny wpływ na siebie.

## Usługi katalogowe i domeny

Duże sieci komputerowe stanowią problem dla projektantów sieciowych systemów operacyjnych działających w modelu klient-serwer. W jaki sposób zarządzać ogromną liczbą systemów, użytkowników, urządzeń peryferyjnych oraz innymi elementami znajdującymi się w sieci? Rozwiązanie sprowadza się do takiego przechowywania informacji w bazie danych położonej w pewnym miejscu sieci, aby dostęp do tych informacji był szybki i niezawodny. Oprogramowanie zarządzające takimi informacjami nosi nazwę *usługi katalogowej*, a podstawowa jednostka używana do przechowywania informacji sieciowych nosi nazwę *domeny*. Domena jest zwykle powiązana z własną bazą danych bezpieczeństwa.

Projektanci sieciowi zdali sobie sprawę, że mogą przechowywać informacje o usługach i aplikacjach dostępnych w sieci, kontrolować, kto i jak może uzyskać dostęp do tych aplikacji, a także monitorować wiele innych właściwości. Ponadto zdali sobie sprawę, że tego rodzaju informacje mogą działać w charakterze klucza w mechanizmie uwierzytelniania i autoryzacji, a taki system zapewnia niemal nieograniczone możliwości rozbudowy. Oznacza to, że w późniejszym okresie te bazy danych mogą być używane do zaspokajania innych wymagań, które nie istniały w trakcie ich pierwotnego opracowywania.

W poprzednich rozdziałach Czytelnik spotkał się już z przykładem usługi katalogowej, którą jest technologia DNS (ang. *Domain Name Service*).



Technologia DNS została omówiona w rozdziale 19.

Sieciowe bazy danych, które zostały zaimplementowane jako usługi katalogowe, działają na zasadzie podobnej do słownika. Są one bliskie idei książki telefonicznej; w wielu ogromnych projektach baz danych słowo *katalog* zostało zastosowane w latach siedemdziesiątych. Ponieważ katalog ten opracowano w celu dostarczania usługi sieciowej, ostatecznie zaczęto stosować pojęcie *usługi katalogowej*. Standaryzacja usług katalogowych w postaci kilku modeli przemysłowych doprowadziła do rozprzestrzenienia się usług katalogowych we wszystkich sieciowych systemach operacyjnych. Ponadto spowodowała zastosowanie ich w ogromnych aplikacjach przemysłowych, służących do zarządzania przechowywanymi danymi różnych rodzajów.

Ponieważ informacje przechowywane w centralnych sieciowych bazach danych niewątpliwie są poufne, muszą być odpowiednio chronione, a ochrona tych danych musi być w pełni powiązana z centralnym magazynem informacji i za jego pośrednictwem zarządzana. Niektóre usługi katalogowe traktują bezpieczeństwo sieci jako jedną całość, podczas gdy inne współpracują z zewnętrznymi systemami bezpieczeństwa.

Usługa katalogowa może być zbudowana za pomocą dowolnego rodzaju bazy danych: pliku jednorodnego, relacyjnie, hierarchicznie, na zasadzie „równy z równym” itd. Najpopularniejsze usługi katalogowe to takie, które są półrelacyjne, hierarchiczne, wysoce skalowalne i przechowują obiekty danych. Skalowalność jest ważnym czynnikiem, ponieważ zawsze występuje potrzeba zachowania wszystkich informacji wraz z rozwojem i zmianami sieci.

Wprawdzie usługa katalogowa jest podobna do bazy danych, ale istnieją pewne istotne różnice. Informacje usługi katalogowej są odczytywane znacznie częściej, niż są w niej zapisywane. Dlatego też nie jest konieczne stosowanie mechanizmów takich jak wycofywanie transakcji. Wspomniane mechanizmy nie są zaimplementowane tak dobrze jak w systemach relacyjnych baz danych (ang. *Relational Database Management Systems*, RDBMS). Poza tym usługi katalogowe nie mają takich samych wymagań w zakresie wydajności i normalizacji (optymalizacji) jak w przypadku relacyjnych baz danych. Można się przekonać, że wiele usług katalogowych tworzy w wielu miejscach powtarzające się zbiory danych, o ile może to przyczynić się do zwiększenia wydajności. Relacyjna baza danych może być zaprojektowana bardzo precyzyjnie, ponieważ jest budowana w celu dostarczania określonej funkcji. Usługa katalogowa może być wykorzystywana do przechowywania różnorodnych danych, powiązanych ze sobą w losowy sposób, a więc wymaga mniej strukturalnego schematu.

## Banyan VINES

Obszar usług katalogowych zawdzięcza bardzo wiele opracowaniu Banyan VINES, powstałemu we wczesnych latach osiemdziesiątych. VINES to skrót od *Virtual Integrated Network Service*; był to sieciowy system operacyjny bazujący na systemie Unix. W swoim stosie sieciowym system VINES używał bardzo popularnego w tamtych czasach zestawu protokołów XNS (ang. *Xerox Network Services*) i miał wbudowany wariant o nazwie VIP (ang. *VINES Internetwork Protocol*). Sieci VINES bazowały na pakietach, używały automatycznego adresowania klientów oraz miały protokół routingu i protokół kontroli internetu. Protokoły warstwy górnej aplikacji zawierały standardowe usługi plików oraz wydruku. Żadna z tych technologii nie jest szczególnie interesująca. Jednak system VINES był unikalny dzięki StreetTalk, usłudze nazw wysokiego poziomu.



XNS był bazującym na pakietach zestawem protokołów LAN, używanych w latach osiemdziesiątych i dziewięćdziesiątych jako podstawa dla oprogramowania Novell NetWare, 3COM oraz innych firm. Sieci TCP/IP całkowicie zastąpiły sieci w technologii XNS.

Usługa StreetTalk była jedną z wczesnych usług katalogowych. W rozproszonej, replikowanej bazie danych tworzyła przestrzeń nazw dla całej sieci i pozwalała różnym sieciom na współdzielenie zasobów. W technologii StreetTalk adres był tworzony na podstawie hierarchicznego schematu nazw, odwzorowującego hierarchię obiektu, i miał postać obiekt@grupa@organizacja. Obiekt mógł być udziałem sieciowym, drukarką sieciową bądź kontem użytkownika. W tamtym czasie oprogramowanie klientów działało w systemach MS-DOS i Windows 3.x. W sieci VINES nie występowały domeny.

Począwszy od 1985 roku, przez niemal dekadę technologia VINES była produktem wybieranym podczas instalacji systemu operacyjnego wraz z osadzoną w nim usługą katalogową. Technologia ta osiągnęła sukces rynkowy i była zainstalowana w ogromnej liczbie systemów. Ostatecznie firma Novell wprowadziła Novell Directory Services, a Microsoft zaprezentował Active Directory — produkty te przyczyniły się do wypchnięcia VINES z rynku. Jim Allchin, kluczowy inżynier w Banyan VINES, dołączył do firmy Microsoft w połowie lat dziewięćdziesiątych i miał ogromny wkład w pracę nad Active Directory. Firma Banyan stawała się coraz bardziej zbędna i porzuciła swoją markę w 1999 roku.

## Typy domen

Każdy system informacji jest zorganizowany wokół jednostki podstawowej. W bazach danych taką jednostką jest rekord, w systemie plików to plik, natomiast w usłudze katalogowej będzie to domena. Domena sieciowa opisuje grupę systemów i powiązanych z nimi zasobów, które są zorganizowane przez usługę katalogową i współdzielą bazę danych bezpieczeństwa oraz model bezpieczeństwa.

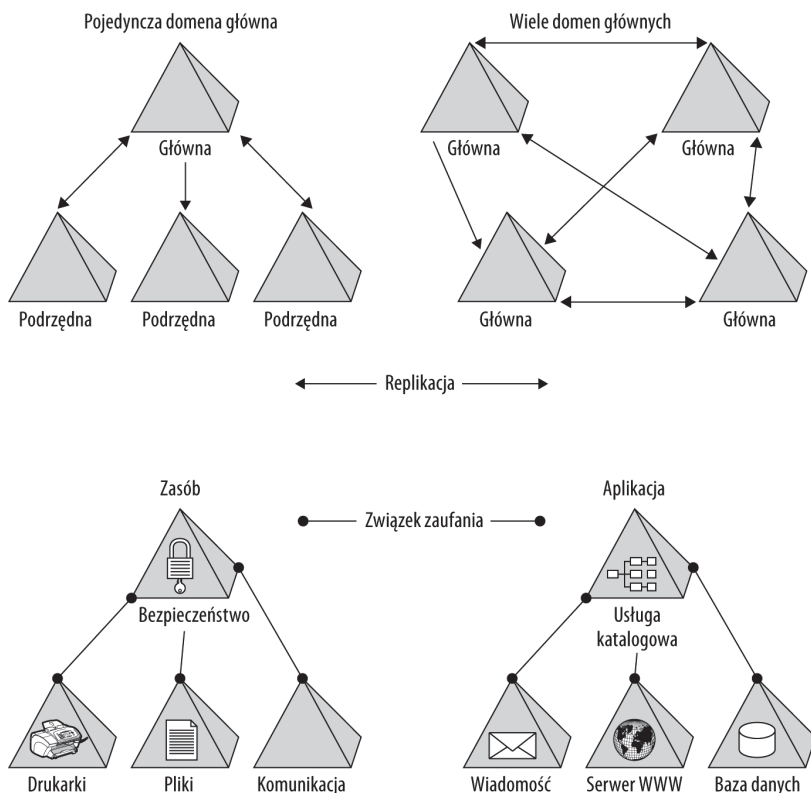
Istnieje wiele różnych schematów używanych do organizowania typów domen. Wśród najczęściej spotykanych można napotkać wymienione poniżej lub ich dowolne kombinacje:

- ♦ centralna domena główna zorganizowana z domenami podrzędnymi w strukturę drzewa, hubu bądź gwiazdy, tzw. „pojedyncza domena główna” (na rys. 21.1);
- ♦ struktura wielu domen głównych;
- ♦ domeny zasobów;
- ♦ domeny zdalne, gdzie łącza przedstawiają zaufane związki i (lub) replikacje, są połączone siecią WAN;
- ♦ domeny charakterystyczne dla aplikacji.

Różne typy domen pokazano na rysunku 21.1.

**Rysunek 21.1.**

*Różne topologie domen*



## Wzajemna współpraca

Migracja usługi katalogowej utworzonej dla dużej sieci do innej usługi katalogowej to jedno z najboleśniejszych zadań dla zespołu IT organizacji, które musi być wykonane. Z dwóch powodów zadanie to okazuje się znacznie trudniejsze niż przeniesienie danych z jednej, przemysłowej bazy danych do innej. Pierwszy — większość baz danych jest dostarczana z funkcjami eksportu i importu albo istnieją dla nich narzędzia firm trzecich, pozwalające na wykonanie tego rodzaju operacji. Drugi — usługi katalogowe są powiązane z funkcjami bezpieczeństwa oraz strukturami własnościowymi, co znacznie utrudnia rozgrzyzenie i wyodrębnienie danych znajdujących się w usługach katalogowych.

Heterogeniczna usługa katalogowa przechowuje informacje o systemach działających pod kontrolą różnych systemów operacyjnych, co jest funkcją cenną z wielu powodów. Sposób, w jaki obce systemy są przedstawiane w usłudze katalogowej, pokazuje, ile producent tego systemu katalogowego włożył pracy, aby osiągnąć dany efekt. W przypadku wielu usług katalogowych heterogeniczność niekoniecznie będzie zaletą, a preferowana będzie homogeniczność.

Wcale nie tak rzadko można się spotkać z sytuacją, w której wiele usług katalogowych działa na różnych serwerach znajdujących się w całej sieci. Usługa katalogowa istnieje dla każdego ważniejszego sieciowego systemu operacyjnego. Wiele z nich może być powiązanych z serwerami WWW, na przykład Apache, podczas gdy inne mogą być częścią korporacyjnego programu do obsługi poczty elektronicznej, takiego jak Microsoft Exchange lub Lotus Notes.

W ogromnych organizacjach można spotkać nawet pięćdziesiąt usług katalogowych. Zarządzanie tymi wszystkimi informacjami rozsianymi po sieci wiąże się z dużym obciążeniem. W tym celu usługi katalogowe często próbują nawiązać połączenie z maksymalną możliwą liczbą systemów i wymieniać z nimi dane. System, który próbuje w ten sposób skonsolidować informacje, bardzo często jest nazywany mianem usługi federacyjnej. Przykładem federacyjnego systemu bazy danych jest zestaw technologii ERP (ang. *Enterprise Resource Planning*) firmy SAP. Technologia ta jest główną bazą danych dla baz danych.

## Serwery domen

System komputerowy, w którego ramach działa usługa katalogowa, jest nazywany serwerem domen sieci lub kontrolerem domen. Ze względów bezpieczeństwa niemal wszystkie usługi katalogowe przechowują swoje dane oraz powiązane z nimi informacje bezpieczeństwa w tym samym serwerze domen.

W małych sieciach serwery domen poza usługą katalogową mogą oferować także kilka innych usług. Przykładem tego rodzaju systemu jest Microsoft Small Business Server (SBS). Wczesne wersje SBS to: usługi katalogu AD, DHCP, DNS, Exchange Server, IIS Web Server, ISA (Microsoft Internet Security and Acceleration) oraz prawdopodobnie SQL Server. Wszystkie wymienione aplikacje znajdowały się w „pudełku” SBS. Jeżeli serwer był wystarczająco potężny, to z maksymalną liczbą licencji dostępowych mógł działać całkiem dobrze. Późniejsze wersje SBS zwiększyły limit dozwolonych połączeń do 75, co wymagało nieco większej mocy serwera. W przypadku wielu instalacji SBS dostępna jest jedynie niewielka część wymienionych aplikacji.

Ekspersi w zakresie bezpieczeństwa twierdzą, że im mniejsza liczba dodatkowych aplikacji i usług działa na serwerze obsługującym usługę katalogu AD, tym bezpieczniejszy będzie ten serwer. W ogromnych sieciach setek i tysięcy użytkowników oraz połączeń serwery domen są bardzo obciążone obsługą żądań. W celu zarządzania żadaniami różne systemy serwerów katalogów tworzą albo duplikat serwera dla domeny i stosują między nimi replikację danych, albo klasę zapasowych serwerów domen. Te różne podejścia mają swoje wady i zalety w związku z odpornością systemu na awarie i zachowaniem spójności danych.

W zależności od natury domeny i usługi katalogowej, a także przeprowadzanych zadań, domena może mieć jeden serwer domen dla dwóch lub trzech systemów. W przypadku tej wielkości sieci wprowadza się na rynek wiele serwerów domowych bazujących na systemie Linux. W ogromnych sieciach serwer domen może obsługiwać od 50 do 500 systemów. Inne serwery w domenie, które nie są serwerami domen, są nazywane serwerami zasobów i aplikacji. Mogą mieć także inne określenia w zależności od wykonywanych zadań: serwer plików i wydruku, serwer tworzenia kopii zapasowej, serwer odpowiedzialny za bezpieczeństwo lub jakikolwiek inny wymagany przez serwer usługi katalogowej.

## Usługi katalogowe

Usługi katalogowe przechowują metadane, czyli dane dotyczące danych. W obiektowej bazie danych przechowującej dane sieciowe metadane dostarczają kontekstu pozwalającego systemowi na określenie sposobu organizacji danych. Schemat katalogu definiuje zestaw klas obiektu, do których są przypisane zestawy atrybutów wymaganych bądź opcjonalnych. Kiedy to tylko możliwe, większość usług katalogowych używa klas obiektu, atrybutów i numerów identyfikacyjnych, które są zarejestrowane przez IANA (ang. *Internet Assigned Numbers Authority*) jako standardy. Każdy obiekt będący zasobem chronionym jest dołączony do listy ACL (ang. *Access Control List*), która określa, kto może używać tego obiektu.

Metadane dostarczają kontekst relacyjny oferujący to, co w zasadzie jest mapowaniem względem zasobów systemu. Wiele informacji systemowych ma cechę charakterystyczną w postaci oddzielenia danych od kontekstu.

Schemat katalogu pokrywa dane w bazie danych w celu dostarczenia szablonu używanego podczas konstruowania rekordów i plików. Schemat pliku XML odgrywa taką samą rolę względem danych XML, pozwalając na utworzenie strukturalnego dokumentu. Ponieważ usługa katalogowa jest bazą danych, nie powinno być zaskoczeniem, że używa ona schematu jako wzorca projektowego. Usługa katalogowa stanowi warstwę abstrakcji, która oddziela realia fizyczne klientów, serwerów i zasobów od logicznych przypisań, stosując funkcję mapowania bazującą na przypisaniu przestrzeni nazw.

Usługa katalogowa staje się konieczna, kiedy względem sieci zostają wysunięte następujące wymagania:

- ♦ scentralizowane zarządzanie usługami sieciowymi;
- ♦ zdefiniowana polityka bezpieczeństwa wraz z odpowiednio dobranymi uprawnieniami;
- ♦ możliwość przydzielenia różnym osobom odpowiedzialności za określone zasoby;

- ♦ możliwość skalowania sieci w celu obsługi większej liczby użytkowników, niż jest obsługiwana w modelu „równy z równym”;
- ♦ możliwość obsługi różnorodnych klientów oraz systemów operacyjnych;
- ♦ możliwość przeprowadzania nadzoru zdarzeń sieciowych.

Usługi katalogowe mają nie tylko zalety, lecz także pewne wady. Oprócz dodatkowego kosztu i zwiększenia stopnia skomplikowania sieci do prawidłowego funkcjonowania usługi katalogowe wymagają również usług domen, które zawsze powinny być dostępne w sieci. W większości przypadków te dodatkowe wymagania ograniczają wykorzystanie domen w sieciach domowych i małych biurach, gdzie podłączonych jest mniej niż 20 systemów.

## Synchronizacja i replikacja

Usługi katalogowe znajdują się wśród najaktywniejszych usług sieciowych. W celu zwiększenia odporności na uszkodzenia oraz poprawienia wydajności usługi katalogowe są replikowane na różne systemy w różnych lokalizacjach. Kiedy usługa jest replikowana, występuje potrzeba przekazania zmian, które wystąpiły w różnych lokalizacjach, przy zastosowaniu pewnego schematu replikacji. Replikacja to proces przekazywania danych do innego systemu i częstego ich uaktualniania. Bardzo ważne jest to, że replikacja nie zawiera informacji o stanie systemu, lecz jedynie jego bieżącą postać. Metody używane przez usługi katalogowe do przeprowadzania synchronizacji i replikacji danych są takie same jak mechanizmy stosowane przez inne rozproszone aplikacje przemysłowe, takie jak systemy baz danych, i mogą różnić się w zależności od produktu.

Replikacja może być pojedynczą jednostką wykonawczą, propagującą zmiany z jednego systemu do wielu innych, lub procesem ciągłym, w trakcie którego zmiany są propagowane jako zbiór transakcji w czasie. Replikacja wymaga, aby dana zmiana była wprowadzona w każdej kopii, co nazywamy replikacją aktywną. Replikacja aktywna działa przy małej liczbie systemów z rozsądnymi połączeniami sieciowymi, ale eliminuje wiele z zalet replikacji, kiedy liczba systemów rośnie lub znajdują się one w sieci WAN. Alternatywnym rozwiązaniem jest wprowadzanie zmian w jednym serwerze, a następnie ich propagowanie między wszystkimi pozostałymi serwerami katalogu, co nosi nazwę replikacji pasywnej. Niemal wszystkie schematy replikacji używane przez usługi katalogowe są pasywnymi schematami replikacji.

Jeżeli pojedyncza kopia pełni funkcję kopii głównej, to topologia systemu to system główny/system zapasowy. Taka metoda była używana we wczesnych wersjach Microsoft Active Directory wraz z systemami *Primary Domain Controller* oraz *Backup Domain Controller*. Zaletą systemu główny/zapasowy jest prosty proces tworzenia kopii zapasowej oraz brak wymagań w zakresie metod służących do kontrolowania wielu jednoczesnych zmian w tym samym rekordzie. Przejście do topologii wielu serwerów głównych powoduje zwiększenie wydajności i odporności na awarie, gdyż całość nie polega tylko na jednym systemie głównym. Jednak odbywa się to kosztem związanym z koniecznością obsługi współbieżności, prawdopodobnie w postaci implementacji rozproszonej usługi zarządzania blokadami lub innej formy eliminowania konfliktów między danymi. Wraz z wprowadzeniem Windows Server 2003 firma Microsoft przeniosła Active Directory do schematu wielu systemów głównych.

Ponieważ jest to proces asynchroniczny, replikacja w postaci wielu serwerów głównych może być niedoskonała z powodu braku spójności będącego skutkiem opóźnień sieci. Ten rodzaj replikacji nie zawsze spełnia wymagania transakcji ACID, które są wymagane przez większość systemów zarządzania bazami danych. Skrót ACID utworzono od wyrazów *Atomicity* (atomowość), *Consistency* (spójność), *Isolation* (izolacja) oraz *Durability* (trwałość); oznacza on metodę określania, czy transakcja bazy danych spełniła wszystkie wymagania, aby została przeprowadzona z zachowaniem gwarancji poprawności.

Technologia AD używa wzorca uaktualniania, który powoduje uaktualnienie wszystkich serwerów katalogowych, ale wymaga pewnego czasu do zakończenia tego procesu. System replikacji dla AD został opisany jako system *Floating Single Master Operations* lub *Operations Masters* i jest na tyle elastyczny, że pozwala na skalowanie rozwiązania na ogromną liczbę domen i wykorzystuje połączenia o różnej przepustowości.

## Jednokrotne logowanie

W środowiskach, w których stosuje się wiele mechanizmów bezpieczeństwa, każdorazowe weryfikowanie uprawnień użytkownika żądającego dostępu do różnych zasobów i nieustanne wyświetlanie okien dialogowych z prośbą o zalogowanie może być bardzo kłopotliwe. Problem ten ma nazwę „zamęczenie hasłami”. Jednym z rozwiązań jest użycie rozszerzenia BugMeNot dla przeglądarki Firefox i przyjęcie innego aliasu (skuteczne, ale niemiłe). Można też skorzystać z programu takiego jak RoboForm, który przechowuje wszystkie hasła i automatyzuje proces logowania. Jednak żadna z tych metod nie jest uniwersalna.

Usługi katalogowe w ogromnych sieciach nieustannie współdziałają z różnymi usługami katalogowymi, domenami, aplikacjami i zasobami. W celu rozwiązania problemu ponownych operacji logowania niektóre usługi katalogowe oferują mechanizm nazywany jednokrotnym logowaniem (ang. *Single Sign On*, SSO) lub (w przedsiębiorstwach) E-SSO (ang. *Enterprise Single Sign On*). Użytkownik loguje się tylko raz do domeny, a jego dane uwierzytelniające są przechowywane i przekazywane do innych chronionych obiektów w formie przez nią akceptowanej. Tak więc dane uwierzytelniające wprowadzone do sieciowego systemu operacyjnego będą akceptowane przez program pocztowy w przedsiębiorstwie bądź inną aplikację.

Najlepsze z wymienionych systemów wymagają połączenia danych uwierzytelniających, które składają się co najmniej z dwóch z trzech wymienionych poniżej składników „coś”:

- ♦ coś, co znasz (identyfikator i hasło);
- ♦ coś, co masz (na przykład smart card);
- ♦ coś, co masz (na przykład odcisk palca, obraz tęczówki lub wizerunek twarzy).

Niektóre mechanizmy bezpieczeństwa używane przez systemy SSO zostały omówione w rozdziale 27.



Systemy SSO nie są łatwe w implementacji, ponieważ metody uwierzytelniania w różnych systemach mogą stosować różne technologie. Przedmiotem krytyki jest również to, że system SSO eliminuje możliwość, aby różne systemy oddzielnie obsługiwały żądania, co powoduje

zmniejszenie bezpieczeństwa sieci. Jedynie kilka usług katalogowych ma tę funkcję, zwykle w postaci bardzo kosztownego modułu. W większości usług katalogowych w celu implementacji tej opcji konieczne będzie użycie programów firm trzecich, na przykład Citrix Password Manager.

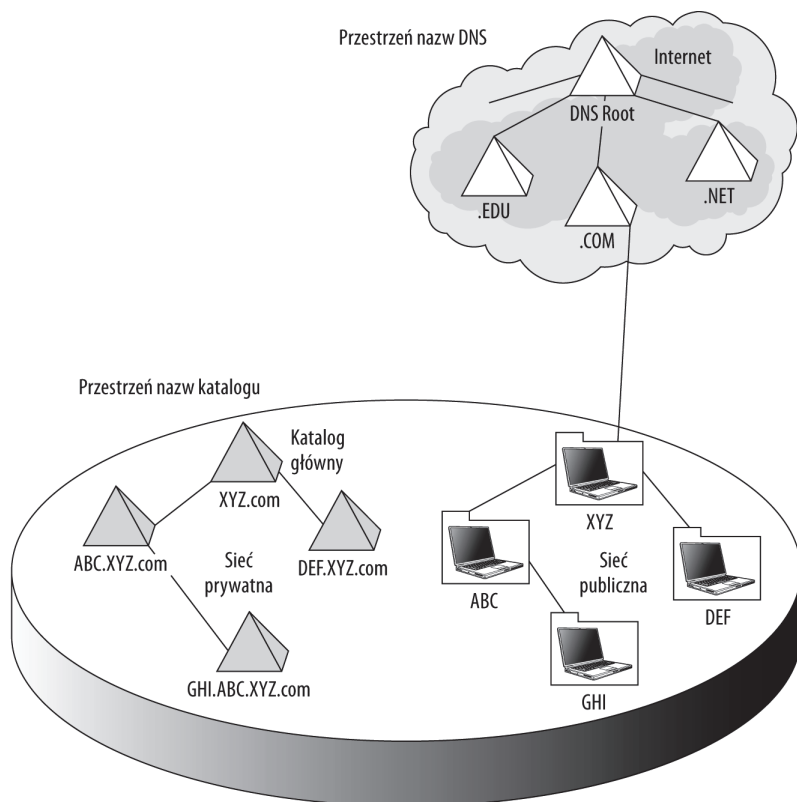
## Przestrzeń nazw

Usługa katalogowa definiuje przestrzeń nazw dla wszystkich przechowywanych obiektów. Czytelnik spotkał się już z użyciem przestrzeni nazw w technologii DNS (ang. *Domain Name Service*), stosowanej w celu przypisania adresów w internecie. Aby zapewnić efektywność, przestrzeń nazw musi tworzyć unikalne oznaczenie, które powinno być logicznym połączeniem różnych gałęzi drzewa. W przypadku DNS będzie to URI (ang. *Uniform Resource Identifier*).

Wiele organizacji zastosowało dla domen schemat nazw odpowiadający sposobowi, w jaki DNS oznacza strukturę katalogów witryny internetowej. Istnieją pewne powody użycia takiego podejścia. Najważniejszy z nich to możliwość późniejszego udostępnienia w internecie struktury domeny bez konieczności wprowadzania znaczących zmian w nazewnictwie. Jednak, jak pokazano na rysunku 21.2, istnieje różnica między stosowaniem nazw w sieci prywatnej a stosowaniem nazw w sieci, która jest połączona z internetem.

### Rysunek 21.2.

Przestrzeń nazw w sieci prywatnej kontra przestrzeń nazw w sieci publicznej



W przypadku katalogu (takiego jak Active Directory) przestrzeń nazw katalogu może zawierać przyrostek `.com`. Nazwa jest budowana na bazie poszczególnych węzłów drzewa. Ścieżka do węzła w DNS jest pobierana na podstawie hierarchii katalogów, na przykład `www.XYZ.com/ABC/GHI`.



Jeżeli w sieci prywatnej ma być używana publiczna przestrzeń nazw DNS, na przykład `.com`, `.gov` lub `.edu`, to trzeba się upewnić, że wewnętrzne i zewnętrzne nazwy domen nie kolidują ze sobą. Publiczny serwer DNS powinien być skonfigurowany w celu przekazywania żądań adresów do wewnętrznego serwera DNS sieci prywatnej.

## Zarządzanie polityką

Podczas przechowywania w bazie danych obiektów z informacjami sieciowymi możliwe jest utworzenie zestawu reguł, które będą określały sposób używania tych obiektów. Wspomniane reguły są przechowywane oddzielnie od mechanizmu bezpieczeństwa wykorzystywanego przez sieciowy system operacyjny, choć niektóre reguły mogą się wzajemnie nakładać.

Polityka będzie definiowała pewne zachowanie sieciowe, włączając w to między innymi:

- ♦ konfigurację systemu klienta;
- ♦ częstotliwość przeprowadzania uaktualnień i instalacji poprawek;
- ♦ zachowanie mechanizmu nadzoru;
- ♦ stopień skomplikowania haseł;
- ♦ zadania przeprowadzane w trakcie operacji logowania i wylogowania.

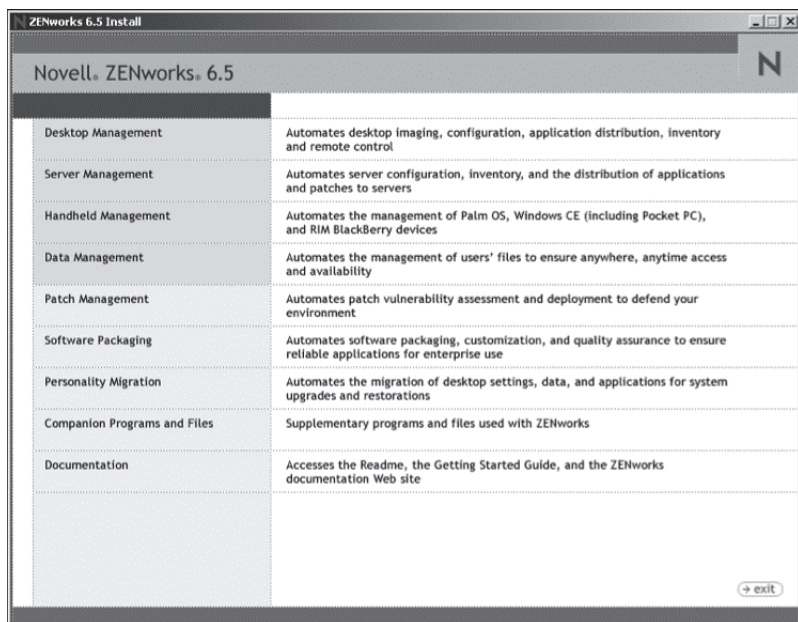
Zarządzanie polityką grupy to mechanizm wymuszający zastosowanie reguł operacyjnych zdefiniowanych dla sieci. Odgrywa taką samą rolę jak reguły biznesowe zapisane w postaci procedur składowanych w systemie relacyjnych baz danych.

Najbardziej znaną usługą zarządzania polityką jest *Group Policies* firmy Microsoft (przechowywana w Active Directory). Istnieje wiele innych usług zarządzania polityką powiązanych z sieciowymi systemami operacyjnymi. SRM (ang. *Solaris Resource Manager*) firmy Sun oferuje zarządzanie polityką ustawiania ograniczeń zasobów. Za pomocą SRM można określić maksymalną liczbę dozwolonych procesów, połączonych użytkowników, liczbę operacji logowania itp. Za pomocą skryptów SRM może wprowadzać nowe zasady polityki tuż po uruchomieniu systemu operacyjnego. Każdy sieciowy system operacyjny implementuje pewną formę zarządzania polityką.

Po rozpoczęciu przeglądania usług zarządzania polityką oferowanych przez firmy trzecie można się przekonać o dostępności ogromnej ilości rozwiązań. Brak miejsca wyklucza dalsze omawianie tutaj tego tematu, ale warto wspomnieć o jednym produkcie: pakiecie aplikacji ZENworks firmy Novell. Produkt ten oferuje wiele możliwości w zakresie usług zarządzania polityką i doskonale działa w heterogenicznym środowisku sieciowym. Na rysunku 21.3 pokazano stronę instalacyjną ZENworks, która pokazuje, jakie możliwości oferuje ten produkt.

**Rysunek 21.3.**

Pakiet ZENworks oferuje dużą liczbę możliwości w zakresie wymuszania stosowania polityki



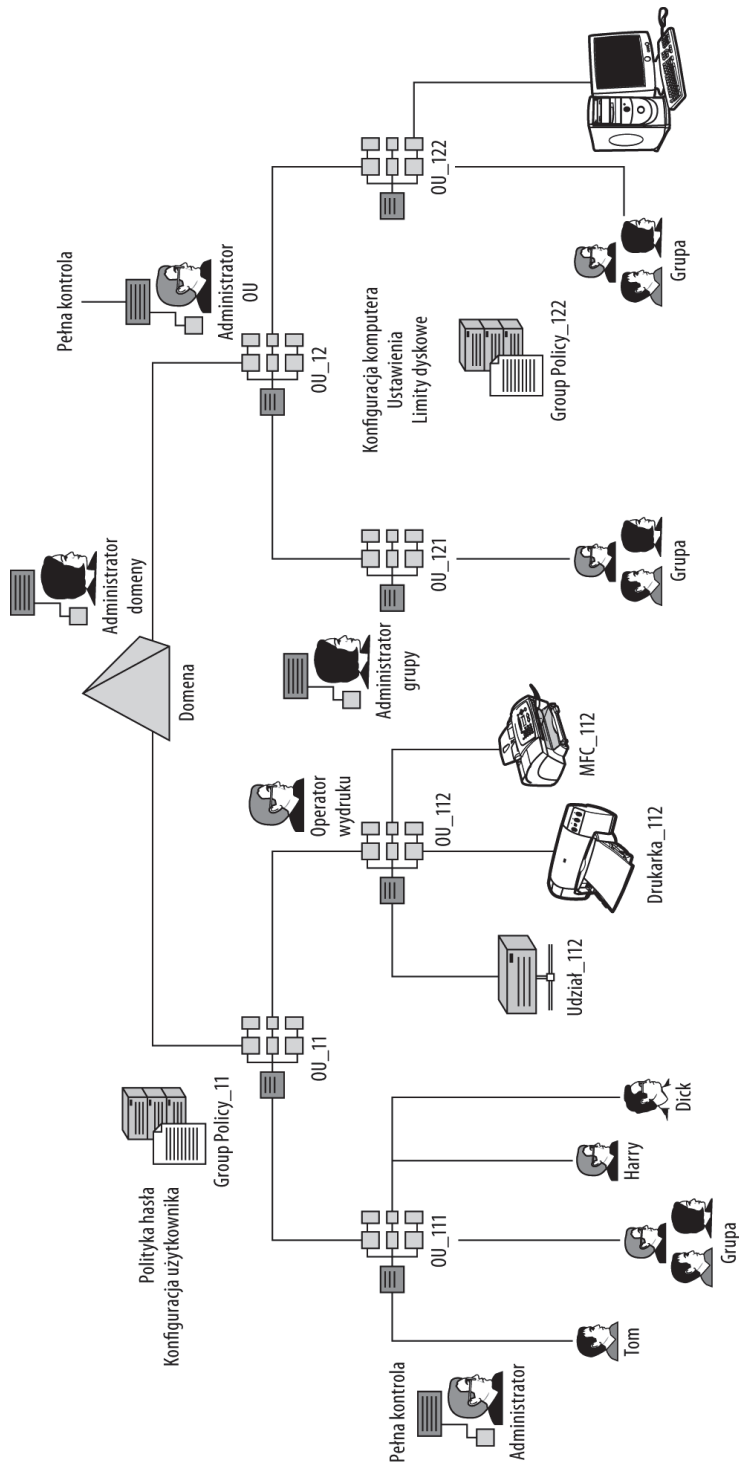
W celu pokazania tego, co można zaimplementować za pomocą silnika napędu polityki, posłużymy się przykładem Microsoft Active Directory. Na rysunku 21.4 można zobaczyć różne grupy polityki, które można zdefiniować w celu kontrolowania, kto ma dostęp do poszczególnych zasobów, sposobów delegowania odpowiedzialności oraz stosowania różnej polityki względem określonych systemów. System zarządzania polityką ma swój początek w Windows 2000 i znajduje się we wszystkich systemach (zarówno klientów, jak i serwerów) wydanych od tamtej chwili. Wraz z wydaniem każdego kolejnego nowego systemu operacyjnego do usługi zarządzania polityką dodawano kolejne możliwości konfiguracji zasad polityki. System Windows Server 2008 jest dostarczany wraz z niemal 2400 ustawieniami zasad polityki.

Domena centralna została podzielona na dwa drzewa w ramach jednostek organizacyjnych (ang. *Organizational Unit*) OU\_11 oraz OU\_12. Administracja domeną została oddelegowana do wzięcia odpowiedzialności za nadzór nad siecią od jednostki OU\_111 w dół, do kolejnego administratora, za operacje wydruku od jednostki OU\_112 do operatora wydruku oraz od jednostki OU\_12 w dół, do administratora. Ponieważ administrator jednostki OU\_12 zachowuje pełną kontrolę, oddelegował administrowanie jednostką OU\_121 do administratora z węższymi uprawnieniami. Oddelegowanie odbywa się jako część mechanizmu bezpieczeństwa, który może, ale nie musi być częścią usługi zarządzania polityką. W przypadku Windows Active Directory polityki bezpieczeństwa są przechowywane w oddzielnej bazie danych. Jednak kontrola nad tymi funkcjami jest możliwa za pomocą centralnej konsoli zarządzania serwerem. Tam można również konfigurować funkcje polityki, jak również innych elementów GUI Windows.

Active Directory pozwala na ustalenie ogólnych zasad polityki, która będzie stosowana względem domeny, oraz na modyfikację zasad tej polityki za pomocą systemu wzorców administracyjnych. Zasady polityki w Windows mogą być zmieniane za pomocą narzędzia

**Rysunek 21.4.**

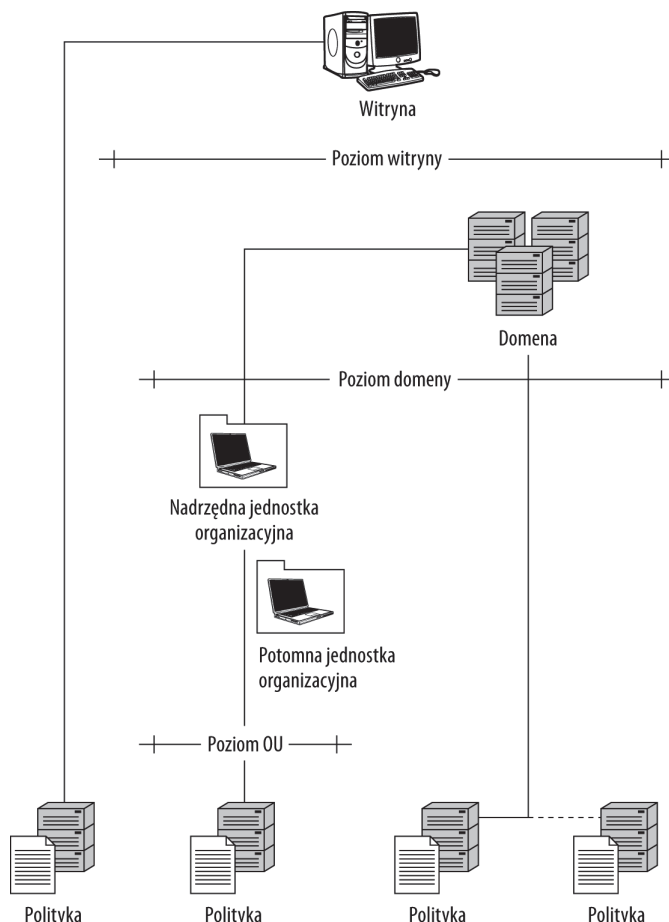
Różne formy grup  
polityki i delegowania



o nazwie *Group Policy Object Editor* w konsoli zarządzania Windows MMC (ang. *Microsoft Management Console*). Zasady polityki ustawiane w Active Directory (zob. rysunek 21.5) mają zastosowanie w systemie Windows. W celu rozszerzenia zarządzania zasadami polityki na systemy Unix, Linux oraz Mac w sieci Windows można użyć produktu takiego jak Centrify DirectControl (<http://www.centrify.com/directcontrol/overview.asp>).

**Rysunek 21.5.**

*Kolejność grup polityki w Active Directory*



W dowolnym miejscu sieci można zastosować grupę polityki, która spowoduje zmianę zachowania węzłów sieciowych znajdujących się na tym samym bądź niższym poziomie. Obiekty polityki grupy mogą być przeznaczone dla witryn, domen oraz jednostek organizacyjnych (OU) i są stosowane w kolejności pierwszeństwa. Polityki grupy dla jednostki organizacyjnej będą stosowane jako ostatnie. Na rysunku 21.4 pokazano dwie zdefiniowane polityki lokalne: politykę grupy\_11, w której polityki nazwy użytkownika i hasła są ustawione dla systemów w jednostce OU\_11 i znajdujących się poniżej; politykę grupy\_122, w której zbiór polityk komputera jest stosowany względem systemów znajdujących się w jednostce OU\_122 i poniżej. Według zestawu reguł zdefiniowanych przez Microsoft lokalne grupy polityki mają pierwszeństwo niż ogólne grupy polityki, ale ich zasięg obejmuje pojedyncze serwery bądź systemy.

Możliwość rejestracji różnych zdarzeń w dziennikach zdarzeń jest ważnym czynnikiem polityki, które dotyczą nadzoru. Wiele usług katalogowych oferuje możliwość tworzenia i przechowywania polityki nadzoru względem obiektów. Nadzór jest stosowany w szczegółowy sposób i może rejestrować dostęp do katalogu bądź zasobu, zdarzenia replikacji oraz wiele innych zmian usługi. Proces nadzoru może wygenerować ogromną ilość danych. Dlatego też w celu zapewnienia maksymalnej wydajności funkcje nadzoru są najczęściej domyślnie wyłączone. Jednak włączenie nadzoru może dostarczyć informacji potrzebnych do diagnozowania błędów systemu, zapewnić dane pomagające w poprawieniu wydajności oraz pomóc w określeniu, jak system bezpieczeństwa odpowiada na zdarzenia. W Windows Server 2008 nadzór można włączyć dla czterech różnych kategorii zdarzeń usługi katalogowej: dostępu, zmian, replikacji oraz replikacji szczegółowej.

## Kontrola dostępu bazująca na roli

Wiele sieciowych systemów operacyjnych implementuje różne klasy użytkowników, do których można odnosić się jak do ról, oraz pewną formę dostępu, nazywaną RBAC (ang. *Role-Based Access Control*). Wspomniane role są bardzo często ułożone w hierarchię, z zachowaniem kolejności pierwszeństwa. Role nadają uprawnienia oraz nakładają ograniczenia w zakresie działań, które mogą zostać podjęte. Wśród systemów używających mechanizmów RBAC znajdują się między innymi Microsoft Active Directory, Sun Solaris, SELinux, SAP R/3, Oracle i FreeBSD.

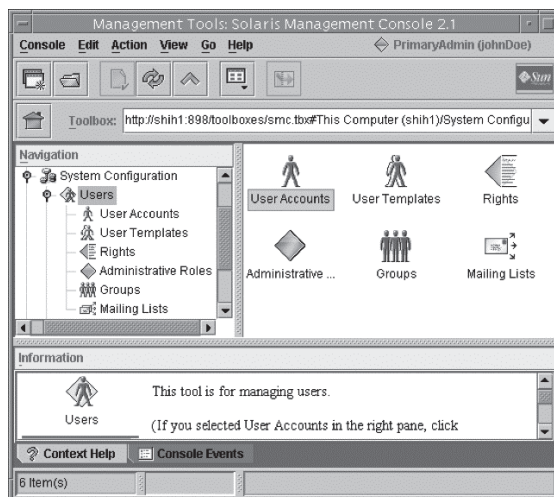
W systemie Windows znajdują się „wbudowane grupy użytkowników”, obejmujące takie kategorie, jak administrator, administratorzy domen, użytkownicy domen, użytkownicy zaawansowani, goście oraz operatorzy wydruku. Zdefiniowane są także powiązane z nimi grupy komputerów, między innymi kontrolery domen, komputery domen oraz replikatory. Oczywiście istnieje możliwość tworzenia własnych.

Mechanizm RBAC w systemie Sun Solaris pojawił się w wersji 8., natomiast w wersji 10. został znacznie rozbudowany. Dostarcza podobnego zestawu ról: wszyscy, administrator główny, administrator systemu, operator, podstawowy użytkownik systemu Solaris itd. Role RBAC mają listę dostępu tworzącą profil, który opisuje możliwości poszczególnych ról. W systemie Solaris z mechanizmem RBAC można pracować z poziomu wiersza poleceń lub za pomocą konsoli SMC (ang. *Solaris Management Console*). Konsola SMC została pokazana na rysunku 21.6. Korzystając z pokazanej konsoli, można dołączać konta użytkowników do ról oraz zarządzać różnymi rolami oferowanymi przez system Solaris.

Pod względem polityki mechanizm RBAC jest neutralny, ma zastosowanie do obiektów niezależnie od polityki, która może stanowić zaprzeczenie danej roli. Zadaniem roli jest symulacja funkcji pracy, a role są definiowane w celu przyspieszenia zarządzania operacjami przypisywania. Rola może zawierać zestaw uprawnień, które pozwalają na przeprowadzanie operacji takich jak dodawanie użytkownika lub wydruk za pomocą wskazanej drukarki. W przeciwieństwie do list ACL (ang. *Access Control List*), które są powiązane z określonym systemem bądź obiektem sieciowym, uprawnienia nadane za pomocą mechanizmu RBAC są powiązane z operacją, na której wykonanie pozwala dana rola. To jest funkcja wyższego poziomu, bardzo często powiązana z aplikacją.

**Rysunek 21.6.**

Konsola Solaris Management Console oferuje dostęp do funkcji RBAC w systemie operacyjnym Solaris



## Zarządzanie tożsamością

Usługi katalogowe przechowują informacje dotyczące użytkowników, ich kont oraz wiele innych powiązanych z nimi właściwości. Z tego powodu usługi katalogowe muszą być blisko powiązane z koncepcją tożsamości oraz mieć możliwość przechowywania informacji zarządzanych przez serwery i usługi obsługi tożsamości. Tożsamość dotyczy zarówno funkcji zarządzania użytkownikiem, jak i bezpieczeństwa. Może zostać zaimplementowana jako funkcja usługi bądź jako samodzielna usługa.

W dużych organizacjach tożsamości użytkowników mogą być przechowywane w wielu różnych miejscach. Usługa tożsamości może pomóc w synchronizacji różnych źródeł informacji w taki sposób, aby zawierały jednakowe dane. Oznacza to synchronizację haseł oraz reguł dostępu, możliwość tworzenia nowych użytkowników i usuwania tych, którzy już nie pracują w organizacji. Ta ostatnia operacja ma zagwarantować, że bezpieczeństwo sieci nie jest zagrożone.

Podobnie jak omówiony wcześniej mechanizm SSO, serwer IDA (ang. *Identity and Access*) musi funkcjonować w różnych systemach sieciowych, aby mógł być użyteczny. W przypadku serwera IDA może być konieczne zapewnienie obsługi następujących funkcji:

- ♦ Zarządzanie certyfikatami oraz kartami smart card, a także połączeniami z różnymi usługami certyfikacji.
- ♦ Zapewnienie federacyjnej usługi wśród wielu usług katalogowych znajdujących się w sieci; zadaniem tej usługi będzie przekazywanie tożsamości między nimi. Najważniejsze usługi katalogowe, których obsługę należy zapewnić, to Microsoft Active Directory, Sun Directory Server, Novell eDirectory oraz IBM Tivoli Directory Server.
- ♦ Praca z usługami tożsamości poczty elektronicznej i komunikatorów internetowych oraz zapewnienie ich synchronizacji, jeśli to konieczne. Lotus Notes i Microsoft Exchange to przykłady dwóch serwerów przechowujących tożsamości, które często współdziałają z tożsamościami innych usług katalogowych.

- ♦ Zarządzanie tożsamościami sieciowej bazy danych tak, aby użytkownik nie mógł się do niej zalogować bez ważnej tożsamości. Oracle, IBM DB2 oraz Microsoft SQL Server to przykłady systemów zarządzania bazami danych, które mogą przechowywać własne konta użytkowników.
- ♦ Praca z aplikacjami korporacyjnymi, takimi jak SAP, aplikacje telefoniczne itd.

Firma Microsoft koncepcje usług tożsamości określa mianem *Identity Lifecycle Management* i dodała te możliwości do serwera MIIS (ang. *Microsoft Identity Information Server*). Serwer MIIS oferuje repozytorium, które zapewnia ujednolicony podgląd danych katalogu znajdującego się w organizacji. Za pomocą MIIS można przeprowadzić konsolidację katalogu, tworzyć konta, wykonywać synchronizację oraz zarządzać hasłami.

## X.500 oraz LDAP

Przemysł telekomunikacyjny utworzył standard w celu umożliwienia współpracy różnych katalogów. Standard ten nosi nazwę *X.500 Directory Access Protocol* (DAP). Protokół ten jest akceptowany przez sieć dowolnego rodzaju. Standard DAP może przechowywać informacje o obiektach dowolnej z siedmiu warstw modelu ISO/OSI. W protokole X.500 klient może wykonać zapytanie do serwera w usłudze katalogowej, używając DAP do komunikacji. Następnie DSA (ang. *Directory System Agent*), czyli baza danych przechowująca informacje, udziela odpowiedzi na to żądanie. Bazy danych DSA są hierarchiczne i połączone ze sobą za pomocą drzewa DIT (ang. *Directory Information Tree*). Z kolei DUA (ang. *Directory User Agent*) to program taki jak *whois*, *finger* bądź polecenie GUI uzyskujące dostęp do DSA.



Za dostosowywanie protokołów LDAP (ang. *Lightweight Directory Access Protocol*) i DAP odpowiedzialna jest organizacja The Open Group (<http://www.opengroup.org>). Więcej informacji na temat protokołu X.500 można znaleźć na witrynie <http://X500Standard.com>. Dostosowanie określa możliwości produktu w zakresie współpracy ze standardami usług katalogowych.

W pełnym schemacie X.500 używane są cztery różne protokoły X.500:

- ♦ **DAP (*Directory Access Protocol*)**. DAP (X.511) definiuje listę operacji, które muszą być obsługiwane przez klienta używającego pełnego modelu OSI. Obejmuje on operacje Add, Bind, Compare, Delete, List, Modify, ModifyRDN, Read oraz Search. Ponieważ istnieje bardzo mała liczba sieci używających pełnego modelu OSI, protokół DAP nigdy nie został szeroko rozpowszechniony. Jednak różne odmiany usług katalogowych LDAP, takie jak Novell eDirectory, zaadaptowały ten zestaw poleceń.
- ♦ **DISP (*Directory Information Shadowing Protocol*)**. X.500 definiuje dwa odmienne mechanizmy służące do replikacji informacji katalogowych: buforowanie oraz *shadowing*. Shadowing to negocjowany mechanizm do replikacji bezpiecznie przechowywanych informacji, natomiast DISP to protokół używany do uaktualniania oraz wymiany danych. Buforowanie polega na przechowywaniu informacji w repozytorium celem ich późniejszego użycia przez innych użytkowników. Buforowanie jest uznawane za mniej niezawodne i bezpieczne, ponieważ może przechowywać informacje z uprzywilejowanych źródeł, do których dostęp mogą uzyskać użytkownicy o mniejszych uprawnieniach.

- ♦ **DOP (*Directory Operational Bindings Management Protocol*)**. Ten protokół jest używany w celu uzgodnienia replikacji danych.
- ♦ **DSP (*Directory System Protocol*)**. Protokół DSP pozwala programowi DSA (ang. *Directory System Agent*) na komunikację z innym programem DSA bądź DUA (ang. *Directory User Agent*). Protokół zapewnia dostęp do informacji bez konieczności posiadania wiedzy dotyczącej miejsca położenia tych informacji.

Kiedy projektanci sieci komputerowej rozpoczynali tworzenie usług katalogowych, w sieciach TCP/IP musieli stosować jedynie X.500, co spowodowało zawężenie definicji X.500 do tylko tego protokołu. Powstały w ten sposób standard został nazwany LDAP (ang. *Lightweight Directory Access Protocol*), choć pojęcie „lightweight” (ang., „lekki”) naprawdę jest niewłaściwe. LDAP to skomplikowana, aczkolwiek zawężona wersja X.500.

## Network Information Service

NIS (ang. *Network Information Service*) to bazujący na RPC system katalogowy klient-serwer przechowujący w bazie danych nazwy użytkowników i systemów dla komputerów w sieci. Ponadto NIS definiuje zestaw procesów używanych w celu zarządzania i uzyskiwania dostępu do usługi katalogowej. Za pomocą NIS administrator może zdefiniować domenę NIS współdzielącą zestaw powszechnie używanych plików konfiguracyjnych. Operacje dodawania tych plików konfiguracyjnych do nowych systemów lub ich modyfikacja mogą być przeprowadzane zdalnie i są względnie łatwe.

Technologia NIS została opracowana przez Sun Microsystems i jest szeroko wykorzystywana w sieciach Unix. Początkowo nosiła nazwę Yellow Pages, jednak spór o znak towarowy z British Telecom doprowadził do zmiany nazwy usługi na NIS. Wszystkie polecenia wiersza poleceń nadal mają przedrostek *yp*. Na przykład polecenie *ypbind* pozwala klientowi NIS na uzyskanie dostępu do serwera NIS za pomocą RPC. Polecenie *ypserv* inicjalizuje proces NIS w serwerze NIS, podczas gdy *rpc.yppasswdd* inicjalizuje demona używanego przez klienty NIS do zmiany haseł bez konieczności ponownego logowania do głównego serwera domeny NIS.



Przewodnik dotyczący konfiguracji NIS można znaleźć na stronie <http://www.freebsd.org/doc/en/books/handbook/network-nis.html>.

W technologii NIS istnieją trzy rodzaje systemów:

- ♦ **Serwer główny NIS**. Te serwery mogą zawierać pliki dla jednej bądź więcej domen NIS.
- ♦ **Serwer zapasowy NIS**. Te serwery mogą zawierać replikowane kopie bazy danych NIS i są stosowane w celu zapewnienia klientom serwerów zapasowych oraz mechanizmu równoważenia obciążenia. Klient zostaje dołączony do serwera NIS, od którego pierwszy otrzymał odpowiedź.
- ♦ **Klient NIS**. Systemy używające usługi NIS w celu pobierania informacji dotyczących bezpieczeństwa.

Technologia NIS przechowuje swoje informacje w tabelach tekstowych w serwerze NIS. Te pliki bazy danych są uważane za mapy NIS i są przechowywane w katalogu *var/yp*. Mapy NIS są generowane w serwerze głównym NIS przy użyciu plików konfiguracyjnych znajdujących się w katalogu */etc*. Jednak plik *master.passwd* nie jest generowany w ten sposób, ma pozostać ukryty. Lista użytkowników znajduje się w katalogu */etc/passwd*, pozostałe pliki, takie jak *master*, *groups* i *hosts*, przechowują w innych lokalizacjach pozostałe informacje NIS. Dane w technologii NIS mogą być szyfrowane za pomocą algorytmu DES, choć ta metoda nie jest tak bezpieczna jak w przypadku większości nowoczesnych usług katalogowych bazujących na LDAP. NIS wymaga, aby przed inicjalizacją mapy NIS z listy kont usunąć informacje dotyczące konta systemowego.

## Serwery LDAP

Obecnie niemal wszystkie nowoczesne usługi katalogowe bazują na protokole LDAP, który zapewnia możliwość współdziałania (aczkolwiek jedynie w niewielkim wymiarze) implementacji tego standardu, oferowanych przez różnych producentów. Dwoma wyjątkami, o których trzeba tutaj wspomnieć, są DNS (ang. *Domain Name System*) i NIS (ang. *Network Information System*), opracowane przed powstaniem standardu X.500 i LDAP.

Poniżej przedstawiono listę kilku z wielu usług katalogowych bazujących na LDAP:

- ♦ Microsoft Active Directory (<http://www.microsoft.com/windowsserver2008/en/us/active-directory.aspx>);
- ♦ Novell eDirectory (wcześniej NDS, czyli NetWare Directory Services; <http://www.novell.com/products/edirectory>);
- ♦ Fedora Directory Server (<http://directory.fedoraproject.org>);
- ♦ OpenDS (<https://opends.dev.java.net>);
- ♦ Oracle Directory Server Service Plus (<http://www.oracle.com/us/products/middleware/identity-management/oracle-directory-services/index.html>);
- ♦ IBM Tivoli Directory Server (<http://www-306.ibm.com/software/tivoli/products/directory-server>);
- ♦ Apple Open Directory (dla systemu Apple OS X Server; <http://www.apple.com/server/macosx/technology/open-directory.html>);
- ♦ ApacheDS (<http://directory.apache.org>).

## LDAP Data Interchange Format

LDIF (ang. *LDAP Data Interchange Format*) to format tekstowy pozwalający różnym serwerom LDAP na wysyłanie i odbieranie rekordów LDAP. Każdy rekord zawiera dane powiązane z obiektem i może być pobrany ze względu na żądania wysłane do usługi katalogowej bądź w celu uaktualnienia. Format LDIF pozostaje standardem IETF. OpenLDAP, Netscape, Mozilla oraz Microsoft mają narzędzia do importu i eksportu informacji w tym formacie. Ponadto istnieją narzędzia takie jak JXplorer, które pozwalają na otwieranie i edytowanie danych LDIF.



W celu zapoznania się z bieżącym dokumentem RFC dla LDIF należy przejść na stronę <http://tools.ietf.org/>, w polu *Doc fetch* wpisać numery dokumentów RFC i potwierdzić, naciskając klawisz *Enter*. Dokumenty te to RFC2849, RFC4510 i RFC4525.

Rekordy LDIF mają następującą postać:

```
DN: CN=Administrator,OU=departmentname,DC=servername,DC=com
objectClass: domain admin
CN: Administrator
```

gdzie DN oznacza *Distinguished Name* (nazwa wyróżniająca), CN — *Common Name* (nazwa wspólna), OU — *Organizational Unit* (jednostka organizacyjna), natomiast DC to *Domain Component* (komponent domeny). Plik LDIF zawiera jeden lub więcej wpisów tego rodzaju, a wiele może zawierać dużą ilość atrybutów o pojedynczej wartości. Polecenia takie jak ADD, REPLACE, DELETE itp. są w podobny sposób osadzone w rekordach.

```
DN: CN=Barrie Sosinsky,OU=Writing,DC=Sample,DC=com
changetype: modify
replace: Location
Location: Room B23
-
DN: CN=Elysian Fields,OU=Evangelism,DC=Sample,DC=com
changetype: modify
add: Location
Location: Room 666
-
itd.
```

Pojedynczy myślnik na końcu jest wymagany w celu oddzielenia rekordów.

## Novell eDirectory

Novell eDirectory to hierarchiczna baza danych zorientowana obiektowo, która obsługuje użytkowników i grupy, role, systemy, aplikacje oraz usługi wraz z właściwościami globalnymi i lokalnymi. Pojęcia **globalne** i **lokalne** wskazują zasięg (na przykład polityki) względem domeny bądź poszczególnych serwerów. Baza danych może być partycjonowana i używa replikacji w postaci wielu serwerów głównych. Novell eDirectory to główny konkurent produktu Microsoft Active Directory, który zostanie przedstawiony w kolejnym podrozdziale. Jednocześnie to bieżąca wersja oprogramowania, które kiedyś nosiło nazwę NetWare Directory Services (NDS); obecnie jest zaimplementowane w niektórych z największych sieci używających usług katalogowych. NDS to usługa katalogowa, która pojawiła się jeszcze przed Active Directory, bazująca na X.500.

eDirectory zapewnia duże możliwości współpracy z innymi produktami i działa na serwerach i klientach Windows, Linux, NetWare, Solaris, HP-UX oraz IBM AIX.

Wśród protokołów używanych przez tę usługę katalogową do komunikacji z obiektami sieciowymi znajdują się:

- ♦ **LDAP**. Protokół *Lightweight Directory Access Protocol* pozwala na wysyłanie zapytań do usługi katalogowej przez sieć TCP/IP, jak przedstawiono we wcześniejszej części rozdziału.

- ♦ **SOAP.** Protokół *Simple Object Access Protocol* jest używany do wymiany strukturalnych informacji XML w sieci.
- ♦ **JDBC.** Protokół *Java Database Connectivity Protocol* to metoda wykonywania zapytań do baz danych w środowisku Java.
- ♦ **ODBC.** Protokół *Open Database Connectivity* to API używane do tworzenia zapytań do baz danych SQL w środowisku Windows.  
ODBC oraz JDBC to podobne technologie, używane na dwóch odmiennych platformach.
- ♦ **DSML.** Protokół *Directory Service Markup Language* reprodukuje usługę katalogową za pomocą XML.
- ♦ **JNDI.** Protokół *Java Naming and Directory Interface* to API Javy, którego klienci Javy używają do wykonywania zapytań względem usługi katalogowej.
- ♦ **ADSI.** Protokół *Active Directory Service Interface* pozwala klientom na wykonywanie zapytań do Active Directory.

## Nazwa wyróżniająca

Wszystkie katalogi LDAP współdzielą zestaw zdefiniowanych obiektów oraz powszechnych metod adresowania, które tworzą nazwę wyróżniającą (ang. *Distinguished Name*, DN) dla obiektu. Dość często spotykane funkcje katalogu LDAP to:

- ♦ **Drzewo katalogu.** Hierarchiczne drzewo wraz z obiektami katalogu jako węzłami.
- ♦ **Węzły.** Węzły to nazwane obiekty pojemników bądź jednostek, którym przypisano zestaw właściwości lub atrybutów. LDAP pozwala na to, aby obiekty miały możliwości rozszerzania, czyli definiowania dodatkowych właściwości.
- ♦ **Atrybuty.** Atrybut jest właściwością, której nazwa jest uznawana jako typ lub opis. Atrybuty mogą mieć jedną lub wiele wartości.
- ♦ **Wpisy.** Wpis stanowi unikalny egzemplarz typu obiektu. Obiekt może mieć przypisaną nazwę wyróżniającą i przez porównanie z jego węzłem nadrzędnym może mieć przypisany RDN (ang. *Relative Distinguished Node*).

Nazwa wyróżniająca jest bardzo ważna, ponieważ pozwala systemowi na wyszukanie i pobranie informacji. Dzięki nazwie wyróżniającej wiadomo, w jaki sposób obiekt jest powiązany z wieloma innymi obiektami. Ogólnie rzecz biorąc, to sposób zapewnienia relacji „jeden do wielu”, która nie jest bezpośrednio obsługiwana w usługach katalogowych.

Microsoft Active Directory używa nazwy wyróżniającej w następującej postaci:

```
/DC=<NazwaDomeny> /O=<NazwaOrganizacji> /OU=<NazwaDziału> /CN=<NazwaSerwera>
```

gdzie DC oznacza *Domain Component* (komponent domeny), O — *Organization* (organizacja), OU — *Organizational Unit* (jednostka organizacyjna), natomiast CN oznacza *Common Name*. Cały zasięg wszystkich możliwych obiektów w tym schemacie adresowania definiuje to, co nazywamy przestrzenią nazw. Przestrzeń nazw definiuje zakres wszystkich możliwych obiektów znajdujących się w katalogu, ale nie każdy i nie wszystkie, które mogłyby istnieć.

Ponieważ usługa katalogowa jest dynamiczna, obiekty można przenosić z jednego miejsca do innego. Po przeniesieniu następuje zmiana nazwy wyróżniającej przeniesionego obiektu. Po przeniesieniu konta komputera Serwer\_1 z Domena\_1 do Domena\_2 nazwa wyróżniająca serwera zostanie odpowiednio zmieniona. W celu zagwarantowania, że obiekt taki jak komputer będzie łatwo identyfikowany, LDAP przypisuje systemowi unikalny identyfikator podczas instalacji systemu operacyjnego. Identyfikator ten ma nazwę UUID (ang. *Universal Global Unique Identifier*).

W produkcie Microsoft Active Directory identyfikator UUID nosi nazwę Microsoft *Globally Unique Identifier* (GUID) i jest numerem przypisanym komputerowi podczas instalacji w nim systemu operacyjnego Windows. Nazwa jest wybierana z przestrzeni nazw zawierającej  $2^{122}$  możliwych liczb, czyli  $5,3 \times 10^{36}$ . To znacznie więcej niż oszacowana liczba gwiazd we wszechświecie ( $7 \times 10^{22}$ ).

## Microsoft Active Directory

Obecnie najczęściej używaną sieciową usługą katalogową jest Microsoft Active Directory (AD). Produkt ten po raz pierwszy pojawił się w Windows Server 2000 i był uaktualniany podczas wydawania każdej kolejnej wersji Windows Server — najnowsza jest wersja trzecia, w zależności od przyjętego sposobu liczenia.

W Active Directory domena jest zbiorem systemów, które zostały pogrupowane za pomocą bazy danych Microsoft Security Account Manager. To jest grupowanie logiczne, bazujące na modelu bezpieczeństwa stosowanym względem elementów składowych w ramach tej samej sieci LAN, systemów znajdujących się w WAN, zdalnych systemów nieregularnie logujących się do domeny, a także wszystkich innych systemów, które mogą być zdefiniowane i z którymi serwer domeny może się łączyć. Każdy system należący do domeny nosi nazwę elementu składowego domeny, a serwer nosi nazwę serwera domeny. Wszystkie pozostałe serwery nazywa się serwerami składowymi lub rzadziej serwerami aplikacji bądź serwerami zasobów.

Active Directory ma szeroką klasę obiektów, którymi może zarządzać. Użytkownicy i grupy są obiektami w katalogu, natomiast kolekcje ich właściwości, praw i uprawnień są nazywane kontami użytkowników i grup. Komputery również są obiektami, ułożonymi względem kont, które w tym przypadku określa się jako konta maszyn. Na rysunku 21.7 pokazano różne obiekty ułożone przez Active Directory. W tabeli 21.1 wymieniono główne obiekty przechowywane w AD.

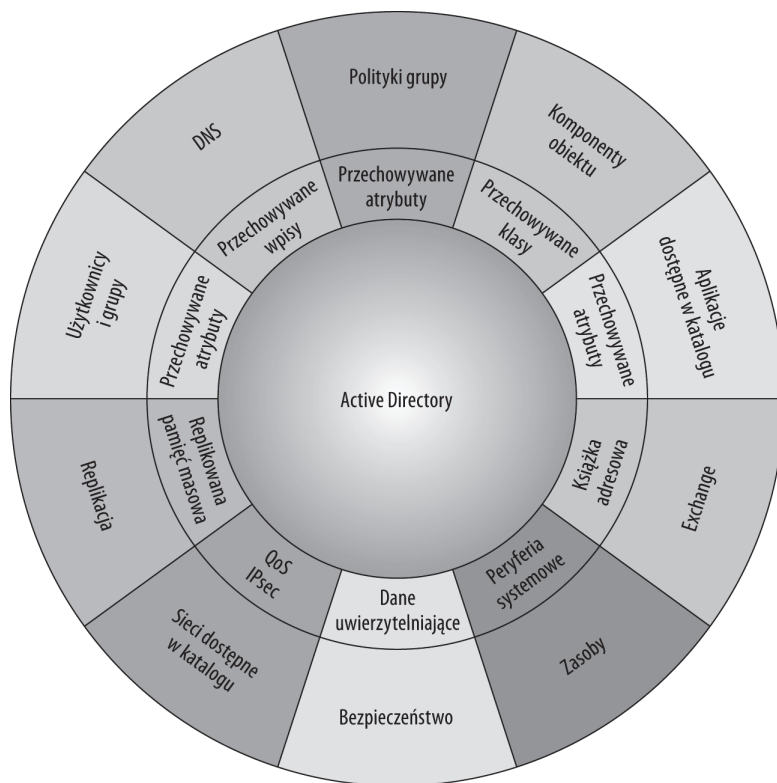
Active Directory używa wersji LDAP bazującej na schemacie nazw X.500. Nazwa wyróżniająca (DN) w Active Directory ma następującą postać:

```
/DC=<NazwaOrganizacji> /OU=<NazwaDziału> /CN=<NazwaSerwera>
```

gdzie DC oznacza klasę komponentu domeny, OU — *Organizational Unit* (jednostka organizacyjna), natomiast CN oznacza *Common Name*. Każdy obiekt w AD ma przypisany identyfikator GUID będący unikalnym, 128-bitowym identyfikatorem, którego nie można zmienić. Niektóre obiekty w AD mają nazwę UPN (ang. *User Principle Name*) i przybierają postać *NazwaUżytkownika@NazwaDomeny*. Active Directory obsługuje nazwy w postaci UNC, URL oraz LDAP URL.

**Rysunek 21.7.**

Obiekty w Active Directory



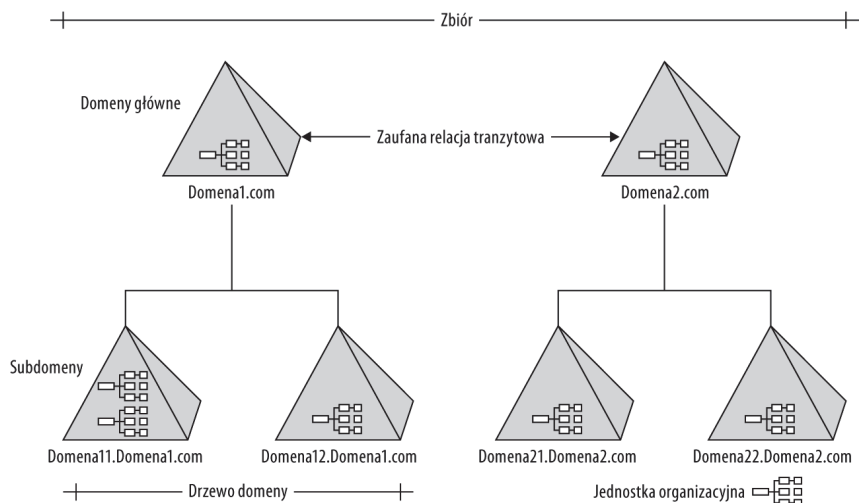
Active Directory rozpoczyna się od utworzenia domeny głównej. Proces ten można przeprowadzić za pomocą kreatora dodawania domeny w Windows Server 2008 bądź za pomocą polecenia `dcpromo`. Dodatkowe domeny można utworzyć w hierarchii, poniżej domeny głównej w drzewie domen. Wspomniane subdomeny są uznawane za domeny potomne domeny głównej. Każda domena utworzona w topologii Active Directory, która jest prywatna, nie musi mieć nazwy rejestrowanej w organizacji ICANN do użycia w internecie.

Jednostki organizacyjne są tworzone w celu oddzielenia funkcji, grup, działów bądź lokalizacji geograficznych. Alternatywne oznaczenie, nazywane miejscem, jest definiowane, kiedy fizyczna charakterystyka części sieci ulegnie zmianie, przykładami mogą być tutaj zdalne biura bądź podsieć.

Kolekcja domen może być ze sobą połączona w postać zbioru — każda domena będzie miała własną bazę danych bezpieczeństwa. Aby w sieci możliwa była komunikacja użytkowników i systemów w różnych domenach, trzeba nawiązać zaufaną relację. Kontrolery domen w zbiorze zawierają informacje o innych domenach w zbiorze dzięki użyciu replikacji. *Zaufana relacja tranzytowa*, jak pokazano na rysunku 21.8, spełnia następujący warunek: jeśli automatyczna zaufana relacja istnieje między domenami A i B oraz B i C, to zaufana relacja istnieje również między domenami A i C. W zbiorze Active Directory jest to wyrażone przez automatyczną zaufaną relację między domeną główną, nadrzędną i pochodną.

**Tabela 21.1.** Przykładowe obiekty przechowywane w Active Directory

Nazwa obiektu	Opis
Użytkownicy	Typ obiektu bezpieczeństwa, osoba.
Grupy	Typ obiektu bezpieczeństwa, grupa kont użytkowników.
Komputery	Typ obiektu bezpieczeństwa, określone stacje robocze lub serwery.
Grupa dystrybucyjna	Obiekty charakterystyczne dla aplikacji.
Domena	Podstawowa kolekcja obiektu Active Directory.
Jednostka organizacyjna	Kolekcja obiektu Active Directory.
Kontakt	Administrator określonego obiektu.
Połączenie	Ścieżka dostępu, zwykle zdefiniowana dla celów replikacji między dwoma systemami.
Katalog współdzielony	Ścieżka dostępu do systemu plików i uzyskanie dostępu do zgromadzonych tam plików.
Drukarka	Obiekt współdzielonej drukarki.
Miejsce	Obiekt pojemnika zwykle zdefiniowany dla położenia geograficznego.
Połączenie miejsc	Obiekt połączenia między dwoma miejscami.
Ustawienia miejsca	Przechowywane obiekty, które są powiązane z danym miejscem.
Podsieć	Grupa adresów sieciowych, które są lokalne względem siebie.
Pojemnik podsieci	Obiekt pojemnika przechowujący obiekty podsieci.
Zaufana domena	Przejsięcie przez obiekt uwierzytelniający.

**Rysunek 21.8.**  
Relacje zbiorów  
względem  
domen  
i jednostek  
organizacyjnych

Baza danych Active Directory przechowuje informacje o zbiorze w trzech oddzielnych kontekstach, czyli partycjach:

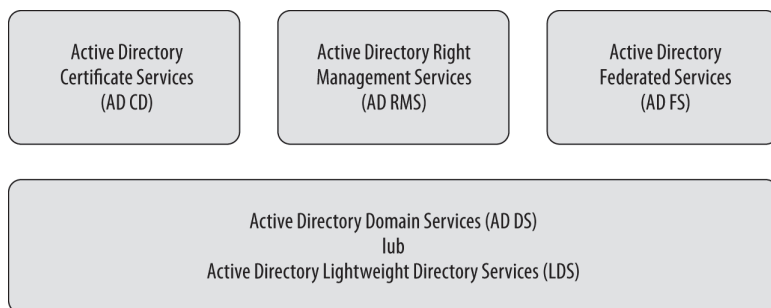
- ♦ **Konfiguracja.** Partycja konfiguracji zawiera fizyczną strukturę zbioru.
- ♦ **Domena.** Partycja domeny przechowuje topologię oraz konfigurację zbioru.
- ♦ **Schemat.** Partycja schematu przechowuje wszystkie obiekty oraz ich atrybuty.

Firma Microsoft dostosowywała Active Directory do różnych edycji systemu Windows. W systemie Windows Server 2003 AD może być skonfigurowane w trybie *Active Directory Application Mode* (ADAM). Użycie trybu ADAM pozwala firmie Microsoft na zaimplementowanie aplikacji takiej jak SQL Server lub Exchange w sieci jako samodzielnej aplikacji z funkcjonującą usługą katalogową bez konieczności tworzenia serwera domeny w tym samym serwerze, w którym działa aplikacja. Tryb ADAM dodał porty SSL i LDAP do wymienionych aplikacji serwerowych oraz umieszcza w dzienniku zdarzeń aplikacji własne zdarzenia.

Jak pokazano na rysunku 21.9, system Windows Server 2008 rozpoznaje różne tożsamości i usługi dostępu pogrupowane w zbiorze roli AD, łącznie z usługami certyfikatów, uprawnień do zarządzania, usługami federacji i usługami domen. Nazwa trybu ADAM została zmieniona na *Active Directory Lightweight Directory Services* (LDS).

### Rysunek 21.9.

*Usługi ról Active Directory w systemie Windows Server 2008*



## Replikacja

Kontrolery domen to bardzo aktywne usługi sieciowe. Ponieważ są uznawane za usługi o znaczeniu krytycznym dla sieci, to albo tworzy się kopie zapasowe kontrolerów domen, albo się je replikuje. Pierwsza wersja Active Directory, która pojawiła się w Windows Server 2000, tworzyła kontroler PDC (ang. *Primary Domain Controller*) jako kontroler główny i replikowała dane do jednego lub więcej kontrolerów BDC (ang. *Backup Domain Controller*). Kiedy kontroler PDC znalazł się w trybie offline lub wymagał operacji konserwacyjnych, można było użyć polecenia `dcpromo` w celu promowania kontrolera BDC do roli PDC. System promowania i degradacji był niewydolny.

Od pojawienia się systemu Windows Server 2003 i po zmianach w systemie Windows Server 2008 firma Microsoft zdecydowała się na system replikacji kontrolerów *Domain Controller* (DC) w trybie wielu kontrolerów głównych, eliminując PDC/BDC, ku rozpaczy niewielu osób. Obecnie każdy serwer, który nie jest kontrolerem DC, pozostaje serwerem

składowym domeny. Proces replikacji powoduje replikację wszystkich danych partycji konfiguracyjnej i schematu do wszystkich pozostałych kontrolerów DC. Trzecia partycja (domeny) jest replikowana jedynie do kontrolera DC w tej samej domenie.

Replikacja domeny dla nowo utworzonego kontrolera DC może prowadzić do wygenerowania znaczącej ilości ruchu sieciowego i jest niepraktyczna w połączeniach WAN o małej przepustowości. W celu umożliwienia zdalnej implementacji nowych kontrolerów DC firma Microsoft utworzyła kontroler RODC (ang. *Read Only Domain Controller*). Wspomniany RODC to kontroler domeny, który zawiera wersję bazy danych Active Directory jedynie do odczytu. Funkcje RODC obejmują replikację jednokierunkową, ograniczone buforowanie danych uwierzytelniających, DNS tylko do odczytu, atrybut filtru zestawu konfiguracyjnego oraz zoptymalizowaną charakterystykę WAN.

## Podsumowanie

W rozdziale przedstawiono usługę katalogową oraz wyjaśniono, dlaczego jest taka istotna. Usługi katalogowe dostarczają wielu informacji, dzięki którym sieć staje się inteligentna.

Usługi katalogowe tworzą przestrzeń nazw, organizują sieć w domeny oraz inne mniejsze jednostki. Domena to zbiór systemów współdzielących tę samą bazę danych bezpieczeństwa.

Większość usług katalogowych bazuje na LDAP, będącym wariantem standardu X.500 DAP. W rozdziale omówiono niektóre funkcje udostępniane przez usługi katalogowe, między innymi silnik napędu polityki, replikację i synchronizację, jednokrotne logowanie, przestrzenie nazw, zarządzanie tożsamością oraz kontrolę dostępu na podstawie ról. Nieco bardziej szczegółowo przedstawiono również produkt Microsoft Active Directory.

W kolejnym rozdziale zostaną omówione usługi plików w sieci oraz sposoby ich implementacji i używania.



# Rozdział 22.

# Usługi plików i buforowanie

## W tym rozdziale:

- ♦ Protokoły i usługi sieciowe zorientowane plikowo
- ♦ W jaki sposób działa NAS?
- ♦ Protokoły usług plikowych
- ♦ Instalacja Samby w systemie Linux
- ♦ W jaki sposób DFS może poprawić wydajność sieci?

Sieciowy dostęp do plików to jedna z najważniejszych usług, jaką może dostarczyć sieć. Usługa ta prawdopodobnie będzie stanowiła ogromny odsetek ruchu w danej sieci. Z tego powodu stosuje się kilka rozwiązań, których celem jest poprawienie czasu udzielania odpowiedzi na sieciowe żądania dostępu do plików, zabezpieczenie treści oraz zagwarantowanie, że treść będzie chroniona.

Każdy sieciowy system operacyjny może zostać skonfigurowany w celu dostarczania plików klientom. Zazwyczaj systemy te nie są zoptymalizowane pod kątem usług plikowych. Klasa serwerów pamięci masowej o nazwie *Network Attached Storage* (NAS) to zoptymalizowany serwer plików, który można wykorzystać we własnej sieci. Serwer NAS często zachowuje się jak urządzenie sieciowe i może być wykorzystywany przez wiele różnych typów klientów. Różnica między NAS i SAN (ang. *Storage Area Network*) polega na tym, że NAS pozwala na transfer plików, podczas gdy SAN i macierze pamięci masowej przeprowadzają transfery bloków.

Obecnie w użyciu jest wiele usług plików służących do efektywnego wysłania pliku przez sieć. Najbardziej znane z tych protokołów to *Network File System* (NFS) oraz *Common Internet File System/Server Message Block* (CIFS/SMB). Protokół NFS jest powszechnie stosowany w systemach Linux i Unix, natomiast CIFS/SMB jest wykorzystywany w większości sieciowych systemów operacyjnych. Przykładem serwera CIFS/SMB jest Samba; w dalszej części rozdziału znajduje się podrozdział omawiający instalację serwera Samba w systemie Ubuntu.

Protokoły usług plikowych dostarczają pewną liczbę ważnych usług. Przeprowadzają uwierzytelnianie klientów żądających dostępu do udziałów sieciowych, obsługują listy dostępu, oferują funkcję przeglądania sieci oraz zarządzają dostępem do plików — umożliwiają blokowanie plików i rekordów. Niektóre z protokołów obsługują również funkcję drukowania poprzez sieć.

Innym rozwiązaniem pozwalającym na rozpowszechnianie plików w sieci jest utworzenie systemu DFS (ang. *Distributed File System*). Technologia ta polega na utworzeniu w różnych miejscach kopii treści, a następnie przestrzeń nazw serwera DFS wskazuje klientom najbliższe położenie żadanego pliku. Technologia DFS jest dostępna w serwerach Windows oraz w postaci rozwiązań firm trzecich.

## Network Attached Storage

NAS (ang. *Network Attached Storage*) składa się z serwerów plików zapewniających klientom sieciowym dostęp do plików. Urządzenia NAS są różnej wielkości, od małych, niewiele większych od zewnętrznego dysku twardego, aż do serwerów wielkości szaf i pojemności wielu terabajtów, jak serwer EMC Celerra NSX. Firma NetApp Inc., dawniej Network Appliance Inc., nazywa oferowane przez siebie systemy *filerami*.

Wiele systemów NAS, szczególnie tych mniejszych, to tak naprawdę urządzenia sieciowe. Takie urządzenie wystarczy podłączyć do zasilania, podłączyć do niego przewód Ethernet i włączyć je — resztą zajmie się samo. System operacyjny NAS zgłasza się do serwera DHCP, otrzymuje dzierżawę adresu IP, a następnie automatycznie pojawia się w sieci. Na tym etapie można przystąpić do konfiguracji udziałów sieciowych, dodawać użytkowników i grupy, nadawać im uprawnienia dostępu oraz wykonywać inne zadania związane z serwerem plików. Systemy NAS w większości są różnorodne — mają wbudowane różne protokoły sieciowe oraz umożliwiają współdzielenie plików z różnymi systemami operacyjnymi.

Większość systemów NAS implementuje bazujące na przeglądarce internetowej narzędzia zarządzające, choć ogromne serwery i urządzenia klasy przemysłowej są dostarczane razem z różnymi programami o potężnych możliwościach, służącymi do tworzenia kopii zapasowej i przeprowadzania replikacji oraz oferującymi wiele innych funkcji dotyczących plików. Urządzenia NAS w większości nie posiadają interfejsów dla monitora, klawiatury i myszy.

Prace nad serwerami plików były prowadzone jeszcze przed wprowadzeniem urządzeń NAS. Firmy Novell Netware i Sun Microsystems pojawiły się w latach 1983 i 1984. Używając protokołów NCP i NFS, mogły utworzyć udziały sieciowe dostępne dla klientów. Jednak były to ogólnego przeznaczenia serwery skonfigurowane jako serwery plików, ale nieoptymalizowane pod tym kątem. Innym znaczącym osiągnięciem było wprowadzenie LAN Manager przez firmy Microsoft i 3Com, co doprowadziło do powstania protokołu NetBIOS poprzez TCP i możliwości używania go przez klienty Windows. W roku 1985 pojawiło się oprogramowanie 3Com 3Server oraz 3+Share, które umożliwiało producentom systemów tworzenie dedykowanych serwerów plików. Przed nadejściem lat dziewięćdziesiątych stało się jasne, że serwery plików to ważna kategoria produktów.

Dobrze poinformowani w dziedzinie przemysłu pamięci masowej uznają firmę Auspex Systems, założoną w roku 1987 przez Larry'ego Bouchera, za pioniera kategorii NAS. Wielu inżynierów i menedżerów z Auspex Systems utworzyło później inne firmy, na przykład NetApp, a sam Boucher stał się jednym z założycieli firmy Adaptec. W roku 1995, wraz z wprowadzeniem filera NetApp — oficjalnie znanego jako server FAS (ang. *NetApp Fabric Attached Storage*), obsługujący protokoły Unix NFS oraz Windows CIFS — powstała kategoria dedykowanych i własnościowych serwerów NAS. Obecnie systemy NAS są oferowane przez wielu różnych producentów.

W kolejnych podrozdziałach zostaną omówione funkcje serwerów plików, a także różnice między urządzeniami NAS i SAN. Urządzenia NAS są bardzo użyteczne w buforowaniu treści w sieci oraz dostarczaniu tej treści do rozproszonych systemów. Ten temat będzie poruszony w dalszej kolejności.

## Funkcje NAS

Filer NAS wymaga czterech elementów:

- ♦ zoptymalizowanych sieciowych funkcji wejścia-wyjścia;
- ♦ zoptymalizowanych dyskowych funkcji wejścia-wyjścia;
- ♦ systemu plików o potężnych możliwościach;
- ♦ dużej ilości przestrzeni dyskowej, najlepiej w postaci chronionej, na przykład RAID (ang. *Redundant Array of Independent Disks*).

Większość funkcji dodatkowych w sieciowych systemach operacyjnych ogólnego przeznaczenia może być usuniętych w celu poprawienia wydajności w wymienionych obszarach. W rzeczywistości urządzenia NAS to najczęściej bardzo okrojone systemy operacyjne, które są zaskakująco niewielkie. Urządzenia NAS mogą być sterowane przez małe, osadzone układy scalone ASIC (ang. *Application-Specific Integrated Circuits*), a niektóre mogą się mieścić na dyskietkach bądź małych pendrive'ach USB.

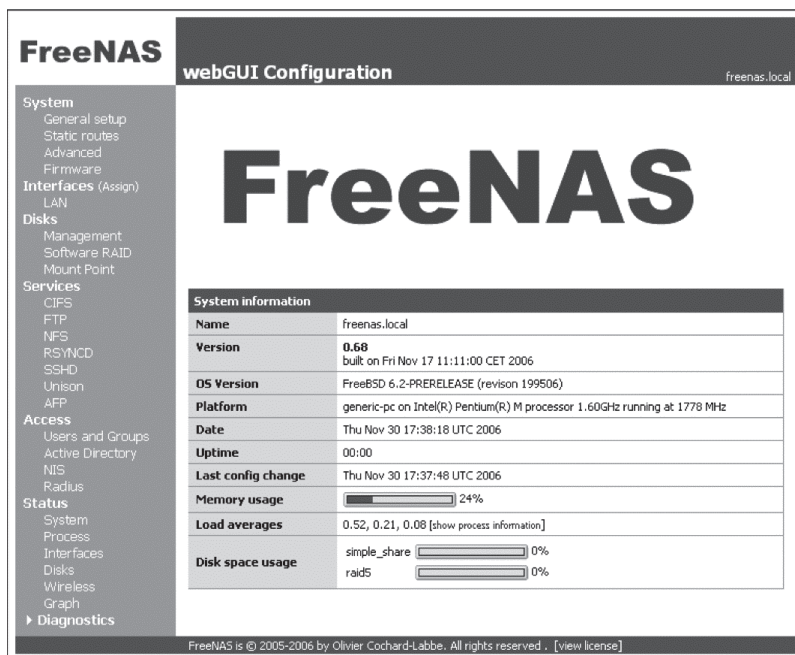
System NAS można zbudować za pomocą niemal dowolnego systemu operacyjnego. Jednak większość sprzedawanych obecnie urządzeń bazuje na dystrybucjach systemu Linux. Dostępnych jest wiele dystrybucji NAS typu open source, z których prawdopodobnie najbardziej znaną jest FreeNAS. Dystrybucja FreeNAS to wersja BSD (ang. *Berkeley Software Distribution*) o zmniejszonej liczbie funkcji i wielkości poniżej 32 MB. Istnieje możliwość skonfigurowania FreeNAS do uruchamiania bezpośrednio z płyty CD (tak zwany *Live CD*), która stanowi dysk startowy i zawiera cały system operacyjny wraz z wszystkimi wymaganymi funkcjami. Inne bezpłatne dystrybucje NAS to między innymi NASLite i Sun Open Storage.

Na rysunku 22.1 pokazano stronę domową FreeNAS, na której następuje konfiguracja urządzenia NAS. Zakres funkcji oferowanych przez FreeNAS jest standardem dla urządzeń NAS w tej kategorii.

Urządzenia NAS zwykle obsługują:

- ♦ szeroki zakres usług i protokołów, tak więc są podłączane do klientów w sieci heterogenicznej;

**Rysunek 22.1.**  
Strona domowa  
systemu FreeNAS



- ♦ utworzoną sprzętowo bądź programowo macierz RAID, powszechne są RAID 0, 1, 0+1 oraz 5;
- ♦ zaawansowane narzędzia dyskowe służące do wykonywania operacji takich jak formatowanie i partycjonowanie;
- ♦ integrację z Active Directory, jak również integrację NIS (ang. *Network Information Service*) w katalogach Unix (Linux);
- ♦ narzędzia zarządzania systemem, zwykle bazujące na przeglądarce internetowej;
- ♦ zarządzanie interfejsem sieciowym i protokołami (na przykład iSCSI) w celu uzyskania dostępu do współdzielonej pamięci masowej.

Microsoft ma bardzo dobry system operacyjny NAS — Windows Storage Server 2003 R2 — który jest używany w wielu systemach OEM (ang. *Original Equipment Manufactures*), na przykład jako Hewlett-Packard NAS.

Niemal każdy ważniejszy producent komputerowy ma w swojej ofercie system NAS. W przypadku firmy Dell jest to linia o nazwie PowerVault. Także HP oferuje urządzenia NAS — Media Vault, modele klasy średniej (seria ProLiant Storage Server), kilka modeli NAS można znaleźć w linii StorageWorks. Firma HP może pochwalić się ogromnym portfolio urządzeń NAS wskutek przejęcia firmy Compaq, która z kolei wcześniej przejęła Digital Equipment Corporation. Obie wymienione firmy miały ogromne oddziały zajmujące się pamięcią masową. Sun Microsystems to kolejny wielki producent urządzeń NAS — oferuje linię Sun StorageTek NAS. Przykłady małych, domowych urządzeń NAS to Snap Server, Kuro Box, TeraStation i LinkStation.

## NAS kontra SAN

Można się spotkać z pewnym zamieszaniem dotyczącym różnic między urządzeniami NAS i SAN. Te dwie kategorie urządzeń zostaną zilustrowane przez przedstawienie dwóch urządzeń pamięci masowej klasy przemysłowej, dostarczanych przez tego samego producenta, firmę EMC: Celerra, czyli serwer NAS, oraz serwer Symmetrix, który jest macierzą pamięci masowej klasy przemysłowej. Różnica między wymienionymi urządzeniami polega na sposobie transferu danych do klienta.

Urządzenie NAS to serwer pamięci masowej wraz z systemem operacyjnym i systemem plików. Kiedy klient wyświetla plik w urządzeniu NAS, używa do tego celu systemu plików tego urządzenia. Wybrany plik jest kopiowany do klienta tylko na żądanie. Z kolei macierze pamięci masowej mają niemal takie same komponenty jak NAS, ale kiedy dochodzi do wyświetlenia pliku z macierzy pamięci masowej, plik jest wyświetlany z systemu plików w systemie operacyjnym klienta. W trakcie żądania dostępu do pliku bądź katalogu w macierzy pamięci masowej tabela mapowania powoduje odwzorowanie tego żądania na zbiór bloków w określonym zestawie dysków. Wskazane bloki są kopiowane do systemu klienta, który następnie jest odpowiedzialny za zarządzanie plikiem lub plikami znajdującymi się w skopiowanych blokach.

Z punktu widzenia użytkownika różnica ta pozostaje subtelna — użytkownik widzi plik w katalogu w systemie plików i może zupełnie nie wiedzieć, gdzie ten plik tak naprawdę się znajduje. Jednak z perspektywy architektury systemu różnica między technologiami NAS i macierzami pamięci masowej SAN jest zasadnicza. Istnieją pewne urządzenia NAS zapewniające wysoką wydajność, ale ponieważ są obciążane koniecznością zarządzania plikami, to ich wydajność jest niższa od wydajności macierzy pamięci masowej, które są obciążane jedynie przez operacje bezpośredniego dostępu do dysku. Macierze pamięci masowej są szczególnie użyteczne w aplikacjach zajmujących się tworzeniem i przywracaniem kopii zapasowej. Nie oferują żadnych dodatkowych korzyści podczas przeprowadzania operacji na plikach. Na przykład kiedy aplikacja uzyskująca dostęp przez sieć pracuje na plikach, takich jak ogromne pliki strumieni wideo, filer NAS będzie doskonałym rozwiązaniem. W tabeli 22.1 wymieniono pewne istotne różnice między urządzeniami NAS i SAN.

## Sieciowe bufory plików

Jednym z zadań serwerów plików jest wysyłanie zawartości plików do różnych miejsc w sieci. To zadanie można zrealizować na wiele sposobów. Jeden z nich to użycie serwerów lustrzanych — replikacja całej zawartości do różnych lokalizacji. Takie rozwiązanie stanowi ogromne obciążenie dla sieci i może być niepraktyczne, kiedy zachodzi konieczność replikacji całego serwera lustrzanego. W tego typu sytuacjach firmy wcześniej tworzą serwery plików z odpowiednią zawartością, a dopiero później wysyłają te serwery do miejsca docelowego, w którym następuje implementacja.

Inne podejście polega na wykorzystaniu urządzeń NAS wraz ze specjalnym oprogramowaniem, które zamienia te filery na ogromne, inteligentne sieciowe bufory plików. Żądania dotyczące plików są kierowane do bufora, który pobiera je z lokalizacji pierwotnej i przechowuje; następne odwołanie do tych samych danych spowoduje pobranie ich z bufora. Niektóre z takich systemów posiadają wiele rozproszonych buforów w sieci wraz ze schematami replikacji. Buforowanie części danych w znaczny sposób podnosi efektywność dostępu do nich.

**Tabela 22.1.** NAS kontra SAN

Cecha	NAS	SAN
Typy sieci	TCP/IP, FDDI, ATM	Fibre Channel.
Protokoły	TCP/IP, NFS, CIFS, HTTP	Enkapsulowany SCSI.
Typy urządzeń	Dowolny system w sieci LAN, który może używać protokołów połączeniowych.	Serwer z SCSI Fibre Channel, który nawiązuje połączenie z oddzielną siecią SAN.
Transferowane dane	Pliki, metadane, bezpieczeństwo, tożsamość użytkownika oraz blokady plików. Identyfikacja plików jest przeprowadzana na podstawie ich położenia na dysku.	Dane blokowe są transferowane na podstawie numeru bloku na dysku.
Klienci	Dowolny system sieciowy, który może się połączyć za pomocą protokołu połączeniowego.	Współdzielenie plików następuje przez system plików połączonego systemu operacyjnego.
System plików	Zarządzany przez NAS.	Zarządzany przez system operacyjny podłączonego serwera.
Kopie zapasowe/lustrzane	Zwykle migawki bądź obrazy, które bazują na plikach, bardzo często przyrostowo przechwytyują zmiany.	Kopiowanie blok po bloku, woluminy są zduplikowane jako bezpośrednie kopie.

Wiele firm oferuje rozwiązania w zakresie buforów sieciowych. Informacje na temat tego rodzaju rozwiązań firmy Cisco można znaleźć na stronie [http://docwiki.cisco.com/wiki/Network\\_Caching\\_Technologies](http://docwiki.cisco.com/wiki/Network_Caching_Technologies). Z kolei firma NetApp opracowała linię sieciowych serwerów buforowania plików, ale rozwiązanie to zostało sprzedane firmie Blue Coat Systems Inc. (<http://www.bluecoat.com>), która oferuje te systemy pod nazwą ProxySG.

Rozwiązania dotyczące buforowania plików odgrywają ważną rolę w internecie. Jedną z firm specjalizujących się w tej technologii jest Akamai (<http://www.akamai.com>). Pojemność sieci buforowania brzegowego (ang. *edge-caching*) jest sprzedawana firmom, które wykorzystują ją w celu przyspieszenia działania serwisów WWW i aplikacji sieciowych. Przede wszystkim chodzi tutaj o dostarczanie informacji multimedialnych czy elektroniczną dystrybucję oprogramowania. Pojęcie *buforowania brzegowego* jest stosowane w celu opisanego dostarczania zawartości z serwera WWW do serwerów buforowania plików, które pod względem geograficznym znajdują się bliżej końcowego klienta. Buforowanie brzegowe jest zwykle sprzedawane w postaci usługi. Tak więc po przejściu na witrynę taką jak XYZ.com, stosującą rozwiązanie w zakresie buforowania, żądanie klienta będzie przekierowane do najbliższego serwera buforowania plików w systemie.

## Protokoły sieciowych systemów plików

Istnieje wiele różnych protokołów sieciowych systemów plików. Protokoły te są omawiane w rozdziale. Najważniejsze z nich to *Network File System* (NFS), *Andrew File System* (AFS) oraz *Server Message Block/Common Internet File System* (SMB/CIFS). Celem tych protokołów jest dostarczenie zdalnym odbiorcom dostępu do magazynów danych. Użytkownicy zdalni wykorzystujący te protokoły postrzegają dane, jakby były zlokalizowane w systemie klienta.

Zalety korzystania z sieciowych systemów plików w celu uzyskania dostępu do zdalnych zasobów są następujące:

- ♦ pamięć masowa może być skonsolidowana i chroniona;
- ♦ zmniejszają się potrzeby klienta w zakresie pamięci masowej;
- ♦ katalog domowy użytkownika może znajdować się w udziale sieciowym, a więc będzie dostępny w dowolnym miejscu sieci;
- ♦ urządzenia pamięci masowej takie jak napędy optyczne mogą być współdzielone przez sieć, co wiąże się z redukcją kosztów.

Protokoły sieciowych systemów plików są protokołami warstwy aplikacji, ale polegają one na oprogramowaniu warstwy prezentacji w zakresie zarządzania transferem danych oraz na zdalnych wywołaniach procedur w celu uzyskania dostępu do danych zdalnego systemu, co będzie omówione w kolejnym podrozdziale.

## Network File System

NFS (ang. *Network File System*) to protokół bardzo popularny w systemach Unix i Linux, który umożliwia komputerom uzyskanie dostępu do udziałów sieciowych. Służy do takiego samego celu jak CIFS/SMB. Protokół ten został opracowany w roku 1983 przez Sun Microsystems i powoli był przejmowany przez organizację IETF (ang. *Internet Engineering Task Force*), która jest odpowiedzialna za najnowszą, czyli czwartą wersję protokołu. Oprogramowanie Sun WebNFS, pozwalające, aby udziały sieciowe NFS były zarządzane i przeglądane za pomocą przeglądarki internetowej, zostało w ostatnim czasie uwolnione i udostępnione jako open source.

Silny wpływ na NFS miał system AFS (ang. *Andrew File System*), podobnie jak omówiony w dalszej części rozdziału system DFS (ang. *Distributed File System*). AFS to rozproszony system plików wykorzystujący protokół Kerberos do uwierzytelniania i autoryzacji oraz listy ACL (*Access Control List*) dla katalogów. System AFS został opracowany na uniwersytecie Carnegie Mellon University; w nazwie *Andrew File System* wykorzystano imię — od Andrew Carnegiego oraz Andrew Mellona. Inne wersje AFS to Transarc (firmy IBM), OpenAFS oraz Aria.

NFS jest uznawany za dojrzały protokół transmisji plików i jest obsługiwany przez niemal wszystkie sieciowe serwerowe systemy operacyjne, choć nie tak powszechnie używany jak CIFS/SMB lub *NetWare Core Protocol* (NCP). Obsługa NFS została zaimplementowana dla systemów Microsoft Windows, Novell Network, Mac OS oraz IBM AS/400.

Protokół NFS jest implementowany w warstwie siódmej (aplikacji) jako zestaw procedur do zarządzania plikami poprzez sieć, które noszą nazwę funkcji procedur i operacji NFS. W rzeczywistości cały protokół NFS rozciąga się od warstwy piątej do siódmej. NFS korzysta ze standardu XDR (ang. *External Data Representation*) do definiowania typów danych, które mogą być wymieniane poprzez sieć, operuje w warstwie prezentacji, pozwala na wymianę informacji pomiędzy systemami o różnych architekturach.



Wersje 1. i 2. protokołu NFS używały UDP zamiast TCP, który ma tendencje do czynienia systemu zawodnym, zwłaszcza w podsieciach i sieciach wewnętrznych. Wersja 3. i późniejsze używają TCP i są bardziej niezawodne.

Ostatni moduł na poziomie sesji to usługa zdalnego wywoływania procedur (ang. *Remote Procedure Call*, RPC). RPC stanowi komponent wszystkich usług plikowych. To te trzy wymienione subprotokoły razem tworzą system NFS. Usługa RPC została opracowana jako część NFS, ale stała się standardem używanym we wzajemnej komunikacji systemów w przemyśle komputerowym, w aplikacjach typu klient-serwer (na przykład platformy .NET), które działają przez TCP/IP. RPC stanowi część modułu NFS odpowiedzialną za przekazywanie wiadomości w obie strony oraz za utrzymanie stanu połączenia.

System NFS musi być skonfigurowany zarówno po stronie serwera, w którym udostępniane są pliki, jak i po stronie klienta. Wiele systemów NAS jest dostarczanych wraz z zainstalowanym NFS i po prostu pozwalają użytkownikowi na wskazanie nowego udziału jako udziału NFS. W systemie Windows Server 2008 kreator odpowiedzialny za utworzenie udziału pozwala na wybór dostępu NFS lub NTFS (bądź obu) w postaci pola wyboru. Kolejne kroki kreatora pozwalają na ustawienie uprawnień użytkownika i grupy. Po stronie klienta, w systemie Windows, konieczne jest dołączenie protokołu NFS do interfejsu sieciowego w celu umożliwienia klientowi dostępu do udziałów.

Instalacja NFS w systemie Ubuntu Linux wymaga ustawienia użytkowników, grup oraz instalacji NFS w serwerze:

1. Ustawienie uprawnień użytkownika i grupy.
2. Instalacja serwera NFS.
3. Utworzenie udziałów serwera, a następnie ich eksport do klienta.
4. Instalacja NFS u klienta.
5. Zamontowanie zdalnego katalogu u klienta — ręcznie lub automatycznie w trakcie uruchamiania systemu.
6. Przetestowanie dostępu do udziału NFS ze strony klienta.

Szczegółowe informacje dotyczące poszczególnych kroków można znaleźć na stronie Ubuntu SettingUpNFSTo pod adresem <https://help.ubuntu.com/community/SettingUpNFSTo>. Inny dokument przedstawiający ogólną procedurę instalacji NFS w systemie FreeBSD znajduje się na stronie <http://www.freebsd.org/doc/en/books/handbook/network-nfs.html>.

## Server Message Block/Common Internet File System

SMB (ang. *Server Message Block*) to protokół warstwy aplikacji (znacznie rzadziej protokół warstwy prezentacji) używany w celu współdzielenia plików, drukarek, portów szeregowych oraz innych zasobów sieciowych. Zasoby mogą również oferować dostęp do sieciowych interfejsów programowania aplikacji (API), nazwanych łączy (połączeń) oraz innych obiektów wirtualnych. SMB używa wielu różnych protokołów warstwy transportowej.

Protokół SMB stosuje mechanizm klient/żądanie serwera/odpowiedź w celu utworzenia połączenia między zasobami dwóch urządzeń. Klient SMB żąda zasobu, na przykład dostępu do pliku w serwerze SMB, a SMB nakłada blokadę na żądany zasób.

Protokół SMB został opracowany w roku 1985 przez IBM dla IBM PC. Microsoft oraz inne firmy przyłączyły się do projektu i stał się on standardem publicznym. SMB jest obsługiwany natywnie przez wszystkie wersje systemu Windows, począwszy od Windows NT. Poza tym protokół SMB był używany przez oprogramowanie LAN Manager. Niemal wszystkie sieciowe systemy operacyjne posiadają możliwość obsługi protokołu SMB poprzez wbudowane lub zewnętrzne rozwiązania.

Polecenie SMB jest wysyłane za pomocą NetBIOS poprzez TCP/IP (firma Microsoft określa to nazwą NBT) w celu utworzenia bezstanowego połączenia między komputerami. Polecenia zawierają pakiety kontroli sesji tworzące połączenie do zasobu sieciowego, pakiety dostępu do pliku, pozwalające na dostęp do udziału i przeprowadzanie operacji otwarcia, odczytu i zapisu. W zależności od zastosowanej polityki bezpieczeństwa mogą być również tworzone pliki i katalogi. Ponadto polecenia zawierają ogólne pakiety wiadomości. Kategoria wspomnianych ogólnych pakietów wiadomości obejmuje pakiety zawierające polecenia, które wysyłają dane do drukarek, wydają zapytania dotyczące stanu zasobu, zarządzają nazwanym połączeniem, MailSlots oraz innymi połączeniami wirtualnymi. SMB ma dwa tryby bezpieczeństwa — poziom udziału i poziom użytkownika, które nieco bardziej szczegółowo zostaną omówione w dalszej części rozdziału.

Microsoft, SCO Group oraz kilku innych producentów utworzyło CIFS (ang. *Common Internet File System*), czyli rozszerzoną wersję SMB. Istnieje wiele różnych implementacji SMB; CIFS jest uznawany za jeden z nich.

Wersja SMB/CIFS opracowana przez Microsoft dostarcza następujące usługi:

- ♦ negocjację protokołu między różnymi implementacjami SMB;
- ♦ blokady nakładane na zasobach sieciowych;
- ♦ blokowanie pliku i rekordu;
- ♦ system informowania o modyfikacji pliku lub katalogu;
- ♦ uwierzytelnianie i autoryzację podczas dostępu do pliku, katalogu i udziału;
- ♦ rozszerzoną obsługę atrybutów pliku;
- ♦ obsługę Unicode;
- ♦ drukowanie sieciowe;
- ♦ przeglądanie sieci i ogłaszanie usług.

SMB/CIFS to obecnie jeden z dwóch ważnych sieciowych systemów plików. Drugim systemem pozostaje NFS. Jako przykład serwera CIFS w kolejnym podrozdziale przedstawiony będzie serwer plików Samba.

## Samba

Samba to najczęściej używane oprogramowanie do współdzielenia plików, a także podstawa szerokiej gamy produktów. Sambę można zainstalować w wybranym systemie operacyjnym; jej udziały można przeglądać przez sieć z poziomu wielu różnych systemów operacyjnych. Samba (<http://www.samba.org>) to oprogramowanie typu open source. Nazwa pochodzi od protokołu SMB (ang. *Server Message Block*) — to ten sam protokół, który jest używany przez sieciowy system plików Windows. Samba to jeden z najlepszych przykładów serwera CIFS/SMB.

Serwer Samba może dołączyć do domeny Windows jako serwer plików bądź serwer wydruku, a nawet może być zainstalowany w kontrolerze domeny w celu zapewnienia usług plikowych tej domenie. CIFS/SMB jest natywnym protokołem transferu plików Samby i Windows. CIFS (ang. *Common Internet File System*) to rozszerzona wersja SMB używana przez Windows i OS/2. Jako aplikacja Windows Samba obsługuje usługi domeny Windows. Umożliwia więc zalogowanie do Active Directory i funkcjonowanie w charakterze elementu składowego domeny, w pełni zgodnego z wszystkimi protokołami bezpieczeństwa Windows.

Kiedy klient Windows nawiązuje połączenie z Sambą, może to zrobić, używając protokołu NetBIOS przez TCP (NBT). W katalogu sieciowym komputer z Sambą pojawia się w taki sam sposób jak każdy inny system Windows. Samba obsługuje MSRPC (ang. *Microsoft Remote Procedure Call*), co powoduje, że staje się zgodna z aplikacjami obsługującymi sieć i zbudowanymi za pomocą platformy .NET. W celu zarządzania serwerem Samba z poziomu zdalnej przeglądarki internetowej można zainstalować narzędzie SWAT (ang. *Samba Web Administration Tool*), które jest dostarczane wraz z Sambą.

Ogólnie rzecz biorąc, trudno jest znaleźć system operacyjny, w którym nie można uruchomić serwera Samby. Wersja 3. Samby działa nie tylko w Windows, ale również w różnych systemach Unix i Linux. Ponadto istnieją wersje dla Sun Solaris, Netware, IBM OS/2, IBM AX, IBM System 390, OpenVMS, Amiga OS i Mac OS X. Wiele systemów Linux zawiera oprogramowanie Samba w dystrybucji, instaluje je jako podstawową część oprogramowania lub ma wersję gotową do pobrania i instalacji. Protokół SMB jest powszechnie używany, ale w przypadku potrzeby wykorzystania CIFS w niektórych wersjach systemów Linux i Unix może wystąpić konieczność instalacji oprogramowania firm trzecich, zapewniającego obsługę CIFS. Istnieje możliwość instalacji narzędzia `smbclient` jako części pakietu Samba, które pozwoli klientom Unix na nawiązywanie połączenia z udziałami Samby, wysyłanie i odbieranie plików oraz pracę ze współdzielonymi drukarkami.

Jeśli chodzi o instalację Samby w systemie Windows, plikowe udziały Samby będą zachowywały się jak lokalne dyski twarde, nawet w przypadku zdalnych systemów. Po instalacji Samby w systemie Unix i połączeniu tego systemu z domeną Windows udziały utworzone na podstawie katalogów Unix będą dostępne w sieci Windows tak, jakby były katalogami standardowymi. Aby udziały Unix pojawiły się w Windows, trzeba je w pierwszej kolejności zamontować. Do tego celu można wykorzystać narzędzie `smbclient`.

Podczas instalacji Samby w systemach z rodziny Linux systemy te powodują sformatowanie partycji Samby w systemie plików SMB (`smbfs`). System `smbfs` wywodzi się z kodu bazowego Samby, ale nie jest obsługiwany przez [Samba.org](http://www.samba.org), choć znajduje się w dystrybucjach Samby dla systemów Linux. Linux ma możliwość zamontowania bezpośrednio w katalogu

udziału Samby, który używa formatu smbfs. Podczas przeglądania plikowego udziału SMB katalog ten przedstawia się jak każdy inny lokalny katalog Linux i daje użytkownikowi pełne uprawnienia dostępu.

## Bezpieczeństwo Samby

Pakiet programów Samby implementuje wszystkie cztery aspekty usług CIFS, o których wspomniano w poprzednim podrozdziale. Demon SMB (`smbd`) jest odpowiedzialny za wszystkie funkcje obsługi plików i wydruku, jak również za uwierzytelnianie i autoryzację wymaganą przez tryb udziału albo użytkownika. Różnica między tymi dwoma wymienionymi trybami polega na tym, że w trybie udziału pojedyncze hasło umożliwia uzyskanie dostępu do udziału każdemu autoryzowanemu użytkownikowi. Natomiast w trybie użytkownika każdy użytkownik ma swoje własne konto; aby uzyskać dostęp do udziału, musi więc podać nazwę użytkownika i hasło. Konta użytkowników są tworzone i zarządzane przez administratora systemu Samby. Samba może również współdziałać z Active Directory (AD) lub działać w trybie serwera, co zwiększa liczbę dostępnych trybów bezpieczeństwa w wersji 3. do czterech.

Kiedy Samba znajduje się w domenie Windows, dane uwierzytelniające pobiera z usług domeny Windows bądź z Active Directory. Samba 2 to pierwsza wersja zapewniająca zgodność z domeną Windows. Począwszy od wersji 3., serwer Samby może funkcjonować jako pełny kontroler domeny. Serwery domeny Samby mogą używać mechanizmu `tbdscam` jako silnika systemu uwierzytelniania, ale wtedy mogą być użyte jako samodzielne PDC tylko w małych sieciach. W przypadku dużych sieci silnik uwierzytelniania musi dostarczać LDAP, na przykład OpenLDAP. Jak już wcześniej wspomniano, istnieje możliwość bezpośredniej instalacji Samby w serwerze Windows PDC.

Samba może być zatem umieszczona w jednym z następujących trybów bezpieczeństwa:

- ♦ **Tryb użytkownika.** Dostęp do Samby przez podanie nazwy użytkownika i hasła.
- ♦ **Tryb udziału.** Dostęp do danego udziału Samby przez podanie nazwy użytkownika i hasła.
- ♦ **Bezpieczeństwo Active Directory.** Uwierzytelnianie jest przeprowadzane przez kontroler domeny Windows.
- ♦ **Tryb serwera.** To przestarzała funkcja poprzedniej wersji Samby. W tym trybie system klienta loguje się do serwera Samby w taki sposób, jakby serwer był w trybie użytkownika.

## Określanie nazw w serwerze Samba i przeglądanie udziałów

Druga podstawowa aplikacja to program `nmbd` obsługujący określanie nazw i przeglądanie udziałów sieciowych. Określanie nazw i przeglądanie udziałów sieciowych może być technologią rozgłaszania wykorzystującą mechanizm żądanie-odpowiedź albo systemem punkt-punkt typu klient-serwer. W tym pierwszym przypadku nadawca buduje listę zasobów sieciowych, natomiast w drugim serwer przekazuje klientowi wcześniej zbudowaną listę zasobów. Microsoft *Windows Internet Name Service* (WINS), czyli wersja serwera nazw *NetBIOS Name Server* (NBNS) używanego w innych systemach operacyjnych, buduje małą

bazę danych dostępnych systemów po wykryciu klienta WINS. Kiedy wymagane jest określenie nazwy, zapytanie zostaje wysłane do bazy danych serwera WINS, który pobiera nazwę czytelną dla człowieka i zwraca adres IP. Klient usługi nazw NetBIOS (czyli `nmblookup`) dołączony do dystrybucji Samby może być wykorzystywany w celu lokalizacji nazw NetBIOS, określania ich adresów IP oraz pobierania list zasobów.

Serwery NBNS mogą budować listy przeglądania obejmujące podsieci. W przeciwieństwie do DNS listy te są dynamiczne. Dostęp do list przeglądania NBNS nie jest chroniony na podstawie systemu. Dlatego też jeżeli użytkownik może uzyskać dostęp do określonej sieci, to może przeglądać wszystkie znajdujące się w niej zasoby.

Zachowanie NBNS można porównać do serwera DNS, gdzie rekordy są dodawane do bazy danych mniej lub bardziej trwale, a najczęściej wykonywane zapytanie do DNS ma na celu określenie nazwy dla danego adresu IP. Oczywiście, istnieją odwrotne zapytania DNS, ale DNS ma problemy dotyczące niewystarczającej częstotliwości uaktualnień, które mogą świadczyć o dostępności bądź istnieniu danego systemu. W przypadku serwera NBNS takiego jak Samba listy przeglądania są dynamiczne, a systemy były lub są zarejestrowane i dostępne online. Jednak ponieważ jest to system luźniejszy niż DNS, mogą pojawiać się pewne konflikty.

NBNS utrzymuje również listy przeglądania zasobów sieciowych, włączając w to udziały plików i drukarek przez wybór LBM (ang. *Local Browse Manager*) obsługującego listę nazw NetBIOS. Kiedy klient otwiera katalog sieciowy, lista przeglądania jest pobierana z LMB (ang. *Local Master Browser*), a następnie jest wykorzystywana do wypełnienia katalogu.

Domeny Windows tworzą DMB (ang. *Domain Master Browser*) partycypujący w tworzeniu listy przeglądania zawierającej resztę domen, które pozostają w zaufanej relacji z pierwszą domeną. Jeżeli w sieci znajduje się LMB, to będzie synchronizował listę przeglądania wraz z DMB. Każdy serwer w domenie, na przykład serwer Samby, dzięki replikacji ostatecznie uzyska tę listę przeglądania. Jednak proces replikacji może być powolny, w zależności od rodzaju połączenia sieciowego oraz liczby urządzeń.

## Samba w Ubuntu

Samba może być zainstalowana w systemie Ubuntu jako serwer plików i wydruku. Ewentualnie może być dostępna jako klient, gdy zainstalowany jest system plików `smbfs`.

W celu instalacji Samby należy wykonać poniższe kroki:

1. Otworzyć okno terminalu i wydać polecenie `sudo aptitude install samba`.

Podać hasło użytkownika z uprawnieniami administratora i nacisnąć klawisz *Enter*. Samba zostanie zainstalowana w systemie. Aby uzyskać dostęp do udziału Samby w sieci, nie ma konieczności instalacji Samby w systemie Ubuntu. System Ubuntu jest skonfigurowany do nawiązywania połączenia z serwerem Samby za pomocą narzędzia `smbclient`. Wymienione narzędzie oferuje funkcje wiersza poleceń podobne do FTP pod tym względem, że pozwalają na nawigację po udziale Samby za pomocą poleceń `cd`, `ls`, `get` i `put`.

Jeżeli zachodzi potrzeba podłączenia zdalnego systemu plików do lokalnego systemu plików z wykorzystaniem protokołu smb, musimy dla polecenia `mount` określić typ systemu jako `smbfs`. W tym celu trzeba zainstalować oprogramowanie `smbfs` w następujący sposób:

1. Otworzyć okno terminalu i wydać polecenie `sudo aptitude install smbfs`.
2. Podać hasło użytkownika z uprawnieniami administratora i nacisnąć klawisz *Enter*.

Po instalacji Samba tworzy publicznie dostępne udziały. Oznacza to, że w systemie Ubuntu można je przeglądać w katalogu *Siec* i nie jest do tego potrzebne żadne hasło. Jeżeli istnieje potrzeba zabezpieczenia udziałów Samby, to funkcję tę można włączyć w pliku konfiguracyjnym Samby o nazwie *smb.conf*.

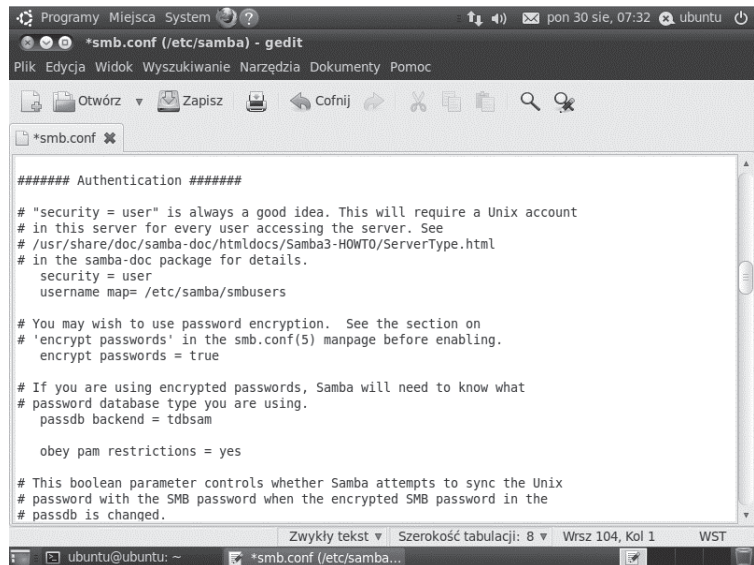
W celu włączenia bezpieczeństwa i utworzenia użytkowników należy wykonać poniższe kroki:

1. Wyświetlić plik *smb.conf* i przeprowadzić jego edycję przez wydanie w oknie terminalu polecenia `sudo gedit /etc/samba/smb.conf`. Oczywiście zamiast `gedit` można użyć innego edytora tekstowego.
2. Wiersz `# security = user` należy zamienić na dwa poniższe:

```
security = user
username map = /etc/samba/smbusers
```

Samba sprawdzi plik *smbusers* w celu pobrania kont użytkowników. Na rysunku 22.2 pokazano plik *smb.conf* po przeprowadzeniu zmian wskazanych w kroku 2.

**Rysunek 22.2.**  
Plik *smb.conf*,  
w którym włączono  
bezpieczeństwo  
użytkowników



3. Ostatni krok to zapisanie zmian w pliku *smb.conf* i zamknięcie edytora tekstu.

Na tym etapie w systemie znajduje się zainstalowany serwer Samby wraz z włączoną autoryzacją użytkowników. W celu uzyskania dostępu do udziału Samby trzeba utworzyć jej użytkowników i dodać ich do pliku *smbusers*. Procedura przedstawia się następująco:

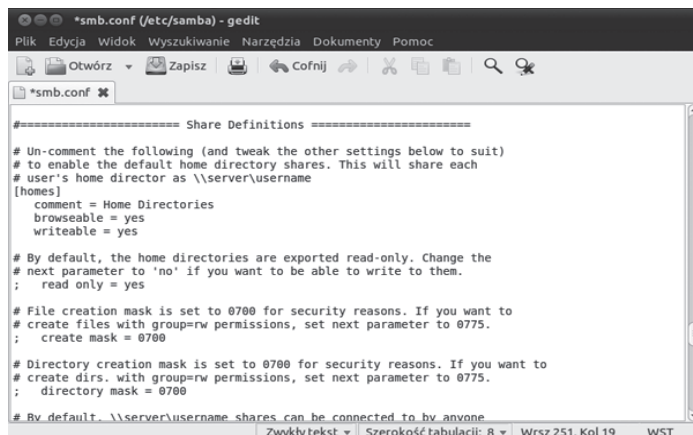
1. Pierwszy krok to wyświetlenie okna terminalu i utworzenie nowego użytkownika za pomocą programu `smbpasswd` przez wydanie polecenia `sudo smbpasswd -a <nazwa_użytkownika>`.
2. Plik `smbusers` należy wyświetlić za pomocą polecenia `sudo gedit /etc/samba/smbusers`.
3. Należy dodać wiersz `<nazwa_użytkownika_ubuntu> = <nazwa_użytkownika_samby>`, a następnie zapisać i zamknąć plik.
4. W oknie terminalu trzeba wydać polecenie `sudo gedit /etc/samba/smb.conf`.
5. Aby utworzyć katalogi domowe (udziały) użytkowników Samby, należy w sekcji *Share Definitions* zmienić tekst i dodać następujące wiersze:

```
[homes]
comment = Home Directories
browseable = yes
writeable = yes
```

Plik `smb.conf` powinien wyglądać podobnie jak pokazany na rysunku 22.3.

### Rysunek 22.3.

Plik `smb.conf`,  
w którym włączono  
katalogi domowe dla  
użytkowników Samby



6. Ostatni krok to zapisanie zmian w pliku i zamknięcie edytora tekstu.

Na koniec musimy uruchomić ponownie Sambę lub Ubuntu. Na tym etapie powinno być możliwe przeglądanie w Windows udziałów użytkowników utworzonych w Ubuntu. Ścieżka dostępu do udziału ma postać `\\<nazwa_komputera_macierzystego>\<nazwa_użytkownika>`.

## Distributed File System

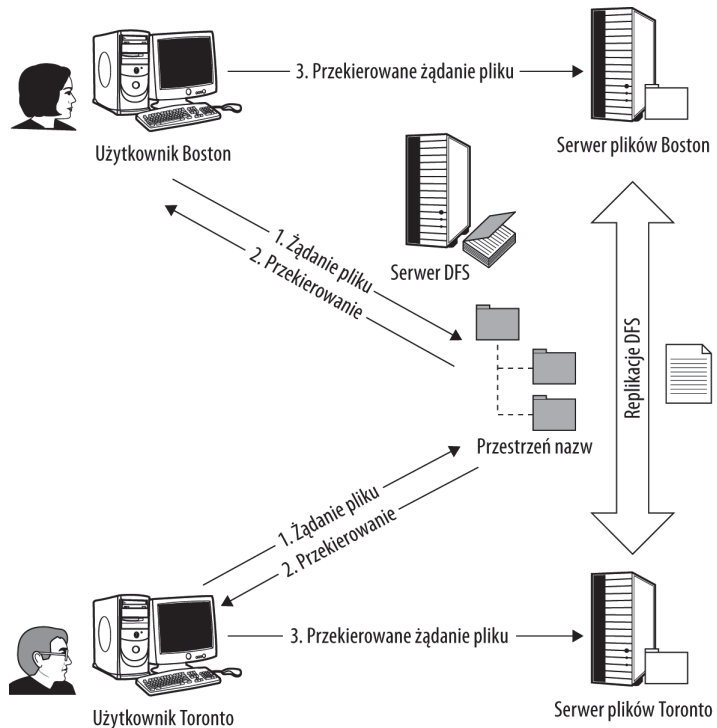
DFS (ang. *Distributed File System*) to architektura klient-serwer, która może zmienić plikowe udziały SMB znajdujące się w wielu systemach rozproszonych w sieci na rozproszony system plików. Ogólnie rzecz biorąc, klient ma dostęp jedynie do części całego systemu plików. Kiedy klient żąda uzyskania dostępu do udziału w DFS, to serwer DFS może pokierować użytkownika do danego udziału w taki sposób, że ten udział pojawia się tak, jakby był zasobem lokalnym.

DFS jest szczególnie użyteczny w ogromnych, geograficznie rozproszonych sieciach, ponieważ kopie udziałów sieciowych mogą być umieszczone w całej sieci, co powoduje poprawę wydajności działania oraz zmniejsza wewnętrzny ruch sieciowy. Węzły są zwykle umieszczane w sieciach LAN. Klient będzie więc mógł być przekierowany do kopii danych znajdującej się najbliżej. Rozproszone systemy plików są niezwykle cenne w środowiskach biurowych. Wynika to nie tylko z oferowanych zalet na polu wydajności, ale również z tego, że jeśli którykolwiek z pozostałych węzłów DFS będzie niedostępny, węzeł lokalny nadal będzie działał, nie tracąc przy tym żadnych danych.

Użycie DFS w sieci wewnętrznej pokazano na rysunku 22.4.

### Rysunek 22.4.

System DFS kieruje użytkownika do lokalnej kopii replikowanych danych



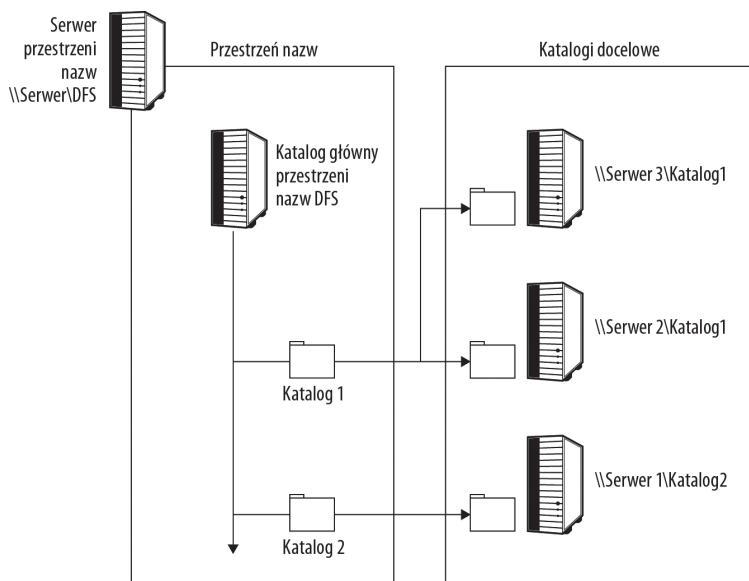
Konceptcja rozproszonego magazynu danych dzieli z DFS pewne cechy charakterystyczne, ale jest zupełnie inną technologią. Rozproszony magazyn danych tworzy grupę pamięci masowej ze zbioru równorzędnych węzłów sieciowych. Dane użytkownika są następnie kopiowane między węzłami.

Firma Microsoft przez długi czas wspierała DFS (wersja ta czasami jest nazywana Dfs). DFS może działać na dowolnej wersji systemu Windows Server, NT i nowszych. Katalog główny DFS może być umieszczony w Windows NT 4.0 oraz Windows 2000 Server, jak również w serwerze Samby. Nowsze wersje Windows — Windows Server 2003, 2008 Enterprise i Datacenter — mogą na tym samym serwerze obsługiwać wiele różnych katalogów głównych DFS. Kiedy DFS stanowi część domeny, jego informacje są przechowywane w Active Directory i umieszczone w kontrolerze domeny. Microsoft DFS zawiera funkcje replikacji i synchronizacji, które przekazują zmiany pomiędzy serwerami DFS, używając usługi FRS (ang. *Microsoft File Replication Service*).

Kluczem do zrozumienia DFS jest przestrzeń nazw utrzymywana przez serwer DFS. Wspomniana przestrzeń nazw mapuje katalogi fizyczne umieszczone w jednym lub wielu miejscach. Mapa przestrzeni nazw DFS jest listą katalogów do listy katalogów docelowych, określonych przez ich ścieżkę dostępu UNC (ang. *Uniform Naming Convention*). Elementy docelowe mają nadane priorytety określające kolejność replikacji katalogów. Jeżeli klient nie będzie w stanie połączyć się z katalogiem w przestrzeni nazw, to możliwe będzie utworzenie w innym serwerze katalogu odpornego na awarie. DFS nie wymaga utworzenia mapowanej przestrzeni nazw, ale funkcja ta powoduje, że DFS jest systemem o znacznie potężniejszych możliwościach.

Na rysunku 22.5 pokazano mapowanie przestrzeni nazw wraz z jej hierarchią.

**Rysunek 22.5.**  
Mapowanie przestrzeni  
nazw i hierarchia



Każdy obiekt w przestrzeni nazw jest określony za pomocą ścieżki dostępu UNC. Replikacja może zająć ogromną ilość przepustowości, więc szczególną uwagę trzeba skierować na wydajność replikacji w sieciach z połączeniami o małej przepustowości. Z tego powodu firmy czasem umieszczają nowy serwer DFS na końcu połączenia o małej przepustowości, na przykład w biurze. Warto utworzyć grupy replikacji, tak aby większość ruchu sieciowego związanego z operacjami replikacji odbywała się w połączeniach o dużej przepustowości.

Istnieje możliwość wyboru serwera DFS jako samodzielnego lub bazującego na domenie. W tym pierwszym przypadku system plików DFS jest dostępny tylko w tym systemie, w którym został zainstalowany. Samodzielny DFS nie bierze udziału w schemacie replikacji i synchronizacji, w którym uczestniczą serwery DFS bazujące na domenie.

Na przestrzeni lat powstało wiele rozproszonych systemów plików; omówiony we wcześniejszym podrozdziale CIFS/SMB to jeden z najczęściej używanych. Do innych ważnych przedstawicieli tej technologii można zaliczyć:

- ♦ Andrew File System (AFS),
- ♦ Apple Filing Protocol (AFP),

- ♦ DCE Distributed File System (DCE/DFS),
- ♦ Netware Core Protocol (NCP),
- ♦ Network File System (NFS),
- ♦ Coda,
- ♦ InterMezzo.



Wydano już wiele rozproszonych systemów plików. Niektóre systemy o wysokiej wydajności są rozproszonymi równoległymi systemami plików, umieszczającymi dane na różnych serwerach w klastrze bądź macierzy. Część z tych systemów została zbudowana w taki sposób, aby zaoferować pewną odporność na awarie. Omówienie ich wykracza poza zakres tematyczny rozdziału. Więcej informacji na temat systemów plików — rozproszonych, dyskowych, pamięciowych, zorientowanych pod kątem rekordów (bazy danych), współdzielonych dyskowych systemów plików, równorzędnych systemów plików i wszelkich innych można znaleźć w Wikipedii, na stronie *List of File Systems*, pod adresem [http://en.wikipedia.org/wiki/List\\_of\\_file\\_systems](http://en.wikipedia.org/wiki/List_of_file_systems).

Niestety, DFS jest wykorzystywany w niewielkim stopniu, ale technologię tę warto poznać, jeżeli sieć jest na tyle duża, aby implementacja DFS przyniosła pożytek.

## Podsumowanie

W rozdziale omówiono wiele różnych technologii udostępniania plików w sieci. Chociaż stosowane są serwery plików ogólnego przeznaczenia, to specjalnie zoptymalizowane serwery plików, nazywane *Network Attached Storage*, stanowią znacznie bardziej eleganckie rozwiązania.

Do tworzenia udziałów sieciowych i ich udostępniania klientom używane są różne usługi plikowe. NFS to powszechnie stosowany protokół w systemach Unix, ale protokół SMB/CIFS jest używany znacznie częściej. SMB to natywny protokół Samby, serwera plików typu open source. W rozdziale przedstawiono możliwości Samby oraz sposób instalacji serwera w systemie Ubuntu Linux.

Inną technologią rozprowadzania plików w sieci jest DFS. Rozproszony system plików pozwala na umieszczenie w sieci wielu kopii systemu plików, a następnie używanie serwera DFS w celu pokierowania użytkownika do najbliższej dostępnej kopii danych.

W następnym rozdziale omówione zostaną usługi sieciowe, serwer WWW i protokół HTTP.



# Rozdział 23.

## Usługi sieciowe

### W tym rozdziale:

- ♦ Protokół HyperText Transfer Protocol (HTTP)
- ♦ Mechanizm żądanie-odpowiedź protokołu HTTP
- ♦ Różne technologie używane do tworzenia usług sieciowych (ang. *Web Service*)
- ♦ Architektura zorientowana na usługi (SOA, ang. *Service Oriented Architecture*)

W rozdziale zostaną przedstawione podstawy tworzenia i opracowywania usług sieciowych. Wraz z coraz większą liczbą aplikacji przenoszonych do internetu usługi sieciowe zyskały większe znaczenie.

HTTP (ang. *HyperText Transfer Protocol*) to protokół warstwy aplikacji wykorzystywany przez przeglądarki internetowe do przekazywania informacji. HTTP używa żądań w postaci zwykłego tekstu z agenta użytkownika (klienta) do serwera w celu uzyskania dostępu do określonego zasobu. Jeżeli żądanie było poprawne, to serwer udziela odpowiedzi wraz z właściwym zasobem w odpowiednim formacie. Aby ułatwić negocjacje i wykonywanie żądań, zdefiniowano zestaw kodów stanu. Z tego rozdziału Czytelnik dowie się, w jaki sposób są tworzone i wykonywane wiadomości HTTP.

Protokół HTTP może przekazywać informacje, używając różnych wersji języka HTML, który po przetworzeniu przez przeglądarkę internetową opisuje sposób utworzenia i sformatowania strony internetowej. Strony internetowe mogą zawierać treść statyczną bądź dynamiczną. Utworzenie i kontrolowanie w sieci treści dynamicznej jest możliwe na wiele różnych sposobów — skrypty działające po stronie serwera lub klienta oraz skrypty CGI to jedne z wielu możliwości.

Usługa sieciowa jest aplikacją pośredniczącą między klientem i serwerem. W rozdziale zostanie przedstawiony przykład implementacji usługi sieciowej z użyciem protokołu komunikacyjnego SOAP, pozwalającego na wymianę wiadomości między żądającym usługi sieciowej i jej dostawcą. W usłudze sieciowej transakcje są realizowane za pomocą usługi pośrednika działającego w innym systemie. Zadaniem wspomnianej usługi pośrednika jest wykrywanie usług sieciowych oraz udzielanie informacji na temat ich możliwości, jak również wymiana informacji między klientem i serwerem.

Architektura oparta na usługach (ang. *Service Oriented Architecture*, SOA) to platforma służąca do budowania aplikacji rozproszonych. Zadaniem architektury SOA jest umożliwienie klientowi tworzenia aplikacji i zarządzania nimi za pomocą usług sieciowych działających w innych systemach. Podczas tworzenia architektury opartej na usługach zastosowanie ma wiele technologii i standardów, które zostaną przedstawione w rozdziale.

## Protokół HyperText Transfer Protocol

Protokół HTTP (ang. *HyperText Transfer Protocol*) jest natywnym protokołem warstwy aplikacji używanym przez serwery WWW oraz klienty w postaci przeglądarek internetowych do wymiany informacji między nimi. HTTP używa mechanizmu żądanie-odpowiedź. Żądanie składa się z tekstu ASCII zawierającego jedną z metod, natomiast odpowiedź jest sformułowana w postaci tekstu sformatowanego podobnie jak w przypadku typu MIME w poczcie elektronicznej. MIME (ang. *Multipurpose Internet Mail Extensions*) to standard formatowania tekstu pozwalający klientom poczty elektronicznej na wysyłanie znaków innych niż znajdujące się w zestawie ASCII, dołączanie plików do wiadomości, dzielenie wiadomości na sekcje oraz stosowanie nagłówków zawierających znaki inne niż ASCII. Obecnie niemal wszystkie wiadomości e-mail wysyłane w internecie są wysyłane przez serwer SMTP jako typ MIME.

HTTP to protokół bezstanowy; informacje wymagane do przetworzenia żądań i odpowiedzi znajdują się w samych wiadomościach. W ten sposób zarówno serwer, jak i klient zostają odciążone od konieczności przechowywania informacji użytkownika i zarządzania nimi. Jednak ponieważ HTTP jest protokołem bezstwowym, to jeżeli witryna internetowa musi zarządzać danymi użytkownika w celu dostosowania się do jego potrzeb, to jest zmuszona do użycia innych rozwiązań. Powszechnie stosowanym rozwiązaniem jest tworzenie i modyfikowanie plików cookies, uwierzytelnianie loginów dla sesji oraz obsługa sesji po stronie serwera.

HTTP jest standardem IETF (ang. *Internet Engineering Task Force*); najnowsza wersja standardu to HTTP 1.1, zgodnie z definicją w dokumencie RFC 2616 (<http://tools.ietf.org/html/rfc2616>). Prace nad tym protokołem są nadzorowane przez konsorcjum World Wide Web Consortium (<http://www.w3.org>), które jest odpowiedzialne za zestaw protokołów internetowych (w tym także HTTP). Wprawdzie HTTP jest używany niemal wyłącznie w sieciach TCP/IP, specyfikacja protokołu nie wymaga stosowania TCP jako metody transportu. Jedynym wymaganiem jest, aby dostarczane dane były sprawdzone pod kątem ich spójności.

W typowej sesji HTTP klient (agent użytkownika) wysyła żądanie do serwera docelowego, który nasłuchuje na porcie przychodzącym numer 80. Adres docelowy jest formowany w postaci znanego już adresu URL (ang. *Uniform Resource Locator*):

`http://helion.pl`

Przykładami tego rodzaju formatu są adresy <http://www.w3.org/2002/03/tutorials> oraz <http://192.168.1.1/index.html>; oba prowadzą do określonego zasobu. W pierwszym przypadku adres URL prowadzi do katalogu o nazwie *tutorials*, podczas gdy w drugim prowadzi do pliku o nazwie *index.html*. Zasób jest unikalnie identyfikowany, ponieważ w prze-

strzeni nazw TCP/IP serwer musi mieć unikalne wpisy. Ponadto zasób musi być również unikalnie identyfikowany w systemie plików serwera. Po naciśnięciu klawisza *Enter* bądź kliknięciu przycisku *Odśwież* w przeglądarce internetowej żądanie spowoduje dostarczenie przez serwer danego zasobu, który następnie będzie wyświetlony w przeglądarce.



Nazwa URN (ang. *Uniform Resource Name*) jest powiązana z koncepcją, w której zasób jest identyfikowany poprzez jego położenie w przestrzeni nazw — na przykład numer książki w katalogu biblioteki. Adresy URL i URN są identyfikatorami zasobów i zaliczają się do ogólnej kategorii systemu identyfikacji o nazwie URI (ang. *Uniform Resource Identifier*).

## Żądania HTTP

Żądanie HTTP składa się z następujących elementów:

1. **Nagłówek.** Wiersz nagłówka zawiera żądanie informacji bądź ustanowienia warunku. Wiersze nagłówka są opcjonalne, ale w protokole HTTP 1 wymagany jest nagłówek *Host*.

Przykładami mogą być: *Accept: text/plain*, *Host: www.whitehouse.gov* lub *Range: bytes=200-500*. Pierwszy przykład ustala rodzaj treści jako zwykły tekst, drugi podaje nazwę domeny serwera, natomiast trzeci wymaga jedynie podania pewnego zakresu danych żadanego zasobu.

2. **Wiersz żądania.** Wiersz żądania zawiera metodę (zob. w dalszej części rozdziału) i żądany zasób, względem którego będzie podjęte wskazane działanie, a także pole wersji protokołu.

Na przykład polecenie *GET / HTTP/1.1* spowoduje zwrócenie strony domyślnej (najczęściej *index.html*) danej domeny, o ile witryna internetowa nie ustawiła w kliencie pliku cookie, który spowoduje zwrócenie zupełnie innej strony.

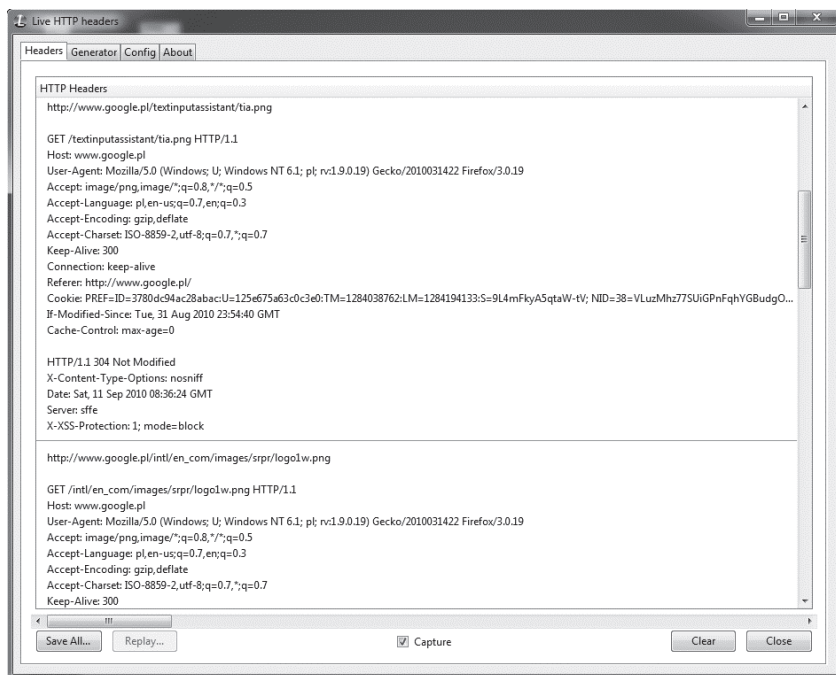
3. **Puste wiersze** zdefiniowane jako znaki CR (ang. *Carriage Return*), po których znajdują się znaki LF (ang. *Line Feed*). Puste wiersze są wymagane w celu oddzielenia nagłówka i wiersza żądania od pozostałych elementów.

W zestawie znaków ASCII symbol CR to trzynasty znak (ósemkowo 015, szesnastkowo 0D), natomiast LR (znak nowego wiersza) to dziesiąty znak (ósemkowo 012, szesnastkowo 0A) 127-znakowego zbioru ASCII. W większości edytorów znaki te można wprowadzić, naciskając klawisz *Enter* (CR) i *Shift+Enter* (LR).

4. **Część główna (opcjonalna)** to informacje zwrócone przez serwer. Jeżeli żądanie dotyczyło strony internetowej, to kod HTML w odpowiedzi zostanie odesłany przeglądarce internetowej właśnie jako część główna odpowiedzi.

Na rysunku 23.1 pokazano żądanie HTTP dla strony *www.google.pl* wyświetlone przez rozszerzenie Live HTTP Headers w przeglądarce internetowej Mozilla Firefox. Serwer udzielił odpowiedzi wraz z kodem stanu 304 („niezmodyfikowano”). Następnie rozpoczyna się pobieranie kolejnego wymaganego zasobu (logo Google). Inne narzędzie zalecane do wyświetlania żądań HTTP to Fiddler — narzędzie niezależne od przeglądarki internetowej, które można znaleźć na stronie <http://www.fiddler2.com/fiddler2/>.

**Rysunek 23.1.**  
*Rozszerzenie Live  
 HTTP Headers  
 w przeglądarce  
 Mozilla Firefox  
 pokazuje skład  
 wiadomości HTTP  
 będącej żądaniem  
 strony głównej  
 Google*



Warto zwrócić uwagę na nagłówek Keep-Alive wraz z wartością 300 sekund. Ten parametr został dodany w HTTP 1.1 w celu utrzymania trwałych połączeń. W poprzednich wersjach HTTP połączenie było zamykane po spełnieniu żądania. Ponieważ HTTP 1.1 może polegać na trwałych połączeniach, ma możliwość przekazywania informacji przy użyciu metod transferu w częściach. Normalnie dane stanowiące odpowiedź HTTP są wysyłane w postaci pojedynczego bloku wraz z długością bloku wskazywaną przez pole nagłówka Content-Length. Jednak w przypadku transferu w częściach zakodowane dane mogą być podzielone i wysłane w postaci skompresowanych fragmentów. Podział na części pozwala przeprowadzić kompresję w locie zamiast przed wysłaniem danych, co przyspiesza cały proces.

Drugie usprawnienie polega na udostępnieniu przez nagłówek Keep-Alive mechanizmu HTTP Pipelining. Pozwala on na wysłanie serii żądań HTTP bez konieczności oczekiwania na odpowiedź na każde kolejne żądanie. Stosowanie mechanizmu HTTP Pipelining skutkuje usprawnieniem w postaci znacznego skrócenia czasu, jakiego przeglądarka internetowa potrzebuje na wyświetlenie strony, zwłaszcza w przypadku połączeń o niskiej przepustowości.

Metody stosowane przez protokół HTTP w wersji 1.1 zostały wymienione w tabeli 23.1. Standard HTTP określa, że pewne metody, takie jak GET, żądają informacji bez modyfikacji zawartości bądź stanu serwera. Tego rodzaju metody są uznawane za bezpieczne. Jednak nie istnieje mechanizm gwarantujący, że metoda nie wprowadzi modyfikacji. Zautomatyzowane systemy pobierania, na przykład roboty sieciowe, mogą dzięki temu indeksować witrynę za pomocą kolejnych żądań GET bez obawy, że zostaną wprowadzone jakiegokolwiek zmiany. Bezpieczne żądanie nadal będzie zarejestrowane, buforowane oraz może zmienić licznik odwiedzin strony internetowej.

**Tabela 23.1.** *Metody HTTP*

Metoda	Opis	Bezpieczna?	Wielokrotne powtórzenie bez zmiany wyniku?
CONNECT	Tworzy tunel, używając nawiązanego połączenia sieciowego. Metoda CONNECT jest najczęściej używana do wysyłania zaszyfrowanych danych przez bezpieczny protokół (na przykład HTTPS).	Nie	Nie
DELETE	Usuwa wskazany zasób.	Nie	Tak
GET	Żąda określonego zasobu.	Tak	Nie
HEAD	Żąda określonego zasobu, ale nie wymaga sekcji głównej w odpowiedzi. Metoda ta jest wykorzystywana w celu pobrania metadanych.	Tak	Nie
OPTIONS	Żądanie, aby serwer zwrócił listę metod obsługiwanych przez serwer dla określonego zasobu.	Tak	Nie
POST	Wysyła dane do zasobu w celu podjęcia dalszych działań. Metoda ta jest używana przez przycisk <i>Wyślij</i> na stronie internetowej, na której znajdują się dane przeznaczone do podjęcia dalszych działań względem nich — na przykład formularz sieciowy, sprawdzenie hasła itd.	Nie	Nie (najczęściej)
PUT	Wysyła zasób do serwera WWW.	Nie	Tak
TRACE	Wymaga odpowiedzi na żądanie. Metoda TRACE zwraca do klienta zapytanie w formie, w jakiej otrzymał je serwer. Pozwala na obserwowanie ewentualnych zmian wprowadzonych przez serwery pośredniczące.	Tak	Nie

Pewne metody działają względem zasobu tylko jednokrotnie, niezależnie od liczby wysłanych żądań. Metoda DELETE może usunąć zasób tylko jeden raz, każde kolejne wysłanie żądania z metodą DELETE po prostu nie odnajdzie w serwerze usuniętego wcześniej zasobu, więc serwer zignoruje to żądanie. Metoda taka jak DELETE działa tylko jednorazowo, niezależnie od liczby wysłanych żądań, a więc jest nazywana idempotentną. Przykładem metody, która nie jest idempotentna, jest POST. W formularzu sieciowym przycisk *Wyślij* zwykle powoduje wywołanie żądania wraz z metodą POST. Z tego powodu w wielu formularzach sieciowych użytkownik jest proszony o nieklikanie przycisku *Wyślij* więcej niż tylko jeden raz dla danej transakcji. Warto ponownie przypomnieć — wprowadzie protokół HTTP 1.1 definiuje określone metody jako idempotentne bądź nie, jednak nie istnieje mechanizm gwarantujący, że takie zachowanie będzie stosowane w danym serwerze WWW.

## Kody stanów HTTP

Odpowiedź na żądanie HTTP zwraca żądany zasób. Jednak w przypadku wystąpienia problemu serwer WWW zwróci klientowi (agentowi użytkownika) kod stanu wraz z opisem. Klient zinterpretuje odpowiedź i wyświetli ją w przeglądarce internetowej albo podejmie ustalone działanie. Klasyczny komunikat o błędzie „404 — nie znaleziono” jest

wyświetlany, gdy serwer z jakiegoś powodu nie może odpowiedzieć na żądanie. Każda przeglądarka internetowa może wyświetlać różne komunikaty, ale przedstawione w tabeli 23.2 wyjaśnienia dotyczące każdego kodu stanu są zaleceniami dla HTTP 1.1.

**Tabela 23.2.** *Kody stanów HTTP*

Klasa	Kod stanu	Opis	Uwagi
1xx		Informacyjny	Odpowiedź tymczasowa, składająca się z wiersza stanu i opcjonalnego nagłówka, kończy się pustym wierszem. Ma zastosowanie jedynie w HTTP 1.1.
	100	Kontynuacja	Klient powinien kontynuować dane żądanie.
	101	Przełączenie protokołów	Serwer działa zgodnie z żądaniem klienta i zmieni protokół aplikacji zgodnie z wiadomością Upgrade w polu nagłówka.
2xx		Sukces	Żądanie zostało otrzymane, zrozumiane i zaakceptowane przez serwer.
	200	OK	Wykonanie żądania zakończyło się powodzeniem.
	201	Utworzono	Żądanie zostało zrealizowane i nastąpiło utworzenie nowego zasobu.
	202	Zaakceptowano	Żądanie zostało zaakceptowane, ale jego przetwarzanie jeszcze się nie zakończyło.
	203	Informacja nieautorytatywna	Dane zwrócone przez serwer w nagłówku nie są ostatecznymi informacjami z serwera początkowego, ale zostały uzyskane z kopii lokalnej bądź innej. Informacje mogą być podzbiorem albo nadzbiorem informacji początkowych.
	204	Brak treści	Serwer spełnił żądanie, ale nie musi zwracać zasobu. Dodatkowe metadane mogą być zwrócone przez serwer, jeżeli żądanie zostało zmienione.
	205	Przywrócenie zawartości	Serwer spełnił żądanie; klient powinien przywrócić wygląd dokumentu.
	206	Częściowa zawartość	Serwer spełnił część żądania GET dotyczącego zasobu. Odpowiedź musi mieć pole nagłówka Range, który informuje o zakresie przesłanych bajtów.
3xx		Przekierowanie	Klient musi podjąć dalsze kroki, aby żądanie zostało spełnione.
	300	Wiele wyborów	Żądany zasób odpowiada zestawowi możliwych odpowiedzi, klient musi więc sprecyzować żądanie.
	301	Trwale przeniesiony	Żądany zasób został przeniesiony pod inny adres URI i dalsze odniesienia do tego zasobu powinny używać zwróconego adresu URI.
	302	Znaleziono	Żądany zasób tymczasowo znajduje się pod innym adresem URI.
	303	Zobacz inne	Odpowiedź na żądanie znajduje się pod innym adresem URI i powinna być pobrana za pomocą metody GET względem tego zasobu.

**Tabela 23.2.** *Kody stanów HTTP — ciąg dalszy*

Klasa	Kod stanu	Opis	Uwagi
	304	Niezmodyfikowany	Jeżeli klient wykonał warunkowe żądanie GET i otrzymał prawo dostępu, ale dokument nie został zmodyfikowany, to serwer powinien udzielić odpowiedzi z tym kodem stanu.
	305	Użyj proxy	Dostęp do żadanego zasobu musi odbyć się za pomocą proxy wskazanego w adresie URI, który znajduje się w polu Location.
	306	Nieużywany	Ten kod stanu nie jest dłużej używany, ale jego numer pozostaje zarezerwowany.
	307	Przekierowanie tymczasowe	Żądany zasób tymczasowo znajduje się pod innym adresem URI.
4xx		Błąd po stronie klienta	Serwer wykrył błąd po stronie klienta. Klient zostaje przekierowany w celu wyświetlenia użytkownikowi komunikatu o błędzie.
	400	Błędne żądanie	Żądanie nie może być spełnione, ponieważ jego składnia jest nieprawidłowa.
	401	Nieautoryzowany dostęp	Żądanie wymaga uwierzytelnienia użytkownika. Odpowiedź musi zawierać pole nagłówka WWW-Authenticate wraz z odpowiednimi danymi dla żądanej odpowiedzi.
	402	Wymagana płatność	Ten kod jest zarezerwowany do użycia w przyszłości.
	403	Zabronione	Serwer zrozumiał żądanie, ale nie jest ono honorowane. Uwierzytelnienie tutaj nie pomoże i żądanie nie powinno być powtórzone.
	404	Nie znaleziono	Serwer nie mógł znaleźć adresu URI odpowiadającego żądaniu. Ten stan może być trwały bądź tymczasowy.
	405	Niedozwolona metoda	Metoda użyta w żądaniu jest niedozwolona dla typu zasobu wskazanego w adresie URI. Odpowiedź serwera musi w nagłówku Allow zawierać te metody, których użycie jest dozwolone względem żadanego zasobu.
	406	Brak akceptacji	Zasób podany w żądaniu nie jest w stanie udzielić odpowiedzi zawierającej treść wymaganego typu, który został określony w zawartości pola nagłówka Content-Type danego żądania.
	407	Wymagane uwierzytelnienie proxy	Klient musi w pierwszej kolejności uwierzytelnić się w proxy. Proxy musi zwrócić pole nagłówka Proxy-Authenticate wraz z odpowiednim żądaniem dla proxy w celu uzyskania dostępu do żadanego zasobu. Ten błąd jest podobny do błędu o kodzie 401.
	408	Przekroczenie czasu żądania	Klient nie wykonał żądania w czasie, który serwer przeznaczył dla danego żądania. Jeżeli zachodzi taka potrzeba, to należy ponownie próbę wykonania żądania.
	409	Konflikt	Żądanie nie może być spełnione ze względu na konflikt dotyczący bieżącego stanu zasobu. Zasób może być na przykład zablokowany. Część główna odpowiedzi powinna zawierać informacje o źródle konfliktu.

**Tabela 23.2.** *Kody stanów HTTP — ciąg dalszy*

Klasa	Kod stanu	Opis	Uwagi
	410	Brak zasobu	Żądany zasób nie jest dłużej dostępny w serwerze i nie można go zlokalizować.
	411	Wymagane podanie długości	Serwer odmówił zaakceptowania żądania bez pola nagłówka Content-Length definiującego długość wiadomości, która ma być zwrócona.
	412	Nieprawidłowy warunek konieczny	Warunek konieczny w polu nagłówka żądania zwraca w serwerze wartość false.
	413	Żądana jednostka jest zbyt duża	Serwer odmówił spełnienia żądania, ponieważ jego spełnienie doprowadziłoby do wygenerowania odpowiedzi o długości nie do zaakceptowania.
	414	Zbyt długi adres URI	Serwer odmówił usługi, ponieważ adres URI jest dłuższy niż adres, który serwer może zinterpretować.
	415	Nieobsługiwany rodzaj mediów	Serwer odmówił spełnienia żądania, ponieważ format żadanego zasobu nie odpowiada żądanej metodzie.
	416	Żądany zakres nie został spełniony	Taka odpowiedź wskazuje, że żądanie zawiera pewien zakres w polu nagłówka Range, który nie jest poprawny dla bieżącego zasobu.
	417	Nieprawidłowe wymagania	Wymagania w polu nagłówka Expect nie mogą być spełnione.
5xx		Błąd po stronie serwera	Serwer wykrył błąd, który ma wpływ na udzielaną odpowiedź.
	500	Wewnętrzny błąd serwera	W serwerze wystąpił nieoczekiwany błąd.
	501	Nie zaimplementowano	Serwer nie ma odpowiednich możliwości do przetworzenia żądania. Może to oznaczać, że serwer nie rozpoznał żądania.
	502	Błędna brama	Serwer działający jako brama bądź proxy otrzymał nieprawidłową odpowiedź od serwera znajdującego się wyżej w hierarchii, wymaganą do przetworzenia żądania.
	503	Usługa niedostępna	Serwer tymczasowo nie może przetworzyć żądania. Ten błąd najczęściej występuje na skutek problemów z przeciążeniem bądź z powodu wyłączenia serwera w celu jego konserwacji.
	504	Przekroczenie czasu bramy	Serwer działający jako brama bądź proxy nie otrzymał w wymaganym czasie odpowiedzi od serwera znajdującego się wyżej w hierarchii.
	505	Nieobsługiwana wersja protokołu HTTP	Serwer nie obsługuje żądanej wersji protokołu HTTP.

Źródło: <http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html>.

Protokół HTTP został rozbudowany o możliwość tworzenia bezpiecznych połączeń. Pierwsze rozwiązanie, które pojawiło się we wczesnych wersjach HTTP, to protokół HTTPS, który szczegółowo będzie omówiony w dalszej części książki. Kiedy następuje żądanie zasobu za pomocą `https://`, przeglądarka internetowa szyfruje wiadomość, używając standardu SSL/TLS. W protokole HTTP 1.1 został dodany nagłówek `Upgrade`. W typowej wymianie wiadomości między klientem i serwerem klient żąda zaszyfrowanego zasobu:

```
GET /encrypted-area HTTP 1.1  
Host: www.domain.ext
```

na co serwer odpowiada:

```
HTTP/1.1 426 Upgrade Required (komunikat stanu)  
Upgrade: TLS/1.0, HTTP/1.1 (to są wymagane protokoły)  
Connection: Upgrade
```

Odpowiedź udzielona przez serwer wskazuje, że żądanie nie może być zrealizowane bez użycia protokołu TLS 1.0.

## Statyczne kontra dynamiczne strony internetowe

Protokół HTTP zapewnia kontrolę na poziomie aplikacji, pozwalającą transferować zasoby sieciowe z serwera WWW do przeglądarki internetowej. Wspomniane zasoby są opisywane za pomocą języka HTML, XHTML lub innego języka znaczników. Po dołączeniu do nich treści następuje budowanie strony internetowej. Kiedy strona internetowa jest budowana na podstawie zbioru plików przechowywanych w serwerze, to nazywamy ją statyczną stroną internetową.

Gdy strona internetowa jest budowana na podstawie zmiennych kryteriów oraz konstruowana indywidualnie dla klienta, wtedy jest nazywana dynamiczną stroną internetową. Dynamiczne strony internetowe bardzo często wyświetlają informacje przechowywane w bazie danych. Strony internetowe mogą być konstruowane i modyfikowane przez skrypty działające po stronie klienta bądź serwera. Zaletą kodu działającego po stronie klienta jest rozłożenie obciążenia związanego z generowaniem strony internetowej także na komputer klienta, co ułatwia skalowanie usług sieciowych. Jak Czytelnik zapewne wie, wadą wykonywania kodu po stronie klienta jest zdecydowanie niższy poziom bezpieczeństwa.

Skrypty działające po stronie serwera WWW wpływają na jego wydajność i często wymagają instalowania na nim dodatkowego oprogramowania. Niektóre możliwości w zakresie skryptów są niemal zawsze dostępne na serwerach WWW, przykładem są tutaj skrypty CGI (ang. *Common Gateway Interface*). Obecnie tendencją jest udostępnianie serwerów z minimalną ilością oprogramowania, co zmniejsza możliwy obszar ataku. Oznacza to brak stuprocentowej pewności, że serwer WWW będzie obsługiwał wybrane przez użytkownika możliwości dynamicznego tworzenia stron internetowych. Podczas wywołania skryptu CGI dane w postaci zmiennych środowiskowych są przekazywane do tego skryptu. Po wykonaniu skryptu wynik jest zwracany w postaci standardowych nagłówków HTTP oraz typu MIME, a następnie przekazywany do klienta (agenta użytkownika), który wykonał dane żądanie.

Ogólny problem ze skryptami działającymi po stronie serwera, a szczególnie z CGI, polega na tym, że w trakcie każdego żądania musi być wczytany do pamięci systemowej program wykonywalny zajmujący się przetwarzaniem danych. Takie podejście nie zapewnia najlepszej

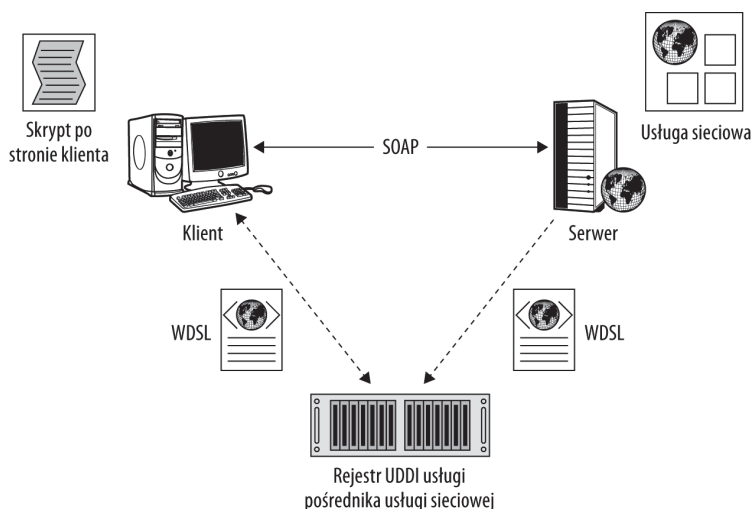
skalowalności. Opracowano więc inne rozwiązania, konkurencyjne dla CGI, rozszerzające możliwości serwerów WWW w taki sposób, aby skrypty działały na samym serwerze WWW i nie musiały być tworzone. Różne serwery WWW używają odmiennych rozszerzeń — moduły Apache, Netscape NSAPI oraz IIS ISAPI — API te zostały opublikowane i udostępnione do użytku publicznego. Inne wersje CGI, zwłaszcza FastCGI oraz SCGI (ang. *Simple Common Gateway Interface*), opracowano w celu umożliwienia aplikacjom CGI jednoczesnego uruchamiania wielu skryptów, a tym samym wyeliminowania konieczności tworzenia tych skryptów więcej razy, niż jest to wymagane.

## Usługi sieciowe

Klasyczna usługa sieciowa składa się z elementów pokazanych na rysunku 23.2 — dostawcy usługi (serwera), odbiorcy usługi (klienta) oraz pośrednika usługi sieciowej. Informacje są wysyłane między żądającym i oferującym usługę sieciową w formie, która pozwala żądającemu na używanie tej usługi w celu osiągnięcia oczekiwanego wyniku. Jak pokazano na rysunku 23.2, protokołem przekazywania wiadomości jest SOAP, natomiast dane są sformatowane w języku WSDL (ang. *Web Services Description Language*).

### Rysunek 23.2.

Aplikacja usługi sieciowej zaimplementowana z użyciem protokołu SOAP



Wiele implementacji usług sieciowych używa protokołu SOAP warstwy aplikacji w celu przekazywania wiadomości między żądającym i dostawcą usługi sieciowej. Protokół SOAP, który wcześniej oznaczał *Simple Object Access Protocol*, a obecnie to po prostu SOAP, formatuje dane w XML i używa zdalnego wywołania procedur (ang. *Remote Procedure Call*, RPC) jako mechanizmu komunikacji między aplikacjami (ang. *Inter-Application Communication*, IAC). SOAP jest zalecany przez konsorcjum W3C; obecna wersja to 1.2.

Wiadomości SOAP mogą być transportowane przez HTTP, HTTPS oraz SMTP. Jest to otwarty standard przemysłowy. Fakt, że SOAP używa XML, niesie ze sobą zarówno wady, jak i zalety. Dzięki językowi XML wiadomości są czytelne i możliwe do edycji za pomocą prostych narzędzi, jak edytor tekstu. W sytuacjach wysokiego obciążenia usługi sieciowej wykorzystanie XML skutkuje niższą szybkością niż w przypadku binarnej reprezentacji danych.

Inne standardy IAC — na przykład CORBA (<http://www.omg.org/technology/documents/formal/components.htm>), General Inter-ORB Protocol (GIOP; <http://www.omg.org/spec/CORBA/3.1>), ZeroC Internet Communications Engine (ICE; <http://zeroc.com/ice.html>) oraz Microsoft Distributed Component Object Model (DCOM; <http://msdn.microsoft.com/library/cc201989.aspx>) — są metodami przekazywania informacji w tworzeniu aplikacji rozproszonych, ale stosują binarny format danych dla formatu wiadomości pochodzących z tych aplikacji. Binarny format XML jest w trakcie opracowywania przez wiele firm i ostatecznie może stać się standardem i być powszechnie stosowany.

Istotne cechy charakterystyczne SOAP oraz każdego innego protokołu przekazywania wiadomości to:

- ♦ zezwolenie na transport w istniejących sieciach oraz współpraca z zaporą sieciową;
- ♦ niezależność od platformy i języka;
- ♦ działania przez HTTP; akceptowane są również inne protokoły;
- ♦ zachowanie możliwości rozszerzania przez różnych producentów.

Usługi sieciowe nie są klasyczną architekturą typu klient-serwer. Żądający i oferujący usługę sieciową używają tak zwanego pośrednika usługi sieciowej. W usłudze sieciowej informacje o różnych usługach dostępnych w serwerze są wysyłane przez specjalną wersję języka XML, o nazwie WSDL (ang. *Web Services Description Language*), do pośrednika usługi sieciowej, który następnie przekazuje te dane dalej, do klienta. GoToMyPC jest przykładem usługi sieciowej; jej architektoniczny diagram pokazany w rozdziale 32. to przykład tego rodzaju konstrukcji.

Wprawdzie pośrednik usługi sieciowej nie jest wymagany przez protokół SOAP, ale jednak ułatwia po stronie klienta generowanie kodu wymaganego przez wiele architektur usług, takich jak Java lub platforma .NET. Wielu pośredników usługi sieciowej używa rejestru w standardzie XML UDDI (ang. *Universal Description, Discovery, and Integration*). UDDI to otwarty standard OASIS (ang. *Organization for the Advancement of Structured Information Standards*; <http://www.oasis-open.org/home/index.php>), podobnie jak format znaczników WDSL i wiele innych. UDDI miał się stać jądrem standardu usługi sieciowej, implementowanym w formie pokazanej na rysunku 23.2 i sformowanym jako podstawa przechowywania tego, co określamy mianem białych, żółtych oraz zielonych stron. Białe strony przechowują identyfikator użytkownika i powiązane z tym dane, żółte strony przechowują kategorie wykorzystywane w określonych dziedzinach do klasyfikacji różnych systemów, natomiast zielone strony przechowują informacje techniczne dotyczące usług używanych w biznesie.

Organizacja WS-I (ang. *Web Services Interoperability Organization*) to grupa przemysłowa, której zadaniem jest promowanie wzajemnej współpracy między różnymi usługami sieciowymi. Praca grupy polega na testowaniu i zalecaniu rozwiązań umożliwiających współpracę. Organizacja WS-I opublikowała trzy specyfikacje: WS-Security, bazującą na SOAP, WS-Reliability, bazującą na standardzie OASIS oraz WS-Transactions.

Alternatywny zestaw specyfikacji ma nazwę WSRF (ang. *Web Services Resource Framework*) i został opublikowany przez OASIS do wykorzystania przez usługi sieciowe. WSRF definiuje różne metody obsługi danych sesji w trakcie transakcji rozproszonych. Kiedy klient komunikuje się z usługą sieciową, wiadomość zawiera identyfikator zasobu w żądaniu.

Informacje te mogą być enkapsulowane wewnątrz nagłówka WS-Addressing jako URI, jako dane XML lub wraz z opisem określonego zasobu docelowego. Operacje WSRF standardyzują metody READ i WRITE (w rzeczywistości GET i SET), które mogą działać ze stanem zasobu, a klient nie musi znać wszystkich danych poszczególnych usług sieciowych.

Ogólny standard OASIS usług sieciowych używany do zarządzania i monitorowania usług to metoda WSDM (ang. *Web Services Distributed Management*). Metoda WSDM odgrywa w zarządzaniu usługami sieciowymi taką samą rolę jak protokół SNMP w zarządzaniu siecią. Producenci wykorzystują metody WSDM w celu tworzenia aplikacji wyświetlających bieżący stan usługi, dostarczających możliwości zarządzania usługą sieciową oraz zdalnego diagnozowania i naprawy systemów.

Wprawdzie zdalne wywoływanie procedur (RPC) dostarcza architekturę bazującą na przekazywaniu wiadomości WSDL, inny model, o nazwie REST (ang. *Representational State Transfer*), jest stosowany w architekturach rozproszonych, w których używane są standardowe metody HTTP. Usługa sieciowa typu RESTful nadal może używać WSDL do przekazywania wiadomości SOAP przez żądanie lub odpowiedź HTTP, ale może być też zaimplementowana przez inne metody bez użycia SOAP.

## Architektura oparta na usługach

Architektura oparta na usługach (ang. *Service Oriented Architecture*, SOA) to platforma służąca do budowy rozproszonych aplikacji sieciowych na podstawie zbioru współpracujących ze sobą usług. Architektura SOA umożliwia abstrakcję żądającego usługi od różnych lokalizacji dostawcy usługi. W rzeczywistości doskonale zaimplementowana architektura SOA zapewnia abstrakcję usługi od dostawcy tej usługi. Żądający usługi sieciowej wyszukuje określoną usługę i musi jedynie wiedzieć, jakie dane wejściowe są pobierane przez usługę oraz jak używać formatu wiadomości SOA do komunikacji z tą usługą. Jeżeli dostawca usługi będzie uaktualniony, przeniesiony lub nawet zastąpiony, ale architektura pozostanie utrzymana, to usługa nadal będzie dostarczała żądanych wyników. W ten sposób komponenty w architekturze SOA pozostają wysoce modułowe i przenośne do różnych sieciowych systemów operacyjnych i języków, a cały system staje się bardzo elastyczny. Wiele usług sieciowych dostarczanych w internecie zostało zbudowanych na bazie architektury SOA.

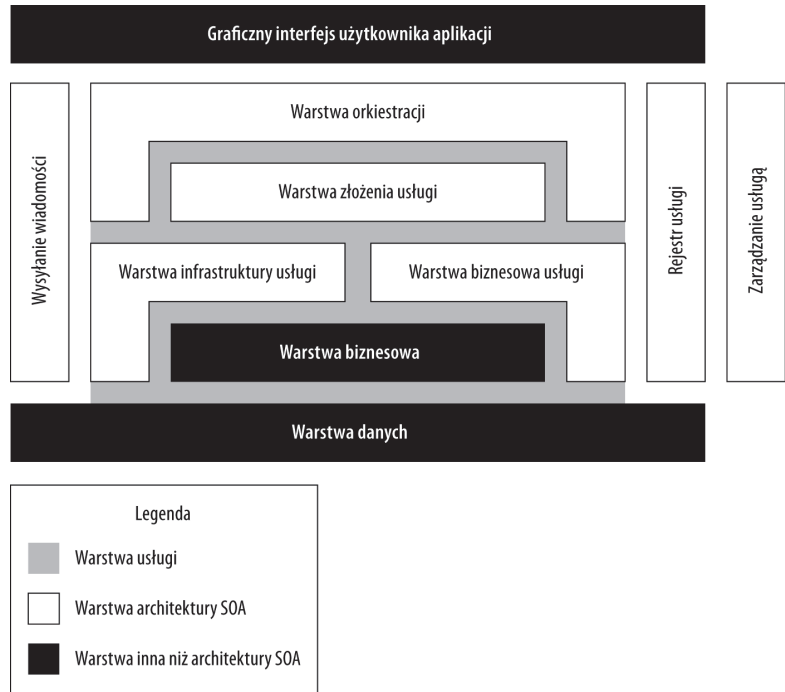


Wiele osób myli architekturę SOA z protokołem SOAP, mimo że oba pojęcia odnoszą się do różnych technologii. SOA to architektura, podczas gdy SOAP to protokół wymiany wiadomości.

W architekturze SOA klient, czyli żądający usługi, to zwykle lekka „aplikacja”, najczęściej mogąca działać w ramach interfejsu przeglądarki internetowej. Słowo „aplikacja” zostało ujęte w cudzysłów, ponieważ klient to tak naprawdę inicjator usług sieciowych działających na jednym lub wielu systemach sieciowych. Tak więc aplikacja to nazwa nadana danemu zestawowi usług, których żądający usługi używa w danej chwili. Na rysunku 23.3 pokazano konceptualny diagram architektury SOA. Warstwa organizacyjna jest używana do opisanie warstwy zawierającej ogromną ilość modułów oprogramowania, które może działać w połączeniu z innymi modułami w celu wykonywania wielu różnorodnych zadań.

**Rysunek 23.3.**

Konceptualny  
diagram architektury  
SOA



Modułowość komponentów architektury SOA oraz niezależna natura każdego dostawcy usługi powodują, że architektura ta jest opracowywana w językach zorientowanych obiektowo, takich jak C#, C++, C, Java i innych. W przeciwieństwie do wielu obiektów obsługiwanych w wymienionych językach programowania moduły dostawcy architektury SOA są ogromnymi obiektami, połączonymi w celu utworzenia programów wykonywalnych. Do tworzenia architektury SOA wykorzystywanych jest wiele technologii łącznie z SOAP, RPC, DCOM, CORBA, REST, Jini oraz Microsoft Windows Communication Foundation (WCF).

Istnieje pewny projekt, w którego ramach opracowywana jest architektura SCA (ang. *Service Component Architecture*). Zadaniem tej architektury jest dostarczenie zestawu standardów, których różne języki będą mogły używać w celu komunikacji z dostawcami usług sieciowych. W ten sposób dokona się abstrakcja języka od wywoływań usługi do dostawcy usługi sieciowej. W architekturze SCA dane mogą być przedstawiane w postaci zbioru obiektów SDO (ang. *Service Data Objects*). Transformacja architektury SCA z przemysłowej grupy roboczej na standard jest nadzorowana przez projekt OASIS CSA (ang. *Open Composite Services Architecture*; <http://www.oasis-opencsa.org/>).

Niektóre ważne platformy SOA, włączając do nich Microsoft .NET i Java EE (Enterprise Edition), nie tylko określają sposób komunikacji między żądającym usługi sieciowej i dostawcą usługi, ale również zapewniają oddzielenie modułu usługi od systemu operacyjnego oraz innych aplikacji działających na serwerze, na którym znajduje się dana usługa. W architekturze SOA różni dostawcy usług pozostają niezależni od pozostałych. Wymienione funkcje pozwalają wielu przestarzałym aplikacjom na działanie w charakterze dostawcy usług, co umożliwia zachowanie często ogromnych zasobów poświęconych na ich opracowanie.

Jak można sobie wyobrazić, w pełni zaimplementowana architektura SOA może być całkiem ogromna i zawierać wiele komponentów. Dla użytkownika przeglądającego interfejs graficzny (GUI), służący do zarządzania (prawdopodobnie za pomocą przeglądarki internetowej), oznacza to zestaw kontrolki, wyświetlanych danych oraz innych funkcji. Jednak każdy element (lub grupa elementów) może działać jako dostarczony przez innego dostawcę usług i przyjąć formę .NET Control lub EJB (ang. *Enterprise Java Bean*). W celu zrozumienia skomplikowanych środowisk i możliwości określenia wpływu różnych zmian, jak również w celu usuwania błędów z systemu konieczne jest zbudowanie mapy systemu, pokazującej różne zależności. Sytuacja przypomina modelowanie bazy danych za pomocą narzędzia typu CASE (ang. *Computer Aided Software Engineering*), takiego jak ERWin, które wykorzystuje diagramy jednostek zależności do normalizacji bazy danych. Narzędzia używane do modelowania architektur SOA bazują na tym, co nazywamy platformą SOMF (ang. *Software Oriented Modeling Framework*).



W Wikipedii można znaleźć stronę oferującą wprowadzenie do modelowania zorientowanego pod kątem usług sieciowych ([http://en.wikipedia.org/wiki/Service-oriented\\_modeling](http://en.wikipedia.org/wiki/Service-oriented_modeling)). Więcej informacji dotyczących platformy SOMF można znaleźć w książce *Service-Oriented Modeling (SOA): Service Analysis, Design, and Architecture*, napisanej przez Michaela Bella (Wiley 2008).

Dla wielu firm architektura SOA to bardzo atrakcyjna technologia, ponieważ pozwala na przekształcenie aplikacji na usługi sieciowe i pobieranie opłat za ich wykorzystywanie. Jeżeli użytkownik posiadał wcześniej pakiet biurowy i zostało opracowane uaktualnienie pewnych komponentów tego pakietu, producent musiał dostarczyć każdemu użytkownikowi uaktualnienie albo nowszą wersję oprogramowania. W tej nowej architekturze w przypadku modyfikacji oprogramowania wystarczy uaktualnić jedynie serwery. Nie jest wymagane ponoszenie żadnego dodatkowego obciążenia związanego z infrastrukturą konieczną do dostarczenia nowych wersji użytkownikom i producentom.

## Podsumowanie

W rozdziale przedstawiono, jak przeglądarki internetowe komunikują się z serwerami WWW w celu pobrania określonych zasobów przez sieć. Protokół HTTP (*HyperText Transfer Protocol*) to protokół warstwy aplikacji używany przez przeglądarki internetowe do przekazywania informacji. HTTP wykorzystuje mechanizm żądanie-odpowiedź w celu wysyłania poleceń, żądań oraz odpowiedzi między przeglądarką internetową i serwerem WWW.

Usługa sieciowa to aplikacja pośrednika między klientem i serwerem. Usługi sieciowe mogą zostać zaimplementowane za pomocą SOAP lub innego protokołu wymiany wiadomości. Protokół ten pozwala na transfer informacji między żądającym usługi sieciowej i dostawcą usługi. Usługi sieciowe wykorzystują pośredników usługi, dzięki którym jest ona wykrywalna dla klienta.

W rozdziale omówiono także architekturę SOA (ang. *Service Oriented Architecture*). Architektura SOA to platforma używana do budowy rozproszonych aplikacji. Architektury SOA były wykorzystywane do utworzenia wielu doskonale znanych aplikacji sieciowych. Stanowią także przyszłą metodę dostarczania aplikacji w postaci usług na żądanie.

W kolejnym rozdziale przedstawiono protokoły pocztowe stosowane w internecie.

# Rozdział 24.

## Protokoły poczty elektronicznej

### W tym rozdziale:

- ♦ W jaki sposób jest wysyłana i odbierana poczta elektroniczna?
- ♦ Funkcje protokołów SMTP, POP3 oraz IMAP4
- ♦ Formaty wiadomości, podział na części oraz kodowania
- ♦ Przegląd różnych serwerów i klientów poczty elektronicznej

W rozdziale zostaną przedstawione różne technologie wymagane do wysyłania poczty elektronicznej przez internet. Jądro tych usług stanowią trzy ważne protokoły IP: *Simple Mail Transfer Protocol* (SMTP), *Post Office Protocol* (POP3) oraz *Internet Message Access Protocol* (IMAP). Razem tworzą one system używany w celu wysyłania wiadomości e-mail z jednego klienta poczty elektronicznej do innego za pomocą serwerów poczty. W rozdziale będzie omówiony mechanizm działania poczty elektronicznej (e-mail).

Wiadomość e-mail składa się z nagłówka oraz części głównej (treści). W celach adresowych wykorzystywane są różne pola w nagłówku. Do formatowania wiadomości e-mail używany jest protokół SMTP. Ten protokół aplikacji dodaje „kopertę” stosowaną przez serwer SMTP do wyznaczenia trasy. Typy MIME (ang. *Multipurpose Internet Mail Extensions*), będące rozszerzeniem SMTP, są używane do segmentowania i formatowania wiadomości e-mail, jak również dostarczania treści multimedialnych w wiadomościach. W rozdziale omówiono sposoby kodowania przez typy MIME danych wykraczających poza zestaw znaków ASCII oraz binarnych.

Przedstawione zostaną również programy służące do obsługi poczty elektronicznej. Klient poczty może obsługiwać protokół POP3 lub IMAP, a także oferować szeroką gamę funkcji, dzięki którym pobieranie wiadomości z serwera poczty przychodzącej będzie znacznie wygodniejsze i bezpieczniejsze. Inne programy pocztowe mogą działać na zasadzie klienta opartego na serwerze WWW lub jako usługa terminalowa.

Protokół POP3 jest używany przez klienty do pobierania wiadomości e-mail z serwera POP3, w którym wiadomość zostanie ostatecznie usunięta i pozostanie jedynie w programie klienta. Z kolei protokół IMAP jest używany przez klienty do obsługi poczty elektronicznej po stronie

serwera. W takim przypadku poczta jest przechowywana na serwerze, ale może być przechowywana również przez klienta. Protokół IMAP jest lepszym rozwiązaniem dla korporacji oraz w celu umożliwienia wielu użytkownikom dostępu do tej samej poczty.

Poczta elektroniczna w internecie to technologia typu klient-serwer. Serwery agentów przesyłania poczty (ang. *Mail Transfer Agent*, MTA) zapewniają funkcje transportu oraz wyznaczania tras. Niektóre z nich można określić mianem platform. Klienci poczty elektronicznej to aplikacje klienckie. Na rynku dostępna jest ogromna liczba klientów poczty e-mail, ale z reguły oferują one powszechnie stosowany zestaw funkcji.

## Trzy główne protokoły

Poczta elektroniczna to jedna z najstarszych istniejących komputerowych usług sieciowych. Istniała jeszcze przed opracowaniem internetu i jego upowszechnieniem. W internecie trzy główne protokoły pocztowe — SMTP, POP3 oraz IMAP — są szeroko rozpowszechnione i stanowią ogromny odsetek wszystkich wiadomości przesyłanych przez sieć.



Poczta elektroniczna jest zdefiniowana przez zestaw standardów IETF. Format wiadomości został opisany w dokumentach RFC 822, 1123 oraz 2822. Dokument RFC 822 zastąpił dokument RFC 733. Przedstawione w dalszej części rozdziału formatowanie wiadomości e-mail za pomocą typów MIME to szkic standardu opisanego w dokumentach RFC od 2045 do 2049. Informacje dotyczące SMTP znajdują się w dokumentach RFC 2821 i 2822. Zagadnienia routingu poczty i DNS zostały opisane w dokumencie RFC 974.

## Przegląd poczty elektronicznej

Ogólna sekwencja wysyłania wiadomości e-mail (rysunek 24.1) jest następująca:

1. Klient poczty elektronicznej nadawcy (ang. *Mail User Agent*, MUA) wysyła przy użyciu agenta *Mail Submission Agent* (MSA) zakodowaną wiadomość w formacie SMTP do serwera poczty wychodzącej SMTP, który jest określany mianem *Mail Transfer Agent* (MTA).
2. Serwer poczty wychodzącej SMTP przetwarza adresy odbiorcy (umieszczone w nagłówku SMTP), szukając symbolu @ w celu ustalenia nazwy domeny. Następnie kontaktuje się z serwerem DNS danej domeny i pobiera rekord Mail eXchange (MX).

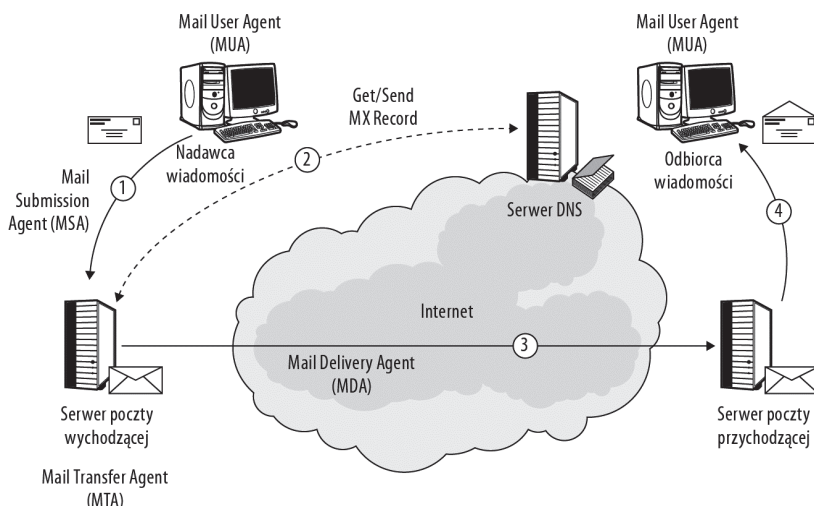
Serwer DNS zwraca rekord MX serwerowi SMTP wraz z adresem serwera obsługującego pocztę elektroniczną dla danej domeny.

3. Wiadomość SMTP jest wysyłana przez agenta *Mail Delivery Agent* (MDA) przez internet do serwera docelowego.
4. Serwer POP3 (lub IMAP) wysyła wiadomość do klienta poczty elektronicznej odbiorcy; klient dekoduje tę wiadomość i umieszcza ją w skrzynce pocztowej.

Kiedy serwer poczty, taki jak Microsoft Exchange lub Lotus Notes, wysyła i odbiera wiadomości e-mail, to używa dla nich formatu własnościowego i przeprowadza konwersję z protokołów standardowych, stosując bramę pocztową albo inną usługę. Jeżeli wiadomość jest obsługiwana przez odbiorcę za pomocą usługi Webmail, to agentem MUA zaangażowanym w ostateczne dostarczenie wiadomości jest przeglądarka internetowa.

**Rysunek 24.1.**

Ogólny proces wysyłania wiadomości e-mail



Routing poczty i jego powiązanie z DNS to ważna część mechanizmu obsługi poczty elektronicznej w internecie. Każdy serwer nazw domeny musi zawierać rekord Mail eXchange (MX), definiujący miejsce, do którego ma być wysyłana wiadomość. Rekord MX może wskazywać określony serwer bądź komputer. Ewentualnie możliwe jest użycie znaków wieloznacznych w celu zdefiniowania rekordu MX prowadzącego do ustawienia domyślnego domeny. Bez tego rodzaju informacji dostarczenie wiadomości będzie niemożliwe.

Podczas gdy klienty i serwery POP3 oraz IMAP stosują różne mechanizmy przekazywania poczty elektronicznej, większość obecnych serwerów i klientów poczty e-mail ma możliwość obsługi obu rodzajów protokołów transportowych. Po wyświetleniu ustawień konfiguracyjnych klienta poczty, na przykład Microsoft Outlook lub Mozilla Thunderbird, można się przekonać, że oba programy pozwalają na stosowanie obu protokołów.

Numery portów powszechnie używane dla różnych usług pocztowych zostały przedstawione w tabeli 24.1. Zgodnie ze standardami międzynarodowymi obsługa ruchu pomiędzy klientem a serwerem i pomiędzy serwerami powinna zostać rozdzielona. Dlatego serwery poczty wychodzącej nasłuchują na porcie 587 (ruch od klientów) i na porcie 25 (ruch pomiędzy serwerami pocztowymi). Jest to istotne, dlatego że część dostawców internetu wprowadziła ograniczenie ruchu na porcie 25 w przypadku łączy przeznaczonych dla użytkowników domowych.

**Tabela 24.1.** Powszechnie stosowane numery portów w usługach poczty elektronicznej

Protokół	Przeznaczenie	Zarówno zwykły tekst, jak i zaszyfrowany	Tylko zwykły tekst	Tylko tekst zaszyfrowany
HTTP	Webmail		80	443
IMAP4	Wejście	143		993
POP3	Wejście	110		995
SMTP	Wyjście	587, 25		465 (niestandardowy)

## Technologia push e-mail

Niektóre systemy poczty elektronicznej oferują usługę push e-mail. Kiedy tylko wiadomość dotrze do serwera, natychmiast jest wysyłana do telefonu bez konieczności wykonywania zapytania do serwera z poziomu telefonu. Technologia push e-mail jest czymś innym niż znajdująca się w klientach poczty e-mail funkcja sprawdzania w określonych odstępach czasu dostępności nowej poczty elektronicznej.

Technologia push e-mail znajduje się w tak zwanych smartfonach, na przykład Research in Motion (RIM) Blackberry. Inne przykłady to nowy mobilny system operacyjny Android, opracowany przez Google, Palm Treos, Windows Mobile (wersja 5.0 i nowsze), Apple iPhone, smartfony Sony Ericsson oraz wiele innych.

Urządzenie RIM stosuje protokół własnościowy, ale polecenie IDLE Push-IMAP oraz protokoły SyncML są często używanymi rozwiązaniami. Jeżeli telefon jest wyposażony w GPRS, to urządzenie może być zlokalizowane przez usługę bezprzewodową i poczta elektroniczna będzie dostarczona do telefonu. System push w Windows Mobile nosi nazwę Direct Push Technology i działa z klientami Microsoft Exchange to Pocket Outlook.

Systemy push e-mail często implementują funkcję powiadamiania, na przykład w postaci komunikatu „Masz wiadomość!”. W systemach Unix program `biff` jest używany do wysyłania do terminalu komunikatu, który pełni funkcję powiadomienia użytkownika o pojawieniu się nowej poczty elektronicznej.

Inną usługą poczty elektronicznej, która została opracowana w latach osiemdziesiątych i dziewięćdziesiątych, jest system poczty X.400. Zgodnie z dokumentem RFC 1006 system X.400 to standard ITU-TS, będący alternatywą dla protokołu SMTP działającego w sieciach TCP/IP. Ten system poczty elektronicznej nie odniósł sukcesu rynkowego w USA, ale do pewnego stopnia jest używany w Kanadzie; znacznie bardziej rozpowszechniony jest w Europie, Azji i Ameryce Południowej. Dotyczy to w szczególności producentów oferujących wiadomości EDI (ang. *Electronic Data Interaction*). W przemyśle militarnym i lotniczym istnieją standardy pochodne od X.400. Stosowanie systemu X.400 zostało przyćmione przez standardy poczty elektronicznej w internecie.

Protokół SMTP działa z adresami w postaci:

*przyjazna.nazwa@serwer.domena.roz*

podczas gdy adres w systemie X.400 ma postać:

`C=no; ADMD= ;PRMD=mojasiec;O=domena;OU=serwer;S=Nazwa;G=Przyjazna`

## Wiadomości w częściach

Wiadomości e-mail są umieszczane w co najmniej dwóch częściach. Absolutnym minimum jest nagłówek oraz treść wiadomości, które zawsze są rozdzielone pustym wierszem. Większość osób za wiadomość e-mail uznaje treść, natomiast z punktu widzenia serwera wiadomością jest cały obiekt danych łącznie z nagłówkiem.

Każdy nagłówek składa się z kilku pól, część z nich jest obowiązkowa, pozostałe są opcjonalne. Wymagane są następujące pola:

From: <nadawca wiadomości>  
To: <adresat wiadomości>  
Subject: <treść opisu>  
Date: <data utworzenia>



Pełna lista pól nagłówka wiadomości znajduje się na stronie  
<http://www.iana.org/assignments/message-headers/perm-headers.html>.

Trzeba w tym miejscu wspomnieć o jednej ważnej rzeczy — pola Reply-To: i From: w nagłówku wiadomości niekoniecznie muszą odpowiadać adresowi nadawcy bądź odbiorcy wiadomości e-mail. Adres wykorzystywany do routingu jest pobierany z nagłówka SMTP. Jeżeli wiadomość e-mail nie zawiera podpisu cyfrowego weryfikującego nadawcę, to w polu From: można umieścić dowolny adres e-mail.

Pola opcjonalne obejmują:

Cc: wysyłanie kopii wiadomości na podane adresy e-mail  
Bcc: wysyłanie ukrytej kopii wiadomości na podane adresy e-mail  
Reply-To: adres, na który ma być wysłana odpowiedź  
Content-Type: instrukcje dotyczące wyświetlania wiadomości, zwykle typy MIME  
In-Reply-To: unikalny identyfikator wiadomości, na który wiadomość odpowiada  
Reference: unikalny identyfikator zarówno dla wiadomości bieżącej, jak i będącej odpowiedzią

Pole Bcc zawiera adresy odbiorców wiadomości e-mail, którzy otrzymają tę wiadomość, ale ich dane (imię, nazwisko, adres) nie będą wyświetlane pozostałym odbiorcom. Pole Reply-To nie musi mieć takiej samej wartości jak adres wysyłającego, nie musi być też pojedynczym adresem. Wszystkie wymienione pola obsługują listy dyskusyjne. Typy MIME będą omówione w dalszej części rozdziału.

Część główna wiadomości, czyli treść, składa się z tekstu zakodowanego w 7-bitowym ASCII. Oznacza to możliwość użycia wszystkich liter oraz symboli „,”, „” i „+”. W celu użycia dodatkowych zestawów znaków i górnych znaków 8-bitowego ASCII te dodatkowe znaki muszą być skonwertowane na postać 7-bitowego ASCII. Proces ten nosi nazwę kodowania treści. Natomiast wyodrębnianie informacji z oryginalnej wiadomości to proces dekodowania. Stosowanych jest kilka różnych schematów kodowania, ale najczęściej używana jest metoda MIME o nazwie Base64 (metoda Base64 będzie omówiona w dalszej części rozdziału). Kiedy treść w formacie 8-bitowego ASCII pojawia się jako znaki 7-bitowego ASCII, to nazywamy ją *8-bit clean*.

Wiele klientów poczty elektronicznej obsługuje nie tylko zwykły tekst, ale również HTML. Kod HTML to po prostu zwykły tekst zawierający osadzone znaczniki. Jednak formatowanie HTML wymaga od klienta poczty e-mail interpretera HTML. Użycie kodu HTML w wiadomościach e-mail powoduje występowanie takich samych problemów jak w przypadku przeglądarek internetowych. Do generowania kodu HTML klient poczty bardzo często używa tego samego interpretera, z którego korzysta systemowa przeglądarka internetowa. Znajdujące się w wiadomości pocztowej łącza oraz treść wykonywalna mogą spowodować pobranie oprogramowania typu malware lub inne problemy.

## Simple Mail Transfer Protocol

*Simple Mail Transfer Protocol* (SMTP) to protokół używany do wysyłania poczty elektronicznej między serwerami w sieciach IP, w tym także w internecie. Większość klientów poczty elektronicznej wysyła pocztę do serwera SMTP jako SMTP, natomiast do odbierania poczty używa protokołu *Post Office Protocol* (POP) lub *Internet Mail Access Protocol* (IMAP). Protokoły POP i IMAP zostaną omówione w kolejnym podrozdziale. Najbardziej znane serwery poczty SMTP to dostępny w systemie Unix *sendmail* (który był pierwszy), Windows Microsoft Exchange, Lotus Notes, Novell GroupWise and NetMail, Sun Java System Messaging, Postfix, qmail oraz ponad 40 innych.

Wiadomość e-mail jest wysyłana z klienta poczty do serwera SMTP w następujący sposób:

1. Użytkownik tworzy wiadomość w programie klienta poczty, a następnie klika przycisk *Wyślij*.
2. Klient poczty nawiązuje połączenie z portem 587 serwera poczty wychodzącej SMTP, zdefiniowanym w opcjach konfiguracyjnych klienta.
3. Serwer SMTP przetwarza adres *sendto*: na nazwę i domenę.
4. Jeżeli wiadomość jest przeznaczona do tej samej domeny, w której znajduje się nadawca, to zostanie przekazana serwerowi POP3 w celu wysłania.
5. Jeżeli wiadomość jest przeznaczona do innej domeny, to serwer SMTP wysyła wiadomość agentowi dostarczania.
6. Serwer SMTP nawiązuje połączenie z serwerem DNS w celu otrzymania adresu rekordu Mail eXchange (MX) serwera SMTP wymienionego dla domeny adresata.
7. Serwer SMTP nadawcy wysyła wiadomość przez port 25 do serwera SMTP adresata; z tego serwera zostanie przesłana do serwera POP3 lub IMAP.
8. Klient poczty adresata, nazywany czasem agentem MUA (ang. *Mail User Agent*), lub pośredni serwer SMTP, nazywany czasem MTA (ang. *Mail Transport Agent*), wysyła żądanie sprawdzenia poczty w celu zainicjowania pobrania nowej poczty.

Nie każda wiadomość może być dostarczona natychmiast, tak więc SMTP kolejkuje wiadomości przez pewny okres, a następnie co jakiś czas próbuje wysłać je ponownie. Wiele programów SMTP używa *sendmail* jako agenta dostarczania; kolejkę wiadomości nazywa się wówczas kolejką *sendmail*. W serwerze można skonfigurować okres, przez który serwer SMTP będzie próbował wysłać wiadomość, częstotliwość prób ponownego wysłania wiadomości z kolejki, częstotliwość wysyłania wiadomości, kiedy nie dotarła do adresata oraz zachowanie w przypadku zwrócenia wiadomości.

Wiadomość SMTP to informacja zawierająca adresy nadawcy i odbiorcy. Podanie nadawcy jest wymagane, ponieważ jeśli wiadomość nie zostanie dostarczona, to nadawca otrzyma odpowiedni komunikat. Część główna wiadomości SMTP składa się z nagłówka oraz treści wiadomości, choć określenie „część główna SMTP” jest rzadko stosowane.

SMTP używa bardzo prostego zestawu poleceń, które są zrozumiałe dla człowieka posługującego się językiem angielskim. W trakcie sesji SMTP przekazywane są wiadomości takie jak *HELO* jako powitanie, *MAIL FROM*: jako adres nadawcy itd. Kiedy serwer SMTP odpowiada

na takie polecenie, to używa do tego pewnego zbioru liczb w charakterze odpowiedzi. Powszechnie stosowane odpowiedzi to 220 (gotowy), 221 (zamknięcie połączenia), 250 (zakończono), 354 (OK, transmisja), 450 (skrzynka pocztowa jest zajęta), 451 (przerwanie ze względu na błąd), 452 (przerwanie ze względu na brak miejsca na dysku), 500 (błąd składni), 550 (skrzynka pocztowa niedostępna bądź nie istnieje), 552 (przerwanie ze względu na przekroczenie ilości przydzielonego miejsca na dysku) oraz 554 (transakcja zakończona niepowodzeniem).

Protokół *Extended Simple Mail Transfer Protocol* (ESMTP) to rozszerzenie SMTP, które pozwala na wysyłanie plików multimedialnych jako wiadomości pocztowych. Protokół ESMTP jest stosowany, gdy klient wyśle polecenie EHL0 (ang. *Extended HELLO*) inicjujące połączenia, a serwer SMTP udzieli odpowiedniej odpowiedzi, wskazującej na nawiązanie połączenia, niepowodzenie lub inny stan. Pewna liczba poleceń ESMTP, między innymi SIZE, BDAT, CHUNKING, DSN, ETRN, obsługuje transfer danych multimedialnych. Protokół ESMTP obsługuje funkcję potokowania, w której jednocześnie można wysłać wiele poleceń.

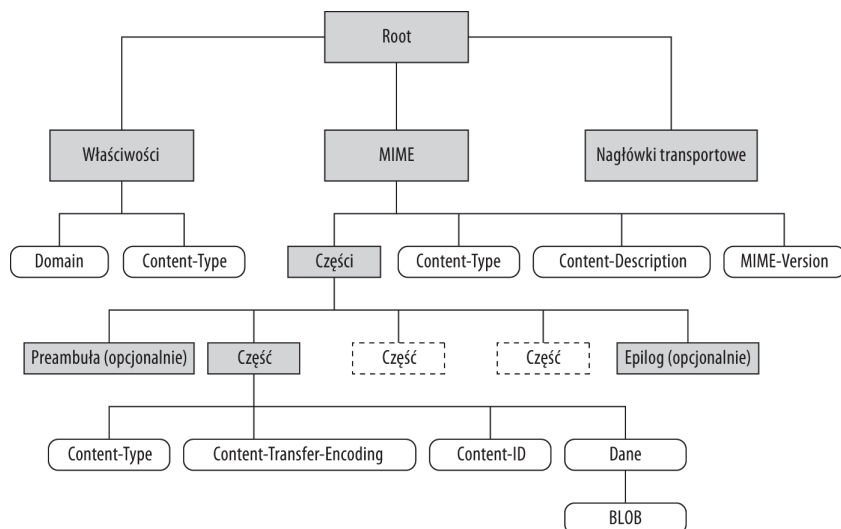
SMTP nie ma wbudowanego mechanizmu bezpieczeństwa. Kiedy potrzebne jest użycie bezpieczniejszej wersji SMTP, można zastosować rozszerzenie SMTP-AUTH protokołu, które wymaga od użytkownika zalogowania się do serwera poczty przed wysłaniem wiadomości. Rozszerzenie SMTP-AUTH pozwala użytkownikowi na uzyskanie dostępu do serwera poczty, ale nie przeprowadza żadnych innych operacji sprawdzenia poprawności bądź przeznaczenia danej wiadomości e-mail. SMTP-AUTH pozwala na przekazywanie poczty, ale serwer przekazywania musi być zaufany względem wysyłającego serwera SMTP. Z tego powodu w internecie rzadko można się spotkać z używaniem rozszerzenia SMTP-AUTH.

## Typy MIME

SMTP zarządza wiadomościami w postaci zwykłych plików tekstowych, które mogą być pobierane przez klienty POP3 i IMAP. Wiele wiadomości zawiera treść dodatkową, niebędącą tekstem. Oznacza to konieczność istnienia mechanizmu pozwalającego na dołączenie tej treści do tekstu. Mechanizmem używanym przez niemal każdego jest *Multipurpose Internet Mail Extensions*, czyli typy MIME. Na rysunku 24.2 pokazano hierarchię wiadomości oraz sposób segmentowania wiadomości przez MIME.

MIME formatuje tekst wysyłany w wiadomościach. W hierarchii formatowania Root oznacza wszystkie wiadomości wysłane wszędzie przez kogokolwiek. Wiadomość udostępnia określone właściwości, przede wszystkim domenę (Domain), z której pochodzi, oraz typ znajdującej się w niej treści (Content-Type). Na powyższym rysunku prostokąty o zaokrąglonych rogach przedstawiają informacje albo metadane. Zwykle prostokąty przedstawiają formatowanie bądź strukturę organizacyjną. Z kolei nagłówki transportu zawierają informacje routingu umieszczone w nagłówku — pola takie jak From:, To:, Reply-To:, Re:, BCC: itd.

Główną częścią hierarchii MIME jest odgałęzienie odpowiedzialne za formatowanie treści wiadomości i podział jej na części. Każda część zawiera treść, opis treści oraz wersję MIME użytą do sformatowania danej części. Części dalej dzielą się na fragmenty, z których każdy zawiera te same dane i metadane formatujące. Części „preambuła” i „epilog” mogą zostać dodane w celu objaśnienia przeznaczenia poszczególnych części, ale to funkcje opcjonalne.

**Rysunek 24.2.**Wiadomość oraz  
hierarchia MIME

W pewnym momencie dochodzimy do części ostatniej (najniższego poziomu), do której można dołączyć dane, pokazane na rysunku jako obiekt BLOB. Obiekt BLOB oznacza *Binary Large Object* i jest plikiem dowolnej wielkości, który może być dołączony do wiadomości. Obiekt BLOB jest rodzajem pojemnika i może przechowywać dokumenty procesora tekstu, pliki graficzne, pliki w formacie PDF i dowolne inne, które zostaną dołączone do wiadomości.

Jak zdefiniowano w dokumentach RFC 822 i 2822, wiadomość e-mail to zwykły 7-bitowy tekst ASCII. Każdy język wykorzystujący znaki wyższego poziomu ASCII (8-bitowe) nie stanowi części standardu e-mail. Różne pliki, takie jak obrazy, dokumenty bądź informacje sformatowane, które mogą spowodować oddzielenie jednej części wiadomości e-mail od innej, również nie stanowią części standardu e-mail. Dzięki typom MIME można rozwiązać wymienione problemy przez dodanie do wiadomości e-mail poleceń zwykłego tekstu, określających dodatkowe możliwości.

Mechanizm typów MIME jest odpowiedzialny za:

- ♦ **Wyświetlanie tekstu innego niż ASCII (symboli).** Protokół SMTP używa 7-bitowego zbioru znaków ASCII. Mechanizm typów MIME rozszerza go do pełnych 8 bitów, dzięki którym staje się możliwa obsługa symboli używanych w innych językach, na przykład *ą, ć, ę, ł, ń, ó, ś, ź, ż* itp.
- ♦ **Specyfikacja załączników takich jak obrazy i dokumenty.**
- ♦ **Podział wiadomości na części.**
- ♦ **Symbolne w nagłówkach wiadomości.**
- ♦ **Kodowanie i dekodowanie treści innej niż ASCII w wiadomości e-mail.**

Prosty nagłówek MIME może rozpoczynać się w sposób podobny do przedstawionego poniżej:

```

MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Content-Description: To jest przykładowa wiadomość MIME
  
```

Content-ID: <part0090829@servername.domain>  
 Content-Location: http://nazwaserwera.domena/nazwapliku.txt  
 Content-Disposition: inline  
 To jest treść wiadomości e-mail.

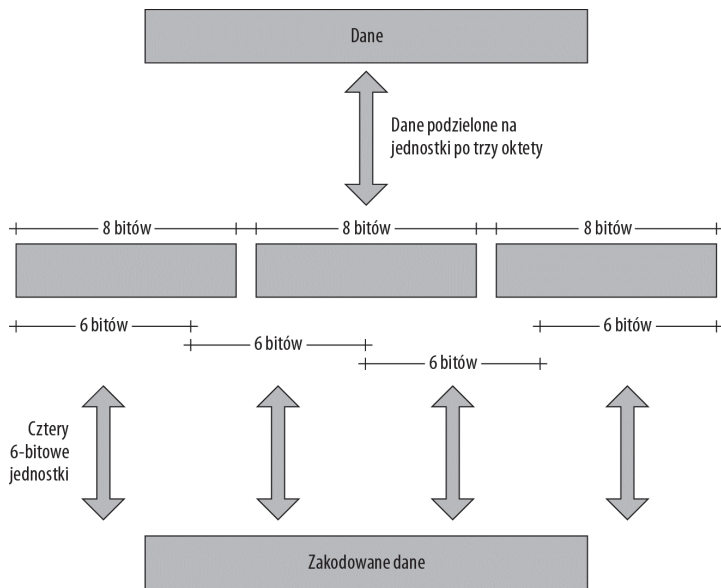
## Kodowanie Base64

Podczas tworzenia wiadomości e-mail w kliencie poczty elektronicznej polecenia MIME są dodawane do wiadomości i wskazują klientowi adresata sposób, w jaki wiadomość powinna zostać wyświetlona. Jeżeli tworzona wiadomość to po prostu 7-bitowy tekst ASCII i nie więcej, to MIME określa treść jako zwykły tekst i wiadomość pozostaje nienaruszona. Kiedy do wiadomości są dołączane załączniki lub w jej treści znajduje się kod HTML, to każda część wiadomości otrzymuje polecenie MIME informujące klienta, jakiej treści powinien się spodziewać oraz w jaki sposób powinien ją obsługiwać.

Proces kodowania i dekodowania powoduje dekonstrukcję treści w trakcie jej wysyłania oraz jej przywrócenie po otrzymaniu przez adresata. Kodowanie Base64 działa przez pobranie danych i podzielenie ich na jednostki o długości trzech bajtów. Takie 24 kolejne bity są dzielone na cztery 6-bitowe jednostki, z których każda jest kodowana na jeden znak ASCII. Sześciobitowy znak zawiera 26 dużych (*A – Z*) i małych (*a – z*) liter ASCII, 10 cyfr (*0 – 9*), symbole *+* i */* oraz przyjmuje wartości kolejno od 0 do 63. Kodowanie Base64 odwołuje się do faktu, że zbiór znaków będzie miał wielkość  $2^6$ , czyli 64 znaki. Proces kodowania został pokazany na rysunku 24.3.

### Rysunek 24.3.

*Proces kodowania może pobierać dane inne niż ASCII, a następnie przekształcić je na postać ASCII w celu wysłania w wiadomości e-mail*



Przeanalizujmy przykład sposobu działania takiej konwersji. Przyjmujemy założenie, że trzy bajty są liczbami 124, 250 oraz 039. Strumień bitów przedstawiający trzy wymienione liczby jest następujący:

```
01111100
11111010
00100111
```

Proces kodowania powoduje konwersję pokazanego wyżej strumienia na cztery następujące liczby 6-bitowe:

```
011111
001111
101000
100111
```

Konwersja czterech 6-bitowych liczb dwójkowych daje w wyniku:

```
31
15
40
39
```

który po przekształceniu według schematu podanego powyżej na znaki ASCII daje następującą sekwencję:

```
f
p
o
n
```

Kodowanie Base64 to nie jedyna metoda stosowana w celu kodowania danych binarnych na postać możliwą do wysłania za pomocą protokołu SMTP. Inne używane to Quoted-Printable lub brak kodowania, oznaczany w nagłówku jako 7bit dla podstawowego SMTP, oraz kodowanie 8-bitowe dla rozszerzonego SMTP, określane jako 8BITMIME. Wprawdzie Base64 to powszechnie stosowany schemat kodowania, ale używane są również schematy Base32 i Base16. Różnica między nimi polega na tym, że Base32 i Base16 wykorzystują mniejszy zakres znaków do kodowania wiadomości.

## Generowanie MIME

Każda wiadomość MIME informuje o swojej obecności przez umieszczenie w nagłówku poniższego wiersza:

```
MIME-Version: 1.0
```

Jeżeli treść jest po prostu zwykłym tekstem ASCII i niczym więcej, to umieszczony będzie poniższy wiersz:

```
Content-Type: text/plain
```

Rodzaj treści może składać się z typu wskazanego w nagłówku Content-Type, jak również podtypów. W celu wskazania istnienia innej treści MIME określa różne fragmenty wiadomości. Załącznik jest wskazywany przez multipart/mixed, natomiast typ załącznika będzie wskazany przez wiadomość nagłówka Content-Disposition wraz z nazwą pliku i rozszerzeniem. Nagłówek Content-Disposition może wskazywać program, za którego pomocą można otworzyć daną treść. Poniżej przedstawiono przykładowy nagłówek:

```
Content-Disposition: attachment; filename="nazwapliku.jpg"
```

Wiersz Content-Disposition pozwala nadawcy na osadzenie opisu w postaci zwykłego tekstu, który będzie opisem przeznaczenia wiadomości MIME.

Mechanizm typów MIME ma zastosowanie również względem innych protokołów internetowych. Wiele żądań HTTP towarzyszą dane opisywane przez MIME i wyświetlane w przeglądarce internetowej. Linia `multipart/alternative` nakazuje klientowi odczyt sekcji `text/plain` albo `text/html`, w zależności od tego, czy klient może wygenerować kod HTML, czy nie. Tego rodzaju ustawienie użytkownika zwykle można skonfigurować w kliencie poczty elektronicznej. Inne rodzaje treści także są wskazywane przez instrukcje `Content-Type`, na przykład `image/jpg`, `audio/mp3` lub `video/mp4`. Dokument aplikacji może być dołączony wraz z wartością `application/msexcel` dla nagłówka `Content-Type`. Pełna lista typów MIME znajduje się na stronie IANA (*Internet Assigned Numbers Authority*) pod adresem <http://www.iana.org/assignments/media-types/>.

Metoda używana przez MIME do kodowania zestawu znaków wykraczającego poza 7-bitowy standard ASCII (8-bitowe ASCII) jest podobna do przedstawionej przy omawianiu Base64. Znak ASCII spoza standardu 7-bitowego jest konwertowany na ciąg tekstowy w następującej formie:

```
=?charset?encoding?encoded text?=
```

Istnieje możliwość użycia dowolnego zestawu znaków zarejestrowanego w IANA; zastosowane kodowanie to Q-encoding (kodowanie Quoted-Printable) lub B-encoding (Base64) plus ciąg tekstowy znaku przeznaczony do konwersji. Między tymi dwoma rodzajami kodowania występują drobne różnice, ale ogólnie działają w podobny sposób. Dlatego też można zobaczyć wiersz podobny do przedstawionego poniżej:

```
Subject: =?iso-8859-2?Q?=Nowa tabela w A2?=
```

który przybiera postać *Nowa tabela w A2*.

Mechanizm MIME używa nagłówka `Content-ID` w celu utworzenia unikalnego identyfikatora fragmentu wiadomości w przypadku wiadomości składającej się z kilku części. Przykładowy wygląd nagłówka `Content-ID` pokazano poniżej:

```
Content-ID: <11.3.23957.2098389882@servername.domain.ext>
```

Jedynym wymaganiem jest to, aby identyfikator był unikalny. Tak więc zgodnie z konwencją został podzielony na znajdującą się po prawej stronie nazwę serwera, znak @ oraz pewną unikalną liczbę. Znacznik czasu zwykle jest umieszczany w lewej części ciągu tekstowego `Content-ID`. Bardzo podobny unikalny nagłówek `Message-ID` jest stosowany w celu identyfikacji całej wiadomości.

*Uuencoding* to alternatywna metoda kodowania znaków innych niż ASCII na postać znaków ASCII. Metoda ta jest stosowana głównie w programach pocztowych systemu Unix. Nazwa *uuencoding* pochodzi od wyrażenia *Unix-to-Unix encoding*. Metoda ta stanowi rozwiązanie alternatywne względem typów MIME. `uuencode` to program systemu Unix odpowiedzialny za operację kodowania, natomiast `uudecode` to program służący do dekodowania zakodowanej wiadomości. Mechanizm typów MIME w przeważającym stopniu zastąpił MIME wraz z Base64 używanym jako technika kodowania.

## Protokół Post Office Protocol

Protokół *Post Office Protocol* (POP) to jeden z dwóch powszechnie używanych przez programy klientów poczty protokołów służących do pobierania poczty z serwerów w sieciach IP. Protokół POP miał już kilka wersji, ostatnia z nich to POP3. Można zaryzykować stwierdzenie, że protokół *Post Office Protocol* to serwer plików tekstowych. Wiadomość jest tekstem dołączanym do pliku adresu e-mail.

Poniżej przedstawiono procedurę żądania poczty za pomocą POP3:

1. Klient POP3 inicjuje żądanie sprawdzenia dostępności poczty i tworzy połączenie z serwerem POP3, który nasłuchuje na porcie 110.
2. Serwer POP3 żąda podania nazwy użytkownika i hasła jako danych uwierzytelniających, które są dostarczane przez program klienta.
3. Konto e-mail otrzymuje prawo dostępu do jego pliku tekstowego wiadomości, a klient przekazuje serwerowi numer ostatniej otrzymanej wiadomości.
4. Wszystkie wiadomości o numerach wyższych niż przekazany serwerowi są wysyłane do programu pocztowego klienta.
5. Serwer POP3 zamyka połączenie i w zależności od konfiguracji klienta pozostawia lub usuwa z pliku tekstowego wysłane wiadomości.

Krok 5. definiuje bardzo istotną potencjalną różnicę między protokołem pocztowym POP3 i IMAP, który zostanie omówiony w kolejnym podrozdziale. IMAP to poczta elektroniczna bazująca na serwerze. Kiedy wiadomość jest wysyłana do klienta IMAP, to pozostaje w serwerze i jest dostępna podczas innej sesji IMAP w późniejszym czasie bądź z innej lokalizacji. W przypadku klienta POP3 opcja konfiguracyjna w jego oprogramowaniu pozwala usunąć z serwera całą pobraną pocztę albo pozostawić ją. Większość osób stosuje ustawienie domyślne, czyli usunięcie poczty z serwera po jej pobraniu.

Gdy klient POP3 ma ustawioną opcję pozostawienia poczty w serwerze, podczas kolejnego połączenia musi mieć możliwość rozpoznania nowych wiadomości. Jeżeli w międzyczasie inny klient POP3 nawiąże połączenie, pobierze wiadomości, a następnie usunie je, to numery wiadomości, które nadejdą później, nie będą dłużej zgadzały się w pierwszym kliencie POP3. W celu rozwiązania tego problemu do identyfikacji wiadomości POP3 używa 32-bitowej liczby UIDL (ang. *Unique IDentification Listing*). Kiedy pierwszy klient POP3 wyświetla liczbę UIDL wiadomości, może mapować tę wiadomość względem identyfikatora bieżącej wiadomości. Klienci IMAP stosują podobny system, ale ich liczby UIDL są przypisywane jako kolejne liczby, tak aby klient IMAP mógł pobrać następny numer sekwencji.

Serwery POP3 używają bardzo prostych poleceń i języka pobierania. Do pobierania poczty nie trzeba koniecznie stosować klienta POP3. Jeżeli użytkownik dysponuje klientem telnet, to może nawiązać połączenie z serwerem POP3 przez port 110 i wysyłać do serwera POP3 polecenia sesji konieczne do pobrania poczty. Po zalogowaniu się i wysłaniu polecenia RETR serwer POP3 wysyła do klienta telnet wiadomości, które można następnie odczytać.

Protokół POP3 pozwala klientom na logowanie się do serwera POP3 za pomocą zwykłego, niezaszyfrowanego tekstu. W celu zapewnienia użytkownikom ochrony dodano do POP3 wiele różnych metod uwierzytelniania. Najczęściej stosowana metoda nosi nazwę *Authenticated POP* (APOP) i wykorzystuje funkcję MD5 do szyfrowania danych uwierzytelniających. Wiele klientów POP3 obsługuje APOP.

## Klienty poczty Webmail

Webmail to klient poczty działający w ramach przeglądarki internetowej. Wiele różnych klientów poczty oferuje wersje przeznaczone dla przeglądarki internetowej, na przykład Microsoft Outlook Web Access. Dostępne są również różne usługi poczty Webmail — liczne z nich bazują na internecie, na przykład Hotmail (teraz będący własnością Microsoft), AOL mail, Yahoo! Mail oraz Gmail (Google).

Dostawcy usługi Webmail dostarczają serwery poczty elektronicznej pozwalające na przechowywanie i wysyłanie poczty, do której użytkownik ma dostęp za pomocą dowolnej przeglądarki internetowej. Oprogramowanie klienta jest osadzone w serwerze i może dostarczyć niemal każdą funkcję oferowaną przez samodzielne aplikacje klienta poczty. Interfejs użytkownika (UI) jest generowany przez przeglądarkę internetową. Usługa Gmail firmy Google używa interfejsu utworzonego w języku JavaScript. Wiele usług Webmail jest bezpłatnych do pewnego poziomu, który zwykle jest powiązany z ilością przestrzeni dyskowej oferowanej użytkownikowi na serwerach dostawcy. Po zapłaceniu za usługę ilość dostępnej przestrzeni jest zwiększana.

Sukces poczty Webmail doprowadził do tego, że możliwość tę zaczęły oferować przemysłowe serwery pocztowe. Istnieje również wiele aplikacji klienta Webmail typu open source, które można wykorzystać do nawiązywania połączenia z serwerami poczty. Większość klientów Webmail została utworzona w celu uzyskania dostępu do serwerów IMAP i SMTP. Jednak istnieje również pewna liczba klientów Webmail oferujących możliwość połączenia się także z serwerami POP3 i IMAP.

Prawdopodobnie najbardziej znanym przykładem witryny Webmail jest *Mail2Web.com*, której właścicielem jest firma SoftCom Technology Consulting Inc. z Toronto. Usługa Mail2Web oferuje wiele funkcji zwykłego klienta poczty wewnątrz przeglądarki internetowej. Za pomocą Web2Mail trzeba podać jedynie konto poczty e-mail i dane uwierzytelniające, a usługa samodzielnie nawiąże połączenie z serwerem i pobierze pocztę. W celu korzystania z bezpłatnej usługi nie trzeba zakładać konta Mail2Web.

## Protokół Internet Message Access Protocol

*Internet Message Access Protocol* (IMAP) to program pocztowy bazujący na serwerze. W przeciwieństwie do opisanego w poprzednim podrozdziale protokołu POP3 IMAP tworzy magazyn danych poczty e-mail na serwerze, do którego dostęp można uzyskać za pomocą klienta IMAP. Microsoft Exchange i Outlook to klasyczne przykłady serwera i klienta IMAP. Protokół IMAP oferuje pewne istotne zalety w stosunku do POP3, szczególnie w przypadku aplikacji biznesowych. W IMAP istnieje trwały rekord dla wiadomości e-mail, a poczta „podąża” za użytkownikiem, niezależnie od tego, skąd nawiązuje on połączenie.

IMAP obsługuje sesje zarówno online (połączone), jak i offline (rozłączone). W sytuacji, kiedy system zostaje odłączony od sieci IP, większość klientów IMAP przechowuje pocztę e-mail lokalnie i synchronizuje dane po połączeniu z serwerem IMAP. Wszystkie zmiany wprowadzone lokalnie są w trakcie następnego połączenia przekazywane do serwera. Analogicznie wszystkie zmiany w serwerze wprowadzone przez użytkownika za pomocą innego klienta IMAP są przekazywane z serwera do bieżącego klienta IMAP.

Jeżeli użytkownik dysponuje komputerami stacjonarnym i przenośnym, to IMAP stanowi rozwiązanie pozwalające na otrzymywanie poczty e-mail w obu systemach oraz zapewnia zautomatyzowany mechanizm synchronizacji poczty. Wprawdzie istnieje możliwość synchronizacji poczty e-mail POP3 między systemami, ale trzeba to robić ręcznie. Nie stanowi to więc części systemu POP3, co utrudnia proces synchronizacji i sprzyja powstawaniu błędów.

Podobnie jak SMTP i POP3, IMAP używa systemu prostych wiadomości. IMAP nasłuchuje na porcie 143.

## Serwery poczty

Serwer poczty (ang. *Mail Transfer Agent*, MTA) to aplikacja serwerowa przeznaczona do przekazywania poczty. Czasami takie systemy są nazywane routerami poczty lub MTA, natomiast bardzo rzadko mailerami internetowymi. Niezależnie od użytej nazwy zawsze oznacza to MTA. Na świecie używanych jest wiele różnych programów MTA, ale ponieważ zwykle nie odpowiadają na zautomatyzowane zapytania dotyczące ich identyfikacji, to udział rynkowy poszczególnych serwerów nie jest całkiem jasny. Niektóre opracowania wskazują, że największy udział mają Microsoft Exchange na platformie Windows oraz sendmail, qmail i Exim na platformie Linux i Unix. Z kolei inne opracowania wskazują znacznie większy udział w rynku wielu innych produktów.

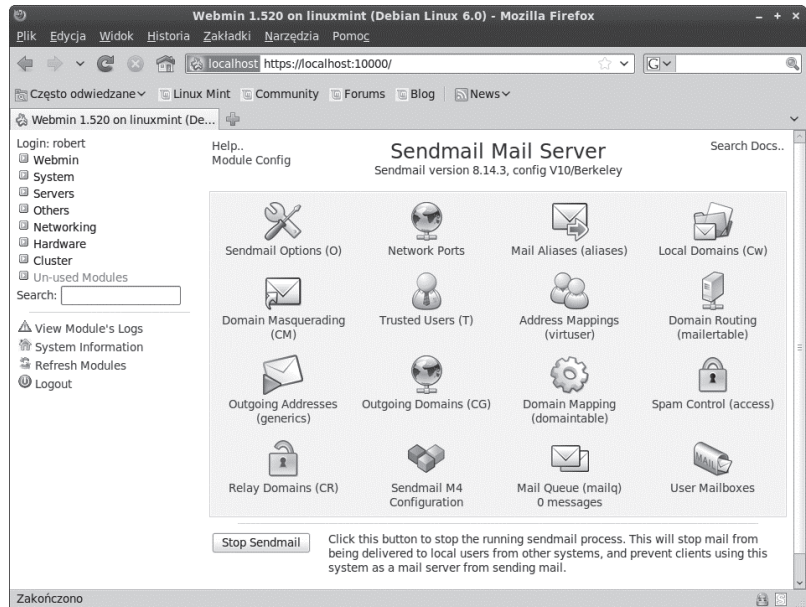
Serwery poczty nie są po prostu aplikacjami transportowymi, choć niektóre z nich są skonfigurowane właśnie w taki sposób. Większość serwerów poczty zarządza magazynami wiadomości, które są obiektami bazy danych zawierającymi wiadomości oraz pozostałą treść przekazywaną we współczesnych wiadomościach e-mail. Fragment aplikacji odpowiedzialny za wiadomości może być bogato wyposażony w funkcje, między innymi filtrowanie, sprytny routing, zarządzanie identyfikacją, zapewniające bezpieczeństwo i wiele innych. Funkcją o kluczowym znaczeniu jest tworzenie kont użytkowników oraz obsługa skrzynek pocztowych. W niektórych systemach skrzynka pocztowa może być pojedynczym plikiem, podczas gdy w innych jest katalogiem plików przechowującym pocztę przychodzącą.

Produkty takie jak Microsoft Exchange i IBM Lotus Domino to serwery oparte na bazach danych klasy przemysłowej, odpowiednio SQL Server i DB2. Program Domino był początkowo opracowany jako serwer Lotus Notes, następnie został zintegrowany w platformę groupware i może funkcjonować jako serwer aplikacji i (lub) jako serwer WWW. Produkt Microsoft Exchange został opracowany jako platforma wymiany wiadomości, do której dodano funkcje współpracy z innymi. Najpopularniejszy używany serwer poczty to sendmail, będący programem typu open source, który zastąpił starszy program o nazwie delivermail. Według szacunkowych danych około 30% wszystkich serwerów poczty opiera się na sendmail.

Program `sendmail` można konfigurować z poziomu wiersza poleceń. Jednym ze sposobów udostępnienia `sendmail` jest użycie Webmin, czyli narzędzia GUI bazującego na przeglądarce internetowej. Pokazany na rysunku 24.4 Webmin (<http://www.webmin.com>) to oprogramowanie typu open source przeznaczone do obsługi usług systemu operacyjnego w systemach OpenSolaris, Linux oraz innych odmianach systemu Unix. `Sendmail` to tylko jedna z wielu aplikacji obsługiwanych przez Webmin. Oprócz tego obsługiwane są między innymi Apache HTTP Server, MySQL i PHP. Każdy moduł Webmin wczytuje odpowiedni plik konfiguracyjny, a więc efektywnie tworzy architekturę rozszerzeń.

#### Rysunek 24.4.

Konfiguracja  
`sendmail` w narzędziu  
GUI o nazwie Webmin



## Konfiguracja klienta poczty

Klient poczty (ang. *Mail User Agent*, MUA) to program pozwalający na tworzenie i wysyłanie wiadomości oraz ich pobieranie i wyświetlanie. W architekturze klient-serwer program klienta poczty elektronicznej jest klientem, natomiast serwer poczty jest serwerem. Pozostałe programy, które mogą wykonywać te funkcje, są nazywane programami pocztowymi, niezależnie od tego, czy działają wewnątrz przeglądarki internetowej, jak na przykład Webmail, czy w wierszu poleceń wewnątrz sesji telnet.

Klient poczty nie działa jako usługa, o ile nie zostanie automatycznie uruchomiony przez system. Klienci poczty są w większości konfigurowane jako klienci SMTP/POP3 lub IMAP. W ten sposób klient poczty może pobierać wiadomości e-mail z niemal każdego serwera poczty w internecie. Niektóre programy, na przykład Eudora, są przeznaczone dla pojedynczego użytkownika, podczas gdy inne, na przykład Microsoft Outlook, zostały zaprojektowane do wykorzystywania przez wielu użytkowników. Struktura organizacyjna skrzynek pocztowych pozwala zatem na obsługę oddzielnych kont. Tak więc Outlook używa pojedynczego pliku skrzynek pocztowych (PST), natomiast Eudora umieszcza skrzynki pocztowe (MBX) w oddzielnych plikach.

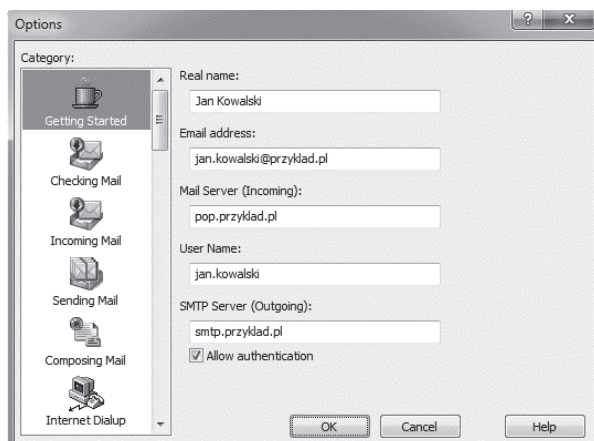
W celu skonfigurowania klienta poczty trzeba dostarczyć następujące informacje:

- ♦ nazwę konta, jeżeli używany jest klient obsługujący wiele kont,
- ♦ wyświetlaną nazwę użytkownika, czyli „prawdziwe imię i nazwisko”,
- ♦ poprawny adres e-mail,
- ♦ adres serwera poczty przychodzącej — POP3 albo IMAP,
- ♦ nazwę użytkownika wykorzystywaną w celu zalogowania się do serwera,
- ♦ nazwę serwera poczty wychodzącej (SMTP).

Typowe okno dialogowe ustawień zostało pokazane na rysunku 24.5; pochodzi ono z programu Eudora 7.1. Program Eudora 7.1 to ostatnia komercyjna wersja wydana przez firmę Qualcomm. Obecnie Eudora przechodzi proces konwersji na postać klienta typu open source, który będzie nosił nazwę Penelope i zaadaptuje niektóre funkcje z prawdopodobnie najbardziej znanego klienta poczty typu open source, czyli Mozilli Thunderbird.

### Rysunek 24.5.

*Ustawienia  
w programie  
pocztowym*



Programy pocztowe firmy Microsoft to Outlook Express (Windows XP i wcześniejsze), Outlook (wszystkie wersje) oraz Windows Mail (Vista). Konfiguracja w wymienionych programach odbywa się za pomocą kreatora tworzącego konto poczty e-mail przed przejściem do ustawiania poszczególnych opcji. Program Windows Mail obsługuje nie tylko POP3 i IMAP, ale również serwery HTML.



Rozbudowana lista klientów poczty e-mail, zawierająca ich bieżące wersje, obsługiwane protokoły oraz funkcje, znajduje się na stronie [http://pl.wikipedia.org/wiki/Porównanie\\_programów\\_pocztowych](http://pl.wikipedia.org/wiki/Porównanie_programów_pocztowych).

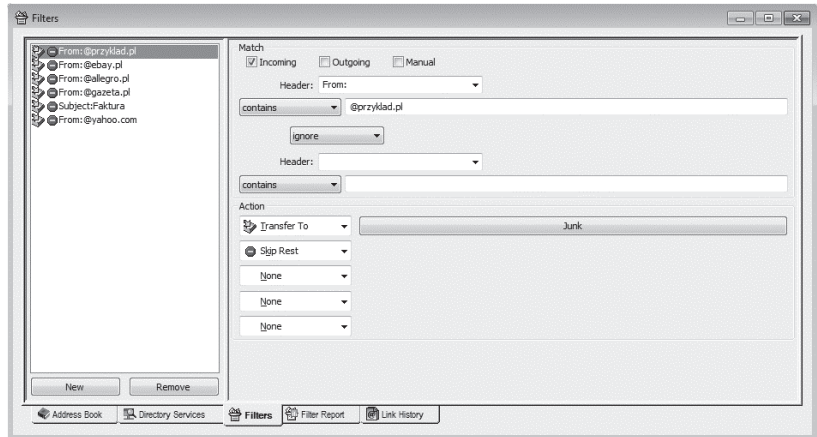
Najbardziej znane klienty poczty elektronicznej to następujące programy: @mail, Eudora, Gnus, Novell GroupWise, IBM Lotus Notes, Kerio WebMail, Apple Mail, Microsoft Entourage (dla komputera Macintosh), Microsoft Office Outlook, Outlook Express, Pine, Mozilla Mail & Newsgroups, Mozilla Thunderbird, Netscape Messenger, Novell Evolution, Opera Mail, SeaMonkey Mail & Newsgroups oraz Squirrelmail.

Niektóre z najprzydatniejszych funkcji znajdujących się w programach pocztowych to:

- ♦ **Szyfrowana baza danych.** W ten sposób plik bazy danych zostaje zabezpieczony przed jego przeglądaniem z zewnątrz.
- ♦ **Indeksowane wyszukiwanie.** Klient poczty przeprowadzający indeksowanie treści w bazie danych pozwala na bardzo szybkie wyszukiwanie. Niektóre z takich programów indeksują dane IMAP, jak również przechowywane w lokalnej bazie danych.
- ♦ **Generowanie wiadomości HTML.** Ta funkcja pozwala na wyświetlenie wiadomości e-mail tak, jakby była stroną internetową. Podczas wyświetlenia takich wiadomości z osadzoną treścią występuje takie samo ryzyko jak w trakcie pracy z przeglądarką internetową.
- ♦ **Blokowanie wyświetlania obrazów.** Oznacza to możliwość wyświetlenia jedynie informacji o obrazie zamiast samego obrazu. Powoduje to skrócenie czasu pobierania wiadomości i chroni przed kliknięciami w niechciane treści.
- ♦ **Filtrowanie spamu.** Ogólnie rzecz biorąc, filtrowanie zawsze jest cenną funkcją. Pozwala na przekierowanie wiadomości e-mail do określonej skrzynki pocztowej na podstawie wybranych kryteriów. Filtr spamu to aktywny mechanizm sprawdzający wiadomość na podstawie zestawu kryteriów i umieszczający ją w skrzynce pocztowej zawierającej spam. Najlepsze filtry antyspamowe używają filtru Bayesian, który uczy się wraz z każdą wiadomością zaklasyfikowaną jako spam i dodaje podobne do listy spamu. Mechanizm filtrowania w Eudorze został pokazany na rysunku 24.6.

### Rysunek 24.6.

*Okno dialogowe tworzenia filtra w programie pocztowym Eudora*



- ♦ **Ochrona przed phishingiem.** To narzędzie uniemożliwia wyświetlanie użytkownikowi łączy z witryn, na których może dojść do przechwycenia informacji użytkownika. Tego rodzaju filtry działają najczęściej na zasadzie czarnych list.
- ♦ **Szablony wiadomości.** Szablony to dokumenty, które można wykorzystać jako wzorce tworzonych wiadomości e-mail.
- ♦ **Szyfrowanie.** Wiele programów pocztowych obsługuje szyfrowanie, stosując własne rozwiązania lub bazujące na otwartych standardach, na przykład PGP (Pretty Good Privacy), OpenPGP, bądź wykorzystując S/MIME (Secure MIME).

- ♦ **Obsługa skryptów.** Oznacza to możliwość tworzenia akcji w postaci skryptów VBScript, JavaScript, Python, Java, PHP i innych. Funkcja ta pozwala użytkownikom zaawansowanym na dodatkową automatyzację klienta poczty. Automatyzacja obejmuje dodawanie podpisu, przeprowadzanie operacji wyszukiwania i zastępowania, modyfikację listy adresowej itd.

## Podsumowanie

Poczta elektroniczna to jedna z najważniejszych usług sieciowych w internecie, oferowana użytkownikom przez protokół IP. Bazuje na trzech ważnych protokołach, które zostały omówione w rozdziale: Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) oraz Internet Message Access Protocol (IMAP). Przedstawiono także metodę używaną do wysyłania wiadomości z jednego klienta poczty do drugiego za pomocą wymienionych usług.

Wiadomości e-mail mają określoną formę i gdy są wysyłane przez SMTP, są formatowane z wykorzystaniem mechanizmu typów MIME. W rozdziale omówiono sposób działania typów MIME oraz kodowania danych przeznaczonych do transferu przez internet.

Zaprezentowano również różne serwery poczty oraz wymieniono programy pocztowe.

W kolejnym rozdziale będzie omówione strumieniowanie dźwięku, wideo oraz innych rodzajów mediów. Usługi strumieniowania pozwalają na transfer w czasie rzeczywistym danych wymagających plików o dużych rozmiarach. Przedstawione będą również specjalne techniki stosowane podczas dostarczania usług strumieniowania.

# Rozdział 25.

# Strumieniowanie multimedialnych

## W tym rozdziale:

- ♦ W jaki sposób strumienie dostarczają multimedia użytkownikom?
- ♦ Strumieniowanie kontra pobieranie progresywne
- ♦ Architektura i protokoły sieci strumieniowania
- ♦ Emisja pojedyncza kontra multiemisja
- ♦ Odtwarzacze, kodeki oraz oprogramowanie serwerowe do strumieniowania

Strumieniowanie multimedialnych to technologia sieciowa pozwalająca wysyłać do użytkownika treść multimedialną, która może być odtwarzana na jego komputerze. Strumieniowanie jest powiązane ze specjalnym rodzajem serwera nazywanego *serwerem strumieniowania*. Powiązana technologia *pobieranie progresywne* pozwala na wykorzystanie serwerów WWW do rozprowadzania plików multimedialnych.

Strumieniowanie treści może wykorzystywać ogromną część dostępnych zasobów sieciowych. W celu utworzenia treści, udostępnienia jej w serwerze, a następnie przekazania jej klientom wymagane jest utworzenie odpowiedniej architektury sieci. Wszystkie rozwiązania strumieniowania używają zestawu protokołów pomagających w pakowaniu plików, kontrolowaniu ruchu multimedialnego oraz zarządzaniu nim. W rozdziale będą omówione cztery standardowe protokoły IETF — *Real-Time Streaming Protocol*, *Real-Time Control Protocol*, *Real-Time Transport Protocol* oraz język znaczników SMIL. Wyjaśniona będzie również różnica między emisją pojedynczą i multiemisją oraz zostaną przedstawione różne systemy dostarczania multimedialnych.

W celu przygotowania treści do strumieniowania bądź pobierania progresywnego pliki multimedialne muszą być zakodowane. Proces ten polega na pobraniu plików źródłowych, a następnie ich odpowiednim skompresowaniu, podzieleniu na segmenty i utworzeniu danych wyjściowych w zależności od potrzeb oprogramowania udostępniającego. Kodowanie polega na utworzeniu treści, która ma stałą albo zmienną wartość bitrate, jak również na utworzeniu pakietu strumieni o różnych wartościach bitrate.

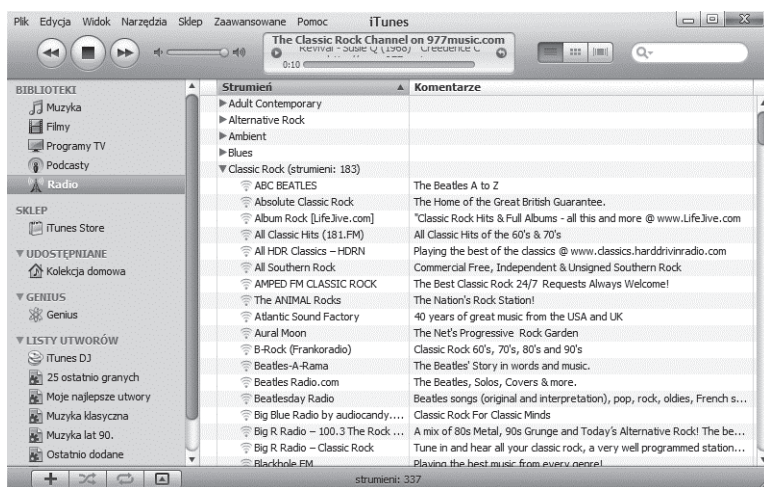
Obecnie są używane cztery główne platformy strumieniowania multimediów: Windows Media Services, RealNetworks Helix Server, Apple QuickTime Streaming Server oraz Adobe Flash Media Streaming Server. Wszystkie wymienione serwery stosują własne formaty, ale działają także z różnymi innymi formatami (z wyjątkiem Flasha).

Adobe Flash to oprogramowanie animacyjne, dostarczające treści stronom internetowym. Flash może zawierać w sobie różne multimedia. Technologia Flash jest niemal wszechobecna w internecie i stosowana w wielu odtwarzaczach multimediów osadzonych na stronach internetowych. Firma Microsoft opracowała alternatywną technologię, Silverlight, która oferuje te same możliwości, ale bazuje na silniku Windows Presentation Foundation (WPF) oraz platformie .NET.

## W jaki sposób działa strumieniowanie?

Strumieniowanie multimediów to dostarczanie treści w czasie rzeczywistym, po jednym fragmencie w danym czasie. Podczas odtwarzania klipu wideo na witrynie *YouTube.com* bądź odcinka programu na witrynie *ABC.com* użytkownik ogląda wideo strumieniowane przez internet. Strumieniowanie obejmuje również odtwarzanie muzyki, audycji radia internetowego, na przykład LastFM w odtwarzaczach multimedialnych takich jak iTunes (zob. rysunek 25.1), oraz przeglądanie wykładów, które mogły zostać pobrane na przykład z uniwersytetu Berkeley lub MIT. Nauka na odległość to rewolucja w edukacji — takie możliwości stwarza technologia omawiana w tym rozdziale.

**Rysunek 25.1.**  
*Radio internetowe odtwarzane w programie Apple iTunes to w przeciwieństwie do podcastów treść strumieniowana*



## Strumieniowanie kontra pobieranie progresywne

Strumieniowanie jest używane w celu przekazywania treści przez sieć; treść ta następnie jest odtwarzana w częściach, kiedy dostarczane są kolejne fragmenty. Pojęcie „strumieniowanie” odnosi się do sposobu, w jaki treść jest przesyłana — jest odbierana w postaci strumienia pakietów. Ujmując to nieco dokładniej, strumieniowanie występuje wtedy, gdy multimedia są wysyłane z serwera strumieniowania do klienta i odtwarzane przez program

z bufora w pamięci, w którym te dane są przechowywane. Podczas odtwarzania strumieniowanej treści program odtwarzający odrzuca wyświetloną już treść. Oznacza to, że strumieniowana treść nigdy nie istnieje w postaci pełnego pliku, który można zapisać na dysku twardym i odtworzyć później w dowolnej chwili. Ta cecha jest cenna z punktu widzenia twórcy lub dostawcy treści, ponieważ chroni jego własność przez znaczne utrudnienie powielania materiału.



Istnieją metody umożliwiające zapisanie strumieniowanej treści za pomocą narzędzi firm trzecich, na przykład w plikach FLV. Zostanie to przedstawione w dalszej części rozdziału.

Nie ma możliwości, aby oprogramowanie DRM (ang. *Digital Rights Management*) mogło chronić treść przed tymi, którzy chcą ją kopiować. W pewnym momencie treść musi być przesłana do analogowego urządzenia odtwarzającego (głośnika czy monitora) jako dane wyjściowe. Może być wówczas nagrana (co prawda jej jakość będzie obniżona) za pomocą kamery, mikrofonu lub przekazana do innego komputera jako dane wejściowe. Dotyczy to również treści strumieniowanej, ponieważ to po prostu inna metoda odtwarzania. Problem ten nosi nazwę „dziury analogowej”. Możliwe jest oznaczenie treści w taki sposób, aby jej kopia została rozpoznana po dokładniejszej analizie, jednak dla przeciętnego odbiorcy nie będzie niczym się różniła od oryginału (poza ewentualnym obniżeniem jakości zapisu).

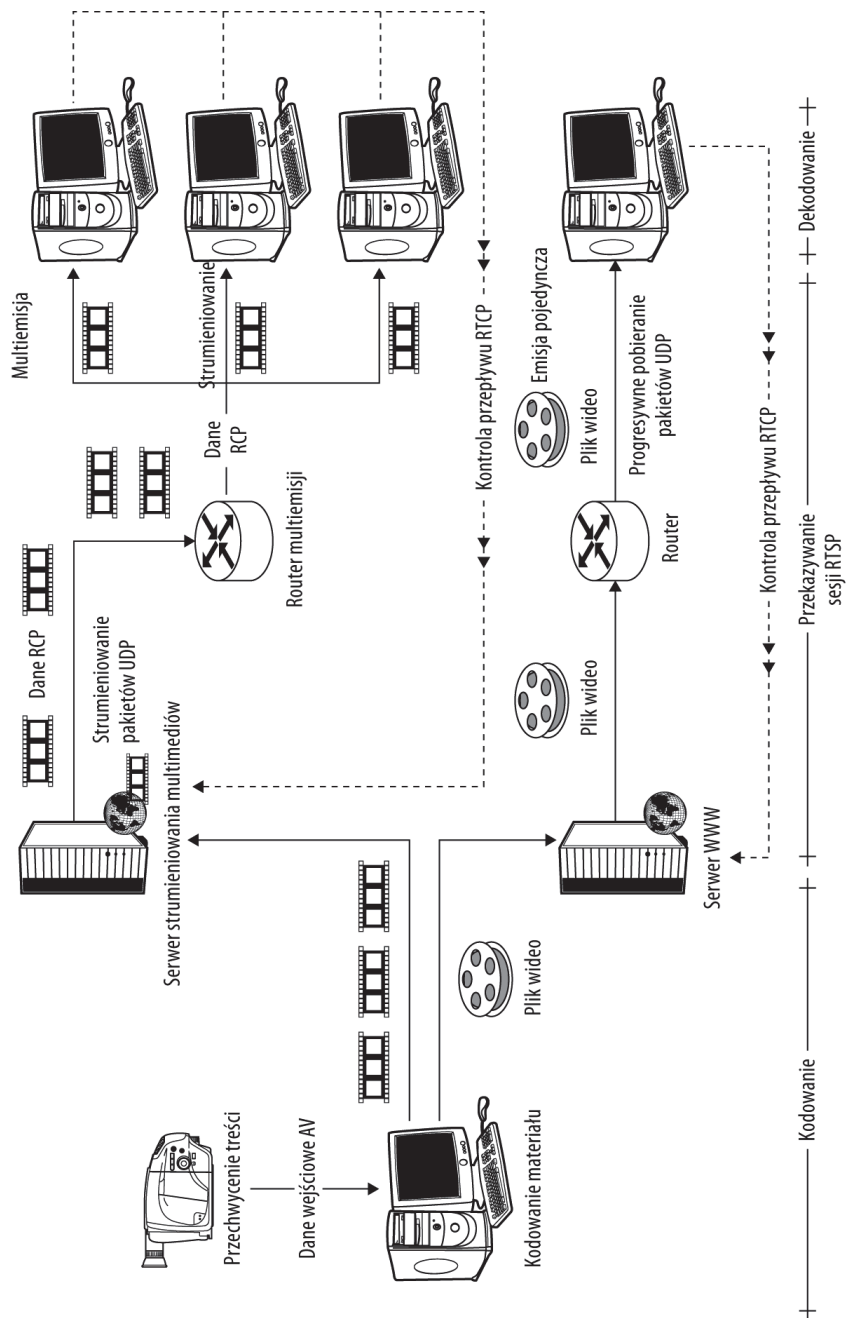
Z kolei pobieranie progresywne polega na tym, że treść z serwera WWW jest dostarczana klientowi, na którym może być odtwarzana w miarę odbierania przez niego kolejnych fragmentów bądź dopiero po pobraniu całości określonego materiału. Technologie RealNetworks i Windows Media stosują strumieniowanie treści, podczas gdy odtwarzacze QuickTime i Flash używają pobierania progresywnego. Większość odtwarzaczy ma możliwość odtwarzania treści dostarczanej przy użyciu obu metod transmisji. Na rysunku 25.2 pokazano schemat zawierający różne komponenty strumieniowania i pobierania progresywnego za pomocą protokołu RTSP (*Real-Time Streaming Protocol*) do sieciowej kontroli strumieniowanych multimediów. Protokół RTSP używa systemu przekazywania wiadomości RTCP (*Real-Time Control Protocol*) i dzieli pliki na pakiety RCP (*Real Control Packets*). RTSP to standard IETF (ang. *Internet Engineering Task Force*) zdefiniowany w dokumencie RFC 2326; będzie przedstawiony dokładniej w dalszej części rozdziału.

Na rysunku 25.2 przechwycona treść jest przekazywana stacji kodującej, w której następuje konwersja plików multimedialnych. Proces kodowania powoduje konwersję pliku na określony format łatwy w wysłaniu. Przykładem formatu kodowania jest popularny H.264. Zakodowany plik może być wysłany do serwera WWW (pokazany na rysunku), a następnie transmitowany klientom przy użyciu emisji pojedynczej (1:1) przez sieć. Ten rodzaj transferu plików może być kontrolowany przez system klienta (prawy dolny róg) o nazwie RTCP (*Real-Time Control Protocol*), stosowany przez klienta do monitorowania przepływu pakietów.

Alternatywne rozwiązanie zostało pokazane na górze rysunku 25.2. Zakodowany plik jest wysyłany do serwera strumieniowania multimediów, gdzie jest dzielony na pakiety i udostępniany jako strumień danych RCP. Fragmenty pliku wideo są wysyłane do routera multimedialnego, za którego pomocą mogą być jednocześnie wysyłane do wielu klientów. Multimedialny również może być kontrolowany przez wiadomości RTCP. Klient dekoduje plik multimedialny, a następnie przywraca ten plik do jego formatu rodzimego w celu odtworzenia.

**Rysunek 25.2.**

Różne  
komponenty  
strumieniowania  
i pobierania  
progresywnego



Wielu użytkowników może nie zauważyć różnicy pomiędzy strumieniowaniem i pobieraniem progresywnym, ponieważ obie metody dostarczają treść, która po odtworzeniu może być taka sama w obu przypadkach. Mało tego, pobieranie progresywne czasami jest uznawane

za pseudostrumieniowanie lub, jak w odtwarzaczu Apple QuickTime, za strumieniowanie z szybkim rozpoczęciem odtwarzania. Główna rozbieżność między tymi dwiema metodami polega na różnicy w zachowaniu się przewijania do przodu, do tyłu i kontroli nawigacji oraz na tym, że pobieranie progresywne powoduje zapisanie na lokalnym dysku twardym kopii pobieranej treści. Pobieranie progresywne pozwala na odtworzenie treści jedynie po kolei, od początku do końca, choć istnieje możliwość przechodzenia do początku i końca tego fragmentu pliku, który został już pobrany i umieszczony w buforze. Treść strumieniowana może być odtwarzana bez zachowania kolejności, ale przy założeniu, że fragment, który użytkownik chce odtworzyć, został już pobrany.

Czytelnik może spotkać się z pojęciami „strumieniowanie HTTP” lub „serwer WWW strumieniowania” — każde oznacza inną wersję pobierania progresywnego. W obu przypadkach podczas pobierania powstaje w lokalnym buforze kopia pliku multimedialnego, która może zostać zapisana przez użytkownika. Kolejna różnica między pobieraniem progresywnym i strumieniowaniem HTTP polega na tym, że użycie strumieniowania HTTP przez port 80 sprawia, że treść znacznie łatwiej przechodzi przez zaporę sieciową niż w przypadku innych metod transmisji.

Relacje z różnych wydarzeń mogą być strumieniowane w czasie rzeczywistym bądź dostarczane w postaci video na żądanie (ang. *Video on Demand*, VOD). Kiedy relacja jest transmitowana przez sieć IP niemal w czasie rzeczywistym, to bywa określana mianem „Live-Live” lub znacznie częściej jako Webcast. Video na żądanie oznacza, że treść została nagrana, jest przechowywana na serwerze i mogła zostać poddana edycji.

W tabeli 25.1 przedstawiono obie omawiane technologie: strumieniowanie i pobieranie progresywne.

**Tabela 25.1.** Strumieniowanie kontra pobieranie progresywne

Funkcja	Pobieranie progresywne	Strumieniowanie
Publiczne udostępnienie	Serwer WWW	Serwer strumieniowania
Najlepsze dla...	Odtworzenie przechowywanej treści	Video na żądanie (VOD), transmisja na żywo
Przepustowość	Brak wrażliwości na warunki sieciowe, zagubione pakiety są ponownie transmitowane	Wrażliwość na warunki sieciowe, zagubione pakiety nie są odtwarzane
Zapory sieciowe	Przyjazne zachowanie względem zapory sieciowej	Przez większość czasu wymaga otwarcia specjalnego portu
Kontrola odtwarzania	Konieczność odtwarzania po kolei	Możliwość przejścia do przodu, jeżeli treść znajduje się w buforze
Kopia	Kopia pozostaje na dysku twardym	Nie jest tworzona żadna kopia
Ochrona treści	Nie	Tak
Casting	Tylko emisja pojedyncza	Obsługiwana multemisja

Możliwość tworzenia sekwencji z grupy plików może być skryptowana w niektórych produktach, na przykład w Adobe Flash. Pliki specjalne, nazywane plikami SMIL (ang. *Synchronized Markup Integration Language*), określające sekwencję, pozwalają również na koordynację ponownego ich odtwarzania. (Pliki SMIL zostaną omówione w dalszej części rozdziału). Jedną z technik stosowanych wraz ze strumieniowaniem treści jest plik typu pre-roll. Plik ten może być używany do przedstawiania materiału reklamowego, informowania widza o treści, która zostanie wyświetlona (na wypadek, gdyby chciał on zrezygnować z jej obejrzenia), oraz służyć do wielu innych celów.

## Emisja pojedyncza kontra multiemisja

Strumieniowanie jest technologią dwupunktową. Serwer definiuje jeden punkt końcowy połączenia, dostarczając treść, natomiast odtwarzacz klienta bądź przeglądarka internetowa definiuje drugi punkt końcowy. Kiedy serwer multimediów mapuje pojedynczy strumień między dwoma punktami końcowymi, to jest to nazywane *emisją pojedynczą*. Emisję pojedynczą można potraktować jako odpowiednik wiadomości prywatnej. Emisja pojedyncza to *narrowcasting*; nadawca ma możliwość dostosowania wiadomości do odbiorcy i zachowuje unikalną kontrolę nad wiadomością, ale z towarzyszącym temu kosztem. Kiedy dostawca treści używa jednego strumienia w celu dostarczenia wiadomości wielu odbiorcom, to technologię tę określa się *multiemisją*. Multiemisja pozwala na utworzenie jednej stałej wiadomości i zastosowanie korzyści skali.



Wiadomości RSS nie są uznawane za aplikację strumieniowania multimediów, ponieważ cały plik musi być dostarczony przed jego użyciem. RSS to usługa subskrypcji bazująca na specyfikacji zawartej w pliku XML albo w pliku tekstowym RSS.

W tabeli 25.2 wymieniono pewne ważne różnice między strumieniowaniem emisji pojedynczej i multiemisji.

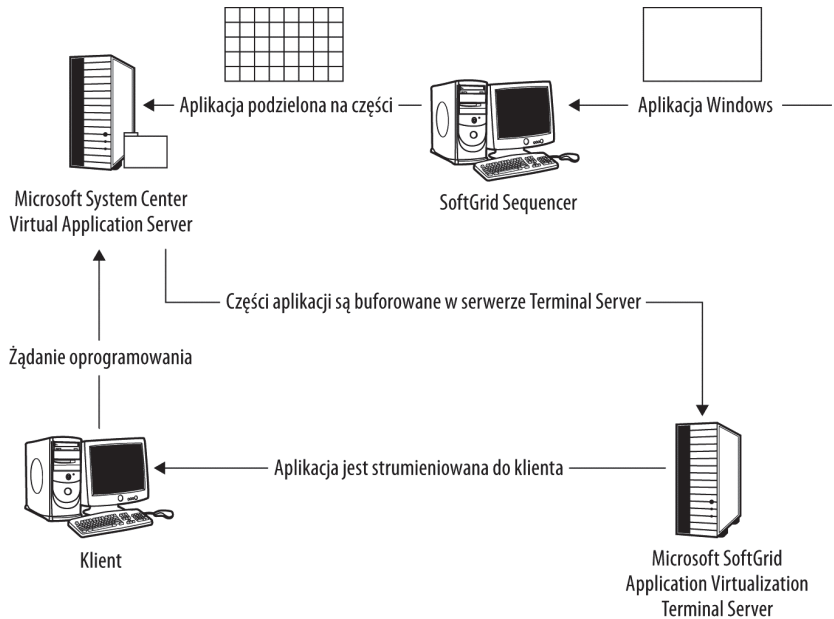
**Tabela 25.2.** *Emisja pojedyncza kontra multiemisja*

Funkcja	Emisja pojedyncza	Multiemisja
Najlepsze dla...	Na żądanie	Transmisja na żywo lub zaplanowana
Wymagania dotyczące przepustowości	Ogromna pojemność dla wielu strumieni	Mała pojemność dla jednego strumienia
Wymagania dotyczące procesora	Duże obciążenie procesora związane z obsługą poszczególnych strumieni	Małe obciążenie procesora związane z obsługą jednego strumienia
Odtwarzanie u klienta	Odtwarzacze zachowują kontrolę nad odtwarzaniem poszczególnych strumieni	Odtwarzacze otrzymują tę samą treść, mają takie same możliwości i czas
Wymagania dotyczące infrastruktury	Przepustowość, którą można poddać skalowaniu	Router (routery) obsługujący multiemisję
Kontrola wiadomości	Wysoka	Niska

Strumieniowanie odgrywa ważną rolę w wielu technologiach przemysłowych. Produkty takie jak Altiris Software Virtualization Solution (SVS), aplikacja serwera strumieniowania Citrix XenApp oraz Microsoft SoftGrid (wraz z technologią Zero Touch) to przykłady rozwiązań bazujących na treści strumieniowanej z serwerów rozproszonych. Wszystkie wymienione systemy pozwalają programistom na implementację oprogramowania i treści przy zastosowaniu topologii multiemisji.

W przypadku produktu SoftGrid aplikacja jest dostarczana w sposób umożliwiający jej działanie w systemie klienta, jeszcze zanim w całości zostanie przekazana temu klientowi; jest to forma wirtualizacji aplikacji. Aplikacja jest przygotowywana przez SoftGrid Sequencer, przeprowadzający jej dekonstrukcję przez określenie jej ustawień systemowych, używanych plików DLL i INI oraz innych elementów. Następnie w pierwszej części strumienia wysyłane są fragmenty wymagane do uruchomienia aplikacji. Klient jako pierwszy żąda aplikacji, jest to zatem technologia pobierania z serwera. Na rysunku 25.3 pokazano implementację używającą Microsoft System Center Virtual Application Server.

**Rysunek 25.3.**  
*Strumieniowanie aplikacji za pomocą SoftGrid*



Systemy strumieniowania Citrix XenApp, Altiris SVS i powiązane z nimi technologie wykorzystują pobieranie z serwera. Kiedy system staje się dostępny, to jest inwentaryzowany przez agenta bądź inną metodę, a następnie dochodzi do implementacji wymaganego oprogramowania. Wszystkie wymienione systemy działają w sieciach IP, ale ogólną regułą jest to, że do strumieniowania multimediów nie używają standardów otwartych, które będą przedstawione w dalszej części rozdziału. Do koordynacji systemu, udzielania odpowiedzi oraz dla plików odpowiedzi stosują zwykle format XML, natomiast do wysyłania strumieni wykorzystują metody własnościowe.

## Protokoły strumieniowania

Strumieniowanie treści multimedialnej obejmuje dostarczanie plików i ich kontrolę. Pliki te są dzielone na segmenty, aby można było łatwiej je dostarczać. W sieciach IP organizacja IETF ma kilka zdefiniowanych protokołów standardowych używanych do strumieniowania treści. W podrozdziale będą omówione cztery najważniejsze standardy: RTSP, RTP, RTCP oraz język znaczników SMIL.

Wymienione protokoły kontrolują dostarczanie treści, czynniki sieciowe takie jak *Quality of Service* (jakość usługi) i przeciążenie itp. Protokoły te przeprowadzają strumieniowanie przez sieci TCP/IP. W większości przypadków do celów transportowych stosują protokół UDP (*User Datagram Protocol*), ale w pewnych sytuacjach używany jest również protokół TCP (*Transport Control Protocol*).

### Protokół Real-Time Streaming Protocol

*Real-Time Streaming Protocol* (RTSP) to protokół warstwy aplikacji wykorzystywany do nadzorowania sposobu, w jaki odtwarzacz multimediiów może kontrolować strumień przychodzący z serwera strumieniowania. Protokół ten bazuje na dokumencie IETF RFC 2326. RTSP wykorzystuje port 554. Za pomocą identyfikatora sesji protokół RTSP śledzi stan sesji. Każda wiadomość wysyłana od klienta do serwera i na odwrót odwołuje się do wspomnianego identyfikatora.

Protokół RTSP najlepiej potraktować jako zestaw poleceń przygotowanych dla odtwarzacza, za których pomocą może on wydawać serwerowi strumieniowania multimediiów polecenia takie jak „odtwarzaj” lub „zatrzymaj”. RTSP nie odgrywa żadnej roli w segmentowaniu, kodowaniu lub transportowaniu treści. Funkcje te są obsługiwane przez inne protokoły, które doskonale współpracują z RTSP. Jednym z powszechnie stosowanych protokołów do strumieniowania multimediiów za pomocą RTSP jest omówiony w kolejnym podrozdziale *Real-Time Transport Protocol* (RTP).

Najważniejsze polecenia RTSP to między innymi:

- ♦ **PLAY** — nakazuje odtwarzaczowi rozpoczęcie odtwarzania strumienia. Istnieje możliwość kolejkwania poleceń **PLAY** oraz wskazania punktu, od którego ma się rozpocząć odtwarzanie. Wydanie polecenia **PLAY** dla strumienia, dla którego wcześniej wydano polecenie **PAUSE**, powoduje ponowne rozpoczęcie odtwarzania. Wiele poleceń **PLAY** w stosunku do jednego adresu powoduje, że odtwarzacz wyświetla wszystkie wskazane strumienie multimediiów.
- ♦ **PAUSE** — powoduje wstrzymanie odtwarzania strumienia multimediiów. Polecenie **PLAY** umożliwia kontynuację odtwarzania strumienia od miejsca, w którym nastąpiło wstrzymanie.
- ♦ **SETUP** — tworzy połączenie dla strumienia i musi zostać wydane przed rozpoczęciem odtwarzania. Polecenie **SETUP** zawiera w sobie adres URL oraz protokół transportowy, jak również numer portu używanego do otrzymywania RTP audio bądź wideo oraz inne metadane transportu RTCP.

- ♦ TEARDOWN — powoduje zakończenie sesji. Po jego wydaniu następuje zakończenie transmisji strumienia multimediów oraz pozbycie się wszystkich danych sesji z bufora serwera.
- ♦ DESCRIBE — zawiera RTSP URL (`rtsp://...`) oraz typ strumieniowanego pliku multimediów, który ma być odtworzony.
- ♦ RECORD — nakazuje wysłanie strumienia do serwera w celu jego przechowywania.

Wymienione tutaj serwery strumieniowania multimediów używają protokołu RTSP: Apple QuickTime Streaming Server, Darwin Streaming Server (open source QuickTime Streaming Server), Alcatel-Lucent pvServer (znany jako PacketVideo Streaming Server), RealNetworks Helix DNA Server, Live555 (open source), VideoLAN, Windows Media Services oraz Maui X-Stream VX30.

## Protokół Real-Time Transport Protocol

Protokół *Real-Time Transport Protocol* (RTP) to metoda wysyłania przez internet pakietów zawierających multimedia. Standard IETF został opisany w dokumentach RFC 1889 i 3550. Protokół RTP jest zwykle wykorzystywany w połączeniu z RTSP (jak wspomniano w poprzednim podrozdziale) i wraz z nim stanowi parę protokołów stosowanych do transportu VoIP, co będzie pokrótce omówione w kolejnym rozdziale. RTP jest stosowany w aplikacjach zarówno emisji pojedynczej, jak i multiemisji. W użyciu pozostaje również skompresowany RTP (CRTP), zdefiniowany w dokumencie RFC 2509, oraz rozszerzony RTP (ERTP).



RealNetworks ma wersję protokołu RTP o nazwie *Real Data Transport* (RDT), który działa z serwerem RealNetworks RTSP.

Transport RTP w sieci IP może być przeprowadzany przez TCP lub UDP. Protokół TCP jest wykorzystywany, kiedy wymagana jest gwarancja dostarczenia, podczas gdy protokół UDP jest stosowany, kiedy można tolerować zagubienie pewnej ilości danych. Transport RTP strumieniowanych multimediów używa UDP i może być przypisany do dowolnego portu w zakresie dynamicznym od 16 384 do 32 767. Zgodnie z konwencją kolejny nieparzysty numer portu jest przypisywany do wymiany wiadomości RTSP.

Użycie portu dynamicznego bardzo często powoduje trudności podczas przejścia przez zaporę sieciową. W celu rozwiązania tego problemu można wykorzystać serwer STUN (*Simple Traversal of User Datagram through NAT (Network Address Translators)*), dostarczający mechanizm pozwalający na przejście przez zaporę sieciową. Serwer STUN działa przez użycie serwerów po obu stronach zapory sieciowej w celu nasłuchiwania na otwartych portach. Jeżeli przejście przez zaporę sieciową z zewnątrz będzie niemożliwe, to STUN może wykonać z wewnątrz żądanie do systemu dotyczące pakietów znajdujących się na zewnątrz.



Serwer STUN znacznie dokładniej będzie omówiony w rozdziale 26.

RTP jest odpowiedzialny za następujące zadania:

- ♦ Identyfikacja treści.
- ♦ Używanie identyfikacji sekwencji na poziomie pakietu — *Protocol Data Unit* (PDU).

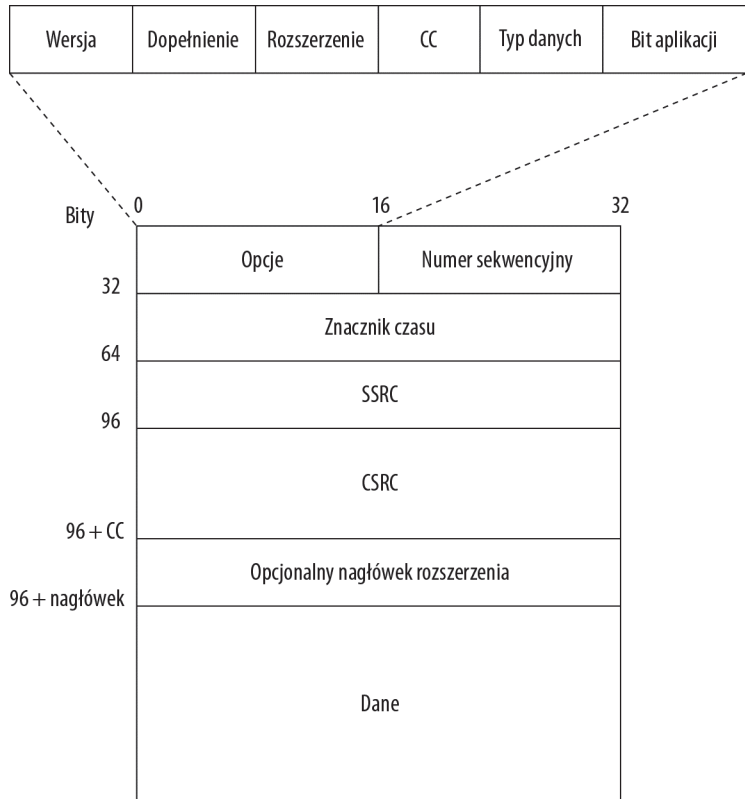
- ♦ Zarządzanie strumieniami za pomocą CSRC (ang. *Contributing Source ID*) w celu dopasowania strumienia do jednego lub więcej źródeł. Możliwość zarządzania oddzielnymi strumieniami pozwala na oddzielną obsługę audio i wideo, co może okazać się przydatne w wielu sytuacjach.
- ♦ Synchronizacja czasu za pomocą SSRC (ang. *Synchronization Source ID*).
- ♦ Sprawdzanie dostarczenia pakietu. Protokół RTSP jest używany w celu monitorowania parametrów jakości usługi (QoS).

PDU (ang. *Protocol Data Unit*) to numery identyfikacyjne przypisane do poniższych funkcji: dla 1. warstwy modelu OSI numer PDU jest przypisany bitowi, dla 2. warstwy modelu OSI numer PDU jest przypisany ramce, dla 3. warstwy modelu OSI numer PDU jest przypisany pakietowi, dla 4. warstwy modelu OSI numer PDU jest przypisany segmentowi, dla warstw od 5. do 7. modelu OSI numer PDU jest przypisany danym. Podobna koncepcja, SDU (ang. *Service Data Unit*), to numer SDU przypisywany danym, które jeden system wysyła do innego na warstwy o jeden niższej. Dla PDU dla  $n$  wartość SDU wynosi  $n-1$ .

Na rysunku 25.4 pokazano strukturę pakietu RTP. Pakiet zawiera w nagłówku wiele opcji (rozszerzona część pakietu) umożliwiających wskazanie typu rozszerzenia, identyfikatora pakietu, źródła oraz typu danych. W nagłówku RTP różne pola mają następujące przeznaczenie:

- ♦ **Wersja.** Bieżąca wersja protokołu; opcja wykorzystuje dwa bity (wersja 2.).
- ♦ **Dopelnienie.** Opcja w postaci pojedynczego bitu, wskazująca, czy na końcu pakietu znajdują się dodatkowe bajty.
- ♦ **Rozszerzenie.** Ta jednobitowa opcja wskazuje, czy istnieje charakterystyczny dla aplikacji Nagłówek rozszerzenia między nagłówkiem i danymi.
- ♦ **CC — Licznik CSRC.** To 4-bitowe pole określa liczbę identyfikatorów CSRC, które zostały dołączone za nagłówkiem.
- ♦ **Bit Aplikacji.** Jednobitowa opcja używana przez aplikację do wskazania, że dane są z jakiegoś względu ważne dla tej aplikacji.
- ♦ **Typ danych.** To 7-bitowe pole zawiera informacje o formacie danych.
- ♦ **Numer sekwencyjny.** 16-bitowe pole zawierające numer sekwencyjny pakietu danych RTP. System odbiorcy używa numeru sekwencyjnego w celu ułożenia danych we właściwej kolejności.
- ♦ **Znacznik czasu.** To 32-bitowe pole stosowane do synchronizacji odtwarzania treści po stronie odbiorcy.
- ♦ **SSRC.** Identyfikator SSRC pozwala na unikalne określenie źródła strumienia.
- ♦ **CSRC.** Wartość CSRC zawiera informacje o źródłach strumienia, jeżeli strumień pochodzi z co najmniej dwóch źródeł.
- ♦ **Opcjonalny nagłówek rozszerzenia.** Ma postać 32-bitowego słowa zawierającego identyfikator określonego profilu oraz długość rozszerzenia.

**Rysunek 25.4.**  
Struktura pakietu RTP



Protokół SRTP (*Secure Real-Time Transport Protocol*) to odmiana protokołu RTP, która definiuje metody służące do szyfrowania i uwierzytelniania danych RTP oraz sprawdzania błędów w strumieniach zarówno emisji pojedynczej, jak i multiemisji. Jest wykorzystywany wraz z *Secure RTCP*, czyli wersją protokołu RTCP stosującą wymienione środki bezpieczeństwa względem wiadomości używanych do kontroli ruchu SRTP. Uwierzytelnianie wiadomości jest wymagane w SRTP, ale wszystkie pozostałe funkcje SRTP pozostają opcjonalne. Ich implementacja zależy od aplikacji. Wymienione protokoły mogą być używane w aplikacjach zarówno VoIP, jak i strumieniowania multimediów.

## Protokół Real-Time Control Protocol

Ostatni z protokołów Real-Time będących w powszechnym użyciu to *Real-Time Control Protocol* (RTCP), zdefiniowany w dokumencie RFC 1889. Ten protokół warstwy sesji to system wymiany wiadomości zapewniający informacje na temat wydajności przepływu danych RTP. Jako taki RTCP można uznać za rodzaj wymuszenia funkcjonalności jakości usługi (QoS). RTCP monitoruje nadchodzące bajty i pakiety, liczbę pakietów, opóźnienie sieciowe oraz inne dane statystyczne. Aplikacje wykorzystujące RTCP mogą użyć tych danych statystycznych do zmiany swojego zachowania w odpowiedzi na zmiany wydajności strumienia, aby dopasować się dożądanego poziomu jakości usługi.

Pakiety RTCP to bardzo małe pakiety wiadomości. Przekazywane są wymienione poniżej typy pakietów:

- ♦ **Raporty nadawcy.** Te dane zawierają informacje o ilości danych wysłanych i odebranych wraz ze znacznikami czasu wymaganymi do synchronizacji pakietów RTP.
- ♦ **Raporty odbiorcy.** Ta wiadomość jest kierowana do klientów, które nie wysyłają pakietów RTP, i zawiera dane statystyczne dotyczące jakości usługi.
- ♦ **Charakterystyczne dla aplikacji.** Ten typ wiadomości może być używany przez aplikacje do zdefiniowania wiadomości przeznaczonych do stosowania przez daną aplikację.
- ♦ **Opis źródła.** Ten typ wiadomości identyfikuje źródło strumienia oraz dostarcza informacje szczegółowe dotyczące właściciela systemu źródłowego.
- ♦ **Do widzenia.** Ta wiadomość jest wysyłana, kiedy źródło powoduje zamknięcie strumienia.

Obecnie protokół RTCP nie może być w łatwy sposób zastosowany względem systemów udostępniających ogromne klipy wideo, na przykład IPTV (telewizja bazująca na protokole IP). Ogromna ilość danych prowadzi do dużych opóźnień w wysyłaniu danych statystycznych RTCP oraz opóźnień podczas analizy tych danych przed odbiorcą.

## Język Synchronized Markup Integration Language

SMIL (ang. *Synchronized Markup Integration Language*) to otwarty standard definiujący język znaczników bazujący na XML. Jego zadaniem jest obsługa skoordynowanego odtwarzania multimediów. SMIL działa na zasadzie danych wejściowych dla transportu RTSP, podobnie jak treść HTML stanowi dane wejściowe dla transportu HTTP. SMIL pobiera zakodowane pliki i określa kolejność ich odtwarzania. Dostępnych jest wiele edytorów SMIL pozwalających na tworzenie plików. W celu odtworzenia sekwencji SMIL odtwarzacz musi mieć wbudowaną obsługę SMIL. Przykładami edytorów SMIL są Adobe GoLive oraz SMOX Editor/SMOX Pad.

Plik SMIL (rozszerzenie *.smil* lub *.smi*) to metaplik wskazujący klientowi sposób obsługi danego strumienia. Plik ten definiuje na poziomie sesji pewną liczbę cech charakterystycznych dla połączenia. Podczas przechowywania wielu plików o różnych wartościach bitrate dla danego strumienia SMIL ma możliwość ustalenia, który plik będzie użyty dla danego strumienia. Inne opcje mogą wskazywać treść przygotowaną w innych językach, wybierać język na podstawie ustawień systemowych bądź wykorzystywać różne klipy wideo lub ścieżki dźwiękowe dla różnych użytkowników na podstawie innych kryteriów. SMIL można dołączyć do przycisków pozwalających na bezpośrednie nadanie formatu treści na podstawie działań użytkownika, który może włączać listy odtwarzania lub inne funkcje zmieniaacza automatycznego. Ponieważ SMIL to zestaw zewnętrznych poleceń kontrolujących treść, istnieje możliwość zastosowania go w celu zmiany sekwencji odtwarzania, zmiany punktów początkowych odtwarzania w ramach określonego klipu bądź wskazania dowolnej liczby innych strumieniowanych multimediów lub serwerów WWW.



Pliki języka znaczników SAMI (ang. *Microsoft Synchronized Accessible Media Interchange*) mają rozszerzenie *.smi*. Technologia ta jest używana do umieszczania napisów w odtwarzanych multimedialach.

Po otwarciu pliku SMIL w edytorze tekstowym można się przekonać, że jego składnia jest podobna do innych plików HTML. Plik SMIL musi rozpoczynać się i kończyć znacznikami odpowiednio <SMIL> i </SMIL>. Sekcja <HEAD> zawiera metadane oraz informacje warstwy prezentacyjnej. Sekcja <BODY> zawiera informacje dotyczące czasu oraz elementów multimedialnych. Natomiast sekcje <PAR> i <SEQ> (równolegle i kolejno) są używane w celu wskazania treści multimedialnych przez podanie ich adresów URL. Dzięki językowi SMIL można wskazać, że dany obiekt multimedialny jest powiązany z określonym poziomem dostępnej przepustowości.

## Kodowanie

Pliki multimedialne są zazwyczaj nagrywane w formatach specyficznych dla danego urządzenia, zapewniających wysoką jakość, które jednak są niepraktyczne w przypadku strumieniowania przez większość połączeń WAN, takich jak internet. W celu przygotowania plików w formatach dogodniejszych do strumieniowania pliki RAW są z reguły kompresowane. Zmniejszeniu ulega liczba ramek na sekundę oraz wartość bitrate dla dźwięku, co wiąże się z pogorszeniem jakości. Tak przygotowany plik jest następnie kodowany; proces ten najczęściej oznacza zastosowanie dużego stopnia kompresji.

Kodowanie to proces, w którego wyniku plik jest modyfikowany przez algorytm przeprowadzający jego kompresję. Natomiast dekodowanie to proces wyodrębnienia zakodowanego pliku. Program przeprowadzający kompresję nazywa się kodekiem (tzn. programem kodującym i dekodującym). Kodeki mogą być zaimplementowane bezpośrednio w sprzęcie, to znaczy w układach scalonych kart przechwytyjących audio i wideo. Istnieje możliwość przekodowania zakodowanego pliku z jednego formatu na inny. Proces kodowania i dekodowania najczęściej bardzo obciąża procesor; zakończenie tego procesu może wymagać dużej ilości czasu.

W tabeli 25.3 przedstawiono porównanie kodowania z użyciem pojedynczej oraz wielu wartości bitrate.

**Tabela 25.3.** Kodowanie z użyciem pojedynczej kontra wielu wartości bitrate

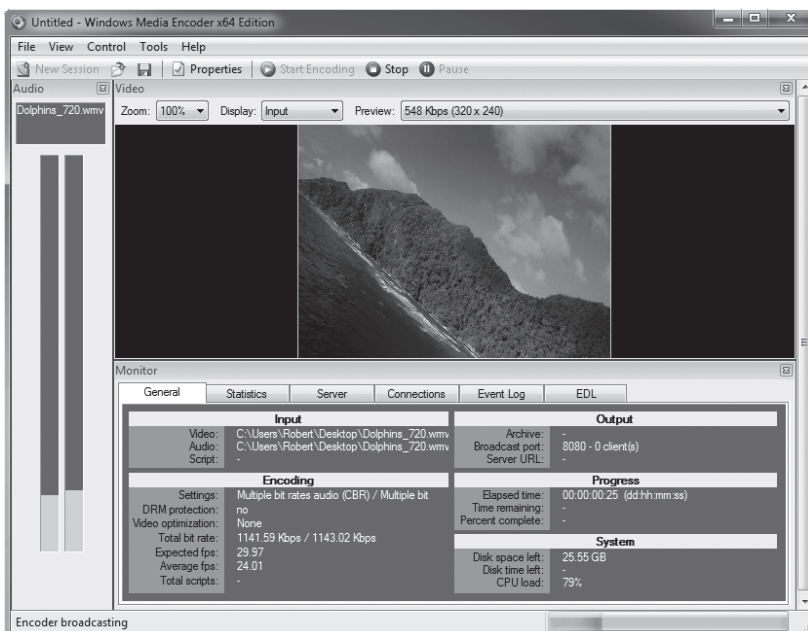
Funkcja	Emisja pojedyncza	Multiemisja
Publiczne udostępnienie	Przez strumieniowanie albo serwer WWW	Przez serwer strumieniowania wraz z obsługującym je oprogramowaniem
Wielkość	Pojedynczy plik	Wiele plików
Przepustowość	Możliwość zatrzymania lub przzerwania odtwarzania, gdy sieć jest przeciążona	Krótkie przerwy, kiedy strumień o różnych wartościach bitrate wypełniają bufor
Wielkość ramki	Wybierana na podstawie przepustowości	Wielkość ramki jest taka sama dla każdej wartości bitrate
Audio	Wybierane na podstawie przepustowości	Ustawienia audio muszą być takie same dla każdej wartości bitrate
Integracja z WWW	Konieczność posiadania poszczególnych kontrolki lub łączy dla oddzielnych strumieni	Pojedyncza kontrolka lub łącze dla wszystkich strumieni

Wprawdzie większość technik kodowania stosuje stały współczynnik bitrate dla danych wejściowych i wyjściowych, ale techniką szczególnie użyteczną pod kątem usprawnienia transmisji przez połączenia o małej przepustowości jest ta, która wykorzystuje kodowanie MBR (ang. *Multiple Bit Rate*). W kodowaniu MBR wiele strumieni zostaje zakodowanych z różnymi wartościami bitrate, a następnie strumienie te są łączone w pojedynczy plik. Klient obsługujący kodowanie MBR będzie negocjował z serwerem użycie strumienia o najlepszej wartości bitrate w zależności od dostępnej przepustowości łącza. Jeżeli przepustowość łącza ulegnie zmianie w trakcie transmisji, to klient może zażądać, aby serwer wysłał strumień o innej wartości bitrate.

W obrębie różnych technologii te inteligentne i adaptacyjne strumienie mają różne nazwy. RealMedia nazywa je SureStream, Microsoft określa je mianem Intelligent Streaming for Windows Media, natomiast Apple uznaje odmienne wartości bitrate za różne wersje filmu. Apple przechowuje strumienie o innych wartościach bitrate w oddzielnych plikach na komputerze Macintosh.

Na rysunku 25.5 pokazano program Windows Media Encoder 9 w trakcie kodowania pliku filmowego na postać strumienia. Firma Microsoft udostępniła ten kodek na swojej witrynie internetowej i można go używać wraz z Windows Media Player. Program Media Encoder ma możliwość przechwytywania treści odtwarzanej na żywo w celu jej późniejszego odtworzenia bądź strumieniowania. Inne możliwości programu to między innymi konwersja pliku na klip wideo, emitowanie relacji z wydarzeń na żywo oraz rejestrowanie wszystkiego, co dzieje się na ekranie. Ponadto obsługuje treść MBR (ang. *Multiple Bit Rate*), informacje DRM (ang. *Digital Rights Management*), a także kodowanie CBR (ang. *Constant Bit Rate*) i VBR (ang. *Variable Bit Rate*).

**Rysunek 25.5.**  
Program Windows Media Encoder 9 konwertuje pliki audio i wideo oraz inne dane wejściowe na postać treści gotowej do strumieniowania



Kodowanie CBR ma najlepsze zastosowanie w sesjach strumieniowania. Wartość bitrate zostaje ustawiona jako stała wraz z małym odchyleniem, dozwolonym przez wielkość bufora. Jakość treści zakodowanej za pomocą CBR jest zmienna, ponieważ stały pozostaje współczynnik wykorzystywanej kompresji. Niektóre ramki są bardziej skomplikowane i kompresują się znacznie gorzej niż prostsze ramki. Z powodu zmiany warunków dostarczania strumieni użytkownicy przekonują się, że jakość odtwarzanych strumieni CBR różni się między poszczególnymi sesjami. Strumienie o niższej wartości bitrate drastycznie zmniejszają jakość odtwarzanej treści.

Kodowanie VBR jest stosowane, gdy treść jest pobierana progresywnie lub odtwarzana lokalnie. Ten rodzaj kodowania lepiej pasuje do treści zróżnicowanej pod kątem stopnia skomplikowania. Poza tym prowadzi do powstania plików o mniejszej wielkości niż w przypadku kodowania CBR, bardzo często mniejszych nawet o 50%.

Poniżej przedstawiono listę najczęściej stosowanych programów i urządzeń kodujących:

- ♦ **Barix Instreamer.** Jest to rozwiązanie w postaci urządzenia sprzętowego typu „wszystko w jednym”, które pobiera dźwięk analogowy i cyfrowy, a następnie konwertuje go na postać strumieni MP3. Instreamer ma możliwość wysyłania strumieni do serwerów strumieniowania takich jak Icecast bądź SHOUTcast, w których treść będzie udostępniana urządzeniom sieciowym. Więcej informacji na temat tego urządzenia można znaleźć na witrynie <http://www.barix.com>.
- ♦ **Nicecast.** Program Nicecast jest używany w celu tworzenia strumieniowanej treści audio. Działa na platformie Mac OS X i jest dostępny na stronie firmy Rouge Amoeba pod adresem <http://www.rogueamoeba.com/nicecast>.
- ♦ **QuickTime Broadcaster.** Jest to rozwiązanie firmy Apple. Tworzy wideo MPEG-4, H.264 bądź wersję mobilną 3GP formatu MPEG-4 na komputerze Macintosh. Program jest dostępny na stronie <http://www.apple.com/quicktime/extending/resources.html> w postaci serwera QuickTime Streaming Server.
- ♦ **RealProducer.** RealProducer firmy RealMedia tworzy pliki w formacie RealAudio i RealVideo. Pozwala na tworzenie treści transmitowanej na żywo, jak również możliwej do pobrania, która następnie jest wykorzystywana w RealNetworks Helix Server. Wersję bezpłatną albo komercyjną kodeka można pobrać na stronie <http://www.realnetworks.com/products-services/realproducer.aspx>.
- ♦ **SAM.** Wtyczka DSP dla programu Winamp, umożliwiająca kodowanie dźwięku do plików w formatach MP3, Ogg i Windows Media. Można ją pobrać na stronie <http://www.spacialaudio.com/?page=winamp-plugins&>.
- ♦ **Windows Media Encoder.** Jak już wspomniano, program ten można pobrać ze strony firmy Microsoft pod adresem [http://www.microsoft.com/expression/products/Encoder4\\_Overview.aspx](http://www.microsoft.com/expression/products/Encoder4_Overview.aspx).
- ♦ **Wirecast.** Dostępny zarówno dla platformy Mac, jak i Windows. Pozwala na tworzenie plików zgodnych z architekturą QuickTime Streaming udostępnianych z serwera QuickTime Streaming Server bądź serwera Darwin. Wirecast jest dostępny na stronie <http://www.teletstream.net/wire-cast/overview.htm>.

## Serwery strumieniowania

Serwery strumieniowania są oferowane przez wielu różnych producentów oraz obsługują różnorodne technologie strumieniowania. Większość serwerów działa na pojedynczej platformie i oferuje jedno rozwiązanie. Niektóre działają na różnych platformach; kilka zapewnia także obsługę wielu technologii. Najczęściej używane serwery strumieniowania multimediów to między innymi:

- ♦ **Windows Media Services.** Serwer ten jest dostępny w postaci usługi instalowanej w Windows Server 2008, wcześniejsza wersja działała w Windows Server 2003. Edycja 2008 obsługuje treść odtwarzaną w Windows Media Player. Dostępne funkcje dodatkowe to szybkie rozpoczęcie odtwarzania, szybkie buforowanie (usługi buforowania i proxy), szybkie odzyskiwanie, szybkie ponowne połączenie, uwierzytelnianie, strumieniowanie za pomocą multimediami i emisji pojedynczej oraz emisja rozłożeniowa. Więcej informacji na temat tego serwera można znaleźć na stronie <http://www.microsoft.com/windows/windowsmedia/forpros/server/server.aspx>.
- ♦ **Helix Server.** Serwer Helix, obecnie w wersji 14., to obsługujący wiele platform i formatów serwer strumieniowania firmy RealNetworks. Obsługuje formaty RealAudio, RealVideo, Windows Media, QuickTime, MPEG-4, 3GPP (H.263/H.264) oraz MP3. Może działać w systemach Windows Server 2003, Red Hat Enterprise Level oraz Solaris (na platformie SPARC). Więcej informacji na temat serwera Helix można znaleźć na stronie <http://www.realnetworks.com/products-services/helix-server-proxy.aspx>.  
  
Firma RealNetworks zaprojektowała serwer Helix Proxy, który udostępnia usługi buforowania, proxy oraz bramy dla treści dostarczanej przez serwer Helix.
- ♦ **Apple QuickTime Streaming Server (QTSS).** Ten produkt Apple działa w serwerach Mac OS X; wraz z sekwencerem QTSS Publisher dostarcza treść QuickTime za pomocą protokołów RTP/RTSP. Technologia QuickTime pozwala na dostarczanie treści H.264, MPEG-4, 3GPP, MP3 oraz AAC, jak również plików MP3 z wykorzystaniem protokołów Icecast. Wersja 6. została zintegrowana z usługami Open Directory. Strona domowa serwera QTSS mieści się pod adresem <http://www.apple.com/quicktime/extending/resources.html>.
- ♦ **Adobe Flash Media Streaming Server 4 (FMSS).** Serwer FMSS dostarcza treść Flash zakodowaną w postaci wideo H.264 lub audio HE-AAC, która jest udostępniana jako strumień bądź pobieranie progresywne. Więcej informacji na temat tego serwera można znaleźć na stronie <http://www.adobe.com/products/flashmediastreaming>.
- ♦ **Wowza Media Server 2.** Serwer ten to znacznie tańsza alternatywa dla Adobe Flash Streaming Server; dostarcza strumieniową treść Flash utworzoną za pomocą kodeków innych niż Flash RTSP/RTP. Więcej informacji na temat tego serwera można znaleźć na stronie <http://www.wowzamedia.com/products.html>.
- ♦ **Darwin Streaming Server.** Darwin to wersja open source serwera QTSS firmy Apple. Opiera się na tym samym kodzie, na którym zbudowano QTSS, ale działa na platformach innych niż Macintosh — między innymi Linux, Windows i Solaris. Strona domowa serwera mieści się pod adresem <http://dss.macosforge.org>.
- ♦ **Icecast Streaming Media Server.** Icecast to rozwiązanie typu open source w postaci serwera strumieniowania multimediów, udostępnione przez Xiph.Org. Koduje

treść na postać Vorbis i strumieniuje ją przez HTTP. Ewentualnie treść może być zakodowana w MP3 i strumieniowana przez protokół SHOUTcast. Oprogramowanie można pobrać z witryny <http://www.icecast.org>.

- ♦ **Nullsoft SHOUTcast.** Serwer strumieniowania multimedialnych SHOUTcast jest używany do tworzenia cyfrowych plików dźwiękowych w formacie MP3 lub HE-ACC. Icecast to otwarta wersja tego oprogramowania. Program SHOUTcast jest dostępny bezpłatnie zarówno na platformę Mac, jak i PC. Oprogramowanie można pobrać z witryny firmy Nullsoft pod adresem <http://www.shoutcast.com/download>.
- ♦ **Telestream Agility.** Serwer ten stanowi kompletne rozwiązanie służące do produkcji wideo, oferuje serwer strumieniowania i pozwala na pracę z różnego rodzaju treścią. Z reguły jest wykorzystywany przez duże firmy zajmujące się multimediami i zawiera bogaty zestaw funkcji, takich jak księgowość, raportowanie i produkcja wideo. Strona domowa oprogramowania Agility mieści się pod adresem <http://www.telestream.net/agility/overview.htm>.
- ♦ **Unreal media Server.** Unreal to serwer własnościowy działający w systemie Windows. Pozwala na strumieniowanie treści Windows Media i QuickTime do przeglądarek internetowych zawierających aplikację Streaming Media Player, kontrolkę ActiveX lub odpowiednią wtyczkę. Bezpłatna wersja serwera obsługuje do piętnastu połączeń. Można ją pobrać z witryny <http://www.umediaserver.net>.

Uruchomienie niektórych z wymienionych serwerów może być trudne. Wiele z nich firmy udostępniają w postaci usług.

Podczas wyboru serwera trzeba wziąć pod uwagę m.in. przepustowość wymaganą do obsłużenia klientów. Minimalne wymagania dotyczące przepustowości dla poszczególnych typów połączeń zostały wymienione w tabeli 25.4. Wartości te muszą być *pomnożone przez liczbę klientów*, którzy mają być bezpośrednio obsługiwani. W celu obsługi obciążenia wykraczającego poza pojedyncze połączenie można wykorzystać zdalny bufor, serwery proxy oraz punkty przyłączeń stosowane jako elementy technologii strumieniowania.

W dalszej części rozdziału przedstawiono kilka różnych odtwarzaczy oraz formatów służących do strumieniowania multimedialnych. Czytelnik może już znać niektóre z wymienionych formatów strumieniowania, na przykład pliki Adobe Flash stosowane przez witrynę *YouTube.com*. Ten obszar technologii jest bardzo dynamiczny, a nowe produkty pojawiają się bardzo często. Przykładem nowego formatu strumieniowania multimedialnych jest Silverlight firmy Microsoft.

## Formaty strumieniowanych plików

Strumieniowane pliki multimedialne używają jednego lub więcej rozszerzeń dla plików odtwarzanych przez poszczególne odtwarzacze oraz jedno lub więcej rozszerzeń dla metaplików wymienionych w łączach na stronie internetowej, które inicjalizują strumień. Jeżeli plik docelowy jest wymieniony w znaczniku HTML `<a href>`, to po kliknięciu łączy plik ten będzie pobierany, a nie strumieniowany. Aby zainicjalizować strumień, jako łączą stosuje się metapliki. Są to najczęściej pliki tekstowe (na przykład XML lub SMIL) opisujące wykorzystywany rodzaj odtwarzacza, inicjujące strumień, a następnie wskazujące ten strumień odtwarzaczowi po stronie klienta.

**Tabela 25.4.** Minimalne wymagania dotyczące przepustowości serwera

Rodzaj strumienia	Bitrate	Jakość	Minimalny typ połączenia
Mowa	800 b/s	Minimum dla mowy	Komutowane
Mowa	8 kb/s	Telefon	Komutowane
Wideo	16 kb/s	Wideotelefon	Komutowane
Audio	32 kb/s	Radio AM (fale średnie)	Komutowane
Audio	96 kb/s	Radio FM	DSL/ISDN
Audio	128 – 160 kb/s	Standardowy odsłuch	DSL/ISDN
Wideo	128 – 384 kb/s	Wideokonferencja	Modem DSL/kablowy
Audio	192 kb/s	Emisja dźwięku cyfrowego	Modem DSL/kablowy
Audio	320 kb/s	CD	Modem DSL/kablowy
Audio	500 kb/s – 1 Mb/s	Dźwięk bezstratny (na przykład FLAC)	Modem DSL/kablowy
Wideo	1,25 Mb/s	Video CD (VCD)	Modem DSL/kablowy
Audio	1,41 Mb/s	Dźwięk PCM dla Compact Disk Digital Audio	Modem DSL/kablowy
Wideo	5 Mb/s	DVD	Modem DSL/kablowy
Wideo	15 Mb/s	HDTV	Modem DSL/kablowy
Wideo	54 Mb/s	Blu-ray	Modem DSL/kablowy



Więcej informacji szczegółowych na temat różnych formatów plików można znaleźć na witrynie <http://Filext.com>.

Zdarza się, że metaplik oraz strumieniowany plik multimedialny używają tego samego rozszerzenia, na przykład *.mov* w przypadku QuickTime. Jednak znacznie częściej będą to inne rozszerzenia. RealMedia wykorzystuje rozszerzenie *.rm* dla treści strumieniowanej oraz rozszerzenia *.rpm* i *.ram* dla metaplików. Z kolei Windows Media używa rozszerzeń *.asf* i *.wmv* dla treści oraz *.asx*, *.wax* i *.wmx* dla metaplików.

Powodem, dla którego pliki *.mov* Apple nie wymagają stosowania metaplików, jest umieszczanie instrukcji strumieniowania właśnie w tych plikach *.mov*. Instrukcje bezpośrednio wskazują serwer strumieniowania. Takie rozwiązanie czasami nie sprawdza się najlepiej, jeśli odtwarzaczem domyślnym nie jest QuickTime Player. Znacznie częściej zdarza się to na platformie Windows niż Macintosh. Gdy użytkownik kliknie łącze RTSP (URL) w przeglądarce internetowej, następuje przekierowanie przy użyciu pliku typu *odnośnik do filmu*, któremu Apple również przypisał rozszerzenie *.mov*. Wspomniany plik odnośnika do filmu jest stosowany także podczas używania kodowania MBR w wersji QuickTime lub alternatywnych wartości bitrate. Plik odnośnika do filmu obsługuje też negocjacje prowadzone podczas wykorzystywania przez Apple schematu różnych wartości bitrate.

Kiedy odtwarzacz QuickTime jest wywoływany w celu strumieniowania treści na żywo, to nie ma pliku *.mov*, z którym pracuje. W takim przypadku Apple wykorzystuje plik SDP (ang. *Session Description Protocol*) jako tekstowy metaplik przekierowujący odtwarzacz do serwera strumieniowania.

## Odtwarzacze

QuickTime, Windows Media Player i RealMedia są dostępne jako samodzielne programy lub jako wtyczki do przeglądarek internetowych. Ponieważ trzy wymienione odtwarzacze są zgodne z plikami utworzonymi w trzech różnych i niekompatybilnych architekturach strumieniowania multimedialnych, dostawcy treści są zmuszeni do obsługi wszystkich trzech albo do pójścia na kompromis.

Cztery najpopularniejsze odtwarzacze strumieniowanych multimedialnych to:

- ♦ **Adobe Flash.** Odtwarzacz Flash obecnie jest dostępny w wersji 10.1x; odtwarza pliki w formacie Flash Video (rozszerzenie *.flv*). Adobe Flash używa apletu instalowanego w przeglądarce internetowej, który dekoduje i odtwarza pliki FLV. Odtwarzacz ten można pobrać ze strony <http://get.adobe.com/pl/flashplayer/>.
- ♦ **Apple QuickTime.** Odtwarzacz QuickTime Player jest dostępny w wersji 7.6; można go pobrać z internetu jako samodzielną aplikację bądź wraz z programem iTunes<sup>1</sup>. Standardowa wersja odtwarzacza jest bezpłatna, ale firma Apple oferuje płatne uaktualnienie do wersji Pro, która pozwala na przeprowadzanie konwersji i kodowanie plików. QuickTime to preferowany format multimedialnych w komputerach Macintosh. QuickTime Player odtwarza pliki w formacie *.mov* (rzadziej *.qt* lub *.qti*). Odtwarzacz można znaleźć na stronie <http://www.apple.com/quicktime/download>.
- ♦ **Microsoft Windows Media Player.** Obecnie odtwarzacz jest dostarczany w wersji 12. wraz z systemem Microsoft Windows i odtwarza pliki Windows Media Audio (WMA), Windows Media Video (WMV) oraz Advanced Streaming Format (ASF). Strona domowa odtwarzacza Windows Media Player mieści się pod adresem <http://www.microsoft.com/windows/windowsmedia/default.mspx>.
- ♦ **RealPlayer.** RealPlayer w wersji 11. to dostępny na wielu platformach odtwarzacz plików w formatach MP3, MPEG-4, QuickTime oraz Windows Media. To także program do odtwarzania plików we własnościowym formacie RM, tworzonych przy użyciu oprogramowania RealMedia. Odtwarzacz RealPlayer jest dostępny dla platform Windows, Mac OS X, Linux, Unix, Windows Mobile oraz Symbian OS. Można go pobrać ze strony <http://europe.real.com/realplayer/>.

Firma RealNetworks oferuje środowisko Helix jako projekt typu open source dla programistów rozwiązań multimedialnych. Klient Helix DNA to środowisko multimedialne, natomiast Helix Player to odtwarzacz multimedialnych bazujący na nim i działający w systemach Linux, Solaris, FreeBSD oraz Symbian. W celu dodania strumieniowanej treści do serwera Helix DNA Server można użyć programu Helix Producer. Witryna Helix znajduje się pod adresem <https://helix-client.helixcommunity.org>.

Wśród wielu innych odtwarzaczy multimedialnych najbardziej znane są BearShare, FLV-Media Player, Musicmatch Jukebox, Napster, PowerDVD, VLC Media Player, WinDVD, xine, Yahoo! Music Jukebox oraz Zinf.

---

<sup>1</sup> Dotyczy to systemu Windows. Dla systemu Mac OS X najnowsza wersja to QuickTime X; tutaj nie ma już wersji Pro. QuickTime X na platformie Macintosh w porównaniu z wersją 7.x ma ubogie możliwości w zakresie konwersji plików na inne formaty — *przyp. tłum.*



Wikipedia zawiera obszerną stronę, na której opisano sporo odtwarzaczy multimedialnych. Znajduje się ona pod adresem [http://en.wikipedia.org/wiki/Media\\_player\\_\(application\\_software\)](http://en.wikipedia.org/wiki/Media_player_(application_software)).

Dzięki wymienionym technologiom większość witryn internetowych dostarczających strumieniowanie multimedialne oferuje tę usługę w dwóch lub więcej formatach, bardzo często z różnymi wartościami bitrate oraz w różnych rozmiarach. Ma to na celu obsługę klientów używających odmiennych odtwarzaczy oraz korzystających z połączeń o różnej przepustowości.

## Flash

Adobe Flash to oprogramowanie animacyjne służące do odtwarzania wideo na stronach internetowych. Dominuje ono w tej dziedzinie wraz z Adobe Shockwave. Technologia Flash została opracowana przez FutureWave i najpierw była przejęta przez firmę Macromedia, a później Adobe. Nazwę „Flash” utworzono od słów „Future” i „Splash”; wiąże się ona ponadto z nazwą FutureWave. Flash Video to zarówno format pliku, jak i technologia dostarczania strumieniowanej treści wideo na stronie internetowej. Prawdopodobnie najbardziej znaną witryną wykorzystującą technologię Flash jest *YouTube.com*.

Na rysunku 25.6 widać kadr z filmu przedstawiającego pajaka; film ten pojawił się jako Flash Video na witrynie Science Friday. Format Flash Video jest odtwarzany w programie Flash Player, który jest wtyczką osadzaną na stronach internetowych. Aktualna wersja odtwarzacza to 10.1x. Aplikację można pobrać ze strony <http://get.adobe.com/flashplayer>. Inne programy, które mogą odtwarzać pliki Flash Video, to między innymi VLC Media Player (Mac, PC, Linux), FLV Player, QuickTime (wymaga wtyczki Perian), RealPlayer, Windows Media Player, MPlayer, xine oraz totem w systemach Linux. Technologia Microsoft DirectShow jest wymagana do odtwarzania Media Player oraz Media Center Flash.

### Rysunek 25.6.

*Flash Video to wszechobecny format służący do strumieniowania wideo na stronach internetowych. Niemal wszystkie odtwarzacze wyglądają podobnie do pokazanego (<http://www.sciencefriday.com/videos/watch/10175>)*



Format pliku Flash Video *.flv* obsługuje kodeki wideo Sorenson Spark H.263, H.264, MPEG-4 ASP, On2 Technologies TrueMotion VP6, jak również audio HE-ACC. Istnieje ponadto możliwość osadzenia Flash Video w plikach Shockwave Flash (SWF). Same pliki Flash Video są definiowane przez otwarty format kontenera, natomiast kodowanie jest przeprowadzane przez własnościowy kodek, wbudowany w programie Adobe Flash oraz innych produktach Adobe, służący do tworzenia plików Flash. Strumień FLV zawiera po jednym strumieniu audio i wideo.

Formaty plików wykorzystujące technologię Flash to m.in.:

- ♦ **F4A.** Format audio dla odtwarzacza Flash Player wraz z typem MIME `audio/mp4`.
- ♦ **F4B.** Format audiobook dla odtwarzacza Flash Player wraz z typem MIME `audio/mp4`.
- ♦ **F4P.** Format chronionego wideo dla odtwarzacza Flash Player wraz z typem MIME `video/mp4`.
- ♦ **F4V.** Format wideo dla odtwarzacza Flash Player wraz z typem MIME `video/mp4`.

Pliki w formacie Flash Video są raczej niewielkie. Mogą być dostarczane jako pliki *FLV*, osadzone pliki *SWF*, wysyłane z serwera WWW za pomocą progresywnego pobierania przez protokół HTTP oraz strumieniowane do klientów z serwera WWW. W przypadku pobierania progresywnego i strumieniowania Adobe używa własnościowego formatu RTMP (*Real-Time Messaging Protocol*). RTMFP (*Real-Time Media Flow Protocol*) to technologia wykorzystywana przez Adobe do komunikacji między odtwarzaczami Flash Player i serwerami aplikacji przez platformę Adobe AIR; może być stosowana w celu rozpowszechniania treści Flash Video. Oprogramowanie serwera RTMP zawiera Adobe Flash Media Server, Wowza Media Server oraz WebORB Integration Server for .NET, Java i ColdFusion.

Jak już wspomniano, strumieniowanie multimediów nie powoduje trwałego pozostawienia kopii pliku w systemie. Oznacza to, że dowolny plik FLV, który użytkownik będzie chciał wyświetlić później, nie będzie dostępny w systemie, o ile nie zostaną podjęte dodatkowe kroki w celu jego zapisania. Istnieją trzy metody pozwalające na zapisywanie plików FLV: wykorzystanie specjalnych witryn internetowych przechwytyjących wideo i wysyłających je użytkownikowi, zastosowanie rozszerzenia bądź wtyczki do przeglądarki internetowej oraz zainstalowanie komercyjnego programu oferującego funkcję zapisu przechwyconego pliku FLV.

Witryny pozwalające na zapisywanie strumieni wideo to między innymi KeepVid (<http://www.keepvid.com>). Rozszerzenie dla przeglądarki Firefox o nazwie Video Downloader również umożliwia zapis strumieniowanych plików FLV. W celu zapisania wideo przechwyconego bezpośrednio z ekranu można użyć programu takiego jak Snagit (firmy TechSmith) lub Snapz Pro X 2 (firmy Ambrosia Software).

## Silverlight

Microsoft Silverlight to środowisko programistyczne służące do dostarczania wzbogaconej treści przeglądarkom internetowym wyposażonym we wtyczkę Silverlight. Technologia Silverlight oferuje takie same możliwości jak Adobe Flash i Shockwave wraz z obsługą animacji i grafiki wektorowej. Wykorzystuje platformę .NET oraz narzędzia programistyczne

i jest częścią silnika WPF (ang. *Windows Presentation Framework*). Wtyczki Silverlight istnieją dla platform Windows, Mac OS X, Linux (jako projekt Moonlight), Windows Mobile 6 oraz Symbian.

Silverlight 2.0 zawiera API Media Stream Source, pozwalające programistom na tworzenie strumieni multimedialnych wraz ze zmienną technologią strumieniowania, którą Microsoft nazywa „strumieniowaniem adaptacyjnym”. Technologia ta umożliwia odtwarzaczowi wybór wartości bitrate na podstawie dostępnej przepustowości łącza i mocy procesora. market.android.com Wspomniane API jest rozszerzalne, wymaga jedynie, aby strumienie znajdowały się w środowisku uruchomieniowym Silverlight w formacie możliwym do zdekodowania, na przykład MP3 lub WAV. Media Stream Source to technologia wykorzystana na witrynie internetowej igrzysk olimpijskich w Pekinie.

Windows Live oferuje Silverlight Streaming Service jako rozwiązanie hostingowe dla aplikacji Silverlight. Usługa ta pozwala na dostarczanie treści Silverlight klientom na platformach Windows i Mac oraz może dostarczyć treść dla witryn internetowych Microsoft Expression. Treść Silverlight można utworzyć w programie Microsoft Expression Encoder, który stanowi część pakietu Expression Studio 2, oraz za pomocą innych narzędzi firm trzecich. Silverlight Streaming integruje się przez Windows Live również z platformą Microsoft adCenter. Więcej informacji na temat tej usługi strumieniowania można znaleźć na witrynie <http://streaming.live.com>.

## Podsumowanie

W rozdziale przedstawiono różne rozwiązania pozwalające na strumieniowanie multimedialnych oraz pobieranie progresywne; podkreślono, że strumieniowana treść bardzo obciąża zasoby sieciowe. Omówiono także wymaganą architekturę sieciową.

Rozwiązania strumieniowania wykorzystują specjalne zestawy protokołów. W rozdziale przedstawiono protokoły *Real-Time Streaming Protocol*, *Real-Time Control Protocol*, *Real-Time Transport Protocol* oraz język znaczników SMIL.

Proces kodowania pozwala na utworzenie treści, która będzie charakteryzowała się stałą albo zmienną wartością bitrate. Możliwe jest również utworzenie pakietów strumieni z różnymi wartościami bitrate.

W rozdziale wspomniano o czterech głównych platformach strumieniowania multimedialnych — Windows Media Services, RealNetworks Helix Server, Apple QuickTime Streaming Server oraz Adobe Flash Media Streaming Server. Krótko omówiono także technologie strumieniowania Flash i Silverlight.

W kolejnym rozdziale będzie przedstawiona technologia powiązana ze strumieniowaniem, czyli „telefon przez internet”. Technologia VoIP zrewolucjonizowała przemysł telekomunikacyjny.

# Rozdział 26.

## Telefonia cyfrowa i VoIP

### W tym rozdziale:

- ♦ Protokoły i usługi telefoniczne
- ♦ Systemy telefonii PBX
- ♦ VoIP
- ♦ Integracja telefonii komputerowej
- ♦ Wideotelefon w działaniu

Nowoczesna telefonia to mariaż komputerów i telefonów oparty na dwóch różnych rodzajach sieci. Telefonia dzisiaj obsługuje szeroką gamę aplikacji multimedialnych, między innymi połączenia głosowe i wideo, programy biznesowe oraz służące rozrywce. Dziedzina ta zawsze była obszarem ogromnego postępu i jest natywnie obsługiwana przez sieciowe systemy operacyjne za pomocą interfejsu programowania aplikacji (API).

Sieć telefoniczną można utworzyć za pomocą systemu PBX<sup>1</sup> (ang. *Private Branch Exchange*) jako serwera zarządzania. PBX pozwala na tworzenie sieci z telefonami PSTN<sup>2</sup> (ang. *Public Switched Telephone Network*), działającymi na liniach telefonicznych, lub z telefonami działającymi przez IP w sieciach LAN i WAN. W rozdziale dokładniej zostaną przedstawione dwa systemy serwerów PBX dla telefonii opartej na IP: system typu open source o nazwie Asterisk oraz Unified Communications Manager firmy Cisco.

Technologia VoIP (ang. *Voice over Internet Protocol*) gwałtownie się rozwija. VoIP można zaimplementować w oprogramowaniu jako softphone<sup>3</sup> albo w telefonach IP, można też zaadaptować istniejący telefon za pomocą adaptera ATA (ang. *Analog Telephone Adapter*) i połączyć go z siecią IP. W rozdziale będą omówione właściwości telefonów IP.

Technologia VoIP do wysyłania i zarządzania komunikacją wykorzystuje specjalny zestaw protokołów, które szczegółowo będą przedstawione w dalszej części rozdziału. Protokoły sesji obejmują SIP (ang. *Session Initiation Protocol*) oraz SCCP (ang. *Skinnny Call Control Protocol*), natomiast pakiety są często wysyłane w formacie RTP (ang. *Real-Time Transport*

---

<sup>1</sup> Centrala prywatna połączona z miejską siecią telefoniczną — *przyp. tłum.*

<sup>2</sup> Publiczna komutowana sieć telefoniczna — *przyp. tłum.*

<sup>3</sup> Oprogramowanie pozwalające na emulowanie telefonu IP w komputerach — *przyp. tłum.*

*Protocol*). W rozdziale zostaną poruszone problemy dotyczące zapór sieciowych oraz NAT (ang. *Network Address Translation*), będą przedstawione również pewne rozwiązania tych problemów z zastosowaniem STUN (ang. *Simple Traversal of User Datagram Protocol*).

System integracji telefonu z komputerem (ang. *Computer Telephony Integration*, CTI) to zestaw aplikacji pozwalających partnerom typu VAR (ang. *Value Added Resellers*) oraz programistom na tworzenie własnych aplikacji telefonicznych. Wymienione aplikacje bazują na API telefonu i są przydatne w firmach oraz centrach obsługi telefonicznej (ang. *call center*), stanowią podstawę systemów inteligentnej telefonii. Możliwości oferowane przez system CTI również zostaną zaprezentowane w tym rozdziale.

Wideotelefonacja to technologia łącząca telefony, telefony bezprzewodowe, kamery internetowe oraz komunikatory (ang. *Instant Messaging*). Niektóre związane z tym aplikacje zostaną przedstawione na końcu rozdziału.

## Telefonia cyfrowa

Telefonia cyfrowa to zestaw usług pozwalających komputerom na transmisję dźwięku analogowego przez sieć w postaci danych cyfrowych. Telefonia cyfrowa wykorzystuje na wejściu konwersję dźwięku na dane cyfrowe oraz na wyjściu konwersję danych cyfrowych na dźwięk analogowy. W pewnych sytuacjach usługi telefoniczne mogą obsługiwać inny rodzaj komunikacji, zwykle w postaci plików dźwiękowych przekazywanych przez standardowe sieci bazujące na pakietach. W innych przypadkach telefonia przekazuje dźwięk w trakcie jego tworzenia i wynik strumieniu do odbiorcy, na przykład VoIP, co zostanie omówione w dalszej części rozdziału.

Aplikacje telefoniczne w sieciowych systemach komputerowych zaliczają się do następujących kategorii:

- ♦ połączenia głosowe przez sieci telefoniczne z komutacją kanałów,
- ♦ systemy symulacji PBX wraz z rozbudowanymi funkcjami obsługi połączeń,
- ♦ konferencje z wykorzystaniem technologii VoIP,
- ♦ systemy odpowiedzi dźwiękowych,
- ♦ połączenia VoIP,
- ♦ systemy współpracujące, współdzielone oraz zdalne systemy biurowe,
- ♦ zautomatyzowane systemy obsługi połączeń.

Oprogramowanie służące do tworzenia telefonii cyfrowej i zarządzania nią zostało dołączone do wielu systemów operacyjnych na zróżnicowanym poziomie zaawansowania. Systemy typu CTI pozwalają obecnie komputerom na zintegrowanie urządzeń wysyłających i odbierających sieciowe dane i dźwięk. W celu obsługi tych technologii wiele systemów operacyjnych jest dostarczanych wraz z odpowiednimi API umożliwiającymi wykorzystywanie wymienionych funkcji. API telefonii w systemie Windows ma nazwę Microsoft Telephony API (TAPI), firma Sun Microsystems, Inc.<sup>4</sup> opracowała Java Telephony API (JTAPI). W systemach operacyjnych Linux oraz dla komputerów Macintosh istnieją podobne API.

---

<sup>4</sup> Firma Sun 27 stycznia 2010 roku została przejęta przez firmę Oracle — *przyp. tłum.*

Telefonia odegrała ogromną rolę w rozwoju sieci komputerowych, zwłaszcza w obszarze przełączników sieciowych oraz routingu. Wiele ogromnych sieci zostało zbudowanych specjalnie dla systemów telefonicznych, co wymagało wysiłku związanego z zastąpieniem ręcznych central telefonicznych systemem zautomatyzowanym. Wynikiem tej automatyzacji było powstanie telefonii typu PSTN. Oprogramowanie komputerowe pozwalające na obsługę zautomatyzowanej centrali telefonicznej określano *centralami sterowanymi programowo* (ang. *Stored Program Control, SPC*), pojęcie to jest historyczne i już się go nie stosuje.

Przed standaryzacją komputerów usługi telefoniczne były wysyłane w postaci sygnału analogowego przez sieć z komutacją kanałów. Obecnie technologia analogowa ma nazwę POTS (ang. *Plain Old Telephone Service*). Kiedy transmisja danych nabrała istotnego znaczenia i nastąpiło zwiększenie ich przesyłu, zaczęto uaktualniać sieci telefoniczne w celu dostarczania usług w technologiach cyfrowych: ISDN (ang. *Integrated Services Digital Network*) oraz DSL (ang. *Digital Subscriber Line*). Po przekształceniu linii telefonicznych na sieci komunikacji cyfrowej przewody miedziane są zastępowane przez kable światłowodowe.

## Systemy PBX

Ogólnie rzecz biorąc, system PBX (ang. *Private Branch Exchange*) to sieć telefoniczna zainstalowana w średniej wielkości biurze. Sieć PSTN łączy się z siecią PBX, dostarczając jedną lub więcej linii telefonicznych dla połączeń przychodzących i wychodzących. Połączenia przychodzące do całej firmy mogą być dostarczane do systemu PBX i stamtąd odpowiednio kierowane. Każdy telefon podłączony do sieci to *telefon wewnętrzny* (ang. *extension*).

Biurowe systemy telefoniczne dostępne są w kilku odmianach:

- ♦ **System klawiszowy.** Kiedy telefon ma zestaw przycisków, które użytkownik naciska w celu wybrania linii wychodzącej, to mówimy o systemie klawiszowym.
- ♦ **Centrex.** Usługa wirtualnej centrali PBX, gdzie wszystkie usługi realizowane są przez centralę miejską. W systemie Centrex poszczególne telefony są połączone liniami bezpośrednio z centralą operatora telekomunikacyjnego.
- ♦ **PBX.** Centrala abonencka tworząca wewnętrzną sieć telefoniczną, najczęściej połączona z siecią publiczną łączami typu ISDN PRI, BRI lub analogowymi.
- ♦ **IP PBX lub IPBX.** Centrala abonencka wykorzystująca do komunikacji protokół IP.

Wymienione systemy wykonują następujące funkcje: nawiązują, obsługują i przerywają połączenia telefoniczne. Większość z nich dostarcza również wielu użytecznych informacji. Zakres funkcji dotyczących obsługi połączeń w systemie PBX może być ogromny. W stosunku do standardowej, domowej linii telefonicznej mogą one zaoferować jeszcze takie funkcje, jak: automatyczna obsługa głosowa, usługi zautomatyzowane, automatyczne pobieranie informacji od osoby dzwoniącej (na przykład położenie geograficzne), dystrybucja połączeń, połączenie konferencyjne, własne komunikaty powitania, odtwarzanie muzyki bądź radia po wstrzymaniu połączenia, przywoływanie, zawansowane usługi poczty głosowej oraz przekazywanie wiadomości głosowych. W kolejnych podrozdziałach zostaną przedstawione trzy systemy IP-PBX: serwer Asterisk typu open source, oprogramowanie Unified Communications Manager firmy Cisco oraz rozwiązanie Microsoft Response Point.

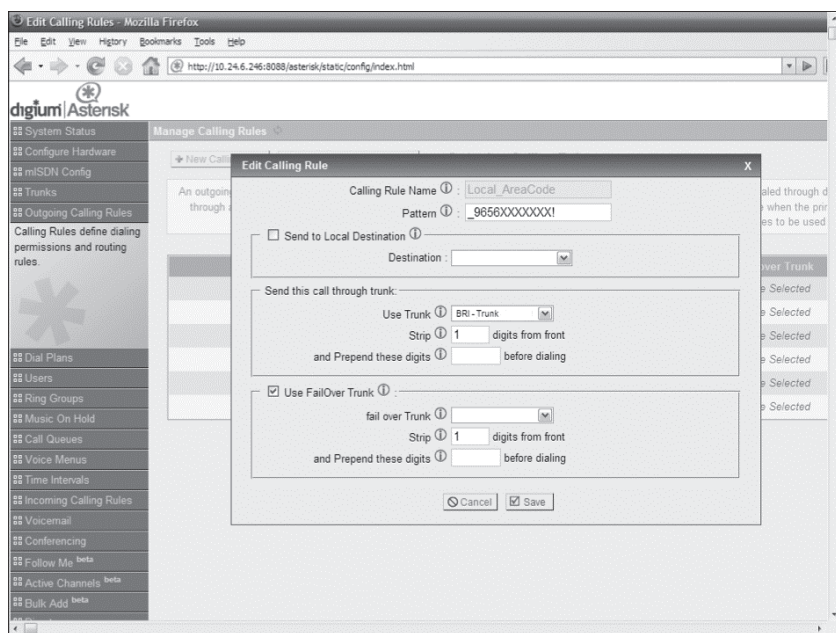
## Asterisk

Digium Asterisk (<http://www.asterisk.org>), oprogramowanie systemu PBX typu open source, to jedno z rozwiązań pozwalających na utworzenie systemu IP-PBX na bazie komputera o stosunkowo niewielkiej wydajności. To jedna z najpopularniejszych i powszechnie używanych aplikacji typu serwer VoIP. Asterisk może działać w różnych wersjach systemu operacyjnego Unix, między innymi OpenBSD, FreeBSD i NetBSD, a także Mac OS X, Sun Solaris oraz Microsoft Windows. (Wersja działająca w systemie Windows to AsteriskWin32). Sprzęt niezbędny do połączenia z serwerem Asterisk łączy PSTN, PRI, BRI jest sprzedawany przez firmę Digium i wielu innych producentów.

Asterisk po instalacji musi zostać skonfigurowana jako system PBX lub VoIP. Początkowa konfiguracja oznacza modyfikację zestawu plików konfiguracyjnych, dla każdego urządzenia system PBX wymaga utworzenia planu dzwonienia. Na rysunku 26.1 pokazano reguły dzwonienia dla połączenia wychodzącego. Gwarantują one, że wywoływane numery telefoniczne będą zgodne z określonym formatem liczbowym. Ponadto określają sposób kierowania połączenia oraz zachowanie w przypadku, kiedy użycie trasy podstawowej dla połączenia zakończy się niepowodzeniem.

**Rysunek 26.1.**

*Interfejs użytkownika Asterisk oferuje możliwość zarządzania PBX przez interfejs przeglądarki internetowej. Na rysunku pokazano okno dialogowe Edit Calling Rule dla połączenia wychodzącego*



Serwer Asterisk ma język programowania, dzięki któremu telefony można dopasować do kontekstów (scenariuszy), a działania mogą być przypisane na podstawie ustalonej logiki. Asterisk Gateway Interface dostarcza API, do którego dostęp jest możliwy z poziomu programów utworzonych w językach Perl, Java, C i PHP.

Aplikacje dostarczane wraz z serwerem Asterisk to:

- ♦ `app_dial` — wykonuje reguły dla połączeń urządzenie-urządzenie,

- ♦ `app_meeting` — tworzy połączenia konferencyjne i zarządza nimi,
- ♦ `app_voicemail` — przechowuje i odtwarza wiadomości głosowe.

Dostępna jest pewna liczba interfejsów GUI — można je zainstalować i używać ich do zarządzania serwerem Asterisk. Firma Digium oferuje `asterisk-gui 2.0`, natomiast FreePBX to inny interfejs GUI. Dystrybucja o nazwie Trixbox (wcześniej znana jako Asterisk@Home) łączy w sobie instalację serwera Asterisk i FreePBX.

## Oprogramowanie Cisco Unified Communications Manager

Unified Communications Manager (CUCM) firmy Cisco to oprogramowanie systemu PBX zarządzające różnymi produktami telefonicznymi oraz komponentami z nimi współpracującymi. Produkt jest bardziej znany dzięki jego wcześniejszej nazwie Cisco CallManager (CCM). Oprogramowanie Cisco CallManager jest instalowane w serwerze Cisco Media Convergence Server (MCS) lub na innej zaakceptowanej platformie. MCS można klastrować wraz z serwerem Publisher, obsługiwany przez osiem serwerów subskrybentów.

Główną funkcją CUCM jest określenie natury numeru telefonu dzwoniącego, a następnie komunikacja z bramą w celu skoordynowania połączeń wychodzących lub przychodzących z telefonu publicznego lub prywatnej sieci IP.

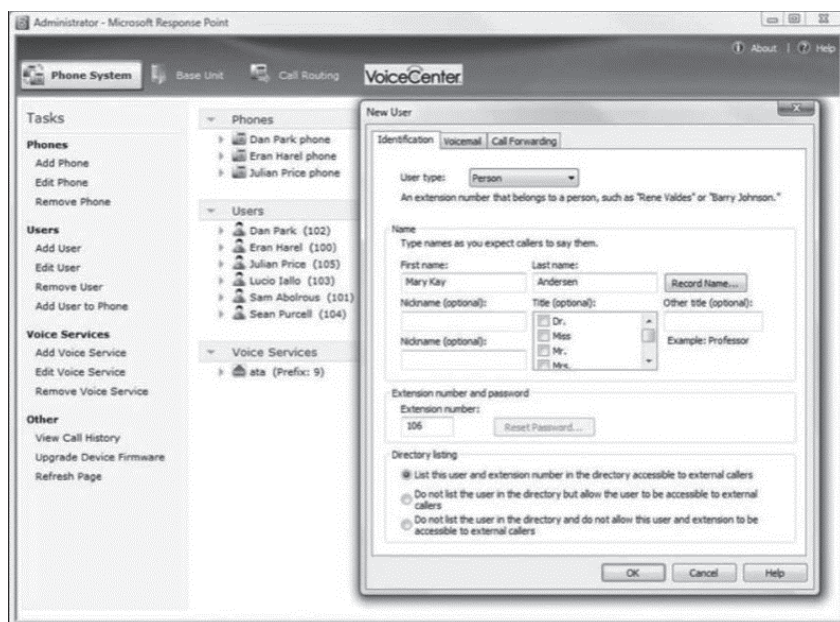
CUCM używa protokołu SCCP (ang. *Skinny Call Control Protocol*) do kontrolowania osprzętu telefonicznego oraz protokołu *Media Gateway Control Protocol* lub *Session Initiation Protocol* (SIP) do komunikacji z bramami i mostkami sieciowymi i innymi komponentami. Za pomocą CUCM można obsługiwać również połączenia telefoniczne VoIP i sesje H.323. Protokoły te zostaną dokładniej omówione w dalszej części rozdziału.

Ostatnią wersję oprogramowania CUCM (8.0) wydano w maju 2010 roku. Firma Cisco oferuje wersję CUCM dla systemu Windows oraz związane z nią urządzenia. W wersji 7. ujednolicono numery wersji różnych komponentów tworzących pakiet Communication Manager i utrwalono zastosowanie bazy danych IBM Informix jako wewnętrznego magazynu danych.

## Microsoft Response Point

Microsoft Response Point (<http://www.microsoft.com/responsepoint/default.aspx>) to aktywowane głosowo oprogramowanie PBX dla biur wyposażonych w maksymalnie 50 telefonów. System z dziesięcioma telefonami zapewnia optymalną wydajność w sieci LAN 100Base-T. Service Pack 1 dla oprogramowania Response Point umożliwia obsługę zarówno telefonów analogowych, jak i VoIP. Połączenia IP używają protokołu SIP. Wśród funkcji Response Point można znaleźć integrację z systemami poczty elektronicznej, a także łatwą konfigurację i zarządzanie za pomocą graficznego interfejsu użytkownika (zob. rysunek 26.2). Rozpoznawanie głosu bazuje na oprogramowaniu Speech Server, oferuje wiele możliwości, ułatwia pracę i nie wymaga wcześniejszego przygotowania. Ewentualne przygotowanie polega na tym, że użytkownik daje próbki głosu, aby system mógł lepiej zrozumieć poszczególne polecenia oraz wzorce mowy.

**Rysunek 26.2.**  
Konsola  
administracyjna  
w Microsoft  
Response Point



Oprogramowanie Response Point zostało zbudowane jako system typu open source współpracujący z urządzeniami wielu różnych producentów. Ponadto jest przystosowane do działania pod kontrolą systemu Microsoft Embedded XP, który jest dostarczany w małych urządzeniach przez wielu różnych producentów sprzętu. Po podłączeniu urządzenia do sieci i jego włączeniu następuje uruchomienie kreatora umożliwiającego podłączenie telefonów i przypisanie ich użytkownikom lub miejscom. Konfiguracja zajmuje około piętnastu minut, co jest niespotykane w przypadku tego rodzaju sprzętu i oprogramowania.

Wczesny model Syspine firmy Quanta pozwala na połączenie do ośmiu linii POTS i jest konfiguracją wyłącznie analogową. Dostawcy OEM (ang. *Original Equipment Manufacturer*) oraz ich partnerzy VAR dostarczają sprzęt serwerowy PBX wraz z funkcjami służącymi do zarządzania oraz zestawy telefoniczne w pełni łączące klientów z systemem Response Point. Serwer musi działać pod kontrolą systemu XP lub Vista, podobnie jak każdy klient wymagający pełnej obsługi telefonii.

Firma Microsoft utrzymuje wymagania oprogramowania Response Point na minimum, a sam system do funkcjonowania nie wymaga serwera nazw, Exchange, SharePoint lub Office Communications Server. Serwer Response Point może udostępniać klientom wymagane usługi sieciowe, na przykład DHCP. W pierwszym wydaniu produktu firmy Microsoft nie istnieje wiele punktów zaczepienia (połączeń specjalnych) — nie ma integracji z serwerem Small Business Server, importu bazy danych kontaktów z Outlooka lub możliwości użycia Active Directory, jeśli sieć ma serwer domeny. Response Point to nowy produkt, oprogramowanie to będzie się z czasem zmieniało<sup>5</sup>.

<sup>5</sup> Na swojej witrynie internetowej firma Microsoft poinformowała, że z dniem 31 sierpnia 2010 roku zaprzestala rozwoju oprogramowania Response Point — *przyp. tłum.*

## Technologia VoIP

*Voice over Internet Protocol* (VoIP) to protokół służący to transmisji głosu przez sieci bazujące na pakietach. VoIP wykorzystuje sieci LAN i WAN i funkcjonuje jako medium przekazywania danych głosowych.

Nie ma żadnych specjalnych wymagań, które muszą być spełnione przez obie strony w trakcie połączenia typu VoIP, poza tym, aby wszystkie strony IP miały bezpośrednie połączenie z siecią. Aby wykonać połączenie pomiędzy telefonem w sieci PSTN a telefonem VoIP, musi istnieć system łączący obie sieci, mający przypisane numery PSTN dla klientów VoIP. Operator VoIP korzysta w takim wypadku z zakresu numerów przydzielonych przez operatora PSTN, do którego sieci terminuje połączenia klientów VoIP. Usługa przyznania zakresu numerów miejskich, pozwalająca na bezpośrednie połączenie z nimi, jest określana jako DDI (ang. *Direct Dial-In*). System DDI jest wykorzystywany w Europie, w USA ma nazwę DID (ang. *Direct Inward Dialing*).

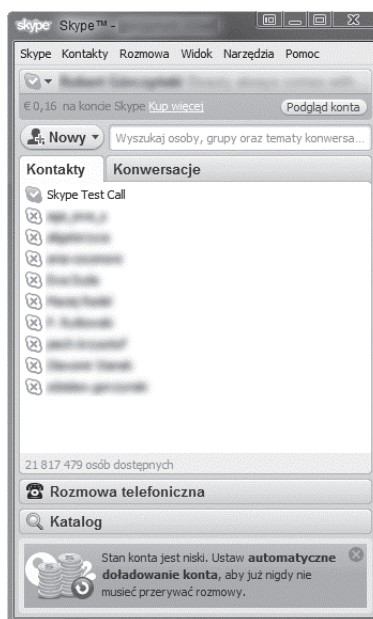
Technologia VoIP opiera się na konwersji DAC (ang. *Digital Audio Conversion*) i służy do przekształcania dźwięku na cyfrowe pliki audio. Podobnie jak w przypadku innych formatów plików dźwiękowych, na przykład MP3, VoIP stosuje techniki kompresji w celu utworzenia plików o mniejszej wielkości, które są dzielone na pakiety i wysyłane przez sieci IP. Pliki VoIP mogą być skompresowane bardzo efektywnie, więc w zależności od wybranego poziomu jakości rozmowa o długości godziny może być zapisana w pliku o objętości mniejszej niż 20 MB — czyli nie większym niż podcast o takiej długości.

Usługi VoIP są implementowane na jeden z następujących sposobów:

- ♦ rozwiązanie bazujące tylko na oprogramowaniu, podobnie jak w przypadku programu Skype pokazanego na rysunku 26.3,

### Rysunek 26.3.

Pokazane na rysunku okno główne programu Skype obsługuje wiadomości IM i telefonowanie; z programu tego korzystają miliony użytkowników



- ♦ dodanie telefonu analogowego przez adapter ATA (ang. *Analog Telephone Adapter*), jak w przypadku Vonage (<http://www.vonage.com>), AT&T CallVantage (<http://www.corp.att.com/voip>) oraz Verizon VoiceWing (<http://www22.verizon.com/residential/homephone/>),
- ♦ połączenie za pomocą modemu kablowego — zwykle jako część pakietu (TV, telefon, internet), jak w przypadku Comcast (<http://www.comcast.com>),
- ♦ z wykorzystaniem systemu IP-PBX podłączonego do sieci IP. System VoIP podłączony do PBX zwykle wymaga połączenia o wysokiej przepustowości. Więcej informacji na ten temat przedstawiono we wcześniejszym podrozdziale.

Podstawową zaletą systemu VoIP było duże zmniejszenie kosztów połączeń międzymiastowych i międzynarodowych. Natomiast główną wadą technologii VoIP to wykorzystywanie jednej linii przez internet i telefon, przez co na przykład awaria połączenia z internetem powoduje utratę obu metod komunikacji. We wczesnych implementacjach VoIP problematyczna była jakość głosu. Obecna technologia umożliwia odtwarzanie głosu o jakości nawet lepszej niż w przypadku linii telefonicznych. W tabeli 26.1 przedstawiono wady i zalety technologii VoIP.

Przełączniki sieciowe firmy Cisco, między innymi 2950, 2955 i 3550, pozwalają, aby ich porty zostały skonfigurowane dla ruchu sieciowego VoIP, jest to funkcja VLAN (ang. *Virtual Local Area Network*). Ten ruch sieciowy wykorzystuje priorytetowe ramki 802.1P, obsługujące CoS (klasa usługi, ang. *Class of Service*), pozwala realizować założenia jakości usług, ang. *Quality of Service*) do transmisji głosu oraz danych.

## Adaptory ATA

Adapter *Analog Telephone Adapter* (ATA) pozwala na podłączenie telefonu analogowego do systemu telefonii cyfrowej, na przykład sieci VoIP, i w efekcie zamienić telefon typu PSTN na telefon IP. Adaptory to najczęściej bardzo małe urządzenia dostarczane wraz z portami Ethernet RJ45 i telefonicznym RJ11, gdy są przeznaczone dla jednego telefonu. Wszystkie adaptory ATA wymagają zasilania.



Listę dostępnych adapterów ATA można znaleźć na witrynie VoIP-Info.org pod adresem <http://www.voip-info.org/wiki/view/Analog+Telephone+Adapters>.

Większe adaptory ATA obsługują wiele połączeń i mają wiele gniazd RJ11 lub gniazda RJ14 (dwie linie), RJ25 (trzy linie) lub RJ45 (cztery linie) dla zastosowań przemysłowych. Adapter ATA przeprowadza konwersję dźwięku analogowego na cyfrowy, co pozwala aparatom telefonicznym na bezpośrednie połączenie z serwerem VoIP. Adapter ATA czasami jest określany *bramką VoIP*; używa protokołów takich jak H.323, SIP, *Media Gateway Control Protocol* (MGCP), *Inter-Asterisk eXchange Protocol* (IAX) oraz zawiera kodek lub zestaw kodeków przeznaczonych do kodowania i dekodowania komunikacji głosowej. Wymienione protokoły zostaną przedstawione w dalszej części rozdziału.

Adapter ATA najczęściej można spotkać w jednej z dwóch postaci. Pierwsza to proste połączenia między telefonem i siecią IP, natomiast druga to urządzenia przeznaczone do współpracy z określonym dostawcą i usługą VoIP, które nie mogą być używane z żadnym innym systemem.

**Tabela 26.1.** Wady i zalety technologii VoIP

Funkcja	Zaleta	Wada
Niezależność od numeru kierunkowego	Dany telefonu może mieć dowolny numer kierunkowy i jednocześnie znajdować się w regionie o innym numerze kierunkowym.	
Integracja z komputerem	Po podłączeniu komputera do adaptera ATA dostępne stają się funkcje dodatkowe, takie jak integracja z zaawansowaną usługą poczty głosowej oraz e-mail.	
Koszt	W przypadku połączeń między urządzeniami VoIP usługi międzymiastowe są tanie.	W przypadku połączeń przy użyciu usługi DDI trzeba liczyć się z dodatkowymi kosztami.
Funkcje	VoIP oferuje rozbudowany zestaw funkcji: połączenia oczekujące, przekierowywanie połączeń, identyfikację dzwoniącego, zaawansowaną usługę poczty głosowej. Z reguły dostępne są również połączenia trójstronne i konferencyjne.	Brak obsługi połączeń z numerami alarmowymi, na przykład 112. Połączenie VoIP nie jest powiązane z określonym miejscem geograficznym, więc nie można ustalić położenia osoby dzwoniącej.
Współpraca		Wykonywanie połączeń przez zapory sieciowe i NAT może być problematyczne. Na pewno nie działają stare telefony z wybieraniem impulsowym.
Jakość	Z reguły taka sama jak w przypadku linii telefonicznych typu PSTN lub lepsza.	Kiepskie połączenie internetowe lub o małej przepustowości skutkuje słabą jakością połączenia telefonicznego. Przeciążenie sieci może prowadzić do przerwania i chwilowych zaników głosu.
Mobilność	Adaptera ATA można używać wszędzie tam, gdzie jest dostęp do internetu i energii elektrycznej.	Telefony komórkowe nie są obsługiwane, a więc konieczne jest posiadanie telefonu komórkowego.
Bezpieczeństwo	Dzięki zastosowaniu protokołów takich jak SRTP (ang. <i>Secure Real-Time Transport Protocol</i> ) istnieje możliwość nawiązywania bezpiecznych połączeń.	

Linksys SPA3102 to przykład adaptera ATA pozwalającego na podłączenie telefonów do sieci IP. Urządzenie SPA3102 umożliwia użytkownikowi wykonanie połączenia lokalnego z telefonu komórkowego bądź stacjonarnego do urządzenia SPA3102, gdzie dane użytkownika są uwierzytelniane, a telefon jest połączony z internetem. Jeżeli urządzenie SPA3102 będzie znajdowało się po stronie odbierającego połączenia, to połączenia VoIP mogą być odebrane bądź przekierowane do dowolnego telefonu PSTN lub komórkowego.

Adapter SPA3102 został pokazany na rysunku 26.4. Zawiera jeden port RJ11 (POTS) FXS, jeden port PSTN FXO, pozwalający na połączenie linii miejskiej, oraz dwa porty 100Base-T RJ45 Ethernet, pozwalające na połączenie z siecią LAN i łączem szerokopasmowym lub

**Rysunek 26.4.**

Urządzenie ATA  
 Linksys SPA3102  
 (zdjęcie z biblioteki  
 obrazów firmy Linksys)



routerem ISP. Oprogramowanie dostarczane wraz z tym adapterem ATA umożliwia niezależną konfigurację linii FXS i FXO. Adapter SPA3102 jest instalowany i konfigurowany przez użytkownika dla określonej usługi VoIP.

## Telefony VoIP

Telefony VoIP mogą być zaimplementowane jako sprzęt albo jako oprogramowanie (tzn. softphone). Oferują funkcje pozwalające na połączenie z siecią IP i komunikację za pomocą protokołów, które wysyłają połączenia głosowe jako dane. Niektórzy dostawcy usług VoIP stosują standardy własnościowe lub dostarczają kilka protokołów standardowych, na przykład *Session Initiation Protocol* (SIP) i *Skinny Call Control Protocol* (SCCP). Jak już wspomniano, istnieje możliwość zamiany zwykłego telefonu na telefon IP przez zastosowanie adaptera typu ATA.

Telefon IP wymagają następujących funkcji:

- ♦ możliwości podłączenia sprzętu (fizycznego aparatu telefonicznego),
- ♦ oprogramowania emulującego (softphone) lub zarządzającego telefonem IP,
- ♦ zestawu protokołów, na przykład SIP, SCCP, H.323 i Skype,
- ♦ klienta DNS,
- ♦ klienta DHCP (czasami),
- ♦ obsługi protokołu RTP (ang. *Real-Time Transport Protocol*),
- ♦ obsługi protokołów tunelowania, na przykład *Simple Traversal of User Datagram Protocol through Network Address Translator* (STUN), aby możliwe było przechodzenie przez zapory sieciowe i bramy.

Na rysunku 26.5 pokazano telefon D-Link DPH-140S Express Ethernet Business IP, jest on dostarczany wraz z wbudowanym gniazdem Ethernet, mikrofonem i głośnikiem, pocztą głosową oraz książką adresową.

**Rysunek 26.5.**

Telefon D-Link  
DPH-140S Express  
Ethernet Business IP  
(zdjęcie pochodzi  
z biblioteki obrazów  
firmy D-Link)



## Protokoły VoIP

Jak wspomniano w poprzednim podrozdziale, telefony IP wymagają zestawu protokołów specjalnych, pozwalających na tworzenie połączeń i zarządzanie nimi. Z reguły protokoły te są połączone w zestaw, tak aby dany telefon IP mógł być używany w różnych sieciach i być dołączany do różnego rodzaju urządzeń i oprogramowania zarządzającego. Poniżej będą omówione powszechnie wykorzystywane protokoły VoIP, między innymi:

- ♦ Session Initiation Protocol (SIP),
- ♦ Skinny Call Control Protocol (SCCP),
- ♦ Real-Time Transfer Protocol (RTP),
- ♦ Session Traversal Utilities for NAT (STUN),
- ♦ H.323,
- ♦ Inter-Asterisk eXchange Protocol (IAX),
- ♦ Media Gateway Control Protocol (MGCP).

Protokół SIP jest używany do transmisji głosu oraz wideo przez internet. Jest wykorzystywany również do strumieniowania multimediów, bywa stosowany w komunikatorach internetowych (IM), a nawet grach wideo. Protokół SIP obsługuje dwustronne połączenia dwupunktowe, czyli sesje emisji pojedynczej, a także technologie multistream, połączenia wielostronne i sesje multemisji. Protokołem warstwy transportowej najczęściej jest: TCP w połączeniach dwupunktowych, UDP w VoIP, grach i aplikacjach, SCTP (ang. *Stream*

*Control Transmission Protocol*) w aplikacjach strumieniowanych. SIP zarządza przypisaniami portów, adresowaniem oraz innymi funkcjami połączenia dla strumieniowanych danych. Ogólnie rzecz biorąc, w modelu ISO/OSI protokół SIP jest protokołem warstwy sesji. Jednak w modelu TCP/IP, gdzie warstwy od 5. do 7. są skonsolidowane, SIP jest protokołem warstwy aplikacji.

## **Protokół Skinny Call Control Protocol**

*Skinny Call Control Protocol* (SCCP) to protokół warstwy sesji używany przez firmę Cisco do podłączania klientów przez przełączniki sieciowe Cisco. Skinny Call obejmuje linię przewodowych i bezprzewodowych telefonów IP Cisco (seria 7900), softphone Cisco IP Communicator oraz serwer poczty głosowej Cisco Unity. Linia telefonów IP firmy Cisco wykorzystuje różne protokoły.

Wszystkie urządzenia mogą być zarządzane przez oprogramowanie CUCM (ang. *Cisco Unified Communication Manager*), służące do obsługi połączeń, nazywane również CCM (ang. *Cisco CallManager*). (Firma Cisco bardzo chętnie stosuje skróty rozpoczynające się literą C). Oprogramowanie CallManager to zasadniczo serwer wiadomości oferujący zarządzanie transakcjami dla różnych protokołów multimedialnych, takich jak SIP, ISDN, wideo H.323 oraz MGCP (ang. *Media Gateway Control Protocol*).

## **Protokoły Real-Time Transport Protocol oraz Real-Time Transfer Control**

*Real-Time Transport Protocol* (RTP) to standardowy format pakietów do wysyłania treści multimedialnych jako danych TCP lub UDP przez sieci IP. Protokół ten może być używany dla danych emisji pojedynczej bądź multiemisji. Z kolei protokół RTCP jest wykorzystywany do zarządzania danymi RTP, jak również oferuje możliwość monitorowania jakości usług (QoS).

Protokół RTP nie określa używanych portów, ale wymaga, aby RTP był przypisany do portu parzystego, natomiast protokół RTCP do kolejnego portu nieparzystego. Para portów dla protokołów RTP i RTCP jest przypisywana w zakresie portów dynamicznych od 16 384 do 32 767. Dane RTP mogą być danymi generowanymi w czasie rzeczywistym oraz danymi interaktywnymi. Dla VoIP pakiety RTP wymagają protokołu sesji, na przykład SIP lub H.323.

## **Protokół Session Traversal Utilities for NAT**

Aplikacje telefoniczne mogą mieć trudność w przeprowadzaniu udanej negocjacji z zaparami sieciowymi i bramami, jeżeli została tam zastosowana technika NAT (ang. *Network Address Translation*). Technika NAT zarówno dla ruchu wewnętrznego, jak i zewnętrznego zarządza dostępem aplikacji do określonych portów oraz dostępem klientów do różnych aplikacji. Implementacje NAT mogą być odmienne w różnych urządzeniach i mają tendencję do uniemożliwiania działania różnych aplikacji IP przez blokowanie dla nich dostępu do zasobów internetowych lub zezwolenie komunikacji z zewnątrz routera na dotarcie do serwera aplikacji. Protokół RTP opisany w poprzedniej sekcji jest szczególnie wrażliwy na problemy z przechodzeniem przez NAT, co wiąże się z dynamicznym przypisywaniem portów.

Protokół *Session Traversal Utilities for NAT* (STUN) to rozwiązanie powyższego problemu. STUN jest używany jako usługa (serwer) po stronie publicznej połączenia WAN (na przykład internetu) i ma za zadanie pobrać odpowiedni publiczny adres IP i numer portu wymagany przez UDP do transmisji danych do urządzenia. Działanie polega na wysyłaniu serii wiadomości STUN przez port nasłuchiwanie STUN (3478) do klienta STUN w sieci LAN. Klient otrzymuje odpowiednie informacje dotyczące portu i zwraca je serwerowi STUN.

Problem z niektórymi klientami STUN polega na tym, że nie są w stanie wykorzystać informacji transportowych (adres IP i numer portu) z ich położenia w sieci. Ponadto nie każdy NAT obsługuje STUN, chociaż wiele nie ma z tym problemu. STUN nie działa z symetrycznym, dwukierunkowym NAT, który jest stosowany w sieciach klasy przemysłowej. Alternatywny dla STUN protokół nosi nazwę TURN (ang. *Traversal Using NAT*) i jest obecnie rozwijany dla urządzeń tej klasy.

Innym rozwijanym obecnie mechanizmem pozwalającym na przejście przez NAT jest ICE (ang. *Interactive Connectivity Establishment*). Jest on w szczególności przeznaczony do łączenia klientów VoIP z innymi klientami w sieci z wykorzystaniem do tego celu protokołu SIP.

## Protokół H.323

Protokół H.323 ITU-T (ang. *International Telephone Union Telecommunication Sector*) to zestaw standardów pozwalający na transport sesji audio-wideo, sygnalizowanie, kontrolowanie przepustowości i zarządzanie nią zarówno dla połączeń dwustronnych, jak i połączeń konferencyjnych. Protokół H.323 jest najczęściej używany przez aplikacje głosowe i aplikacje do wideokonferencji, w szczególności aplikacje zaimplementowane w internecie, które działają w czasie rzeczywistym. H.323 jest stosowany również w publicznych sieciach telefonicznych, sieciach komórkowych 3G, sieciach ISDN itp. Oprogramowanie firmy Microsoft o nazwie NetMeeting także bazuje na protokole H.323.

H.323 opiera się na stosowaniu zdefiniowanych elementów sieci. Najważniejsze z tych elementów to terminal, jednostki MCU (ang. *Multiple Control Unit*), bramy, elementy brzegowe gatekeeper zapewniające określanie nazw. Między tymi komponentami, które w aplikacjach H.323 są nazywane punktami końcowymi połączenia, zdefiniowana jest ścieżka. Minimalna definicja ścieżki obejmuje dwa terminale.

## Protokół Inter-Asterisk eXchange

Protokół *Inter-Asterisk eXchange* (IAX) jest używany przez system IP-PBX typu open source o nazwie Asterisk, który został opisany we wcześniejszej części rozdziału. W swojej drugiej wersji IAX2 stał się protokołem pozwalającym wielu producentom na współpracę z produktami VoIP bazującymi na rozwiązaniu Asterisk. IAX2 oferuje łączenie kilku rozmów w jeden strumień UDP, co pozwala zmniejszyć zapotrzebowanie na szerokość łącza.

Protokół IAX2 transportuje dane VoIP przez UDP i zwykle ma przypisywany port 4569. Strumień danych jest monitorowany przez zestaw poleceń i parametrów, które umożliwiają kontrolę multipleksowania sygnałów VoIP oraz przepływu ruchu. IAX2 jest kompatybilny zarówno z zaporą sieciową, jak i NAT, ponieważ sygnały i dane używają tej samej metody transportu. Dzięki temu protokół ten można porównać z innymi omówionymi w tym

podrozdziale, na przykład SIP, H.323 i MGCP. Wymienione metody polegają na komunikacji RTP do kontrolowania sesji, co jest metodą typu *poza pasmem*. Określenie „poza pasmem” oznacza, że komunikacja RTP odbywa się za pomocą innego kanału.

## Protokół Media Gateway Control Protocol

Protokół *Media Gateway Control Protocol* (MGCP) opisuje architekturę, która może być używana do kontrolowania urządzeń bram w sieciach IP bądź publicznych sieciach telefonicznych. Protokół opisuje zestaw sygnałów i poleceń kontrolnych stosowanych do monitorowania ruchu VoIP i jest często wykorzystywany przez ruch sieciowy zarówno H.323, jak i SIP. MGCP jest protokołem wewnętrznym używanym przez MGC (ang. *Media Gateway Controller*) oraz MG (ang. *Media Gateway*). MGC to urządzenie zajmujące się obsługą połączeń, stanowiące połączenie między urządzeniami sygnalizującymi IP. MGCP używa agenta połączeń i bramy multimediów do konwersji sygnałów VoIP przechodzących przez różne układy.

Protokół MGCP stał się popularny w aplikacjach VoIP, ponieważ nie przeprowadza kodowania ani nie transportuje ruchu VoIP. Funkcje te są zarezerwowane dla innych protokołów, wymienionych wcześniej. MGCP zapewnia mechanizm przełączania oraz funkcje sygnalizowania i zarządzania ścieżką, które są wykorzystywane przez wiele bram multimedialnych.

## System integracji telefonu z komputerem

System integracji telefonu z komputerem (ang. *Computer Telephony Integration*, CTI) wykorzystuje komputery do zarządzania zestawem usług używanych w centrach obsługi telefonicznej. System ten może przekierowywać połączenia do odpowiednich osób, wyświetlać okno z numerem telefonu osoby dzwoniącej, podawać jej dane, historię wcześniejszych połączeń z tą osobą, a także przeprowadzać inne dodatkowe operacje. System CTI wymaga stosowania specjalizowanego oprogramowania, bardzo często wykorzystuje API telefonii znajdujące się w sieciowym systemie operacyjnym, jak również wymaga sprzętu koniecznego do podłączenia komputera do różnych urządzeń telefonicznych. System CTI może być zaimplementowany w pojedynczym komputerze i funkcjonować tak, jakby był centrum obsługi telefonicznej. Ewentualnie może to być oprogramowanie typu klient-serwer, działające w rzeczywistym centrum obsługi telefonicznej.

System CTI oferuje szeroki zestaw możliwości, które w dużej mierze są uzależnione od oprogramowania, sprzętu oraz oczywiście od programisty. Poniżej wymieniono kilka z najczęściej stosowanych funkcji:

- ♦ uwierzytelnianie,
- ♦ zarządzanie kolejką połączeń,
- ♦ przekierowywanie połączeń oraz automatyczna obsługa połączeń,
- ♦ identyfikacja dzwoniącego, nazywana również ANI (ang. *Automatic Number Identification*),
- ♦ udzielanie pomocy klientowi,

- ♦ automatyczne wiadomości telefoniczne (Robocalls) zintegrowane z automatycznym wybieraniem numerów telefonów z podanej bazy,
- ♦ telemarketing,
- ♦ konferencje wideo,
- ♦ rozpoznawanie głosu oraz interaktywne odpowiedzi głosowe (IVR).

Wymienione usługi są obsługiwane przez Microsoft Windows Telephony Application Programming Interface (TAPI) oraz powiązane z nimi API, na przykład AT&T/Lucent/Novell's Telephone Service Application Programming Interface (TSAPI), w celu łatwego połączenia tych aplikacji z osprzętem.

Firma Telcordia (wcześniej znana jako Bell Communications Research) opracowała architekturę telefoniczną *Advanced Intelligent Network* (AIN lub IN) w celu umożliwienia rozszerzania systemu CTI bez konieczności polegania wyłącznie na funkcjach wbudowanych w przełącznikach sieciowych i routerach. Sektor Normalizacji Telekomunikacji (ang. *International Telecommunications Union*, ITU) używa modelu AIN w celu opracowania produktu Capability Set 1 (CS-1). AIN działa na poziomie przełącznika sieciowego lub punktu przełączania usługi (ang. *Service Switching Point*, SSP) i przekierowuje połączenia telefoniczne do logiki znajdującej się w punkcie kontroli usługi (ang. *Service Control Point*, SCP). Następnie logika analizuje podane numery i dopasowuje je do usługi żądanej przez dzwoniącego. W niektórych sytuacjach logika może dostarczać dzwoniącemu pewnych informacji, w innych następuje przekierowanie do kolejnego urządzenia typu *Intelligent Peripheral* (IP), które jest dołączone do odmiennego punktu kontroli usługi, gdzie nastąpi dalsze przetwarzanie połączenia. Wymienione terminy zostały zdefiniowane jako część modelu AIN.

Jedną z usług dostarczanych przez AIN jest przenośność numeru lokalnego (ang. *Local Number Portability*, LNP). Podczas zmiany operatorów, ale po pozostawieniu danego numeru telefonu, połączenie jest kierowane przez przełącznik sieciowy do nowej usługi telefonicznej, w której zostanie obsłużone.

Protokół *Computer Supported Telephony Applications* (CSTA) to zintegrowany standard (ECMA, Europejskie Stowarzyszenie na rzecz Standaryzacji), który został ratyfikowany przez ITU.

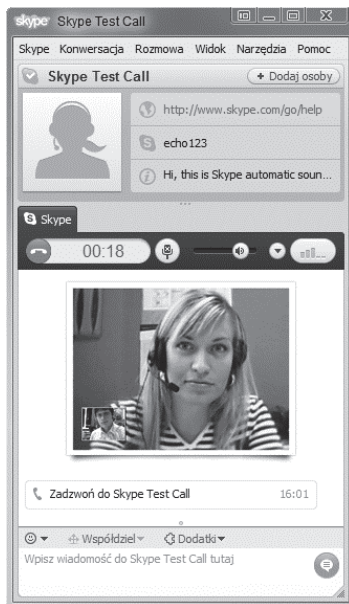
## Wideotelefonia

Wideotelefonia pozwala dwóm użytkownikom na rozmowę z możliwością wzajemnego widzenia się dzięki strumieniowi zsynchronizowanego wideo. Telefon wideo lub inaczej wideotelefon został po raz pierwszy zademonstrowany przez firmę AT&T w jej pawilonie na wystawie New York World's Fair (1964) oraz Expo w Montrealu (1967). Tak zwany Picturephone, wprowadzony na rynek konsumencki w 1971 roku przez AT&T, sprzedawał się tak kiepsko, że firma zakończyła jego produkcję w roku 1974. W tamtym czasie cena była zbyt wysoka lub użytkownicy nie chcieli widzieć się wzajemnie podczas rozmowy telefonicznej. Wprowadzenie w Meksyku w roku 2006 połączeń wideo z wykorzystaniem protokołu H.324 i wideotelefonów LG-Nortel również nie zdobyło dużej popularności.

Jednym z popularniejszych rozwiązań oferujących konferencje wideo jest Skype, aplikacja VoIP oferująca także funkcje komunikatora internetowego, transmisję wideo oraz transfer plików. Moduł VoIP został utworzony przez ten sam zespół programistów, który wcześniej zbudował sieć Kazaa — program Skype stał się równie popularny. Powodzenie aplikacji Skype wynika z faktu udostępniania przez nią wielu usług, na przykład bezpłatnego połączenia międzynarodowego wykonywanego między komputerami. Istnieje możliwość zakupu usług dodatkowych, umożliwiających na przykład wykonywanie połączeń telefonicznych za pomocą Skype'a. Firma Skype została kupiona przez eBay, ale obecnie jest wyodrębniona jako oddzielny podmiot. Na rysunku 26.6 pokazano wideokonferencję przeprowadzaną za pomocą Skype'a.

### Rysunek 26.6.

*Wideokonferencja w programie Skype; małe zdjęcie pokazuje osobę, która zainicjowała połączenie*



## Mobile VoIP

Mobile VoIP to aktywnie rozwijana technologia, która pozwala na wideopołączenia telefoniczne przez sieć bezprzewodową. Stanowi ona funkcję sieci i charakteryzuje się dużą szybkością.

Jednym z podejść jest użycie klienta SIP w telefonie do komunikacji z siecią z wykorzystaniem pakietów RTP dla kanału głosowego. To jest najczęściej stosowana metoda. Inne podejście polega na utworzeniu programowej bramy służącej do wysyłania danych do serwera SIP, w którym dane SIP i RTP mogą być skonwertowane na postać protokołów sieci bezprzewodowej.

Niektóre telefony GSM (ang. *Global System for Mobile Communications*) wykorzystują do transportu VoIP przez sieć GSM technologię *Unlicensed Mobile Access* (UMA) *Generic Access Network* (GAN). UMA to nazwa marki, natomiast 3GPP GAN to technologia. Sieci GAN transmitują dane SIP przez sieci IP.

Wysokiej wydajności technologie EVDO w wersji A (*Evolution-Data Optimized*), HSDA (*High-Speed Downlink Packet Access*), Wi-Fi oraz WiMAX (*Worldwide Interoperability for Microwave Access*) oferują na tyle dużą szybkość, że pozwalają na obsługę połączeń wideo. Ogólna zasada jest taka, że sieci Wi-Fi są znacznie tańsze niż EVDO lub HSDPA, ale te dwie ostatnie oferują większy zasięg.

Telefonia wideo zaczęła być szerzej dostępna w telefonach komórkowych działających w sieciach GSM 3G (ang. *Universal Mobile Telecommunications System*, UMTS). Według analityków Wireless Intelligence w drugim kwartale 2009 sprzedano ponad 130 milionów telefonów wyposażonych w funkcję połączeń wideo. Sieci GSM są dostępne w 59 krajach na świecie. Nie ma żadnych danych dotyczących stopnia wykorzystania funkcji połączeń wideo, ale bardzo szybko zwiększa się ich dostępność; coraz powszechniejsze jest stosowanie funkcji przechwytywania wideo, co może potwierdzić każdy wielbiciel serwisu YouTube.

Telekomunikacja wideo to dobrodziejstwo dla osób cierpiących na schorzenia związane ze słuchem lub mową. W Stanach Zjednoczonych Federalna Komisja Łączności (ang. *Federal Communications Commission*, FCC) wraz z dostawcami telefonów komórkowych wprowadza program Video Relay Service, którego celem jest umożliwienie wykorzystywania języka migowego podczas komunikacji telefonicznej.

## Kamery internetowe

Aplikacje biznesowe służące do wideokonferencji oraz stosowane w telefonii zyskały powszechną akceptację. Ich popularność może się zwiększyć jeszcze bardziej, gdy podróże służbowe staną się droższe. Spora liczba producentów sprzedaje systemy przeznaczone do prowadzenia wideokonferencji lub integruje je z pakietami telekomunikacyjnymi. Pakiet Unified Communications Manager firmy Cisco to jeden z przykładów tego rodzaju oprogramowania — istnieje wiele innych. Zestaw głośnomówiący Polycom pozwala na dodanie połączeń wideo do oferowanego systemu.

Na rynku dostępnych jest duża liczba laptopów wyposażonych we wbudowane kamery internetowe, na przykład modele firmy Apple (seria Macbook), Sony Vaio, Dell XPS oraz Asus Eee. Kamery są zazwyczaj umieszczone nad ekranem laptopa i obsługują funkcje wideo dla VoIP.

Obsługę połączeń wideo przy użyciu tych kamer można znaleźć w różnych programach, takich jak AOL Instant Messenger (AIM), Skype, Windows Live Messenger, Yahoo! Messenger, iChat, Camfrog. Szeroko rozpowszechnione są też inne możliwości.

Kamery internetowe są również powszechnie stosowane w monitoringu. Niektóre są podłączone do komputerów za pomocą linii telefonicznych, inne są połączone z sieciami Ethernet. Oddzielną klasą kamer internetowych są urządzenia z wbudowanym serwerem WWW, których obraz można wyświetlać w przeglądarce internetowej. Tego rodzaju urządzenia, często pod nazwą *kamery sieciowe*, są sprzedawane przez firmy Axis i Panasonic.

Kamery internetowe można znaleźć wszędzie, na przykład w miejscach publicznych. Są zainstalowane m.in. w Parku Narodowym Yellowstone (pokazując Old Faithful Geyser, rysunek 26.7) czy na placu Times Square w Nowym Jorku.

**Rysunek 26.7.**  
Strumieniowany  
obraz kamery  
internetowej w Parku  
Narodowym  
Yellowstone (USA)



Niektóre z tych kamer są skonfigurowane w celu dostarczania obrazów statycznych, zazwyczaj z częstotliwością jednego obrazu na minutę, jednak nowsze modele pozwalają na strumieniowanie wideo w czasie rzeczywistym. Na rysunku 26.7 pokazano nowszą kamerę strumieniującą wideo, ale na witrynie internetowej parku nadal widnieje obraz ze starej kamery, dostarczającej jedynie obraz statyczny.

Kilka witryn w internecie kataloguje łącza do kamer internetowych; najbardziej znana to *Earthcam.com*. Oglądanie pochodzących z nich obrazów może być pewną rozrywką czy też umożliwiać sprawdzenie warunków pogodowych w rejonie, do którego chcielibyśmy się wybrać.

## Podsumowanie

W rozdziale omówiono telefonię komputerową oraz aplikacje VoIP. Telefonia komputerowa oznacza używanie telefonów i komputerów w sieci telefonicznej lub Ethernet bądź też w obu tych sieciach.

Systemy operacyjne pozwalają na obsługę telefonii dzięki rodzimym API, które producenci aplikacji wykorzystują do budowy swoich programów. Komputery mogą być łączone z telefonami i zarządzać nimi oraz tworzyć podstawy systemów PBX. Aplikacje telefoniczne są budowane z zastosowaniem struktur służących do tworzenia aplikacji i stanowią podstawę dla systemów CTI. W bardzo skomplikowanych systemach telefonicznych wykorzystuje się technologię CTI.

W rozdziale przedstawiono także aplikacje umożliwiające połączenia głosowe i wideo. Obejmują one wideotelefony, kamery internetowe oraz oprogramowanie do prowadzenia wideokonferencji.

Następna część zawiera rozdziały poświęcone bezpieczeństwu w sieci. Zostaną w nich omówione protokoły bezpieczeństwa, takie jak HTTPS i SSL. Czytelnik pozna ich funkcjonowanie, sposoby ich wykorzystywania oraz chronione przez nie usługi sieciowe.



## Część VI

# Bezpieczeństwo w sieci

### **W tej części:**

**Rozdział 27.** Usługi i protokoły bezpieczeństwa

**Rozdział 28.** Zapory sieciowe, bramy i serwery proxy

**Rozdział 29.** Sieci VPN



## Rozdział 27.

# Usługi i protokoły bezpieczeństwa

### W tym rozdziale:

- ♦ Zabezpieczanie sieci
- ♦ Rodzaje ataków i exploity
- ♦ Ochrona systemów
- ♦ Metody szyfrowania
- ♦ System bezpieczeństwa sieciowego Kerberos

Bezpieczeństwo w sieci jest realizowane za pomocą zestawu technologii ułożonych warstwowo i wzajemnie na siebie nachodzących. W rozdziale zostaną przedstawione różne obszary sieci, które mogą być wykorzystywane na przykład przez hakerów w celu włamania się do systemów sieciowych i zyskania dostępu do nich oraz przechowywanych w nich danych. Istnieje możliwość sprawdzania (skanowania) sieci pod kątem potencjalnych luk w zabezpieczeniach. Zaprezentowane będą więc pewne standardowe narzędzia, takie jak baza danych National Vulnerability Database, oraz powiązane z nimi zasoby.

Zostanie też przedstawiona lista najważniejszych kroków, które można podjąć w celu zabezpieczenia sieci.

Omówione będą ponadto dwie adaptacyjne technologie zapewniające bezpieczeństwo sieci. Pierwsza to *Network Location Awareness* (NLA), która może być wykorzystywana do wykrywania stanu połączenia sieciowego oraz do odpowiedniego dostosowywania polityki systemowej. Druga technologia, *Network Access Protection* (NAP), może aktywnie poddawać kwarantannie systemy, które nie spełniają systemowej polityki bezpieczeństwa.

Wysyłanie ruchu sieciowego przez internet obejmuje także stosowanie połączeń niezabezpieczonych. W rozdziale zostaną omówione trzy protokoły bezpieczeństwa: IPsec, *Transport Layer Security/Secure Socket Layer* oraz HTTPS. Technologie te pozwalają na szyfrowanie danych albo tworzenie bezpiecznych połączeń za pomocą tunelowania lub innych metod.

Zaprezentowane będą też różne metody szyfrowania ruchu sieciowego. Czytelnik pozna różnorodne formy szyfrowania stosowane w kryptografii, a także wykorzystywanie symetrycznych i asymetrycznych algorytmów kluczy. Wymienione szyfry mogą być używane zarówno do uwierzytelniania i sprawdzania danych, jak i do ich ochrony. Jako przykład tego rodzaju technologii zostanie omówiony system bezpieczeństwa Kerberos.

## Ogólny opis bezpieczeństwa sieci

Sieć jest atakowana na coraz bardziej wyrafinowane sposoby, które nieustannie są rozwijane. Wydaje się, że bieżące wiadomości zawsze mogą zawierać najnowszego wirusa, konia trojańskiego lub robaka, a w wiadomości e-mail z banku może znajdować się ostrzeżenie dla danego klienta, że ktoś przechwycił informacje związane z jego kartą kredytową. Jeżeli funkcjonowanie sieci wydaje się dziwne lub działa w niej jakiś system, to użytkownik jest usprawiedliwiony, kiedy zachowuje się jak paranoik. Zapewnienie bezpieczeństwa sieci przypomina trochę kreskówkę *Spy vs. Spy*<sup>1</sup>. Żyjemy w niepewnych czasach, ale zawsze istnieje możliwość zniechęcenia potencjalnych atakujących przez lepsze zabezpieczenie sieci, a tym samym zmuszenie ich do poszukania łatwiejszego celu ataku.

Nie ma jednej skutecznej metody ochrony sieci. Każdy system bezpieczeństwa może zostać złamany, jeżeli nie z zewnątrz, to z wewnątrz. Najlepszym sposobem zapewnienia bezpieczeństwa sieci jest stosowanie różnych warstw zabezpieczeń. W takim przypadku, zanim atakujący uzyska dostęp, będzie musiał pokonać co najmniej dwa systemy zabezpieczeń. Regularna zmiana parametrów bezpieczeństwa, na przykład haseł, oraz podział sieci na części to dwie kolejne metody, które są nieocenione. W rozdziale zostaną przedstawione niektóre technologie używane do zabezpieczania systemów sieciowych i ruchu przechodzącego przez sieć.

## Luki w zabezpieczeniach sieci

Luki w zabezpieczeniach sieci to słabe punkty, które można wykorzystać w celu uzyskania dostępu do danego systemu. Przyczyny złamania zabezpieczeń mogą być różne: stosowanie słabych haseł przez użytkowników, wirusy i konie trojańskie, błędy w oprogramowaniu, pliki wykonywalne lub skrypty uruchomione w systemie, a także umieszczenie fragmentów kodu w systemie. Kiedy luka w zabezpieczeniach staje się znana, są tworzone programy, które ją wykorzystują. Programy takie określa się *exploitami*, rozpoznając je równie szybko jak wirusy.

Każdy program zawiera jakieś błędy bądź procedury, które można złamać. Aktualizacje regularnie dostarczane przez firmy, na przykład infrastruktura Microsoft Update, mają za zadanie usuwać odkryte luki. Ujawnienie luki w systemie przed opracowaniem aktualizacji poprawiającej dany błąd naraża system na ataki z wykorzystaniem tej luki. Ataki tego rodzaju są nazywane *Zero Day Exploit*. Można w to wierzyć bądź nie, ale istnieją firmy dostarczające usługę subskrypcji, która informuje klientów o sposobie wykorzystania Zero Day

---

<sup>1</sup> Znana amerykańska kreskówka, a także gra komputerowa dostępna na różnych platformach, takich jak C64, Atari, Amiga, PC, konsole do gier — *przyp. tłum.*

Exploit do atakowania systemów. Oczywiście istnieją też inne firmy, które z kolei informują klientów, jak się bronić przed tego rodzaju atakami. Jesteśmy więc świadkami nieustannego wyścigu między atakującymi i atakowanymi.

Najlepszym zaleceniem dotyczącym Zero Day Exploit jest stosowanie we wszystkich systemach uaktualnień tuż po ich wydaniu. Wielu administratorów wzdrga się przed traktowaniem tej sugestii jako przykładu najlepszego rozwiązania, ponieważ aktualizacje mogą wyeliminować pewne błędy, ale jednocześnie wprowadzić nowe. Automatyczne uaktualnianie systemów produkcyjnych wprowadza element niepewności, który by nie występował, gdyby oprogramowanie systemowe nie ulegało zmianom.

Jedną z metod stosowanych do wykrywania luk w zabezpieczeniach sieci jest próbkowanie sieci za pomocą narzędzia analizy ryzyka — skanera luk w zabezpieczeniach. Tego rodzaju skanery działają w ten sposób, że skanują sieć dla wszystkich przypisanych adresów IP, określają otwarte porty, a następnie budują listę programów i systemów operacyjnych, które funkcjonują w różnych systemach. Skanerami tego typu są skanery portów, skanery sieciowe, skanery witryn internetowych oraz dedykowane narzędzia znajdujące się w platformach struktur przeznaczonych do zarządzania. Po zakończeniu badania początkowego skaner może zbudować mapę sieci albo utworzyć raport. Jeżeli skaner używa SNMP, WMI lub innego protokołu zarządzania, to ma możliwość sprawdzania systemów i aplikacji w celu określenia nie tylko ich rodzaju, ale także numerów wersji i poziomu aktualizacji. Mogą być stosowane oznaczenia poziomów zagrożenia oraz listy zaleceń i działań, które administratorzy powinni podjąć w celu dalszego zabezpieczenia sieci.

Przemysłowy standard określania podatności systemu komputerowego na luki w zabezpieczeniach ma nazwę *Common Vulnerability Scoring System* (CVSS). Ocena bazuje na zestawie pomiarów i dotyczy podstawowych lub poważnych luk w zabezpieczeniach, wskazuje zagrożenia oraz uwzględnia czynniki związane z implementacją bądź środowiskiem. Więcej informacji na temat systemu oceny można znaleźć na witrynie internetowej CVSS FIRST (ang. *Forum of Incident Response and Security Teams*), znajdującej się pod adresem <http://www.first.org/cvss/>. Standard ten (obecnie w wersji 2.) został opracowany przez grupę *CVSS Special Interest Group* — SIG. Do kalkulatora online dostarczanego przez bazę danych National Vulnerability Database w sekcji SVSS Scoring można wprowadzić różne dane w celu otrzymania określonych ocen (więcej na ten temat w dalszej części rozdziału).

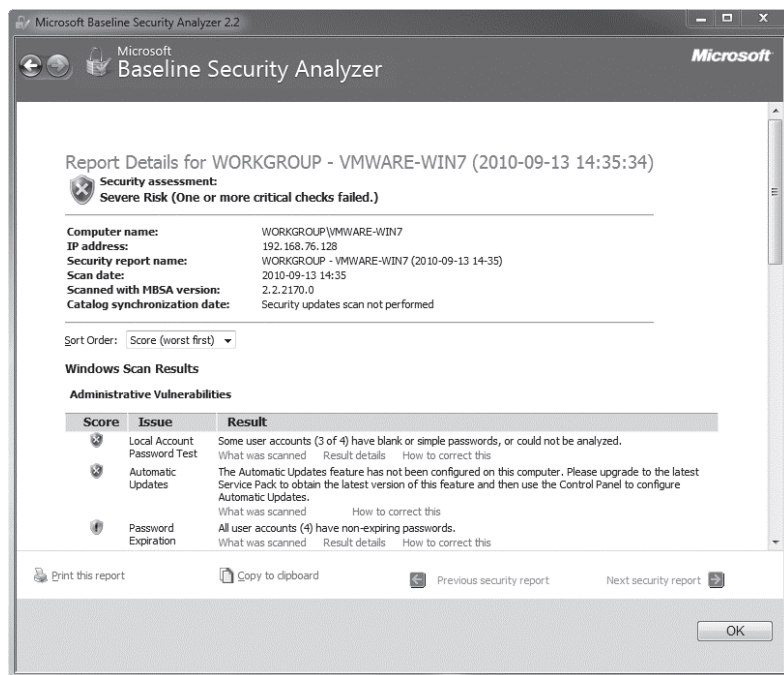
Powszechnie dostępne są również inne narzędzia. Jednym z przykładów jest *Microsoft Baseline Security Analyzer* (MBSA; <http://technet.microsoft.com/en-us/security/cc184924.aspx>), które zostało ostatnio wydane w wersji 2.2. Narzędzie MBSA używa infrastruktury Microsoft Update oraz agenta lokalnego w celu określenia, czy system Windows jest bezpieczny i uaktualniony. Według firmy Microsoft ta bazująca na internecie usługa przeprowadza tygodniowo sprawdzanie trzech milionów systemów pod kątem istnienia luk w zabezpieczeniach. MBSA może skanować systemy nie tylko takie jak Vista/Server 2008, ale również Windows CE i Embedded, serwery Microsoft SQL Server oraz Microsoft Internet Information Server. Przykładowy raport narzędzia MBSA został pokazany na rysunku 27.1.

Informacje używane do określenia podatności sieci na luki w zabezpieczeniach są dostarczane przez wiele firm i organizacji, między innymi:

- ♦ Common Vulnerabilities and Exposures (CVE, <http://cve.mitre.org>),
- ♦ Computer Emergency Response Team (CERT, <http://www.cert.org>) na uniwersytecie Carnegie Mellon,

**Rysunek 27.1.**

Przykładowy raport dotyczący luk w zabezpieczeniach wygenerowany przez narzędzie Microsoft Baseline Security Analyzer



- ♦ Microsoft Security Response Center ([http://technet.microsoft.com/pl-pl/library/cc751383\(en-us\).aspx](http://technet.microsoft.com/pl-pl/library/cc751383(en-us).aspx)),
- ♦ Open Source Vulnerability Database (OSVDB, <http://www.osvdb.org>),
- ♦ Open Web Application Security Project (<http://www.owasp.org/index.php/Category:Vulnerability>),
- ♦ SANS Institute (<http://www.sans.org>),
- ♦ archiwum luk w zabezpieczeniach prowadzone przez Secunia (<http://secunia.com>),
- ♦ archiwum luk w zabezpieczeniach prowadzone przez SecurityFocus (<http://www.securityfocus.com/bid>),
- ♦ archiwum luk w zabezpieczeniach prowadzone przez VUPEN (<http://www.vupen.com/english/security-advisories/>).

Skanowanie pod kątem luk w zabezpieczeniach oraz rozpoznawanie sieci to techniki stosowane również przez atakujących, którzy próbują uzyskać dostęp do sieci, a także funkcje niektórych robaków.

## Baza danych National Vulnerability Database

Na początku listy wymienionej w poprzednim podrozdziale zamieszczono CVE (ang. *Common Vulnerabilities and Exposures*) — słownik zagrożeń bezpieczeństwa obsługiwany przez MITRE Corporation dla wydziału National Cyber Security Division Departamentu Bezpieczeństwa Krajowego Stanów Zjednoczonych. CVE używa systemu identyfikatorów, które unikalnie identyfikują znane zagrożenia. Czynniki zagrożenia są czasami określane

jako identyfikatory CVE, nazwy, numery, identyfikatory lub po prostu CVE. Umieszcza się je w bazie danych po zidentyfikowaniu ich przez firmy trzecie jako potencjalnych czynników zagrożenia. Czynniki takie otrzymuje numer CAN (ang. *Candidate Number*), następnie jest analizowany oraz potwierdzany i staje się oficjalnym wpisem na liście CVE.

Funkcją MITRE Corporation w obsłudze tej bazy danych jest opisywanie zagrożeń, nadawanie im numerów CAN oraz publiczne udostępnianie zebranych informacji. Baza danych CVE zawiera znane zagrożenia zebrane z całego świata i jest dostępna bezpłatnie. Z punktu widzenia CVE luka w zabezpieczeniach jest błędem w oprogramowaniu, który umożliwia uzyskanie nieuprawnionego dostępu do systemu bądź sieci. Błąd w prawidłowym stosowaniu oprogramowania lub pozostawienie systemu otwartego nie jest uznawany za lukę w zabezpieczeniach, a tym samym nie znajduje się w bazie danych. Jeżeli na przykład sieciowy system operacyjny pozwala na ustalanie silnych haseł, ale użytkownik nie jest zmuszany do ich stosowania lub w ogóle nie musi stosować hasła, to w takim przypadku nie mówimy o luce w zabezpieczeniach. (Krótkie hasła są często celem ataku z wykorzystaniem słownika).

Luka w zabezpieczeniach występuje, gdy:

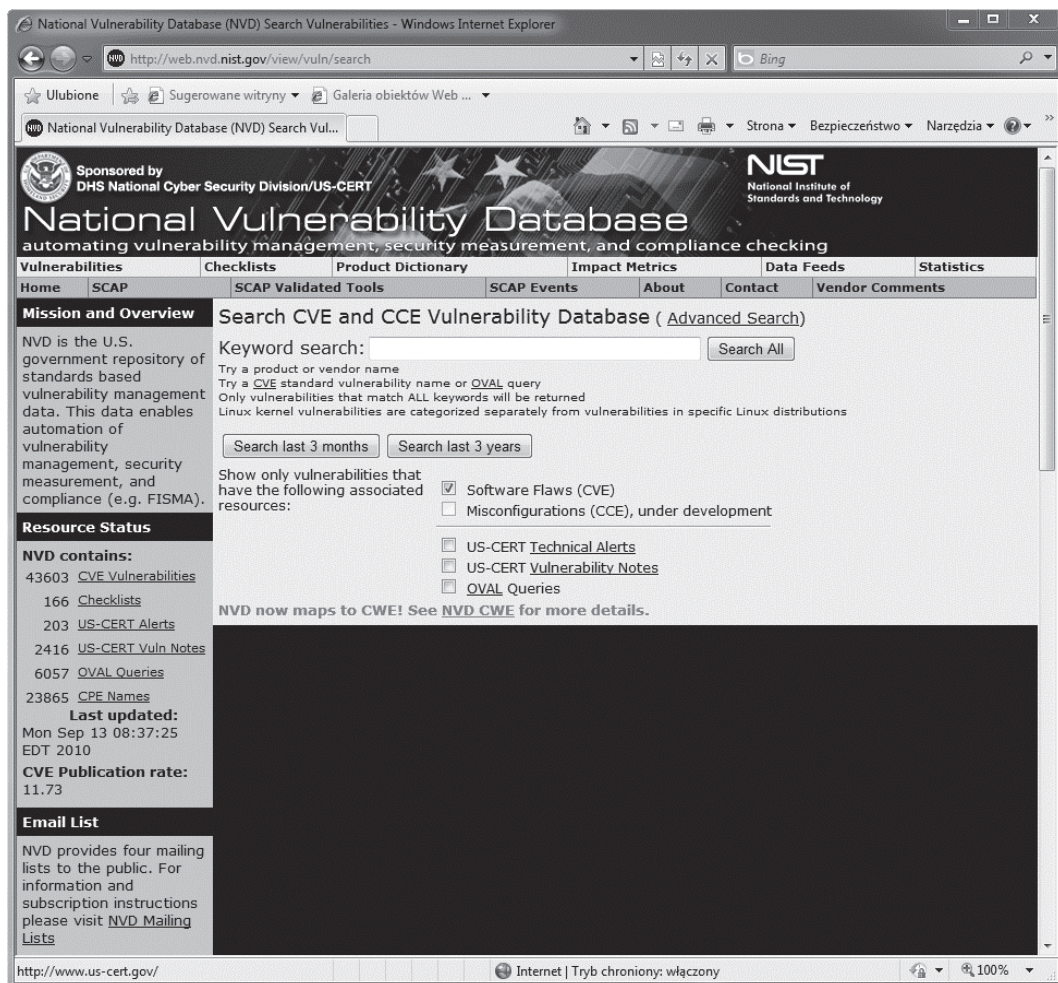
- ♦ atakujący może uzyskać dostęp do danych, do których nie ma uprawnień,
- ♦ atakujący może podszyć się pod innego użytkownika,
- ♦ atakujący może doprowadzić do sytuacji, w której usługa będzie niedostępna dla innych użytkowników.

Istnieje możliwość przeszukania listy CVE w bazie danych National Vulnerability Database (NVD) przy wykorzystaniu witryny internetowej <http://nvd.nist.gov/>. Na rysunku 27.2 pokazano stronę internetową podczas operacji przeszukiwania NVD. Obecnie baza danych zawiera informacje o 45 335 znanych lukach w zabezpieczeniach i może zostać pobrana w celu jej przeglądania online. Dane znajdujące się w bazie obsługują program ISAP (ang. *U.S. Information Security Program*) oraz działają w charakterze repozytorium dla protokołu *Security Content Automation Protocol*, używanego do monitorowania bezpieczeństwa sieci i szacowania poziomu zagrożenia.

Baza danych NVD wykorzystuje strukturalny system nazw dla różnych typów systemów informatycznych, oprogramowania oraz innych pakietów. System ten ma składnię podobną do używanej w adresach URI (ang. *Uniform Resource Identifiers*) stosowanych w internecie; ma nazwę *Common Product Enumeration* (CPE) (katalog produktów) i jest dostarczany w formacie możliwego do pobrania pliku XML jako część bazy danych. Plik CPE XML znajduje się pod adresem [http://static.nvd.nist.gov/feeds/xml/cpe/dictionary/official-cpe-dictionary\\_v2.2.xml](http://static.nvd.nist.gov/feeds/xml/cpe/dictionary/official-cpe-dictionary_v2.2.xml).

## Miejsca ataku

Bezpieczeństwo sieci najczęściej jest naruszane z zewnątrz. Typowy atak dotyczy luk w zabezpieczeniach, w oprogramowaniu bądź sprzęcie. Jednak luki w bezpieczeństwie, które pozwalają na dostanie się do wewnątrz sieci, bardzo często są najskuteczniejsze, ponieważ mogą działać niewykryte.



**Rysunek 27.2.** Baza danych National Vulnerability Database zawiera informacje o znanych zagrożeniach sieciowych oraz dostarcza powiązanych z nimi informacji o poziomie niebezpieczeństwa i potencjalnych sposobach ochrony

Najczęstszymi obszarami ataków są:

- ♦ **Zewnętrzne — dostępność systemu.** System może być przeciążony przez rozgłoszenie w sieci z dużą liczbą komputerów sfalszowanego pakietu ICMP, w którym zmieniono adres źródła na adres atakowanego systemu, co skutkuje dużą ilością odpowiedzi ECHO do atakowanego systemu. W takim przypadku mamy do czynienia z tzw. atakiem smerfów (ang. *Smurf Attack*).
- ♦ **Zewnętrzne — odmowa usług (DoS, Denial of Service).** Atak, w którym usługa sieciowa jest zasypana żądaniami, nazywa się odmową usług (DoS). Najbardziej znanym przykładem ataku DoS jest atak na serwer nazw domeny (DNS). Kiedy taki atak się powiedzie, to dla systemów obsługiwanych przez zaatakowany DNS adresy innych systemów w internecie lub intranecie będą niemożliwe do ustalenia, a tym samym niedostępne.

Atak *Distributed Denial of Service* (DDoS) oznacza atak przeprowadzony przez ogromną liczbę złamanych systemów, które działają jak tzw. komputery zombies i mogą być zamienione w botnety, czyli „roboty sieciowe”.

- ♦ **Zewnętrzne lub wewnętrzne — uwierzytelnianie.** Atakujący podszywa się pod tożsamość innego użytkownika.
- ♦ **Dane w trakcie transportu.** Ruch sieciowy jest przechwytywany w trakcie transmisji, modyfikowany, a następnie wysyłany do miejsca przeznaczenia. Taki atak nazywa się „atakami z osobą pośrodku” (ang. *man-in-the-middle attack*); jego efektem może być podsłuchanie danych.
- ♦ **Wewnętrzne — robaki, konie trojańskie oraz inne programy otwierające tylne drzwi.** Wymienione programy dostarczają atakującemu metod kontrolowania systemów wewnątrz sieci oraz możliwość zmiany komputerów na zombies. Tylne drzwi mogą być programami wykonywalnymi lub algorytmami, które mogą omijać mechanizm uwierzytelniania sieciowego, przeprowadzać różne operacje i pozostawać w ukryciu.

Rootkit to rodzaj programu otwierającego tylne drzwi — potrafi ukrywać się jako sterownik niskiego poziomu lub moduł jądra. Rootkit nie pojawia się w systemie plików, a na liście procesów może widnieć jako zwykły proces systemowy.
- ♦ **Bezpośredni dostęp wewnątrz.** Atak może nastąpić z nośnika takiego jak dysk optyczny, pamięć USB, napęd przenośny itp.

W trakcie opracowywania oprogramowania firma Microsoft używa modelu szacowania zagrożenia, który został nazwany podejściem STRIDE (<http://msdn.microsoft.com/en-us/magazine/cc163519.aspx>). Skrót STRIDE oznacza:

- ♦ *Spoofing Identity (authentication)*, czyli podszywanie się pod inną osobę (uwierzytelnianie) — atakujący może podszyć się pod innego użytkownika. Użytkownicy i systemy muszą stosować uwierzytelnianie za pomocą haseł, certyfikatów cyfrowych bądź innych metod.
- ♦ *Tampering with Data (integrity)*, czyli złośliwa modyfikacja danych (spójność) — atakujący modyfikuje dane. Metody stosowane do zapewnienia spójności danych obejmują między innymi procedury sprawdzania błędów w danych.
- ♦ *Repudiation (non-repudiation)*, czyli wyparcie się (brak możliwości wyparcia się) — poszczególne osoby odrzucają odpowiedzialność za przeprowadzane operacje.
- ♦ *Information Disclosure (confidentiality)*, czyli dotarcie do informacji przez osobę niemającą odpowiednich uprawnień (zapewnienie poufności). W tym przypadku atakujący zyskuje dostęp do informacji poufnych. Sieci stosują ograniczenia dostępu za pomocą list dostępu, domen, usług katalogowych oraz innych funkcji sieciowych systemów operacyjnych, aby dostęp mogły uzyskać tylko te osoby, które mają do tego uprawnienia.
- ♦ *Denial of Service (availability)*, czyli odmowa usług (dostępność). Atak typu DoS może doprowadzić do tego, że określona usługa stanie się niedostępna. Użytkownicy i systemy muszą być w niezawodny sposób połączeni z inicjowanymi zdarzeniami. Istnieje możliwość stosowania dzienników rejestrujących wszelkie zdarzenia, dołączenia danych uwierzytelniających użytkownika i systemu do danych, a także

zapewnienia bezpiecznych kanałów komunikacji w celu transferu danych. W przypadku ważnych systemów powinny istnieć kopie bezpieczeństwa, które zapewniają możliwość działania po wystąpieniu awarii.

- ♦ *Elevation of Privilege (authorization)*, czyli nieautoryzowane zwiększenie uprawnień (uwierzytelnianie). W tej sytuacji użytkownik systemu zyskuje większe uprawnienia, niż powinien mieć. Zasoby muszą być dostępne, kiedy jest to wymagane. Systemy odpowiedzialne za zarządzanie dostępem do zasobów muszą być bezpieczne. Natomiast użytkownicy powinni mieć najmniejszy poziom uprawnień, który pozwoli im na wykonywanie pracy.

## Reguły tworzenia bezpiecznej sieci

Środki bezpieczeństwa powinny koncentrować się na trzech oddzielnych poziomach:

- ♦ **Szacowanie ryzyka i ochrona przed zagrożeniem.** Do najefektywniejszych technologii ochrony przed zagrożeniami zalicza się kontrolę dostępu użytkownika, szyfrowanie i zapory sieciowe, które będą dokładniej omówione w rozdziale 28.
- ♦ **Wykrywanie zagrożeń.** Systemy wykrywania zagrożeń obejmują skanery antywirusowe i antyspyware'owe, systemy wykrywania włamań (ang. *Intrusion Detection System*, IDS), badanie zdarzeń oraz heurystyczną analizę zdarzeń w dziennikach zdarzeń.
- ♦ **Odpowiedź.** Odpowiedzią na wykrycie włamania do systemu może być kwarantanna systemu bądź podsieci, przywrócenie stanu z ostatniej dobrej kopii zapasowej, naprawa i uaktualnienie mechanizmu ochrony.



Biorąc pod uwagę stopień skomplikowania nowoczesnych systemów, trzeba zastrzec, iż nie ma stuprocentowej gwarancji, że naprawiony po włamaniu system w pełni powróci do stanu sprzed ataku. Atakujący stosują coraz bardziej zaawansowane metody w celu zainfekowania systemu bądź zdobycia nad nim kontroli i mogą w nim osadzać zamienniki podstawowych jego komponentów. Dlatego też zaleca się posiadanie wielu obrazów systemu, które można wykorzystać do przywrócenia jego stanu sprzed ataku. W przypadku systemów o znaczeniu krytycznym warto rozważyć tworzenie systemów lustrzanych, stosowanie metody BCV (ang. *Business Continuity Volumes*) oraz innych metod tworzenia kopii zapasowej.

Z punktu widzenia kosztów i trudności implementacji każdy z trzech wymienionych poziomów bezpieczeństwa jest zwykle o rząd wielkości droższy niż poziom niższy. Dlatego wykrywanie zagrożeń może kosztować dziesięciokrotnie więcej niż szacowanie zagrożenia, natomiast odpowiedź może być już stukrotnie droższa od ochrony przed zagrożeniem. Warto zastanowić się nad kosztem instalacji oprogramowania skanowania antywirusowego i antyspyware'owego lub zapory sieciowej w stosunku do ilości czasu i kosztu związanego z naprawą wielu systemów, które padły ofiarą ataku.

Jedną z najważniejszych reguł bezpiecznego projektu sieci jest minimalizacja „obszaru ataku” w systemie lub sieci. Obszar ataku to ujawniony profil systemu, który jest dostępny do przeglądania przez użytkownika bądź atakującego, zawierający na przykład następujące informacje:

- ♦ protokoły działające w danej sieci bądź systemie,
- ♦ interfejsy sieciowe, które mogą odpowiadać na zapytania lub wiadomości,

- ♦ otwarte porty,
- ♦ usługi działające w dostępnym systemie,
- ♦ pola danych wejściowych użytkownika.

Im mniejsza liczba dróg, którymi atakujący może spenetrować system, tym większe bezpieczeństwo. Jednak kiedy atakujący dostanie się do systemu, to mniejszy obszar ataku wcale nie ogranicza ilości zniszczeń, których intruz może dokonać.

Serwer *Microsoft Internet Security and Acceleration* (ISA) to przykład koncepcji systemu „domyślnie bezpiecznego”. Serwer ISA to brama buforowania treści oraz serwer proxy opracowany na podstawie oryginalnego serwera Microsoft Proxy Server. Podczas instalacji serwera ISA następuje zamknięcie wszystkich portów, nie ma aktywnych protokołów i nie ma zdefiniowanych wpisów dla sieci użytkownika. Inicjalizacja serwera polega na otwarciu portów, za których pomocą ma być obsługiwany ruch wychodzący i przychodzący, mapowaniu ruchu portu HTTP do portu 8080 serwera ISA, otwarciu kilku dodatkowych portów dla HTTPS, FTP i IMAP oraz udostępnieniu wybranych usług. Kolejnym krokiem jest zdefiniowanie systemów, które posiadają uprawnienia do wysyłania danych, i systemów, które mogą przyjmować dane. Administrator definiuje zestaw reguł, które są stosowane w kolejności narzucającej hierarchię lub pierwszeństwo. Utworzenie polityki bezpieczeństwa sieci może być zajęciem czasochłonnym, ale minimalizuje obszar ataku, na który będzie narażony serwer ISA.

Poniżej przedstawiono 14 najlepszych wskazówek dotyczących bezpieczeństwa sieci.

1. **Używaj zapory sieciowej.** Zawsze należy pracować za zaporą sieciową. Warto wybierać sprzętową zaporę sieciową zamiast programowej i upewnić się, że oferuje ona izolację zarówno fizyczną, jak i protokołu. System połączony z internetem i pozbawiony zapory sieciowej może być złamany w ciągu kilku minut.
2. **Wymuszaj stosowanie silnych haseł.** Zawsze trzeba zmieniać każde hasło domyślne. Należy stosować hasła o długości minimum ośmiu znaków, łączące małe i duże litery, cyfry oraz znaki w ciągu tekstowe, które nie występują w słowniku.
3. **Zainstaluj oprogramowanie antywirusowe i antyspyware’owe.** Szczególnie dotyczy to bram sieci.
4. **Stosuj niezawodną politykę tworzenia kopii zapasowej systemu.** Obrazy systemu należy przechowywać dla wszystkich systemów.
5. **Aktualizuj oprogramowanie.** Zawsze należy aktualizować oprogramowanie tuż po wydaniu aktualizacji, ale warto mieć kopię zapasową na wypadek wystąpienia jakichkolwiek problemów związanych z aktualizacją. Szczególną uwagę trzeba poświęcić każdemu programowi, który ma styczność z siecią publiczną. Bardzo ważne jest aktualizowanie na przykład serwera WWW i przeglądarki internetowej.
6. **Podziel sieć na podsieci.** To zapewnia fizyczną izolację sieci dzięki adresom IP.
7. **Szyfruj poufne dane i używaj bezpiecznych protokołów podczas transmisji danych.** Danych, których nigdy nie opublikowalibyśmy w *dzienniku ogólnokrajowym*, nie należy wysyłać w postaci zwykłego tekstu.

8. **Uważaj na pobieraną treść, łącza internetowe oraz niechciane wiadomości e-mail.** Należy wyłączyć domyślne wykonywanie skryptów.
9. **Zminimalizuj liczbę sposobów ataku na system.** Trzeba zamknąć wszystkie niepotrzebne porty i wyłączyć wszystkie nieużywane protokoły sieciowe.
10. **Uważaj na udziały sieciowe i na udzielanie pełnych praw dostępu do współdzielonych zasobów.** Udziały stanowią potencjalny mechanizm rozprzestrzenienia w sieci wirusów, robaków, koni trojańskich i innego złośliwego oprogramowania. Należy stosować silną politykę list kontroli dostępu w sieciowym systemie operacyjnym.
11. **Uważaj na systemy mobilne i nośniki.** Trzeba izolować laptopy, które są używane poza firmą, do chwili, gdy zostaną dokładnie sprawdzone. Należy się upewnić, że systemy poufne mają zablokowaną możliwość obsługi nośników, na przykład pamięci USB.
12. **Bezpieczny oznacza bezpieczny.** Trzeba się upewnić, że połączenia w trakcie używania formularzy bądź połączenia HTTPS są bezpieczne. Należy weryfikować połączenia przez sprawdzanie certyfikatów bezpieczeństwa na witrynach internetowych. Trzeba zamykać przeglądarkę internetową po zakończeniu sesji; nie wystarczy jedynie zamknięcie karty bądź okna przeglądarki.
13. **Poświęć czas na opracowanie polityki bezpieczeństwa.** Należy we właściwy sposób wykorzystywać polityki bezpieczeństwa oferowane przez używany sieciowy system operacyjny.

Polityki bezpieczeństwa w Windows Server 2008 mogą blokować dostęp do zasobów na podstawie użytkowników lub grup, uniemożliwiać instalację oprogramowania bądź sterowników urządzeń, uniemożliwiać wykorzystywanie różnych klas urządzeń, blokować pulpit i przeglądarki internetowe, kontrolować dostęp do załączników poczty elektronicznej, uniemożliwiać zapisywanie płyt DVD, przeprowadzać kwarantannę sieciową, ustalać działania związane z ochroną konta użytkownika oraz przeprowadzać inne operacje. Prawdopodobnie około 40% z 2400 ustawień polityk w Windows Server 2008 dotyczy bezpieczeństwa. Inne sieciowe systemy operacyjne i produkty związane z politykami bezpieczeństwa, takie jak Novell ZenWare, także oferują szerokie możliwości konfiguracji.

Gdy wszystkie wymienione powyżej wskazówki będą przestrzegane, sieć będzie dla intruzów trudniejszym celem.

## Technologie NLA oraz NAP

Istnieje tak wiele sposobów, na które sieć może zostać zaatakowana, że tym, co tak naprawdę trzeba mieć przygotowane do obrony przed zagrożeniami, jest adaptacyjna strategia sieciowa. Firma Microsoft opracowała kilka takich strategii i dostarcza je wraz z systemami Windows Server 2008 oraz Vista. Pierwsza technologia to *Network Location Awareness* (NLA) — powoduje ona, że Windows Server ma możliwość wykrywania systemów, połączeń i stanu sesji oraz odpowiedniego zastosowania właściwej polityki względem klienta.

W wielu przypadkach klient sieciowy używa polecenia ping albo wysyła pakiet ICMP w celu sprawdzenia, czy po drugiej stronie znajduje się zasób sieciowy, z którym można się połączyć. Kiedy laptop nawiązuje połączenie z domeną Windows, używając polecenia ping, to stanowi ono mechanizm, który domena wykorzysta w celu określenia stanu klienta. Dlatego jeżeli działanie polecenia ping zakończy się niepowodzeniem, domena nie będzie mogła zastosować swojej polityki grupy. Reagowanie na pakiet ICMP jest często wyłączane w zaporze sieciowej, więc ten mechanizm również nie będzie niezawodny w modyfikacji połączenia klienta. W celu rozwiązania tych problemów opracowano technologię NLA, a informacje klienta są wymieniane za pomocą połączenia VPN. W trakcie każdego odświeżania połączenia VPN odświeżeniu ulega również polityka grupy zarówno dla użytkowników, jak i komputerów.

Wykorzystując technologię *Network Location Awareness*, w systemie klienta można wprowadzić następujące zmiany:

- ♦ Opcje mogą być ustawiane automatycznie na etapie PXE (ang. *Pre-Execution Environment*).
- ♦ Polityka grupy klienta może być uaktualniana automatycznie, kiedy nawiązuje on połączenie z domeną. Inne zdarzenia, na przykład połączenie urządzenia mobilnego, nawiązanie sesji VPN, wybudzenie klienta ze stanu hibernacji bądź wstrzymania lub przeniesienie systemu odizolowanego w kwarantannie do sieci produkcyjnej, również powoduje odświeżenie polityki grupy.
- ♦ Istnieje możliwość konfiguracji klientów na podstawie wykrytych zasobów. Jeśli karta interfejsu sieciowego nie zostanie wykryta, to sterownik dla tej karty nie będzie automatycznie wczytany. Zawieszenie wczytywania niepotrzebnych sterowników urządzeń powoduje skrócenie czasu rozruchu.
- ♦ Przepustowość łącza do klienta również może być częścią polityki, która jest stosowana, gdy klient nawiązuje połączenie z domeną.

Istnieje także drugie podejście do ochrony sieci — *Network Access Protection* (NAP). Ono także opiera się na zarządzaniu zasobami na podstawie zdefiniowanych polityk. Mechanizm NAP sprawdza stan dostępnych klientów (Vista), kiedy próbują zalogować się do domeny. Zanim klient zostanie uwierzytelniony i otrzyma dostęp do połączenia sieciowego, mechanizm NAP próbuje określić, czy nastąpiło złamanie którejkolwiek z wymienionych poniżej polityk:

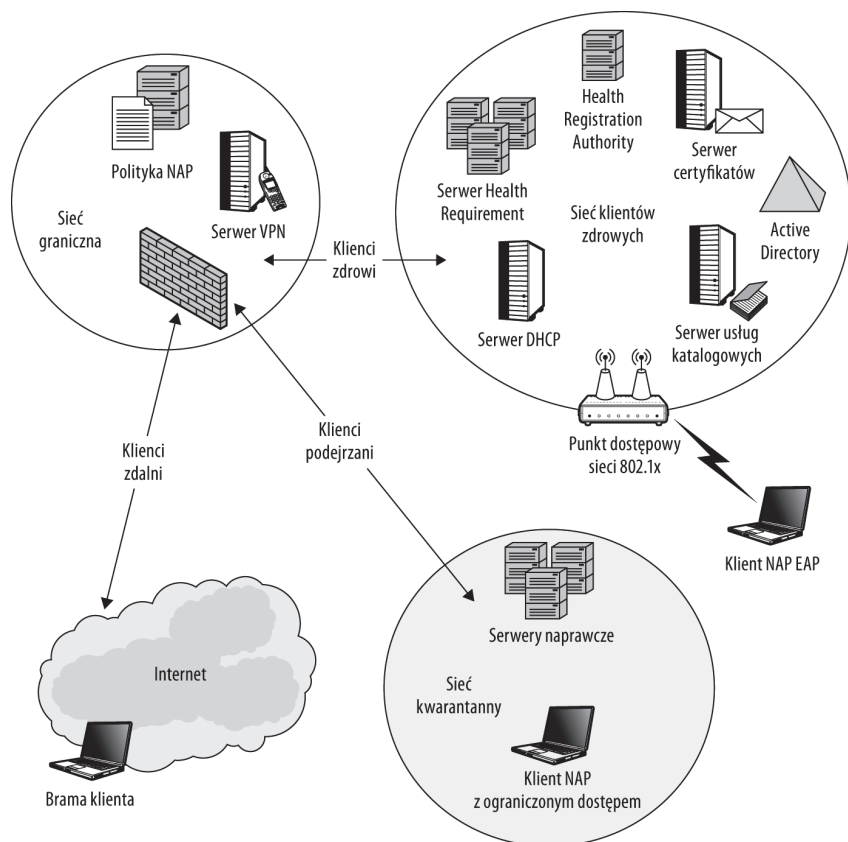
- ♦ zapora sieciowa klienta jest włączona;
- ♦ oprogramowanie antywirusowe i antyspyware'owe działa, jego definicje są aktualne, a skanowanie było przeprowadzone niedawno;
- ♦ zainstalowane zostały wszystkie aktualizacje udostępniane przez Microsoft;
- ♦ inne polityki charakterystyczne dla danej sieci.

Niespełnienie tych warunków powoduje poddanie systemu kwarantannie aż do jego naprawienia i spełnienia przez niego wszystkich wymagań. NAP dostarcza dodatkowych kryteriów, których spełnienie jest wymagane do zagwarantowania, że bezpieczeństwo nie będzie naruszone z wewnątrz sieci. Technologia ta przedstawia nowy kierunek, który wiele sieciowych systemów operacyjnych zaadaptuje, aby sieci stały się bezpieczniejsze. Tego

typu mechanizmy mogą być zmodyfikowane jako polityki systemowe stosowane następnie do określonych konfiguracji sieciowych. Na rysunku 27.3 pokazano diagram systemu NAP zaimplementowanego w Windows Server 2008.

### Rysunek 27.3.

*Technologia NAP oddziela zdrowe klienty od podejrzanych i umieszcza ich w oddzielnych sieciach*



W poprawnie skonfigurowanej usłudze NAP oprogramowanie odpowiedzialne za politykę NAP jest obsługiwane przez serwery *Health Requirement* oraz *Trusted Health Registration Authority*. Obsługą identyfikacji i uwierzytelniania klientów zajmują się serwery usług katalogowych i certyfikatów. Kiedy klient NAP nie spełni wymagań polityki dotyczącej jego kondycji, zostanie zalogowany do oddzielnej podsieci, gdzie będzie zarządzany przez serwer naprawczy, który zajmie się jego mankamentami.

## Bezpieczne protokoły w internecie

Internet to niewątpliwie niebezpieczne środowisko. W większości przypadków każdy odbywający się w nim ruch sieciowy może być przechwycony i buforowany. W celu zagwarantowania poufności danych wysyłanych przez internet opracowano kilka różnych protokołów komunikacyjnych, dzięki którym można chronić dane. W tym podrozdziale zostaną przedstawione trzy różne protokoły: *IPsec*, *Transport Layer Security* (poprzednio *Secure Sockets Layer*) i *HTTPS*.

IPsec to metoda szyfrowania ruchu IP oraz weryfikacji danych po ich dotarciu do miejsca przeznaczenia. Wymóg stosowania IPsec to jeden z głównych powodów, dla których protokół IPv6 jest bez wątpienia znacznie bezpieczniejszy niż IPv4. Natomiast TLS i SSL to metody szyfrowania danych i wysyłania ich przez warstwę transportową. HTTPS to technologia szyfrowania zespólona z bezpiecznym połączeniem. W technologii tej następuje utworzenie tunelu łączącego klienta z serwerem. Trzy wymienione metody pozwalają na działalność banków internetowych, komunikację organów rządowych i wojskowych, a także na wykorzystanie wszystkich innych udogodnień oferowanych przez nowoczesne sieci.

## IPsec

*Internet Protocol Security* (IPsec) to metoda szyfrowania i weryfikowania ruchu sieciowego wysyłanego przez sieci TCP/IP będąca standardem otwartym, zdefiniowanym w dokumencie IETF RFC 2401 (<http://www.ietf.org/rfc/rfc2401.txt>). Zestaw protokołów zawiera bazujący na kluczu mechanizm szyfrujący do ustanawiania unikalnej identyfikacji punktów końcowych połączenia. W celu użycia IPsec oba węzły muszą mieć lokalnie uruchomiony ten protokół. Za pomocą protokołu IPsec można korzystać z emisji pojedynczej lub multimijsji. W trakcie multimijsji wszystkie węzły docelowe muszą współdzielić te same informacje bezpieczeństwa.

IPsec może operować w dwóch trybach:

- ♦ transportowym,
- ♦ tunelu.



Pisownia „IPsec” z małymi literami jest zalecana przez organizację IETF. Bardzo często można spotkać się z pisownią „IPSec”, ale w książce stosujemy się do zalecenia IETF.

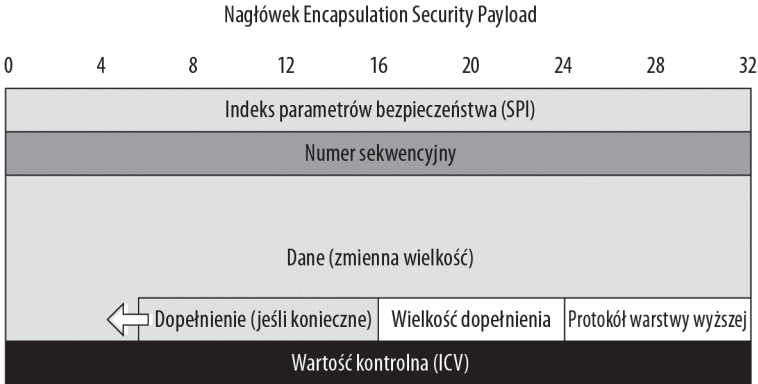
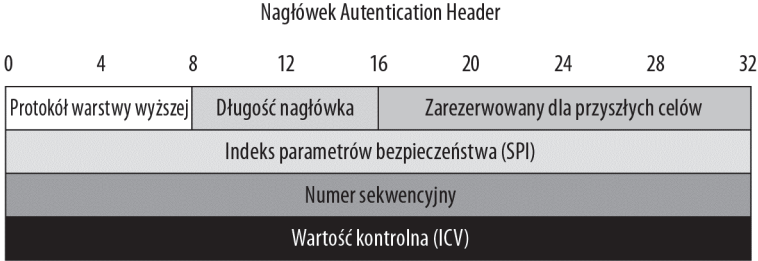
W trybie transportowym w pakiecie pozostaje oryginalny nagłówek IP w przeciwieństwie do trybu tunelu, gdzie nagłówek ten jest zamieniany na nowy, a oryginalny jest enkapsulowany. Różnica została zaprezentowana na rysunku 27.4. Tryb transportowy jest zazwyczaj stosowany w komunikacji pomiędzy urządzeniami końcowymi, natomiast tryb tunelu jest głównie stosowany do łączenia dwóch sieci. Tryb tunelu jest często używany w tworzeniu sieci VPN (ang. *Virtual Private Network* — wirtualna sieć prywatna).

Istnieje również możliwość używania IPsec, kiedy tylko jeden punkt końcowy połączenia obsługuje protokół IPsec. W takim przypadku pakiet IPsec jest szyfrowany i enkapsulowany w routerze brzegowym (lub w innym zewnętrznym), a następnie deszyfrowany i wydrebniany w routerze granicznym dla systemu docelowego. Po skonfigurowaniu IPsec w taki właśnie sposób ruch sieciowy jest widoczny dla obu punktów końcowych w sieci, ale bezpieczny po opuszczeniu podsieci, w której znajduje się system wysyłający pakiet.

W modelu OSI IPsec jest protokołem warstwy sieciowej (poziom 3.), natomiast w modelu TCP/IP protokołem warstwy internetu. W zestawie protokołu IPsec najważniejsze są trzy wymienione poniżej protokoły:

- ♦ **Authentication Header (AH)**. Protokół AH dostarcza mechanizm gwarantujący uwierzytelnianie i integralność pakietów IP w IPsec. W tym celu stosuje wartość kontrolną ICV (ang. *Integrity Check Value*), której wartość protokół AH oblicza,

**Rysunek 27.4.**  
Struktura nagłówków  
AH (na górze) i ESP  
(na dole)



używając algorytmu kodującego oraz współdzielonego klucza. Wartość kontrolna ICV pełni taką samą funkcję jak sprawdzanie danych CRC. Odbiorca pakietu deszyfruje dane, uruchamia te same algorytmy i sprawdza, czy obliczona wartość kontrolna ICV jest taka sama jak w datagramie, co zapewnia uwierzytelnienie nadawcy. Na górze rysunku 27.4 przedstawiony jest nagłówek AH.

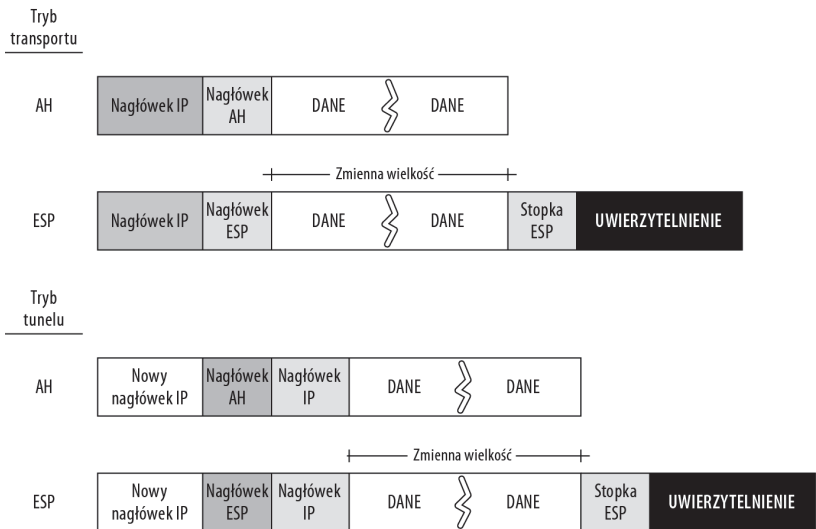
- ♦ **Encapsulating Security Payload (ESP).** Protokół ESP szyfruje dane używane w komunikacji IPsec i zapewnia formę uwierzytelniania, integralności danych (wartość kontrolna ICV) oraz ochrony treści danych IPv4 lub IPv6. ESP można stosować w trybie tylko szyfrowania albo tylko uwierzytelniania, ale najczęściej włączone są obie funkcje. ESP w przeciwieństwie do AH nie zapewnia integralnej ochrony nagłówka IP. Na dole rysunku 27.4 przedstawiony jest nagłówek ESP.
- ♦ **Internet Key Exchange (IKE) v1 oraz v2.** Protokół IKE dostarcza mechanizm współpracy między dwoma punktami końcowymi połączenia, ustala dostępne protokoły bezpieczeństwa i określa, które z nich będą używane. Następnie przeprowadza szyfrowanie i tworzy klucze uwierzytelnienia wysyłane do systemu docelowego, aby wysyłany pakiet mógł być poprawnie zidentyfikowany i odszyfrowany. Protokół IKE został zdefiniowany w dokumencie IETF RFC 2409 (<http://tools.ietf.org/html/rfc2409>).

Do wymiany danych i negocjacji parametrów bezpieczeństwa (SA, ang. *Security Association*) IKE używa protokołu *Internet Security Association and Key Management Protocol* (ISAKMP). ISAKMP pozwala na obsługę różnych metod wymiany kluczy. Dwa najczęściej stosowane protokoły wymiany kluczy to

OAKLEY i SKEME. Ten pierwszy jest najczęściej używany jako technologia wymiany kluczy w IKE, natomiast od drugiego (SKEME) IKE „pożycza” pewne funkcje, na przykład technologię szyfrowania klucza publicznego.

Na rysunku 27.5 pokazano strukturę nagłówka zarówno AH, jak i ESP w trybach transportowym i tunelu. Pole danych ma zmienną wielkość.

**Rysunek 27.5.**  
Struktura nagłówków  
AH i ESP pakietu IPsec



Protokół ESP szyfruje dane w datagramie IPsec, używając algorytmów kryptograficznych, takich jak DES, 3DES, AES i inne. Punkty końcowe w sesji IPsec muszą mieć współdzielony klucz. ESP można stosować jako samodzielny protokół bądź w połączeniu z protokołem AH. Na rysunku 27.5 pokazano różne komponenty pakietu IPsec szyfrowane przez ESP: nagłówek ESP, stopkę ESP oraz dane ESP. Przedstawiony na rysunku 27.4 nagłówek ESP ma parametr SPI zawierający wynegocjowane parametry bezpieczeństwa (SA) i numer sekwencyjny stosowany do obrony przed atakami typu reply. Stopka zawiera informacje o dopełnieniu, długości dopełnienia oraz o nagłówku protokołu warstwy wyższej. Opcjonalną funkcją w protokole ESP jest uwierzytelnienie pola danych przez użycie algorytmu do tworzenia wartości kontrolnej ICV, która następnie będzie porównywana za pomocą współdzielonego klucza.

Miejsce umieszczenia komponentów IPsec w datagramie gwarantuje, że po danych znajdzie się stopka zawierająca dopełnienie o długości odpowiedniej do tego, aby zachować standardową wielkość bloku, wymaganą przez algorytmy do dalszego przetwarzania danych. Jeżeli będzie użyte uwierzytelnianie, to dane uwierzytelniające ESP ze stopki staną się częścią danych zaszyfrowanych, ponieważ zostałyby usunięte, gdyby znajdowały się w polu nagłówka. Dane te muszą znajdować się tuż za danymi pakietu, aby możliwe było prawidłowe przeprowadzenie procesu odszyfrowania.

Ponieważ IPsec operuje na tym samym poziomie co sam protokół IP, pozostaje niezależny od aplikacji i może być używany do bezpiecznego wysyłania pakietów z dowolnej aplikacji. Taka sytuacja nie ma miejsca w przypadku innych protokołów bezpieczeństwa, na przykład SSL, które operują na wyższych poziomach i wymagają od aplikacji wbudowania ich obsługi.

IPsec negocjuje metodę stosowaną do przekazywania datagramów w danym formacie między punktami końcowymi. Dwa punkty końcowe wraz z wynegocjowaną polityką bezpieczeństwa są przechowywane w SA. Polityka bezpieczeństwa określa, które pakiety są zabezpieczane i kiedy wykorzystują protokół AH lub ESP. Algorytmy używane do szyfrowania oraz do uwierzytelniania są wybierane z listy, a następnie współdzielone, podobnie jak klucze niezbędne do odszyfrowania danych w obu procesach. Polityki są przechowywane lokalnie w bazie danych SPD (ang. *Security Policy Database*) każdego urządzenia. Natomiast SA są przechowywane w bazie danych SAD (ang. *Security Association Database*) każdego urządzenia. Kiedy datagram IPsec dociera do urządzenia, w którym ma być przetworzony, urządzenie przeszukuje indeks parametrów bezpieczeństwa (ang. *Security Parameter Index*, SPI) w bazie danych SPD, a następnie stosuje ustawienia przechowywane dla danego indeksu SPI w bazie danych SAD.

Wprowadzie IPsec jest komponentem opcjonalnym w komunikacji IPv4, jest jednak wymagany i stanowi zintegrowaną część IPv6. Jeżeli Czytelnik nie używa IPsec już teraz, to może być pewny, że będzie musiał to robić w przyszłości.

## Zestaw protokołów Transport Layer Security

*Transport Layer Security* (TLS) to zestaw protokołów kryptograficznych wykorzystywanych do szyfrowania danych wysyłanych na poziomie warstwy transportowej w sieci TCP/IP. Ten rozwijany standard został zdefiniowany w dokumencie IETF RFC 5246 (<http://tools.ietf.org/html/rfc5246>). TLS obsługuje nadzbiór doskonale znanego protokołu SSL (ang. *Secure Socket Layer*), opracowanego przez firmę Netscape i używanego przez wiele lat. Protokół SSL 3.0 był pierwszym protokołem sieciowym wybranym przez firmy obsługujące płatności przeprowadzane za pomocą kart internetowych do bezpiecznej obsługi transakcji w internecie.

Protokół TLS zarówno szyfruje, jak i uwierzytelnia dane wysyłane z serwera do uwierzytelnionego klienta, tak więc zapewniane jest bezpieczeństwo komunikacji. Protokół ten jest najczęściej wykorzystywany w celu umożliwienia serwerom WWW komunikacji z klientami, na przykład przeglądarkami internetowymi. Jednak może być też stosowany w przypadku ruchu sieciowego TCP/IP, generowanego przez dowolne aplikacje.



Protokół TLS może doprowadzić do problemów, jeśli jest używany wraz z serwerami wirtualnymi, co wiąże się z faktem, że serwery wirtualne muszą współdzielić ten sam certyfikat w serwerze. W sytuacji, kiedy do uwierzytelniania jest stosowany certyfikat X.509, może wystąpić konieczność użycia certyfikatu typu Wildcard bądź ponownego wydania certyfikatu po skorzystaniu z nowego serwera wirtualnego.

W swojej najprostszej postaci TLS używa serwera uwierzytelnionego oraz klienta niewierzytelnionego. Jeżeli została zainstalowana infrastruktura klucza publicznego (ang. *Public Key Infrastructure* — PKI), TLS można skonfigurować w taki sposób, aby oba punkty końcowe połączenia mogły być wzajemnie uwierzytelniane. Proces ten opiera się na trzech krokach:

1. **Obsługa negocjacji protokołu.** Klient wysyła do serwera TLS listę obsługiwanych metod szyfrowania oraz funkcji kodujących, serwer wybiera najmocniejszą. Krok ten określa się „uściskiem dłoni TLS” (ang. *TLS handshake*); może on być prostym procesem bez uwierzytelniania klienta.

**2. Wymiana klucza i system pojedynczego bądź wzajemnego uwierzytelniania.**

Serwer zwraca klientowi certyfikat cyfrowy zawierający nazwę serwera oraz dane uwierzytelniające z centrum certyfikacji (ang. *Certificate Authority*, CA). Klient może zweryfikować te informacje w serwerze centrum certyfikacji.

**3. Szyfrowanie symetryczne i uwierzytelnianie wiadomości.** Klient szyfruje losowo wybraną liczbę za pomocą klucza publicznego serwera i wysyła ten klucz sesji serwerowi, gdzie będzie odszyfrowany za pomocą klucza prywatnego. Zarówno serwer, jak i klient powinny wygenerować losowe liczby, które następnie będą użyte przez różne algorytmy do wygenerowania odpowiednich kluczy.

TLS obsługuje pewną liczbę różnych algorytmów kryptograficznych zarówno w celu tworzenia i wymiany klucza, jak i uwierzytelniania. Kiedy dwa punkty końcowe prowadzą negocjacje, dochodzi do wyboru algorytmu wymiany klucza oraz algorytmu uwierzytelniania. Uwierzytelnianie wiadomości obejmuje także użycie kodów uwierzytelniania wiadomości (ang. *Message Authentication Code*, MAC), które są tworzone za pomocą funkcji kryptograficznych. Z kolei SSL do utworzenia swoich kodów MAC wykorzystuje pseudolosową funkcję. Ogólnie rzecz ujmując, negocjacje TLS polegają na wyborze algorytmów z pakietu kryptograficznego.

Aby aplikacja mogła używać TLS, musi mieć wbudowaną obsługę protokołu TLS. Wprawdzie protokół TLS jest stosowany przede wszystkim dla ruchu HTTP podczas transportu przez TCP, ale jest wykorzystywany również do zabezpieczania ruchu SMTP, FTP, NNTP oraz XMPP. OpenVPN (<http://openvpn.net>) używa TLS do utworzenia połączenia VPN między dwoma punktami końcowymi. W przypadku OpenVPN może być zastosowany dowolny protokół sieciowy; program spowoduje, że system docelowy stanie się dla źródłowego systemem lokalnym. Innym obszarem, na którym TLS jest szeroko wykorzystywany, jest ruch VoIP (ang. *Voice over IP*), gdzie protokół sygnalizacyjny SIP (ang. *Session Initiation Protocol*) jest szyfrowany i uwierzytelniany.

Dla wielu aplikacji pozbawionych obsługi TLS istnieją produkty firm trzecich enkapsulujące ruch TLS i transportujące go między punktami końcowymi. Jeden z takich programów to stunnel (<http://stunnel.mirt.net>). Jest to działająca na wielu platformach bezpłatna (typu open source) aplikacja tunelowania TLS/SSL. Działa na zasadzie enkapsulacji danych do TLS i może używać infrastruktury PKI do tworzenia bezpiecznych połączeń.

## Protokół HTTPS

*HyperText Transfer Protocol Secure* (HTTPS) łączy w sobie protokół *HyperText Transfer Protocol* (HTTP) z protokołami *Transport Layer Security* (TLS) albo *Secure Sockets Layer* (SSL), które zostały przedstawione w poprzednim podrozdziale. Uwierzytelniony serwer WWW używa HTTPS w celu nawiązania bezpiecznego połączenia z przeglądarką internetową klienta. Podczas nawiązywania połączenia w pasku adresu URL zamiast standardowego prefiksu *http://* podaje się *https://*. O ile nie zostanie to zmodyfikowane, domyślnie ruch sieciowy HTTP będzie używał portu numer 443.

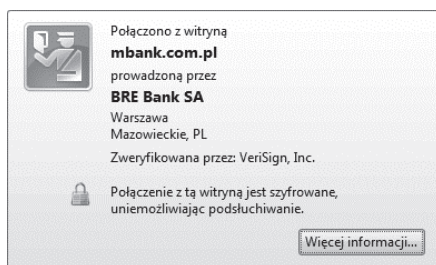


Wyświetlenie ikony kłódki w przeglądarce internetowej wskazującej na połączenie szyfrowane za pomocą SSL/TLS nie jest gwarancją bezpieczeństwa. Przeglądarka internetowa może zostać przechwycona i nadal wyświetlać ikonę kłódki. Zawsze należy sprawdzić certyfikat i upewnić się, że wyświetlane w nim informacje są zgodne z oczekiwanymi.

Na rysunku 27.6 pokazano bezpieczne połączenie z lokalnym bankiem nawiązane w przeglądarce Mozilla Firefox 3.0. Warto zwrócić uwagę, że ikona certyfikatu firmy pojawia się po lewej stronie adresu URL. Kliknięcie tej ikony powoduje wyświetlenie okna dialogowego zawierającego więcej informacji szczegółowych. Przeglądarka Microsoft Internet Explorer powiela tę funkcję, umieszczając ikonę po prawej stronie pasku adresu. Jeżeli nawiązane zostało zweryfikowane połączenie HTTPS, pasek adresu będzie zielony.

### Rysunek 27.6.

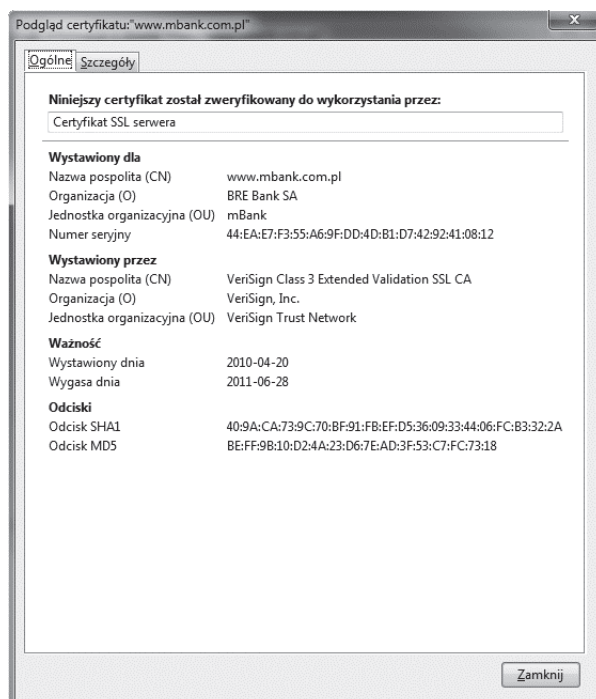
*Ikona bezpieczeństwa w przeglądarce Mozilla Firefox 3.0 — gdy użytkownik ją kliknie, wyświetlą się informacje o certyfikacie na danej stronie*



Wszystkie przeglądarki internetowe dostarczają większej ilości informacji wraz z informacjami szczegółowymi dotyczącymi samego certyfikatu. Okno dialogowe *Podgląd certyfikatu* w przeglądarce Mozilla Firefox 3.0 zostało pokazane na rysunku 27.7. Kiedy użytkownik nawiąże bezpieczne połączenie, ale będzie miał wątpliwości dotyczące jego uwierzytelnienia, powinien wyświetlić wymienione okno dialogowe i sprawdzić, czy wszystkie pola są wypełnione odpowiednimi danymi. Wprawdzie istnieje możliwość utworzenia fałszywego połączenia, ale jest mało prawdopodobne, aby ktoś mógł podmienić pola w oknie dialogowym wyświetlającym informacje o certyfikacie. Wspomniane pola są wypełniane przez firmę trzecią, w tym przypadku przez serwer centrum certyfikacji.

### Rysunek 27.7.

*Okno dialogowe wyświetlające w przeglądarce Mozilla Firefox 3.0 informacje szczegółowe o certyfikacie*



Certyfikaty stosowane przez serwery WWW są certyfikatami klucza publicznego, które zostały utworzone przez oprogramowanie i wysłane do centrum certyfikacji w celu ich weryfikacji. Taki certyfikat jest cyfrowo podpisywany przez centrum certyfikacji, co oznacza, że każdemu zainteresowanemu dostarcza klucza publicznego niezbędnego do weryfikacji i sprawdzenia, czy informacje podawane przez serwer WWW są prawidłowe. Aby przeglądarka internetowa mogła zweryfikować certyfikat, musi dysponować podpisanym certyfikatem centrum autoryzacji. Ponieważ taka funkcja będzie bezużyteczna bez certyfikatów, certyfikaty większości głównych centrów certyfikacji są dostępne we wszystkich najważniejszych przeglądarkach internetowych.

Firmy i użytkownicy prywatni mogą ustanawiać własne centra certyfikacji, ale będą one nadawały się jedynie do szyfrowania ruchu sieciowego, tak aby inni nie mogli podglądać danych. Certyfikat prywatny lub firmowy nie uwierzytelnia nadawcy. Jednak jeżeli firma wysyła dane ze swojego serwera WWW do swoich przeglądarek internetowych, to w takim przypadku certyfikat tej firmy potwierdzi prawdziwość nadawcy. Oprócz certyfikatów dla serwerów firmy mogą tworzyć certyfikaty dla klientów i umieszczać je w przeglądarkach internetowych poszczególnych użytkowników. Certyfikat klienta może zweryfikować w serwerze dane użytkownika bez konieczności jego logowania i pozwala serwerowi na sprawdzenie tej informacji podczas każdego połączenia z klientem. To są naprawdę bardzo przydatne funkcje.

## Szyfrowanie i kryptografia

Kryptografia to nauka o metodach szyfrowania (ukrywania) informacji. Związane z nią zagadnienia mieszczą się w obrębie zarówno informatyki, jak i matematyki. Istnieje wiele metod kryptograficznego zabezpieczania informacji, między innymi używanie haseł, biometriki lub innych urządzeń, szyfrowanie danych za pomocą algorytmów, używanie kluczy itp.

Szyfrowanie oznacza proces przekształcania informacji na postać danych, które tracą swój kontekst. Deszyfrowanie to proces całkowicie odwrotny, to znaczy przekształcanie danych z powrotem na postać informacji, które mogą być odczytane i zrozumiane. Oba procesy, tj. dwa algorytmy odpowiedzialne za szyfrowanie i deszyfrowanie, nazywamy kodowaniem. Niektóre systemy kodowania wymagają używania klucza, który stanowi informację wykorzystywaną do modyfikacji operacji kodowania. W takich przypadkach nadawca i odbiorca mogą współdzielić klucz publiczny, ale nie wymieniają kluczy prywatnych koniecznych do przeprowadzenia procesu kodowania. Aby zachować pełną poufność, klucz powinien być zmienny (to znaczy generowany na nowo w trakcie każdego użycia), w przeciwnym razie traci swoją możliwość ochrony kodu przed osobami z zewnątrz. Wszystkie wymienione elementy komunikacji — kodowanie, klucze i zaszyfrowane dane — są przedmiotem działania dla metod uwierzytelniających, które weryfikują, czy informacje zostały dostarczone prawidłowo, i ustalają źródło ich pochodzenia.

Nowoczesne metody kodowania są wyjątkowo dobre i bardzo trudne do złamania. Trzy najlepiej znane algorytmy kryptograficzne stosowane w informatyce to:

- ♦ **Data Encryption Standard (DES).** Opracowany przez firmę IBM i wybrany w 1976 roku przez Narodowe Biuro Standardów jako oficjalny Federalny Standard Przetwarzania Informacji (ang. *Federal Information Processing Standard*, FIPS)

ządu Stanów Zjednoczonych. Algorytm DES używa algorytmu klucza symetrycznego oraz klucza 56-bitowego. Obecnie DES nie jest uznawany za bezpieczny, ale różne jego odmiany, na przykład 3DES i następca *Advanced Encryption Standard* (AES), pozostają w powszechnym użyciu.

- ♦ **Algorytm Diffie-Hellman Key Agreement** jest algorytmem uzgadniania kluczy, który pozwala na otrzymanie przez dwie strony tej samej liczby, niemożliwej do odgadnięcia przez podsłuchanie. Algorytm D-H został opublikowany po raz pierwszy w roku 1976 przez Whitfielda Diffiego oraz Martina Hellmana i bazował na rozwiązaniu polegającym na użyciu rozprowadzania klucza publicznego. Rozwiązanie to zostało opracowane przez Ralpha Merkle'a z Wielkiej Brytanii i było utrzymywane w tajemnicy do roku 1997. Z tego powodu czasami (naprawdę rzadko) można się spotkać z określeniem tej metody jako Diffie-Hellman-Merkle. Diffie jest teraz szefem bezpieczeństwa w firmie Sun Microsystems (przejętej w roku 2009 przez Oracle).
- ♦ **Algorytm klucza publicznego RSA** bazuje na rozwiązaniu Roniego Rivasta, Adiego Shamira oraz Leonarda Adlemana z MIT i zostało opublikowane w roku 1977, a opatentowane w roku 1983. Algorytmy RSA obejmują generowanie kluczy, szyfrowanie i deszyfrowanie za pomocą pary kluczy publicznego i prywatnego. Klucz publiczny jest używany do szyfrowania danych, które mogą zostać odszyfrowane jedynie za pomocą klucza prywatnego.

Wszystkie wymienione powyżej technologie kryptograficzne zostaną dokładniej omówione. Technologie kryptograficzne i szyfrowanie to skomplikowana dziedzina, której bliższe przedstawienie mogłoby zająć całą książkę. W poniższych podrozdziałach znajdują się ogólne informacje dotyczące sposobów wykorzystania tych technologii do zabezpieczania sieci komputerowych.

## Atak siłowy i ignorancja

Nigdy nie można udowodnić, że dany szyfr jest nie do złamania. Poza jednym wyjątkiem teoretycznie każdy kod można złamać przy założeniu, że do tej operacji zostaną wykorzystane odpowiednie zasoby. Wspomniany wyjątek to system, w którym jako klucz jest używane dopełnienie z szyfrowaniem za pomocą klucza jednorazowego, a ten szyfr stosuje generowanie liczb naprawdę losowych. Claude Shannon dowiódł, że szyfr z kluczem jednorazowym jest nie do złamania pod warunkiem, że naprawdę będzie stosował liczby losowe, zostanie wykorzystany tylko jeden raz, a jego wielkość będzie równa szyfrowanym danym lub większa.

Żadna współczesna metoda szyfrowania nie jest idealna, ponieważ idealne systemy szyfrowania wymagają przeprowadzania zbyt wielu obliczeń. Jednak kiedy potencjalna liczba kombinacji w zbiorze danych staje się wystarczająco duża, to złamanie takiego szyfru przez jakikolwiek system jest praktycznie niemożliwe. Można to zilustrować następującym przykładem.

Hasło to klucz udzielający dostępu do bezpiecznego konta. Jeżeli włamywacz dowie się, że w systemie jest stosowane hasło o długości dwóch małych liter, to może ręcznie wprowadzić każdą z 676 kombinacji, czyli  $26^2$  możliwych haseł. W takim przypadku w ciągu

godziny można odkryć prawidłową kombinację. Jeżeli hasło będzie składało się z małych i dużych liter, to liczba kombinacji wzrasta do 2704 ( $52^2$ ) i jej odkrycie wymaga czterokrotnie więcej czasu. Takie podejście, polegające na próbie odgadnięcia hasła, nazywa się „podejściem siłowym” (ang. *brute force*). Zamek składający się z czterech kółek z cyframi od 0 do 9 daje zbiór kombinacji od 0000 do 9999 (czyli 10 000 możliwych kombinacji). Złamanie takiego hasła może zająć większą część dnia.



Kombinacje dwuliterowe można znaleźć na stronie [http://en.wikipedia.org/wiki/List\\_of\\_all\\_two-letter\\_combinations](http://en.wikipedia.org/wiki/List_of_all_two-letter_combinations), natomiast kombinacje trzyliterowe, nazywane TLA (ang. *Three-Letter Acronym*) zajmują w Wikipedii aż 16 stron ([http://en.wikipedia.org/wiki/Category:Lists\\_of\\_TLAs](http://en.wikipedia.org/wiki/Category:Lists_of_TLAs)).

Szybkość pracy komputerów powoduje, że ataki siłowe stały się bardzo skuteczne. Nowoczesne komputery biurowe są całkiem potężne — w przeszłości taką mocą obliczeniową dysponowały komputery typu mainframe. Atak siłowy przeprowadzany za pomocą nowoczesnego komputera PC pozwala na znalezienie sześcioletowego hasła w ciągu kilku godzin, natomiast hasła składającego się z sześciu znaków (małe i duże litery, cyfry i znaki przestankowe) w ciągu kilku dni. Złamanie ośmioznakowego hasła stosującego znaki z pełnego zbioru ASCII może zająć miesiąc lub dwa. Obejrzenie pokazu skuteczności ataku siłowego może być dla wielu osób zdumiewające.

Generalnie można przyjąć, że większość atakujących, którzy próbują uzyskać dostęp do danej sieci, poświęci najwyżej dzień lub dwa na złamanie hasła, chyba że zasoby tej sieci będą warte włożenia większego wysiłku.



Większość systemów bezpieczeństwa zawiera funkcję blokowania, która powoduje zablokowanie konta po określonej liczbie nieudanych prób logowania. Taka funkcja ma za zadanie chronić system przed atakiem siłowym lub z wykorzystaniem metody słownikowej.

Ataki siłowe zazwyczaj łączą w sobie losowe odgadywanie hasła z przygotowanym słownikiem zawierającym większość krótkich kombinacji znaków (powiedzmy do trzech – czterech), jak również powszechnie używanych nazw i słów w danym języku (językach). Przeprowadzając atak na bazie słownika, w ciągu kilku godzin można wypróbować wiele milionów najczęściej wykorzystywanych kombinacji. Takie podejście jest zwykle efektywniejsze niż zwykły atak siłowy, ponieważ niewielka liczba osób stosuje hasła prawdziwie losowe. Widać więc, dlaczego skomplikowane hasła losowe oferują znacznie większe bezpieczeństwo niż tylko litery. Ponadto da się zauważyć, że ilość pracy koniecznej do włożenia w złamanie hasła wzrasta w postępie geometrycznym wraz z każdym kolejnym znakiem.



W internecie można znaleźć sporo generatorów haseł losowych. Niektóre z nich generują hasła losowe bezpośrednio na stronie, inne są samodzielnymi aplikacjami, które można pobrać lub kupić. Aby zapewnić prawdziwą losowość, najlepsze generatory haseł losowych wykorzystują liczby odzwierciedlające na przykład fluktuację temperatury procesora. W przypadku stosowania generatora haseł losowych trzeba się upewnić, że hasła są przechowywane w bezpiecznym miejscu.

Atak siłowy ma swoje ograniczenia. Firma Electronic Freedom Foundation w roku 1998 kosztem 250 tysięcy dolarów zbudowała system DES Cracker, składający się z 1800 układów, i zademonstrowała, że 56-bitowy szyfr DES może być złamany w ciągu kilku dni.

System, który może powtórzyć ten wyczyn, obecnie można zbudować kosztem około 10 tysięcy dolarów. Wraz ze zwiększaniem długości dowolnego klucza ilość pracy, którą trzeba włożyć w operację złamania szyfru, rośnie w postępie geometrycznym. Współczesne technologie szyfrowania, takie jak AES, 3DES, Twofish, Serpent i inne standardy, mają klucze o długości co najmniej 128 bitów, choć mogą stosować również klucze o długości 192 lub 256 bitów.

Czytelnik mógłby posiłkować się wiedzą z zakresu fizyki i stwierdzić, że 128-bitowy klucz symetryczny jest nie do złamania. Równanie Neumanna-Landeura pozwala na obliczenie najmniejszej ilości energii potrzebnej do przeprowadzenia operacji odwrócenia bitów. W przypadku zbioru o wielkości  $2^{128}$  ( $3,40 \cdot 10^{38}$ ) komputer operujący w temperaturze pokojowej musiałby zużywać 30 gigawatów ( $10^{18}$  dżuli) energii rocznie w celu przeprowadzenia  $2^{128}$  jednobitowych operacji. Wartość ta nie jest w stanie przybliżyć ilości energii potrzebnej do sprawdzenia poprawności klucza. Ilość czasu wymagana do przeprowadzenia operacji zamiany bitów przy szybkości działania  $10^{18}$  zamian bitów na sekundę to  $10^{13}$  lat, czyli w przybliżeniu wiek wszechświata. W obliczeniach przyjęto założenie, że klucz został wygenerowany naprawdę losowo.

Pewnego dnia być może będziemy dysponowali komputerami kwantowymi operującymi na znacznie większych szybkościach oraz w temperaturze bliskiej zera bezwzględnego. Wówczas podstawowe założenia powyższego przykładu stracą swoją ważność. Jednak parafrazując Aragorna z *Powrotu Króla*, „to nie jest ten dzień”.

## Algorytmy klucza symetrycznego

Pierwsze dostępne algorytmy kryptograficzne bazujące na kluczu były algorytmami klucza symetrycznego. Najczęściej stosowane algorytmy klucza symetrycznego używają szyfru blokowego, szyfru strumieniowego oraz funkcji kodującej. Poniżej przedstawiono krótki opis każdego z wymienionych rodzajów szyfrowania.

### Szyfr blokowy

W przypadku szyfru blokowego algorytm operuje na bloku tekstu, używając klucza, który przekształca dane wyjściowe na blok zaszyfowanego tekstu o tej samej wielkości. Kiedy wielkość wiadomości jest większa niż wykorzystywany blok, algorytm stosuje blok i klucz w celu zaszyfowania kolejnego zestawu znaków o wielkości bloku. Cały proces jest powtarzany aż do zaszyfowania wszystkich znaków. Szyfr blokowy może iteracyjnie powtarzać szyfrowanie bloku i zmienić algorytm używany dla każdego bloku, który jest szyfrowany.

*Data Encryption Standard* (DES) oraz *Advanced Encryption Standard* (AES) to przykłady algorytmów szyfru blokowego. Wprawdzie DES nie jest wykorzystywany w komunikacji o wysokim stopniu bezpieczeństwa, ale standard pozostaje bardzo popularny ze względu na dużą szybkość szyfrowania i odszyfrowywania danych. Istnieje duże prawdopodobieństwo, że używany przez Czytelnika klient poczty stosuje szyfrowanie na bazie DES, podobnie jak w przypadku komunikacji ATM oraz zaszyfowanych bezpiecznych połączeń, na przykład zdalnego pulpitu.

## Szyfr strumieniowy

Szyfr strumieniowy działa przez wygenerowanie długiego klucza jako strumienia, znak po znaku. Tworzenie klucza bazuje na procesie, którego nie można przewidzieć; przykładem może być generowanie haseł losowych na podstawie zmiennej temperatury, jak wspomniano w poprzednim podrozdziale. Im dłuższy klucz, tym bezpieczniejszy szyfr strumieniowy.

Szyfry strumieniowe nie wymagają generowania klucza w czasie rzeczywistym. Istnieje więc możliwość wcześniejszego wygenerowania zestawu kluczy dla szyfrowania strumieniowego i wykorzystania ich, gdy staną się niezbędne. Najbardziej znany przykład takiego szyfrowania strumieniowego to „szyfrowanie z użyciem klucza jednorazowego”. W przypadku szyfrowania za pomocą klucza jednorazowego każda wiadomość jest szyfrowana unikalnym kluczem, który po użyciu jest usuwany — można to porównać do wydzierania pierwszej kartki notesu po jej zapisaniu. Istotną funkcją szyfrowania strumieniowego jest to, że każdy klucz pozostaje losowy i unikalny.

Najbardziej znane szyfrowanie strumieniowe to standard RC4, który został opracowany przez Rona Rivesta z RSA Security, wydany i zarejestrowany w roku 1987, ale sam algorytm pozostał tajny do roku 1994. Skrót RC oznacza „Rivest Cipher” (szyfr Rivest) albo „Ron’s Code” (kod Rona). Szyfr ten jest dostępny w kilku wariantach, na przykład RC2, RC5 i RC6. W roku 1994 szyfr RC4 został ujawniony i stanowi odtąd własność publiczną. Algorytm RC4 jest standardem szyfrowania w protokołach bezpieczeństwa WPA i WEP sieci bezprzewodowych, jak przedstawiono w rozdziale 14., oraz w protokole *Transport Layer Security* (TLS), przedstawionym wcześniej w tym rozdziale.

RC4 tworzy pseudolosowy strumień kluczy (ang. *keystream*), od jednej do 256 możliwych kombinacji bajtów, oraz dwa 8-bitowe wskaźniki indeksów stosujące algorytm KSA (ang. *Key Scheduling Algorithm*) do utworzenia klucza o długości od 40 do 256 bitów. Wymieniony strumień kluczy jest następnie używany do zaszyfrowania tekstu przez wykorzystanie operacji alternatywy wykluczającej (ang. *Exclusive OR*, XOR) na bitach. Kiedy RC4 pracuje na kolejnych znakach tekstu, algorytm generowania pseudolosowego (PRGA) zwiększa wartości indeksów w celu modyfikacji strumienia kluczy. Algorytm XOR pobiera dwa operandy i przeprowadza logiczną dysjunkcję, a więc wynik jest jedną lub drugą wartością, ale nigdy oboma. Operacja ta została graficznie pokazana w tabeli 27.1. Deszyfrowanie po prostu powtarza ten proces, przekształcając tekst zaszyfrowany na zwykły tekst.

**Tabela 27.1.** Tabela pokazująca operację XOR

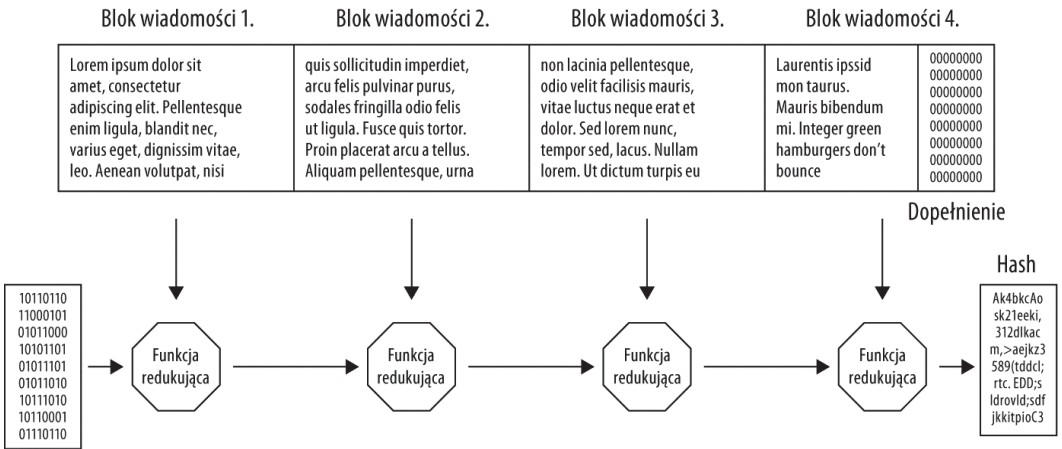
X	Y	Wynik
0	0	0
0	1	1
1	0	1
1	1	0

Algorytm RC4 nie jest niepodważalny, ale pozostaje trudny do złamania. Przykładowo 104-bitowy standard RC4 używany w 128-bitowym szyfrowaniu WEP sieci bezprzewodowej może zostać złamany przez narzędzie AIRCRACK-PTW w ciągu czasu krótszego niż jedna minuta.

**Funkcja „skrót”, haszująca**

Ostatni powszechnie wykorzystywany algorytm bazujący na kluczu to funkcja haszująca, która pobiera wiadomość o dowolnej wielkości i stosuje względem niej krótki, stałej wielkości kod. W wyniku otrzymywana jest krótsza (niż początkowe dane wejściowe) wartość hash. Funkcja haszująca to funkcja matematyczna, która przyporządkowuje wiadomość o dowolnej długości, wartości, o stałej wielkości („skrót”). Można powiedzieć, że funkcja „skrót” zwraca wartość indeksu; wartość ta jest nazywana wartością hash, czasami digest, kodem hash, sumą hash lub po prostu hash. Wartość hash można upublicznić bez obawy o bezpieczeństwo początkowych danych wejściowych.

Funkcje „skrót” są funkcjami jednokierunkowymi. Ich wartości mogą być obliczone, ale obliczona wartość nie zawiera żadnych informacji bądź metod służących do przywrócenia początkowych danych. Wynika to z faktu, że wartość hash to zredukowany zestaw danych i nie zawiera wystarczających informacji do przywrócenia danych początkowych. Funkcja haszująca, która okazuje się być poza zakresem obliczeniowym dla innych danych wejściowych generujących taką samą wartość hash, jest określana jako funkcja kodująca typu *weakly collision-free*. Funkcja haszująca gwarantująca unikalne wygenerowanie wartości hash dla każdego unikalnych danych wejściowych jest określana mianem funkcji kodującej typu *strongly collision-free*. Na rysunku 27.8 pokazano sposób stosowania funkcji kodującej względem wiadomości w celu utworzenia wartości hash. Proces rozpoczyna się od bloku wiadomości po lewej stronie i przesuwają się do bloku wiadomości po prawej stronie. Każdy blok dostarczający dane wejściowe wartości hash jest pobierany w prawym dolnym rogu rysunku.



**Rysunek 27.8.** Użycie funkcji „skrót” do utworzenia wartości hash

Funkcje haszujące są stosowane w algorytmach sprawdzania błędów, sum kontrolnych, skrótach danych oraz innych technologiach. Można je wykorzystać również do wyszukiwania rekordów powielonych w bazie danych, takich samych genomów w sekwencji bazy danych itp.

Kiedy kryptograficzna funkcja haszująca zostanie zastosowana do danych takich jak wiadomość e-mail, to tworzy wartość hash będącą w zasadzie podpisem cyfrowym. Odbiorca wiadomości pobiera dane, oblicza wartość hash i sprawdza, czy dane są identyczne (poprzez

porównanie wygenerowanych wartości hash) z tymi, które zostały wysłane. Zmiana choć jednego znaku w zaszyfrowanej wiadomości o dowolnej długości powoduje wygenerowanie zupełnie innej wartości hash. Dlatego też kryptograficzna funkcja „skrótów” jest istotnym narzędziem w metodach weryfikacji, ponieważ tworzy to, co nazywamy podpisem cyfrowym. Prawdziwe podpisy cyfrowe wymagają szyfrowania asymetrycznego, to znaczy pary klucza — prywatnego i publicznego.

Najbardziej znana kryptograficzna funkcja haszująca to MD4 (obecnie złamana i porzucona), która została zastąpiona przez znacznie bezpieczniejszą funkcję MD5. MD oznacza *Message Digest*, czyli algorytm opracowany przez Ronalda Rivesta w roku 1990 na uczelni MIT. Algorytm MD4 używał 128-bitowej wartości hash do wygenerowania podpisu cyfrowego. Algorytm MD4 jest wykorzystywany do sprawdzania haseł w Windows NT, Windows XP, Windows Server 2003 oraz Windows Vista i Windows Server 2008. Wiele obecnych funkcji kodujących, łącznie z MD5, algorytmem *Secure Hash Algorithm* (SHA) opracowanym przez Agencję Bezpieczeństwa Narodowego (ang. *National Security Agency*, NSA) Stanów Zjednoczonych oraz *RACE Integrity Primitive Evaluation Message Digest* (RIPEMD) bazuje na technologii MD4.

Technologia powiązana z funkcjami kodującymi to metodologia kodu *Message Authentication Code* (MAC). MAC używa algorytmu oraz tajnego klucza i operuje na danych wejściowych w celu wygenerowania kodu MAC lub znacznika przedstawiającego dane wejściowe. Ponieważ wykorzystywany jest tajny klucz, dane są nie tylko uwierzytelniane przez znacznik, ale również mogą być dzięki niemu zweryfikowane. MAC nie wymaga, aby dane, na których operuje, były szyfrowane podczas wysyłania; tym zajmuje się inna technologia, *Message Integrity Code* (MIC). Kiedy technologia MIC jest stosowana względem wiadomości, to po użyciu tego samego algorytmu wartością zwrótną zawsze będzie taki sam znacznik. W przypadku MAC ta sama wiadomość zwraca ten sam znacznik tylko wtedy, gdy zostanie użyty ten sam klucz. Ponieważ jest to technologia szyfrowania z wykorzystaniem klucza symetrycznego, nie można jej stosować jako podpisu cyfrowego. Oznacza to, że MAC nie gwarantuje możliwości unikalnego zidentyfikowania nadawcy dokumentu.

W przypadku technologii MAC tajny klucz jest generowany przez komputer-wyrocnię, który możemy tutaj traktować jak „czarne pudełko” wyposażone w interfejs maszyny Turing. Użytkownik zadaje pytanie komputerowi-wyrocni i otrzymuje odpowiedź. W przypadku MAC pytanie dotyczy tajnego klucza, który jest potrzebny do odczytania danej wiadomości. Jedynym sposobem, w jaki atakujący może złamać MAC, jest zdobycie wiadomości i uzyskanie dostępu do komputera-wyrocni generującego wiadomość. Prosty dostęp do komputera-wyrocni nie zapewni klucza bez wysłania wiadomości.

## Algorytmy asymetryczne, czyli algorytmy klucza publicznego

Druga szeroka klasa technologii kryptograficznych bazujących na kluczach to algorytmy asymetryczne, czyli algorytmy klucza publicznego. Tego rodzaju algorytmy używają klucza publicznego do szyfrowania danych oraz klucza prywatnego do odszyfrowania i (lub) zweryfikowania wartości hash wiadomości bądź samej wiadomości. Algorytmy

Diffie-Hellman-Merkel i RSA, które zostały pokrótce omówione na początku tego podrozdziału, są technologiami klucza asymetrycznego. Inne algorytmy zaliczające się do tej kategorii to systemy kryptograficzne Cramer-Shoup, szyfrowanie ElGamal oraz algorytm Elliptic Curve.

Szyfrowanie z użyciem asymetrycznego klucza i podpisu cyfrowego polega na wykorzystaniu dwóch kluczy. Pierwszy to klucz publiczny wykorzystujący jeden algorytm i służący do szyfrowania danych. Natomiast drugi to klucz prywatny stosowany do odszyfrowania danych za pomocą drugiego algorytmu. Klucze mogą być wygenerowane w tym samym czasie jako para dwóch powiązanych ze sobą kluczy, ale nie ma możliwości wygenerowania jednego klucza na podstawie drugiego. Kombinacja użycia dwóch kluczy oznacza również, że treść może być unikalnie zidentyfikowana jako pochodząca z określonego komputera. Opracowanie kryptografii klucza publicznego jest uznawane za jedno z najważniejszych osiągnięć w informatyce na przestrzeni ostatnich 50 lat.

Algorytmy leżące u podstaw kluczy publicznych są technologiami generowania kluczy bazującymi na rozwiązywaniu bardzo trudnych problemów obliczeniowych. Trzy stosowane metody polegają na rozkładzie liczby całkowitej na czynniki, gdzie duża liczba jest tworzona przez pomnożenie ogromnej ilości małych liczb. Algorytm RSA używa metody rozkładu liczby całkowitej na czynniki i dowiódł, że odgadnięcie 200-cyfrowej liczby wymaga obliczeń komputerowych trwających około 50 lat. Algorytm D-H-M wykorzystuje technologię bazującą na obliczeniach logarytmicznych, w których logarytm jest rozwiązaniem równania  $gx = h$ , gdzie  $g$  i  $h$  są elementami skończonych grup cyklicznych. Trzeci algorytm szuka rozwiązania krzywych eliptycznych, bazując na wzorze  $y^2 = x^3 + ax + b$ . Wszystkie trzy wymienione problemy są pod względem obliczeniowym trudne do rozwiązania za pomocą współczesnych technologii informatycznych.

Podpisy cyfrowe są stosowane we wszystkich ważnych technologiach infrastruktury klucza publicznego, takich jak SSL/TLS, VPN, Kerberos itp. Dwa najczęściej używane algorytmy klucza publicznego to *Rivest-Shamir-Adleman* (RSA) oraz *Digital Signature Algorithm* (DSA).

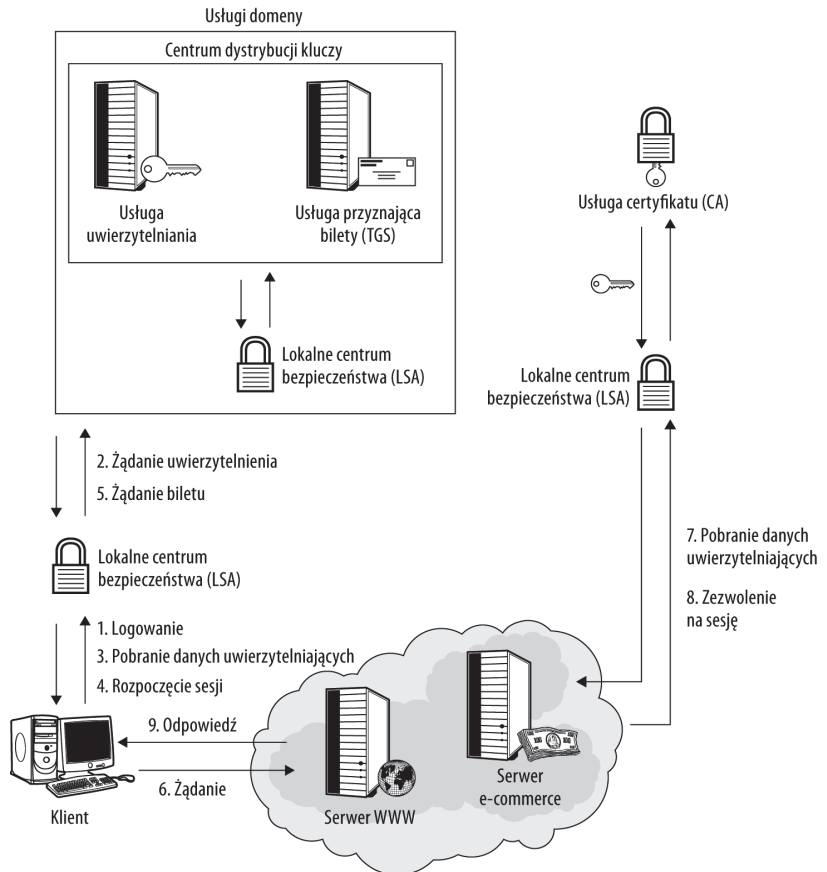
## Kerberos

Protokół Kerberos to system uwierzytelniania sieciowego, który bazuje na infrastrukturze klucza symetrycznego oraz zaufanym systemie firmy trzeciej. Na tej podstawie ustala tożsamość stron komunikacji i gwarantuje, że dane zostaną dostarczone bez ingerencji lub przejęcia. System Kerberos został utworzony w celu umożliwienia wysyłania danych przez niezabezpieczone połączenia (na przykład internet) przy jednoczesnym zagwarantowaniu, że nie zostaną podejrzone lub ponownie przetransmitowane jako część ataku z osobą pośrodku (ang. *man-in-the-middle attack*) lub ataku powtórzeniowego (ang. *replay attack*). Od chwili opracowania na uczelni MIT Kerberos został rozszerzony na wiele sposobów i zawiera uwierzytelnianie z użyciem algorytmu klucza asymetrycznego. Na rysunku 27.9 pokazano obecną implementację mechanizmu Kerberos w systemie Windows Server 2008/Vista.

Pokazany na rysunku 27.9 mechanizm Kerberos podczas uwierzytelniania działa w następujący sposób:

1. Klient loguje się do sieci, a informacje logowania są wysyłane do systemu lokalnego centrum bezpieczeństwa (ang. *Local Security Authority*, LSA).

**Rysunek 27.9.**  
*Mechanizm  
 i infrastruktura  
 Kerberos w Microsoft  
 Server 2008*



2. System LSA przekazuje żądanie do usługi uwierzytelniania wraz z żądaniem uwierzytelnienia klienta przez LSA.
3. Żądanie jest przekazywane do polecenia Pobranie danych uwierzytelniających z systemu LSA, a system LSA wysła klientowi odpowiednie dane uwierzytelniające.
4. Klient rozpoczyna sesję.
5. Bilet żądania dla danej aplikacji, sesji lub operacji jest przekazywany do LSA przez klienta, a następnie przesyłany dalej do serwera przyznającego bilety (ang. *Ticket Granting Service, TGS*). Bilet utworzony w TGS jest zwracany klientowi.
6. Żądanie jest przekazywane do serwera WWW w celu bezpiecznego pobrania informacji z systemu e-commerce.
7. Serwer WWW może przekazać żądanie do serwera E-Commerce, a następnie wysłać polecenie Pobranie danych uwierzytelniających do systemu LSA, który z kolei przekazuje żądanie do usługi certyfikatu (ang. *Certificate Service*).
8. Usługa certyfikatu wysła dane uwierzytelniające do systemu LSA, który następnie wykonuje polecenie Zezwolenie na sesję.
9. Serwer WWW wysła informacje żądane przez klienta.

Nazwa „Kerberos” pochodzi od Cerbera (*Cerberus*), mitycznego trzygłowego psa, który strzegł Hadesu. Kerberos został opracowany jako część projektu Athena na uczelni MIT i po raz pierwszy pojawił się w wersji 4. w roku 1988. Wersja 5. pojawiła się w roku 1993 i została opublikowana przez IETF jako dokument RFC 1510. Standard MIT Kerberos jest dostępny bezpłatnie i wielu ważnych graczy w internecie, między innymi Sun Microsystems, Microsoft, Google, Apple oraz inne firmy, utworzyło konsorcjum Kerberos Consortium w celu kontynuowania prac w MIT nad tym standardem. Kerberos jest używany w wielu sieciowych systemach operacyjnych, o których Czytelnik mógł przeczytać w tej książce, takich jak Solaris, BSD UNIX, sieci Windows (od wersji 2000 wzwyż), Mac OS X czy Red Hat Linux (v.4 i późniejsze).



W celu uzyskania informacji na temat dowolnego dokumentu RFC w IETF można zapoznać się z jego opisem na stronie wyszukiwania dokumentów RFC, znajdującej się pod adresem <http://www.ietf.org/rfc.html>.

Kerberos pierwotnie używał szyfrowania DES, co doprowadziło do tego, że władze Stanów Zjednoczonych zakazały eksportu tej technologii do innych krajów w ramach przepisów o zakazie eksportu uzbrojenia, obowiązujących do roku 2000. Windows Server 2000 to pierwszy ważniejszy sieciowy system operacyjny, który zawierał technologię Kerberos wraz z DES-56. Od tej chwili Microsoft korzysta z algorytmu RC4 w swoim szyfrowaniu Kerberos. Poza Stanami Zjednoczonymi opracowano inne wersje systemu Kerberos, które nie stosowały algorytmu DES. Do najbardziej znanych implementacji zaliczają się eBones i Heimdal.

Kerberos używa dwóch protokołów komunikacji opracowanych przez Rogera Needhama i Michaela Schroedera. Protokół *Symmetric Key Protocol* wykorzystuje algorytm szyfrowania symetrycznego w celu utworzenia klucza sesji między punktami końcowymi połączenia. Protokół *Public Key Protocol* stosowany w systemie Kerberos służy do ustanowienia wspólnego uwierzytelnienia między punktami końcowymi. Zaufaną firmę trzecią w systemie Kerberos określa się mianem centrum dystrybucji kluczy (ang. *Key Distribution Center*, KDC); jest ona umieszczona w dwóch oddzielnych usługach: serwerze uwierzytelniania (AS) oraz serwerze przyznającym bilety (TGS).

Bilety są rozpowszechniane w celu umożliwienia klientowi samoidentyfikacji w sesji. Centrum dystrybucji kluczy ma zbiór tajnych kluczy zapisanych w magazynie danych dla każdego węzła sieciowego. Tajny klucz jest znany tylko węzłowi oraz centrum dystrybucji kluczy, nikt inny go nie zna. Kiedy nawiązywane jest połączenie, centrum dystrybucji kluczy generuje klucz sesji używany do uwierzytelnienia punktów końcowych połączenia.

Wprawdzie mechanizm Kerberos angażuje co najmniej osiem różnych wiadomości między klientem, serwerem przyznającym bilety i usługą serwera, ale wiadomości te pozwalają każdemu węzłowi w systemie zarówno na samoidentyfikację, jak i weryfikację wiadomości pochodzących z innego węzła. Sukces każdej operacji

- ♦ logowania klienta,
- ♦ uwierzytelniania klienta,
- ♦ autoryzacji usługi klienta,
- ♦ żądania usługi klienta

zależy zarówno od dwóch wiadomości wymieniających bilety, jak i dopasowania kluczy sesji. Żadna wiadomość nie zawiera obu tych informacji. Kerberos powoduje obciążenie sieci, ale system jest bezpieczny. Kerberos jednak nie jest pozbawiony problemów. Jeden z nich to serwer przyznający bilety — to pojedynczy punkt systemu, który w przypadku awarii powoduje błędne działanie całości. Dlatego też trzeba umożliwić mu funkcjonowanie w przypadku awarii.

Ponadto Kerberos zależy od znaczników czasu umieszczanych w wiadomościach na każdym etapie, więc wszystkie systemy muszą pozostać zsynchronizowane za pomocą usługi takiej jak NTP (ang. *Network Time Protocol*) lub WTS (ang. *Windows Time Service*). Kerberos może tolerować drobny brak synchronizacji, zwykle do około dziesięciu minut. Większa asynchroniczność prowadzi do tego, że bilety stają się nieważne. Wymienione czynniki można dostosować jako część polityk domeny oraz w ustawieniach mechanizmu Kerberos.

Ostatnia niedogodność wiąże się z faktem, że serwer uwierzytelniania przechowuje wszystkie tajne klucze. Jeżeli ktoś uzyska dostęp do tego serwera, to bezpieczeństwo całej sieci będzie zagrożone. Na poziomie poszczególnych klientów złamanie systemu może doprowadzić do ujawnienia hasła klienta. Mimo to Kerberos jest obecnie najnowocześniejszą technologią uwierzytelniania sieciowego i usługą identyfikacji oraz ilustruje wiele reguł, które omówiono w tym rozdziale.

## Podsumowanie

W tym rozdziale przedstawiono różne aspekty dotyczące bezpieczeństwa sieciowego. Czytelnik dowiedział się, jak wiele miejsc w sieci może zostać zaatakowanych oraz jak wiele metod może być stosowanych przez atakującego. Do zabezpieczenia sieci potrzebna jest wielowarstwowa i wielokierunkowa obrona. W rozdziale omówiono wybrane podstawowe reguły, które można zastosować w celu zabezpieczenia sieci.

Zaprezentowane zostały trzy protokoły bezpieczeństwa w internecie: IPsec, TLS/SSL oraz HTTPS. Technologie szyfrowania oferują zabezpieczenie przed przejęciem danych. W rozdziale omówiono trzy różne technologie szyfrowania bazujące na kluczach oraz pokazano sposoby ich działania. Przedstawiono także system Kerberos.

W rozdziale 28. będą szczegółowo opisane zapory i bramy sieciowe. Zapora sieciowa to podstawowe narzędzie służące do ochrony sieci.



## Rozdział 28.

# Zapory sieciowe, bramy i serwery proxy

### W tym rozdziale:

- ♦ W jaki sposób można używać zapór sieciowych w celu ochrony sieci?
- ♦ Filtry, które można zastosować
- ♦ Używanie mechanizmu NAT do ukrywania systemów
- ♦ Stosowanie serwerów proxy do zabezpieczania usług sieciowych

W rozdziale zostanie przedstawionych kilka różnego rodzaju usług sieciowych wykorzystywanych do zabezpieczania sieci: zapory sieciowe, bramy oraz serwery proxy. Usługi te mogą być zaimplementowane sprzętowo bądź za pomocą oprogramowania. Ich zastosowanie pomaga w ochronie sieci i znacznie utrudnia użytkownikom z zewnątrz uzyskanie nieupoważnionego dostępu do sieci prywatnej.

Zapora sieciowa kontroluje ruch sieciowy i decyduje o dalszym przekazaniu bądź odrzuceniu ruchu sieciowego. Kryteria, na których podstawie zapora sieciowa podejmuje decyzję, są nazywane filtrami. Filtry mogą bazować na informacjach w nagłówkach pakietów, takich jak adres źródłowy, używany protokół, oraz na wielu innych czynnikach. Zaawansowane zapory sieciowe mogą przeglądać pakiety na poziomie aplikacji i przeprowadzać głęboką analizę pakietu (ang. *Deep Packet Inspection*).

Urządzenia sprzętowe mogą przeprowadzać operację tłumaczenia adresów sieciowych (ang. *Network Address Translation* — NAT), co zostanie wyjaśnione w dalszej części rozdziału. Mechanizm NAT polega na pobraniu żądania od klienta znajdującego się w sieci publicznej i przekierowaniu go do systemów w sieci prywatnej. Dzięki tej funkcji systemy w sieci prywatnej zachowują anonimowość i możliwość komunikacji z siecią publiczną urządzeń z adresami IP z zakresu adresacji prywatnej.

Brama jest systemem działającym w charakterze interfejsu między dwoma różnymi sieciami i jest urządzeniem warstwy aplikacji (warstwa 7.). Dostępne są również bramy bezpieczeństwa odpowiedzialne za bezpieczeństwo. Serwer proxy to produkt pośredni między bramą i zaporą sieciową. Serwer proxy działa w charakterze substytutu dla systemów znajdujących

się w sieci prywatnej, przechwytuje wszystkie żądania i obsługuje udzielanie wszystkich odpowiedzi. Wiele serwerów proxy zapewnia także buforowanie. Inne są skonfigurowane jako serwery odwrotnego proxy i mogą wykonywać wiele funkcji aplikacji i usług sieciowych.

## Zapory sieciowe

W budynku ściana przeciwpożarowa<sup>1</sup> to warstwa składająca się z materiału ognioodpornego, której zadaniem jest izolacja i ochrona przed ogniem w sytuacji, kiedy pożar obejmie sąsiednią ścianę. W sieci komputerowej odpowiednikiem ściany przeciwpożarowej jest zaporą sieciową — bariera ochronna, którą stanowi zbiór procedur bezpieczeństwa izolujących i chroniących systemy danej sieci przed podejrzaną aktywnością. Może to być oddzielenie sieci za pomocą odrębnych urządzeń sprzętowych (fizycznych interfejsów sieciowych), zawierających wiele połączeń z siecią. Taki mechanizm nazywa się izolacją fizyczną. Zapora sieciowa może kontaktować się z siecią zewnętrzną, używając jednego protokołu sieciowego, natomiast z siecią wewnętrzną — za pomocą innego protokołu sieciowego. Określa się to izolacją protokołu. W dzisiejszych czasach posiadanie systemów połączonych z internetem bez żadnej zapory sieciowej jest bardzo nierozważne.

Zapora sieciowa może być zarówno bardzo prosta, jak i niezwykle skomplikowana. Może być zaimplementowana w oprogramowaniu lub być oprogramowaniem zainstalowanym na dedykowanych serwerach i urządzeniach. Może działać w ramach używanego systemu operacyjnego, na przykład Linuksa, Uniksa lub Windows, albo być rodzajem „czarnego pudełka”, czyli samodzielną jednostką działającą pod kontrolą własnego systemu operacyjnego. Zapory sieciowe mogą być podzielone na następujące kategorie:

- ♦ osobiste zapory sieciowe takie jak zaporą sieciową w systemie Windows, ZoneAlarm i inne,
- ♦ zapory sieciowe w routerach,
- ♦ sprzętowe zapory sieciowe zarówno proste, jak i bardzo skomplikowane,
- ♦ zapory sieciowe w postaci proxy,
- ♦ zapory sieciowe w postaci serwerów.

Zapora sieciowa najczęściej oferuje funkcje, które można zaliczyć do więcej niż tylko jednej z wymienionych kategorii. Podczas porównywania zapór sieciowych trzeba wziąć pod uwagę trzy czynniki: oferowane funkcje, wydajność (mierzoną przepustowością) oraz cenę. Zapory sieciowe to urządzenia sieciowe, dla których nie istnieją standaryzowane testy wydajności. Producenci wiedzą, że klienci używają zapór sieciowych na wiele różnych sposobów, i nie znoszą przedstawiania testów wydajności potencjalnym nabywcom.

## Funkcje zapory sieciowej

Niezależnie od natury zaimplementowanej zapory sieciowej jej działanie polega na stosowaniu zestawu filtrów ruchu sieciowego przechodzącego przez tę zaporą sieciową. Zapora sieciowa może przekazać dalej albo odrzucić dany ruch sieciowy. W modelu OSI zaporą

---

<sup>1</sup> Ściana przeciwpożarowa to w języku angielskim *firewall*; słowo to w informatyce oznacza zaporą sieciową — *przyp. tłum.*

sieciowa może być filtrem warstwy sieci (warstwa 3.) bądź aplikacji (warstwa 7.) lub dowolnej warstwy między trzecią i siódmą.

Poniżej wymieniono wybrane funkcje, na które warto zwrócić uwagę podczas porównywania zapór sieciowych:

- ♦ **Filtrowanie pakietów.** Operacja filtrowania pakietów odczytuje pola nagłówka pakietu IP i używa zdefiniowanych reguł w celu zezwolenia na ruch przychodzący do systemu lub zablokowania tego ruchu. Filtrowanie pakietów można również zastosować wobec ruchu wychodzącego.
- ♦ **Filtry danych wejściowych interfejsu sieciowego.** Filtry te blokują ruch sieciowy na podstawie parametrów takich jak źródłowy adres IP lub zakres adresów, numer portu czy użyty protokół.
- ♦ **Mechanizm tłumaczenia adresów sieciowych (NAT).** NAT to system konwersji, którego zadaniem jest zmiana źródłowych lub docelowych adresów IP, zazwyczaj również portów TCP/UDP w przepływających pakietach. Mechanizm NAT wykorzystuje tablice translacji i współpracuje z nieroutowalnymi w sieci publicznej sieciami prywatnymi. Mechanizm NAT to nie jest, ściśle rzecz biorąc, funkcja zapory sieciowej — znacznie częściej jest powiązany z routerami i serwerami proxy — jednak dostarcza technologię pozwalającą na ukrycie adresu IP systemów sieci prywatnej, co jest cenną funkcją.
- ♦ **Stateful Inspection.** Filtry typu Stateful Inspection przeprowadzają analizę wszystkich pakietów wychodzących i rejestrują ich adresy docelowe w tabeli stanu. Kiedy ruch sieciowy jest wysyłany z powrotem z systemu zewnętrznego, zaporą sieciową używa tabeli stanu w celu określenia, czy pakiety powinny być przekazywane. Ogólna reguła jest taka, że filtry typu Stateful Inspection są o wiele większym obciążeniem dla zapory sieciowej i działają znacznie wolniej niż statyczne filtrowanie pakietów.
- ♦ **Analiza połączeń.** W filtrze tego typu sesje są zarządzane, zamiast po prostu odwoływać się do pakietów lub połączenia w tabeli stanu. Sesje wymagają żądania pochodzącego z systemu znajdującego się za zaporą sieciową i mogą obsługiwać aplikacje tworzące wiele połączeń. Protokoły z wieloma połączeniami obejmują między innymi sesje HTTP przeglądarki internetowej, pobieranie plików za pomocą FTP oraz strumieniowanie multimedialne.

Funkcja analizy połączeń znacznie utrudnia przeprowadzenie udanego ataku typu IP spoofing (fałszowanie źródłowego adresu IP), DoS (ang. *Denial of Service* — odmowa usług) i prób rozpoznania sieci. Filtry powiązane z funkcją analizy połączeń stanowią mniej efektywną ochronę przed atakami typu DoS.

- ♦ **Zapora sieciowa w postaci proxy.** Zapora sieciowa w postaci proxy działa w charakterze pośrednika między klientem znajdującym się wewnątrz zapory sieciowej i systemem lub serwerem na zewnątrz. Między obiema stronami nie ma bezpośredniego połączenia przez zaporę sieciową. Zapora sieciowa w postaci proxy tworzy dwa oddzielne połączenia, po jednym dla każdej strony zapory sieciowej. Klient wewnątrz komunikuje się jedynie z proxy, które z perspektywy klienta jest jego punktem docelowym. Serwer proxy może zwiększyć wydajność działania przez buforowanie najczęściej lub ostatnio używanych danych. Ma również możliwość

weryfikacji protokołów przekazywanych przez zaporę sieciową. Pozwala także na zarządzanie w taki sposób, aby żądania były przekazywane na bazie identyfikatora użytkownika i (lub) członków grupy.

Z powodu wszystkich wymienionych powyżej funkcji zaporą sieciową w postaci proxy wymaga najwięcej zasobów i jest najwolniejszym filtrem. Jednak taki rodzaj zapory sieciowej może chronić sieć zarówno przed atakami typu IP spoofing, DoS, próbami rozpoznania sieci, jak i przed wirusami, końmi trojańskimi i robakami. Zapora sieciowa w postaci proxy oferuje jedynie ograniczoną ochronę na poziomie aplikacji.

- ♦ **Filtrowanie aplikacji.** Filtrowanie na poziomie aplikacji to technologia tzw. głębokiej analizy pakietów (ang. *deep packet inspection*). Metoda ta jest najbardziej skomplikowana i najwolniejsza z wymienionych na tej liście. Filtry tej metody analizują pakiety pod kątem zawartych w nich danych, a następnie modyfikują je, jeśli zachodzi taka potrzeba.

Przedstawione funkcje i filtry będą po kolei dokładniej omówione w kolejnych podrozdziałach.

## Osobista zapora sieciowa

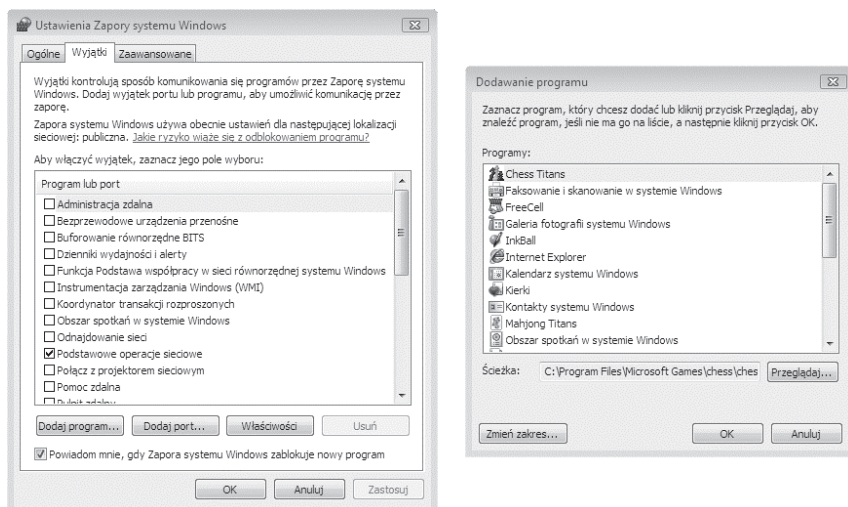
Osobista zapora sieciowa została zaprojektowana w celu ochrony pojedynczego komputera lub rzadziej sieci w domu bądź małym biurze, która współdzieli pojedyncze połączenie. Przykładami osobistych zapór sieciowych są produkty CA Personal Firewall, Comodo Firewall Pro, IPFilter, ipfirewall, Kaspersky Internet Security, Lavasoft Personal Firewall, Norton 360, Outpost Firewall Pro, PC Tools Firewall Plus, Sunbelt Personal Firewall, Sygate Personal Firewall, Trend Micro Internet Security oraz ZoneAlarm, przy czym ZoneAlarm jest najlepiej znany z całej grupy.



Porównanie osobistych zapór sieciowych można znaleźć w Wikipedii, na stronie [http://en.wikipedia.org/wiki/Comparison\\_of\\_firewalls](http://en.wikipedia.org/wiki/Comparison_of_firewalls).

Obecnie wiele systemów operacyjnych jest dostarczanych wraz z osobistymi zaporami sieciowymi. Przykładem wbudowanej zapory sieciowej jest *Zapora systemu Windows*, dostarczana z Windows, począwszy od wydania XP SP1. Dodanie tej zapory sieciowej do systemu miało ogromny wpływ na uodpornienie systemu Windows na ataki z zewnątrz. Wprawdzie to bardzo prosta zapora, ale jednak wykonuje swoje zadanie. Na rysunku 28.1 pokazano zaporę systemu Windows dostępną w systemie Vista SP1. Wersja ta okazała się dużym usprawnieniem w stosunku do początkowej wersji zapory sieciowej dodanej do systemu Windows XP. Zapora sieciowa dostępna w systemie Vista pozwala na filtrowanie na podstawie źródłowego i docelowego adresu IP, źródłowego i docelowego numeru portu TCP, dla ruchu wewnętrznego i zewnętrznego oraz względem identyfikatora użytkownika. Jediną podstawową funkcją niedostępną w zaporze sieciowej systemu Vista, która znajduje się w niemal każdym produkcie wymienionym na powyższej liście, jest filtrowanie względem źródłowego i docelowego adresu MAC. Z kolei zapora sieciowa znajdująca się w systemie Windows XP nie ma możliwości filtrowania względem docelowego adresu IP, numeru portu źródłowego (i do pewnego stopnia numeru portu docelowego) oraz identyfikatora użytkownika. Nie ma też możliwości filtrowania ruchu wychodzącego. W opinii autora zaporę sieciową systemu Windows XP warto zastąpić inną, natomiast bez obaw można używać zapory sieciowej dostarczanej wraz z Windows Vista.

**Rysunek 28.1.**  
Zapora sieciowa  
w systemie  
Windows Vista  
pozwala na  
konfigurację reguł  
względem numeru  
portu, protokołu,  
jak również  
używanej aplikacji



Autor nie jest zwolennikiem osobistych zapór sieciowych, ale dostrzega ich użyteczność. Wiele zapór sieciowych ma ogromny wpływ na wydajność systemów — w szczególności słabszych, m.in. w laptopach. Niektóre zapory sieciowe, na przykład ZoneAlarm, nieustannie przerywają pracę, wyświetlając wyskakujące okna oraz okna dialogowe z pytaniem o pozwolenie na przeprowadzenie danej operacji. Podczas wyboru osobistej zapory sieciowej są to ważne czynniki, które należy wziąć pod uwagę. Warto pamiętać, że osobista zapora sieciowa powinna być zarówno niedroga (wiele jest bezpłatnych), jak i łatwa w konfiguracji. Ponadto osobiste zapory sieciowe są przeznaczone do działania na wyłączność. Uruchomienie w tym samym czasie dwóch lub więcej zapór sieciowych jest niepotrzebne i niepożądane.

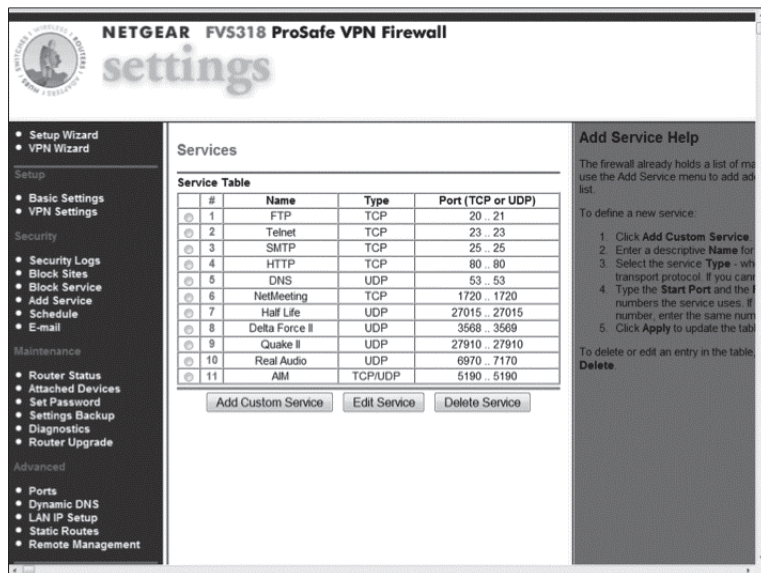
## Zapory sieciowe w routerach

Wiele routerów jest dostarczanych wraz z wbudowaną zaporą sieciową. Niedrogie routery zwykle obsługują blokowanie adresu i portu, a także pewną odmianę mechanizmu NAT w celu ukrywania adresów sieci prywatnej. Tanie routery są często oferowane jako urządzenia umożliwiające uzyskanie połączenia z internetem. Dostawca usług internetowych może więc zainstalować taki router w sieci domowej jako część okablowania bądź połączenia DSL. Takie routery to zwykle urządzenia zawierające kilka ustawień. Należy pamiętać, że tanie routery funkcjonujące jako zapory sieciowe są dostarczane przez producenta w konfiguracji, która efektywnie blokuje niechciany ruch internetowy. Do rozpoczęcia pracy z reguły wystarcza więc zmiana identyfikatora konta administracyjnego oraz jego hasła. Jeżeli zachodzi taka potrzeba, to można przeprowadzić dodatkową konfigurację.

Urządzenie Netgear FVS318 ProSafe Firewall to przykład taniego routera z wbudowaną zaporą sieciową. Bazuje ono na technologii opracowanej przez firmę SonicWALL (<http://www.sonicwall.com>), czyli jedną z najbardziej znanych firm na polu sprzętowych zapór sieciowych. Model FVS318 jest konfigurowany za pomocą przeglądarki internetowej. Na rysunku 28.2 pokazano ustawienia na stronie *Services*, pozwalającej na konfigurację otwartych portów. Inne funkcje dostępne w tym prostym routerze to między innymi mechanizm NAT, przypisywanie portów, blokowanie względem domeny i adresu IP, przypisywanie routingu statycznego, funkcja *Stateful Packet Inspection* (SPI) i wiele innych.

**Rysunek 28.2.**

Strona ustawień  
Services w routerze  
(zaporze) sieciowej  
Netgear FVS318  
pozwala na  
konfigurację portów  
i aplikacji



Istnieje ogólna tendencja do ustalania cen routerów (zapor) sieciowych na podstawie liczby użytkowników, których dane urządzenie może jednocześnie obsłużyć, co często znacząco podnosi koszt. W systemach oferowanych przez SonicWALL można mieć wbudowane oprogramowanie antywirusowe uaktualniane automatycznie przez internet. Ponadto istnieje możliwość dodania różnych rodzajów filtrów na poziomie aplikacji wraz z głęboką analizą pakietów oraz wiele innych funkcji. Router wyższej klasy z zaporą sieciową zbliża się pod kątem funkcji do dedykowanej zapory sieciowej, ale generalnie charakteryzuje się niższą ceną i mniejszą przepustowością niż sprzętowa zaporą sieciową.

Router i zaporą sieciową „w jednym” to bardzo wygodny wybór; obie funkcje sieciowe mogą być zarządzane w jednym miejscu. Koszt takiego urządzenia jest stosunkowo niski (obecna wersja FVS318 kosztuje około 350 zł), natomiast koszt lepiej wyposażonych urządzeń tego rodzaju może sięgać kilku tysięcy złotych. Ogólnie rzecz ujmując, routery niższej klasy mają ograniczony zestaw funkcji, z reguły dostarczają jedynie podstawowe opcje konfiguracyjne, do efektywnego działania wymagają skonfigurowania wielu ustawień i mają przy tym ograniczoną przepustowość, zwłaszcza w przypadku rejestrowania zdarzeń w dzienniku zdarzeń.

## Sprzętowe zapory sieciowe

Sprzętowe zapory sieciowe są urządzeniami dedykowanymi do pełnienia funkcji zapory sieciowej i zwykle mają ograniczone możliwości w zakresie routingu. Urządzenia klasy niższej w tej kategorii są urządzeniami typu „włącz i pracuj”, przeznaczonymi dla segmentu domowego i małych biur (ang. *Small Office/Home Office*, SOHO). W wielu przypadkach urządzenia te używają tego samego oprogramowania, które jest dostępne w znacznie droższych modelach produktów danego producenta; po uiszczeniu specjalnej opłaty zostają włączone dodatkowe funkcje.

Najtańsze urządzenia w tej kategorii oferują statyczne filtrowanie pakietów, mechanizm NAT, filtrowanie na bazie adresów i numerów portów, zdalne filtrowanie oraz możliwość jednoczesnej obsługi od dziesięciu do tysięcy użytkowników, przy czym pięćdziesięciu użytkowników to często spotykane najmniejsze ograniczenie. Urządzenia te zwykle są niedrogie i łatwe w obsłudze, oferują niższą wydajność i stosunkowo kiepskie możliwości w zakresie uaktualnienia. Połączenie routera i zapory sieciowej wydaje się popularniejszym rozwiązaniem niż dedykowana sprzętowa zapora sieciowa niższej klasy, ponieważ oferuje więcej funkcji w tej samej cenie.

Wysokiej klasy sprzętowe zapory sieciowe to całkiem inna historia. Te urządzenia mają uniemożliwiać przenikanie do sieci, być systemami o wysokiej wydajności oraz dostępności — są przeznaczone dla sieci klasy przemysłowej lub dla dostawców usług sieciowych. Wiele tych systemów produkcyjnych zapewnia odporność na awarie dzięki mechanizmom *Failover*, pozwalającym na przejście zadań uszkodzonego urządzenia przez zapasowe.

Sprzętowe zapory sieciowe o najwyższej wydajności bardzo często są dostarczane wraz z funkcjami zaawansowanymi, których zadaniem jest poprawienie wydajności. Podczas porównywania urządzeń tego rodzaju należy wziąć pod uwagę następujące cechy:

- ♦ **Liczba interfejsów Gigabit Ethernet światłowodowych lub elektrycznych.** Wyższa szybkość operacji wejścia-wyjścia przekłada się na większą przepustowość.
- ♦ **Solidne buforowanie danych.** Zaawansowane buforowanie może w dużym stopniu poprawić wydajność, ale wymaga dedykowanych mu zasobów dyskowych.
- ♦ **Usługi proxy lub odwrotnego proxy.** Proxy to usługa działająca w imieniu innej usługi lub aplikacji, tak jak serwer dostarczający usługi. Proxy to serwer WWW pobierający żądania z wewnątrz sieci, a następnie przetwarzający te żądania (na przykład za pomocą danych z bufora) albo kierujący je do odpowiednich serwerów WWW znajdujących się na zewnątrz sieci. Odwrócony serwer proxy pobiera żądania z zewnątrz sieci (prawdopodobnie internet), następnie je przetwarza albo przekierowuje do serwera WWW wewnątrz sieci.
- ♦ **Szyfrowanie (deszyfrowanie) IPsec przerzucone do dedykowanych serwerów.** Szyfrowanie IPsec jest używane w ruchu sieciowym VPN oraz podczas udostępniania sieciom publicznym (lub w internecie) usług sieci wewnętrznej. W większości zapór sieciowych IPsec to proces szczególnie powolny, więc jego przyspieszenie znacznie zwiększa wydajność zapory sieciowej.
- ♦ **Zmniejszenie obciążenia związanego z SSL.** Szyfrowanie SSL to proces intensywnie wykorzystujący procesor. Akcelerator SSL może pomóc w zmniejszeniu poziomu użycia procesora przez zaporę sieciową obsługującą daną witrynę sieciową. Kiedy zapora sieciowa jest punktem końcowym połączenia SSL, to wydajność działania danej witryny internetowej może wzrosnąć.
- ♦ **Modułowość i możliwości w zakresie skalowania.** Modułowość oznacza możliwość dodawania kolejnych podsystemów, kiedy zajdzie taka potrzeba.

Funkcje odróżniające sprzętowe zapory sieciowe wyższej klasy od innych urządzeń to między innymi obsługa filtrowania na poziomie aplikacji, usprawnione rejestrowanie zdarzeń i powiadamianie, możliwość uaktualniania urządzeń, solidna obsługa i pomoc techniczna ze strony producenta oraz oczywiście wysoka cena. Sprzętowa zapora sieciowa wyższej klasy

może jednocześnie obsłużyć od 5000 do 500 000 sesji. Większe możliwości tego rodzaju urządzeń oznaczają, że do ich obsługi firmy muszą posiadać wykwalifikowany personel bądź korzystać w tym zakresie z usług firm trzecich.

## Zapory sieciowe w postaci serwerów

Chociaż sprzętowe zapory sieciowe wyższej klasy z reguły działają na własnym sprzęcie i pracują pod kontrolą własnego systemu operacyjnego, wielu producentów wybrało implementację zapory sieciowej w standardowym serwerowym systemie operacyjnym i udostępnienie jej jako rozwiązania otwartego. Zaletą takiego podejścia jest to, że sposób działania serwera jest lepiej znany przez personel (a więc potrzeba mniej szkoleń i pomocy technicznej), sprzęt można właściwie dobrać do wykonywanego zadania, a ponadto dostępna jest szersza gama rozwiązań. Implementacja zapory sieciowej w standardowym sieciowym systemie operacyjnym oznacza również, że każda struktura lub aplikacja zarządzająca używana w innych systemach serwerowych może być wykorzystana także do obsługi tego rodzaju zapory sieciowej, co jest bardzo wygodne. Zapory sieciowe tej kategorii mają ponadto ogromne możliwości w zakresie buforowania.

Pod względem funkcji może istnieć jedynie niewielka różnica między serwerową zaporą sieciową wyższej klasy i sprzętową zaporą sieciową. Jednak zaporą sieciową w postaci serwera bardzo często jest łatwiejsza do zintegrowania, zapewnia większe możliwości skalowania i może być klastrowana oraz równoważona pod względem obciążenia w celu zapewnienia większego poziomu dostępności niż urządzenia dedykowane. Sprzętowa zaporą sieciową z reguły jest lepiej zoptymalizowana niż zaporą sieciową w postaci serwera. Aby zatem zaporą sieciową w postaci serwera działała na takim samym poziomie jak sprzętowa, konieczne jest użycie sprzętu wyższej klasy. Ponadto w przypadku doskonale znanych systemów operacyjnych zaporą sieciową serwera jest wrażliwsza na atak niż sprzętowa zaporą sieciową.

## Bramy bezpieczeństwa

Brama jest urządzeniem warstwy aplikacji (warstwa 7.) działającym w charakterze interfejsu między sieciami. Bramy mogą być zaimplementowane jako urządzenia sprzętowe bądź jako oprogramowanie. Pojęcie „brama” jest ogólne i generalnie oznacza występowanie pewnego rodzaju konwersji protokołów. W warstwie aplikacji brama musi przekształcać jeden rodzaj pliku na inny, w warstwie prezentacji konwersja może zastępować dany rodzaj szyfrowania innym lub wykonywać inne funkcje. Bramy mogą przeprowadzać konwersje na poziomie transportowym (warstwa sieci) z IP na AppleTalk. Ogólnie rzecz ujmując, brama to urządzenie, które może działać na dowolnym poziomie modelu OSI. W wyniku tego bardzo często można się spotkać z bramami opisywanymi jako „brama pocztowa”, „brama WWW” lub nawet „brama bezpieczeństwa”.

Aby brama mogła funkcjonować między sieciami, bardzo często musi mieć możliwość działania jako router dostarczający funkcji mapowania adresów. Bardzo często bramy pełnią funkcję serwera proxy lub zapory sieciowej. Jeżeli Czytelnik spotka się z pojęciem bramy bezpieczeństwa, to powinien mieć świadomość, że termin ten może odnosić się do urządzenia zaliczającego się do jednej z omówionych kategorii zapór sieciowych. Aby pojęcie bramy miało jakiegokolwiek rzeczywiste znaczenie, to według autora musi być położony nacisk na zdolność systemu do przeprowadzania konwersji na poziomie warstwy aplikacji.

## Strefy sieciowe

Zapora sieciowa dzieli obszar sieci na strefy o różnych poziomach zaufania, jak pokazano na przykładzie trzywarstwowej sieci klasy przemysłowej (rysunek 28.3). Przedstawiona na rysunku sieć została podzielona na poniższe strefy i sieci:

- ♦ **Internet.** Internet to strefa o zerowym poziomie zaufania. Wszystkie pakiety pochodzące z internetu są podejrzane aż do chwili ich przeanalizowania.
- ♦ **Sieć brzegowa.** Sieć brzegowa składa się z routera widocznego w internecie. Routery mają co najmniej dwa fizyczne połączenia. Interfejs zewnętrzny tego konkretnego routera ma połączenie z adresem IP witryny *Wiley.com*, natomiast interfejs wewnętrzny ma połączenie z pierwszym adresem sieci prywatnej. Sieci brzegowe kończą się na interfejsie wychodzącym granicznej zapory sieciowej (192.168.1.2).

Router brzegowy przeprowadza konwersję adresów, natomiast jego dwa interfejsy zapewniają fizyczną izolację sieci. Dotyczy to również innych routerów i zapór sieciowych w omawianym przykładzie. W przypadku każdej zmiany w tej sieci, zwłaszcza kiedy zmiana dotyczy sieci prywatnej, ilość wysiłku koniecznego do bezproblemowego przejścia przez zaporę sieciową wzrasta w postępie geometrycznym.

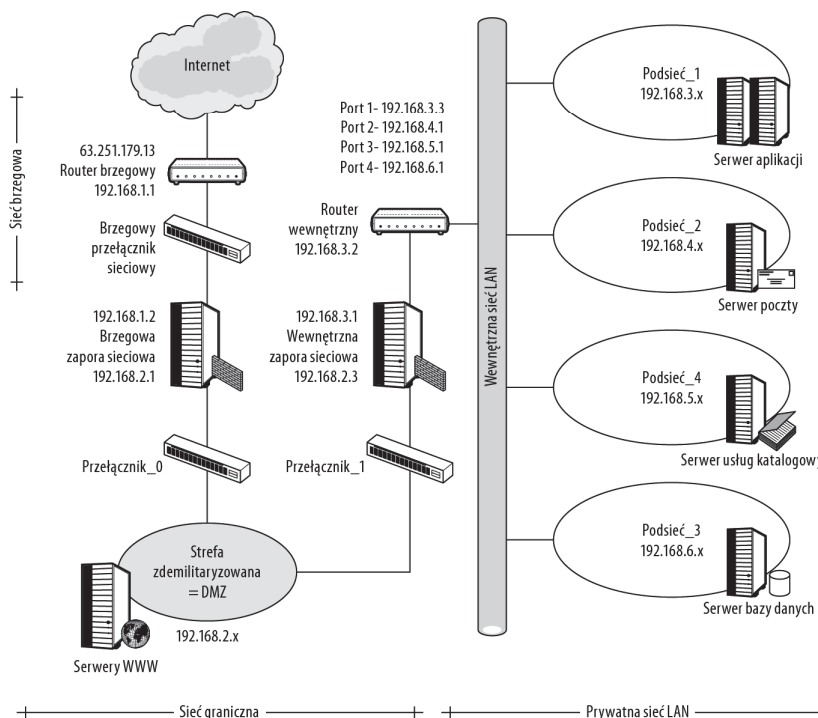
Dopóki systemy wewnętrzne nie zostaną złamane, przejście przez kilka zapór sieciowych jest praktycznie niemożliwe. W sytuacji, kiedy nastąpi złamanie systemu w pierwszej podsieci, system może dowiedzieć się o istnieniu innych systemów w tej podsieci oraz poznać numer portu w routerze wewnętrznym, do którego jest podłączona ta podsieć (192.168.3.3). Ponieważ router zapewnia izolację portów (inna forma izolacji fizycznej), złamany system nie dowie się o istnieniu innych podsieci przy założeniu, że nie nastąpiło złamanie usługi katalogowej.

- ♦ **Brzegowa zapora sieciowa.** Brzegowa zapora sieciowa jest nazywana również graniczną; istnieje w celu utworzenia strefy zdemilitaryzowanej (ang. *Demilitarized Zone*, DMZ). Ogólnie rzecz biorąc, jedyny ruch sieciowy, jaki powinien przechodzić przez brzegową zaporę sieciową, to HTTP na porcie 80, HTTPS na porcie 443 oraz maksymalnie ograniczona liczba innych otwartych portów. Jeżeli w strefie DMZ znajduje się serwer FTP, to powinien być otwarty port 20 (dla danych) i prawdopodobnie 21 (dla poleceń kontrolnych). Otwarte powinny być też inne porty, które są wymagane do obsługi usług udostępnianych w strefie DMZ.
- ♦ **Strefa zdemilitaryzowana (DMZ) w sieci brzegowej.** Strefa DMZ to obszar średniego poziomu zaufania, bardzo często używany przez serwery WWW, dostępne w internecie do przekazywania poczty e-mail, oraz przez serwery FTP. Systemy znajdujące się w strefie DMZ powinny zawierać jedynie publicznie dostępne informacje. Ruch sieciowy przychodzący do strefy DMZ ma względną swobodę działania — może na przykład uruchamiać skrypty w serwerze WWW — ale większość operacji nadal pozostaje zabroniona. Strefa DMZ rozbudowuje interfejs przychodzący brzegowej zapory sieciowej (192.168.2.1) do interfejsu wychodzącego wewnętrznej zapory sieciowej (192.168.2.3). Izolowana strefa DMZ umieszczona w intranecie nazywa się siecią zamaskowaną.

Strefa DMZ to dobre miejsce ograniczenia dostępu dla klientów sieci zewnętrznej, które nie przeszły testów dotyczących kondycji systemu. Jeżeli dostępna jest sieć z serwerem NAP (ang. *Network Access Policy*), to system ten może sprawdzać

**Rysunek 28.3.**

Różne rodzaje zapór sieciowych oraz ich względne umieszczenie



klienty mobilne pod kątem aktualności ich oprogramowania antywirusowego oraz przeprowadzać okresowe skanowanie ich systemów. Serwer Microsoft NAP sprawdza systemy między innymi pod kątem instalowania uaktualnień systemowych. Jeżeli system nie przejdzie procesu weryfikacji, to będzie miał dostęp jedynie do strefy DMZ (lub innej podobnie ograniczonej podsieci), w której znalezione mankamenty systemu będą poprawione, zanim uzyska on dostęp do wewnętrznej sieci LAN.

- ♦ **Wewnętrzna zapora sieciowa (serwer proxy).** Wewnętrzna zapora sieciowa zapewnia inną konwersję adresów sieciowych prowadzącą do różnych podsieci prywatnych. Ruch ze strefy DMZ do sieci wewnętrznej jest poddawany różnym zestawom reguł, mniej restrykcyjnych niż w brzegowej zaporze sieciowej, a następnie przekazywany do routera wewnętrznego. Niektóre zapory sieciowe oferują usługi na poziomie aplikacji. Zapory sieciowe wykonujące wspomniane usługi analizują typy pakietów, a następnie przekazują ruch sieciowy do odpowiedniego serwera aplikacji — zapory sieciowe tego rodzaju odgrywają rolę serwera proxy.
- ♦ **Wewnętrzna sieć LAN (sieć prywatna).** Wewnętrzna sieć LAN składa się z systemów zaufanych i poddawanych najmniejszej liczbie ograniczeń w dowolnej podsieci całego systemu.

Przykład pokazany na rysunku 28.3 jest skomplikowany, aby Czytelnik mógł poznać szeroki zakres miejsc umieszczania zapór sieciowych, a ponadto zawiera więcej komponentów niż typowa sieć SOHO. W najczęściej stosowanej konfiguracji połączenie internetowe dochodzi do routera (na przykład w postaci modemu kablowego lub DSL). Router łączy się z zaporą sieciową, która z kolei łączy się z systemami w sieci bezpośrednio albo za pomocą przełącznika sieciowego. Jeżeli zapora sieciowa ma co najmniej trzy interfejsy, to sieć moż-

na skonfigurować w taki sposób, aby router, sieć LAN i podsieć zamaskowana (DMZ) były osobno podłączone do różnych interfejsów zapory sieciowej. Prawdopodobnie najczęstsza konfiguracja sieci typu SOHO to modem kablowy połączony z internetem; sam modem kablowy pełni funkcję huba, przełącznika sieciowego lub punktu dostępowego i jest pozbawiony funkcji routera i zapory sieciowej.

## Filtry bezstanowe

Klasycznym przykładem bezstanowych zapór sieciowych są te, które używają filtrowania pakietów. Filtrowanie pakietów to funkcja dostępna w niemal każdej zaporze sieciowej; było pierwszą z głównych technologii dołączanych do tego rodzaju produktów. Pakiet podczas filtrowania jest analizowany i jeśli informacje znajdujące się w nim zostaną dopasowane do reguły wyłączenia, to będzie on odrzucony. Informacje, które można pobrać z pakietu, składają się z pól nagłówka zawierających adresy źródłowy i docelowy, użyty protokół, typ danych oraz, w przypadku TCP/UDP, numer portu wykorzystany w celu uzyskania dostępu do sieci bądź w celu filtrowania portu.

Filtrowanie pakietu to technologia zapory sieciowej operująca w warstwie sieci. Ten rodzaj filtrowania jest uznawany za „bezstanowy”, ponieważ w trakcie dopasowywania reguły filtrowania dotyczy samego pakietu bez uwzględniania jego kontekstu. Brak kontekstu podczas dopasowywania zestawu reguł oznacza, że filtry bezstanowe nie mają możliwości ochrony sieci przed ruchem, który próbuje oszukać system, podszywając się za ruch pochodzący z zaakceptowanego źródła, zawierający zaakceptowany typ danych, lub stosując inny rodzaj nadużycia, kiedy tak naprawdę dane są zupełnie czymś innym.

W rzadkich przypadkach zaporę sieciową może być skonfigurowana w taki sposób, aby zwracać potwierdzenie o filtrowaniu pakietu. Na ogół zachowanie anonimowości zapory sieciowej jest uznawane za ważną funkcję bezpieczeństwa.

## Filtry stanu

Filtry stanu analizują połączenie używane przez każdy pakiet i wykorzystują je w celu ustalenia, czy nastąpiło utworzenie nowej sesji oraz czy można zezwolić na wykorzystanie danego połączenia. Filtr określa więc, czy wykorzystywane jest aktualnie używane połączenie, czy nieznane, które trzeba odrzucić. Ten rodzaj filtrowania jest często nazywany filtrowaniem połączenia. Ponieważ dla różnych sesji zaporę sieciową obsługuje tabelę połączeń (tras) w tabeli stanu (lub na liście stanu), ten rodzaj zapory sieciowej stosuje podejście filtrowania „stanu”. Jest ono zaklasyfikowane jako dynamiczna technologia filtrowania pakietów, gdyż bazuje na sesji bądź połączeniu, a zmiany są przeprowadzane na podstawie współdziałania z klientami znajdującymi się na zewnątrz zapory sieciowej.

Do zarządzania połączeniami sieciowymi filtry stanu używają funkcji SPI (ang. *Stateful Packet Inspection*). Przykładem tego rodzaju reguły może być „Zezwól na ruch sieciowy z podsieci 1” lub „Nie zezwalaj na ruch sieciowy z domeny XYZ.com”. Zapory sieciowe obsługujące filtrowanie stanu są technologiami warstwy sieci, podobnie jak bezstanowe filtrowanie pakietów.

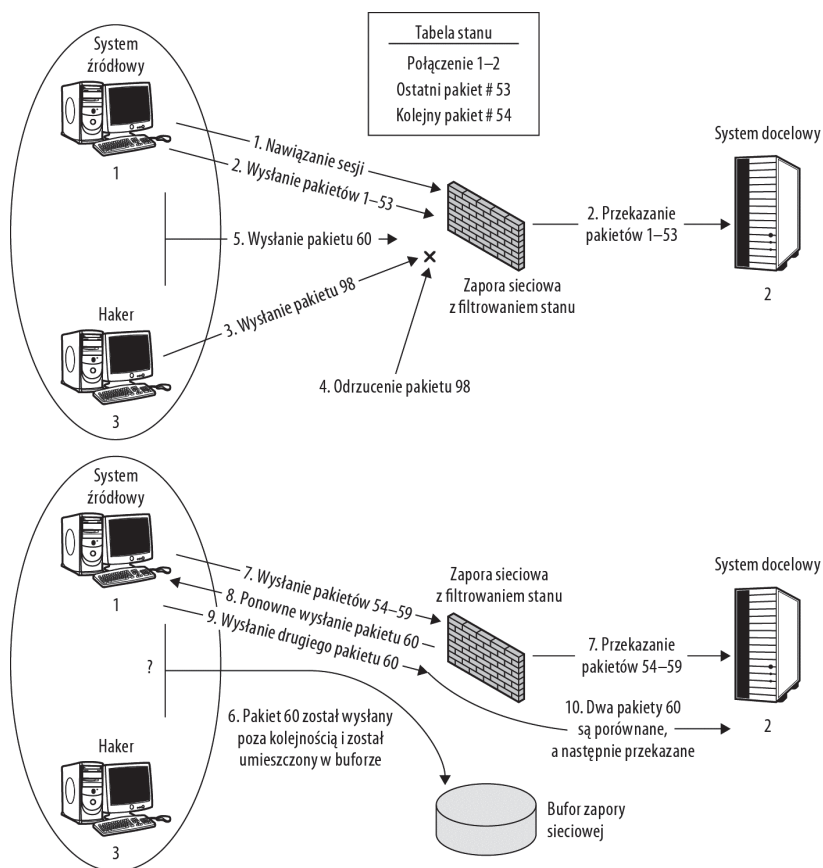
Filtry stanu rozwiązują dość powszechnie spotykany problem bezpieczeństwa związany z używaniem dowolnego portu. Jeżeli aplikacja, na przykład klient FTP, tworzy połączenie do dowolnego portu spoza zakresu doskonale znanych portów, to zaporę sieciową stosującą

filtrowanie bezstanowe nie będzie mogła określić, czy generowany ruch sieciowy jest dozwolony, i pakiet będzie odrzucony. Z kolei zaporę sieciową wykorzystującą filtrowanie stanu będzie miała połączenie FTP zarejestrowane w swojej tabeli połączeń wraz z numerem portu używanego w danej sesji. Kolejne pakiety będą więc przepuszczane do sieci chronionej.

Tabela połączeń zawiera atrybuty każdego połączenia — źródłowy i docelowy adres (adresy) IP, numer portu (numery portów) — kiedy pakiety przechodzą przez system, następuje zarejestrowanie ich numerów sekwencyjnych. Wpis w tabeli połączeń istnieje tylko przez okres trwania sesji i po jej wygaśnięciu zostaje usunięty.

Połączenie stanu wymusza stosowanie reguł bazujących na bieżącym połączeniu. Na rysunku 28.4 pokazano mechanizm służący do obsługi pakietów spoza sekwencji oraz spoza zakresu. Warto przeanalizować prosty przykład filtru stanu, kiedy sesja jest w toku (rysunek 28.4). Ostatni pakiet przechodzący przez zaporę sieciową ma numer 53, a więc kolejny powinien mieć numer 54. Nagłówek IP zawiera informacje pozwalające na określenie wielkości wysyłanych danych. W omawianym przykładzie odpowiada to strumieniowi danych o długości 80 pakietów, przy założeniu, że wielkość pakietów jest stała.

**Rysunek 28.4.**  
Mechanizm używany  
przez filtr stanu  
zapory sieciowej



Pakiet o numerze 54 jest automatycznie przepuszczany przez zaporę sieciową, natomiast pakiet o numerze 60 wymaga podjęcia decyzji. W ścisłej sesji zapory sieciowej pakiet o numerze sekwencyjnym 60 przybyły poza kolejnością może zostać buforowany, choć prawdopodobnie będzie odrzucany aż do chwili, kiedy przez zaporę sieciową przejdą pakiety o numerach od 55. do 59. Stan pakietu 60. pozostaje nieznany, stąd znak zapytania pokazany w sekwencji znajdującej się w lewym dolnym rogu rysunku. W celu zweryfikowania stanu pakietu 60. do systemu nadawcy można wysłać polecenie ACK wraz z prośbą o ponowne dostarczenie pakietu 60. Następnie można przystąpić do porównania nowego pakietu o numerze 60. z otrzymanym wcześniej i sprawdzić, czy są identyczne. Każdy pakiet o numerze wyższym niż 80. będzie automatycznie odrzucony wraz z założeniem o niepoprawności znajdujących się w nim danych. Różne zapory sieciowe oferujące filtrowanie stanu będą stosowały odmienne reguły obsługi pakietów przychodzących poza kolejnością — czyli w sytuacji, kiedy dwie kopie o tym samym numerze sekwencyjnym są dostarczane niemal w tym samym czasie — i powodowanymi przez nie problemami.

Nawiązanie połączenia i rejestracja informacji wiąże się z pewnym obciążeniem. Kiedy protokołem transportowym jest TCP, połączenie wymaga zakończenia powodzeniem negocjacji w tak zwanej formie *three-way handshake*. Gdy system chce nawiązać połączenie, wysyła pakiet z włączonym (ON) bitem SYN. Jeżeli zaporę sieciową przeanalizuje pakiet i uzna go za pochodzący z zaakceptowanego źródła, to odeśle pakiet z powrotem wraz z ustawionymi bitami SYN i ACK. Połączenie zostanie ustanowione (stan ESTABLISHED), gdy system inicjujący połączenie odeśle z powrotem drugi pakiet wraz z ustawionym bitem ACK.

Kiedy połączenie zostanie ustanowione, pakiety należące do nawiązanej sesji będą mogły przechodzić przez zaporę sieciową. Żądanie logowania inicjalizuje sesję — kolejne pakiety z prawidłowymi parametrami sesji będą mogły przechodzić przez zaporę sieciową. Inny klient, który spróbuje zalogować się w tym samym czasie, będzie miał pakiety z polami nagłówka niezawierającymi koniecznych parametrów sesji. Dlatego też te pakiety zostaną zablokowane i odrzucone.

Poleganie na negocjowaniu połączenia oraz proces *three-way handshake* podczas nawiązywania połączenia powodują, że zaporę sieciową stosującą filtrowanie stanu jest podatna na ataki typu odmowa usług (DoS). Atak typu DoS rozpoczyna się, kiedy wiele systemów wysyła ogromną liczbę pakietów żądań połączenia (SYN), co ma nazwę *powódź pakietów SYN*. Ofiara ataku rozpoczyna tworzenie połączeń, doprowadzając do przepełnienia tabeli stanu połączeń, co skutkuje brakiem możliwości tworzenia kolejnych połączeń. Ataki typu DoS bardzo często są przeprowadzane za pomocą sieci zombies, czyli ogromnych sieci komputerów, które zostały zainfekowane przez robaki bądź konie trojańskie.

Po nawiązaniu połączenia TCP rozpoczyna się efektywne przekazywanie danych. Każdy pakiet spełniający parametry połączenia jest przepuszczany po przeprowadzeniu względnie prostej operacji odczytania informacji nagłówka. Zapory sieciowe stosujące filtrowanie stanu zwykle nie przeprowadzają filtrowania ruchu wychodzącego z systemu docelowego w strefie zaufanej do systemu znajdującego się na zewnątrz zapory sieciowej. Przyjmowane jest tutaj założenie, że system chroniony przez zaporę sieciową pozostaje bezpieczny. Nawiązane połączenia istnieją przez ustalony okres bezczynności (brak jakiegokolwiek ruchu sieciowego), po którego upływie następuje zamknięcie połączenia i usunięcie wszelkich informacji o tym połączeniu. Jeżeli aplikacja chce zachować połączenie, może wówczas

wysyłać pakiet `keepalive` lub odpowiadać na żądania zapory sieciowej dotyczące stanu połączenia. Połączenie może być zakończone na żądanie, nie trzeba czekać, aż upłynie ustalony czas bezczynności.



Struktura pakietów IP została omówiona w rozdziale 18., natomiast w rozdziale 17. dokładnie przedstawiono proces nawiązywania połączenia TCP.

Bezstanowy protokół transportowy, na przykład UDP, jest przez zaporę sieciową stosującą filtrowanie stanu obsługiwany inaczej niż stanowy protokół połączenia taki jak TCP. Kiedy pojawia się żądanie UDP pakiety są przepuszczane przez zaporę sieciową. Połączenie jest utrzymywane aż do upływu zdefiniowanego czasu bezczynności, po czym następuje jego zamknięcie. Nie istnieje mechanizm zamknięcia połączenia UDP inny niż upływ czasu bezczynności.

Kiedy zapora sieciowa stosująca filtrowanie stanu nawiąże połączenie, filtrowanie pakietów przychodzących wymaga odczytania pół nagłówka i sprawdzenia ich względem tabeli stanu połączeń. Proces ten nie wiąże się z dużym obciążeniem i jest przeprowadzany efektywnie.

## Filtry aplikacji

Filtry aplikacji filtrującej ruch sieciowy polegają na aplikacji bądź protokołach używanych do tworzenia lub przekazywania pakietu. Filtry aplikacji, które czasami są nazywane filtrowaniem bazującym na proxy, radzą sobie również, kiedy aplikacje wykorzystują inne niż standardowo im przypisane porty. Bazując na swoich ustaleniach, filtr aplikacji może zablokować, przekierować lub zmodyfikować pakiet, kiedy zajdzie taka potrzeba. Filtry aplikacji z reguły znajdują się w znacznie droższych i oferujących więcej funkcji zaporach sieciowych, ponieważ są najbardziej skomplikowanymi i najwolniejszymi używanymi filtrami.

Filtr aplikacji rozszerza koncepcję filtru stanu w celu blokowania ruchu sieciowego na podstawie protokołu używanego przez pakiet, jak również na podstawie sposobu stosowania tego protokołu. W filtrze stanu zapora sieciowa mogła mieć regułę o treści „Zezwól na cały ruch sieciowy przez port 80”. Port 80 to standardowy port dla ruchu sieciowego HTTP. Wiele aplikacji przekazuje swoje dane przez HTTP w celu zapewnienia zgodności z interfejsami bazującymi na przeglądarkach internetowych. Filtr aplikacji może następnie dodać kolejną regułę: „Blokuj ruch sieciowy zawierający dane VoIP”. Ponieważ filtr aplikacji może przeanalizować zawartość pakietu i określić, co jest używane przez aplikację, ma możliwość zastosowania wymienionego filtru, podczas gdy filtry stanu oraz bezstanowe nie mają takiej możliwości. Filtr aplikacji można uznać za rozszerzenie filtru stanu.

Zapora sieciowa aplikacji analizującej ruch sieciowy przekazywany przez protokół HTTP — lub inne powiązane z nim protokoły (na przykład HTTPS, SOAP, XML-RPC) — czy treść dostarczana przez inną dowolną usługę sieciową jest nazywana *Deep Packet Inspection Firewall* (zapora sieciowa z głęboką analizą pakietów). Głęboka analiza pakietów pozwala na identyfikację treści niespełniającej warunków przez porównanie danych znajdujących się w pakiecie z bazą danych sygnatur ataków lub przez określenie, czy zachowanie ruchu sieciowego jest zgodne z normalnym zachowaniem aplikacji.

Filtry aplikacji są szczególnie użyteczne, ponieważ mogą być dynamiczne i inteligentnie reagować na zmieniające się warunki. Warto rozważyć sytuację, kiedy filtr aplikacji monitoruje ruch sieciowy przychodzący do portu numer 53, który jest standardowym portem dla

DNS. Podczas ataku DoS żądania przypisaną DNS powodują przeciążenie systemu i zaporą sieciową w odpowiedzi zamyka port numer 53. Jeżeli zaporą sieciową będzie stosowała filtrowanie stanu, to po prostu zamknie port 53. Jednak filtr aplikacji może wykryć, że system wewnętrzny otrzymuje żądania DNS od systemu zewnętrznego, i dynamicznie otwierać port 53 w celu przepuszczenia tego żądania przez zaporę sieciową. Kiedy filtr aplikacji przepuści żądanie DNS, w tabeli stanu zarejestruje warunki stanu tego żądania. Następnie, gdy dane DNS będą zwrócone z systemu zewnętrznego w odpowiedzi na wewnętrzne żądanie DNS, filtr aplikacji odczyta te dane i bazując na danych sesji, rozpozna je jako prawidłową odpowiedź, otworzy port 53 dla przychodzących danych DNS i przekaże odpowiedź odpowiedniemu systemowi w sieci wewnętrznej. Bardzo łatwo można dostrzec, jak cenna jest ta funkcja. Nawet w trakcie ataku sieć nadal może przeprowadzać rozpoznawanie adresów dla systemów w sieci lokalnej, wymaganych do przeglądania sieci oraz obsługi wielu innych usług.

Filtry aplikacji są zwykle dodawane do zapór sieciowych, które mogą je przetwarzać, kiedy zachodzi taka potrzeba. Użytkownik może rozpocząć od podstawowego zbioru filtrów aplikacji, na przykład od filtru DNS, a następnie dodawać lub kupować kolejne filtry odpowiedzialne za wykrywanie wirusów, sprawdzanie treści, analizę leksykalną lub analizę witryny.



Analiza leksykalna to metoda konwertowania ciągu tekstowego znaków, na przykład kodu źródłowego, na postać sekwencji tokenów. Token jest kategoryzowany jako blok tekstu lub leksem, na przykład słowo kluczowe, identyfikator, literał lub znak przestankowy. Podczas analizy leksykalnej leksemy są kategoryzowane względem funkcji, która dostarcza ich kontekst, czyli znaczenie. Proces kategoryzacji nazywa się tokenizacją. Leksemy są wysyłane do analizatora składniowego, gdzie sekwencja tokenów jest poddawana analizie zgodnie z regułami gramatycznymi danego języka programowania, za którego pomocą zostały utworzone.

Należy pamiętać, że zapory sieciowe na poziomie aplikacji zazwyczaj obsługują analizę zwykłego tekstu, ale nie mają możliwości filtrowania zaszyfrowanego ruchu sieciowego. W przypadku witryny internetowej ze sklepem internetowym używającym szyfrowania SSL polecenia protokołu będą ukryte w zaszyfrowanych danych. Zaporą sieciową z filtrowaniem na poziomie aplikacji w odmienny sposób obsługuje zaszyfrowaną komunikację. Wśród stosowanych podejść można znaleźć usuwanie zaszyfrowanych pakietów w zaporze sieciowej, odszyfrowanie, a następnie ponowne zaszyfrowanie pakietów w zaporze sieciowej przed ich wysłaniem do serwera WWW lub po prostu przekazanie pakietów SSL przez zaporę sieciową do wewnętrznego serwera w celu ich dalszego obsłużenia.

## Domyślnie odmawiaj

Standardową regułą używaną przez każdą technologię zapewniającą wysoki poziom bezpieczeństwa jest inicjalizacja urządzenia wraz ze stanem *domyślnie odmawiaj*. Wiele zapór sieciowych, serwerów proxy oraz innych systemów bezpieczeństwa jest standardowo dostarczanych w postaci całkowicie zamkniętej. Może to wywołać zdziwienie u kogoś, kto wcześniej nie spotkał się z taką sytuacją. W przypadku całkowicie zamkniętego systemu zaleca się, aby administrator włączał jednorazowo po jednej wymaganej usłudze. Typowe jest stosowanie poniższej sekwencji reguł:

- ♦ **Odrzucaj każdy ruch sieciowy, chyba że istnieje odpowiednia reguła, która dopuszcza ten rodzaj ruchu.** To jest właśnie stan *domyślnie odmawiaj*.

- ♦ **Zablokuj wszystkie pakiety przychodzące z adresami sieci wewnętrznej oraz wszystkie pakiety wychodzące z adresami zewnętrznymi.** Wymienione pakiety zwykle pochodzą od atakujących bądź są błędne.
- ♦ **Skonfiguruj ruch sieciowy DNS odpowiednio dla zapytań DNS bazujących zarówno na UDP, jak i TCP.** Bez usługi rozpoznawania adresów większość innych funkcji sieci nie będzie działała.
- ♦ **Należy zezwalać na ruch sieciowy HTTP i prawdopodobnie na HTTPS przez otworenie portu numer 80 oraz odpowiednie przekierowanie tego ruchu.** Jeżeli dla tego ruchu stosowany jest serwer proxy, to trzeba go skonfigurować jako punkt końcowy połączenia. Na przykład serwer Microsoft ISA Server może być serwerem proxy i wymaga, aby ruch sieciowy HTTP był kierowany przez port numer 8080. Standardowy port dla ruchu sieciowego HTTPS to 443, a więc przekierowanie ruchu sieciowego HTTP na port 80 albo 8080 oznacza dla administratorów sieciowych znaczne uproszczenie ruchu wewnętrznego.
- ♦ **Jeżeli używane są serwery poczty, to należy włączyć SMTP i (lub) POP3 przez otworenie ich portów.**
- ♦ **Jeżeli sieć na to pozwala, można otworzyć porty serwera FTP, czyli 20 dla danych i 21 dla poleceń kontrolnych.**
- ♦ **Należy odpowiadać na prośby o pomoc kierowane przez otwieranie poszczególnych portów lub tras po sprawdzeniu tych prób i upewnieniu się, że funkcje sieciowe wymagają tego rodzaju dostępu.**

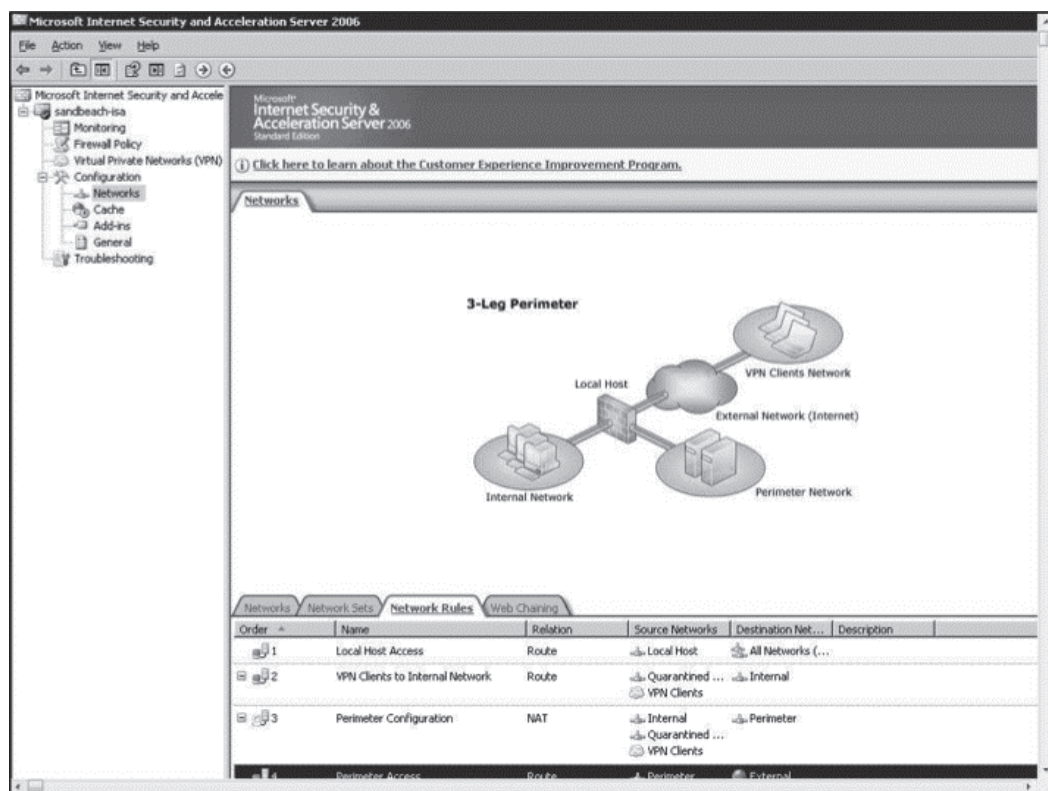
Wymienione reguły są stosowane w kolejności od początku listy. W serwerze Microsoft ISA Server istnieje możliwość użycia różnych konfiguracji zapory sieciowej, a podstawowe zestawy reguł są generowane na bazie wzorca bezpieczeństwa sieci. Na rysunku 28.5 pokazano jedną z takich konfiguracji w ISA Server 2006.

Celem jest utrzymywanie sieci w stanie maksymalnie zamkniętym przy jednoczesnym umożliwieniu działania wszystkim wymaganym usługom i funkcjom. Przy odrobinie szczęścia opracowane reguły będzie można zapisać i wykorzystać w innych urządzeniach tego samego typu.

## Mechanizm NAT

Tłumaczenie adresów sieciowych, czyli NAT (ang. *Network Address Translation*), to podstawowy mechanizm routingu, pozwalający na zastąpienie adresów sieciowych datagramów lub pakietów na podstawie wpisów w tabeli mapowania. Mechanizm NAT jest szczególnie cenny ze względu na możliwość przekierowywania ruchu sieciowego do adresów sieci prywatnej, które bez wykorzystania tego mechanizmu nie podlegają routingowi w sieci publicznej. Ogólnie rzecz biorąc, mechanizm NAT rozszerza pojedynczy przypisany statycznie adres IP na sieć adresów. Bez mechanizmu NAT protokół IPv4 już dawno temu wyczerpałby dostępną pulę adresów IP.

Kiedy urządzenie stosuje mechanizm NAT względem pakietu przychodzącego, to zmienia adres docelowy w nagłówku danego pakietu. Cały zakres urządzeń w sieci prywatnej jest ukryty przed siecią zewnętrzną; ujawniony jest tylko pojedynczy adres interfejsu sieci zewnętrznej



**Rysunek 28.5.** Reguły zapory sieciowej serwera Microsoft ISA Server po skonfigurowaniu zapory sieciowej jako Three-Leg Perimeter

urządzenia zapewniającego routing. Mechanizm NAT to ogólna funkcja pozwalająca na mapowanie dowolnego adresu na inny. Niekoniecznie musi to być zakres prywatnych adresów IP. Pakiety wychodzące są przedmiotem mapowania odwrotnego. Mechanizm NAT zmienia adres źródłowy pakietów (czyli prywatnych adresów IP) na adresy IP interfejsu sieci zewnętrznej routera, które pozwalają na routing.

Mechanizm NAT w postaci oprogramowania można znaleźć między innymi w:

- ♦ Internetwork Operating System (IOS) firmy Cisco;
- ♦ Microsoft Windows Internet Connection Sharing (ICS);
- ♦ IPFilter (<http://coombs.anu.edu.au/~avalon>) — pakiet typu open source dostępny w wielu implementacjach systemu Unix, na przykład FreeBSD, NetBSD i Solaris 10;
- ♦ Packet Filter (PF) — filtr NAT znajdujący się w OpenBSD, dostępny też w wielu innych systemach operacyjnych;
- ♦ Netfilter — znany również jako iptables, dołączony do niektórych dystrybucji systemu Linux;
- ♦ WinGate (<http://www.wingate.com>) — system zintegrowanego zarządzania bramą dla Windows;

- ♦ Microsoft Internet Security and Acceleration Server — serwer proxy i buforowania możliwy do zainstalowania w systemie Windows Server 2003 lub 2008.

Podczas konfigurowania mechanizmu NAT istnieje możliwość trwałego przypisania mapowania w tabeli mapowania, co prowadzi do utworzenia tak zwanego statycznego mechanizmu NAT. Podstawowa forma mechanizmu podczas przejścia przez NAT powoduje zmianę adresu docelowego pakietów przychodzących oraz adresu źródłowego pakietów wychodzących. Bardziej zaawansowane formy mechanizmu NAT powodują zmianę adresu IP, jak również przypisania portu źródłowego i docelowego, co jest wymagane do przekierowywania portów dla kierowanego ruchu sieciowego. Taka forma mechanizmu NAT ma nazwę tłumaczenia adresów portów (ang. *Port Address Translation* — PAT), tłumaczenia adresów portów sieciowych (ang. *Network Address Port Translation* — NAPT) lub przeciążonego NAT (Cisco). Wszystkie formy mechanizmu NAT wymagają podczas każdego przejścia przez NAT ponownego obliczenia sumy kontrolnej CRC (ang. *Checksum*) i umieszczenia jej w nagłówkach pakietów.

Efekt przejścia przez NAT jest nieskomplikowany. Sposób działania mechanizmu NAT wewnątrz urządzenia obsługującego routing jest już trudniejszy do wyjaśnienia. Istnieje kilka metod mapowania adresów. Spójrzmy na kilka powszechnie stosowanych schematów mapowania, które zostały zdefiniowane jako część pierwotnego protokołu STUN. Poniżej opiszemy cztery schematy mapowania NAT — „jeden do jednego”, czyli *Full Cone NAT*, *Address Restricted Cone NAT*, *Port Restricted Cone NAT* oraz *Symmetric NAT*.

- ♦ *Full Cone NAT*. Wszystkie odwołania z tego samego adresu IP i portu wewnętrznego są mapowane do tego samego zewnętrznego adresu IP i portu. Ponadto wszystkie zewnętrzne systemy mogą wysyłać pakiety do systemów wewnętrznych, korzystając ze zmapowanego adresu zewnętrznego.
- ♦ *Address Restricted Cone NAT*. Wszystkie odwołania z tego samego adresu IP i portu wewnętrznego są mapowane do tego samego zewnętrznego adresu IP i portu. Zewnętrzny system może wysyłać pakiety do systemu wewnętrznego tylko wtedy, gdy wcześniej system wewnętrzny wysłał pakiet do tego systemu zewnętrznego. W tym wypadku numer portu nie ma znaczenia.
- ♦ *Port Restricted Cone NAT*. Mapowanie adresów wewnętrznych do zewnętrznych jak w dwóch poprzednich schematach mapowań. W tym schemacie transmisja z systemu zewnętrznego z adresu źródłowego X i portu Y będzie dozwolona, jeśli źródłowy system docelowy wysłał pakiet na adres X i port Y.
- ♦ *Symmetric NAT*. Wszystkie odwołania z tego samego wewnętrznego adresu IP i portu są mapowane do specyficznego zewnętrznego adresu IP i portu. Jeśli ten sam system źródłowy wysłał pakiet z tym samym źródłowym adresem IP i portem, ale do innego systemu zewnętrznego, mapowanie jest inne. Zewnętrzny system może odwoływać się do systemu wewnętrznego tylko wtedy, gdy wcześniej system wewnętrzny wysłał pakiet na adres tego systemu zewnętrznego.

W swoich urządzeniach wielu producentów wybiera połączenie różnych aspektów mapowania. Na przykład powszechnie stosowana implementacja łączy w sobie mapowanie z wykorzystaniem schematu *Symmetric NAT* wraz ze statycznym mapowaniem portu w zależności od kierunku, z którego pochodzi ruch sieciowy, oraz miejsca jego przeznaczenia.

W celu obsługi pakietów kontrolnych IP takich jak ICMP muszą być stosowane dodatkowe techniki NAT, podobnie jak w przypadkach, gdy mechanizm NAT nie może prawidłowo przetworzyć danych TCP lub UDP. W takich sytuacjach mechanizm NAT musi ponownie utworzyć nagłówki TCP/UDP oraz obliczyć sumę kontrolną CRC. Mechanizm NAT często ma problemy z przetwarzaniem szyfrowania; IPsec to jeden z przykładów tego rodzaju problemu. Brak standardowych technik do współpracy z protokołami transportowymi jest głównym powodem, dla którego programiści IPv6 wolą pozostawać z dala od mechanizmu NAT.

Można spotkać się również z implementacjami NAT charakterystycznymi dla danego producenta. *Destination NAT* (DNAT) to technika, w której adres docelowy pakietu jest zmieniany na inny, a gdy system docelowy udzieli odpowiedzi, adres źródłowy w tym pakiecie zostanie ponownie zamieniony. Technika ta często jest nazywana *port forwarding*. DNAT pozwala usługom wewnętrznym na ich udostępnienie pod publicznym adresem IP, nawet jeśli dane pochodzą z sieci prywatnej. W przypadku *Source NAT* (SNAT) zmieniany jest adres źródłowy pakietu — stosowane w przypadku komunikacji sieci z adresacją prywatną z siecią internet.

Termin SNAT zazwyczaj odnosi się do pojęcia *Source NAT*, ale nie zawsze. Niektórzy ogromni producenci używają tego pojęcia zupełnie inaczej. Akronim SNAT jest wykorzystywany przez firmę Microsoft jako nazwa usługi jej serwera *Internet Security and Acceleration* (ISA) i oznacza *Secure NAT*. Dla firmy Cisco SNAT oznacza *Stateful NAT*. Z kolei organizacja IETF uznaje SNAT za *Software Network Address Translation*. Technologia ta oznacza tłumaczenie adresów sieciowych, co jest wymagane do połączenia ze sobą sieci IPv6 i IPv4.

Wobec tak wielu znaczeń pojęcia SNAT nie można się dziwić, że początkowa nazwa protokołu STUN — *Simple Traversal of User Datagram Protocol through Network Address Translators* — musiała zostać zmieniona na *Session Traversal Utilities for NAT* i wcale nie jest prosta.

Mechanizm NAT nie jest procesem transparentnym i istnieje wiele różnych typów protokołów i aplikacji, które ulegają awarii podczas próby wysyłania danych przez mechanizm NAT. Największe problemy pojawiają się w aplikacjach polegających na różnych strumieniach danych, które próbują wysłać dane, oraz w trakcie sesji kontrolnych — FTP i SIP to najbardziej znane przykłady. SIP to protokół kontrolny dla technologii *Voice over IP*. To jest powód, dla którego opracowano technologie takie jak STUN i ICE (ang. *Internet Connectivity Establishment*), pomagające w przechodzeniu przez NAT. Inne potencjalne rozwiązania problemów przejścia przez NAT to użycie technologii automatycznego wykrywania urządzeń, na przykład *Universal Plug and Play* (UPnP) oraz Bonjour (NAT-PMP), kiedy są udostępniane przez mechanizm NAT. Technologia Bonjour łączy NAT z protokołem mapowania portów.

## Serwery proxy

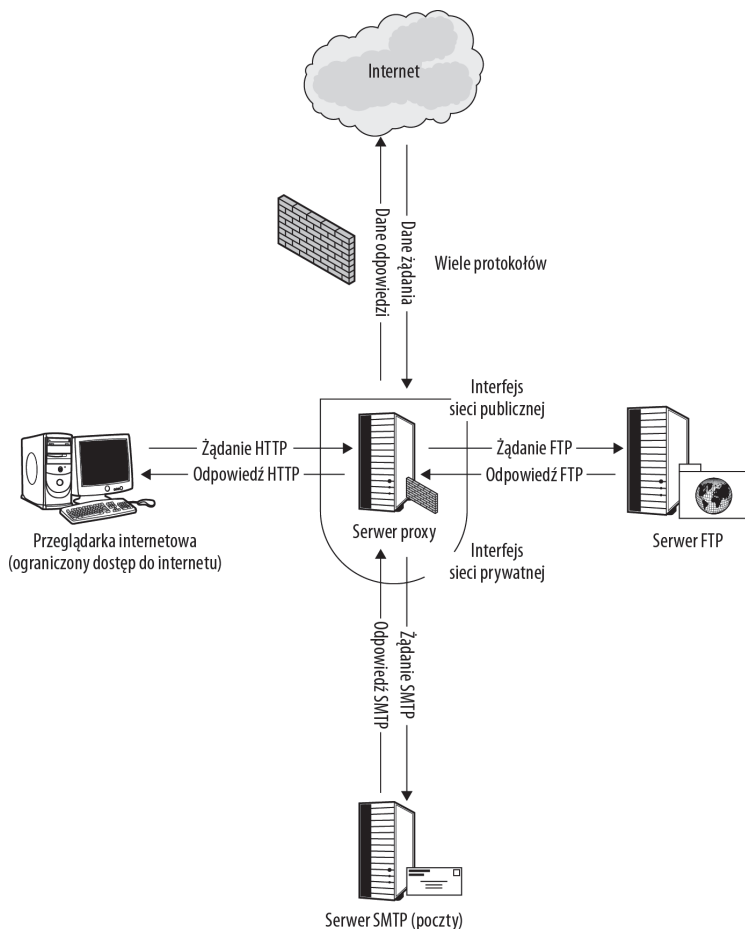
Serwer proxy to komputer bądź aplikacja działająca w charakterze pośrednika między klientem i usługą sieciową. Żądania klienta otrzymane w serwerze proxy są przekazywane do usługi, a wynik wraca do serwera proxy, który z kolei przekazuje ten wynik klientowi. Usługa proxy wykonuje funkcję przekierowania, nie przeprowadza żadnego przetwarzania

żądań i jest jedynym systemem widzianym przez klienta lub usługę w trakcie danej transakcji. W takiej postaci serwer proxy może być nazwany bramą lub znacznie rzadziej proxy tunelującym.

Ponieważ z marketingowego punktu widzenia pojęcie *brama* wydaje się bardziej pociągające niż *serwer proxy*, rzadko można spotkać się z serwerem proxy, który przekazuje wszystkie żądania i odpowiedzi w postaci nietkniętej. Serwery proxy zwykle wykonują dodatkowe zadania z nimi powiązane. W opinii autora serwer proxy stanowi hybrydę zapory sieciowej i bramy. Za pomocą protokołu HTTP serwer proxy może komunikować się z serwerem WWW lub przeglądarką internetową klienta; używając protokołu SMTP, może komunikować się z serwerem poczty, natomiast za pomocą protokołu FTP z serwerem FTP. Warto w tym miejscu dodać, że aplikacje znajdujące się za serwerem proxy nie muszą rozumieć protokołów innych niż te, które zostały zaprojektowane do pracy z nimi. Serwery proxy są implementowane sprzętowo albo w postaci oprogramowania. Mogą więc być samodzielnymi fizycznymi serwerami lub po prostu oprogramowaniem (usługa proxy) uruchomionym na tym samym komputerze co aplikacja, dla której proxy zostało przeznaczone. Na rysunku 28.6 pokazano podstawowe elementy usługi proxy jako wysokiego poziomu translatora protokołu oraz jako substytutu dostępu do internetu dla klientów.

### Rysunek 28.6.

Funkcja podstawowa  
serwera proxy  
— skrzyżowanie  
zapory sieciowej  
i bramy



Poniżej wymieniono niektóre z najlepiej znanych serwerów proxy:

- ♦ Apache HTTP Server (<http://httpd.apache.org>)
- ♦ Blue Coat SGOS (<http://www.bluecoat.com>)
- ♦ I2P (<http://www.i2p2.de>)
- ♦ Microsoft ISA Server (<http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/default.aspx>)
- ♦ Novell BorderManager (<http://www.novell.com/products/bordermanager>)
- ♦ Privoxy (<http://www.privoxy.org>)
- ♦ Squid (<http://www.squid-cache.org>)
- ♦ Oracle iPlanet Web Proxy Server (<http://www.oracle.com/technetwork/middleware/index-090943.html?ssSourceSiteId=ocomen>)
- ♦ Tinyproxy (<http://www.banu.com/tinyproxy>)
- ♦ Tor (<http://www.torproject.org>); szczegółowo omówiony w rozdziale 9.
- ♦ Varnish (<http://www.varnish-cache.org/>)
- ♦ WinGate (<http://www.wingate.com>)
- ♦ yProxy (<http://www.yproxy.com>)
- ♦ Zeus Web Server (<http://www.zeus.com>)
- ♦ Ziproxy (<http://ziproxy.sourceforge.net>)

Serwery proxy oferują wiele funkcji zapory sieciowej. Niektóre potrafią filtrować ruch sieciowy na podstawie treści, domen, adresów URL, typów MIME, słów kluczowych oraz na podstawie wzorców adresów URL i atrybutów treści. Z kolei do przepuszczania ruchu sieciowego używają białych list, natomiast do zatrzymania — czarnych list. Serwery proxy nie są efektywne podczas analizy zaszyfrowanego ruchu sieciowego i będą przepuszczały ten ruch sieciowy bez możliwości stosowania filtrowania względem niego.

Ponieważ wiele działań podejmowanych przez serwery proxy to ważne zdarzenia i w pewnym momencie może wystąpić potrzeba ich analizy, niemal każdy serwer proxy rejestruje w pliku dziennika zdarzeń informacje o podejmowanych decyzjach. Wspomniany plik prawie zawsze jest standardową bazą danych lub formatem arkusza kalkulacyjnego, takim jak CSV. Jeden z ważnych zestawów filtrów bezpieczeństwa, który serwer proxy powinien móc stosować, to uzyskanie dostępu do usług proxy na podstawie danych uwierzytelniających użytkownika; może to wymagać od użytkownika zalogowania.

Powszechnie stosowanym usprawnieniem jest dodanie do serwera proxy bufora (wiąże się to z wyposażeniem serwera w dowolny typ urządzenia pamięci masowej) oraz logiki, niezbędnej, aby serwer wiedział, kiedy żądanie zostało już obsłużone. W takim przypadku bufor proxy zwróci dopasowany wynik prosto z bufora, zamiast przekazywać żądanie usłudze. Buforowanie zawsze jest funkcją powiązaną z serwerem proxy obsługującym ruch internetowy; w takich wypadkach proxy może być nazywane *web proxy*. Niemal wszystkie serwery web proxy ukrywają prawdziwą tożsamość użytkownika łączącego się z jednej sieci do drugiej (najczęściej z internetem) i jako takie mogą być uznawane za proxy otwarte lub serwer anonimizujący (ang. *anonymous proxy*).

Istnieje wiele sytuacji, w których usługi sieciowe nie chcą przekazywać ruchu sieciowego z otwartego serwera proxy. Dotyczy to na przykład ruchu sieciowego związanego z pocztą e-mail oraz IRC. Niektóre systemy sprawdzają dostępność otwartego proxy, podczas gdy inne sprawdzają znane listy otwartych systemów proxy i odmawiają przekazywania ich danych przez swój system.

## Przezroczyste serwery proxy i przynęty

Ponieważ serwer proxy może ukrywać tożsamość użytkowników jednej sieci w innej, to możliwe jest wykorzystywanie serwerów proxy do analizy ruchu sieciowego między dwoma punktami końcowymi, co może być przeprowadzane z różnych powodów. Kiedy motywacją jest nikczemna, proxy jest określane mianem wrogiego proxy. Gdy celem jest przechwycenie ruchu sieciowego i zastosowanie względem niego zdefiniowanej polityki, proxy może być nazywane proxy przechwytyjącym. Proxy przechwytyjące pełni funkcję bramy i może być przezroczyste dla użytkownika. Firma Cisco stosuje pojęcie *proxy transparentne* w celu zdefiniowania protokołu *Web Cache Control Protocol* używanego do określenia tras dla ruchu wychodzącego na podstawie zawartości bufora — to inna forma przekierowania.

Inne użycie serwerów proxy to utworzenie pułapek bezpieczeństwa nazywanych *przynętami*. Tego rodzaju pułapka służy jako przynęta dla nieuwierzytelnionych użytkowników danego systemu — przejmując ich ruch sieciowy i pozwala na monitorowanie ich działań w celu ujawnienia ich tożsamości. Pułapki te są systemami otwartymi i czasami noszą nazwę *sugarcane*. Przynęta nie powinna zawierać żadnych cennych danych ani być systemem produkcyjnym. Ponieważ istotą przynęty jest zezwolenie intruzowi na dostanie się do środka systemu, to jest bardzo ważne, aby przynęta została dokładnie odizolowana od innych cennych systemów. W celu tworzenia pozornie ważnych informacji czasami są używane programy określane gospodarzami-ofiarami. Programy te są wabikami, których zadaniem jest przyciągnięcie uwagi intruza. Mogą być również skonstruowane w taki sposób, aby dostarczyć dokładnych informacji na temat natury danego ataku.

## Serwery odwrotnego proxy

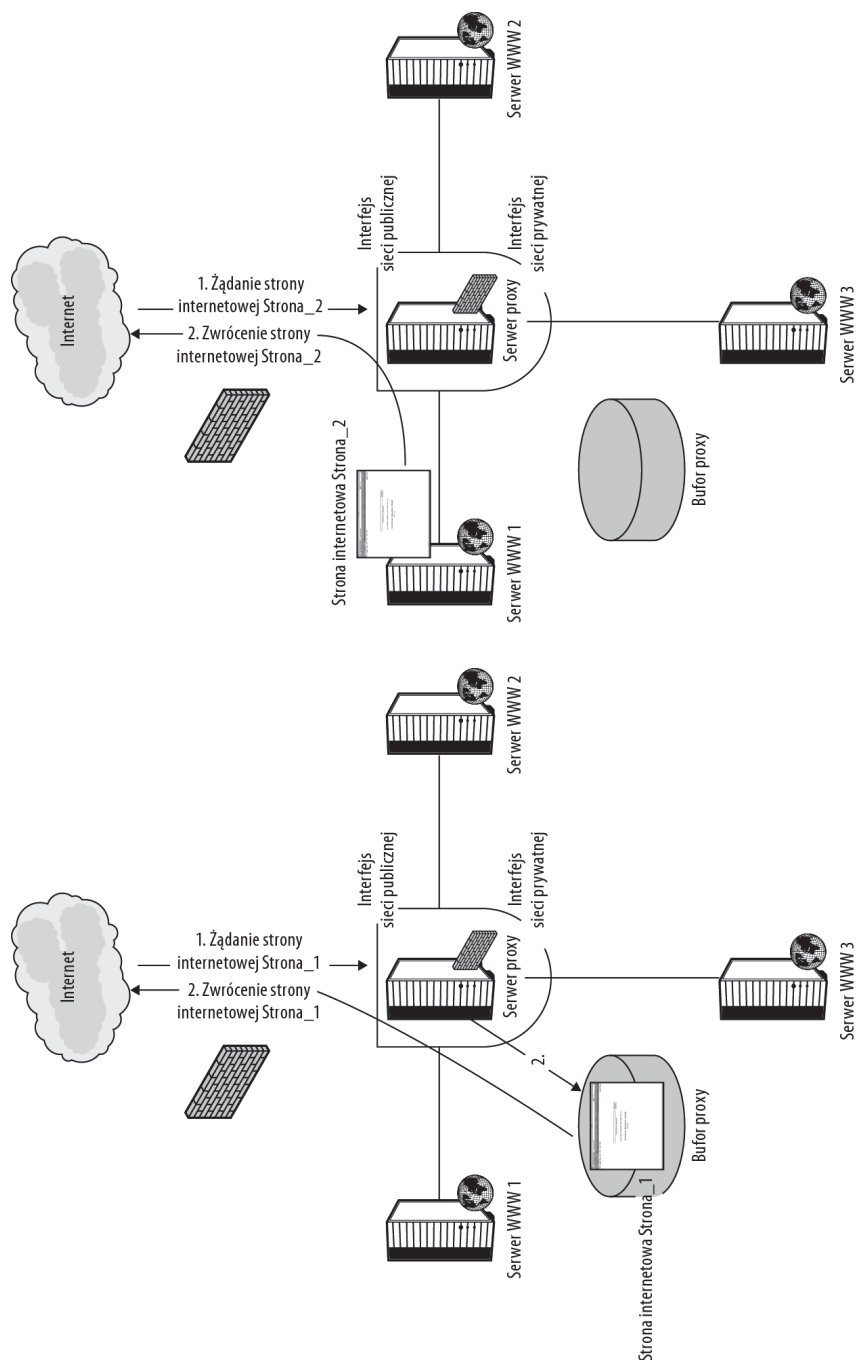
Istnieją pewne formy serwera proxy nazywane odwrotnym proxy, kiedy to usługa przekazuje dane bezpośrednio do serwera proxy. Najczęściej spotykany przykład odwrotnego proxy to sytuacja, kiedy serwer WWW wysyła dane do lokalnego serwera proxy w celu ich dalszego przetworzenia.

Serwer odwrotnego proxy może przeprowadzać operację szyfrowania i deszyfrowania SSL (ang. *Secure Socket Layer*) dla serwera WWW, używając do tego akceleratora SSL lub modułu odciążającego. Przeprowadzając tę operację dla wielu serwerów WWW, serwer odwrotnego proxy może pozwolić, aby serwery WWW korzystały z tego samego certyfikatu serwera SSL, który jest używany przez serwer odwrotnego proxy. Inną zaletą serwera odwrotnego proxy może być szybsza kompresja oraz możliwość opublikowania usługi w innej sieci, co ma nazwę *Extranet Publishing*. Buforowanie treści to niemal zawsze funkcja serwera odwrotnego proxy.

Na rysunku 28.7 pokazano sposób implementacji serwera odwrotnego proxy internetowego

**Rysunek 28.7.**

Odwrotne proxy  
wydaje się być  
serwerem WWW



Po lewej stronie rysunku 28.7 widać, że żądanie jest wykonywane przez klienta z zewnątrz sieci i dotyczy strony statycznej *Strona\_1* z serwera WWW. Żądanie dochodzi do serwera proxy. W pierwszej kolejności serwer proxy, wiedząc, że to jest strona statyczna, przeprowadza sprawdzenie bufora, znajduje wskazaną stronę i przekazuje ją z bufora do

klienta. W tym przypadku serwer proxy spełnił funkcję serwera WWW. W drugim przypadku klient żąda strony *Strona\_2*. Po sprawdzeniu bufora i nieznalezieniu w nim strony, ponieważ strony dynamiczne nigdy nie powinny być buforowane, serwer odwrotnego proxy przekazuje żądanie do jednego lub więcej serwerów WWW w celu dostarczenia strony *Strona\_2*. Serwer WWW znajduje stronę (treść statyczna) albo tworzy stronę (treść dynamiczna), a następnie wysyła ją serwerowi proxy, który z kolei przekazuje ją dalej klientowi. Z punktu widzenia klienta serwer proxy ponownie jest serwerem WWW. Serwer odwrotnego proxy odegrał więc rolę aplikacji lub usługi, dla której stanowi front.

Zaletą takiego podejścia polega na tym, że buforowanie powoduje zwiększenie wydajności, a serwer proxy może równoważyć obciążenie między trzema serwerami WWW. Kiedy jeden serwer WWW potrzebuje treści z innego, to serwer proxy może ją dostarczyć. W wyniku tego działalność serwera proxy powoduje, że serwery WWW są znacznie wydajniejsze.

## Podsumowanie

Zapora sieciowa oferuje zaawansowaną ochronę przed wieloma niebezpieczeństwami sieciowymi. Zwiększa poziom bezpieczeństwa sieci i utrudnia użytkownikom z zewnątrz uzyskanie nieuprawnionego dostępu do sieci prywatnej. Zapora sieciowa stosuje filtry w celu obsługi przychodzącego i wychodzącego ruchu sieciowego. Zaawansowana zapora sieciowa może korzystać z funkcji głębokiej analizy pakietu, aby dokładnie zinterpretować jego treść. Zapory sieciowe są umieszczane w różnych miejscach sieci i służą do różnych celów.

Mechanizm tłumaczenia adresów sieciowych (ang. *Network Address Translation* — NAT) pobiera żądanie od klienta sieci publicznej i przekazuje je do systemów znajdujących się w sieci prywatnej. Funkcja ta pozwala systemom sieci prywatnej na zachowanie anonimowości.

Bramy są systemami odgrywającymi rolę interfejsu między dwiema sieciami. Serwer proxy to z kolei hybryda bramy i zapory sieciowej. Serwer proxy może służyć jako rodzaj substytutu internetu dla systemów znajdujących się w sieci prywatnej.

W kolejnym rozdziale zostaną omówione wirtualne sieci prywatne, które pozwalają na tworzenie bezpiecznych kanałów komunikacji między komputerami niezależnie od tego, gdzie te komputery się znajdują.

# Rozdział 29.

## Sieci VPN

### **W tym rozdziale:**

- ♦ Charakterystyka sieci VPN
- ♦ Topologie sieci VPN
- ♦ Urządzenia i narzędzia dla sieci VPN
- ♦ Protokoły w sieciach VPN

Wirtualne sieci prywatne VPN (ang. *Virtual Private Network*) są podstawą bezpiecznych łączy sieciowych i bezpiecznych połączeń pomiędzy sieciami. Tworząc sieć VPN, zwykle wykorzystuje się publiczne łącze internetowe, zazwyczaj za pośrednictwem sieci jednego z dostępnych operatorów.

Sieci VPN są tworzone z wykorzystaniem protokołów znajdujących się w warstwie łącza danych i warstwie sieci — poziomy 2. i 3. modelu OSI. Niektóre z tych protokołów są stosowane do zabezpieczenia przesyłanych danych, zazwyczaj przez odpowiedni proces szyfrowania. Inne protokoły są odpowiedzialne za przygotowanie danych i zapewnienie niezbędnych mechanizmów wsparcia połączenia VPN. Jeszcze inne protokoły są używane do transportu danych w sieci VPN.

Po zaszyfrowaniu blok danych jest umieszczany w odpowiedniej strukturze, a następnie jest przesyłany za pomocą łącza VPN. Jeśli w rozwiązaniu zastosujemy szyfrowanie całych pakietów, wraz z nagłówkami, będziemy korzystać z tunelowania VPN. Tunelowanie VPN jest najczęściej stosowane w celu połączenia odległych od siebie sieci intranet (np. dwóch lokalizacji firmy) lub w celu udostępnienia zasobów intranetu zdalnie.

Rozwiązania VPN są realizowane z wykorzystaniem określonego sprzętu i oprogramowania. Sieci VPN wymagają zapewnienia funkcji routingu do nawiązania połączenia oraz oprogramowania niezbędnego do translacji i przygotowania danych do transmisji. W rozwiązaniach VPN stosuje się różne urządzenia — routery, bramki, koncentratory i serwery dostępu do sieci.

Na rynku istnieje wiele różnych wersji oprogramowania dla VPN, takich jak OpenVPN, LogMeIn Hamachi i TINC, które zostaną opisane w niniejszym rozdziale. Przedstawiono tu również procedury tworzenia łącza VPN w systemach Vista i Windows Server 2008.

Rozdział zawiera też informacje na temat tunelowania i protokołów szyfrowania, a także enkapsulacji danych. Szyfrowanie w sieciach IP często jest realizowane z wykorzystaniem zestawu protokołów IPsec. Powszechnym protokołem enkapsulacji danych jest Generic Routing Encapsulation. Zdalny dostęp do zasobów intranetowych zapewnimy za pomocą jednego z protokołów połączeń typu punkt-punkt — PPTP lub L2TP.

## Technologie VPN

W świecie zawładniętym siecią trzeba zapewnić bezpieczeństwo komunikacji. Sieci lokalne (LAN) są zabezpieczone za pomocą różnych systemów, na przykład protokołu CHAP (ang. *Challenge Handshake Authentication System*). Zastosowanie tego protokołu w sieci współdzielonej lub przy użyciu sieci rozległej WAN nie zapewnia wymaganego stopnia bezpieczeństwa. Wprowadzenie użytkowników zdalnych do sieci powoduje nowe problemy, które trzeba rozwiązać, a koszt utrzymania linii dzierżawionych dla łączy WAN jest zbyt duży.

Rozwiązaniem jest wykorzystanie wirtualnych sieci prywatnych VPN do tworzenia bezpiecznych połączeń, zdefiniowanych za pomocą obwodów wirtualnych. VPN jest siecią łączącą węzły poprzez łącza publiczne za pomocą technik tunelowania i protokołów bezpieczeństwa.

## Rodzaje VPN

Pierwsze sieci VPN były zestawiane na dzierżawionych łączach linii telefonicznych, później — za pośrednictwem sieci publicznych. Na początku łącza tworzone z wykorzystaniem prywatnych linii dzierżawionych, dzięki czemu zapewniano wymagany poziom zabezpieczeń. Ten rodzaj VPN jest określany mianem zaufanego VPN. Ponieważ w tej formie transmisja może odbywać się przez wiele urządzeń pośrednich, bezpieczeństwo klientów sieci VPN było uzależnione od dostawcy usług.

W systemach zaufanego VPN wykorzystuje się następujące technologie (warstwa 2. i 3. modelu OSI):

- ♦ Łącza wirtualne ATM, warstwa 2.
- ♦ Łącza wirtualne Frame Relay, warstwa 2.
- ♦ Transport ramek warstwy 2. przez MPLS, warstwa 2.
- ♦ Protokół Draft-Martini. Ta technologia wykorzystuje ATM, Frame Relay, Ethernet, Ethernet VLAN, PPP, HDLC lub dowolny inny protokół transportowy dla połączeń typu punkt-punkt poprzez MPLS. Protokół Draft-Martini jest czasami nazywany AToM (ang. *Any Transport over MPLS* — dowolny protokół transportowy poprzez MPLS). Protokół Draft-Martini działa w warstwie 2.
- ♦ Routing MPLS kontrolowany przez protokół BGP (warstwa 3.), używany w internecie.

Zapewnienie bezpieczeństwa w sieci internet jest nie lada wyzwaniem. W technologii zaufanego VPN, zastosowanej w internecie, nie można liczyć na ochronę danych, bo w trakcie transmisji pakietów poprzez urządzenia sieciowe może dojść do ich przechwycenia lub podsłuchu. Aby zabezpieczyć taką transmisję VPN, użyto odpowiedniego szyfrowania w łączu internetowym. Ta odmiana VPN nosi nazwę *bezpiecznego VPN* (ang. *Secure VPN*).

W bezpiecznym VPN wykorzystuje się następujące protokoły:

- ♦ **Szyfrowanie IPsec (tunel lub protokół transportowy).**
- ♦ **L2TP over IPsec (dostęp zdalny, oparty na modelu klient-serwer).**
- ♦ **SSL w wersji 3.0 albo TLS.**

IPsec, L2TP i TLS są standardami IETF<sup>1</sup>. Protokół SSL jest wcześniejszą wersją protokołu TLS. Wymienione protokoły znajdują się w warstwie transportowej (warstwa 4. modelu ISO); ich zadaniem jest tworzenie zaszyfrowanych bloków danych i przekazywanie ich warstwom niższym.

Trzecia kategoria VPN łączy aspekty dwóch pierwszych i nazywa się *hybrydowym VPN*. W tym rozwiązaniu internet jest traktowany jako sieć rozległa, w której trzeba zastosować bezpieczny VPN. Pozostałe segmenty sieci po obu stronach mogą nie być zabezpieczone, ale można tam przynajmniej skonfigurować zaufany VPN. Dostawcy oferujący hybrydowe rozwiązania dostarczają wraz z nimi konsolę zarządzania, dzięki której można tworzyć i modyfikować VPN, zapewniając wymaganą, gwarantowaną jakość usług (QoS) rozwiązania. Hybrydowe sieci VPN mogą być tworzone na wszelkiego rodzaju bezpiecznych połączeniach VPN, które mogą przenosić ruch zaufanego VPN.

## Łączy VPN

Obecnie są cztery rodzaje łączy VPN:

- ♦ **Wewnętrzne łącze sieci LAN.** Jest to połączenie dwóch komputerów w ramach sieci LAN.
- ♦ **Intranetowe łącza WAN.** Są to łącza pomiędzy sieciami LAN realizowane poprzez jedną sieć.
- ♦ **Ekstranetowe łącza WAN.** Są to łącza pomiędzy sieciami LAN zestawiane poprzez różne sieci zewnętrzne, z reguły pomiędzy lokacjami danej firmy.
- ♦ **Łącze zdalnego dostępu.** Jest to łącze tymczasowe w WAN, zestawiane od zdalnego użytkownika lub systemu. Takie łącza nie są współdzielone.

Łącza VPN mogą być tworzone za pośrednictwem połączeń dial-up, dostępu szerokopasmowego do sieci, a nawet na bazie łączy bezprzewodowych. Ogólnie rzecz biorąc, można tworzyć łącza pomiędzy lokacjami albo na zasadzie zdalnego dostępu. Technologie, w których blok danych jest szyfrowany bez nagłówka, są nazywane *metodami transportowymi*. Jeśli szyfrowaniu ulega zarówno część nagłówkowa, jak i blok danych pakietu, są nazywane metodami *tunelowymi VPN*.

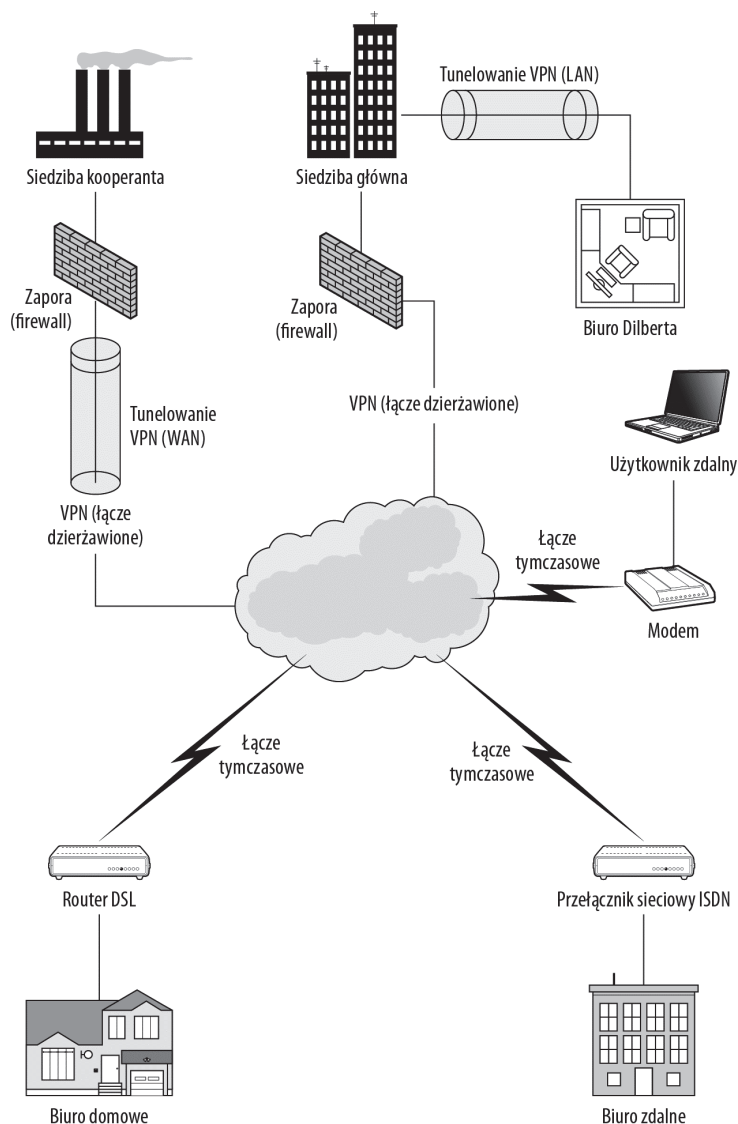
---

<sup>1</sup> IETF (ang. *Internet Engineering Task Force*) — międzynarodowe stowarzyszenie zajmujące się standardami technicznymi i organizacyjnymi w internecie — *przyj. tłum.*

Rysunek 29.1 przedstawia koncepcję VPN przez różne rodzaje łącz WAN, takie jak łącza dzierżawione, standardowej sieci LAN lub łącza Wi-Fi. Routery, przełączniki i inne urządzenia niezbędne do uruchomienia VPN nie są pokazane na tym rysunku (nie są one rzeczywistymi węzłami końcowymi VPN). Sieć VPN może być konfigurowana i zarządzana przez klienta, jak pokazano na przykładzie tunelu pomiędzy Dilbertem i jego biurem w domu, albo przez dostawcę usług linii dzierżawionych lub dostępu do internetu.

### Rysunek 29.1.

Rodzaje sieci VPN



Rozwiązania VPN oferowane przez dostawców usług można sklasyfikować następująco:

- ♦ IPsec VPN
- ♦ VPLS (ang. *Virtual Private LAN Service*)

- ♦ VPWS (ang. *Virtual Private Wire Service*)
- ♦ IPL (ang. *IP Private LAN Service*)
- ♦ VR (ang. *Virtual Router*)
- ♦ BGP/MPLS

Klient VPN realizuje zazwyczaj jedną z następujących czynności:

- ♦ IPsec VPN
- ♦ VPN GRE

## Topologie połączeń między lokacjami

VPN może być realizowany sprzętowo lub z wykorzystaniem odpowiedniego oprogramowania, najczęściej za pomocą kombinacji obu technik. Wysokiej wydajności rozwiązania sprzętowe VPN można znaleźć w wielu urządzeniach sieciowych. Urządzenia te można scharakteryzować przez ich miejsce w sieci i pełnione funkcje. Najszerzą gamę urządzeń można znaleźć w sieciach VPN w topologii site-to-site, gdzie dwie lokacje łączy się za pośrednictwem łącza wykupionego u dostawcy, lub szkieletowej sieci VPN. Rysunek 29.2 przedstawia topologię site-to-site, zawierającą wiele elementów VPN:

- ♦ **Urządzenia klienta C (ang. *Customer*) i dostawcy P (ang. *Provider*).** Komputery, routery lub przełączniki znajdujące się po dwóch stronach łącza LAN są połączone przez VPN. Wszystkie urządzenia tych systemów są widoczne jako węzły lokalne, VPN jest niewidoczny. Urządzenia dostawcy P nie mogą łączyć się z siecią klienta.
- ♦ **Urządzenia brzegowe klienta CE (ang. *Customer Edge*) i urządzenia brzegowe dostawcy PE (ang. *Provider Edge*).** Połączenie dwóch urządzeń brzegowych tworzy łącze WAN. Zasoby sieci VPN klienta są dostępne dla urządzenia CE i jednocześnie niedostępne dla urządzenia PE, jeżeli VPN jest w sieci klienta. Zasoby sieci VPN dostawcy są dostępne dla urządzenia PE i jednocześnie niedostępne dla CE, jeśli VPN jest w sieci dostawcy.

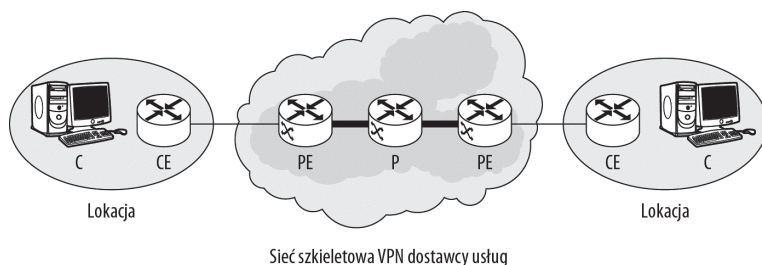
Router brzegowy klienta i przełącznik są oznaczane odpowiednio jako CE-r i CE-s. Urządzenia po stronie dostawcy to PE-r i PE-s. Jeśli urządzenie pełni zarówno funkcję routera, jak i przełącznika, otrzymuje końcówkę „rs”.

- ♦ **Gateway lub koncentrator.** Urządzenie to może być punktem końcowym dla połączeń VPN (gateway) lub zbiorem punktów końcowych połączeń VPN (koncentrator). Urządzenia te pełnią funkcję elementów brzegowych CE, zapewniając zdalny dostęp do sieci prywatnej. Poszczególne urządzenia mają różne nazwy, w zależności od miejsca w sieci i obsługiwanego protokołu. Na przykład: PPTP Network Server (PNS), L2TP Network Server (LNS) lub L2F Home albo gateway.
- ♦ **Serwer NAS (ang. *Network Access Server*).** Urządzenie to zapewnia interfejs do sieci publicznej, na przykład PSTN, sieć szkieletowa IP. Serwer może być punktem końcowym tunelu VPN.

Głównym zadaniem serwera NAS jest uwierzytelnianie żądań logowania użytkownika i kierowanie ruchu. NAS zapewnia usługi również dla telefonii VoIP.

**Rysunek 29.2.**

Topologia VPN  
site-to-site

**Objaśnienia**

C – system klienta  
CE – urządzenie brzegowe klienta  
P – urządzenie dostawcy  
PE – urządzenie brzegowe dostawcy



Akronim *NAS* oznacza również technologię umożliwiającą połączenie zasobów dyskowych bezpośrednio do sieci komputerowej (ang. *Network Attached Storage*). Urządzenia te są opisane w rozdziale 22.

- ♦ **Serwery AAA.** Te serwery VPN służą do uwierzytelniania, autoryzacji i bilingowania użytkowników (zarządzanie kontami).

Moduł uwierzytelniania weryfikuje konta użytkowników, grup i komputerów. Moduł autoryzacji zapewnia dostęp do zasobów na podstawie uprawnień użytkowników. Obie te funkcje są dostępne zazwyczaj bezpośrednio z kontrolera domeny lub innego elementu zarządzającego zasobami. Jeżeli nie ma urządzenia lub elementu zabezpieczającego, zadania te przejmuje serwer AAA. Moduł bilingowania użytkowników zapewnia dane, dzięki którym można poprawiać zarządzanie użytkownikami i naliczać opłaty.

Dostawcy usług VPN często wykorzystują wewnętrznie zabezpieczone, dodatkowe łącze szkieletowe, zwane usługą VPLS (ang. *Virtual Private LAN Service*). Ten typ VPN jest tworzony przez rozdzielenie urządzenia PE na część użytkownika (U-PE) i część sieciową (N-PE). Rysunek 29.3 przedstawia elementy sieci szkieletowej VPLS.

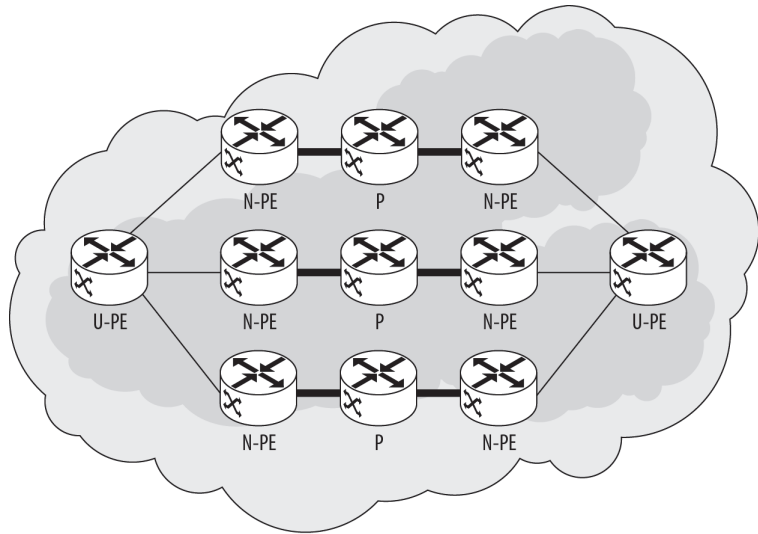
VPLS oraz podobne rozwiązanie IPLS (*IP Only LAN Service*) są nazywane wielopunktowymi sieciami prywatnymi (ang. *Multipoint-to-Multipoint VPN*, M2M VPN). Przykładem sieci P2P VPN jest WPSN VPN, Draft Martini i emulowane łącza L2TP v.3. Wymienione technologie są oparte na protokołach warstwy 2.

## Urządzenia w sieci VPN

Grupa Virtual Private Network Consortium (VPNC), która przyczynia się do tworzenia standardów sieci prywatnych, prowadzi listę członków publikowaną na stronie <http://www.vpnc.org/member-list.html>. Listę funkcji obsługiwanych przez produkty korzystające z protokołu IPSec można sprawdzić na stronie <http://www.vpnc.org/vpnc-ipsec-features-chart.html>. Tam również można zobaczyć, które z urządzeń obsługują SSL: <http://www.vpnc.org/vpnc-ssl-features-chart.html>.

**Rysunek 29.3.**

Sieć szkieletowa VPLS



Sieć szkieletowa dostawcy VPLS

Większość urządzeń dla VPN na rynku pochodzi od dwóch firm: VPN Cisco Systems (<http://www.cisco.com/en/US/products/hw/vpndevc/>) i Juniper Networks (<http://www.juniper.net>).

Cisco jest dostawcą rozwiązań VPN end-to-end, które sprawdzają się w wielu sytuacjach i środowiskach. Routery Cisco serii 1700 posiadają wbudowany moduł VPN. Te routery można również skonfigurować jako firewalle w Cisco Internetwork Operating System (Cisco IOS), zainstalowanym w modelu 1700s. Urządzeniem o wyższej wydajności jest Cisco Adaptive Security Appliance (ASA); zastąpiło ono rozwiązanie oparte na PIX Firewall i koncentratorze VPN 3000 Series. Najbardziej aktualne modele ASA weszły na rynek w 2010 roku jako seria 5585. Router 5585 jest wyposażony w system ASA OS 8.4, który obsługuje SSL i IPsec do 10 000 zdalnych użytkowników połączonych jednocześnie.

## Oprogramowanie VPN

Istnieje wiele rozwiązań oprogramowania VPN. W niniejszym rozdziale zostaną przedstawione niektóre z nich, najbardziej znane, z naciskiem na rozwiązania na licencji open source i freeware oraz moduły wbudowane w systemy operacyjne.

Jednym z najpopularniejszych pakietów obsługi VPN jest OpenVPN (<http://openvpn.net/index.php/home.html>), oprogramowanie typu klient-serwer, obsługujące SSL. OpenVPN jest dostępny dla systemów operacyjnych Linux, Windows (wersja 2.1 obsługuje Vistę i Windows 7) i Macintosh. OpenVPN jest konfigurowalny zarówno z wiersza poleceń (demon lub usługa), jak i za pomocą jednego z graficznych interfejsów użytkownika, które można pobrać ze strony <https://community.openvpn.net/openvpn/wiki/RelatedProjects>.

Z OpenVPN można utworzyć różne połączenia SSL/TLS, między innymi umożliwiając zdalny dostęp, połączenie site-to-site i Wi-Fi, oraz łączyć sieci szkieletowej. Wersja Enterprise wspiera obsługę sytuacji krytycznych oraz umożliwia równoważenie obciążenia między serwerami, a także zapewnia kontrolę dostępu do zasobów. Połączenia VPN mogą być

uwierzytelnione w OpenVPN za pomocą certyfikatów, kart inteligentnych i innych dostępnych metod. Na stronie <http://openvpn.net/index.php/documentation/howto.html#install> znajdują się szczegółowe instrukcje dotyczące omawianego programu.

Innym popularnym produktem dla systemu Windows jest LogMeIn Hamachi (<https://secure.logmein.com/products/hamachi/vpn.asp?lang=pl>). Warto zwrócić uwagę na to narzędzie ze względu na łatwość jego instalacji i konfiguracji. Hamachi to VPN, który nawiązuje połączenie między dwoma punktami końcowymi za pośrednictwem serwera mediacji UDP, a następnie tworzy obiekt połączenia bezpośredniego. Po zestawieniu połączenia serwer nie uczestniczy w procesie zapewniania usługi VPN.

LogMeIn, pierwotnie produkt na licencji freeware, oferował podstawową wersję za darmo i komercyjną wersję Premium. LogMeIn Hamachi jest usługą VPN, udostępniającą wirtualną sieć złożoną z maksymalnie 256 systemów i 50 podłączonych użytkowników przez internet.

Oto inne funkcje oferowane przez LogMeIn Hamachi:

- ♦ Firewall i router szerokopasmowy NAT.
- ♦ Kontrola zdalnego dostępu do systemu Windows poprzez Remote Desktop.
- ♦ Dostęp do dysków sieciowych.
- ♦ Zapewnia realizację połączeń peer-to-peer i czatów grupowych.
- ♦ Konta użytkowników z hasłami i kontrolą uprawnień.
- ♦ Przekazniki połączeń, gdy bezpośrednie połączenie nie może być zestawione w konfiguracji punkt-punkt.
- ♦ Wbudowany serwer sieciowy proxy dla użytkowników podłączonych do sieci Hamachi z sieci publicznej, np. z kawiarenki internetowej.
- ♦ Program ten może być uruchamiany na serwerze Windows jako usługa.

Innym programem VPN na licencji open source, który jest dostępny dla wielu platform, jest TINC (<http://www.tinc-vpn.org/>). TINC działa w systemach Linux, OpenBSD, NetBSD, Windows 2000/XP, Mac OS X i Sun Solaris i wspiera protokół IP w wersjach 4. i 6. TINC dąży do tego, aby ruch pomiędzy punktami końcowymi tunelu zawsze był realizowany z wykorzystaniem bezpośredniej (optymalnej) drogi. Program oferuje możliwość łączenia segmentów sieci Ethernet.

Rozwiązanie Microsoft Internet Security and Acceleration (ISA) Server 2006, które działa na platformie Windows Server 2003, może być skonfigurowane jako punkt końcowy sieci VPN. W roku 1997 to narzędzie zostało wydane pod nazwą Microsoft Proxy Server i stało się platformą bezpieczeństwa (firewall), routingu i obsługi funkcji buforowania. ISA Server tworzy VPN przy użyciu protokołu L2PT over IPsec (*Layer 2 Tunneling Protocol*) lub protokołu PPTP (*Point-to-Point Tunneling Protocol*). Obydwa protokoły są omówione szczegółowo w dalszej części rozdziału.

ISA Server 2006 posiada funkcję o nazwie Quarantine Control. Gdy klient łączy się zdalnie z serwerem, jest oceniany przy użyciu szeregu kryteriów w modelu zabezpieczeń systemu Windows lub serwera RADIUS. Jeżeli klient nie posiada programu antywirusowego lub najnowszych aktualizacji pobieranych z witryny Microsoft Update, otrzymuje jedynie ograniczony dostęp do sieci.

Nowa wersja narzędzia Microsoft ISA Server ukazała się w systemie Windows Server 2008 pod nazwą Microsoft Forefront Threat Management Gateway (TMG). To narzędzie jest częścią Windows Essential Business Server. Produkt ten można znaleźć na stronie <http://www.microsoft.com/forefront/default.aspx>.

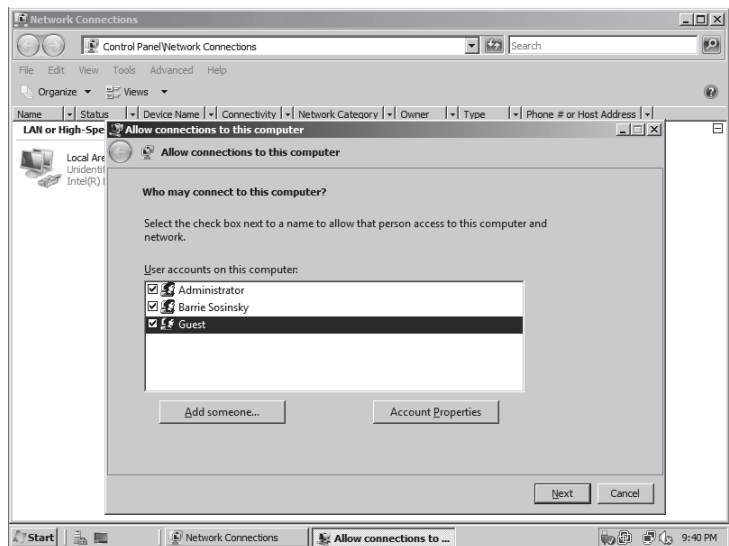
## Usługa VPN w Windows Server 2008

Aby utworzyć połączenie przychodzące VPN w Windows Server 2008, należy włączyć usługę za pomocą następującej procedury:

1. W panelu sterowania (*Control panel*) wybrać *Network and Sharing Center*, następnie z *Task* (zadania) wybrać *Manage network connections* (skonfiguruj połączenie lub sieć), w oknie dialogowym *Network Connections* (połączenia sieciowe) kliknąć menu *File* (plik), a następnie wybrać *New incoming connection* (nowe połączenie przychodzące).
2. W oknie dialogowym *Who may connect to this computer?* (kto może podłączyć się do komputera?) kreatora *Allow connections to this computer* (zezwól na połączenia do komputera), przedstawionego na rysunku 29.4, należy wybrać użytkowników, a następnie kliknąć *Next* (dalej).

### Rysunek 29.4.

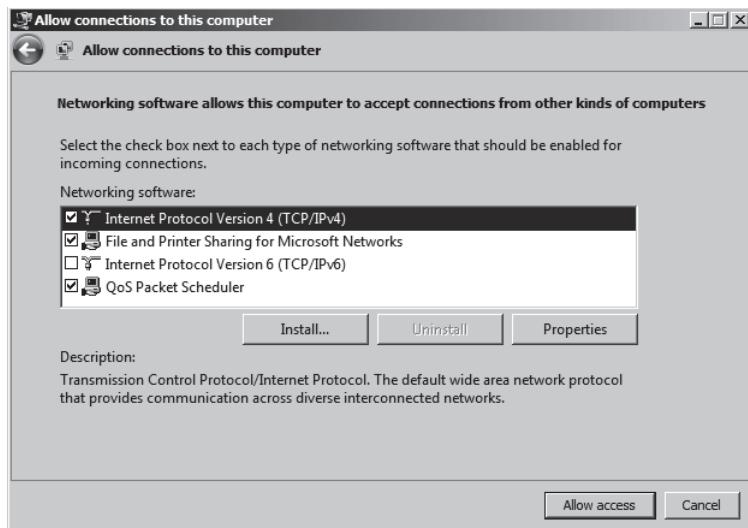
Okno dialogowe *Who may connect to this computer?* (kto może podłączyć się do komputera?)



3. W oknie *How will people connect?* (sposób połączenia) należy wyłączyć pole wyboru *Through Internet* (za pośrednictwem internetu), jeśli VPN jest używany w sieci LAN, lub pozostawić je włączone dla połączenia WAN, a następnie kliknąć przycisk *Next* (dalej).
4. W polu *Networking software allows this computer to accept connections from other kinds of computers* (oprogramowanie obsługujące połączenia sieciowe zezwala na przyjmowanie połączeń przychodzących z innych komputerów) definiujemy kryteria przyjmowania połączeń (rysunek 29.5). W tym miejscu trzeba się upewnić, że protokoły sieciowe wymagane do realizacji połączenia są zainstalowane, a ich parametry są poprawnie zdefiniowane dla łącza VPN, a następnie kliknąć przycisk *Next* (dalej).

**Rysunek 29.5.**

*Okno dialogowe Networking software allows this computer to accept connections from other kinds of computers (oprogramowanie obsługujące połączenia sieciowe zezwala na przyjmowanie połączeń przychodzących z innych komputerów)*

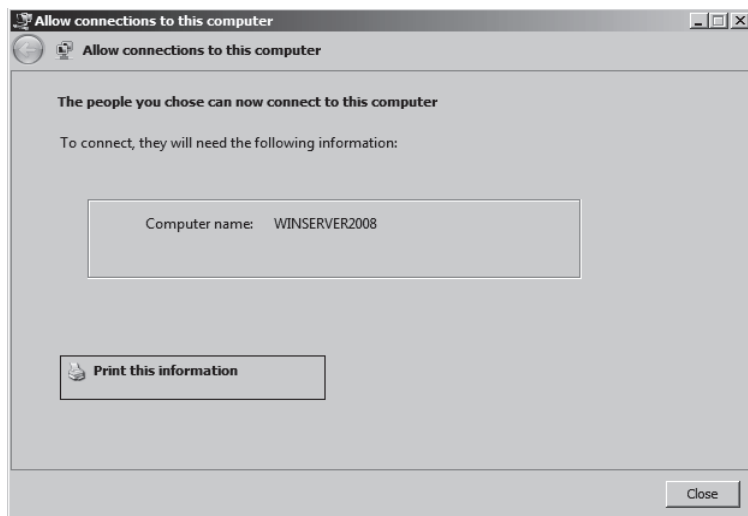


Należy się upewnić, że po stronie klienta będzie wykorzystywany protokół IP w wersji 4., albo zainstalować IP w wersji 6. w razie potrzeby.

5. Kreator tworzy połączenie przychodzące, a następnie wyświetla okno przedstawione na rysunku 29.6.

**Rysunek 29.6.**

*Wybrani użytkownicy mają dostęp do komputera*



## Klient w systemie Vista

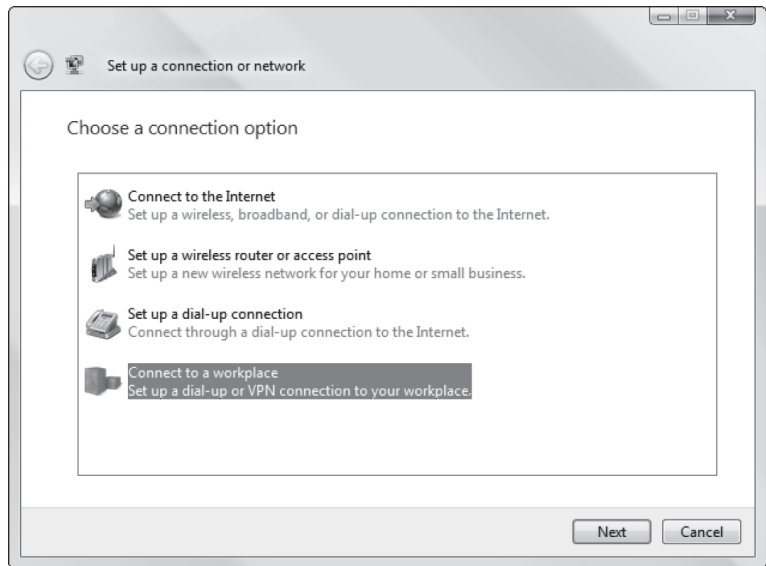
Oprogramowanie klienta VPN jest podobne dla większości systemów operacyjnych. Jako przykład prześledźmy konfigurację VPN dla Windows Vista 64:

1. Klikamy przycisk *Start*, wybieramy w *Control panel (Panel sterowania)* polecenie *Network and Sharing Center (Centrum sieci i udostępniania)*, następnie z *Task (Zadania)* należy wybrać *Manage network connections (Skonfiguruj połączenie lub sieć)*.

2. W oknie *Choose a connection option* (*Wybierz opcję połączenia*, rysunek 29.7) klikamy *Connect to a workplace* (*Połącz z miejscem pracy*), następnie przycisk *Next* (*Dalej*).

**Rysunek 29.7.**

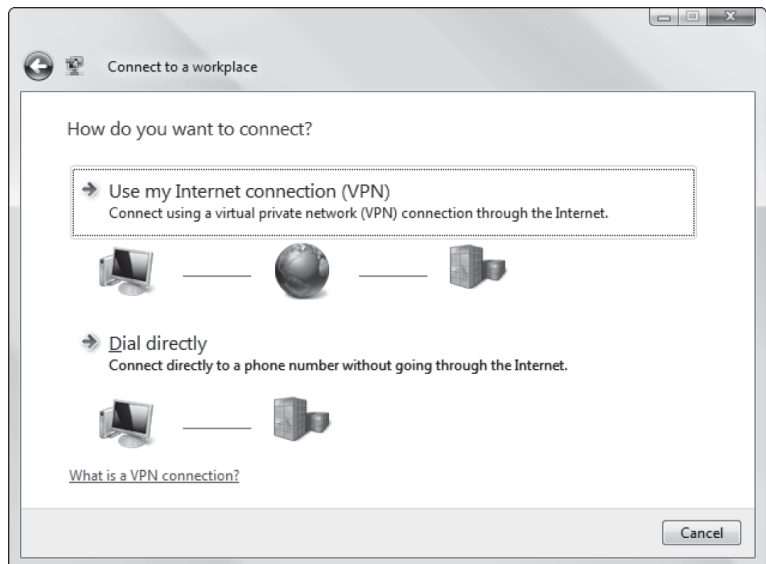
Okno *Choose a connection option* (*Wybierz opcję połączenia*)



3. W oknie *How do you want to connect?* (*Jak chcesz się łączyć?*, rysunek 29.8) klikamy opcję *Use my Internet connection (VPN)* (*Użyj mojego połączenia internetowego (VPN)*).

**Rysunek 29.8.**

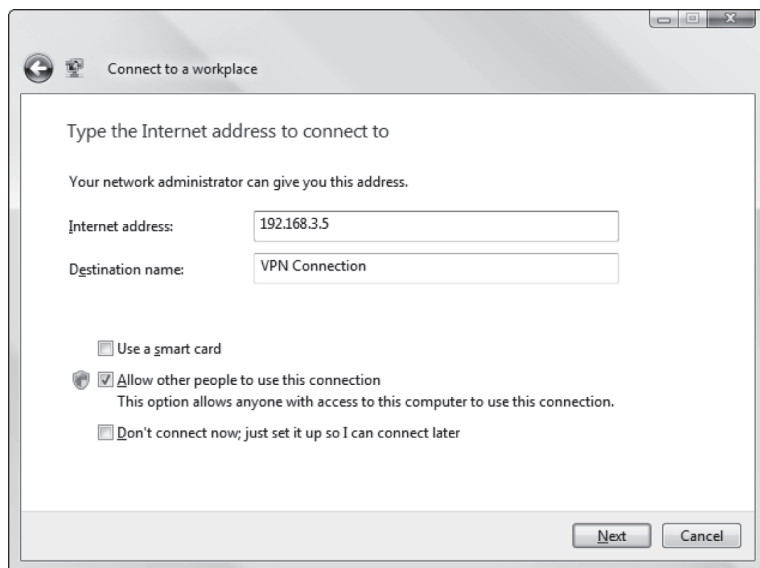
Okno *How do you want to connect?* (*Jak chcesz się łączyć?*)



4. W polu *Internet address* (*Adres internetowy*) wpisujemy w pełni kwalifikowany adres internetowy lub adres IP (patrz rysunek 29.9).

**Rysunek 29.9.**

Okno dialogowe *Type the Internet address to connect to* (Wpisz adres internetowy, z którym chcesz się połączyć)



5. W polu *Destination name* (Nazwa miejsca docelowego) wpisujemy nazwę, która ma się pojawić w przypadku wirtualnego interfejsu sieciowego w oknie dialogowym *Network connections* (Połączenia sieciowe).
6. Zaznaczamy pole wyboru *Use a smart card* (Użyj karty inteligentnej), *Allow other people to use this connection* (Zezwól innym osobom na korzystanie z tego połączenia) albo *Don't connect now* (Nie łącz teraz), a następnie klikamy przycisk *Next* (Dalej).

Można zaznaczyć jedno lub więcej z tych pól wyboru i później zmienić ustawienia VPN.

7. W polu *Type your user name and password* (Wpisz nazwę użytkownika i hasło) podajemy odpowiednie dane, a następnie klikamy przycisk *Connect* (Połącz).

Połączenie zostanie ustanowione, a interfejs sieci VPN pojawi się w oknie dialogowym *Network connections* (Połączenia sieciowe). Serwer będzie widoczny w folderze *Network* (Sieć) podczas przeglądania zasobów.

## Szyfrowanie

Ruch VPN jest szyfrowany i deszyfrowany za pomocą oprogramowania zainstalowanego w końcowych punktach połączenia VPN. Szyfrowanie jest realizowane poprzez wykorzystanie klucza publicznego lub klucza szyfrowania symetrycznego. Szyfrowanie z kluczem publicznym, znane również jako szyfrowanie z kluczem asymetrycznym, jest oparte na kluczu publicznym (proces szyfrowania) i prywatnym (proces deszyfrowania). Powszechnie znane rozwiązanie PGP korzysta z systemu szyfrowania z użyciem klucza publicznego. Szyfrowanie oparte na kluczu symetrycznym polega na zastosowaniu tego samego klucza w punktach końcowych (szyfrowanie i deszyfrowanie).



Więcej informacji dotyczących technik szyfrowania znajduje się w rozdziale 27.

Mechanizm szyfrowania opartego na kluczu symetrycznym działa na zasadzie wymiany kluczy. Powszechnie stosowana w tym celu jest metoda Diffiego-Hellmana. W tym mechanizmie nadawca i odbiorca mają utworzoną parę kluczy (publiczny i prywatny). Klucze publiczne są następnie wymieniane pomiędzy nadawcą i odbiorcą. Każdy punkt końcowy wymiany informacji uczestniczy w tworzeniu wspólnego hasła, które jest używane jako klucz dla algorytmu symetrycznego.

Łącze VPN przebiegające pomiędzy komputerem w LAN A a komputerem w LAN B można podzielić na następujące segmenty:

1. Komputer w LAN A do serwera LAN A.
2. Serwer w LAN A do routera LAN A.
3. Router w LAN A do zapory LAN A.
4. Zapora w LAN A, poprzez WAN, do zapory w LAN B.
5. Zapora w LAN B do routera w LAN B.
6. Router w LAN B do serwera w LAN B.
7. Serwer w LAN B do komputera w LAN B.

Łącze segmentu 4. jest zawsze szyfrowane, niezależnie od wybranych punktów końcowych, ze względu na transfer danych przez publiczną sieć WAN i możliwość podsłuchu danych. Wiele routerów pełni również funkcję zapór brzegowych; na trasie można umieszczać serwery pośrednie, ale nie trzeba, a końcowym urządzeniem może być serwer sieciowy — mnogość rozwiązań wiąże się z wieloma dostępnymi konfiguracjami dla VPN.

## Tunelowanie

*Tunelowanie* jest nazwą procesu enkapsulacji (umieszczania danych w specjalnych ramkach-kontenerach), routingu i deenkapsulacji po transmisji w miejscu docelowym. Tunele nie wymagają wykorzystania szyfrowania danych, ale prawie zawsze zabezpiecza się dane w trakcie tunelowania. Tunel jest logiczną trasą, która przypomina połączenie punkt-punkt. Poszczególne urządzenia występujące w tunelu (routery, bramki, przełączniki lub serwery proxy) są niewidoczne (przezroczyste) dla strony wysyłającej i odbierającej dane.

Ruch VPN jest najczęściej szyfrowany za pomocą *IPsec*. Gdy do szyfrowania bloku danych pakietu IP wykorzystuje się *IPSec*, mówimy o *transporcie IPsec*.

Jeśli *IPsec* (lub inny protokół transportowy) szyfruje cały pakiet (wraz z nagłówkiem) i tak zaszyfrowany pakiet jest wysyłany do punktów końcowych sieci VPN, mówimy o *tunelu VPN*. Tunelowanie polega na umieszczeniu zaszyfrowanego pakietu wewnątrz innego pakietu. Pakiet transportowany jest zaszyfrowany, natomiast pakiet-kontener pozostaje jawny i zawiera informacje adresowe. Na obu końcach tunelu znajdują się interfejsy umożliwiające przetworzenie i dalszą transmisję pakietu.

Tunelowanie jest uważane za bezpieczniejsze od trybu transportowego. W pierwszym przypadku szyfrujemy pakiet łącznie z oryginalnym nagłówkiem IP, w drugim oryginalny nagłówek IP pozostaje niezaszyfrowany. Tunelowanie wprowadza większą nadmiarowość w porównaniu z trybem transportowym.

Dzięki temu, że tunel VPN szyfruje pakiety, można w ten sposób przesyłać różne dane, nie zwracając uwagi na zawartość. Można wysłać dowolny typ danych przez tunel i wykorzystywać nieroutowalne adresy IP. Wykorzystanie tunelu umożliwia użytkownikowi przesyłanie pakietów zwykle zabronionych na poziomie interfejsu sieciowego lub ze względu na politykę bezpieczeństwa. Jeśli nadawca zna adres lokalny odbiorcy, np. 192.168.1.10, to dzięki tunelowi może zaszyfrowane pakiety wysłać na podany adres, nawet jeśli pochodzą spoza wspomnianej sieci LAN. Funkcja ta sprawia, że technologia VPN jest bardzo użyteczna.

## Protokoły tunelowania

W tunelowaniu wykorzystuje się różne protokoły transportowe. Można je podzielić na kilka grup: protokoły enkapsulacji zaszyfrowanych pakietów, protokoły transportowe (na przykład SSL/TLS) oraz protokoły opakowujące dane (tzw. wrappery), zawierające dane adresowe, które są stosowane w szyfrowanym nagłówku. Do enkapsulacji pakietów można użyć IPSec, GRE, PPTP i L2TP. Na przykład w internecie podstawowym protokołem jest TCP/IP, a komunikacja pomiędzy systemami po dwóch stronach tunelu może wykorzystywać inne protokoły — NBT dla systemu Windows, IPX w przypadku Netware albo po prostu IP.

## Protokół Generic Routing Encapsulation

Generic Routing Encapsulation (GRE) jest powszechnie używany jako protokół enkapsulacji w VPN, łączący jedną sieć z inną. GRE nie szyfruje pakietów, może wykonywać transmisje w trybie emisji pojedynczej, multemisji i rozgłoszeniowym. Router brzegowy korzysta z GRE w celu opakowania pakietu transportowanego, a router brzegowy w sieci docelowej odczytuje informacje nagłówka GRE, wydobywa pakiet transportowany i wysyła go dalej. Zastosowanie protokołu GRE sprawia, że odległe od siebie sieci lokalne są ze sobą połączone, a ich zasoby są dostępne lokalnie (na obu końcach połączenia). Wygląda to tak, jakby odległe sieci połączone tunelem były względem siebie lokalne. Tunele GRE są często wykorzystywane w połączeniu z protokołami szyfrującymi przesyłane dane.

GRE obsługuje adresy interfejsów zarówno fizycznych, jak i logicznych. Na przykład podczas tworzenia łącza VPN pomiędzy lokacjami można użyć adresu interfejsu sieciowego, który ma dostęp do zasobów klienta, lub adresu interfejsu pętli zwrotnej routera (ang. *loopback*). Adres pętli zwrotnej to nie to samo co adres NIC. Interfejs pętli zwrotnej jest interfejsem logicznym (lub zbiorem interfejsów logicznych) na routerze, który jest zawsze włączony.

## Tunel IPSec

IPSec to zestaw protokołów, które mogą być używane do enkapsulacji ruchu IP w tunelu zdalnego dostępu, jak również łącza pomiędzy lokalizacjami. IPSec wymaga zastosowania klucza współdzielonego w urządzeniach i konfiguracji wspierającej ten rodzaj ruchu.

IPsec może być wykorzystywany w trybie tunelu IPsec. W tym trybie IPsec zapewnia również enkapsulację pakietów. Zazwyczaj tunele IPsec mają zastosowanie w topologii typu site-to-site pomiędzy dwoma urządzeniami CE danego dostawcy usług. Głównym powodem stosowania tuneli IPsec jest możliwość wykorzystywania ich w routerach, bramkach i innych urządzeniach, w których nie można uruchomić L2TP over IPsec lub tuneli PPTP VPN.

## TLS/SSL

Protokół TLS tworzy bezpieczne połączenie dla użytkowników zdalnych. Protokół TLS to nowszy standard IETF, który jest rozwinięciem protokołu SSL v.3. Pod wieloma względami oba protokoły są bardzo podobne.

SSL jest starszym protokołem, opracowanym przez firmę Netscape. Tworzenie i konfigurowanie połączeń jest stosunkowo proste dzięki wbudowaniu SSL we wszystkich nowoczesnych przeglądarkach.

## Tunelowanie punkt-punkt

Tunele VPN przez łącza zdalnego dostępu korzystają z protokołu PPP (ang. *Point-to-Point Protocol*) jako nośnika w sieciach IP.

### Protokół PPTP

Protokół PPTP (ang. *Point-to-Point Tunneling Protocol*) tworzy tunel zdalnego dostępu PPP pomiędzy zdalnym użytkownikiem a serwerem NAS lub bramą (koncentratorem). Tunel PPTP można również skonfigurować tak, aby włączyć zdalny system do określonego fragmentu sieci.

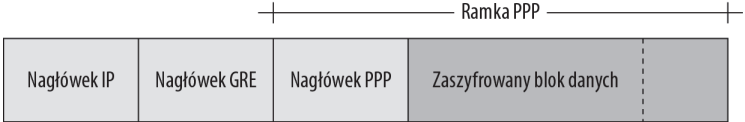
PPTP zapewnia szyfrowanie połączenia za pomocą 40-, 56- lub 128-bitowych kluczy (protokół MPPE, ang. *Microsoft Point-to-Point Encryption*). W połączeniach PPTP można wykorzystywać protokoły autentykacji, takie jak PAP, CHAP, MS-CHAP v1 i v2 lub EAP-TLS. PPTP umożliwia jedynie uwierzytelnienie użytkownika, któremu dostęp zapewnia PPP, a więc protokół ten powinien być stosowany tylko wtedy, gdy serwer lub brama docelowa tworzonego tunelu nie muszą być uwierzytelniane.

Pakiety PPP umieszczone w ramach PPTP posiadają nagłówki GRE i IP. Do szyfrowania PPTP w systemie Windows można skorzystać z protokołu MPPE. MPPE tworzy klucze sesji za pomocą haseł przy użyciu protokołu MS-CHAP (ang. *Challenge Handshake Authentication Protocol*) lub EAP (ang. *Extensible Authentication Protocol*), co oznacza, że szyfrowanie jest zależne od siły hasła użytkownika.

Rysunek 29.10 przedstawia pakiet PPTP. Proces enkapsulacji polega na dodaniu pola nagłówka IP oraz nagłówka protokołu (tutaj GRE) do zaszyfrowanych pakietów. Z punktu widzenia routera pojawi się zwykły pakiet IP, gdzie ramka PPP jest przesyłanym blokiem informacyjnym.

PPTP jest protokołem obsługiwanym w systemie Windows, ale nie ma wersji na inne platformy. Microsoft zaleca użytkownikom stosowanie protokołu L2TP zamiast PPTP.

**Rysunek 29.10.**  
Format pakietu PPTP



**Protokół L2F**

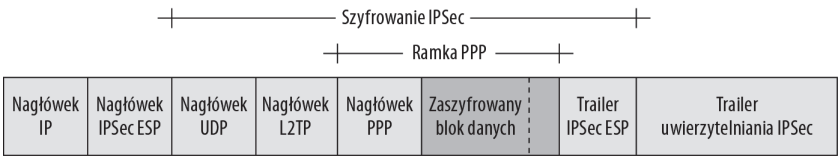
Protokół L2F (ang. *Layer 2 Forwarding*) to protokół utworzony przez Cisco; służy on do tunelowania pakietów PPP lub SLIP (ang. *Serial Line Interface Protocol*). L2F jest zwykle zaimplementowany w serwerach NAS i koncentratorach VPN.

**Protokół L2TP**

Protokół L2TP v.3 (ang. *Layer 2 Tunneling Protocol*) pozwala zdalnemu użytkownikowi (klientowi, LAC, ang. *L2TP Access Concentrator*) na utworzenie tunelu do serwera NAS, bramy (LNS, ang. *L2TP Network Server*) i przesyłanie ramek PPP.

Ponieważ L2TP nie zapewnia bezpieczeństwa, jego ruch jest zazwyczaj zabezpieczony przez IPsec. Ruch może przebiegać przez sieci ATM, Frame Relay, PPP, VLAN lub PPP w sieciach IP. L2TP v.3 jest ostatnim z trzech omawianych protokołów i zawiera zarówno elementy PPTP, jak i L2F. L2TP enkapsuluje ramki PPP w pakietach, a IPsec szyfruje zawartość tych pakietów. Zastosowanie L2TP over IPsec nie tylko zapewnia uwierzytelnianie PPP, ale również wymaga uwierzytelnienia maszyny przez odpowiedni certyfikat lub klucz. L2TP jest protokołem dostępu zdalnego PPP. Rysunek 29.11 przedstawia pakiet L2TP.

**Rysunek 29.11.**  
Struktura pakietu L2TP



ESP = Encapsulating Security Payload

L2TP jest powszechnie stosowanym protokołem w sieciach VPN, ale poza wymienionymi zaletami ma również wady. Tak jak wiele technologii WAN, L2TP over IPsec często ma problemy z translacją NAT na starszych platformach. Routing NAT działa na zaporze lub w serwerze proxy, zmieniając adres IP i ewentualnie numer portu w nagłówku UDP, pozostawiając część pakietu IPsec bez zmian. Jeśli przekierowanie nie jest wykonane prawidłowo, pakiet będzie usunięty, gdy dotrze do miejsca przeznaczenia.

**Podsumowanie**

W tym rozdziale omówiono sieci VPN i ich zastosowania w tworzeniu bezpiecznego połączenia w sieci przez publiczne łącza WAN i internet. Nowoczesne sieci nie mogłyby istnieć bez tych ważnych technologii. Pierwsze łącza VPN zostały utworzone w celu przesyłania danych w sieci telefonicznej. Później uruchomiono VPN w systemach łączy dzierżawionych, a następnie w internecie.

VPN wykorzystuje kilka protokołów warstw 2. i 3. Łączy VPN to zazwyczaj łączy zdalnego dostępu lub bezpiecznego łączy site-to-site. Pakiety danych VPN są wysyłane w trybie transportowym lub tunelowania. W rozdziale tym szczegółowo opisano techniki stosowane w celu zabezpieczenia danych w sieciach VPN — szyfrowanie, enkapsulację i inne. Przedstawiono również wiele typów sieci VPN.

Kolejny rozdział opisuje metody zarządzania siecią. Sieci to duże, złożone struktury, które często ulegają zmianom. Oprogramowanie i odpowiednie metody zarządzania sieciami są ważne w systemach o każdej wielkości.



## Część VII

# Diagnostyka i zarządzanie siecią

### **W tej części:**

**Rozdział 30.** Zarządzanie siecią

**Rozdział 31.** Polecenia diagnostyczne sieci

**Rozdział 32.** Dostęp zdalny

**Dodatek A** Przypisania portów TCP — UDP



# Rozdział 30.

## Zarządzanie siecią

### W tym rozdziale:

- ♦ Kategorie zarządzania siecią
- ♦ Narzędzia, które można wykorzystać do wysledzenia błędów sieci
- ♦ Sposoby używania zdarzeń do określenia wydajności działania sieci
- ♦ Obecnie stosowane systemy zarządzania siecią

Narzędzia służące do zarządzania siecią mają ogromne znaczenie dla sieci każdej wielkości. Opracowanie dużych sieci w przemyśle telekomunikacyjnym i wojskowym zapoczątkowało proces standaryzacji, który doprowadził do powstania wielu standardów protokołów sieciowych używanych do zarządzania nowoczesnymi sieciami. W rozdziale wykorzystano klasyfikację ITU-T o nazwie *FCAPS* dla oprogramowania służącego do zarządzania siecią, pozwalającego na organizację różnego rodzaju narzędzi administracyjnych. Akronim *FCAPS* oznacza *Fault, Configuration, Accounting and Administration, Performance, and Security*, czyli: usterki, konfiguracja, rozliczenia i administracja, wydajność oraz bezpieczeństwo.

Oprogramowanie do zarządzania usterekami pozwala na wykrycie określonych zdarzeń powiązanych z błędami i pomaga administratorowi w ustaleniu przyczyn usterek. Zdarzenia mogą być przeglądane w przeglądarce zdarzeń, a różne właściwości powiązane z każdym zdarzeniem umożliwiają ich identyfikację. Ponieważ usterki mogą generować kolejne zdarzenia i prowadzić do powstania ich lawiny, ich wykrycie usterek stanowi prawdziwe wyzwanie.

Oprogramowanie służące do zarządzania konfiguracją pozwala administratorowi na określenie konfiguracji różnych urządzeń sieciowych, zmianę tej konfiguracji i zapisanie wprowadzonych modyfikacji. W rozdziale omówione będą również zagadnienia pokrewne, czyli wdrażanie<sup>1</sup> oprogramowania sieciowego, uaktualnienia, zarządzanie i cykl życiowy systemu.

Przedstawione będą także różne czynniki wpływające na zarządzanie sieciami zdarzeniami dotyczącymi rozliczeń, bezpieczeństwa i monitorowania wydajności. Wszystkie wymienione zadania obejmują przechwytywanie zdarzeń odpowiedniego rodzaju oraz analizę

---

<sup>1</sup> Termin stosowany przez Microsoft (<http://www.microsoft.com/poland/technet/article/art0173.msp>) — przyp. tłum.

ich przebiegu. Narzędzia służące do monitorowania stanowią rozszerzenie operacji rejestrowania zdarzeń w celu określenia wartości liczbowych, które mogą być wykorzystane podczas zarówno usuwania usterek w sieci, jak i optymalizacji jej wydajności. Zaprezentowana będzie koncepcja liczników i agentów stosowana w analizie zdarzeń pomiarowych.

Na rynku dostępnych jest wiele systemów zarządzania sieciami. Część z tych narzędzi to aplikacje w postaci platform, podczas gdy inne stanowią rozwiązania własnościowe; w rozdziale będą przedstawione niektóre z nich.

## Znaczenie zarządzania siecią

Zarządzanie siecią zawsze stanowi wyzwanie. Potencjalne problemy zwiększają się w postępie geometrycznym wraz ze wzrostem liczby węzłów sieciowych. Kiedy sieć rozrośnie się ponad wielkość małej grupy roboczej, koszt pracy wkładanej w systemy zarządzania siecią szybko przekroczy koszt omówionych w rozdziale systemów zautomatyzowanych. Dlatego też oprogramowanie do zarządzania siecią charakteryzuje się wysokim wskaźnikiem zwrotu z inwestycji (ang. *Return of Investment* — ROI) i bardzo krótkimi okresami tego zwrotu, które często są liczone w miesiącach, a nie latach.

Niestety, wiele sieci rozrasta się do ogromnych rozmiarów, zanim właściciele odkryją istnienie zależności między oszczędnościami, które można poczynić dzięki zastosowaniu zautomatyzowanych systemów zarządzania, i kosztem nieustannego zwiększania personelu IT zajmującego się ręcznym zarządzaniem siecią. Oczywiście zwiększenie rocznego kosztu obsługi każdego komputera w sieci o dodatkowe 250 – 500 dolarów stanowi barierę w adaptacji oprogramowania zarządzającego, podobnie jak tendencja, aby w każdym z tego rodzaju produktów ograniczać klientów jedynie do określonych technologii. Dopóki nie zostaną obliczone rzeczywiste koszty działania systemu bez oprogramowania służącego do zarządzania siecią, personel IT odpowiedzialny za administrowanie siecią musi poświęcać coraz więcej czasu na usuwanie występujących w niej problemów.

W poniższych podrozdziałach zostaną przedstawione niektóre z najważniejszych funkcji pakietów oprogramowania służącego do zarządzania siecią. Pakietem takim jest FCAPS (*Fault, Configuration, Accounting and Administration, Performance, and Security* — usterki, konfiguracja, rozliczenia i administracja, wydajność oraz bezpieczeństwo); będzie on przedstawiony jako pierwszy. Po kolei zostaną omówione wymienione aspekty zarządzania siecią.

### FCAPS

Większość standardów zarządzania siecią pochodzi z dwóch głównych obszarów, w których najwcześniej pojawiły się doświadczenia związane z sieciami heterogenicznymi, czyli z przemysłu telekomunikacyjnego i wojskowego.

Jak już wspomniano w rozdziale 13., przemysł telekomunikacyjny był pionierem projektowania i obsługi ogromnych sieci komutowanych. Do końca lat siedemdziesiątych przez tworzenie różnych grup roboczych ustanowił standardy wielu technologii. Pewnym bodźcem był podział Ma Bell (sieci AT&T) na Baby Bells. Ostatecznie część odpowiedzialna

za zarządzanie siecią została skonsolidowana w organizacji ITU-T, w grupie TMN (ang. *Telecommunications Management Network*). Międzynarodowa Organizacja Standaryzacyjna (ISO) opracowała standard zarządzania siecią, który często jest nazywany OSI SMO (ang. *Systems Management Overview*). Po wprowadzeniu FCAPS przez ITU-T ISO dołączyła go do swojego modelu zarządzania sieciami. Z założenia model służący do zarządzania siecią miał być systemem otwartym, w którym każdy obszar zarządzania ma własny zestaw protokołów.

FCAPS obejmuje większość obszarów w standardzie zarządzania siecią ITU-T:

- ♦ *Fault* — zarządzanie usterkami; obejmuje rejestrację zdarzeń, analizę błędów, usuwanie błędów i odzyskiwanie danych.
- ♦ *Configuration* — zarządzanie konfiguracją; obejmuje zarządzanie zasobami, inwentaryzację, wdrażanie oprogramowania, zarządzanie pakietami i udostępnianiem usług sieci.
- ♦ *Accounting and Administration* — zarządzanie rozliczeniami i administracją; funkcje te obejmują dostarczanie danych statystycznych oraz zintegrowane funkcje rozliczeniowe.
- ♦ *Performance* — zarządzanie wydajnością; jest to rozszerzenie operacji monitorowania zdarzeń i obejmuje zbieranie danych dotyczących systemów w sieci oraz jej komponentów, a także funkcje dostarczające informacje na temat oprogramowania.
- ♦ *Security* — zarządzanie bezpieczeństwem; obejmuje wdrożenie i rozwój polityki bezpieczeństwa, pozwala na zarządzanie użytkownikami i identyfikatorami systemów za pomocą samodzielnej funkcjonalności bądź w połączeniu z usługami katalogowymi.

Chociaż początkowa koncepcja ISO zakładała utworzenie oddzielnych protokołów dla każdego z pięciu tych obszarów, które miały się składać na standard o nazwie SMO (ang. *Systems Management Overview*), to w trakcie prac stało się jasne, że obszary te mogą być obsługiwane za pomocą ujednoliconego podejścia z użyciem jednego protokołu. W wyniku prowadzonych prac powstał protokół CMIP (ang. *Common Management Information Protocol*) udostępniony w postaci rekomendacji ITU-T X.700 (<http://www.itu.int/rec/T-REC-X.700/en>). Systemy CMIP działają z obiektami zarządzanymi, każdy posiada unikalny deskryptor w przestrzeni nazw znany jako DN (ang. *Distinguished Name*). Koncepcja ta jest bardzo podobna do usług katalogowych X.500 (LDAP), które szczegółowo zostały omówione w rozdziale 21.

Protokół CMIP to konkurent częściej używanego protokołu SNMP (ang. *Simple Network Management Protocol*), czyli standardu IETF, oferujący więcej możliwości. Protokół CMIP zawiera pewną liczbę operacji w postaci poleceń, które pozwalają na modyfikację zarządzanych elementów sieciowych. Z drugiej strony protokół SNMP umożliwia jedynie zmianę stanu zarządzanego elementu przez użycie polecenia SET. Polecenie SET to generalnie operacja zapisu (WRITE) wartości obiektu. Powodem, dla którego protokół SNMP jest tak doskonale znany w przeciwieństwie do CMIP, jest wbudowanie jego obsługi w większości urządzeń sieciowych przeznaczonych dla sieci TCP/IP. Osprzęt SNMP jest mniej skomplikowany i lepiej się sprzedaje. Ponadto jest tańszy w implementacji, co oznacza niższy koszt produkcji i wdrożenia całego rozwiązania.



Protokół SNMP został szczegółowo omówiony w rozdziale 4.

Systemy zarządzania mają długą historię w przemyśle komputerowym i istnieje wiele standardów stosowanych do zarządzania systemami biurowymi, wdrażania systemów oraz przeprowadzania innych operacji związanych z zarządzaniem. Czytelnik spotkał się już z niektórymi z protokołów zarządzania, na przykład SNMP i WEBM. Poniżej wymieniono kilka innych standardów protokołów:

- ♦ NETCONF (<http://www.ietf.org/html.charters/netconf-charter.html>), który podobnie jak SNMP jest standardem IETF.
- ♦ *Common Information Model* (<http://www.dmtf.org/standards/cim/>), WS-Management (protokół SOAP; <http://www.dmtf.org/standards/wsman>) oraz SMASH (ang. *Systems Management Architecture for Server Hardware*; <http://www.dmtf.org/standards/smash/>) — są to standardy bądź inicjatywy DMTF. Standard *Desktop Management Interface* (DMI; <http://www.dmtf.org/standards/dmi/>) to inna platforma DMTF służąca do zarządzania PC, ale została porzucona na rzecz nowszego standardu CIM.
- ♦ JMX (*Java Managed Extensions*; <http://www.oracle.com/technetwork/java/javase/tech/javamanagement-140525.html>) to rozwiązanie Javy przeznaczone do zarządzania obiektami sieciowymi (MBeans lub Managed Beans).

Istnieje więcej standardów protokołów, które są albo charakterystyczne dla danego przemysłu, albo tak słabo znane, że nie warto o nich wspominać w tym miejscu.

Wprawdzie FCAPS nie jest tak doskonale znany jak siedmiowarstwowy model sieciowy ISO/OSI, ale stanowi wygodny schemat organizacyjny do opisywania różnych funkcji zarządzania sieciowego. W kolejnych fragmentach podrzędnika omówiono różne aspekty modelu FCAPS; dalej zamieszczono przykłady platform sieciowych.

## Zarządzanie usterkami

Usterka to błąd w sprzęcie bądź oprogramowaniu, który prowadzi do niepożądanych skutków. Celem zarządzania usterkami jest ich wykrywanie, izolowanie ich przyczyn oraz dostarczenie informacji niezbędnych do usunięcia usterek (ich przyczyn). Większość systemów operacyjnych i aplikacji ma bardzo dobre funkcje informujące o powstawaniu błędów. Systemy zarządzania usterkami również mają świetne funkcje pozwalające na przechwytywanie i wyświetlanie informacji o błędach. Z kolei ich niedoskonałością jest brak możliwości dokładnego określenia natury powstałej usterki.

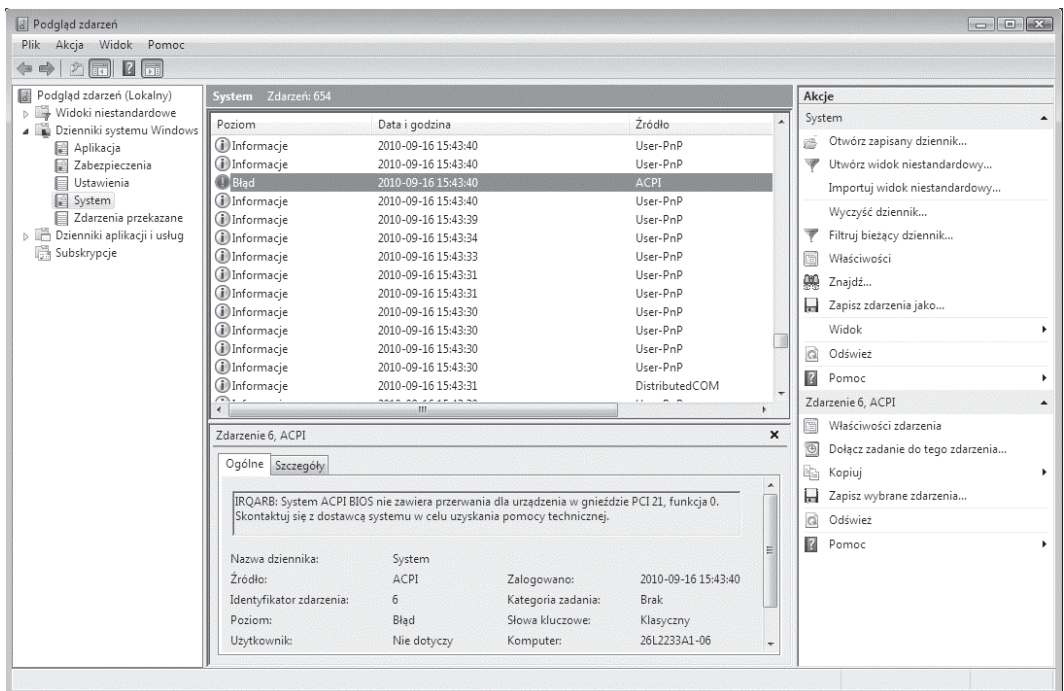
Systemy zarządzania usterkami działają na zasadzie wykrywania określonych zdarzeń, które są powiązane z błędem, lub wykrywają usterki na podstawie zbioru zdarzeń. Wszystkie nowoczesne sieciowe systemy operacyjne oraz ich biurowe odpowiedniki działają na bazie zdarzeń. Oznacza to, że oprogramowanie pozostaje w stanie oczekiwania aż do chwili otrzymania polecenia zmuszającego aplikację do podjęcia określonego działania. Niektóre zdarzenia dotyczą ogólnej obsługi systemu, inne mogą wywoływać sprawdzenie spójności pamięci itd. Zdarzenia mają ustalone typy i mogą być przechwytywane selektywnie, na przykład zapis interesujących użytkownika zdarzeń w pliku dziennika zdarzeń (zwykle

w bazie danych), i (lub) wysyłane przez sieć w standardowym protokole warstwy aplikacji, takim jak SNMP, bądź w przypadku niektórych producentów za pomocą protokołu własnościowego. Izolacja i zrozumienie zdarzeń różnych typów jest pierwszą linią obrony w każdej procedurze zarządzania usterkami.

Dalej zostaną przedstawione sposoby rejestrowania zdarzeń, wywoływania alarmu przez zdarzenie na podstawie ustalonych warunków, a także to, jak analiza zdarzeń może być pierwszą linią obrony w rozwiązywaniu problemów i optymalizacji sieci.

## Pliki dzienników zdarzeń

Na rysunku 30.1 pokazano narzędzie *Podgląd zdarzeń* w systemie Windows Vista 64; podświetlone zostało zdarzenie błędu w dzienniku systemowym. Różne systemy operacyjne są dostarczane z podstawowym zestawem zdarzeń i narzędzi do rejestracji i przeglądania, które choć mają inne nazwy, to jednak są do siebie podobne. Przeglądarka zdarzeń w systemie Windows jest przykładem tej klasy narzędzi. Warto zwrócić uwagę na fakt, że każde zdarzenie ma przypisany zestaw właściwości: identyfikator zdarzenia, datę i godzinę, źródło oraz nazwę pliku dziennika, w którym zostało zapisane. Ponieważ w dzienniku znajduje się wiele zdarzeń, wszystkie narzędzia tego rodzaju pozwalają na stosowanie filtrów selekcyjnych wyświetlane zdarzenia. Pokazane na rysunku narzędzie Podgląd zdarzeń zawiera zdarzenia lokalne, ale umożliwia również zalogowanie się do systemu zdalnego i wyświetlanie różnych plików dzienników zdarzeń systemu.



**Rysunek 30.1.** Narzędzie Podgląd zdarzeń



Identyfikator zdarzenia, opis i inne właściwości dostarczane przez sieciowe systemy operacyjne i aplikacje są bardzo często opisywane w informacjach technicznych, publikowanych na witrynach internetowych ich producentów. Bardzo często najlepszym sposobem poznania znaczenia danego błędu jest poszukiwanie informacji na jego temat w wyszukiwarce internetowej, na przykład Google.

Pokazane na powyższym rysunku narzędzie Podgląd zdarzeń jest komponentem konsoli MMC (ang. *Microsoft Management Console*) i może być uruchomione jako samodzielne narzędzie albo, jak w przypadku systemu Windows Server 2008, w ramach konsoli *Menedżer serwera* (omówionej w dalszej części rozdziału).

Różne wersje systemów Unix i Linux przechowują swoje zdarzenia w pliku *messages* lub *syslog*, który może być przeglądany za pomocą poleceń konsoli bądź narzędzi graficznych (GUI). W systemie Ubuntu dzienniki systemowe są domyślnie umieszczane w katalogu */var/log*, który zawiera między innymi pliki *syslog*, *dmesg*, *kern.log*, *daemon.log* itp. Zakładając, że użytkownik ma uprawnienia do przeglądania plików dzienników zdarzeń systemu, można skorzystać z narzędzia *Przeglądarka dzienników systemowych* w Ubuntu, które po uruchomieniu wygląda podobnie jak pokazane na rysunku 30.1. Wymienione pliki dzienników zdarzeń są przechowywane w postaci tekstu ograniczonego znakami (na przykład tabulatorami), co umożliwia przeglądanie ich w sesji terminalu z wykorzystaniem polecenia *grep*.

Istnieją dwa rodzaje systemów przechwytyjących zdarzenia: liczniki i agenty. Liczniki są wbudowane w aplikację bądź system operacyjny przez jego programistów, podczas gdy agenty to małe programy wykonywalne, instalowane przez inne programy w celu monitorowania wartości liczników. Ogólnie rzecz biorąc, liczniki działają z większymi uprawnieniami niż agenty i mają dostęp niskiego poziomu do informacji zdarzeń. Jednak doskonale przygotowany pakiet zarządzania siecią, na przykład Altiris, zainstaluje w systemie agenta lokalnego, który jest programem niskiego poziomu, trudnym do usunięcia. W każdym razie dane przechwycone przez licznik lub agenta powinny być identyczne.

Liczniki i agenty są wykorzystywane nie tylko do przeprowadzania operacji odczytu i zapisu (READ i WRITE) w dziennikach zdarzeń, ale również do dostarczania danych używanych do określania wydajności. Ponieważ przeglądarki zdarzeń to narzędzia przeznaczone jedynie do wyświetlania informacji o zdarzeniach, użytkownik nie może stosować tych narzędzi do uzyskania jakiegokolwiek kontroli nad licznikami i agentami. W celu zmiany sposobu monitorowania zdarzeń lub w ogóle włączenia ich monitorowania trzeba wykorzystać aplikacje monitorowania wydajności, które będą przedstawione w dalszej części rozdziału.

## Alarmy

Oprócz wykrywania usterek funkcje zarządzania usterkami mają również wywoływać alarmy. Alarm to wykryty stan błędu, który może być skatalogowany w kategoriach typu i ważności oraz zarejestrowany w bazie danych bądź wysłany w formie powiadomienia. Ponieważ stan alarmu jest wykrywany poprzez pojawienie się zdarzenia alarmu, systemy zarządzania to po prostu inna postać przeglądarki zdarzeń z filtrami typów zdarzeń i pewnymi regułami określającymi sposób obsługi zdarzeń monitorowanego typu.

Kiedy funkcja urządzenia lub systemu automatycznie wywołuje alarm, system ten określa się pasywnym systemem zarządzania. Gdy program wysyła zapytania do urządzeń, na

przykład odpowiedzi na polecenie ping, mamy do czynienia z aktywnym systemem zarządzania. Funkcje systemu w zależności od sposobu tworzenia pakietu odpowiedzialnego za zarządzanie siecią mogą być aktywne albo pasywne lub aktywne i pasywne.

Alarmy mogą być kategoryzowane jako analogowe lub cyfrowe. Alarm cyfrowy to system dwójkowy z dwoma stanami: ON lub OFF, 1 lub 0, TRUE lub FALSE. W rejestrze alarmu w rzeczywistości jest przechowywana wartość 1 lub 0, natomiast użytkownik widzi jedynie funkcję zajmującą się odpowiednim formatowaniem danych wyjściowych. Rejestr to po prostu adres w pamięci, do którego można się odwołać, zawierający wartość odnoszącą się do pewnej zmiennej. W rzadkich przypadkach systemy zarządzania alarmem dwójkowym dostarczają trzecią wartość, która pojawia się jako NULL lub NA (ang. *Not Available* — niedostępna) albo po prostu pozostawia puste miejsce w danych wyjściowych. Wiele aplikacji bazodanowych obsługuje w ten sposób pola dwójkowe.

Alarm analogowy może pobierać zakres wartości. Przykładem pola analogowego może być to, które zawiera liczbę zagubionych ramek. Alarm analogowy ma właściwość w postaci wartości, która może być dowolną liczbą z podanego zakresu. Jeżeli zakres nie został zdefiniowany, to wartość może być dowolną liczbą o liczbie cyfr obsługiwanej przez rejestr danego alarmu. Czytelnik może odkryć, że aplikacja, której używa do zarządzania siecią, pozwala na ustawienie poszczególnych fragmentów zakresu w sposób podobny do poniższego:

- ♦ niski-niski: 0 — < 20%;
- ♦ niski: 20 — <35%;
- ♦ średni: 35 — <65%;
- ♦ wysoki: 65 — <80%;
- ♦ wysoki-wysoki: 80 — 100%.

Ponieważ wartości analogowe są użyteczniejsze podczas sprawdzania wydajności, to z reguły są stosowane w celu dostarczania współczynników bądź wartości, na przykład liczby ramek gubionych w ciągu sekundy lub liczby najbliższych routerów, które odpowiedziały na polecenie. Dlatego też bywają wbudowywane w narzędzia monitorowania wydajności.

Aplikacje zarządzania alarmami są bardzo często stosowane, gdyż sygnalizują usterki, które wymagają usunięcia. Tego rodzaju aplikacje najczęściej są dostarczane wraz z funkcją powiadamiania. Istnieje wiele metod wykorzystywanych do powiadamiania innych aplikacji o wystąpieniu stanu błędu. Błąd może więc zostać wyświetlony w aplikacji GUI, takiej jak konsola Alarm Human Machine Interface (HMI), alarm może wygenerować zdarzenie SNMP, które zostanie wysłane do innej aplikacji. Ponadto alarm może zostać umieszczony w wiadomości e-mail i być wysłany za pomocą protokołu SMTP do serwera poczty lub jako faks (stara szkoła) albo wiadomość tekstowa SMS (nowa szkoła).

## Korelacja zdarzeń

Pakiety służące do zarządzania usterkami muszą być napisane w sposób pozwalający im na rozpoznanie, kiedy wiele zdarzeń zostało spowodowanych przez wystąpienie tego samego stanu błędu — ten proces nazywa się korelacją zdarzeń. W systemach, w których wystąpiła

usterka bądź wystąpił błąd, rzadko się zdarza, aby zostało wygenerowane pojedyncze zdarzenie błędu. Jeżeli aplikacja na przykład wymaga uzyskania dostępu do urządzenia USB, a próba połączenia z tym urządzeniem zakończy się niepowodzeniem, to system może wielokrotnie próbować nawiązać połączenie aż do przekroczenia czasu przeznaczonego na wykonanie danej operacji i za każdym razem generować zdarzenie błędu. System zarządzania usterkami zgłaszający setki razy ten sam błąd nie przynosi żadnego pożytku. Niemal wszystkie pakiety służące do zarządzania usterkami zawieszają lub skonsolidują powielające się zdarzenia błędów, aby użytkownikowi zostały przedstawione jedynie istotne informacje.

Oprogramowanie przeprowadzające analizę korelacji zdarzeń to korelator zdarzeń. Systemy takie wykorzystują sztuczną inteligencję. W korelacji zdarzeń często występują cztery etapy:

- ♦ **Filtrowanie** — odrzucanie nieistotnych zdarzeń.
- ♦ **Agregacja** — czyli usuwanie powielających się tych samych zdarzeń.
- ♦ **Maskowanie** — skutkuje ukrywaniem zdarzeń będących wynikiem błędu i niedotyczących rzeczywistego błędu. Czasami funkcja ta jest określana mianem maskowania topologicznego.
- ♦ **Analiza przyczyn źródłowych** (ang. *Root Cause Analysis* — RCA) to metodologia, która wykorzystuje zależności zdarzeń do utworzenia modelu środowiskowego, pozwalającego na ujawnienie ostatecznej przyczyny błędu. Analiza przyczyn źródłowych może skutkować informacją taką jak „dysk XYZ jest pełny” zamiast „niepowodzenie operacji WRITE na XYZ”.

Wiele systemów korelacji zdarzeń jest używanych w biurach pomocy (ang. *Help Desk*) i działa w połączeniu z systemem typu *Trouble Ticket* lub *Incident Management* (IcM). Kiedy zostanie wykryty błąd, otrzymuje swój identyfikator, a karta błędu jest wprowadzana do bazy danych i rejestrowana. Zebrane informacje dotyczące danego błędu zostają umieszczone w bazie danych i są przechowywane aż do znalezienia wyjaśnienia bądź rozwiązania. Takie systemy często zawierają informacje o stanie danego zadania, co pozwala organizacjom na ich wykorzystywanie w trakcie prac nad danym projektem. Są więc użyteczne podczas zarządzania siecią, ponieważ pozostają w projektach tworzenia oprogramowania.

Znacznie bardziej kłopotliwa jest sytuacja, kiedy usterka wywołuje lawinę zdarzeń. Wracając do wspomnianego wcześniej urządzenia USB, przyjmijmy założenie, że urządzenie jest dyskiem USB zawierającym plik, który musi być użyty przez inną aplikację. Program wysłał więc polecenie odczytu (READ) pliku, które zostaje przekierowane przez system operacyjny. Pomimo wielokrotnych prób system nie może uzyskać dostępu dożądanego pliku i cały proces rozpoczyna generowanie różnych błędów w systemowym dzienniku zdarzeń. Brak dostępu może być wynikiem uszkodzenia samego urządzenia, portu USB bądź skutkiem błędu w szynie USB. Kiedy błąd pnie się do góry w łańcuchu zdarzeń, następuje generowanie lawiny błędów powiązanych z tymi zdarzeniami. Błędy może zgłaszać system operacyjny, aplikacja itd. Wszystkie zgłoszone błędy odnoszą się do tej samej usterki, ale ponieważ zostają umieszczone w pliku dziennika błędów, to do użytkownika należy określenie ich przyczyny.

Im bardziej skomplikowany pakiet zarządzania usterkami, tym lepiej radzi sobie podczas przetwarzania powiązanych ze sobą błędów i określania usterki będącej ich przyczyną. Nawet najbardziej wyróżniające się pakiety zarządzania usterkami często będą przedstawiały

użytkownikowi powiązane ze sobą błędy, które trzeba będzie rozpatrzyć we właściwym kontekście, aby ustalić ostateczną przyczynę usterki. Stąd rada autora: jeżeli Czytelnik kiedykolwiek będzie musiał wybierać pakiet zarządzania siecią, to warto przyjąć jako jeden z kluczowych wyróżników wydajności to, jak dobrze dany pakiet obsługuje lawinę zdarzeń i powielające się zdarzenia. Ponadto warto sprawdzić, jak pakiet radzi sobie z ustalaniem związków między zdarzeniami i ich przyczynami.

## Zarządzanie konfiguracją

Zarządzanie konfiguracją odnosi się do zadań związanych z zarządzaniem konfiguracją i identyfikacją systemów oraz użytkowników w sieci, jak również wprowadzaniem wymaganych modyfikacji.

Zadania, które zaliczają się do zarządzania konfiguracją, to między innymi:

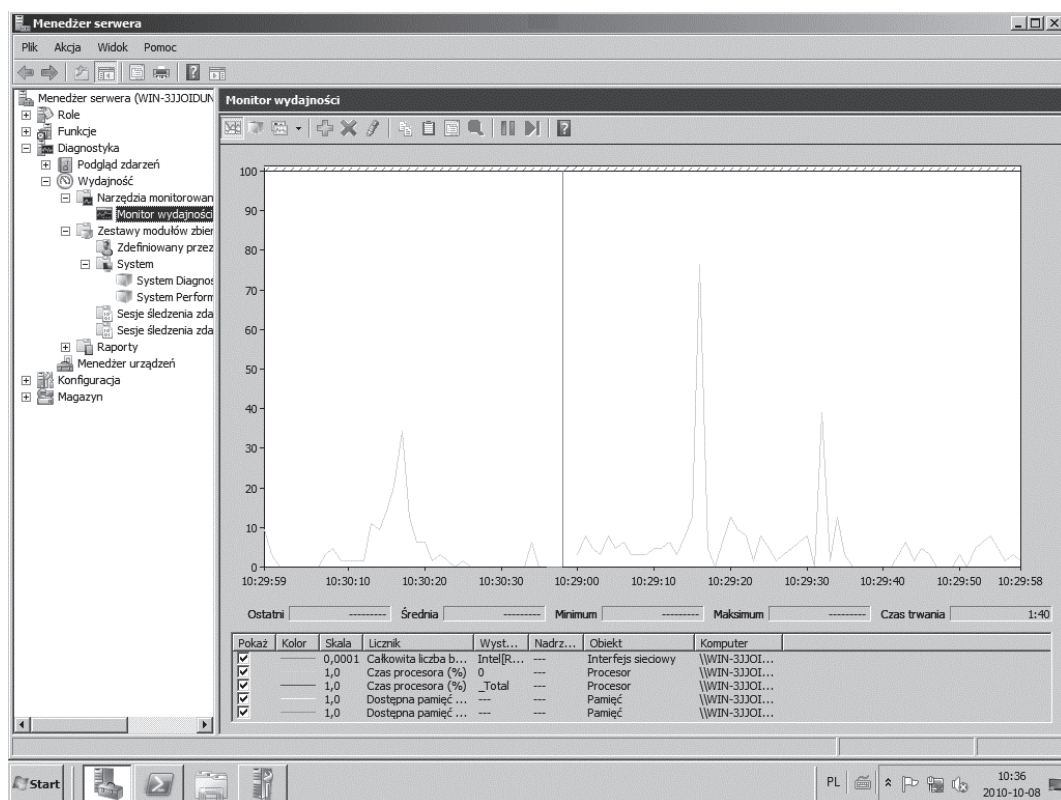
- ♦ konfigurowanie komputerów i urządzeń sieciowych;
- ♦ instalacja i konfiguracja oprogramowania; proces ten jest nazywany zarządzaniem konfiguracją oprogramowania, czyli SCM (ang. *Software Configuration Management*);
- ♦ zarządzanie różnymi użytkownikami i grupami w sieci, łącznie z ich kontami i rolami;
- ♦ uaktualnianie oprogramowania i systemów, gdy zachodzi taka potrzeba;
- ♦ zapewnianie dedykowanych połączeń sieciowych;
- ♦ dokumentowanie konfiguracji wszystkich komponentów sieciowych.

Celem zarządzania konfiguracją jest ustawienie systemów w taki sposób, aby zautomatyzować wykonywanie powtarzających się zadań, zmniejszyć stopień skomplikowania konfiguracji przez stosowanie zestawu standardów oraz aktywne monitorowanie stanu systemów. Jednym ze sposobów zmniejszenia poziomu skomplikowania zarządzania konfiguracją jest zdefiniowanie standardów dla sprzętu i oprogramowania, które ma działać w danej sieci. System standardowy, który został przetestowany i certyfikowany, tworzy rodzaj platformy wzorcowej. System ten może być następnie powielony bądź sklonowany, co zmniejsza ilość pracy, jaką trzeba włożyć w konfigurację poszczególnych systemów.

Większość pakietów zarządzania systemami wykorzystuje konsolę w celu monitorowania sieci i zarządzania nią. Poniżej zostaną przedstawione niektóre powszechnie spotykane aspekty konsoli. Kluczowym zadaniem zarządzania jest zarządzanie cyklami żywotnymi systemów sieciowych. To zagadnienie będzie omówione dalej.

### Konsole

Lokalne zarządzanie konfiguracją jest uciążliwe, tak więc większość zadań zarządzania to rozwiązania zdalne, najczęściej realizowane w scentralizowanej konsoli zarządzania lub tzw. dashboardzie. Dashboard długo był podstawową funkcją platform zarządzających, ale obecnie występuje również jako funkcja zarządzania w systemach operacyjnych. Firma Microsoft, kontynuując prace rozwojowe nad konsolą MMC, była w stanie skonsolidować większość narzędzi zarządzających dla sieciowego systemu operacyjnego w postaci konsoli w Windows Server 2008, która ma nazwę Menedżer serwera (rysunek 30.2).



**Rysunek 30.2.** Menedżer serwera w systemie Windows Server 2008 to aplikacja konsoli MMC, która pomaga w zapanowaniu nad chaosem

Struktura aplikacji Menedżer serwera wyświetla w panelu znajdującym się po lewej stronie hierarchiczne drzewo zawierające rozwijane widoki dziesiątek narzędzi, pozwalając administratorowi na zarządzanie systemami lokalnymi i zdalnymi z jednego miejsca. Po kliknięciu ikony narzędzia, na przykład Monitora wydajności, wyświetla się ono w centralnym panelu konsoli. Wprawdzie nie zostało to pokazane na powyższym rysunku, ale kiedy narzędzie ma dostępne opcje, po prawej stronie pojawia się trzeci panel, zawierający odpowiednie polecenia. Używając Menedżera serwera, można jednocześnie mieć otwartych kilka z tych narzędzi, na przykład narzędzie konfiguracyjne Active Directory, narzędzie konfiguracyjne zasad zarządzania grupami oraz inne, i zapisać konfigurację w celu późniejszego jej wykorzystania.

Chociaż inne funkcje systemu Windows Server 2008, takie jak powłoka PowerShell, mogą w dłuższej perspektywie wydawać się znacznie ważniejsze, z administracyjnego punktu widzenia żadna inna funkcja nie ma równie dużego znaczenia jak konsolidacja narzędzi w ramach Menedżera serwera. Nie oznacza to, że konsola ta ma unikalny układ lub wnosi coś zupełnie nowego; po prostu ma wszechstronne zastosowanie i stanowi część systemu, którą administrator na pewno będzie wykorzystywał.

Centralna konsola zapewnia oszczędność czasu, a staranność wykonania i jakość tego rodzaju konsoli to cechy pożądane w każdym narzędziu zarządzającym. Wszystkie platformy sieciowe omówione w dalszej części tej książki dostarczają aplikację w postaci kontenera, taką

jak konsola MMC, w której można instalować narzędzia. Niektóre z tych pakietów zarządzających są rozwiązaniami zamkniętymi i własnościowymi, ale wielu producentów tych platform publikuje API, pozwalając w ten sposób firmom trzecim na tworzenie modułów przeznaczonych dla danej platformy.



Na stronie [http://msdn.microsoft.com/en-ul/library/ms692755\(VS.85\).aspx](http://msdn.microsoft.com/en-ul/library/ms692755(VS.85).aspx) firma Microsoft opublikowała informacje dotyczące interfejsu pozwalającego na tworzenie modułów do konsoli MMC.

## Cykl życiowy oprogramowania i wdrażanie

Całe oprogramowanie i sprzęt są użyteczne do momentu zakończenia ich cyklu życiowego. Celem zarządzania konfiguracją jest zagwarantowanie, że cykl życiowy komponentów sieciowych będzie maksymalnie długi.

Systemy — obejmujące zarówno oprogramowanie, jak i sprzęt — przechodzą przez sześć etapów, czyli stanów. Stany te zostaną przedstawione poniżej w kolejności od początku do końca cyklu życiowego systemu. Wszystkie one mają różne wymagania w stosunku do oprogramowania służącego do zarządzania konfiguracją. Wprawdzie każdy pakiet zarządzający inaczej obsługuje konfigurację, ale istnieją pewne cechy wspólne, które mogą być powiązane z każdym etapem. Technologia wdrażania — określana również mianem ESD (ang. *Electronic Software Distribution*), zarządzaniem biurowym lub zautomatyzowanym dostarczaniem oprogramowania — to podstawowa funkcja pożądana w technologii platformy sieciowej. Jeżeli funkcja ta nie znajduje się w podstawowym pakiecie platformy, to najczęściej jest pierwszym kupowanym modułem.

### Etap 1. Nowo kupowane systemy oraz istniejące

Na pierwszym etapie pakiet zarządzania konfiguracją musi zostać dodany do nowego systemu i uzyskać możliwość monitorowania systemu. Jeżeli nowy system nie został zakupiony jako w pełni zainstalowany, oprogramowanie zarządzające musi mieć możliwość przeprowadzenia konfiguracji systemu zgodnie z opisem przedstawionym w etapie drugim. Na pierwszym etapie pakiet zarządzający musi mieć również możliwość instalacji agenta oraz rejestracji różnych właściwości systemu w bazie danych zasobów. Wśród wielu właściwości, które mogą być przechowywane w celu ich przeglądania, znajdują się:

- ♦ identyfikator zasobu lub numer rejestracyjny dla oprogramowania;
- ♦ numery seryjne i rodzaje komponentów powiązanych z systemem;
- ♦ dokładny model lub nazwa produktu, a także numer jego wersji;
- ♦ przypisane wartości takie jak nazwy systemu przechowywane w usłudze katalogowej.

Nie wszystkie platformy zarządzające są dostarczane z pełnymi modułami rozliczeń i inwentaryzacji. W niektórych systemach będą to moduły dodatkowe, które trzeba zakupić oddzielnie. Jednak wszystkie platformy zarządzające wymagają pewnych form identyfikacji systemów w celu zachowania możliwości identyfikacji poszczególnych systemów, które są przeznaczone do wdrożenia bądź aktualizacji. Nie wszystkie systemy wymagają zarządzania. Z punktu widzenia kosztów lub bezpieczeństwa może być nawet wskazane, aby niezarządzane systemy zostały odizolowane od monitorowania z zewnątrz.

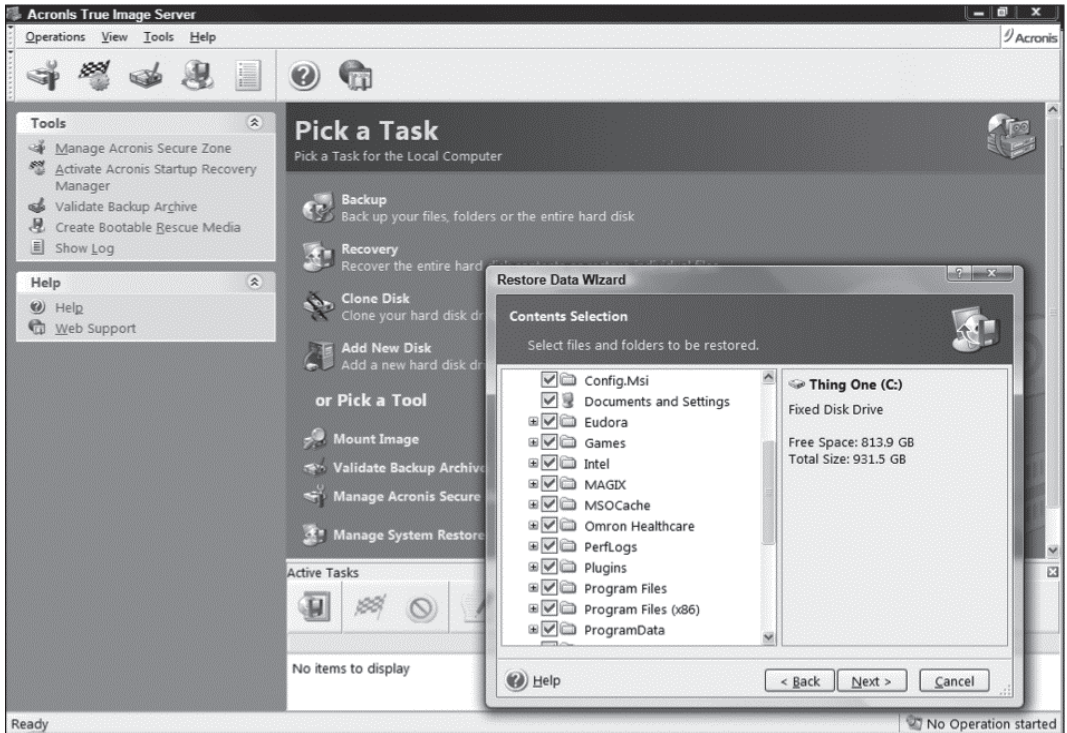
## **Etap 2. Systemy zinwentaryzowane lub przeznaczone do implementacji**

Oprogramowanie do zarządzania konfiguracją może tworzyć i przechowywać stany systemów w postaci możliwych do instalacji pakietów oprogramowania określonego typu albo pełnych systemów komputerowych zapisanych w pliku kontenera, który bardzo często jest nazywany plikiem obrazu. Większość osób zna różne pliki obrazów, które dostarczane są w różnorodnych postaciach. Najbardziej znane pliki obrazów to pliki w formacie ISO (ang. *International Organization for Standardization*). Pliki ISO są czasami nazywane plikami archiwów lub obrazami dysków, a ich definicja wynika ze sposobu organizacji systemu plików ISO 9660 na płytach CD-ROM. System plików 9660 został zastąpiony przez *Universal Disk Format* (UDF; ISO/IEC 13346, czyli ECMA-167), opracowany przez Optical Storage Technology Association (OSTA) i przeznaczony do używania w przypadku każdego rodzaju nośników optycznych.

Inne formaty plików obrazów obejmują pliki Microsoft Windows Imaging Format (WIM), pliki GHO, czyli Symantec Ghost (ang. *General Hardware Oriented System Transfer*), pliki Acronis True Image Server oraz wiele innych. Wszystkie wymienione formaty plików mają zaimplementowane pewne ogólne koncepcje w postaci właściwości — przechowują możliwości do przeglądania indeksu opisującego zawartość poszczególnych plików, katalogów lub napędów w danym obrazie. Ponadto zawierają dane przechowywane w postaci oryginalnej (a więc możliwej do bezpośredniego kopiowania) albo skompresowanej. W tym drugim przypadku dane muszą być wydodrężnione w trakcie procesu przywracania zawartości obrazu. Ponieważ pliki obrazów są kontenerami, większość narzędzi pozwala na dodawanie treści lub usuwanie plików z obrazów. Tym samym dostarczają możliwość tworzenia migawki dysku, własnych instalacji na podstawie podzbioru plików znajdujących się w obrazie oraz wiele innych funkcji. Na rysunku 30.3 pokazano plik TIB programu Acronis, czyli rodzimy plik Acronis w formacie True Image Backup.

Używanie plików obrazów w celu instalacji systemów operacyjnych miało bardzo interesujący wpływ na sposób, w jaki firma Microsoft obecnie rozprowadza różne wersje systemu Windows. W systemach Windows wcześniejszych niż Windows Server 2008 i Vista różne wersje wymagały oddzielnych nośników instalacyjnych. Począwszy od wersji 2008, firma Microsoft skonsolidowała wszystkie pliki w jeden plik kontenera WIM i pozwala użytkownikowi na wybór wersji. Stosowanie jednego nośnika dla wszystkich wersji jest korzystne ze względów ekonomicznych.

Pliki obrazów są używane nie tylko przez narzędzia do tworzenia kopii zapasowych, ale stanowią główny element wszystkich narzędzi służących do wdrażania gotowych rozwiązań. W ściśle zarządzanej sieci organizacje pozyskują nowe systemy i weryfikują konfiguracje, które chcą obsługiwać. Uzyskane w taki sposób systemy wzorcowe są następnie wdrażane w sieci. System wzorcowy może zawierać pewne ograniczenia — celem takiego podejścia jest zmniejszenie liczby problemów, z którymi później musi zmagać się personel IT. Ograniczenia mogą dotyczyć na przykład obsługi jedynie danego sprzętu i oprogramowania, uprawnień użytkownika i dostępnych dla niego funkcji oraz mogą określać oprogramowanie, które może być instalowane. Wdrożenie zwykle polega na dostarczeniu skryptu wskazującego plik obrazu znajdujący się w sieci i zapewnieniu wymaganego stopnia automatyzacji całego procesu.



**Rysunek 30.3.** Pliki Acronis True Image Backup (TBI) są plikami obrazów dysku, które mogą być używane w celu tworzenia kopii zapasowej i przywracania danych, klonowania systemów operacyjnych oraz przeprowadzania innych wdrożeń

Firma Microsoft dostarcza pewnego zestawu sieciowych narzędzi służących do wdrażania systemów. Narzędzia te są dostępne w postaci platformy Microsoft Deployment Toolkit<sup>2</sup> (<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=3bd8561f-77ac-4400-a0c1-fe871c461a89&displayLang=en>). Za jej pomocą można przeprowadzić wdrożenie systemów operacyjnych Windows Server 2003, XP oraz Windows Server 2008, Vista i Windows 7 z plików obrazów dostosowanych do własnych potrzeb z uwzględnieniem odpowiednich sterowników, pakietów Windows Update, dodatków Service Pack, a także zainstalowanych aplikacji Microsoft Office itp. Wymieniony pakiet narzędziowy jest doskonałym sposobem poznania technologii wdrażania. Wiele przedstawionych tutaj rozwiązań ma zastosowanie również w innych dostępnych pakietach służących do zarządzania wdrożeniami.

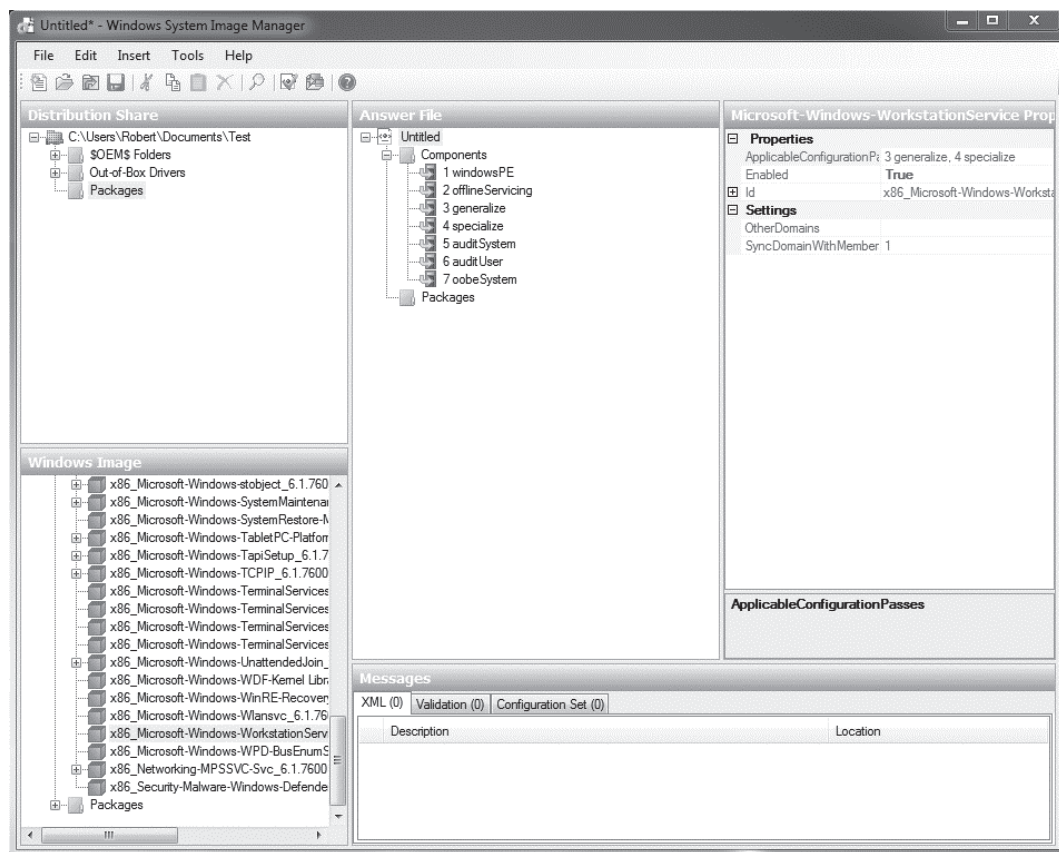
Pakiet Microsoft Deployment Toolkit zawiera następujące narzędzia służące do przeprowadzania wdrożeń:

- ♦ **Application Compatibility Toolkit** — przeprowadza porównanie aplikacji z bazą danych zgodności.
- ♦ **Microsoft Assessment and Planning** — porównuje sprzęt z listą zgodności (ang. *Hardware Compatibility List*).

<sup>2</sup> Wprowadzenie w języku polskim do platformy Microsoft Deployment Toolkit można znaleźć na stronie <http://www.microsoft.com/poland/technet/article/art0173.mspx> — przyp. tłum.

- ♦ **Microsoft Deployment Workbench** — interfejs podobny do przeglądarki internetowej dla wszystkich narzędzi oraz odnośników do zasobów dokumentacji takich jak białe księgi lub najlepsze praktyki.
- ♦ **Windows Automated Installation Kit (WAIK)** — zestaw narzędzi służący do tworzenia i wdrażania obrazów systemów. W skład narzędzi wchodzi Windows System Image Manager do zarządzania biblioteką obrazów, ImageX, czyli narzędzie wiersza poleceń do tworzenia obrazów, Windows Preinstallation Environment (Windows PE) oraz narzędzie User State Migration Tool (USMT) służące do przechwytywania informacji profilu użytkownika.
- ♦ **Windows Deployment Services** — nowa wersja serwera Microsoft Remote Image Server.

Na rysunku 30.4 pokazano narzędzie Windows System Image Manager. Pozwala ono na wybór obrazu systemu w formacie Windows WIM, dostosowanie tego obrazu do własnych potrzeb przez dodanie sterowników i pakietów instalacyjnych, zbudowanie „plików odpowiedzi” (będących skryptami wymaganymi do uruchamiania zautomatyzowanych instalacji Windows) oraz konfigurację udziałów sieciowych służących jako udziały dystrybucyjne podczas instalacji sieciowej.



**Rysunek 30.4.** Narzędzie Windows System Image Manager

Po przeprowadzeniu konfiguracji w narzędziu Microsoft Deployment Toolkit obraz może być przeznaczony do wdrożenia za pomocą metody Zero Touch (proces zautomatyzowany, niewymagający interakcji ze strony użytkownika) lub Lite Touch (konfiguracja ręczna wdrożenia na życzenie administratora). Utworzone obrazy mogą być wdrażane za pomocą Microsoft System Center Configuration Manager 2007 lub wcześniejszej wersji tego pakietu zarządzającego, czyli Microsoft System Management Server 2003 (SMS).

Jeżeli sprzęt na to pozwala, to wszystkie ostatnie wersje komputerów obsługują tryb pracy PXE (ang. *Preboot Execution Environment*). W przypadku systemu skonfigurowanego do uruchomienia w trybie PXE po włączeniu takiej możliwości w BIOS-ie komputer zostanie uruchomiony pod kontrolą minimalnego systemu operacyjnego i rozpocznie proces przywracania danych z serwera PXE przez sieć. Jeżeli system wykryje serwer PXE, to nastąpi wymiana danych uwierzytelniających i rozpocznie się proces przesyłania obrazu całego systemu operacyjnego przez sieć z serwera do klienta. Tryb pracy PXE jest używany w aplikacjach cienkich klientów-serwerów, ale może być zastosowany także do zdalnego wdrożenia obrazu dysku na zwykłym komputerze.



Jeżeli intencją jest przywrócenie systemu z powrotem do takiego samego stanu po zakończeniu sesji użytkownika, to istnieją znacznie lepsze sposoby odświeżenia systemu niż przeprowadzanie operacji przywracania go z obrazu przez sieć. W takich sytuacjach warto rozważyć użycie narzędzia Faronics Deep Freeze (<http://www.faronics.com/>). Dzięki temu można uniknąć konieczności obsługi przesyłania gigabajtów danych.

Oprogramowanie służące do zarządzania konfiguracją może pomóc w testowaniu i weryfikacji standardowych systemów wzorcowych, w zarządzaniu biblioteką obrazów oraz podczas przeprowadzania zdalnych instalacji tych obrazów w sieci.

### **Etap 3. Systemy się starzeją i muszą być monitorowane**

Oprogramowanie służące do zarządzania konfiguracją nie tylko dostarcza możliwości zarządzania zasobami (co zostanie omówione w dalszej części rozdziału), ale również pozwala na podejmowanie decyzji na podstawie wieku, stopnia wykorzystania, wymagań licencyjnych oraz wydajności systemu. Na rynku dostępna jest duża liczba pakietów służących do monitorowania sieci. Do najważniejszych funkcji pakietów monitorujących zaliczamy:

- ♦ automatyczne wykrywanie urządzeń (niemal wszystkie programy monitorujące używają protokołu SNMP) i mapowanie;
- ♦ instalacja agenta i monitorowanie rozproszone;
- ♦ rejestracja zdarzeń, obsługa wyzwalaczy i powiadomień;
- ♦ trendy w danych, tworzenie wykresów i raportów (to obejmuje również umowy SLA, ang. *Service Level Agreement*) oraz przewidywanie;
- ♦ inwentaryzacja;
- ♦ zgodność licencji;
- ♦ obsługa skryptów i możliwości rozbudowy za pomocą rozszerzeń, dodatków itd.;
- ♦ interfejs sieciowy.

Różne pakiety obsługują określone zestawy funkcji wymienionych na powyższej liście.



Porównanie różnych systemów do monitorowania sieci można znaleźć na stronie [http://en.wikipedia.org/wiki/Comparison\\_of\\_network\\_monitoring\\_systems](http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems). Inna strona z informacjami na temat narzędzi monitorujących dostępna jest na witrynie Stanford SLAC pod adresem <http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html>.

#### **Etap 4. System wymaga poprawki lub konieczne jest wprowadzenie drobnego uaktualnienia**

Kiedy w organizacji znajdują się różne systemy, w których trzeba instalować poprawki, przeprowadzać aktualizację aplikacji lub instalować pełne dodatki typu Service Pack, po prostu zezwala się użytkownikom lub systemom na automatyczną aktualizację. Jednak poprawki, uaktualnienie oraz inne oprogramowanie wymagane do wdrożenia w systemie produkcyjnym najlepiej jest skonfigurować za pomocą oprogramowania nadzorującego politykę bezpieczeństwa. Można wtedy zdefiniować reguły określające, kto i kiedy ma dostęp do danego oprogramowania, a także wykorzystać skrypt lub zautomatyzować te aktualizacje jako instalacje sieciowe. W starannie zarządzanych sieciach każde uaktualnienie aplikacji jest dokładnie testowane przed wdrożeniem.

#### **Etap 5. System jest przestarzały i musi być uaktualniony**

Komputery wyprodukowane w ciągu ostatnich kilku lat bardzo często mają większe możliwości niż systemy operacyjne, z którymi zostały dostarczone. Dlatego też jest całkiem możliwe, że wraz z wiekiem systemu jego uaktualnienie może przynieść dodatkowe korzyści. Istnieją trzy metody uaktualniania systemu:

- ♦ **Od zera.** Ta metoda polega na usunięciu wszystkich poprzednich danych i instalacji systemu od zera wraz z wszystkimi używanymi programami.
- ♦ **Bezpośrednie uaktualnienie.** Uaktualnienie systemu następuje przez instalację nowej wersji bezpośrednio na starej. W przypadku większości sieciowych systemów operacyjnych i aplikacji taka metoda uaktualnienia jest obsługiwana, jeżeli wersje nie różnią się zbyt wiele od siebie; pozostają wtedy ustawienia użytkownika.
- ♦ **Uaktualnienie typu „jeden przy drugim”.** W takiej metodzie uaktualnienia wszystkie aplikacje i ustawienia są przenoszone ze starego systemu do systemu zawierającego nowszą wersję systemu operacyjnego. Ten rodzaj uaktualnienia jest najtrudniejszy do przeprowadzenia.

Warto pamiętać, że instalacja typu „od zera” daje najczystszy i najbardziej stabilny system, ale nie zachowuje przy tym konfiguracji systemu wprowadzonej wcześniej przez użytkownika. Bezpośrednie uaktualnienie jest kompromisem — jego wynikiem jest funkcjonujący system, który może wymagać dodatkowej pracy w celu wyeliminowania usterek. Natomiast uaktualnienie typu „jeden przy drugim” jest najtrudniejsze do przeprowadzenia i wymaga dodatkowego, specjalnego oprogramowania, które porównuje aplikacje z bazą danych, zawierającą znane i zgodne wersje oprogramowania.

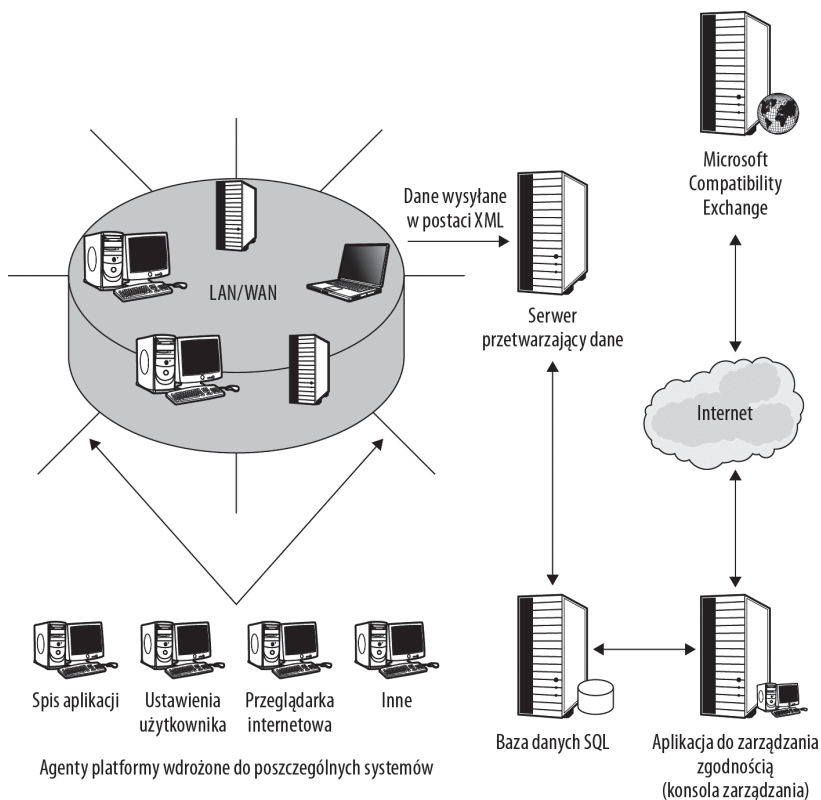
W technologii wdrożeń opracowanej przez Microsoft narzędzie Application Compatibility Toolkit (ACT) przeprowadza operację weryfikacji oprogramowania. Narzędzie ACT instaluje w aktualizowanym systemie zestaw agentów, których zadaniem jest zebranie informacji o systemie. Następnie informacje te są porównywane w konsoli zarządzania, która będzie zawierała także informacje pochodzące z usługi Microsoft Compatibility Exchange.

Usługa ta dostarcza również zasoby, które można wykorzystać do uzyskania dodatkowych informacji na temat zgodności określonego oprogramowania, a także prowadzi do forów, gdzie inni profesjonalści wymieniają się swoimi doświadczeniami. W celu instalacji agentów ACT i zarządzania tym procesem można wykorzystać Microsoft System Center Operations Manager (SCOM).

Na rysunku 30.5 pokazano sposób funkcjonowania narzędzia ACT w połączeniu z usługą Microsoft Compatibility Exchange, działającą przez konsolę zarządzania. Na rysunku 30.5 systemy w sieci LAN/WAN mają zainstalowany zestaw agentów: spis aplikacji, ustawienia użytkownika, przeglądarkę internetową i inne. Agenty dostarczają informacji o stanie poszczególnych systemów i mogą wysyłać dane w postaci XML do serwera przetwarzającego dane, który przechowuje je w bazie danych SQL. Są one wykorzystywane przez serwer aplikacji do zarządzania zgodnością (Application Compatibility Manager) w celu określenia (w połączeniu z usługą Microsoft Compatibility Exchange) kroków, które muszą być podjęte, aby usunąć mankamenty.

### Rysunek 30.5.

*Narzędzie Microsoft ACT to bazujący na agentach system inwentaryzacji sieciowej, działający w połączeniu z Microsoft System Center, używany do sprawdzania zgodności aplikacji podczas procesu uaktualniania*



Uaktualnienia, podobnie jak inne wdrożenia systemu operacyjnego, są instalowane poprzez sieć za pomocą narzędzi zarządzających. Jednak w przeciwieństwie do czystych instalacji operacja uaktualniania systemu często wymaga narzędzi sieciowych służących do przechwylenia, przechowania i przywrócenia zarówno ustawień personalizacyjnych, jak i danych użytkownika ze starego systemu do uaktualnianego. Ustawienia te są „stanem użytkownika”, który jest nie tylko profilem użytkownika (na przykład katalog *Documents and Settings*

w systemie Windows), ale także jego danymi. Kiedy system obsługuje wielu użytkowników, konieczne jest przechwycenie stanu wszystkich użytkowników. Technologia wdrożeń opracowana przez firmę Microsoft oferuje narzędzie wiersza poleceń o nazwie *scanstate*, służące do przechwytywania stanu użytkowników, oraz narzędzie *loadstate* do przywracania stanu użytkowników.

### **Etap 6. System jest przestarzały i musi zostać zastąpiony nowym**

Ostatni etap to uznanie, że system nie jest dłużej użyteczny. Systemy, które zakończyły swój cykl życiowy, mogą znaleźć zastosowanie w obsłudze mniej wymagających aplikacji, na przykład jako routery, systemy PBX itp. Niektóre systemy mogą być przydatne dla innych użytkowników, a inne powinny być po prostu usunięte.

## **Zarządzanie rozliczeniami i administracja**

Funkcja zarządzania rozliczeniami w narzędziach zarządzających odnosi się do pomiaru stopnia wykorzystania danych. Pomiary te są potrzebne do sporządzania rachunków dla klientów lub wydziałów, zagwarantowania, że usługi są dystrybuowane prawidłowo, oraz do weryfikacji spełniania warunków umów SLA (ang. *Service Level Agreement*) dla usług sieciowych. Usługi rozliczeniowe polegają na trendach danych dostarczanych przez narzędzia monitorujące wydajność wraz z dodatkową możliwością określenia, którzy użytkownicy (grupy) są odpowiedzialni za daną czynność albo są jej beneficjentami.

Przykładami funkcji sieciowych wykorzystywanych do zbierania informacji w celach rozliczeniowych są:

- ♦ ilość danych przekazanych w ramach połączenia;
- ♦ ilość poszczególnych zdarzeń powiązanych z czynnością, na przykład tworzeniem zdalnego połączenia;
- ♦ ilość wykorzystanych określonych zasobów sieciowych, na przykład udziałów dyskowych;
- ♦ wartości szczytowe podczas używania usług.

Funkcje rozliczeniowe są wbudowane w różne protokoły, między innymi RADIUS, TACACS oraz Diameter, które często są określane mianem usług AAA. AAA oznacza *Authentication* (uwierzytelnianie), *Authorization* (autoryzacja) i *Accounting* (rozliczenia). Na przykład RADIUS (*Remote Authentication Dial-In User Service*) to protokół połączenia używany przez dostawcę usług internetowych (ISP), usługi poczty e-mail, sieciowe punkty dostępowe, serwery WWW oraz inne funkcje sieciowe, w których konieczne jest zapewnienie bezpieczeństwa i przeprowadzanie operacji rozliczeniowych. Usługa AAA zazwyczaj działa przez przekazanie pewnych funkcji, na przykład autoryzacji, do innych usług sieciowych.

Rozliczenia są dostępne w wielu aplikacjach platform sieciowych, chociaż najczęściej funkcja ta jest kupowana jako moduł dodatkowy i nie stanowi części produktu podstawowego, który można kupić od producenta. Wyjątkami od tej reguły są produkty platform sieciowych oferujących usługi, na przykład te, które zostały wymienione w poprzednim akapicie.

Ponieważ wiele sieci nie wymaga funkcji rozliczeniowych, pojęcie *administracja* zostało użyte jako alternatywne w celu otrzymania akronimu FCAPS. Funkcje administracyjne obejmują zarządzanie użytkownikami i grupami, ustawianie uprawnień do zasobów, zapewnianie dostępu do ważnych funkcji sieciowych, takich jak konfiguracja polityki, a także do wykonywania kopii zapasowej lub przeprowadzania replikacji, zarządzania kopiami zapasowymi, konfigurowania pamięci masowej itp. Funkcje administracyjne w różnych narzędziach platform sieciowych mogą istotnie się różnić. Ponadto w pewnym zakresie funkcje administracyjne nakładają się na inne obszary modelu FCAPS, na przykład na bezpieczeństwo i konfigurację.

## Zarządzanie wydajnością

Celem zarządzania wydajnością jest określenie sposobu działania sieci w warunkach standardowych, jak również umożliwienie przeprowadzenia optymalizacji wydajności. Pomiar wydajności sieci tworzy podstawę, z którą będą porównywane późniejsze zmiany. Monitorowanie wydajności wymaga używania liczników i agentów w celu ilościowego pomiaru informacji dostarczanych przez system. Dane zbierane przez narzędzia do monitorowania wydajności pomagają w przeprowadzaniu pomiarów szerokiej gamy czynników, które wpływają na sieć. Poniżej wymieniono pewne najważniejsze funkcje monitorowania wydajności:

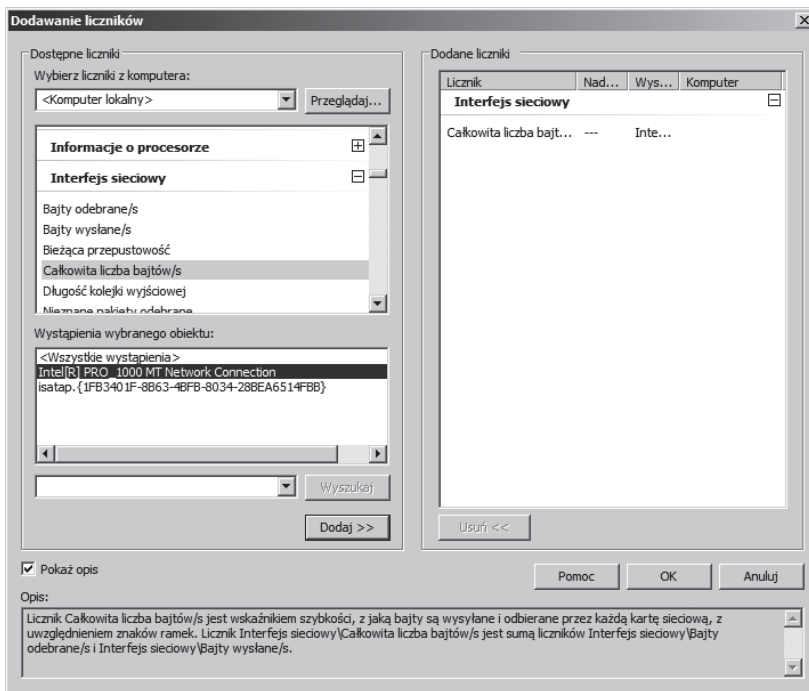
- ♦ ruch sieciowy jako funkcja użytego protokołu;
- ♦ obciążenie sieci i przepustowość węzła bądź segmentu;
- ♦ współczynnik kolizji;
- ♦ współczynniki błędów ramki;
- ♦ ruch sieciowy jako funkcja węzła.

Kluczem do pracy z narzędziem monitorującym wydajność jest zrozumienie sposobu używania liczników. Liczniki odgrywają istotną rolę podczas tworzenia systemu operacyjnego. Kiedy programiści „budują” system operacyjny, umieszczone przez nich liczniki w różnych modułach systemu operacyjnego dostarczają programistom natychmiastowych danych na temat zmian wprowadzonych w programach. Tak więc oprócz przechwytywania i rejestrowania zdarzeń niektóre typy zdarzeń są mierzone pod kątem częstotliwości, czasu trwania, wartości lub pod kątem innego parametru, który jest najbardziej potrzebny do zrozumienia danego podsystemu monitorowanego przez ten licznik. W przypadku procesorów liczniki monitorują stopień wykorzystania procesora, długość kolejki procesora, czas procesora itd. Z kolei w przypadku dysków liczniki będą monitorowały dostęp do dysku, ilość przekazanych danych, długość kolejki itd. Po uruchomieniu aplikacji monitorującej wydajność systemu, a każdy system operacyjny ma taki program, wyświetlane tam dane bazują właśnie na wspomnianych licznikach. Każda aplikacja, która została zoptymalizowana pod kątem wydajności, ma zestaw używanych liczników. Ponadto liczniki są dostępne w większości aplikacji klasy przemysłowej, na przykład w ogromnych bazach danych.

Na rysunku 30.6 pokazano okno dialogowe *Dodawanie liczników* w narzędziu Monitor wydajności znajdującym się w systemie Windows Server. Wiele obiektów, których wydajność może zainteresować użytkownika, na przykład interfejsy sieciowe, oferuje pewną liczbę wartości parametrów dostarczanych przez liczniki. Dodawane liczniki pojawiają się w Monitorze wydajności jako wykresy.

**Rysunek 30.6.**

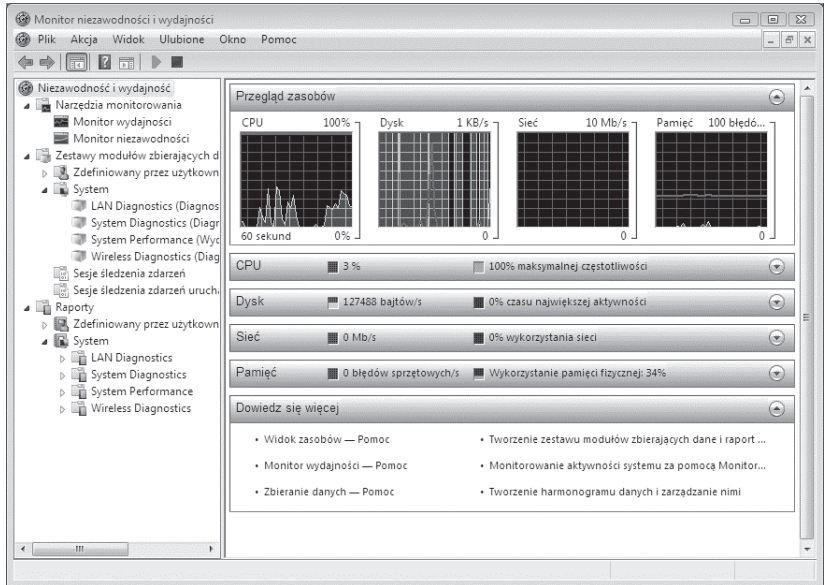
*W celu pomiaru różnych aspektów wydajności systemu i liczników do narzędzia monitorującego wydajność można dodawać liczniki*



Jeżeli Czytelnik pracował już z narzędziem służącym do pomiaru wydajności, to już wie, że pierwsza operacja wyboru obserwowanych liczników powoduje wyświetlenie długiej listy zorganizowanej według klas i że następnie trzeba poczekać na dane spływające do narzędzia. Różne systemy operacyjne nadają licznikom różne nazwy i udostępniają różne zestawy zainstalowanych liczników, ale stosowana koncepcja pozostaje niemal taka sama. Wiele liczników nie jest udostępnianych użytkownikowi, ponieważ ich włączenie ma wpływ na wydajność systemu. Na przykład firma Microsoft nie udostępnia niektórych liczników dysków i jeżeli użytkownik jest nimi zainteresowany, to w pierwszej kolejności musi wiedzieć o ich istnieniu, a następnie je zainstalować. Różni producenci aplikacji stosują odmienne polityki dotyczące używania oferowanych liczników. Niektórzy je udostępniają, inni wręcz przeciwnie. Niestety, wielu producentów aplikacji nie zadaje sobie trudu zoptymalizowania ich wydajności i w ogóle nie dostarcza żadnych liczników. Aby dowiedzieć się więcej na temat liczników, trzeba poszukać nieco informacji na temat danego produktu.

Analiza wydajności za pomocą narzędzia służącego do monitorowania wydajności może być nieocenioną pomocą w wykrywaniu usterek sieci i systemu. Najczystszy obraz sytuacji uzyskuje się przez analizę typów zdarzeń, jak również wartości metrycznych w tych zdarzeniach. Mówiąc najogólniej, narzędzia do zarządzania siecią są albo monitorem zdarzeń albo monitorem wydajności. Kilka takich narzędzi jest i jednym, i drugim. Każdy sieciowy system operacyjny jest dostarczany wraz z monitorem wydajności. Monitor wydajności w Windows to perfmon; jest on modulem konsoli MMC, który może być uruchomiony jako samodzielne narzędzie, jako komponent Menedżera zadań Windows (narzędzie dostępne po naciśnięciu klawiszy *Ctrl+Alt+Del*) lub jako część narzędzia Monitor niezawodności i wydajności (rysunek 30.7) dostarczanego wraz z systemami Windows Server 2008 i Vista.

**Rysunek 30.7.**  
*Aplikacja Monitor niezawodności i wydajności w systemie Windows Vista zawiera zarówno narzędzie perfmon, jak i narzędzia menedżera usterek*



Jedną z klas narzędzi służących do monitorowania wydajności sieci jest sniffer. Narzędzie to jest znane pod różnymi nazwami: analizator pakietów, analizator sieciowy, sniffer pakietów, sniffer Ethernet i analizator protokołu. Sniffer pakietów przechwytytuje ruch sieciowy przechodzący przez sieć, tak że zawartość może być odczytana, przeanalizowana i zapisana w pliku dziennika zdarzeń. Sniffer pakietów ma również możliwość dekodowania zawartości pakietu oraz kategoryzowania natury używanych protokołów.

#### Ostrzeżenie

Sniffer pakietów to broń wybierana przez wielu hakerów. Po instalacji tego rodzaju programu trzeba się upewnić, że nieupoważniony personel nie uzyska dostępu do tego typu narzędzia znajdującego się w danej sieci.

Sniffer pakietów może być skonfigurowany w taki sposób, aby przechwytywał ruch sieciowy w segmencie, porcie przełącznika sieciowego, routerze lub komputerze lub w innym miejscu uznanym za port monitorowania. Port monitorowania pobiera wszystkie pakiety przychodzące do przełącznika sieciowego i je powiela. Pakiety oryginalne są wysyłane do miejsca przeznaczenia, natomiast powielone są przekazywane do analizy. W przypadku sieci bezprzewodowych sniffer Wi-Fi zwykle przechwytytuje ruch na danym kanale. Sniffery pakietów zaliczają się do najczęściej używanych dostępnych obecnie narzędzi monitorujących wydajność i mogą być wykorzystane do wielu różnych zadań, między innymi:

- ♦ analizy usterek sieci;
- ♦ wykrywania naruszenia bezpieczeństwa;
- ♦ zbierania danych statystycznych dotyczących wykorzystania sieci, do tworzenia raportów oraz optymalizacji wydajności;
- ♦ ustalania używanych protokołów oraz filtrowania pakietów na podstawie reguł;
- ♦ przechwytywania sesji.

Istnieje spora liczba snifferów pakietów, które można pobrać z internetu; większość z nich jest dostępna bezpłatnie. Microsoft Network Monitor (NETMON; <http://www.microsoft.com/downloads/en/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f&displaylang=en>) to prawdopodobnie najbardziej znany sniffer używany w systemie Windows. Kismet, tcpdump oraz Wireshark to programy dostępne dla systemów Windows, Mac OS X, Linux, BSD i Solaris. Firma Sun<sup>3</sup> rozprowadza program SNOOP będący snifferem pakietów dla systemu Solaris.

Wysokiej jakości komercyjnym snifferem pakietów jest OmniPeek firmy WildPackets (<http://www.wildpackets.com/>), będący połączeniem serwera sieciowego (sprzęt) i pakietu oprogramowania. OmniPeek jest dostarczany z rozszerzeniem API, które pozwala na zautomatyzowanie monitorowania sieci. Gdy powstawała ta książka, ceny OmniPeek rozpoczynały się od poziomu 1200 dolarów za zestaw z wymienionym rozszerzeniem. Zestaw umożliwia zdalne monitorowanie przełączników sieciowych i punktów dostępowych Cisco, komputerów pracujących pod kontrolą systemu Linux oraz urządzeń sieciowych innych producentów. Urządzenia sprzętowe tego typu są często nazywane systemami zarządzania siecią (ang. *Network Management Systems* — NMS).

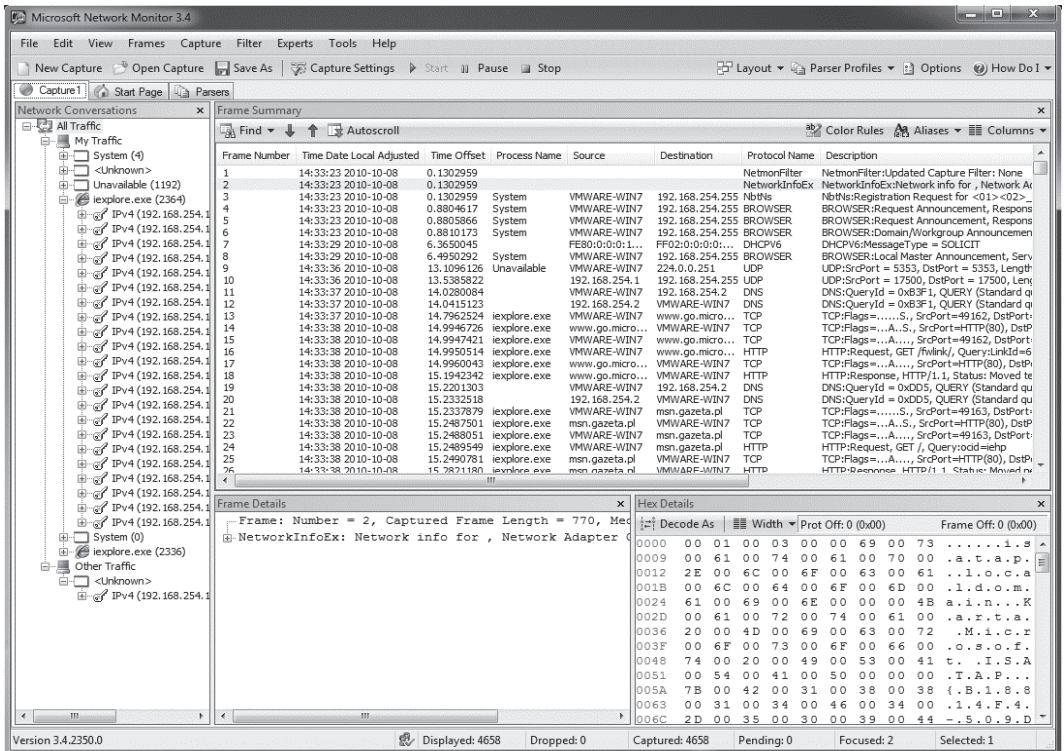
Na rysunku 30.8 pokazano sesję przechwyconą w programie Microsoft Network Monitor. Panel znajdujący się po lewej stronie pokazuje różne punkty końcowe ruchu sieciowego, podczas gdy panel środkowy po prawej stronie zawiera dane pochodzące z rzeczywistych pakietów. Aplikacja Network Monitor może działać w trybie nazywanym Promiscuous Mode, w którym można wyświetlać pełną treść pakietów.

## Zarządzanie bezpieczeństwem

Funkcja zarządzania bezpieczeństwem w sieciowych narzędziach zarządzających zapewnia możliwość udzielenia bądź odmowy dostępu użytkownikom lub grupom do zasobów sieciowych. Większość sieciowych systemów operacyjnych oferuje funkcję zarządzania bezpieczeństwem jako komponent systemu operacyjnego. Dlatego też w tych systemach operacyjnych oprogramowanie służące do zarządzania bezpieczeństwem daje możliwość dostępu do ustawień systemowych i ich modyfikacji. To może oznaczać, że narzędzie pozwoli na przeglądanie ważnych ustawień sieciowych przechowywanych w usłudze katalogowej, umożliwi uzyskanie dostępu do zmiennych środowiskowych systemów oraz innych funkcji. W przypadku systemów sieciowych, które nie posiadają usług katalogowych, narzędzie zarządzania bezpieczeństwem może dostarczać kompletne rozwiązanie w tym zakresie.

Bezpieczeństwo sieciowe bazuje na dwóch ważnych funkcjach: uwierzytelnianiu użytkowników i systemów oraz ochronie danych przekazywanych przez sieć za pomocą metod takich jak szyfrowanie. Oprogramowanie służące do zarządzania bezpieczeństwem może tworzyć infrastrukturę bazującą na kluczach, stosować szyfrowanie i deszyfrowanie lub wykonywać inne funkcje, które pozwolą na działanie wymienionych usług. Inną ważną kategorią usług dostarczanych przez oprogramowanie zarządzające bezpieczeństwem jest ocena i analiza ryzyka.

<sup>3</sup> Firma Sun w roku 2009 została przejęta przez Oracle — *przyp. tłum.*



**Rysunek 30.8.** Microsoft Network Monitor to sniffer pakietów, który można wykorzystać do analizy ruchu sieciowego

## Kategorie oprogramowania do zarządzania siecią

Platforma zarządzania siecią odnosi się do formy oprogramowania zarządzającego systemem, które jest wykorzystywane do zintegrowania różnych kategorii narzędzi sieciowych w ramach pojedynczego interfejsu użytkownika oraz wspólnego API aplikacji. Taka platforma dostarcza niezbędne usługi, na przykład agenty zdalnego wdrażania i agenty komunikacji sieciowej, które pozwalają na funkcjonowanie aplikacji platformy. Niektóre platformy są własnościowe i tworzą systemy zamknięte, podczas gdy inne pozostają otwarte i umożliwiają ich rozbudowę. Większość aplikacji platformy jest sprzedawanych w różnych konfiguracjach (inaczej nazywanych „poziomami”), które zwykle zawierają funkcje podstawowe i pozwalają na instalację ewentualnych rozszerzeń.

Ceny tego rodzaju systemów są zmienne i mogą zawierać koszt systemu podstawowego, zależeć od liczby konsol lub wdrożonych serwerów zarządzania; koszt licencji klientów może bazować na liczbie stanowisk lub może być stosowany niemal dowolny schemat cen. Ponieważ wiele takich instalacji jest dostosowywanych do potrzeb organizacji kupującej dany system, producenci platform zarządzania sieciowego często nie podają cen, tylko ustalają je dla poszczególnych klientów po poznaniu ich wymagań.

Ponieważ aplikacje platformy zostały zaprojektowane w sposób umożliwiający ich dostosowanie do własnych potrzeb i przez to konsolidują wiele różnego rodzaju aplikacji, opisywanie funkcji tej kategorii oprogramowania jest podobne do opisywania różnego rodzaju oprogramowania działającego pod kontrolą różnych sieciowych systemów operacyjnych. Pod pewnymi względami platformy sieciowe przypominają sieciowe systemy operacyjne z wyjątkiem tego, że sieciowe systemy operacyjne działają na wszystkich poziomach modelu sieciowego, podczas gdy platformy zarządzania sieciowego stanowią systemy warstwy aplikacji wraz z takimi elementami, jak zdalne agenty i protokoły transportu operujące na poziomie warstwy sieci lub wyższej.

Na przedstawionej poniżej liście autor spróbował uporządkować różne funkcje systemów zarządzania sieciowego, które są zwykle dostępne w przodujących na rynku produktach. Zastosowano kolejność od najczęściej implementowanych funkcji (zostały wymienione na początku listy) do najrzadziej implementowanych (na końcu listy). Przedstawiona lista ma jeszcze jedną ważną cechę: im wyższe miejsce na liście zajmuje dana funkcja, tym większe prawdopodobieństwo, że będzie znajdowała się w pakiecie podstawowym produktu platformy sieciowej. Analogicznie — im niższa pozycja danej funkcji na liście, tym większe prawdopodobieństwo, że będzie musiała zostać zakupiona oddzielnie jako moduł dodatkowy.

Funkcje zarządzania systemem dostępne w aplikacjach platformy to:

- ♦ monitorowanie aktywności użytkownika i systemu,
- ♦ monitorowanie stopnia wykorzystania zasobów sieciowych,
- ♦ zarządzanie zasobami i inwentaryzacja,
- ♦ wdrażanie systemu operacyjnego oraz oprogramowania,
- ♦ obsługa zgodności licencji,
- ♦ zarządzanie kopią zapasową,
- ♦ monitorowanie antywirusowe oraz antyspyware'owe,
- ♦ zarządzanie pamięcią masową,
- ♦ zarządzanie bezpieczeństwem,
- ♦ zarządzanie usługami katalogowymi.

## Platformy sieciowe

Platforma sieciowa to specyfikacja projektowa bazująca na opublikowanych API (ang. *Application Programming Interface* — interfejs programowania aplikacji), używanych do tworzenia oprogramowania, które może działać jednakowo w podobnych środowiskach. W kontekście systemów takich jak Microsoft .NET lub Java pojęcie platformy odnosi się do zbioru bibliotek, narzędzi, metod programowania lub skryptów oraz innych elementów wykorzystywanych do budowania modułu oprogramowania. Producenci bardzo często publikują API dla swoich platform w nadziei, że programiści będą tworzyli aplikacje użyteczne dla klientów.

Konsola Microsoft Management Console (MMC) to przykład aplikacji platformy, której celem jest dostarczenie spójnego interfejsu dla modułów. Dzięki temu konsola MMC może zostać skonfigurowana w taki sposób, aby dostarczać odpowiedniego typu narzędzia zarządzające lub konfiguracyjne wymagane przez administratora.

W tabeli 30.1 wymieniono niektóre najbardziej znane i powszechnie używane pakiety zarządzania sieciowego. Zastosowano przybliżoną kolejność na podstawie udziału poszczególnych produktów w rynku:

- ♦ Hewlett-Packard OpenView<sup>4</sup>
- ♦ Microsoft SMS/Service Center Manager
- ♦ Novell ZENworks
- ♦ BMC Patrol
- ♦ IBM Tivoli Framework
- ♦ CA NSM (poprzednio Unicenter)
- ♦ Avocent LANDesk
- ♦ Symantec Altiris

**Tabela 30.1.** *Pakiety służące do zarządzania sieciowego*

Nazwa produktu	Właściciel	FCAPS	Platforma	Witryna producenta
Altiris Management Suite	Altiris	FCAPS	Własnościowa	<a href="http://www.symantec.com/business/theme.jsp?themeid=altiris">http://www.symantec.com/business/theme.jsp?themeid=altiris</a>
CA NSM (poprzednio Unicenter Network and Systems Management)	Computer Associates	FCAPS	Własnościowa	<a href="http://www.ca.com/us/system-management.aspx">http://www.ca.com/us/system-management.aspx</a>
CiscoWorks LAN Management Solution	Cisco Systems	FCAP-	Własnościowa	<a href="http://www.cisco.com/en/US/products/ps11200/index.html">http://www.cisco.com/en/US/products/ps11200/index.html</a>
IBM Director	IBM	FC---	Własnościowa	<a href="http://www-03.ibm.com/systems/software/director/index.html">http://www-03.ibm.com/systems/software/director/index.html</a>
KACE	KACE Networks	-CA-S	Własnościowa, używa SNMP, WMI oraz PXE	<a href="http://www.kace.com/">http://www.kace.com/</a>
LANDesk Management Suite	LANDesk	FCAPS	Własnościowa	<a href="http://www.landesk.com/">http://www.landesk.com/</a>
NetDirector	Emu Software	FC--S	Własnościowa, XML-RPC	<a href="http://www.netdirector.org/">http://www.netdirector.org/</a>
Netrac	TTI Telecom	FC-P-	Własnościowa	<a href="http://www.tti-telecom.com/">http://www.tti-telecom.com/</a>

<sup>4</sup> Firma Hewlett-Packard zmieniła nazwę pakietu na rozwiązania HP Business Technology Optimization — *przyp. tłum.*

**Tabela 30.1.** Pakiety służące do zarządzania sieciowego — ciąg dalszy

Nazwa produktu	Właściciel	FCAPS	Platforma	Witryna producenta
OpenView	Hewlett-Packard	FCAPS	Własnościowa	<a href="http://www.managementsoftware.hp.com/">http://www.managementsoftware.hp.com/</a>
PATROL	BMC Software	-CAP-	Własnościowa	<a href="http://www.bmc.com">http://www.bmc.com</a>
Realité	SMILabs/ Digital Zone	-CA-S	Własnościowa	<a href="http://realite.ru/">http://realite.ru/</a>
Spiceworks IT Desktop	Spiceworks	F-A--	Open source	<a href="http://www.spiceworks.com">http://www.spiceworks.com</a>
System Center Configuration Manager (poprzednio Systems Management Server, czyli SMS)	Microsoft	-CA-S	Własnościowa, używa SNMP i WMI	<a href="http://www.microsoft.com/systemcenter/configurationmanager/pl/pl/default.aspx">http://www.microsoft.com/systemcenter/configurationmanager/pl/pl/default.aspx</a>
TeamQuest Performance Software	TeamQuest Corporation	-CAP-	Własnościowa	<a href="http://www.teamquest.com/">http://www.teamquest.com/</a>
Tivoli Framework	IBM	FCAPS	Własnościowa, używa COBA, SNMP, WMI i CIM	<a href="http://www-01.ibm.com/software/tivoli/">http://www-01.ibm.com/software/tivoli/</a>
WhatsUp Gold	Ipswitch Systems	FCAPS	Własnościowa	<a href="http://www.whatsupgold.com/">http://www.whatsupgold.com/</a>
ZABBIX	ZABBIX SIA	--AP-	System otwarty, używa SNMP, ICMP i innych komponentów	<a href="http://www.zabbix.com/">http://www.zabbix.com/</a>
Zenoss Core	Zenoss	FCAP-	System otwarty, używa SNMP, WMI, XML-RPC i SSH	<a href="http://www.zenoss.com/product/systems-management">http://www.zenoss.com/product/systems-management</a>
ZENWorks	Novell	FCAPS	Własnościowa	<a href="http://www.novell.com/products/zenworks/configurationmanagement/">http://www.novell.com/products/zenworks/configurationmanagement/</a>
Zyrion Traverse	Zyrion	F--P-		<a href="http://www.zyrion.com/">http://www.zyrion.com/</a>

Objaśnienie do tabeli: akronim FCAPS oznacza *Fault Management, Configuration Management, Accounting and Administration, Performance Management, and Security Management*, czyli zarządzanie usterkami, zarządzanie konfiguracją, rozliczenia i administracja, zarządzanie wydajnością oraz zarządzanie bezpieczeństwem.



W ostatnich latach OpenView firmy Hewlett-Packard był kilkakrotnie zmieniany. Obecnie te produkty są oferowane w ramach oprogramowania i usług Hewlett-Packard, ale nazwy i funkcje produktów pozostają takie same.

Niektóre z platform zarządzających mają długą historię i obsługują ogromną liczbę powiązanych z nimi aplikacji, na przykład produkty OpenView i Tivoli. Ze względu na brak miejsca nie można tutaj przedstawić wszystkich dostępnych narzędzi. Aby poznać zakres funkcji oferowanych przez wymienione platformy zarządzania sieciowego, warto zapoznać się z opisem produktów na witrynach internetowych producentów, które podano w tabeli 30.1.

Inną, zyskującą coraz większą popularność opcją na polu zarządzania sieciowego jest dostawca usług zarządzanych (ang. *Managed Service Provider* — MSP), który specjalizuje się w tego rodzaju zadaniach monitorowania i obsługi sieci.

## Podsumowanie

W rozdziale przedstawiono różne kategorie narzędzi zarządzania sieciowego i sposoby ich używania w celu poprawienia wydajności sieci oraz wyeliminowania błędów. Zastosowano klasyfikację modelu FCAPS do omówienia typów oprogramowania służącego do zarządzania siecią. Akronim FCAPS oznacza *Fault Management, Configuration Management, Accounting and Administration, Performance Management, and Security Management*, czyli zarządzanie usterkami, zarządzanie konfiguracją, rozliczenia i administracja, zarządzanie wydajnością oraz zarządzanie bezpieczeństwem.

Zrozumienie zdarzeń i oprogramowania pozwalającego na ich monitorowanie ma kluczowe znaczenie podczas wykonywania zadań związanych z zarządzaniem siecią. Zdarzenia można monitorować za pomocą liczników systemowych i agentów — ogólnie rzecz biorąc, i jedno, i drugie są małymi programami. Narzędzia do monitorowania wydajności mogą być używane zarówno do usuwania usterek w sieci, jak i do optymalizacji wydajności.

Usterki mogą spowodować generowanie powtarzających się zdarzeń i doprowadzić do lawiny zdarzeń. Ustalenie usterki jest wyzwaniem. Oprogramowanie do zarządzania konfiguracją pozwala na zmianę konfiguracji różnych urządzeń sieciowych oraz wdrażanie oprogramowania w sieci. Omówiono też takie zagadnienia, jak wdrożenia sieciowe, uaktualnienia, zarządzanie poprawkami i cykl życiowy systemu.

Systemy zarządzania sieciowego są pakietami narzędzi umożliwiającymi przeprowadzanie różnorodnych zadań z zakresu zarządzania. W rozdziale wymieniono aplikacje najważniejszych na rynku platform i produkty własnościowe zaliczające się do tej grupy oprogramowania.

W następnym rozdziale zostaną bliżej przedstawione niektóre zaprezentowane tu narzędzia oraz ich zastosowanie w diagnozowaniu różnych powszechnie spotykanych problemów z sieciami.



# Rozdział 31.

# Polecenia

# diagnostyczne sieci

## W tym rozdziale:

- ♦ Zarządzanie siecią z poziomu wiersza poleceń
- ♦ W jaki sposób polecenia diagnostyczne pozwalają na znalezienie usterki?
- ♦ Powłoki poleceń
- ♦ Telnet, NetShell oraz PowerShell

W tym rozdziale skoncentrujemy się na różnych narzędziach wiersza poleceń służących do wykrywania problemów dotyczących sieci, określania jej kondycji oraz do modyfikacji różnych jej parametrów. Tego rodzaju narzędzia pozwalają na testowanie po kolei poszczególnych komponentów sieci, a tym samym zawężanie zakresu potencjalnych problemów aż do znalezienia niewłaściwie działającego elementu bądź systemu.

Powłoki poleceń stanowią od niepamiętnych czasów część technologii komputerowej. Pozostają popularne wśród użytkowników i administratorów sieci, ponieważ dają potężne możliwości w zakresie kontrolowania sieci, jak również mogą być wykorzystywane w środowiskach o stosunkowo niewielkich wymaganiach sprzętowych. W rozdziale będą omówione różne powłoki poleceń oraz interfejsy wiersza poleceń (ang. *Command Line Interface* — CLI) używane do zarządzania siecią. Wiele z tych powłok jest przeznaczonych nie tylko do wykonywania jednego polecenia, ale może uruchamiać również małe programy bądź skrypty. Przykładem zastosowania powłoki CLI podczas testowania i wykrywania usterki będzie użycie poleceń `ping` i `ipconfig` w celu sprawdzenia niedziałającego połączenia z internetem.

W rozdziale zaprezentowany jest także zestaw poleceń powiązanych z siecią i przeznaczonych dla powszechnie używanych powłok w systemach Linux, Windows i Unix; omówiono też składnię tych poleceń. Przedstawiona składnia jest tylko przykładem — jest ona zależna od danej platformy.

Polecenia powłoki Windows NetShell są wykorzystywane do zarządzania elementami sieci już od czasów systemu Windows NT. Za pomocą wiersza poleceń NETSH można zarządzać usługami, zmieniać ustawienia urządzeń, konfigurować i dodawać zasoby sieciowe

oraz uzyskiwać dostęp do obiektów Windows Management Instrumentation (WMI) w sieci. W systemach Windows Server 2008 i Vista firma Microsoft wprowadziła środowisko wiersza poleceń o nazwie PowerShell, które oferuje znacznie większe możliwości i pozwala na wykonywanie wymienionych zadań. Środowisko PowerShell również zostanie tutaj omówione.

## Diagnostyka sieci

Problemy sieciowe mogą być trudne do znalezienia i wymagają znajomości różnych narzędzi. Wraz z osiągnięciem dojrzałości przez sieciowe systemy operacyjne i zaadaptowaniem licznych technologii producenci zaczęli w nich umieszczać narzędzia sieciowe działające z poziomu wiersza poleceń i oferujące potężne możliwości. Istnieją też inne narzędzia, których funkcje opatrzone graficznym interfejsem użytkownika systemu operacyjnego bądź wbudowano je w narzędzia graficzne. W rozdziale zostanie przedstawiona szeroka gama narzędzi sieciowych, które można wykorzystać do diagnozowania problemów z siecią oraz ich rozwiązywania. Zaprezentowane będą również odmienne podejścia stosowane w trakcie tego rodzaju operacji. Wiele wspomnianych w tym rozdziale narzędzi zostało już wymienionych we wcześniejszych rozdziałach. Jednak tutaj przedstawiono także nowe, wraz z wyjaśnieniem, kiedy i jak się nimi posługiwać.

Najlepsze podejście podczas rozwiązywania problemów z siecią to zastosowanie poniższej metody:

1. Udokumentowanie problemu wymagającego rozwiązania.
2. Zebranie wszelkich niezbędnych informacji dotyczących używanego systemu i wykorzystywanych połączeń.
3. Wybranie odpowiedniego narzędzia lub narzędzi i przeanalizowanie wyników ich działania.
4. Nieustanne zawężanie zasięgu problemu.
5. Segmentowanie, izolowanie i sprawdzanie potencjalnych usterek z zastosowaniem testowania, zastępowania i wymiany komponentów.
6. Potwierdzenie hipotezy przez znalezienie sposobu usunięcia usterki.

## Polecenia sieciowe

Polecenia wprowadzane w wierszu poleceń stanowią metodę określania stanu sieci, modyfikowania warunków i przeprowadzania wielu innych zadań. Poniżej zostaną przedstawione różne powłoki CLI dostępne w systemach Linux, Windows i Unix. Ponadto będą omówione najważniejsze polecenia powiązane z siecią.

## Narzędzia wiersza poleceń

Powłoka poleceń lub interpreter wiersza poleceń to interfejs tekstowy dla programu pobierającego dane wejściowe od użytkownika konwertujący je na polecenia, które mogą być wykonane przez system operacyjny. Narzędzia wiersza poleceń wykorzystują różne języki

programowania, co w połączeniu z tym, jak producenci implementują sieciowe systemy operacyjne, oznacza istnienie rozbieżności w składni poleceń sieciowych i sposobach implementacji ich opcji. Powłoka CLI jest dostępna w komputerach od początku lat sześćdziesiątych i charakteryzuje się minimalnymi wymaganiami sprzętowymi dla takiego środowiska, szybkością wprowadzania poleceń i generowaniem małego obciążenia. Z tego powodu każdy oferowany obecnie sieciowy system operacyjny (ang. *Network Operating System* — NOS) jest dostarczany wraz z rodzimą powłoką CLI. Ponadto dostępne są powłoki CLI opracowane przez firmy trzecie; większość z nich działa na wielu platformach. Sieciowe narzędzia powłoki CLI stanowią większą część zbioru poleceń dostępnego dla danego systemu. Zostaną tutaj przedstawione niektóre z najważniejszych poleceń tego typu.



Ogólnie rzecz biorąc, praca z powłoką CLI oferuje użytkownikowi znającemu powłokę większą kontrolę i większe możliwości działania w środowisku komputera niż analogiczne narzędzia graficzne (GUI). Jednak opanowanie narzędzi powłoki wymaga wysiłku. Autor zaleca koncentrowanie się na przeznaczeniu danego narzędzia i poszukiwanie się pomocą dostępną bezpośrednio w powłoce CLI albo w internecie w celu znalezienia informacji wymaganych do zrealizowania określonego zadania. Systemy operacyjne i powłoki stosują różne metody wyświetlania pomocy. Do najczęściej wykorzystywanych należy podanie polecenia z opcją `/?` lub wydanie polecenia `man <nazwa_narzędzia>`. Wyszukanie nazwy narzędzia bądź polecenia w wyszukiwarce internetowej (na przykład Google) z reguły dostarcza dokładnych informacji na jego temat.

Wśród dostępnych programów powłoki znajdują się między innymi:

- ♦ **cmd.com.** Narzędzie to jest odpowiedzialne za wiersz poleceń w systemach Windows 7, Vista, Windows Server, Windows CE oraz OS/2.
- ♦ **sh, bash, csh i ksh.** Wymienione powłoki systemu Unix oznaczają Bourne Shell (sh), Bourne Again Shell (bash), C Shell (csh) i Korn Shell (ksh). W zależności od używanej wersji systemu Unix lub Linux domyślnie może być stosowana inna powłoka, a sam system może mieć możliwość uruchamiania więcej niż tylko jednej powłoki. W systemach z rodziny Unix rzadziej wykorzystuje się powłokę Almquist Shell (ash) i jej odpowiednik w Debianie (dash), a także TENEX C Shell (tcsh), ES Shell, Easy Shell (esh), Friendly Interactive Shell (fish), RC Shell, Scheme Shell (scsh), Stand-alone Shell (sash), Windows SSH (lub Secure Shell) oraz Z Shell (zsh).
- ♦ **telsh i wish.** Powłoki te używają języka skryptowego Tcl.
- ♦ **efi.** W nowoczesnych procesorach powłoka Extensible Firmware Interface (efi) działa jako zamiennik dla BIOS-u.
- ♦ **Windows Script Host (wsh).** Powłoka ta jest używana w systemie Windows do automatyzowania różnych procedur języka Active Scripting bazujących na językach JScript, VBScript, PerlScript oraz innych (i ma możliwości rozbudowy). Jest to technologia automatyzacji mająca szerokie możliwości w zakresie programowania wsadowego. Zastosowania powłoki wsh to skrypty logowania, konfigurowanie systemu i zarządzanie siecią.
- ♦ **PowerShell.** Ten język skryptowy został zaimplementowany w Windows jako powłoka wiersza poleceń dla systemów Windows 7, Vista, Server 2008/2003 oraz XP (z dodatkami SP2 i SP3). Do uruchamiania skryptów wykonujących zadania administracyjne powłoka PowerShell używa platformy .NET.

- ♦ **rexx.** Powłoka języka skryptowego opracowana przez firmę IBM.
- ♦ **phpsh.** Powłoka dla języka PHP.
- ♦ **python.** Interpreter języka Python może być uruchomiony w powłoce CLI.
- ♦ **JavaScript oraz BeanShell.** JavaScript jest interaktywnym interfejsem dla języka skryptowego JavaScript, natomiast BeanShell to powłoka dla Javy. Istnieje kilka różnych wersji JavaScript.



Tabelę zawierającą porównanie różnych powłok można znaleźć na stronie [http://en.wikipedia.org/wiki/Comparison\\_of\\_computer\\_shells](http://en.wikipedia.org/wiki/Comparison_of_computer_shells).

Istnieje wiele różnych powłok CLI, ale na powyższej liście znalazły się te, które charakteryzują się największym zestawem funkcji powiązanych z siecią.

Oto narzędzia stanowiące część zestawu poleceń TCP/IP: arp, finger, ftp, hostname, ipconfig/ifconfig, lpq, lpr, nbtstat, netstat, nslookup, ping, rcp, rexec, route, rsh, tftp i tracert. Szczegółowo zostały omówione we wcześniejszych rozdziałach.



Wiele poleceń TCP i IP zostało przedstawionych w rozdziałach odpowiednio 17. i 18.

Przeanalizujemy teraz zestaw powszechnie spotykanych problemów, w których rozwiązywaniu narzędzia wiersza poleceń są szczególnie użyteczne i oferują potężne możliwości — jeden z nich to sytuacja, kiedy przeglądarka internetowa nie ma połączenia z internetem. Można wtedy podjąć następujące kroki:

1. Uruchomienie drugiej przeglądarki internetowej w celu sprawdzenia, czy brak połączenia z internetem nie dotyczy tylko pierwszej przeglądarki.
2. Uruchomienie wiersza poleceń i wydanie polecenia `ping www.yahoo.com`.

Jeżeli wykonanie polecenia `ping` zakończy się powodzeniem, to znaczy, że system dysponuje działającym połączeniem z internetem, a serwer DNS prawidłowo tłumaczy adresy IP. W takim przypadku problem prawdopodobnie dotyczy używanej przeglądarki internetowej. W przykładzie została wykorzystana witryna Yahoo!, ponieważ jest ona niemal zawsze dostępna, a ponadto nie ma wyłączonego odpowiadania na żądania polecenia `ping`. Wszystkie podobne witryny mają wyłączone odpowiadanie na polecenia `ping`.

3. W wierszu poleceń należy wydać polecenie `ping 69.147.76.15` (to adres IP witryny `www.yahoo.com`).

Jeżeli wykonanie polecenia `ping` zakończy się powodzeniem, to znaczy, że system dysponuje działającym połączeniem z internetem, ale nie potrafi tłumaczyć zewnętrznych zapytań DNS. W celu rozwiązania problemu należy sprawdzić dokumentację DNS, natomiast w przypadku działającego serwera DNS trzeba sprawdzić jego konfigurację.

4. W wierszu poleceń należy wydać polecenie `ping <adres IP bramy>`.

Adres bramy to ten, który został podany do użycia w interfejsie sieciowym udostępniającym połączenie z internetem. Jeżeli wykonanie polecenia `ping` zakończyło się niepowodzeniem, to należy sprawdzić stan bramy (lub zapory sieciowej), jak również kable prowadzące do bramy.

5. W wierszu poleceń należy wydać polecenie `ping <nazwa węzła sieciowego>`.

Węzeł może być dowolnym systemem w sieci bądź routerem, który pozwala na śledzenie trasy z bramy do komputera. Polecenie `ping <nazwa węzła sieciowego>` może być również wykorzystane do sprawdzenia systemów oraz konfiguracji DNS. Jeżeli wyeliminowano wszelkie problemy z połączeniem prowadzącym do systemu, to ostatnim elementem do sprawdzenia jest sam lokalny komputer.

6. W wierszu poleceń należy wydać polecenie `ipconfig` (w systemach Windows lub Macintosh) bądź `ifconfig` (w systemach Unix lub Linux).

Jeżeli ustawienia adresu są nieprawidłowe, to należy je zmienić. Jeżeli nie zastosowano dynamicznego przydzielania adresów IP, to trzeba odświeżyć ustawienia DHCP i sprawdzić stan serwera DHCP. Do tego celu służą polecenia `ipconfig /release` i `ipconfig /renew`. (W różnych platformach mogą być stosowane nieco inne nazwy opcji).

Polecenie `ping` zawsze zwraca jedną z poniższych odpowiedzi:

- ♦ **Normalna odpowiedź.** Komputer macierzysty ma połączenie z internetem w ramach parametru Time-To-Live (zwykle od 1 do 10 przeskoków).
- ♦ **Cel nie odpowiada.** Nie otrzymano żadnej odpowiedzi.
- ♦ **Nieznany host.** Docelowy host jest nieznany i pozostaje nieosiągalny.
- ♦ **Cel nieosiągalny.** Cel jest znany, ale brama domyślna nie przekierowuje do niego.
- ♦ **Sieć lub docelowy host jest nieosiągalny.** W tabeli routingu nie ma wpisu dla danego hosta lub sieci.

Kroki od 1. do 6. przedstawiają praktykę polegającą na nieustannym zawężaniu zasięgu problemu; jest to teoretycznie najlepsze podejście. Jednak problem z lokalnym komputerem może być inny niż wymienione na liście. W takim przypadku na wczesnym etapie procesu warto wypróbować polecenie `ipconfig /ifconfig`. Na rysunku 31.1 pokazano sekwencję kroków podobną do omówionej.

Przyjmijmy założenie, że wykonano wszystkie przedstawione powyżej kroki, interfejs sieciowy jest skonfigurowany i działa, wszystkie węzły pośrednie odpowiadają na polecenia `ping` oraz działa tłumaczenie zapytań DNS w celu otrzymania witryn internetowych, które odpowiadają na żądania `ping`. Wszystkie elementy połączenia internetowego funkcjonują prawidłowo, ale przeglądarka internetowa nadal nie działa i nie wyświetla poprawnych informacji. Kolejne kroki, które trzeba podjąć, to sprawdzenie innych aspektów połączenia. Należy więc sprawdzić czas udzielania odpowiedzi i upewnić się, że jest rozsądną wartością. Zazwyczaj długi czas udzielania odpowiedzi wiąże się z pewną liczbą odpowiedzi „brak odpowiedzi”. W takim przypadku można użyć polecenia `tracert` w celu sprawdzenia trasy prowadzącej do witryn docelowych, jak również wydajności każdego węzła znajdującego się po drodze.

**Rysunek 31.1.**

*Prosta sesja, której celem jest zdiagnozowanie połączenia sieciowego potrzebnego do prawidłowego funkcjonowania przeglądarki internetowej*

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Wersja 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\Robert>ping www.yahoo.com

Badanie www.yahoo.com [87.248.122.122] z 32 bajtami danych:
Odpowiedź z 87.248.122.122: bajtów=32 czas=45ms TTL=128
Odpowiedź z 87.248.122.122: bajtów=32 czas=70ms TTL=128
Odpowiedź z 87.248.122.122: bajtów=32 czas=70ms TTL=128
Odpowiedź z 87.248.122.122: bajtów=32 czas=51ms TTL=128

Statystyka badania ping dla 87.248.122.122:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
    (0% straty),
Szacunkowy czas błędzenia pakietów w millisekundach:
    Minimum = 45 ms, Maksimum = 70 ms, Czas średni = 59 ms

C:\Users\Robert>ping 192.168.254.2

Badanie 192.168.254.2 z 32 bajtami danych:
Odpowiedź z 192.168.254.2: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.254.2: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.254.2: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.254.2: bajtów=32 czas<1 ms TTL=128

Statystyka badania ping dla 192.168.254.2:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
    (0% straty),
Szacunkowy czas błędzenia pakietów w millisekundach:
    Minimum = 0 ms, Maksimum = 0 ms, Czas średni = 0 ms

C:\Users\Robert>ipconfig

Konfiguracja IP systemu Windows

Karta Ethernet Połączenie lokalne:

    Sufiks DNS konkretnego połączenia : localdomain
    Adres IPv6 połączenia lokalnego . : fe80::19aa:7649:cb3a:2b8c::11
    Adres IPv4 . . . . . : 192.168.254.128
    Maska podsieci . . . . . : 255.255.255.0
    Brana domyślna. . . . . : 192.168.254.2

Karta tunelowa isatap.localdomain:

    Stan nośnika . . . . . : Mośnik odłączony
    Sufiks DNS konkretnego połączenia : localdomain

Karta tunelowa Teredo Tunneling Pseudo-Interface:

    Sufiks DNS konkretnego połączenia :
    Adres IPv6 . . . . . : 2001:0:5ef5:79fd:2cc3:368:3f57:17f
    Adres IPv6 połączenia lokalnego . : fe80::2cc3:368:3f57:17f::13
    Brana domyślna. . . . . : ::

C:\Users\Robert>
  
```

Następny krok to sprawdzenie zdolności przyłączeniowej w celu określenia, czy używany protokół może być wysyłany i odbierany. Na przykład serwer Microsoft ISA domyślnie wykorzystuje port 8080 dla ruchu sieciowego HTTP. Należy sprawdzić ustawienia zapory — zarówno sieciowej, jak i lokalnej — i przekonać się, czy ruch sieciowy HTTP jest dozwolony, a także, co ważniejsze, czy dana przeglądarka internetowa jest aplikacją, która może używać portu HTTP.

W tabeli 31.1 wymieniono różne polecenia powłoki CLI powiązane z siecią i dostępne dla systemów Linux (L), Unix (U) oraz Windows (W). Wprawdzie przedstawiono również składnię tych poleceń, ale jest ona różna w zależności od używanej powłoki, a w przypadku systemu Windows także w zależności od konkretnej wersji systemu operacyjnego. Składnia przedstawiona dla Windows bazuje na powłocie cmd.com dla systemu Windows XP. Prawidłową składnię można sprawdzić w dokumentacji wykorzystywanej platformy. W dokumentacji tej można również znaleźć objaśnienia różnych opcji poleceń.

Polecenie ipconfig i jego odpowiednik w systemach Linux i Unix, czyli ifconfig, mogą być najszybszymi poleceniami TCP/IP w dostępnym arsenale. Oprócz wyświetlania informacji o stanie interfejsu sieciowego polecenie ipconfig pozwala również na zmianę statycznego adresu IP, a także na zwolnienie i odnowienie dowolnego dynamicznego adresu IP.

Tabela 31.1. Polecenia powłoki powiązane z siecią

Polecenie	Platforma	Opis	Składnia
ac	L/U	Wyświetla dane statystyczne dotyczące czasu połączenia użytkownika.	<pre>ac [-d   --daily-totals] [-y   --print-year] [-p   --individual-totals] [people] [-f   --file nazwa_pliku] -&gt;[-a   --all-days] [--complain] [--reboots] [--suppliants] -&gt;[--timewarps] [--compatibility] [--tw-lenieny liczba] -&gt;[--tw-suspicious liczba] [-z   --print-zeros] [--debug] -&gt;[-v   --version] [-h   --help]</pre>
arp	L/U/W	Wyświetla i modyfikuje wpisy w buforze protokołu Address Resolution Protocol (ARP) zawierającym jedna lub więcej tabel, które są używane do przechowywania adresów IP oraz ich przetłumaczonych adresów Ethernet bądź fizycznych Token Ring. Dla każdego adaptera Ethernet i Token Ring zainstalowanego w komputerze istnieje oddzielna tabela.	<pre>arp [-a [inetaddr] [-N ifaceaddr]] [-g [inetaddr] -N ifaceaddr]] [-d inetaddr [ifaceaddr]] -&gt;[-s inetaddr etheraddr [ifaceaddr]]</pre>
atmadm	W	Monitoruje połączenia i adresy, które zostały zarejestrowane przez ATM Call Manager w sieci ATM (ang. <i>Asynchronous Transfer Mode</i> ). Polecenie atmadm można wykorzystać do wyświetlenia danych statystycznych dotyczących wywołań przychodzących i wychodzących w adapterach ATM. Użycie tego polecenia bez żadnych opcji powoduje wyświetlenie danych statystycznych monitorujących stan aktywnych połączeń ATM.	<pre>atmadm [/c]/[a] [/s]</pre>
bash	L/U	Uruchamia powłokę bash.	<pre>bash [opcje]</pre>
chdir (cd)	L/U/W	Wyświetla nazwę katalogu bieżącego lub powoduje zmianę katalogu bieżącego. Polecenie użyte tylko z literą dysku (na przykład chdir c:) powoduje wyświetlenie nazwy bieżącego dysku oraz katalogu. Użycie polecenia bez żadnych opcji powoduje wyświetlenie bieżącego dysku i katalogu.	<pre>chdir [/d] [Napęd:][Ścieżka] [...] [/d] [Napęd:][Ścieżka] -&gt;[...]</pre> <pre>cd [/d] [Napęd:][Ścieżka] [...] [/d] [Napęd:][Ścieżka] [...]</pre>

Tabela 31.1. Polecenia powłoki powiązane z siecią — ciąg dalszy

Polecenie	Platforma	Opis	Składnia
chkdsk	W	Tworzy i wyświetla raport dotyczący stanu dysku. Polecenie chkdsk powoduje również wyświetlenie i naprawienie błędów znalezionych na dysku.  Polecenie z wymienionymi obok parametrami jest dostępne jedynie podczas używania konsoli odczytywania. Polecenie chkdsk wraz z różnymi parametrami jest dostępne z poziomu wiersza poleceń.	chkdsk [napęd:] [/p] [/r]
cmstp	W	Instaluje bądź usuwa profil usługi menedżera połączenia. Użycie polecenia cmstp bez parametrów opcjonalnych powoduje instalację profilu usługi wraz z ustawieniami domyślnymi, które są odpowiednie dla systemu operacyjnego i uprawnień użytkownika.	Nazwapikuprofiluusiugi.exe /q:a /c:"cmstp.exe" →nazwapikuprofiluusiugi.inf [/mf] [/mi] [/ns] [/s] [/su] [/u]" cmstp.exe [/mf] [/mi] [/ns] [/s] [/su] [/u]"[Ścieżka] →nazwapikuprofiluusiugi.inf"
comp	W	Porównuje baji po bajcie zawartość dwóch plików lub zestawów plików. Polecenie comp może porównywać pliki znajdujące się na tym samym dysku lub różnych dyskach oraz w tym samym katalogu bądź różnych katalogach. Kiedy polecenie comp porównuje pliki, wyświetla ich położenie i nazwy. Użycie polecenia bez parametrów powoduje wyświetlenie zapytania o pliki, które mają być porównane.	comp [dane1] [dane2] [/d] [/a] [/l] [/n=liczba] [/c]
compact	W	Wyświetla i zmienia stopień kompresji plików lub katalogów znajdujących się w partycji NTFS. Użycie polecenia bez parametrów powoduje wyświetlenie informacji na temat stanu kompresji katalogu bieżącego.	compact [{/c}/u] [/s[:katalog]] [/a] [/i] [/f] [/q] →[nazwapiku[...]]
compress	L/U	Kompresuje plik i dodaje rozszerzenie .z.	compress [-c][-f][-v] nazwapików
copy (cp)	L/U/W	Kopiuje jeden plik lub więcej plików z jednego miejsca do drugiego.	copy [/d] [/v] [/n] [{/y}/-y]] [/z] [{/a}/b}] Źródło →[{/a}/b}] [+ Źródło [{/a}/b}] [+ ...]] [Cel [{/a}/b]]]
crontab	L/U	Tworzy i wyświetla pliki, które będą uruchamiane według harmonogramu.	crontab [-e] [-l] [-r] [nazwapiku]
csh	L/U	Uruchamia powłokę C Shell.	csh [-b] [-c] [-e] [-f] [-i] [-n] [-s] [-t] [-v] [-x] [-X] [nazwaskryptu]]

dhclient	L/U	Protokół DHCP (ang. <i>Dynamic Host Configuration Protocol</i> ) automatycznie przypisuje adresy IP klientom DHCP.	dhclient [-p port] [-d] [-e VAR=wartość] [-q] [-1] [-r] ↪ [-1f plikdzierżaw] [-pf plikpid] [-cf plikkonfiguracyjny] [-sf plikszyfrowany] [-e ENVVAR=wartość] [-s server] ↪ [-g przekazywanie] [-n] [-nw] [-w] [if0 [... ifn]]
dig	L/U	Narzędzie wyszukiwania DNS — automatycznie konwertuje nazwy czytelne dla człowieka na adresy IP.	dig [@server] [-b adres] [-c klasa] [-f nazwapliku] ↪ [-k nazwapliku] [-p numerportu] [-t typ] [-x adres] ↪ [-y nazwa.klucz] [-4] [-6] [nazwa] [typ] [klasa] [opcjezapytania...]
dirncmp	L/U/W	Porównuje pliki w dwóch katalogach i następnie wskazuje, które są identyczne, a które nie.	dirncmp [-d] [-s] [-w n] pierwszyskatalog drugikatalog
diskcopy	W	Kopiuje zawartość dyskiety w stacji źródłowej na sformatowaną bądź niesformatowaną dyskietkę znajdującą się w stacji docelowej. Użycie polecenia bez parametrów spowoduje wykorzystanie bieżącego napędu jako dysku źródłowego i docelowego.	diskcopy [napęd1 : [napęd2:]] [/v]
expand	L/U/W	Wyodrębnia co najmniej jeden skompresowany plik. Polecenie jest używane w celu wyodrębnienia skompresowanych plików z dysków dystrybucyjnych.	expand [-r] Źródło [Cel] expand -d źródło.cab [-f:pliki] expand źródło.cab -f:pliki Cel
finger	L/U/W	Wyświetla informacje o użytkowniku bądź użytkownikach na określonym komputerze zdalnym (zazwyczaj na komputerze działającym pod kontrolą systemu Unix), w którym uruchomiono demona lub usługę <i>Finger</i> . Komputer zdalny określa format oraz wyświetla dane zawierające informacje o użytkownikach. Zastosowanie polecenia <i>finger</i> bez parametrów powoduje wyświetlenie treści pomocy.	finger [-i] [Użytkownik] [@komputermacierzysty] [...]
ftp	L/U/W	Pozwala na przekazywanie plików między komputerami, w których uruchomiono usługę FTP (ang. <i>File Transfer Protocol</i> ), na przykład serwer IIS (ang. <i>Internet Information Services</i> ). Polecenia <i>ftp</i> można użyć interaktywnie lub w trybie wsadowym przez przetwarzanie plików tekstowych ASCII.	ftp [-v] [-d] [-i] [-n] [-g] [-s:nazwapliku] [-a] ↪ [-w:wielkośćokna] [-A] [komputermacierzysty]
getfac1	L/U	Wyświetla atrybuty plików.	getfac1 [-a] [-d] Plik

Tabela 31.1. Polecenia powłoki powiązane z siecią — ciąg dalszy

Polecenie	Platforma	Opis	Składnia
Getmac	W	Zwraca adres MAC (ang. <i>Media Access Control</i> ) i wyświetla listę protokołów sieciowych powiązanych z każdym adresem dla wszystkich kart sieciowych we wszystkich komputerach, zarówno lokalnych, jak i w sieci.	<code>getmac[.exe] [/s Komputer [/u Domena\Użytkownik [/p Hasło]]] → [/fo {TABLE LIST CSV}] [/nh] [/v]</code>
gpresult	W	Wyświetla ustawienia polityki grupy oraz RSOP (ang. <i>Resultant Set of Policy</i> ) dla użytkownika bądź komputera.	<code>gpresult [/s Komputer [/u Domena\Użytkownik [/p Hasło]]] → [/user docelowanazwa\użytkownika] [/scope {user computer}] → [/v] [/z]</code>
host	L/U	Narzędzie wyszukiwania DNS — automatycznie konwertuje nazwy czytelne dla człowieka na adresy IP.	<code>host [-acdInrtw] [-c klasa] [-N ndots] [-R liczba] [-t typ] [-W oczekiwanie] [-4] [-6] {nazwa} [-*]</code>
hostname	L/U/W	Wyświetla nazwę hosta pobraną z pełnej nazwy danego komputera.	<code>hostname</code>
ipconfig	W	Wyświetla wszystkie wartości konfiguracyjne sieci TCP/IP oraz odświeża ustawienia DHCP (ang. <i>Dynamic Host Configuration Protocol</i> ) i DNS (ang. <i>Domain Name System</i> ). Użycie polecenia bez parametrów powoduje wyświetlenie adresu IP, maski podsieci i domyślnej bramy dla wszystkich kart sieciowych.	<code>ipconfig [/all] [/renew [kartasieciowa]] [/release → [kartasieciowa]] [/flushdns] [/displaydns] [/registerdns] → [/showclassid kartasieciowa] [/setclassid kartasieciowa → [ID_klasy]]</code>
ifconfig	L/U	Polecenie identyczne z poleceniem <code>ipconfig</code> w Windows, ale zawiera parametry charakterystyczne dla danej platformy.	<code>ifconfig [-L] [-m] interface [create] [rodzinaadresu] [address[/długośćprefiksu] [adresdocelow]] [Parameter] ifconfig interface destroy ifconfig -a [-L] [-d] [-m] [-u] [rodzinaadresu] ifconfig -l [-d] [-u][rodzinaadresu] ifconfig [-L] [-d] [-m] [-u] [-C]</code>
ifup/ifdown	L/U	Powoduje otworzenie lub zamknięcie interfejsu sieciowego.	<code>ifup [-nv] [--no-act] [--verbose] [-i PLIK --interfaces=PLIK] → [-a low KLASA] -a IFACE ... ifdown [-nv] [--no-act] [--verbose] [-i PLIK -- interfaces=PLIK] → [-a low KLASA] -a IFACE ...</code>

Ipsccmd	W	Pozwala na konfigurację polityki IPsec (ang. <i>Internet Protocol Security</i> ) w usłudze katalogowej bądź w rejestrze lokalnym lub zdalnym. Polecenie <code>ipseccmd</code> to alternatywa dla narzędzia Polityka bezpieczeństwa IP konsoli MMC; ma trzy tryby pracy: dynamiczny, statyczny i zapytań.	W celu dodania reguły: <code>ipseccmd [\ \ nazwakomputera] -f listafiltrów</code> → <code>[-n listapolitykinegociacji] [-t adrestunelu]</code> → <code>[-a listanetodawczyteliniana] [-ls listanetodbezpieczeństwa]</code> → <code>[-lk głównytrybustawień] [-lp] [-lf listafiltrówm]</code> → <code>[-le czaswygaśnięcia] [-soft] [-confirm] [{-dialup   -lan}]</code> W celu usunięcia całej polityki dynamicznej: <code>ipseccmd -u</code>
ipxroute	W	Wyświetla i modyfikuje informacje dotyczące tabel routingu używanych przez protokół IPX. Zastosowanie polecenia bez parametrów powoduje wyświetlenie ustawień domyślnych dla pakietów wysyłanych do adresów nieznanych, rozgłaszania i multimiisji.	<code>ipxroute servers [/ttype=x]</code> <code>ipxroute ripout sieć</code> <code>ipxroute resolve {guid   name} {guid   nazwakartyściowej}</code> <code>ipxroute board=n [def] [qbr] [mbr] [remove=xxxxxxxxxx]</code> <code>ipxroute config</code>
irftp	W	Wysyła pliki przez port podczerwiieni. Użycie polecenie <code>irftp</code> bez parametrów bądź jedynie z parametrem <code>/s</code> powoduje wyświetlenie okna dialogowego Wireless Link, w którym można wybrać pliki przeznaczone do wysłania bez użycia wiersza poleceń.	<code>irftp [Napęd:\ ] [[Ścieżka] nazwapliku] [/h]</code> <code>IRFTP /s</code>
ksh	L/U	Uruchamia powłokę Korn Shell.	<code>ksh [-a] [-b] [-c] [-e] [-f] [-h] [-i] [-k] [-m] [-n] [-o] [-p]</code> → <code>[-s] [-t] [-u] [-v] [-x] [+ o opcja] [+A nazwa] [argument]</code>
lodctr	W	Powoduje zarejestrowanie nowych nazw licznika wydajności i wyświetlenie tekstu objaśnienia dla usługi lub sterownika urządzenia. Ponadto zapisuje i przywraca ustawienia licznika oraz tekstu objaśnienia.	<code>lodctr [\ \nazwakomputera] nazwapliku [/s:nazwapliku]</code> → <code>[/r:nazwapliku]</code>
logman	W	Ustawia harmonogram licznika i dziennika rejestrowania zdarzeń w systemach lokalnych i zdalnych.	<code>logman [create {counter   trace} nazwakolekcji] [start nazwakolekcji] [stop nazwakolekcji] [delete nazwakolekcji]</code> → <code>[query { nazwakolekcji   providers}] [update nazwakolekcji]</code>
lpq	L/U/W	Wyświetla informacje na temat stanu kolejki wydruku komputera, w którym uruchomiono demona LPD (ang. <i>Line Printer Daemon</i> ). Użycie polecenia bez parametrów powoduje wyświetlenie tekstu pomocy przygotowanego dla polecenia <code>lpq</code> .	<code>lpq -S nazwaservera -P nazwadrukarki [-l]</code>

Tabela 31.1. Polecenia powłoki powiązane z siecią — ciąg dalszy

Polecenie	Platforma	Opis	Składnia
<code>lpr</code>	L/U/W	Powoduje wysłanie pliku do komputera, w którym uruchomiono demona LPD w celu jego przygotowania do wydruku. Użycie polecenia bez parametrów powoduje wyświetlenie tekstu pomocy przygotowanego dla polecenia <code>lpr</code> .	<code>lpr [-S ID_Serwera] -P nazwadrukarki [-C klasazadania] ↪ [-J nazwazadania] [{-o   -o 1}] [-d] [-x] nazwapliku</code>
<code>mi-i-tool</code>	L/U	Narzędzie pozwalające na wyświetlenie lub ustawienie interfejsu sieciowego jednostki MII (ang. <i>Media Independent Interface</i> ). Karty sieciowe Fast Ethernet używają tej funkcji w celu negocjacji parametrów połączenia.	<code>mi-i-tool [-v, --verbose] [-V, --version] [-R, --reset] ↪ [-r, --restart] [-w, --watch] [-1, --log] ↪ [-A, --advertise-media....] [-F, --force-media] ↪ [interfejs ...]</code>
<code>mkdir</code>	L/U/W	Powoduje utworzenie katalogu bądź podkatalogu.	<code>mkdir [napęd:]ścieżka</code> <code>md [napęd:]ścieżka</code>
<code>mount/umount</code>	L/U	Powoduje zamontowanie lub odmontowanie systemów plików i zasobów systemów zdalnych.	<code>mount [-p   -v]</code> <code>mount [-F typsystemplików] [opcjeogólne] [-o opcjedokładne] ↪ [-O] specjal   punktmontowania</code> <code>mount [-F typsystemplików] [opcjeogólne] [-o opcjedokładne] ↪ [-O] specjal punktmontowania</code> <code>mount -a [-F typsystemplików] [-V] [opcjebieżące] ↪ [-o opcjedokładne] [punktmontowania ...]</code> <code>umount [-V] [-o opcjedokładne] specjal   punktmontowania</code> <code>umount -a [-V] [-o opcjedokładne] [punktmontowania ...]</code>
<code>mountvol</code>	W	Tworzy, usuwa lub wyświetla punkty montowania woluminów. Polecenie <code>mountvol</code> to sposób podłączenia woluminu bez konieczności użycia litery.	<code>mountvol [Napęd:] Ścieżka nazwawoluminu</code> <code>mountvol [Napęd:] Ścieżka /d</code> <code>mountvol [Napęd:] Ścieżka /L</code> <code>mountvol Napęd: /s</code>
<code>move (mv)</code>	L/U/W	Powoduje przeniesienie jednego lub więcej plików z jednego katalogu do wskazanego.	<code>move [{/y /-y}] [źródło] [cel]</code> <code>mv [-f] [-i] [źródło] [cel] ]</code>

nbstat	W	Wyświetla dane statystyczne dotyczące protokołu NetBIOS przez TCP/IP (NetBT), nazwy tabel NetBIOS zarówno dla komputera lokalnego, jak i zdalnego oraz nazwę bufora NetBIOS. Polecenie nbstat pozwala na odświeżenie nazwy bufora NetBIOS i nazw zarejestrowanych w WINS (ang. <i>Windows Internet Name Service</i> ). Użycie polecenia bez parametrów powoduje wyświetlenie tekstu pomocy przygotowanego dla nbstat.	nbstat [-a <i>nazwa_zdalnej</i> ] [-A <i>adres_ip</i> ] [-c] [-n] [-r] [-R] ↳[-RR] [-s] [-S] [ <i>odstepczasu</i> ]
netstat	L/U/W	Wyświetla aktywne połączenia TCP, porty, na których komputer nasłuchuje danych, dane statystyczne dotyczące Ethernetu, tabelę routingu IP, dane statystyczne IPv4 (dla protokołów IP, ICMP, TCP oraz UDP), a także dane statystyczne IPv6 (dla protokołów IPv6, ICMPv6, TCP oraz IPv6 i UDP oraz IPv6). Użycie polecenia netstat bez parametrów powoduje wyświetlenie aktywnych połączeń TCP.	netstat [-a] [-e] [-n] [-o] [-p <i>Protokół</i> ] [-r] [-s] ↳[ <i>odstepczasu</i> ]
nslookup	L/U/W	Wyświetla informacje, które można wykorzystać do diagnozowania infrastruktury DNS (ang. <i>Domain Name System</i> ). Przed użyciem narzędzia warto zapoznać się ze sposobem działania DNS. Polecenie nslookup jest dostępne tylko wtedy, gdy zainstalowano protokół TCP/IP.	nslookup [-podpolecenie ...] [{ <i>komputer_dozwolazienia</i> }] ↳[-Server]}} Podpolecenia: exit, finger, help, ls, lserver, root, server, ↳set, set all, set class, set d2, set debug, set defname, ↳set domain, set ignore, set port, set querytype, set ↳recursive, set retry, set root, set search, set srchlist, set timeout, set type, set vc oraz view

Tabela 31.1. Polecenia powłoki powiązane z siecią — ciąg dalszy

Polecenie	Platforma	Opis	Składnia
pathping	W	Wyświetla informacje dotyczące opóźnienia sieciowego oraz strat sieciowych podczas przeskoków pośrednich między miejscem źródłowym i docelowym. Przez ustalony czas polecenie pathping wysyła wiele zapytań Echo do każdego routera znajdującego się między miejscem źródłowym i docelowym, a następnie oblicza wynik na podstawie pakietów zwróconych z każdego routera. Ponieważ polecenie pathping wyświetla stopień strat w pakietach w każdym routerze lub połączeniu, istnieje możliwość określenia, które routery bądź podsieci mogą mieć problemy sieciowe. Pod względem identyfikacji routerów znajdujących się na danej trasie działanie polecenia pathping jest podobne do tracert. Następnie polecenie pathping wysyła przez określony czas polecenia ping do wszystkich routerów i oblicza dane statystyczne na podstawie liczby zwróconych pakietów z każdego z nich.	pathping [-n] [-h maksymalnąliczbaprzeskoków] →[-g listakomputerówmacierzystych] [-p okresczasu] →[-q liczbazapytań] [-w czaswygaśnięcia] [-T] [-R] [nazwamiejscadocełowego]
perfmom	W	Pozwala na uruchomienie konsoli monitora wydajności Windows.	perfmom.exe [nazwapliku] [/HTMLFILE:plikkonwertowany →plikustawień]
ping	L/U/W	Weryfikuje połączenie na poziomie IP z innym komputerem w sieci TCP/IP przez wysyłanie wiadomości Echo ICMP (ang. <i>Internet Control Message Protocol</i> ). Na ekranie są wyświetlane wiadomości otrzymywane od adresata wraz z czasem podróży danej wiadomości. ping to podstawowe polecenie TCP/IP służące do rozwiązywania problemów z połączeniem, osiąganiem zdalnych komputerów oraz tłumaczeniem nazw.	ping [-t] [-a] [-n Licznik] [-i Wielkość] [-f] [-i TTL] [-v TOS] →[-r Licznik] [-s Licznik] [{-j listakomputerówmacierzystych →} -k listakomputerówmacierzystych }] [-w czaswygaśnięcia] →[nazwamiejscadocełowego]
print	W	Wysyła plik tekstowy do drukarki.	print [/d:Drukarka] [Napęd:] [Ścieżka] nazwapliku [ ...]

rasdial	W	Istnieje możliwość zautomatyzowania procesu nawiązywania połączenia z dowolnego klienta Microsoft przez użycie prostego pliku wsadowego oraz polecenia rasdial. Polecenie rasdial nawiązuje połączenie sieciowe, wykorzystując wskazany wpis w pliku wsadowym.	rasdial nazwaPołączenia [nazwaUżytkownika [Hasło   *]] → [/ domain: Domena] [/ phone: numerTelefonu] [/ callback: numerAktoryoddzwonić] [/ phonebook: ścieżkaKsiążkiTelefonicznej] [/ prefiksRozszerzenie]  Polecenie rasdial łączy połączenie sieciowe, używając następującej składni:  rasdial [nazwaPołączenia] / disconnect
rcp	L/U/W	Pozwala na kopiowanie plików między komputerem działającym pod kontrolą systemu Windows XP i komputerem z systemem z uruchomionym demonem rshd (ang. <i>Remote Shell Daemon</i> ). Systemy Windows XP i Windows 2000 nie oferują usługi rshd.	rcp [{-a   -b}] [-h] [-r] [komputerMacierzysty] [.Użytkownik:] → [Zródło] [komputerMacierzysty] [Użytkownik:] [Ścieżka\ <nazwąmiejscadocelowego]< td=""></nazwąmiejscadocelowego]<>
relog	W	Wyodrębnia liczniki wydajności z plików dzienników liczników wydajności i zapisuje je w innych formatach, na przykład tekstu rozdzielonego tabulatorami (ang. <i>Tab Separated Text</i> — TSV), tekstu rozdzielonego przecinkami (ang. <i>Comma Separated Text</i> — CSV), binarnym lub SQL.	relog [nazwaPliku [nazwaPliku ...]] [-a] [-c Ścieżka → [Ścieżka ...]] [-cf nazwaPliku] [-f {bin csv SQL}] → [-t wartość] [-o {plikWyjściowy   DSN PlikDziennikaLicznika}] → [-b M/d/yyyyr [gg:mm:ss] [-e M/d/yyyyr [gg:mm:ss]] → [-config nazwaPliku] [-q]
rename (ren)	W	Zmienia nazwę pliku lub zbioru plików.	rename [Napęd:] [Ścieżka] nazwaPliku1 nazwaPliku2 ren [Napęd:] [Ścieżka] nazwaPliku1 nazwaPliku2
remsh (rsh)	L/U/W	Zdalna powłoka pozwala na wykonywanie poleceń w systemie zdalnym.	remsh [opcje] [-l nazwaUżytkownika] → nazwaKomputerMacierzystego [numerPortu] Polecenie
replace	W	Zastępuje pliki w katalogu docelowym plikami pochodzącymi z katalogu źródłowego, które mają takie same nazwy. Istnieje również możliwość użycia polecenia replace w celu dodania unikalnych nazw plików do katalogu docelowego.	replace [Napęd1:] [Ścieżka1] nazwaPliku [Napęd2:] [Ścieżka2] → [/a] [/p] [/r] [/w] replace [Napęd1:] [Ścieżka1] nazwaPliku [Napęd2:] [Ścieżka2] → [/p] [/r] [/s] [/w] [/u]
rexec	L/U/W	Pozwala na wykonywanie poleceń na komputerach zdalnych za pomocą usługi (demon) rexec. Przed wykonaniem wskazanego polecenia rexec uwierzytelnia nazwę użytkownika na komputerze zdalnym. Systemy Windows XP i Windows 2000 nie dostarczają usługi rexec.	rexec [komputerMacierzysty] [-l nazwaUżytkownika] [-n] → [Polecenie]
rmdir (rm)	L/U/W	Usuwa katalog.	rmdir [Napęd:] Ścieżka [/s] [/q] RD [Napęd:] Ścieżka [/s] [/q]

Tabela 31.1. Polecenia powłoki powiązane z siecią — ciąg dalszy

Polecenie	Platforma	Opis	Składnia
Route	W	Wyświetla i modyfikuje wpisy w lokalnej tabeli routingu IP.	route [-f] [-p] [Polecenie [miejscedocelewowe] ↳[mask maskasięciowa] [Brama] [metric Metryka]] [tf Interfejs]]
rsh	W	Pozwala na wykonywanie poleceń na komputerach zdalnych za pomocą usługi (demon) rsh. Systemy Windows XP i Windows 2000 nie dostarczają usługi rsh.	rsh [komputermacierzysty] [-l nazwaużytkownika] [-n] [Polecenie]
sh	L/U	Pozwala na uruchamianie zadań za pomocą powłoki Bourne Shell.	sh [-a] [-c] [-o] [-e] [-E] [-f] [-h] [-i] [-I] [-k] [-m] ↳[-n] [-p] [-r] [-s] [-t] [-T] [-u] [-v] [-x] [argument]
shutdown	L/U/W	Pozwala na wyłączenie bądź ponowne uruchomienie komputera lokalnego lub zdalnego. Zastosowanie polecenia shutdown bez parametrów spowoduje wylogowanie bieżącego użytkownika.	shutdown [{-l -s -r -a}] [-f] [-m [\\nazwakomputera]] [-t xx] ↳[-c "wiadomość"] [-d[u] [p]:xx:yy]
subst	W	Powoduje powiązanie ścieżki dostępu z literą napędu. Kiedy polecenie zostanie użyte bez parametrów, wyświetli nazwy napędów wirtualnych znanych systemowi.	subst [napęd1: [napęd2:]ścieżka] subst napęd1: /d
taskkill	W	Powoduje zakończenie zadania lub zadań bądź procesów w systemie lokalnym (domyślnie) albo zdalnym. Proces może zostać zakończony przez podanie identyfikatora procesu lub nazwy obrazu.	taskkill [/s komputer] [/u Domena\Użytkownik [/p Hasło]] ↳[/fi nazwafiletru] [/pid ID_Procesu] [/im nazwaobrazu] ↳[/f][/t]
tasklist	W	Wyświetla listę aplikacji i usług wraz z ich identyfikatorami procesu (PID) dla wszystkich zadań działających na komputerze lokalnym lub zdalnym.	tasklist [-.exe] [/s komputer] [/u Domena\Użytkownik ↳[/p Hasło]] [/fo {TABLE LIST CSV}] [/nh] [/fi nazwafiletru ↳[/fi nazwafiletru2 [ ... ]]] [/m [nazwamodułu]   /svc   /v]
tcmsetup	W	Włącza lub wyłącza klienta TAPI.	tcmsetup [/q] [/x] /c Serwer1 [Serwer2...] tcmsetup [/q] /c /d

telnet	L/U/W	<p>Pozwala na komunikację z komputerem zdalnym za pomocą protokołu Telnet. Wydanie polecenia telnet bez parametrów umożliwia przejście do kontekstu Telnet, na co wskazuje znak zachęty (telnet&gt;). Z poziomu kontekstu Telnet można wydawać poniższe polecenia wraz z ich odpowiednimi parametrami w celu zarządzania komputerem, na którym uruchomiono klienta Telnet: close, display, enter, open, quit, set, statis, unset oraz ?/help.</p>	<pre>telnet [\\serverzdalny] Sesje Telnet zostaną omówione w dalszej części rozdziału.</pre>
tftp	L/U/W	<p>Pozwala na przekazywanie plików do oraz z komputera zdalnego będącego zazwyczaj komputerem działającym pod kontrolą systemu Unix, w którym uruchomiono demona lub usługę TFTP (ang. <i>Trivial File Transfer Protocol</i>).</p>	<pre>tftp [-i] [Host] [{get   put}] [Żródło] [Cel]</pre>
tracert	W	<p>Przetwarza dzienniki zdarzeń dotyczące zdarzeń śledzenia lub danych dostarczanych w czasie rzeczywistym przez dostawcę śledzenia zdarzeń i pozwala na generowanie raportów dotyczących śledzenia i plików CSV zawierających wygenerowane zdarzenia.</p>	<pre>tracert [nazwapliku [nazwapliku ...]] [-o [nazwapliku]] →[-report [nazwapliku]] [-rt nazwasesji [nazwasesji ...]] →[-summary [nazwapliku]] [-config [nazwapliku]]</pre>
tracert	W	<p>Ustala trasę prowadzącą do miejsca docelowego przez wysyłanie wiadomości ICMP Echo do miejsca docelowego wraz z kolejno zwiększaną wartością pól TTL (ang. <i>Time-To-Live</i>). Wyświetlona trasa jest listą sąsiadujących interfejsów routerów w routerach znajdujących się na trasie między źródłowym komputerem macierzystym i docelowym. Interfejs sąsiadujący jest interfejsem routera, który znajduje się najbliższej wysyłającego komputera macierzystego na danej trasie.</p>	<pre>tracert [-d] [-h maksymalnaIliczbaprzeskoków] →[-j listaKomputerówmacierzystych] [-w czaswygaśnięcia] →[nazwamięscadocełowego]</pre>
tracert	L/U	<p>Polecenie identyczne z poleceniem tracert w Windows, ale zawiera parametry charakterystyczne dla używanej platformy.</p>	<pre>tracert [-d] [-F] [-I] [-n] [-v] [-x] [-f pierwszyttl] →[-g Brama]   -r [-i interfejs] [-m maksymalnyttl] →[-p port] [-q Iliczbazapytań] [-s adresźródłowy] [-t tos] →[-w czasoczekiwania ] host [wielkośćpakietu]</pre>
tree	W	<p>Wyświetla w sposób graficzny strukturę katalogów w podanej ścieżce dostępu lub napędzie.</p>	<pre>tree [Napęd:[Ścieżka] [/f] [/a]</pre>

Tabela 31.1. Polecenia powłoki powiązane z siecią — ciąg dalszy

Polecenie	Platforma	Opis	Składnia
typeperf	W	Wyświetla dane licznika wydajności w oknie wiersza poleceń lub zapisuje je do pliku dziennika zdarzeń w obsługiwanym formacie. W celu zatrzymania działania polecenia typeperf należy nacisnąć klawisze <i>Ctrl</i> + <i>C</i> .	<pre>typeperf [Ścieżka [Ścieżka ...]] [-cf nazwapliku] ↳ [-f {csv tsv bin}] [-st odstępczasu] [-o nazwapliku] ↳ [-q [obiekt]] [-qx [obiekt]] [-sc ProbkI] [-config nazwapliku] ↳ [-s nazwaskomputera]</pre>
unlodctr	W	Usuwa z rejestru systemowego nazwy liczników wydajności oraz tekst objaśnienia dla danej usługi bądź sterownika urządzenia.	<pre>unlodctr [\nazwaskomputera] nazwasterownika</pre>
w32tm	W	Narzędzie stosowane do diagnozowania problemów związanych z usługą Czas systemu Windows.	<pre>w32tm {/config [/computer: nazwaskomputera] [[/update] ↳ [/manualpeerlist: listanazwkomputeró]] [/syncfrom flags: ↳ listaopcji ] /monitor [/ntpserver register resync ↳ [{:nazwaskomputera] [/nowait]] [/rediscover]] /tz unregister}</pre>
w	L/U	Wyświetla bieżących użytkowników i zadania.	<pre>w [-husfvo] [Użytkownik]</pre>
whois	L/U/W	Wyświetla informacje „teledresowe” dotyczące właściciela domeny, adresu IP itd.	<pre>whois [-h komputermacierzysty] Identyfikator</pre>
xinit	L/U	Powoduje uruchomienie sesji systemu X Window. W charakterze interfejsu dla polecenia xinit jest używany skrypt startx.	<pre>x [opcje]</pre>
xcopy	W	Powoduje skopiowanie plików i katalogów łącznie z podkatalogami.	<pre>xcopy Źródło [Cel] [/w] [/p] [/c] [/v] [/q] [/f] [/l] [/g] ↳ [d[:mm-dd-rrrr]] [/u] [/i] [/s [/e]] [/t] [/k] [/r] [/h] ↳ [a m] [/n] [/o] [/x] [/exclude:Plik1[+Plik2]] [+Plik3]] ↳ [{/y /y} [/z]</pre>

Źródło: <http://technet.microsoft.com/en-us/library/bb490864.aspx>.  
Legenda: L = Linux, U = Unix, W = Windows, kursywa oznacza zmienne dane, tekst pogrubiony oznacza tekst wymagany, który musi być wprowadzony. Elementy w nawiasach kwadratowych ([]) są opcjonalne, natomiast w nawiasach klamrowych ({}), oznaczają zbiór możliwości, z których można użyć tylko jednej. Więcej informacji na temat poszczególnych elementów wymienionych poleceń można znaleźć na podanej stronie źródłowej.

## Powłoki sieciowe

Powłoki sieciowe to interfejsy wiersza poleceń obsługujące narzędzia do zarządzania siecią, w szczególności przeznaczone do administracji zdalnej. Konsole to powłoki sieciowe dostępne na wszystkich platformach oraz obsługiwane przez procesy lokalne zainstalowane przez system operacyjny albo oprogramowanie zarządzające. Powłoka sieciowa charakteryzuje się dwoma następującymi wymaganiami:

- ♦ agent, demon lub proces musi istnieć w systemie zdalnym, który akceptuje polecenia, najczęściej w postaci zdalnego wywoływania procedur (ang. *Remote Process Call* — RPC);
- ♦ narzędzie klienta lub powłoka są wymagane w celu formatowania i wysyłania polecenia do zdalnego procesu.

Powłoki dla Windows to między innymi środowisko NetShell dostarczane ze wszystkimi wersjami Windows, jak również PowerShell, czyli środowisko poleceń administracyjnych (skryptowania) dostarczane z systemami Windows Server 2008 i Vista. Powłoka PowerShell ma zastąpić powłokę NetShell oraz inne narzędzia obsługi skryptów Windows CLI. Poniżej pokrótce omówiono niektóre z wymienionych środowisk.

### Powłoka Windows NetShell

W systemie Windows NT wprowadzono NetShell — narzędzie wiersza poleceń dla administratorów sieciowych. Używając powłoki NetShell CLI można wykonywać polecenia wsadowe oraz skrypty bądź wydawać pojedyncze polecenia z poziomu konsoli, które powodują modyfikację ustawień i wykonanie innych operacji w systemach zdalnych. API powłoki NetShell będące częścią Microsoft Windows Software Development Kit (SDK) pozwala programistom na tworzenie pomocniczych bibliotek DLL (ang. *Dynamic Link Libraries*), które implementują różne polecenia powłoki NetShell we własnych programach.

Polecenie powłoki NetShell działa w określonym kontekście, który ma zasięg danego obszaru sieciowego. Na przykład polecenia NetShell działające z pomocniczą biblioteką DLL mogą łączyć się z biblioteką dynamiczną, która kontroluje określone funkcje sieciowe, a następnie modyfikować te funkcje. Często przytaczanym przykładem jest modyfikacja DHCP (ang. *Dynamic Host Configuration Protocol*), gdzie polecenia powłoki NetShell są kierowane do biblioteki *dhcpcsvc.dll*, odpowiedzialnej za zwalnianie, odnawianie i odświeżanie adresów dynamicznych.

Po wczytaniu powłoki NetShell następuje odczytanie rejestru systemu Windows w celu pobrania listy pomocniczych bibliotek DLL, z których większość jest dostarczana wraz z Windows, oraz dodatkowych rozszerzeń możliwych do dodania. Firma Microsoft publikuje listę tych bibliotek pomocniczych w różnych dokumentach Resource Kit.

Główną zaletą powłoki NetShell, oferowaną zwykłemu użytkownikowi Windows lub administratorowi, jest możliwość uruchomienia środowiska powłoki NetShell i wydawanie poleceń z poziomu wiersza poleceń. Aby przejść do powłoki NetShell w kontekście root, należy wykonać następujące kroki:

1. W systemie Windows trzeba kliknąć menu *Start*, a następnie wybrać opcję *Uruchom...*, wpisać *cmd* i nacisnąć klawisz *Enter*.
2. W wierszu poleceń po znaku zachęty *C:\* należy wydać polecenie *netsh* i nacisnąć klawisz *Enter*.

Wyświetli się znak zachęty *netsh>*, wskazujący, że użytkownik znajduje się w powłoce NetShell w kontekście *root*. Opuszczenie środowiska NetShell następuje po wydaniu polecenia *exit* lub *bye*.

Istnieje tak wiele możliwości wykorzystania poleceń powłoki NetShell, że ich opisem można by wypełnić cały rozdział. W ramach powłoki NetShell można zasymulować większość funkcji Eksploratora Windows, co zostanie przedstawione w przykładzie znajdującym się w dalszej części rozdziału. Na rysunku 31.2 pokazano sesję powłoki w systemie Vista, gdzie użytkownik uruchomił powłokę NetShell, a następnie wykonał różne polecenia oferowane przez kontekst *root*. Inne dostępne konteksty to *advfirewall*, *bridge*, *dhcpcclient*, *firewall*, *http*, *interface*, *ipsec*, *lan*, *nap*, *netio*, *p2p*, *ras*, *rpc*, *winhttp* oraz *wlan*. Jeżeli sesja zostanie uruchomiona w systemie Windows Server, to można zobaczyć konteksty powłoki NetShell powiązane z funkcjami serwera. W tabeli 31.2 wymieniono niektóre z najczęściej używanych poleceń *netsh*.

### Rysunek 31.2.

Wyświetlenie poleceń dostępnych w kontekście *root* powłoki NetShell

```

C:\Windows\system32\cmd.exe - netsh
Microsoft Windows [Wersja 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\Robert>netsh
netsh>?

Dostępne są następujące polecenia:

Polecenia w tym kontekście:
?               - Przechodzi jeden poziom kontekstu wyżej.
abort          - Wyświetla listę poleceń.
add            - Odrzuca zmiany wprowadzone w trybie offline.
advfirewall    - Dodaje wpis konfiguracji do listy wpisów.
alias          - Zmiany w kontekście 'netsh advfirewall'.
branchcache    - Dodaje alias.
bridge         - Zmiany w kontekście 'netsh branchcache'.
bye            - Zmiany w kontekście 'netsh bridge'.
commit        - Kończy pracę programu.
delete        - Potwierdza zmiany dokonane w trybie offline.
dhcpcclient    - Usuwa wpis konfiguracji z listy wpisów.
dnscclient     - Zmiany w kontekście 'netsh dhcpcclient'.
dump          - Zmiany w kontekście 'netsh dnscclient'.
exec          - Wyświetla skrypt konfiguracji.
exit          - Uruchamianie plik skryptu.
firewall       - Kończy pracę programu.
help          - Zmiany w kontekście 'netsh firewall'.
http          - Wyświetla listę poleceń.
interface     - Zmiany w kontekście 'netsh http'.
ipsec         - Zmiany w kontekście 'netsh interface'.
lan           - Zmiany w kontekście 'netsh ipsec'.
mbn           - Zmiany w kontekście 'netsh lan'.
namespace    - Zmiany w kontekście 'netsh mbn'.
netio         - Zmiany w kontekście 'netsh namespace'.
offline       - Zmiany w kontekście 'netsh netio'.
online        - Zmienia bieżący tryb na tryb offline.
p2p           - Zmienia bieżący tryb na online.
pushd        - Zmiany w kontekście 'netsh p2p'.
quit          - Zdejmuje kontekst ze stosu.
ras           - Unieszcza bieżący kontekst na stosie.
set           - Kończy pracę programu.
show          - Zmiany w kontekście 'netsh ras'.
trace         - Zmiany w kontekście 'netsh rpc'.
unalias       - Aktualizuje ustawienia konfiguracji.
wcn           - Wyświetla informacje.
wfp           - Zmiany w kontekście 'netsh trace'.
winhttp       - Usuwa alias.
winsock       - Zmiany w kontekście 'netsh wcn'.
wlan          - Zmiany w kontekście 'netsh wfp'.

Dostępne są następujące konteksty podrzędne:
advfirewall branchcache bridge dhcpcclient dnscclient firewall http interface ipsec
lan mbn namespace nap netio p2p ras rpc trace wcn wfp winhttp winsock wlan

Aby wyświetlić pomoc dla polecenia, wpisz polecenie, potem spację, a
następnie wpisz ?.

netsh>

```

**Tabela 31.2.** Polecenia powłoki NetShell

Polecenie	Kontekst	Opis
..	Globalny	Przejdźcie o jeden poziom w górę.
? lub help	Globalny	Wyświetlenie tekstu pomocy dla danego polecenia.
aaaa	Globalny	Wejście do kontekstu aaaa.
aaaa add/delete/set/ ↳show acctserver	RAS	Konfiguruje lub wyświetla serwery rozliczeń RADIUS.
aaaa add/delete/set/ ↳show authserver	RAS	Konfiguruje lub wyświetla serwery uwierzytelniania RADIUS.
aaaa set/show accounting	RAS	Konfiguruje lub wyświetla dostawcę rozliczeń.
aaaa set/show authentication	RAS	Konfiguruje lub wyświetla dostawcę uwierzytelniania.
add alias	Globalny	Dodaje alias do polecenia.
add helper	Globalny	Dodaje bibliotekę pomocniczą DLL do powłoki netsh.
add/delete/show authtype	RAS	Konfiguruje lub wyświetla dozwolone typy uwierzytelniania.
add/delete/show client	RAS	Konfiguruje lub wyświetla aktualne połączenia klientów zdalnych.
add/delete/show link	RAS	Konfiguruje lub wyświetla ustawienia oprogramowania kompresji oraz rozszerzenia LCP (ang. <i>Link Control Protocol</i> ).
add/delete/show multilink	RAS	Konfiguruje lub wyświetla ustawienia protokołu BAP (ang. <i>Multilink and Bandwidth Allocation Protocol</i> ).
add/delete/show registeredserver	RAS	Konfiguruje lub wyświetla ustawienia konfiguracyjne dotyczące tego, kiedy określony serwer zdalny jest członkiem grup bezpieczeństwa RAS i IAS Servers w usłudze katalogowej Active Directory dla określonej domeny.
appletalk set access	RAS	Ustala, kiedy ruch sieciowy AppleTalk pochodzący od klientów zdalnych będzie przekazywany do sieci, z którymi połączony jest dany serwer zdalny.
appletalk set negotiation	RAS	Ustala, kiedy ruch sieciowy AppleTalk będzie negocjowany dla połączeń dostępu zdalnego.
appletalk show config	RAS	Wyświetla konfigurację AppleTalk systemu zdalnego.
cmd	Globalny	Wyświetla okno wiersza poleceń.
commit	Globalny	Zatwierdza zmiany wprowadzone w trybie offline.
delete alias	Globalny	Usuwa alias z wiersza poleceń.
delete helper	Globalny	Usuwa bibliotekę pomocniczą DLL z powłoki netsh.
dhcp	Globalny	Powoduje wejście do kontekstu dhcp.
dump	Globalny	Zapisuje konfigurację w pliku tekstowym.
Exec	Globalny	Wykonuje plik skryptu, który zawiera polecenia powłoki netsh.

**Tabela 31.2.** *Polecenia powłoki NetShell — ciąg dalszy*

Polecenie	Kontekst	Opis
Flush	Globalny	Odrzuca zmiany wprowadzone w trybie offline.
interface	Globalny	Powoduje wejście do kontekstu interface.
interface ip	Globalny	Powoduje wejście do kontekstu interface ip.
interface ipv6	Globalny	Powoduje wejście do kontekstu interface ipv6.
interface portproxy	Globalny	Powoduje wejście do kontekstu interfejsu portproxy.
interface protocol security	Globalny	Powoduje wejście do kontekstu ipsec.
ip add/delete range	Routing	Dodaje lub usuwa zakres adresów z puli statycznych adresów IP.
ip add/delete/set/show filter	Routing	Dodaje, usuwa, konfiguruje bądź wyświetla filtry pakietów IP dla określonego interfejsu.
ip add/delete/set/show interface	Routing	Dodaje, usuwa, konfiguruje bądź wyświetla ogólne ustawienia routingu IP dla określonego interfejsu.
ip add/delete/set/ ↳show persistentroute	Routing	Dodaje, usuwa, konfiguruje lub wyświetla stałe trasy.
ip add/delete/set/ ↳show preference forprotocol	Routing	Dodaje, usuwa, konfiguruje lub wyświetla poziom preferencji dla protokołu routingu.
ip add/delete/set/show rtmroute	Routing	Dodaje, usuwa, konfiguruje lub wyświetla nietrwałe trasy Route Table Manager.
ip add/delete/set/show scope	Routing	Dodaje, usuwa lub wyświetla zakres multemisji.
ip add/delete/show boundary	Routing	Dodaje, usuwa lub wyświetla ustawienia ograniczeń multemisji w określonym interfejsie.
ip autodhcp add/delete exclusion	Routing	Dodaje lub usuwa wyłączenia z zakresu adresów alokatora DHCP.
ip autodhcp set/show global	Routing	Konfiguruje bądź wyświetla globalne parametry alokatora DHCP.
ip autodhcp set/show interface	Routing	Konfiguruje bądź wyświetla ustawienia alokatora DHCP dla określonego interfejsu.
ip delete pool	RAS	Usuwa pulę statycznych adresów IP.
ip dnsproxy set/show global	Routing	Konfiguruje lub wyświetla globalne parametry DNS proxy.
ip dnsproxy set/show interface	Routing	Konfiguruje lub wyświetla parametry DNS proxy dla określonego interfejsu.
ip igmp add/delete/set/ ↳show interface	Routing	Dodaje, usuwa, konfiguruje bądź wyświetla IGMP dla określonego interfejsu.
ip igmp set/show global	Routing	Konfiguruje lub wyświetla globalne ustawienia IGMP.
ip igmp show grouptable	Routing	Wyświetla tabelę grup komputerów macierzystych IGMP.
ip igmp show ifstats	Routing	Wyświetla dane statystyczne dotyczące IGMP dla każdego interfejsu.

**Tabela 31.2.** Polecenia powłoki NetShell — ciąg dalszy

Polecenie	Kontekst	Opis
ip igmp show iftable	Routing	Wyświetla grupy komputerów macierzystych IGMP dla każdego interfejsu.
ip igmp show proxygrouptable	Routing	Wyświetla tabelę grupy IGMP dla interfejsu IGMP proxy.
ip igmp show rasgrouptable	Routing	Wyświetla tabelę grupy dla interfejsu wewnętrznego używanego przez serwer zdalny.
ip nat add/delete addressmapping	Routing	Dodaje lub usuwa mapowanie adresu NAT.
ip nat add/delete addressrange	Routing	Dodaje lub usuwa zakres adresów do puli adresów publicznego interfejsu NAT.
ip nat add/delete portmapping	Routing	Dodaje lub usuwa mapowanie portu NAT.
ip nat add/delete/set/ ↳show interface	Routing	Dodaje, usuwa, konfiguruje bądź wyświetla ustawienia tłumaczenia adresów sieciowych (NAT) dla określonego interfejsu.
ip nat set/show global	Routing	Konfiguruje lub wyświetla globalne ustawienia tłumaczenia adresów sieciowych (NAT).
ip ospf add/delete/set/show area	Routing	Dodaje, usuwa, konfiguruje bądź wyświetla obszar OSPF.
ip ospf add/delete/set/ ↳show interface	Routing	Dodaje, usuwa, konfiguruje bądź wyświetla protokół dynamicznego routingu OSPF w określonym interfejsie.
ip ospf add/delete/set/ ↳show virtif	Routing	Dodaje, usuwa, konfiguruje bądź wyświetla interfejs wirtualny protokołu dynamicznego routingu OSPF.
ip ospf add/delete/ ↳show neighbor	Routing	Dodaje, usuwa, konfiguruje bądź wyświetla otoczenie sieciowe protokołu dynamicznego routingu OSPF.
ip ospf add/delete/ ↳show protofilter	Routing	Dodaje, usuwa, konfiguruje bądź wyświetla źródła informacji o routingu dla zewnętrznych tras protokołu dynamicznego routingu OSPF.
ip ospf add/delete/ ↳show routefilter	Routing	Dodaje, usuwa, konfiguruje bądź wyświetla filtrowanie tras dla zewnętrznych tras protokołu dynamicznego routingu OSPF.
ip ospf set/show global	Routing	Konfiguruje lub wyświetla globalne ustawienia protokołu dynamicznego routingu OSPF. Funkcja ta nie jest dostępna w systemach operacyjnych Windows działających w systemach bazujących na Itanium. Ta treść nie jest dostępna w tym wczesnym wydaniu.
ip ospf show areastats	Routing	Wyświetla dane statystyczne obszaru OSPF.
ip ospf show lsdb	Routing	Wyświetla stan bazy danych dla łącza OSPF.
ip ospf show virtifstats	Routing	Wyświetla dane statystyczne dla wirtualnego łącza OSPF.
ip relay add/delete dhcpserver	Routing	Dodaje lub usuwa adresy IP serwera DHCP do listy adresów serwera DHCP.
ip relay add/delete/set interface	Routing	Dodaje, usuwa lub konfiguruje ustawienia agenta przekazywania DHCP w określonym interfejsie.

**Tabela 31.2.** *Polecenia powłoki NetShell — ciąg dalszy*

Polecenie	Kontekst	Opis
ip relay set global	Routing	Konfiguruje globalne ustawienia agenta przekazywania DHCP.
ip relay show ifbinding	Routing	Wyświetla adresy IP powiązane z interfejsami.
ip relay show ifconfig	Routing	Wyświetla konfigurację agenta przekazywania DHCP dla każdego interfejsu.
ip relay show ifstats	Routing	Wyświetla dane statystyczne DHCP dla każdego interfejsu.
ip set access	RAS	Ustala, kiedy ruch sieciowy IP pochodzący od zdalnych klientów będzie przekazywany do sieci, z którymi połączony jest zdalny serwer.
ip set addrassign	RAS	Konfiguruje metodę, za której pomocą zdalny serwer będzie przypisywał adresy IP połączeniom przychodzącym.
ip set addrreq	RAS	Ustala, kiedy klienci zdalnych systemów lub routery połączeń na żądanie mogą żądać własnych adresów IP.
ip set negotiation	RAS	Ustala, kiedy negocjacje IP będą przeprowadzane dla połączeń dostępu zdalnego.
ip set/show loglevel	Routing	Ustala lub wyświetla globalny poziom rejestrowania zdarzeń w dzienniku zdarzeń dla protokołu IP.
ip show boundarystats	Routing	Wyświetla ograniczenia dla multiemisji IP.
ip show config	RAS	Wyświetla konfigurację IP dla dostępu zdalnego.
ip show helper	Routing	Wyświetla subkonteksty IP dla wszystkich narzędzi powłoki netsh.
ip show mfe	Routing	Wyświetla wpisy dotyczące przekazywania multiemisji.
ip show mfe stats	Routing	Wyświetla wpisy dotyczące danych statystycznych przekazywania multiemisji.
ip show protocol	Routing	Wyświetla wszystkie działające protokoły routingu IP.
ip show rtmdestinations	Routing	Wyświetla miejsca docelowe w tabeli routingu Route Table Manager.
ip show rtmroutes	Routing	Wyświetla trasy w tabeli routingu Route Table Manager.
network bridge	Globalny	Powoduje wejście do kontekstu bridge.
network diagnostics (diag)	Globalny	Powoduje wejście do kontekstu diag.
offline	Globalny	Ustawia tryb na offline.
online	Globalny	Ustawia tryb na online.
Popd	Globalny	Usuwa kontekst ze stosu. Stos jest przechowywanym buforem ostatnio wydanych poleceń.
pushd	Globalny	Umieszcza aktualny kontekst w stosie.
quit lub by albo exit	Globalny	Powoduje wyjście z powłoki netsh.
ras set/show authmode	RAS	Ustala, czy i kiedy połączenia komutowane będą uwierzytelniane, lub wyświetla informacje o tym.

**Tabela 31.2.** Polecenia powłoki NetShell — ciąg dalszy

Polecenie	Kontekst	Opis
Remote access	Globalny	Powoduje wejście do kontekstu ras.
routing	Globalny	Powoduje wejście do kontekstu routing.
rpc helper	Globalny	Powoduje wejście do kontekstu rpc.
set audit-logging	Globalny	Włącza lub wyłącza zapis w dzienniku zdarzeń.
set loglevel	Globalny	Ustawia poziom zapisu informacji w dzienniku zdarzeń.
set machine	Globalny	Ustawia system, względem którego będą wykonywane polecenia powłoki NetShell.
set mode	Globalny	Ustawia tryb na online lub offline.
set/show authmode	RAS	Konfiguruje lub wyświetla ustawienia konfiguracyjne dotyczące tego, czy i kiedy połączenia komutowane będą uwierzytelniane.
set/show credentials	Interface	Konfiguruje lub wyświetla nazwę użytkownika, hasło oraz nazwę domeny dla interfejsu połączenia na żądanie.
set/show interface	Interface	Włącza, wyłącza, łączy, rozłącza interfejsy połączeń na żądanie oraz wyświetla ich konfigurację.
set/show tracing	RAS	Konfiguruje lub wyświetla ustawienia dotyczące śledzenia.
set/show user	RAS	Konfiguruje lub wyświetla ustawienia zdalnego dostępu dla kont użytkowników.
show activeservers	RAS	Wyświetla bieżące serwery, w których działa routing lub remote access w sieci.
show alias	Globalny	Wyświetla wszystkie zdefiniowane aliasy.
show audit-logging	Globalny	Wyświetla ustawienia dotyczące zapisu informacji w dzienniku zdarzeń.
show helper	Globalny	Wyświetla biblioteki pomocnicze DLL w powłoce netsh.
show loglevel	Globalny	Wyświetla dane dotyczące poziomu zapisu informacji w dzienniku zdarzeń.
show machine	Globalny	Wyświetla system, względem którego będą wykonywane polecenia powłoki NetShell.
show mode	Globalny	Wyświetla aktualny tryb.
show netdlls	Globalny	Wyświetla wersje bibliotek pomocniczych DLL w powłoce netsh.
show version	Globalny	Wyświetla wersję systemu Windows oraz narzędzia netsh.
wins	Globalny	Powoduje wejście do kontekstu wins.

Źródło: Microsoft Technet (<http://technet.microsoft.com/en-us/default.aspx>).

Powszechnym celem użycia powłoki NetShell jest uruchamianie i zatrzymywanie usług sieciowych. Służące do tego polecenie ma następującą składnię:

```
net [start/stop/pause/continue] <nazwa_uslugi>
```

Powyższe polecenia powielają działania dostępne w konsoli usług Windows i odpowiadają kliknięciu przycisków *Uruchom*, *Zatrzymaj*, *Wstrzymaj* i *Wznów*. W przypadku usługi, o której można sądzić, że działa nieprawidłowo lub uległa zawieszeniu, istnieje możliwość wykonania poniższej sekwencji, co prowadzi do ponownego uruchomienia usługi:

```
netsh>net stop dhcp  
netsh>net start dhcp
```

Powłoka NetShell pozwala na wykonywanie poniższych głównych klas poleceń:

- ♦ NET — zarządzanie zasobami sieciowymi;
- ♦ MODE — konfiguracja urządzeń systemowych;
- ♦ SC — zezwolenie na kontrolę usługi;
- ♦ PsService — zapewnienie możliwości przeglądania i kontrolowania usług;
- ♦ WMI Service — zezwolenie użytkownikowi na uzyskanie dostępu do kontroli WMI nad usługami.

## Sesje Telnet

Telnet oznacza protokół sieci telekomunikacyjnej (ang. *Telecommunications Network*) i jest jednym z najwcześniejszych protokołów internetowych. Za pomocą klienta Telnet można użyć powłoki CLI w celu wykonywania poleceń w systemie zdalnym. Z powodu swojej długiej historii Telnet jest obsługiwany we wszystkich sieciowych systemach operacyjnych, a ponadto dostępnych jest wiele klientów Telnet opracowanych przez firmy trzecie. Popularność Telnetu jest ograniczona głównie do systemów z rodziny Unix (dotyczy to szczególnie użytkowników starszych stażem); na nowoczesnych kursach z zakresu administrowania siecią zwykle przedstawiane są inne metody przeprowadzania tekstowych sesji powłoki.

Telnet to 8-bitowy protokół transmisyjny, którego polecenia są przekazywane w postaci 7-bitowego ASCII wraz z pojedynczym znakiem z górnego zestawu ASCII, określanym jako „znak Telnet”. Port TCP o numerze 23 to doskonale znany port Telnet. Wprawdzie wczesne wersje Telnet nie były standaryzowane, ale wersje wydane po roku 1973 zwykle są zgodne z tym, co określa się mianem standardu „Net Telnet”, który stanowi rozszerzenie dokumentu IETF RFC 15. Używane rozszerzenia oznaczają, że Telnet w danym sieciowym systemie operacyjnym (NOS) może być nieco odmienny od Telnetu w innym systemie operacyjnym.

Wprawdzie Telnet jest wygodny, przystępny i łatwy w użyciu, ale pewne rządzące nim reguły powodują, że jest niebezpieczny:

- ♦ sesje Telnet powodują wysyłanie i odbieranie zwykłego tekstu, nieszyfrowanych danych, które można łatwo przechwycić;
- ♦ demony (procesy) Telnet były wielokrotnie atakowane i dotąd nie zostały skutecznie zabezpieczone;
- ♦ sesje Telnet nie pozwalają określić, czy punkty końcowe połączenia są autentyczne; użytkownik po prostu podaje swoją nazwę, którą można przechwycić.

Podjęmowano sporadyczne próby dodania zabezpieczeń do protokołu Telnet, ale w większości przypadków używanie klientów SSH okazało się znacznie lepszym rozwiązaniem do prowadzenia zdalnych sesji powłoki. Jednak nadal można się spotkać z wykorzystywaniem

Telnetu w komputerach typu mainframe i starszych systemach, a także jako sposobu wejścia do routerów i przełączników sieciowych w bardzo nietypowych sytuacjach. Narzędzie typu open source o nazwie PuTTY (<http://www.chiark.greenend.org.uk/~sgtatham/putty/>) to połączenia klienta Telnet i SSH, którego można używać w systemach zarówno Windows i Unix, jak i w emulatorze terminalu xterm.

Począwszy od systemu Windows Vista, firma Microsoft zaprzestała wydawania klienta Telnet jako standardowej części systemu. Jednak klienta Vista Telnet można łatwo zainstalować z powrotem w systemie Vista jako komponent dodatkowy. Listę różnych poleceń klienta Telnet można znaleźć na stronie <http://technet.microsoft.com/en-us/library/bb491013.aspx>.

## PowerShell

PowerShell to ostatnia wersja interfejsu wiersza poleceń, wprowadzona w systemach Windows Server 2008 i Vista (dostępna również dla systemów Windows Server 2003 i XP), służąca do administrowania. PowerShell konsoliduje powłokę CLI i standaryzowany język zawierający ponad 60 poleceń oraz możliwość uruchamiania skryptów. Powłoka PowerShell została zaprojektowana z zachowaniem wstecznej zgodności ze starszymi technologiami firmy Microsoft i innymi powszechnie używanymi powłokami CLI na innych platformach. Polecenia powłoki PowerShell mogą dotyczyć tysięcy obiektów, między innymi Windows, Office, platformy .NET i WMI. Ponadto mogą być wykonywane w systemach zarówno lokalnych, jak i zdalnych, rejestrach, usłudze katalogowej Active Directory oraz usługach. Celem, który przyświecał firmie Microsoft, było przepisanie konsoli wiersza poleceń aplikacji przemysłowych i wykorzystanie powłoki PowerShell jako struktury bazowej dla wspomnianych konsol. Najnowsza wersja serwera Exchange to jednocześnie pierwsza aplikacja dostarczana z konsolą zarządzającą tego rodzaju.

Wśród wielu funkcji, które można kontrolować za pomocą powłoki PowerShell, znajdziemy:

- ♦ zarządzanie systemem lokalnym i zdalnym;
- ♦ usługi systemowe, procesy i rejestr;
- ♦ obiekty ActiveX Data Object (ADO), Component Object Model (COM) i platformy .NET;
- ♦ obiekty Active Directory Service Interface (ADSI);
- ♦ obiekty Windows Management Instrumentation (WMI);
- ♦ zarządzanie serwerem Terminal Server i jego konfiguracja;
- ♦ zarządzanie serwerem Internet Information Services 7.0 i jego konfiguracja;
- ♦ pliki HTML lub bazujące na XML;
- ♦ skrypty utworzone w różnych językach skryptowych lub wdrożone za pomocą Windows Scripting Host.

Powłoka Windows PowerShell to zarówno powłoka Windows, jak i środowisko interpretera poleceń z wbudowanym językiem skryptowym. Silnik środowiska uruchomieniowego PowerShell składa się z własnego analizatora składni i automatyzacji dołączania parametrów

poleceń. Początkowo powłoka PowerShell 1.0 była dostarczana ze 129 wbudowanymi poleceniami `cmdlet`, które mogły być stosowane do obiektów. Niektóre z tych poleceń mogły być używane do formatowania i wyświetlania wyników w PowerShell CLI.



Witryna powłoki PowerShell mieści się pod adresem <http://www.microsoft.com/powershell> i zawiera informacje dotyczące pobrania tego środowiska. Wersja 1.0 działa w systemach Windows XP, Server 2003, Vista, Server 2008, Windows 7 i jest dostępna dla platform x86, x86-64 oraz IA-64 (Itanium). Wersja 2.0 została wydana pod koniec roku 2009. Późniejsze wersje wymienionych systemów operacyjnych mają powłokę PowerShell dostępną jako dodatek Windows znajdujący się na nośniku dystrybucyjnym systemu operacyjnego.

Aby uruchomić powłokę PowerShell z wiersza poleceń, należy wykonać poniższe kroki:

1. Kliknąć menu *Start*, a następnie *Uruchom...* bądź nacisnąć klawisze *Windows+R* i wpisać `cmd` w wyświetlonym oknie dialogowym.
2. Następnie należy nacisnąć klawisz *Enter* w celu uruchomienia wiersza poleceń.
3. Trzeba przejść do katalogu zawierającego program PowerShell, wydając polecenie `%SystemRoot%\System32\WindowsPowerShell\v2.0`, a następnie nacisnąć klawisz *Enter*.
4. Wydanie polecenia `powershell.exe -NoProfile` powoduje uruchomienie powłoki PowerShell bez profilu używanego do modyfikacji programu.

Inna możliwość to uruchomienie powłoki PowerShell bezpośrednio z menu *Start* — należy wybrać *Start/Wszystkie Programy/Akcesoria/Windows PowerShell*, a następnie kliknąć *Windows PowerShell*, co spowoduje uruchomienie powłoki.

Uruchomienie powłoki powoduje wczytanie konsoli i modułów (zbioru `cmdlet` i dostawców), a następnie przetwarzane są pliki profilu. Profil można potraktować jako skrypt, który dostosowuje środowisko PowerShell do potrzeb użytkownika, dodaje aliasy, zmienia konfigurację konsoli oraz dodaje pewne funkcje specjalne. Profil może być zastosowany dla administratora, wszystkich użytkowników, pojedynczego użytkownika bądź grupy użytkowników. Powłoka PowerShell ma funkcję „Execution Policy”, która uniemożliwia użytkownikom wykonywanie skryptów bez określonych zabezpieczeń.

Powłoka PowerShell wykorzystuje zbiór poleceń `cmdlet` oraz dostawców, co tworzy moduły o powiązanych ze sobą funkcjach. Każdy moduł działa w ramach własnej przestrzeni nazw. Na przykład przestrzeń nazw modułu Core to `Microsoft.PowerShell.Core`. Polecenia modułu Core zmieniają sposób działania silnika powłoki PowerShell. Inne dostępne moduły to `Host`, `Management`, `Security` i `Utility`. Aby sprawdzić, które moduły zostały zainstalowane, należy wydać poniższe polecenie:

```
get-psnapin
```

W celu określenia poleceń `cmdlet` znajdujących się w module trzeba użyć poniższego polecenia:

```
GET-command -commandtype cmdlet | where-object {$_.psnapin -match "<nazwa_modulu>"}
```

Aby wyświetlić dołączonych dostawców, należy zastosować poniższe polecenie:

```
get-psprovider | format-table name, psnapin
```

W tabeli 31.3 wymieniono niektóre z najważniejszych poleceń `cmdlet` powłoki PowerShell.

Tabela 31.3. Polecenia cmdlet w powłoce PowerShell 1.0

Nazwa	Definicja	Opis
add-content (ac)	add-content [-Path] <String[]> [-Value] <Object[]...>	Dodanie treści do elementu.
add-history	add-history [[-InputObject] <PSObject[]>] [-Pass...]	Dodanie wpisów do sesji historii.
add-member	add-member [-MemberType] <PSMemberTypes> [-Name]...	Dodanie elementu składowego do określonego obiektu powłoki PowerShell.
add-psnapin	add-psnapin [-Name] <String[]> [-PassThru] [-Ve...]	Dodanie modułu do konsoli.
clear-content (clc)	clear-content [-Path] <String[]> [-Filter <Strin...>	Usunięcie treści z elementu bądź wskazanego położenia.
clear-host (clear/clh)	clear-host	Wyczyszczenie zawartości ekranu.
clear-item (cli)	clear-item [-Path] <String[]> [-Force] [-Filter ...]	Usunięcie treści ze zmiennej lub aliasu.
clear-itemproperty (cIp)	clear-itemproperty [-Path] <String[]> [-Name] <S...>	Usunięcie właściwości z elementu.
clear-variable (clv)	clear-variable [-Name] <String[]> [-Include <Str...>	Usunięcie wartości zmiennej.
compare-object	compare-object [-ReferenceObject] <PSObject[]> [...]	Porównanie wskazanych obiektów.
convertfrom-securestring	convertfrom-securestring [-SecureString] <Secure...>	Konwersja bezpiecznego ciągu tekstowego na standard zaszyfrowanego ciągu tekstowego.
convert-path (cvpa)	convert-path [-Path] <String[]> [-Verbose] [-Deb...]	Konwersja ścieżki dostępu PS na ścieżkę dostępu dostawcy.
convertto-html	convertto-html [[-Property] <Object[]>] [-Input0...]	Konwersja danych wejściowych na postać tabeli HTML.
convertto-securestring	convertto-securestring [-String] <String> [-Sec...]	Konwersja ciągu tekstowego, zaszyfrowanego za pomocą standardu, na postać bezpiecznego ciągu tekstowego.
copy-item (copy/cpi)	COPY-ITEM [-Path] <String[]> [[-Destination] <St...>	Skopiowanie elementu ze wskazanego położenia w przestrzeni nazw.
copy-itemproperty (cpp)	copy-itemproperty [[-path]] [-literalPath] ] string[] ↳ [[-destination] string[]]...	Skopiowanie właściwości wraz z jej wartością.
do	[ :Etykieta_pętl ] do { blok_poleceń } while (warunek)	Pętla będzie wykonywana, dopóki warunek przyjmuje wartość true.

Tabela 31.3. Polecenia cmdlet w powłoce PowerShell 1.0 — ciąg dalszy

Nazwa	Definicja	Opis
Exit		Wyjście z powłoki PowerShell lub skryptu.
export-alias	export-alias [-Path] <String> [[-Name] <String>]...	Eksport do pliku listy aliasów.
export-clixml	export-clixml [-Path] <String> [-Depth <Int32>] ...	Utworzenie pliku CLIXML zawierającego obiekty powłoki PowerShell.
export-console	export-console [[-Path] <String>] [-Force] [-NoC...]	Eksport konfiguracji konsoli do pliku.
export-csv (epcsv)	export-csv [-Path] <String> -InputObject <PSObject>...	Eksport do formatu CSV, czyli wartości rozdzielonych przecinkami (format arkusza kalkulacyjnego).
for	for (wartość początkowa; warunek; powtórzenie) {blok_poleceń}	Polecenia pętli będą wykonywane dla elementów, które spełniają warunek.
foreach (foreach)	foreach (element in kolekcja) {BlokSkryptu}	Polecenia pętli będą wykonywane dla każdej wartości w potoku.
foreach-object	foreach-object [-Process] <ScriptBlock> [-Input...]	Polecenia pętli będą wykonywane dla każdego obiektu w potoku powłoki PowerShell.
format-custom (fc)	format-custom [[-Property] <Object>] [-Depth <...>]	Utworzenie własnego formatu do wyświetlenia danych wyjściowych.
format-list (fl)	format-list [[-Property] <Object>] [-GroupBy <...>]	Sformatowanie danych wyjściowych na postać listy właściwości.
format-table (ft)	format-table [[-Property] <Object>] [-AutoSize...]	Sformatowanie danych wyjściowych na postać tabeli.
format-wide (fw)	format-wide [[-Property] <Object>] [-AutoSize] [...]	Sformatowanie danych wyjściowych na postać tabeli zawierającej pojedynczą właściwość.
get-acl	get-acl [[-Path] <String>] [-Audit] [-Filter <...>]	Pobranie uprawnień dla pliku bądź klucza rejestru.
get-alias (gal)	get-alias [[-Name] <String>] [-Exclude <String>]...	Zwrócenie nazwy aliasu dla danego polecenia cmdlet.
get-authenticode signature	get-authenticode signature [-FilePath] <String>...	Pobranie obiektu sygnatury pliku.
get-childitem (dir/ls/gci)	get-childitem [[-Path] <String>] [[-Filter] <S...>]	Pobranie zawartości katalogu bądź klucza rejestru, który odnosi się do elementu potomnego.
get-command (gcm)	get-command [[-ArgumentList] <Object>] [-Verb ...]	Zwrócenie opisu danego polecenia.

get-content (cat/type/gc)	get-content [-Path] <String[]> [-ReadCount <Int64> ...]	Pobranie treści z elementu bądź wskazanego położenia.
get-credential	get-credential [-Credential] <PSCredential[]> [-Verbose] ...	Pobranie danych uwierzytelniających (nazwa użytkownika i hasło).
get-culture	get-culture [-Verbose] [-Debug] [-ErrorAction <Action> ...]	Pobranie informacji dotyczących opcji regionalnych i językowych systemu.
get-date	get-date [[-Date] <DateTime>] [-Year <Int32>] [-Format <String>] ...	Pobranie bieżącej daty i czasu.
get-eventlog	get-eventlog [-LogName] <String> [-Newest <Int32>] [-ErrorAction <Action> ...]	Pobranie danych dziennika zdarzeń.
get-executionpolicy	get-executionpolicy [-Verbose] [-Debug] [-ErrorAction <Action> ...]	Pobranie informacji o polityce wykonywania stosowanej w powłocie.
get-help (help)	get-help [[-Name] <String>] [-Category <String>] [-ErrorAction <Action> ...]	Otworzenie pliku pomocy.
get-history (history/h/ghy)	get-history [[-Id] <Int64>] [[-Count] <Int32>] [-ErrorAction <Action> ...]	Pobranie informacji o poleceniach zapisanych w sesji historii.
get-host	get-host [-Verbose] [-Debug] [-ErrorAction <Action> ...]	Pobranie informacji o komputerze macierzystym (systemie).
get-item (gi)	get-item [-Path] <String[]> [-Filter <String>] [-ErrorAction <Action> ...]	Pobranie pliku, obiektu rejestru lub innego obiektu przestrzeni nazw.
get-itemproperty (gp)	get-itemproperty [-Path] <String[]> [[-Name] <String>] [-ErrorAction <Action> ...]	Pobranie właściwości obiektu.
get-location (pwd/ gl)	get-location [-PSProvider <String>] [-Path <String>] [-ErrorAction <Action> ...]	Pobranie i wyświetlenie informacji dotyczących bieżącego położenia.
get-member (gm)	get-member [[-Name] <String>] [-InputObject <PSObject>] [-ErrorAction <Action> ...]	Wyświetlenie właściwości obiektu.
get-pfxcertificate	get-pfxcertificate [-FilePath] <String> [-Verbose] [-ErrorAction <Action> ...]	Pobranie informacji o certyfikacie PF.
get-process (ps/gps)	get-process [[-Name] <String>] [-Verbose] [-ErrorAction <Action> ...]	Pobranie listy procesów działających w komputerze.
get-psdrive (gdr)	get-psdrive [[-Name] <String>] [-Scope <String>] [-ErrorAction <Action> ...]	Pobranie informacji DriveInfo dla wskazanego napędu PSDrive.
get-psprovider	get-psprovider [[-PSProvider] <String>] [-Verbose] [-ErrorAction <Action> ...]	Pobranie informacji dotyczących wskazanego dostawcy.
get-pssnapin	get-pssnapin [[-Name] <String>] [-Registered] [-ErrorAction <Action> ...]	Wyświetlenie modułów powłoki PowerShell używanych na danym komputerze.
get-service (gsv)	get-service [[-Name] <String>] [-Include <String>] [-ErrorAction <Action> ...]	Pobranie listy usług.

Tabela 31.3. Polecenia cmdlet w powłoce PowerShell 1.0 — ciąg dalszy

Nazwa	Definicja	Opis
get-tracesource	get-tracesource [-Name] <String[]> [-Verbose] ...	Pobranie komponentów używanych podczas śledzenia.
get-uiculture	get-uiculture [-Verbose] [-Debug] [-ErrorAction] ...	Pobranie informacji regionalnych i językowych dotyczących interfejsu użytkownika.
get-unique (gu)	get-unique [-InputObject <PSObject>] [-AsString] ...	Pobranie unikalnych elementów w kolekcji.
get-variable (gv)	get-variable [-Name] <String[]> [-ValueOnly] [...]	Pobranie zmiennej PowerShell.
get-wmiobject (gwmi)	get-wmiobject [-Class] <String> [[-Property] <String>] ...	Pobranie egzemplarzy klas WMI lub informacji o dostępnych klasach.
group-object (group)	group-object [[-Property] <Object[]>] [-NoElement] ...	Zgrupowanie obiektów zawierających tę samą wartość dla właściwości współdzielonej.
if	if (warunek) { polecenia_do_wykonania } [ elseif (warunek2) { polecenia_do_wykonania } ] else { polecenia_do_wykonania } ...	Wykonywanie poleceń na podstawie stanu warunku.
import-alias (ipal)	import-alias [-Path] <String> [-Scope <String>] ...	Import aliasu z pliku.
import-clixml	import-clixml [-Path] <String[]> [-Verbose] [-De...]	Import pliku CLIXML i jego użycie w celu ponownego zbudowania obiektu PS.
import-csv (ipcsv)	import-csv [-Path] <String[]> [-Verbose] [-Debug] ...	Pobranie wartości z pliku CSV i wysłanie obiektów do potoku.
invoke-expression	invoke-expression [-Command] <String> [-Verbose] ...	Wykonanie wyrażenia powłoki PowerShell.
invoke-history (r/ihy)	invoke-history [[-Id] <String>] [-Verbose] [-Deb...]	Wywołanie z historii poprzednio uruchomionego polecenia cmdlet.
invoke-item (ii)	invoke-item [-Path] <String[]> [-Filter <String>] ...	Wywołanie pliku wywoływalnego, czyli otworenie pliku.
join-path	join-path [-Path] <String[]> [-ChildPath] <String> ...	Połączenie ścieżki dostępu z potonną ścieżką dostępu.
measure-command	measure-command [-Expression] <ScriptBlock> [-In...]	Pomiar czasu wykonywania polecenia cmdlet.
measure-object	measure-object [[-Property] <String[]>] [-Input0...]	Pomiar właściwości obiektu.
move-item (move/mv/mi)	move-item [-Path] <String[]> [[-Destination] <St...]	Przeniesienie elementu do nowego położenia.

move-itemproperty (mp)	move-itemproperty [-Path] <String[]> [-Destination]...	Przeniesienie właściwości z jednego położenia do drugiego.
new-alias (na)	new-alias [-Name] <String> [-Value] <String> [-D...]...	Utworzenie aliasu.
new-item (ni)	new-item [-Path] <String[]> [-ItemType <String>]...	Utworzenie nowego elementu w przestrzeni nazw.
new-itemproperty	new-itemproperty [-Path] <String[]> [-Name] <String>...	Ustawienie nowej właściwości elementu w podanym położeniu.
new-object	new-object [-TypeName] <String> [[[-ArgumentList]...]...	Utworzenie nowego obiektu .NET.
new-psdrive (mount/ndr)	new-psdrive [-Name] <String> [-PSProvider] <String>...	Utworzenie nowego napędu PSDrive.
new-service	new-service [-Name] <String> [-BinaryPathName] <String>...	Utworzenie nowej usługi.
new-timespan	new-timespan [[[-Start] <DateTime>] [[[-End] <DateTime>]...	Utworzenie obiektu TimeSpan.
new-variable (nv)	new-variable [-Name] <String> [[[-Value] <Object>]...	Utworzenie nowej zmiennej.
out-default	out-default [-InputObject] <PSObject> [-Verbose]...	Wysłanie danych wyjściowych do domyślnego wyjścia.
out-file	out-file [-FilePath] <String> [[[-Encoding] <String>]...	Wysłanie danych wyjściowych polecenia do pliku.
out-host (oh)	out-host [-Paging] [-InputObject] <PSObject> [-V...]...	Wysłanie danych wyjściowych potoku do komputera macierzystego.
out-null	out-null [-InputObject] <PSObject> [-Verbose] [-...]...	Wysłanie danych wyjściowych do urządzenia null.
out-printer (lp)	out-printer [[[-Name] <String>] [-InputObject] <PSObject>...	Wysłanie danych wyjściowych do drukarki.
out-string	out-string [-Stream] [-Width <Int32>] [-InputObject]...	Wysłanie obiektów do komputera macierzystego w postaci ciągów tekstowych.
pop-location (popd)	pop-location [-PassThru] [-StackName <String>] [-...]...	Ustawienie bieżącego położenia na podstawie stosu.
powershell	ps	Uruchomienie sesji konsoli PowerShell.
push-location (pushd)	push-location [[[-Path] <String>] [-PassThru] [-S...]...	Usunięcie bieżącej pozycji ze stosu.
quest ad cmdlets		Odczyt lub zapis do usługi katalogowej.
read-host	read-host [[[-Prompt] <Object>] [-AsSecureString]...]...	Odczyt wiersza danych wejściowych z konsoli komputera macierzystego.

Tabela 31.3. Polecenia cmdlet w powłoce PowerShell 1.0 — ciąg dalszy

Nazwa	Definicja	Opis
remove-item ↳ (rm)/del/erase/rmdir/rmdir	remove-item [-Path] <String[]> [-Filter <String>...]	Usunięcie elementu.
remove-itemproperty (rp)	remove-itemproperty [-Path] <String[]> [-Name] <...>	Usunięcie z elementu właściwości i jej wartości.
remove-psdrive (rdr)	remove-psdrive [-Name] <String[]> [-PSProvider <...>]	Usunięcie zdefiniowanego napędu PSDrive.
remove-pssnapin	remove-pssnapin [-Name] <String[]> [-PassThru] [...]	Usunięcie z komputera modułu powłoki PowerShell.
remove-variable (rv)	remove-variable [-Name] <String[]> [-Include <String>...]	Usunięcie zmiennej.
rename-item (ren/rni)	rename-item [-Path] <String> [-NewName] <String>...	Zmiana nazwy elementu.
rename-itemproperty (rnp)	rename-itemproperty [-Path] <String> [-Name] <String>...	Zmiana nazwy właściwości elementu.
resolve-path (rvpa)	resolve-path [-Path] <String[]> [-Credential <PSObject>]	Przetłumaczenie znaków wieloznacznych w ścieżce dostępu.
restart-service	restart-service [-Name] <String[]> [-Force] [-PassThru] [-Pa...]	Zatrzymanie i ponowne uruchomienie usługi.
resume-service	resume-service [-Name] <String[]> [-PassThru] [-...]	Wznowienie pracy usługi, której działanie zostało wcześniej zawieszone.
run/call (&)	& [cmdlet]	Wykonanie polecenia (operator wywołania).
select-object (select)	select-object [[-Property] <Object[]>] [-InputObject...]	Wybór właściwości obiektu.
select-string	select-string [-Pattern] <String[]> -InputObject...]	Przeszukiwanie ciągów tekstowych i plików w celu dopasowania wzorca.
set-acl	set-acl [-Path] <String[]> [-AclObject] <Object>...	Ustawienie uprawnień.
set-alias (sal)	set-alias [-Name] <String> [-Value] <String> [-D...]	Utworzenie bądź zmiana aliasu.
set-authenticodesignature	set-authenticodesignature [-FilePath] <String[]>...	Umieszczenie sygnatury w pliku lub skrypcie .psl.
set-content (sc)	set-content [-Path] <String[]> [-Value] <Object>...	Pobranie i ustawienie zawartości z elementu bądź wskazanego położenia.
set-date	set-date [-Date] <DateTime> [-DisplayHint <Display>...]	Ustawienie bieżącej daty i godziny dla systemu.

set-executionpolicy	set-executionpolicy [-ExecutionPolicy] <ExecutionPolicy> [-Value] <Object> [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Modyfikacja danych polityki wykonywania dla powłoki na podstawie preferencji użytkownika.
set-item (si)	set-item [-Path] <String[]> [-Value] <Object> [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Zmiana wartości elementu.
set-itemproperty (sp)	set-itemproperty [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Ustawienie wartości właściwości.
set-location (cd/chdir/sl)	set-location [-Path] <String> [-PassThru] [-Ve...]	Ustawienie aktualnej lokalizacji roboczej.
set-psdebug	set-psdebug [-Trace <Int32>] [-Step] [-Strict] [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Włączenie lub wyłączenie skryptu usuwania błędów.
set-service	set-service [-Name] <String> [-DisplayName <String> [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Zmiana trybu uruchomienia lub właściwości usługi.
set-tracetrace	set-tracetrace [-Name] <String> [-Option] <String> [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Komponent powłoki PowerShell odpowiedzialny za śledzenie.
set-variable (set/sv)	set-variable [-Name] <String> [-Value] <Object> [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Ustawienie lub zapisanie wartości w zmiennej.
sort-object (sort)	sort-object [-Property] <Object[]> [-Descending] [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Sortowanie obiektów według wartości właściwości.
split-path	split-path [-Path] <String[]> [-LiteralPath <String> [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Zwrócenie fragmentu ścieżki dostępu.
start-service (stsv)	start-service [-Name] <String[]> [-PassThru] [-I...]	Uruchomienie usługi.
start-sleep (sleep)	start-sleep [-Seconds] <Int32> [-Verbose] [-Debug] [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Zawieszenie aktywności powłoki lub skryptu.
start-transcript	start-transcript [-Path] <String> [-Append] [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Rozpoczęcie procesu transkrypcji sesji poleceń powłoki.
stop-process (kill/spps)	stop-process [-Id] <Int32[]> [-PassThru] [-Verbose] [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Zatrzymanie działającego procesu.
stop-service (spsv)	stop-service [-Name] <String[]> [-Force] [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Zatrzymanie usługi.
stop-transcript	stop-transcript [-Verbose] [-Debug] [-ErrorAction] [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Zatrzymanie procesu transkrypcji.
switch		Wiele poleceń if.
suspend-service	suspend-service [-Name] <String[]> [-PassThru] [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Zawieszenie działania aktywnej usługi.
tee-object	tee-object [-FilePath] <String> [-InputObject <P...]	Wysłanie obiektów danych wejściowych do dwóch miejsc.
test-path	test-path [-Path] <String[]> [-Filter <String> [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Zwraca wartość true, jeśli ścieżka dostępu istnieje. W przeciwnym razie wartość zwrócona jest false.
trace-command	trace-command [-Name] <String[]> [-Expression] <String> [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Śledzenie polecenia bądź wyrażenia.
update-formatdata	update-formatdata [[-AppendPath] <String[]> [-Path] <String[]> [-Name] <String[]> [-PassThru] [-Ve...]	Uaktualnienie i dodanie plików formatu danych.

Tabela 31.3. Polecenia cmdlet w powłoce PowerShell 1.0 — ciąg dalszy

Nazwa	Definicja	Opis
update-typedata	update-typedata [-AppendPath] <String[]> [-Pre...	Uaktualnienie bieżącego rozszerzonego typu konfiguracji.
where-object (where)	where-object [-FilterScript] <ScriptBlock> [-Inp...	Filtrowanie obiektów, które są przekazywane do potoku.
while	while (warunek) {blok_polecen}	Polecenia pętli są wykonywane, dopóki warunek zwraca wartość true.
write-debug	write-debug [-Message] <String> [-Verbose] [-Deb...	Wyświetlenie komunikatu procesu usuwania błędów na ekranie komputera macierzystego.
write-error	write-error [-Message] <String> [-Category <Erro...	Zapisanie obiektu do potoku błęd.
write-host	write-host [[-Object] <Object>] [-NoNewline] [-S...	Wyświetlenie obiektów za pomocą interfejsu użytkownika komputera macierzystego.
write-output (echo)	write-output [-InputObject] <PSObject[]> [-Verbo...	Zapisanie obiektów w potoku.
write-progress	write-progress [-Activity] <String> [-Status] <S...	Wyświetlenie paska postępu.
write-verbose	write-verbose [-Message] <String> [-Verbose] [-D...	Wyświetlenie ciągu tekstowego na ekranie komputera macierzystego.
write-warning	write-warning [-Message] <String> [-Verbose] [-D...	Wyświetlenie komunikatu o ostrzeżeniu.
#	# <String>	Utworzenie komentarza lub pozostawienie uwagi.

Wielokropek w tabeli oznacza, że do polecenia można dodać dodatkowe parametry, które są identyczne z wymienionymi wcześniej.



i *Hive Key Local Machine*. Magazyn Certificate jest montowany jako napęd *CERT:*. W ten sposób powłoka PowerShell jest unikalna. Nie można uzyskać dostępu do rejestru w wierszu poleceń *cmd.exe* lub Eksploratorze Windows, a wymienione polecenie powłoki PowerShell daje administratorowi wszechstronny dostęp do systemu zarówno lokalnego, jak i zdalnego.

Aby wyświetlić pełną listę obiektów WMI, można wykonać poniższe polecenie:

```
get-wmiobject -list
```

Powłoka PowerShell zwróci od 200 do 300 dostawców WMI. Jeżeli użytkownik chce uzyskać informacje dotyczące określonej usługi, to może podać jej nazwę. Po wydaniu polecenia `get-wmiobject win32_process` użytkownik może być zaskoczony poziomem szczegółowości dostarczanych informacji. PowerShell zawiera też temat pomocy dotyczący `wmiobject`, do którego dostęp umożliwia polecenie `get-help wmiobject`. Po wydaniu poniższego polecenia:

```
get-wmiobject win32_service -computename <AdresIP lub NazwaSystemu>
```

powłoka PowerShell wyświetli usługi działające w systemie o wskazanym adresie IP.

Skrypt powłoki PowerShell to plik tekstowy z rozszerzeniem *.ps1*. Skrypt można uruchomić przez wydanie polecenia `<ścieżka_dostępu>\<nazwa_skryptu.ps1>` po znaku zachęty. Ścieżka dostępu musi być w pełni kwalifikowaną ścieżką dostępu, natomiast podanie rozszerzenia *.ps1* jest opcjonalne.

W powłoce PowerShell trzeba skonfigurować politykę wykonywania, która pozwala na uruchamianie skryptów. Skrypty nie zostaną uruchomione bez wcześniejszego ich zweryfikowania. Jako część procesu weryfikacji można wykorzystać podpis cyfrowy. Więcej informacji na temat podpisu cyfrowego można uzyskać po wydaniu polecenia `get-help about_signing`.

Powłoka PowerShell obsługuje skrypty WSH, oferuje dostęp do obiektów automatyzacji COM oraz ma możliwość dostarczania interaktywnych sesji powłoki.

Idąc dalej, każdy, kto jest zainteresowany wykorzystaniem wiersza poleceń do zarządzania sieciowymi systemami Windows, powinien skoncentrować się na nauce stosowania powłoki PowerShell zamiast starszych narzędzi, takich jak polecenia NET, Windows Scripting Host (WSH) czy inne tego typu technologie.

## Podsumowanie

W rozdziale omówiono narzędzia wiersza poleceń służące do zarządzania siecią. Powłoki i interpretery wiersza poleceń pozwalają na wydawanie poleceń i kontrolę sieci, a jednocześnie są lekkimi środowiskami, w których można przeprowadzać testowanie. Przedstawiono różne powłoki (CLI) wykorzystywane do zarządzania siecią. Wiele z omówionych powłok nie tylko przetwarza pojedyncze polecenia, ale umożliwia również uruchamianie małych programów i skryptów.

Zaprezentowano powłoki używane w systemach Linux, Unix i Windows. Nieco dokładniej opisano polecenia powłoki NetShell i PowerShell.

W kolejnym rozdziale zostaną omówione narzędzia służące do zdalnej pracy w sieci.

# Rozdział 32.

## Dostęp zdalny

### W tym rozdziale:

- ♦ Metody dostępu zdalnego
- ♦ W jaki sposób są używane aplikacje systemu zdalnego?
- ♦ Protokoły połączenia zdalnego
- ♦ Serwerowe role dostępu zdalnego stosowane w trakcie uwierzytelniania i udzielania dostępu

Określenie „zdalny dostęp” opisuje system typu klient-serwer, pozwalający klientowi (zdalnemu) na uzyskanie dostępu do usług oferowanych przez serwer znajdujący się w innej lokalizacji (serwer zdalny). W rozdziale zostanie przedstawione oprogramowanie dostępu zdalnego pozwalającego na łączenie klientów za pomocą sieci PSTN (ang. *Public Switched Telephone Network*). Jednak ogólnym trendem w tym obszarze jest używanie klientów dostępu zdalnego za pomocą połączeń wirtualnej sieci prywatnej (ang. *Virtual Private Network* — VPN) przez internet. W połączeniach zdalnych stosowane są różnorodne protokoły, między innymi SLIP, PPP, PPPoE, PPTP oraz L2TP. Omówione będzie ich powiązanie z oprogramowaniem dostępu zdalnego.

Omówione w tym rozdziale oprogramowanie dostępu zdalnego pozwala systemowi klienta na połączenie z systemem zdalnym w taki sposób, aby aplikacje znajdujące się na tym komputerze były dostępne dla systemu klienta. Tego rodzaju oprogramowanie jest wykorzystywane między innymi do przeprowadzania zdalnych obliczeń, zarządzania systemami zdalnymi, w aplikacjach pomocy technicznej, zdalnej nauce oraz aplikacjach cienkiego klienta (serwera). Protokoły dostępu zdalnego to połączenia wymagające małej przepustowości łącza, które zostały zoptymalizowane do przesyłania danych graficznych z serwera do klienta.

Przedstawione będą także różne protokoły połączeń zdalnych, na przykład ICA, RDP, X11 i inne. Wśród przedstawionych aplikacji znajdują się Microsoft Remote Desktop Connection oraz Citrix GoToMyPC.

Serwery dostępu zdalnego umożliwiają nie tylko połączenie z siecią, ale również dostęp do sieci na podstawie danych uwierzytelniających użytkownika. Jednym z powszechnie wykorzystywanych serwerów dostępu zdalnego jest system RADIUS (ang. *Remote Authentication Dial-In User Service*). RADIUS to serwer uwierzytelniania (ang. *authentication*), autoryzacji (ang. *authorization*) i rozliczania (ang. *accounting*) — tak zwane „potrójne A”.

Zaprezentowana będzie sesja RADIUS, a także zakres różnych urządzeń, które można znaleźć w usłudze RADIUS. Usługę tę można ponadto wykorzystać do weryfikacji klientów mobilnych. Omówiona będzie też przyszła wersja protokołu RADIUS — Diameter.

## Dostęp zdalny

Technologia dostępu zdalnego pojawia się niemal w każdym sieciowym serwerowym systemie operacyjnym, jest obsługiwana przez aplikacje dostarczane przez producenta systemu operacyjnego lub aplikacje firm trzecich. Przyjęło się umożliwianie klientom zdalnym bezpiecznego łączenia się z siecią lokalną. Zazwyczaj oprogramowanie typu RAS (ang. *Remote Access Server*) działa w serwerze, natomiast u klienta działa oprogramowanie typu RAC (ang. *Remote Access Client*) jako aplikacja typu klient-serwer. Klient nawiązuje połączenie z serwerem za pomocą połączenia komutowanego lub przez internet, używając standardowej technologii połączeń internetowych, na przykład ADSL i ISDN, lub czegoś innego, na przykład VPN.

Serwer dostępu zdalnego zwykle jest preferowaną technologią połączenia, kiedy klienci nawiązują połączenia za pomocą połączeń komutowanych w sieci telefonicznej. Dostęp komutowany ma wiele istotnych zalet: linie telefoniczne są powszechnie używane na całym świecie, technologia modemu bazuje na konwersji DAC (ang. *Digital Audio Conversion*), która jest niedroga i prosta w miniaturyzacji. Ponadto technologia połączeń komutowanych zwykle jest niezależna od jakiegokolwiek sprzętu bądź oprogramowania sieciowego wykorzystywanego przez dany system.

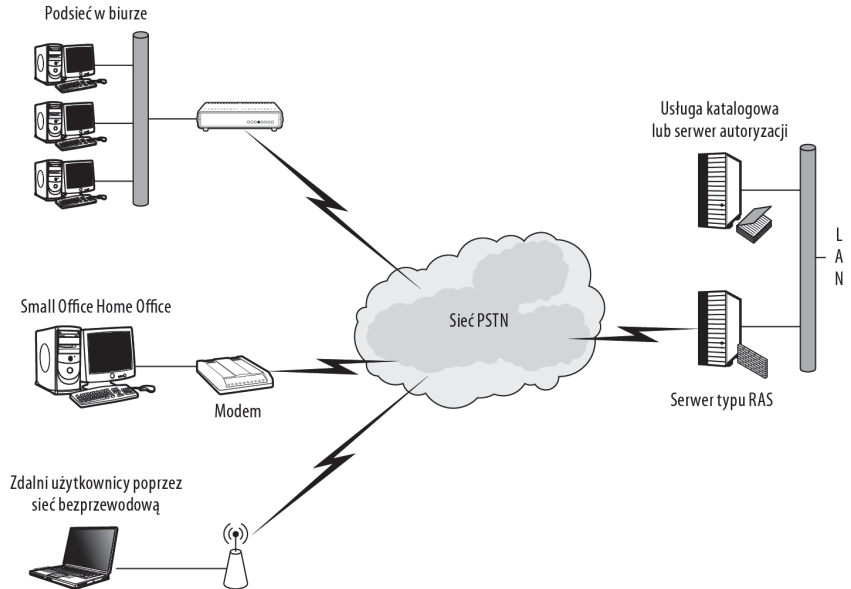
Na rysunku 32.1 pokazano niektóre powszechnie stosowane rozwiązania w technologii dostępu zdalnego. Cztery najczęściej spotykane scenariusze dostępu zdalnego to połączenie użytkowników z siecią LAN wykorzystujące serwer typu Remote Access Server (często RADIUS), połączenie klienta z inną siecią LAN (na przykład podsieć w biurze) za pomocą internetu, połączenie z komputera SOHO (ang. *Small Office Home Office*) oraz nawiązywanie połączenia przez zdalnego klienta (najczęściej laptop) za pomocą bezprzewodowego punktu dostępowego.

W początkowym okresie wykorzystywania połączeń komutowanych ich koszt był stosunkowo wysoki, a bezpieczeństwo było dość słabe, ale technologia ta stawała się coraz tańsza i opracowano dla niej protokoły bezpieczeństwa. Jedynym czynnikiem, który nie może być usprawniony, jest ogólna szybkość transferu danych. Przepustowość standardowego połączenia za pomocą linii telefonicznej wynosi 56 kbit/s i chociaż modemy mogą wykorzystywać tę przepustowość wraz z zaawansowaną technologią kompresji, to jednak nie ma możliwości przekroczenia tego limitu. Użycie wielu linii telefonicznych połączonych razem stanowiło tymczasowe rozwiązanie tego problemu, ale w większości sytuacji połączenia takie zostały zastąpione stałymi połączeniami do internetu lub mobilnymi przez sieć komórkową.

Z powyższych powodów technologia dostępu zdalnego z wykorzystaniem łącz komutowanych nie jest już popularna, jednak serwery RAS nadal stanowią istotny komponent połączeń zdalnych, szczególnie ich funkcje związane z uwierzytelnianiem, autoryzacją i rozliczaniem, na przykład w sieciach VPN. Użycie serwerów RAS w internecie stało się popularną formą dostępu zdalnego, ponieważ w większości krajów i regionów normą stało się połączenie z internetem. Podczas nawiązywania połączenia z serwerem RAS przez internet

**Rysunek 32.1.**

*Dostęp zdalny najczęściej jest stosowany w przypadku usług dostarczanych klientom zdalnym połączonym za pomocą publicznej sieci telefonicznej*



i połączenia VPN użytkownik zyskuje większą przepustowość i ponosi mniejsze koszty niż w przypadku linii telefonicznych. Ponadto dostępnych jest wiele opcji uwierzytelniania i szyfrowania, które zostały opracowane dla zestawu protokołów internetowych.



Połączenia VPN zostały omówione w rozdziale 29.

Celem dostępu zdalnego jest zapewnienie użytkownikom wykorzystującym tego rodzaju połączenia takiego samego komfortu pracy, jaki mają użytkownicy stosujący bezpośrednie połączenia z siecią LAN. Aby osiągnąć ten cel, przepustowość połączenia musi być wystarczająco wysoka, dostęp użytkownika do zasobów musi być uwierzytelniany i autoryzowany, a ponadto połączenie musi być chronione w wystarczającym stopniu. Nowoczesne technologie dostępu zdalnego koncentrują się na tych kwestiach i dostarczają funkcje rozliczeniowe, które są potrzebne dostawcom usług.

Poniżej będą omówione niektóre ze standardowych protokołów umożliwiających nawiązywanie połączeń zdalnych, usługi działające z wymienionymi protokołami standardowymi oraz technologie pozwalające na przeglądanie systemu zdalnego w komputerze lokalnym.

## Protokoły połączenia zdalnego

Zarządzanie połączeniem między użytkownikiem zdalnym i serwerem zdalnym jest możliwe dzięki wykorzystaniu protokołu dostępu zdalnego. Obecnie najczęściej stosowane protokoły dostępu zdalnego to:

- ♦ Serial Line Internet Protocol (SLIP)
- ♦ Point-to-Point Protocol (PPP)
- ♦ Point-to-Point Protocol over Ethernet (PPPoE)

- ♦ Point-to-Point Tunneling Protocol (PPTP)
- ♦ Layer 2 Tunneling Protocol (L2TP)



Wszystkie wymienione protokoły połączenia zostały szczegółowo omówione w rozdziale 29.

Protokoły SLIP, PPP i PPPoE są wykorzystywane w przypadku dostępu zdalnego przez połączenia komutowane, natomiast protokoły PPTP i L2TP są protokołami VPN pozwalającymi na połączenie dwóch sieci LAN przez łącza WAN. Dostęp zdalny wymaga nieco więcej niż zwykłej metody połączenia. W celu uwierzytelnienia i autoryzacji połączenia zdalnego musiały zostać opracowane różne protokoły. Najważniejszą usługą autoryzacji pozostaje usługa RADIUS (ang. *Remote Authentication Dial-In Service*), omówiona szczegółowo w dalszej części rozdziału. Opracowana przez firmę Microsoft wersja usługi RADIUS ma nazwę IAS (ang. *Internet Authentication Service*) dla systemów wcześniejszych niż Windows Server 2003 oraz NPS (ang. *Network Policy Server*) dla systemów Windows Server 2003 i nowszych.

Początkowym protokołem komutowanego połączenia zdalnego był SLIP, który został opracowany jako metoda łączenia terminali z systemami mainframe, w szczególności z ogromnymi systemami bazującymi na Uniksie. SLIP (ang. *Serial Line Internet Protocol*) to metoda nawiązywania połączenia z internetem za pomocą portów szeregowych oraz komunikacji modemowej. Protokół SLIP jest obecnie uznawany za przestarzały i został zastąpiony przez PPP, który charakteryzuje się zaawansowaną obsługą adresowania i kontroli błędów. Protokół SLIP nadal jest w ograniczonym zakresie używany w sytuacjach, w których metoda komunikacji o niewielkim obciążeniu ma istotne znaczenie, na przykład w aplikacjach mikrokontrolerów oraz w protokole BlueCore Serial Protocol stosowanym przez niektóre kontrolery Bluetooth.

## Usługi dostępu zdalnego

Usługa dostępu zdalnego to usługa sieciowa akceptująca połączenia przychodzące od użytkowników zdalnych, weryfikująca dane uwierzytelniające danego użytkownika, tworząca bezpieczne połączenia i służąca jako brama pozwalająca na uzyskanie dostępu do zasobów sieciowych. Serwery dostępu zdalnego mogą być zaimplementowane w celu akceptowania połączeń w dowolnym z wymienionych typów:

- ♦ połączenia PPP lub SLIP z wykorzystaniem modemów DSL, pozwalające na łączenie ze sobą odległych lokalizacji;
- ♦ trasowanie ruchu w sieci IP;
- ♦ połączenia VPN z wykorzystaniem tunelu IPsec lub inny rodzaj połączenia bezpiecznego;



Połączenia VPN i tunele IPsec zostały omówione w rozdziale 29.

- ♦ szerokopasmowe połączenia z wykorzystaniem ATM lub innych protokołów WAN;
- ♦ asynchroniczne połączenia terminali za pomocą Telnetu, TN3270 itp.

Wiele serwerów dostępu zdalnego akceptuje dowolne kombinacje tych typów połączeń i może przeprowadzać konwersję między używanymi protokołami, o ile będzie to niezbędne.

Wprawdzie większość początkowych serwerów RAS obsługiwała połączenia komutowane, ale obecnie dostępne serwery RAS są najczęściej wykorzystywane do obsługi szerokopasmowych usług zdalnych. Kiedy serwer dostępu zdalnego jest używany do przekierowywania ruchu internetowego, ma nazwę szerokopasmowego serwera RAS, ewentualnie BRAS lub BBRAS. Serwery BRAS są stosowane w celu agregowania ruchu sieciowego z DSLAM (ang. *Digital Subscriber Line Access Multipliers*), aby można było zarządzać tym ruchem sieciowym i zapewnić odpowiednią jakość usług (ang. *Quality of Service*). Serwer BRAS jest punktem końcowym połączeń PPP klientów zdalnych (lub PPPoE lub PPPoA). Wiele serwerów BRAS współdziała z serwerami AAA (*Authentication*, czyli uwierzytelnianie, *Authorization*, czyli autoryzacja, oraz *Accounting*, czyli rozliczanie), z których najczęściej stosowanym pozostaje RADIUS (szczegółowo omówiony w dalszej części rozdziału).

## Pulpit zdalny

Pojęcie *pulpitu zdalnego* (ang. *Remote Desktop*) odnosi się do oprogramowania i protokołu połączenia pozwalającego systemowi zdalnemu na wyświetlenie interfejsu systemu, z którym jest połączony ten pierwszy. Technologia pulpitu zdalnego jest formą dostępu zdalnego, ale zarówno pod względem implementacji, jak i skutków jest inna niż pozostałe metody dostępu zdalnego, na których skoncentrowano się w rozdziale. Chociaż dostęp zdalny umożliwia klientowi korzystanie z zasobów sieciowych w taki sposób, jakby ten klient znajdował się w systemie lokalnym, to oprogramowanie podłączenia pulpitu zdalnego pozwala klientowi na kontrolowanie i podgląd systemu serwera tak, jakby użytkownik siedział przed danym serwerem. Aktywne połączenie pulpitu zdalnego określa się *sesją*; taka sama nazwa jest stosowana w przypadku połączenia z serwerem terminalu.

Technologia pulpitu zdalnego jest wykorzystywana w następujących aplikacjach:

- ♦ aplikacje obliczeń zdalnych;
- ♦ aplikacje zdalnego zarządzania systemem;
- ♦ aplikacje pomocy technicznej;
- ♦ aplikacje zdalnej nauki;
- ♦ aplikacje cienkiego klienta (serwera).

Klienty pulpitów zdalnych nawiązują połączenia z systemami za pomocą protokołów VPN, które są zoptymalizowane do transmisji danych niewymagających dużej przepustowości (dane wejściowe klawiatury i myszy w systemie klienta) oraz wyświetlania danych wyjściowych z serwera. Wspomniane protokoły połączenia najczęściej są szyfrowane; dane przekazywane za pomocą tych połączeń są wysoce skompresowane. Dzięki temu klient może połączyć się z serwerem przez połączenie o małej przepustowości, na przykład za pośrednictwem linii telefonicznej, i nadal osiągać dobrą wydajność. Protokoły połączenia pulpitu zdalnego są przez to formą protokołu połączenia VPN z naciskiem na zoptymalizowane możliwości w zakresie grafiki i druku zdalnego, lecz niekoniecznie skoncentrowane na ogólnej przepustowości danych.



Porównanie oprogramowania zapewniającego obsługę pulpitów zdalnych z uwzględnieniem nazwy produktu, systemu operacyjnego i jego możliwości można znaleźć na stronie [http://en.wikipedia.org/wiki/Comparison\\_of\\_remote\\_desktop\\_software](http://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software).

Najważniejsze używane obecnie protokoły obsługujące pulpity zdalne to:

- ♦ **Independent Computing Architecture (ICA)** — protokół własnościowy firmy Citrix, który jest stosowany z Citrix WinFrame i XenApp (poprzednia nazwa to Citrix MetaFrame and Presentation Servers).
- ♦ **Remote Desktop Protocol (RDP)** — protokół połączenia firmy Microsoft wykorzystywany przez jej oprogramowanie obsługi pulpitów zdalnych do nawiązywania połączenia z systemami Windows. Klienci używające protokołu RDP są dostępne dla wszystkich nowoczesnych systemów operacyjnych. Ponadto klienci RDP mogą nawiązywać połączenia z systemami, stosując technologię Windows TS Gateway, dostępną w Windows Server 2008.
- ♦ **X Window System v X11** — używany przez wiele systemów operacyjnych, choć przede wszystkim w przypadku systemów z rodziny Unix i Linux ma możliwość łączenia systemów klientów z serwerami.
- ♦ **NX Technology (NX)** — protokół, który może być wykorzystywany przez systemy X Window System jako alternatywa dla protokołu X11.
- ♦ **Virtual Network Computing (VNC)** — używający protokołu RFB (ang. *Remote Frame Buffering*) do nawiązywania połączeń z pulpitemi zdalnymi; stosowany przez oprogramowanie typu open source o nazwie RealVNC.

ICA, RDP i X11 wykorzystują sterowniki na poziomie jądra w celu przekierowania danych wyjściowych podsystemu graficznego do klienta zdalnego. Inne protokoły do obsługi pulpitów zdalnych używane przez oprogramowanie takie jak PC Anywhere, VNC i inne aplikacje stosują oprogramowanie warstwy aplikacji do tworzenia połączenia VPN i zarządzania nim.

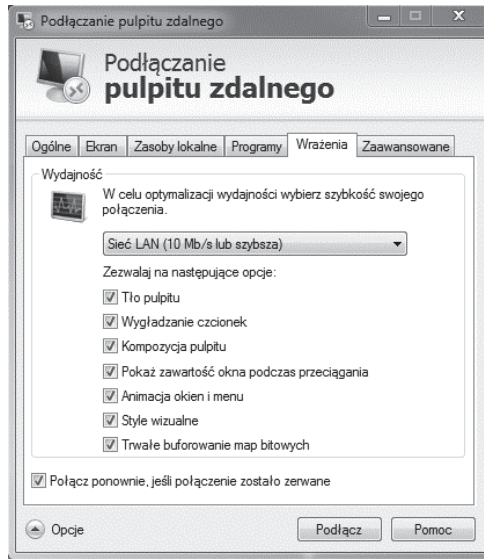
Rodzime oprogramowanie serwera Windows RDP firmy Microsoft ma nazwę *Usługi terminalowe* w Windows 2000, *Menedżer połączeń usługi Dostęp zdalny* w Windows Server 2003, XP, Windows Server 2008, Vista i Windows 7. Na platformie Mac OS X oprogramowanie to ma nazwę *Remote Desktop*. Dostępne są również klienty typu open source: XRDP (<http://xrdp.sourceforge.net>) i RDESKTOP (<http://www.rdesktop.org>). Na rysunku 32.2 pokazano okno dialogowe przedstawiające właściwości *Podłączania pulpitu zdalnego*, które pozwala na zmianę funkcji znajdujących się w oprogramowaniu klienta pulpitu zdalnego na podstawie szybkości połączenia. Użytkownik może również włączać i wyłączać pewne funkcje w celu poprawienia wydajności działania oprogramowania.



Firma Microsoft oferuje usługę konferencji internetowych o nazwie Microsoft Live Meeting (<http://www.microsoft.com/online/pl-pl/office-live-meeting.mspx>); przemysłowy serwer tej firmy obsługujący konferencje to Office Communications Server 2007 (<http://www.microsoft.com/poland/communicationsserver/>). Usługa LiveMeeting zastąpiła starszy produkt NetMeeting. Inne ważne produkty w tej dziedzinie to między innymi IBM Lotus Sametime (<http://www-142.ibm.com/software/products/pl/pl/sametime>), Glance (<http://www.glance.net>) i WebEx (<http://www.webex.com>).

**Rysunek 32.2.**

Klient Podłączania pulpitu zdalnego w systemach Windows 7 i Vista pozwala na dostosowanie dostępnych funkcji do własnych potrzeb z wykorzystaniem okna programu



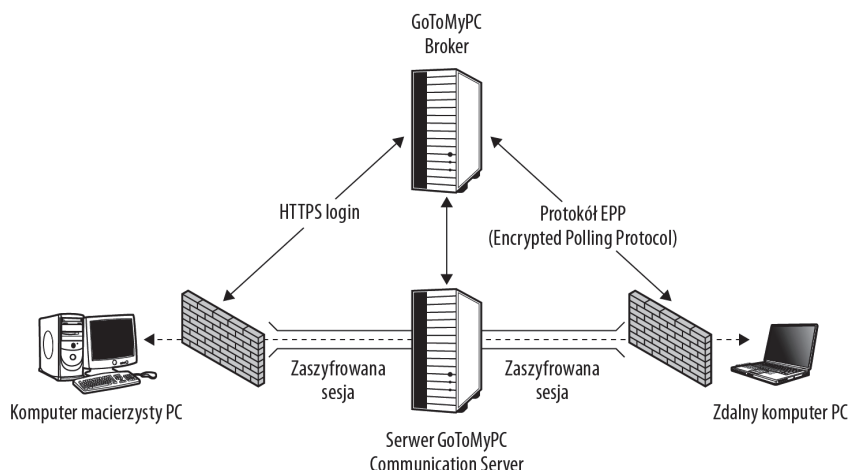
Oprogramowanie obsługi pulpitu zdalnego jest szeroko wykorzystywane w obszarze pomocy technicznej. Dwa najlepiej sprzedające się produkty w tej kategorii to Symantec (poprzednio Norton) pcAnywhere v12.5 (<http://www.symantec.com/norton/symantec-pcanywhere>) oraz produkt firmy Citrix Systems o nazwie GoToMyPC (<http://www.gotomypc.com/>). Symantec sprzedaje swój produkt jako aplikację typu klient-serwer, podczas gdy firma Citrix połączyła oprogramowanie klient-serwer z bazującą na internecie usługą subskrypcji, która przesyła silnie zaszyfrowane dane w sposób pozwalający klientom GoToMyPC na pracę z wybranymi zaporami sieciowymi.

Na rysunku 32.3 pokazano architekturę systemu GoToMyPC, który używa narzędzia GoToMyPC Broker w celu nasłuchiwania żądań sesji połączenia, następnie uwierzytelnia klienty i rozpoczyna sesję GoToMyPC. Kiedy sesja jest w toku, GoToMyPC Broker korzysta z protokołu EPP (ang. *Encrypted Polling Protocol*), gwarantującego, że zdalny pulpit komputera PC oraz komputer macierzysty PC są zweryfikowanymi punktami końcowymi w utworzonej przez nich sesji. Takie podejście uniemożliwia innym systemom przechwycenie ruchu sieciowego GoToMyPC. Ponieważ przepływ wszystkich danych odbywa się przez serwer GoToMyPC Communications Server, w którym przekazywane są zaszyfrowane pakiety, komunikacja między narzędziem GoToMyPC Broker i wymienionym serwerem jest dodatkowym czynnikiem zapewniającym weryfikację komputera macierzystego i systemu zdalnego w sesji.

Produkt GoToMyPC rozbudowany o funkcję konferencyjną GoToAssist jest sprzedawany przez Citrix Systems jako usługa subskrypcyjna o nazwie GoToMeeting. Za pośrednictwem internetu oprogramowanie to udostępnia pulpit zdalny zbiorowi klientów GoToMeeting. Komunikacja jest szyfrowana i chroniona hasłem. Ponadto używana jest architektura bazująca na komputerze macierzystym, podobna do zastosowanej w produkcie GoToMyPC. Usługa GoToMeeting może pozwolić na udostępnienie pojedynczej aplikacji lub całego komputera. Inna cecha to możliwość przejęcia systemu komputera macierzystego przez dowolnego uczestnika, jak również rejestracja całej sesji w celu jej późniejszego odtworzenia. Dostępna jest też rozszerzona wersja GoToMeeting o nazwie GoToWebinar, która umożliwia obsługę większej liczby użytkowników.

**Rysunek 32.3.**

Architektura systemu GoToMyPC używa bazującego na internecie zestawu serwerów obsługujących uwierzytelnianie sesji oraz przekazujących dane sesji i zarządzających nimi



## Serwery RADIUS

*Remote Authentication Dial-In User Service* (RADIUS) to nazwa protokołu sieciowego, który pozwala użytkownikom zdalnym na uwierzytelnienie i uzyskanie dostępu do sieci LAN. Protokół ten jest implementowany w postaci serwera RADIUS. Dostępny zakres obejmuje systemy od małych serwerów RADIUS instalowanych w sieciach SOHO dla kilku użytkowników aż do serwerów RADIUS klasy przemysłowej w dużych firmach telekomunikacyjnych lub u dostawców usług internetowych (ISP), którzy obsługują tysiące połączeń użytkowników. RADIUS odgrywa również ważną rolę w bezpieczeństwie stosowanym w standardzie IEEE 802.11i i działa wraz z WEP w celu utworzenia bezpiecznego tunelu między klientem zdalnym i siecią Wi-Fi za pomocą protokołu EAP (ang. *Extensible Authentication Protocol*) lub PEAP (ang. *Protected Extensible Authentication Protocol*). Protokół RADIUS jest też powszechnie wykorzystywany przez systemy VoIP, kiedy klienci zdalne, na przykład telefony IP, nawiązujące połączenie z serwerem VoIP za pomocą bezpiecznej technologii, takiej jak protokół SIP (ang. *Session Initiation Protocol*), łączą się z serwerem rejestratora SIP.



Technologie 802.11x Wi-Fi zostały omówione w rozdziale 14. Więcej informacji na temat VoIP można znaleźć w rozdziale 26.

Serwery RADIUS to, ogólnie rzecz ujmując, bramy bezpieczeństwa. Zaliczają się one do klasy usług sieciowych określanych mianem serwerów AAA („potrójne A”). Nazwa „serwer AAA” odnosi się do następujących funkcji:

- ♦ **Authentication (uwierzytelnienie).** Serwer RADIUS zapewnia możliwość uwierzytelnienia użytkownika zdalnego oraz włączenia bądź wyłączenia jego połączenia. W trakcie uwierzytelniania serwer RADIUS może określić, czy numer telefonu użytkownika jest autoryzowanym numerem telefonu i czy użytkownik prowadzi jakąkolwiek sesję w toku, jak również może wykonać inne zadania. Dlatego też serwer RADIUS może uniemożliwić użytkownikowi posługującemu się skradzionym hasłem uzyskanie dostępu do systemu z nieznanego numeru telefonu.

Serwer RADIUS może obsługiwać kopię kont użytkowników sieciowych lub stanowić część architektury określanej mianem *dołączalne moduły uwierzytelniania* (ang. *Pluggable Authentication Service* — PAM). W architekturze tej dane uwierzytelniające są przekazywane przez serwer dostępu sieciowego lub serwer domeny. Wprawdzie z punktu widzenia zarządzania przechowywanie informacji na temat kont użytkownika w serwerze RADIUS niewątpliwie jest wygodne, ale takie rozwiązanie dostarcza atakującemu pełnych informacji o bezpieczeństwie, wymaganych do złamania sieci i uzyskania dostępu do systemu. Z tego powodu zaleca się, aby w poszczególnych sesjach przekazywać dane uwierzytelniające RADIUS do innych serwerów.

- ♦ **Authorization (autoryzacja).** Serwer RADIUS określa prawa dostępu i uprawnienia, jakimi użytkownik dysponuje w sieci. Autoryzacja określa również rodzaj połączenia, który może dostarczyć klient RADIUS, na przykład PPP lub Telnet.
- ♦ **Accounting (rozliczanie).** Serwer RADIUS obsługuje szczegółowy dziennik rejestracji zdarzeń i może układać dane zdarzeń w taki sposób, aby dostarczać informacje konieczne do wystawienia rachunku bądź przeprowadzenia innych rozliczeń. Okresowo w trakcie sesji klient RADIUS wysyła do serwera informacje dotyczące wykorzystania usług. Podczas operacji logowania lub wylogowania klient może wysłać do serwera żądanie podania rozliczenia.



RADIUS to standard otwarty zgodnie z opisem przedstawionym w dokumencie ETF RFC 2865 (<http://tools.ietf.org/html/rfc2865>). Funkcja rozliczeń w RADIUS została przedstawiona w dokumencie IETF RFC 2866 (<http://tools.ietf.org/html/rfc2866>). Ponieważ protokół RADIUS umożliwia rozbudowę, różni producenci zaimplementowali go, używając własnego zestawu atrybutów.

Serwery RADIUS są używane w wielu różnych aplikacjach. RADIUS można znaleźć jako jedną z usług w routerach, bezprzewodowych punktach dostępowych, tuż za zaporami sieciowymi lub serwerami proxy w sieci brzegowej, jako część serwerów poczty, w urządzeniach korzystających z internetu i w systemach VPN. RADIUS to domyślny protokół uwierzytelniania w sieciach bezprzewodowych zgodnych z nowym standardem 802.11i.

W swoich routerach i serwerach sieciowych firma Cisco używa protokołu zdalnego uwierzytelniania o nazwie *Terminal Access Controller Access-Control System* (TACACS). Pierwotna wersja TACACS została zaprojektowana do używania podczas uwierzytelniania serwerów Unix. Firma Cisco poszła dalej — uaktualniła i rozszerzyła TACACS do wersji TACACS+, która jest własnościowym standardem Cisco, niezgodnym z początkową wersją TACACS. Firma Cisco zaleca stosowanie TACACS+ zamiast RADIUS, choć w routerach oferowanych przez Cisco wbudowano obsługę obu wymienionych protokołów. Firma Cisco opublikowała specyfikację dla TACACS+ w postaci szkicu dokumentu IETF RFC (<http://tools.ietf.org/html/draft-grant-tacacs-02/>). Standard TACACS+ jest stosowany podczas uwierzytelniania i autoryzacji, ale nie do rozliczeń. Domyślnie działa na porcie TCP o numerze 49.

Poniżej zostaną przedstawione podstawy sesji protokołu RADIUS oraz sposób, w jaki RADIUS pozwala klientom mobilnym na tak zwany roaming.

## Sesje RADIUS

Sesja RADIUS składa się z następujących kroków:

1. Użytkownik zdalny nawiązuje połączenie z urządzeniem klienta RADIUS, wykorzystując protokół PPP lub inny protokół warstwy danych, i inicjalizuje logowanie.
2. Klient RADIUS — router, brama, serwer NAS (ang. *Network Access Server*) lub inne urządzenie — przesyła hasło do serwera RADIUS, używając mechanizmu MD5 w celu jego zabezpieczenia.

Do uwierzytelniania RADIUS korzysta z portu UDP o numerze 1812, natomiast do rozliczeń — z portu 1813. Starsze implementacje RADIUS używały do wymienionych funkcji nieoficjalnych portów o numerach odpowiednio 1645 i 1646. Niektóre implementacje RADIUS stosują oba zestawy portów. Firma Microsoft wykorzystuje porty 1812 i 1813, podczas gdy serwery RADIUS firm Cisco i Juniper Networks używają portów 1645 i 1646.

3. Wiadomość RADIUS Access Request jest przekazywana serwerowi RADIUS wraz z danymi uwierzytelniającymi (identyfikator użytkownika i hasło), informacjami dotyczącymi systemu (adres sieciowy i położenie użytkownika) za pomocą protokołu PAP (ang. *Password Authentication Protocol*), CHAP (ang. *Challenge-Handshake Authentication Protocol*) lub EAP (ang. *Extensible Authentication Protocol*).
4. Serwer RADIUS weryfikuje żądanie logowania względem lokalnej bazy danych albo usługi uwierzytelniania działającej w sieci.

Usługa uwierzytelniania może obejmować serwery LDAP (w przypadku weryfikacji domeny), serwery Active Directory (w sieciach Windows), serwery Kerberos (w celu weryfikacji certyfikatu) lub serwer SQL Server (lub innej bazy danych w przypadku weryfikacji na podstawie bazy danych).

5. Weryfikacja skutkuje odpowiedzią Access Accept, Access Reject lub Access Challenged:
  - ♦ Access Accept — udziela użytkownikowi dostępu do żadanego zasobu. Odpowiedź Access Accept nie ma zastosowania do wszystkich zasobów; dostęp do każdego kolejnego zasobu jest udzielany w miarę potrzeb. Okresowo klient RADIUS również weryfikuje początkowe zaoferowane mu uprawnienia dostępu.
  - ♦ Access Reject — uniemożliwia użytkownikowi dostęp do sieci, a także do żądanych przez niego zasobów.
  - ♦ Access Challenged — występuje, kiedy system wymaga pewnych informacji dodatkowych w celu utworzenia bezpiecznego kanału z serwera RADIUS do klienta zdalnego. Utworzony kanał będzie tunelowany za pomocą klienta RADIUS.
6. Odpowiedź Access Accept może zawierać następujące atrybuty: przypisanie określonego adresu IP, przypisanie wartości TTL (ang. *Time To Live*) dla sesji, pobranie list ACL (ang. *Access Control List*) klienta oraz ustawienie wymaganych parametrów sesji dla L2TP, VLAN i QoS.

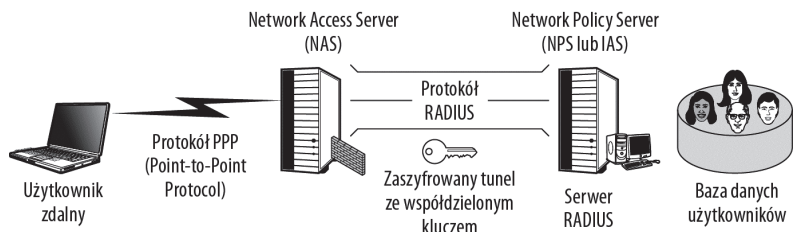
7. Po ustanowieniu sesji w kliencie RADIUS rozliczanie rozpoczyna się wraz z wiadomością Accounting Start, która tworzy rekord rozliczeniowy sesji. Kolejne wiadomości Interim Accounting wypełniają rekord rozliczeniowy sesji, natomiast wiadomość Account Stop powoduje zamknięcie rekordu rozliczeniowego sesji.

Przechowywane informacje rozliczeniowe zawierają następujące dane: czas trwania sesji, liczba przekazanych pakietów, ilość przekazanych danych, identyfikator użytkownika i komputera, adres sieciowy, a także punkt dołączenia informacji. Następnie baza danych może zostać użyta w celu wygenerowania informacji wykorzystywanych do sporządzenia rachunku oraz danych statystycznych lub też do innych celów.

Serwery RADIUS są dostępne jako programy typu open source, freeware i shareware, na przykład FreeRADIUS (<http://www.freeradius.org>), GNU Radius (<http://www.gnu.org/software/radius>) i OpenRADIUS (<http://www.xs4all.nl/~evbergen/openradius/>). Ponadto są dostępne jako programy komercyjne, na przykład Steel Belted Radius (<http://www.juniper.net/us/en/products-services/software/ipc/sbr-series/enterprise/>) firmy Juniper Networks, oraz w pewnych serwerowych, sieciowych systemach operacyjnych, na przykład w Windows Server. Począwszy od dodatku Option Pack dla Windows Server 2000, RADIUS jest dodawany do systemu Windows jako serwer IAS.

W systemie Windows Server 2008 zmieniono nazwę serwera Microsoft RADIUS z *Internet Authentication Service* (IAS) na *Network Policy Server* (NPS), ale funkcjonalność pozostała taka sama. Obecnie RADIUS to względnie dojrzała technologia. Na rysunku 32.4 pokazano, w jaki sposób serwer NPS jest implementowany w sieci Windows. W przedstawionym schemacie NAS działa jako klient RADIUS i dostarcza niezbędny dostęp sieciowego po zwróceniu odpowiedzi Access Accept przez serwer RADIUS.

**Rysunek 32.4.**  
Serwer RADIUS  
zaimplementowany  
w sieci systemu  
Windows Server  
2003 lub nowszego



Serwer RADIUS może zostać skonfigurowany jako klient RADIUS względem innych serwerów RADIUS. Oznacza to, że serwer może pełnić funkcję klienta proxy, przekazując innym serwerom RADIUS dane uwierzytelniające i rozliczeniowe. Funkcja proxy jest istotna podczas implementacji RADIUS w sieci brzegowej, gdy istnieje wymaganie zapewnienia uwierzytelnionego dostępu do innych części sieci.

## Roaming RADIUS

Wiele implementacji RADIUS wymaga, aby klient był mobilny. Konieczna jest wówczas obsługa funkcji roamingu. Kiedy klient RADIUS wykonuje roaming między sieciami, stan AAA klienta musi zostać przeniesiony do innego serwera RADIUS. Każdy zbiór serwerów RADIUS istnieje w tzw. *strefie*. W celu identyfikacji użytkownika zdalnego połączanego z serwerem RADIUS informacje serwera są dodawane za pomocą znaku @ i przyrostka lub

przez dodanie znaku \ i prefiksu do nazwy klienta bądź też jednego i drugiego. Przykładem rozszerzonej nazwy jest `domena_1.ext\id_uzytkownika@domena_2.ext`, gdzie wskazano dwie strefy. Strefa to po prostu nazwa nadana grupie serwerów RADIUS i nie jest zarejestrowana ani śledzona w żaden sposób. Dlatego też nazwy stref mogą być nadawane zupełnie dowolnie.

Strefy są przechowywane w tabelach w serwerach RADIUS. Każda nieznaną strefa musi być w pierwszej kolejności dołączona lub skonfigurowana, zanim zostanie udzielone zezwolenie na roaming klienta do sieci. Z tego powodu serwery RADIUS odgrywają rolę serwerów proxy pod tym względem, że przekazują żądania AAA pochodzące z roamingu użytkownika zdalnego, którego nie mogą znaleźć w tabeli strefy, do serwera domeny lub klienta roamingu. Tabela roamingu pozwala na zarządzanie; istnieje możliwość dodania innych serwerów RADIUS, ich modyfikacji lub usunięcia z tabeli. Protokół RADIUS nie określa sposobu implementacji wymienionych funkcji zarządzających.

Klient zdalny nawiązuje połączenie przez klienta RADIUS, używając bezpiecznego, uwierzytelnionego połączenia. Kiedy klient przeprowadza roaming, pojawiają się kwestie bezpieczeństwa dotyczące ustanowienia nowego bezpiecznego połączenia. RADIUS rozwiązuje ten problem przez utworzenie dwuwarstwowego schematu bezpieczeństwa. Szczegóły dotyczące implementacji tego schematu zależą od danego producenta. W przypadku protokołu EAP bezpieczny tunel jest tworzony między uwierzytelniającym serwerem RADIUS (wewnętrzna tożsamość) i serwerem domeny. Ponadto tworzony jest dodatkowy tunel (zewewnętrzna tożsamość), który przeprowadza komunikację za pomocą zwykłego tekstu i jest wykorzystywany w celu umożliwienia systemom proxy odpowiedniego przekazywania pakietów. System roamingu może również tworzyć bezpieczne, szyfrowane tunele między serwerami RADIUS, a tym samym ukrywać przed dalszym przeglądaniem informacje dotyczące bezpieczeństwa użytkownika.

## Protokół Diameter

Technologia RADIUS powoli staje się przestarzała. Po raz pierwszy została przedstawiona przez Merrit Network dla NSFnet i opracowana przez Livingston Enterprises w roku 1991. Obecnie trwają prace nad technologią, która ma zastąpić RADIUS, czyli protokołem Diameter. Protokół Diameter zastępuje protokół transportowy UDP innymi, solidnymi protokołami transportowymi TCP i SCTP. Nazwa Diameter (ang. — „średnica”) powstała na bazie nazwy RADIUS (ang. — „promień”), ponieważ średnica jest dwukrotnie większa od promienia; poza ową ciekawostką nazwa ta nie ma innej, istotnej genezy. Na dzisiejszym etapie prac protokół Diameter nie zapewnia wstecznej zgodności z protokołem RADIUS, ale systemy RADIUS będą mogły zostać uaktualnione do Diameter.

Protokół Diameter jest obecnie zdefiniowany przez dokument IETF RFC 3588 (<http://tools.ietf.org/html/rfc3588>) i zawiera wszystkie elementy serwera AAA, które ma RADIUS. Usługa Diameter może być rozszerzona za pomocą atrybutów charakterystycznych dla danego dostawcy i o polecenia dodatkowe. Podobnie jak w przypadku protokołu RADIUS, Diameter jest protokołem połączenia, a nie aplikacji. Oferuje bezpieczeństwo zarówno warstwy sieci, jak i transportu oraz ma możliwość tworzenia bezpiecznych tuneli poprzez IPsec lub TLS, połączenia stanowe lub bezstanowe. Istnieje spora liczba nowych lub usprawnionych funkcji protokołu Diameter, których nie znajdziemy w protokole RADIUS, między innymi:

- ♦ dynamiczne odkrywanie węzłów za pomocą DNS SRV (ang. *Domain Name Service Records*) lub NAPTR (ang. *Name Authority Pointer Records*);
- ♦ potwierdzanie na poziomie warstwy aplikacji i wiadomości błędów;
- ♦ negocjacja zgodności sesji;
- ♦ architektura klient-serwer;
- ♦ usprawnione możliwości w zakresie roamingu;
- ♦ pełny zestaw funkcji AAA.

Sesja Diameter między dwoma węzłami rozpoczyna się od utworzenia połączenia TCP lub SCTP. Jeden z węzłów działa jako inicjator, natomiast drugi jest celem. Inicjator wysyła do celu żądanie CER (ang. *Capabilities-Exchange-Request*), który z kolei odpowiada za pomocą CEA (ang. *Capabilities-Exchange-Answer*), co prowadzi do negocjacji połączenia TLS. Kiedy połączenie zostanie nawiązane, aplikacje mogą rozpocząć wymianę wiadomości.

Połączenie TLS jest monitorowane pod kątem aktywności. Jeżeli zostanie wykryty określony czas braku aktywności, to jeden z węzłów wysyła do drugiego żądanie DWR (ang. *Device-Watchdog-Request*), natomiast ten drugi musi odpowiedzieć żądaniem DWA (ang. *Device-Watchdog-Answer*). Niepowodzenie w trakcie wymiany tych informacji prowadzi do wysłania wiadomości DPR (ang. *Disconnect-Peer-Request*) przez jeden z węzłów. Jeżeli w odpowiedzi nadawca nie otrzyma wiadomości DPA (ang. *Disconnect-Peer-Answer*), to nastąpi kontakt z protokołem transportowym i połączenie zostanie przerwane.



W celu znalezienia dokumentów RFC wymienionych na poniższej liście można użyć wyszukiwarki znajdującej się na stronie <http://www.ietf.org/rfc.html>. Ogólna postać adresu URL każdego dokumentu RFC jest następująca: <http://www.ietf.org/rfc/rfc####.txt>, gdzie #### oznacza numer dokumentu RFC dopełniony zerami, jeśli nie składa się z czterech cyfr.

Wśród różnych aplikacji obsługujących protokół Diameter i jak dotąd zdefiniowanych przez IETF znajdują się między innymi:

- ♦ aplikacje będące częścią podsystemu 3GPP IP Multimedia (<http://www.3gpp.org/>) dla połączeń bezprzewodowych;
- ♦ funkcja Bootstrapping Server Function do wzajemnego uwierzytelniania urządzeń sieci komórkowych i serwerów, stanowiąca część standardu 3GPP (<http://www.3gpp.org/>);
- ♦ Diameter Credit-Control Application (DCCA, RFC 4006; <http://tools.ietf.org/html/rfc4006>);
- ♦ Diameter Extensible Authentication Protocol Application (RFC 4072; <http://tools.ietf.org/html/rfc4072>);
- ♦ Diameter Mobile IPv4 Application (MobileIP, RFC 4004; <http://tools.ietf.org/html/rfc4004>);
- ♦ Diameter Network Access Server Application (NASREQ, RFC 4005; <http://tools.ietf.org/html/rfc4005>);
- ♦ Diameter Session Initiation Protocol Application (RFC 4740; <http://tools.ietf.org/html/rfc4740>).

## Podsumowanie

W rozdziale przedstawiono różne technologie dostępu zdalnego. Pierwotnie dostęp zdalny był wiązany z połączeniami telefonicznymi o małej przepustowości między klientami i serwerami. Wraz z rozwojem technologii szerokopasmowych i internetu dostęp zdalny zdominowały połączenia VPN.

Omówiono też oprogramowanie służące do obsługi pulpitu zdalnego, które jest powiązane z technologią klient-serwer do dostępu zdalnego. Jednak w przeciwieństwie do dostępu zdalnego, w którym połączenie jest zoptymalizowane w celu przekazania maksymalnej ilości danych, a klienty zdalne są dostępne jako podłączone węzły w sieci, połączenia pulpitu zdalnego są optymalizowane do przekazywania danych graficznych oraz przystosowane do małej przepustowości łącza.

Serwery dostępu zdalnego funkcjonują nie tylko jako punkty dostępu do sieci, ale muszą również przeprowadzać weryfikację klientów i selektywnie zezwalać im na uzyskiwanie dostępu do zasobów sieci. W rozdziale omówiono serwer RADIUS jako przykład tak zwanego serwera „potrójnego A”, które oznacza uwierzytelnianie (ang. *authentication*), autoryzację (ang. *authorization*) i rozliczanie (ang. *accounting*).

# Dodatek A

## Przypisania portów TCP — UDP

**W dodatku:**

- ◆ Wymieniono różne przypisania portów

W tabeli A.1 wymieniono wiele powszechnie używanych portów zarówno przez protokół TCP jak również UDP. W kolumnie *Port* zostało to oznaczone literą odpowiednio T i U. Najczęściej używane porty zwykle pochodzą z zakresu numerów od 1 do 1023 i są portami przypisanymi na stałe (ang. *Port well-known ports*). Różni producenci zarejestrowali ogromną liczbę przypisań portów, które są wykorzystywane przez wiele odmiennych aplikacji. Wraz z upływem czasu wiele wspomnianych przypisań portów stało się równie popularnych jak porty przypisane na stałe. Porty zarejestrowane mieszczą się w zakresie numerów od 1024 do 49191. Pozostałe porty, to znaczy z zakresu numerów od 49152 do 65535, organizacja ICANN pozostawiła wolne i można je przypisywać dynamicznie bądź do użytku prywatnego. Porty w najwyższym zakresie nie są ani zarejestrowane ani nie mają przypisań — pozostają dostępne do użycia przez każdego w dowolnym czasie.

W wielu przypadkach TCP i UDP używają tych samych numerów portów dla tego samego protokołu, ale to nie jest regułą. Podobnie, pojedynczy protokół taki jak HTTP niekoniecznie będzie przypisany tylko do jednego portu. Dany protokół może być przypisany do wielu portów. Przykładowo, w przypadku protokołu HTTP dwa powszechnie stosowane przypisania portów nie znajdują się w ciągłym zakresie: powszechnie używane są numery portów 80 i 8080 (dla zapór sieciowych).

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane)

Port	Przypisanie	Uwagi
0 - T, U	Zarezerwowany	Oficjalnie
0 - T, U	Shirt Pocket netTunes, Shirt Pocket launchTunes	Oficjalnie
1 - T, U	TCP Port Service Multiplexer	Oficjalnie
2 - T, U	Narzędzie zarządzające	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
3 - T, U	Proces kompresji	Oficjalnie
5 - T, U	Zdalne wprowadzanie zadań	Oficjalnie
6 - T, U	Nieprzypisany	Oficjalnie
7 - T, U	Echo	Oficjalnie
8 - T, U	Nieprzypisany	Oficjalnie
9 - T, U	Nie używany	Oficjalnie
10 - T, U	Nieprzypisany	Oficjalnie
11 - T, U	Aktywni użytkownicy	Oficjalnie
12 - T, U	Nieprzypisany	Oficjalnie
13 - T, U	Czas dzienny (dokument RFC 867)	Oficjalnie
14 - T, U	Nieprzypisany	Oficjalnie
15 - T, U	Nieprzypisany	Oficjalnie
16 - T, U	Nieprzypisany	Oficjalnie
17 - T, U	Cytat dnia	Oficjalnie
18 - T, U	Message Send Protocol	Oficjalnie
19 - T, U	Generator znaków	Oficjalnie
20 - T, U	FTP — domyślnie dla danych	Oficjalnie
21 - T, U	FTP — polecenia kontrolne	Oficjalnie
22 - T, U	SSH Remote Login Protocol	Oficjalnie
23 - T, U	Telnet	Oficjalnie
24 - T, U	Każdy prywatny system poczty	Oficjalnie
25 - T, U	Simple Mail Transfer Protocol (SMTP)	Oficjalnie
26 - T, U	RSFTP	Nieoficjalnie
27 - T, U	NSW User System FE	Oficjalnie
28 - T, U	Nieprzypisany	Oficjalnie
29 - T, U	MSG ICP	Oficjalnie
30 - T, U	Nieprzypisany	Oficjalnie
31 - T, U	Uwierzytelnianie MSG	Oficjalnie
32 - T, U	Nieprzypisany	Oficjalnie
33 - T, U	Display Support Protocol	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
34 - T, U	Nieprzypisany	Oficjalnie
35 - T, U	Każdy protokół prywatnego serwera wydruku	Oficjalnie
35 - T, U	Protokół serwera wydruku QMS Magicolor 2	Nieoficjalnie
36 - T, U	Nieprzypisany	Oficjalnie
37 - T, U	Protokół TIME	Oficjalnie
38 - T, U	Remote Access Protocol	Oficjalnie
39 - T, U	Resource Location Protocol (RLP)	Oficjalnie
40 - T, U	Nieprzypisany	Oficjalnie
41 - T, U	Grafika	Oficjalnie
42 - T, U	ARPA Host Name Server Protocol	Oficjalnie
42 - T, U	WINS	Nieoficjalnie
43 - T, U	Protokół WHOIS	Oficjalnie
44 - T, U	MPM FLAGS Protocol	Oficjalnie
45 - T, U	Moduł przetwarzania wiadomości	Oficjalnie
46 - T, U	MPM (wysyłanie domyślne)	Oficjalnie
47 - T, U	NI FTP	Oficjalnie
48 - T, U	Digital Audit Daemon	Oficjalnie
49 - T, U	TACACS Login Host Protocol	Oficjalnie
50 - T, U	Remote Mail Checking Protocol	Oficjalnie
51 - T, U	IMP Logical Address Maintenance	Oficjalnie
52 - T, U	Xerox Network Services (XNS) Time Protocol	Oficjalnie
53 - T, U	Domain Name System (DNS)	Oficjalnie
54 - T, U	Xerox Network Services (XNS) Clearinghouse	Oficjalnie
55 - T, U	ISI Graphics Language	Oficjalnie
56 - T, U	Uwierzytelnianie Xerox Network Services (XNS)	Oficjalnie
56 - T, U	Route Access Protocol (RAP)	Nieoficjalnie
57 - T	Mail Transfer Protocol (MTP)	Nieoficjalnie
57 - T, U	Każdy prywatny system poczty	Oficjalnie
58 - T, U	Poczta Xerox Network Services (XNS)	Oficjalnie
59 - T, U	Każda prywatna usługa plików	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
60 - T, U	Nieprzypisany	Oficjalnie
61 - T, U	NI Mail	Oficjalnie
62 - T, U	Usługi ACA	Oficjalnie
63 - T, U	whois++	Oficjalnie
64 - T, U	Communications Integrator (CI)	Oficjalnie
65 - T, U	Usługa bazy danych TACACS	Oficjalnie
66 - T, U	Oracle SQL*NET	Oficjalnie
67 - T, U	Bootstrap Protocol Server (BOOTP)	Oficjalnie
68 - T, U	Bootstrap Protocol Client (BOOTP)	Oficjalnie
69 - T, U	Trivial File Transfer Protocol (TFTP)	Oficjalnie
70 - T, U	Protokół Gopher	Oficjalnie
71 - T, U	Usługa zdalnego wprowadzania zadań	Oficjalnie
72 - T, U	Usługa zdalnego wprowadzania zadań	Oficjalnie
73 - T, U	Usługa zdalnego wprowadzania zadań	Oficjalnie
74 - T, U	Usługa zdalnego wprowadzania zadań	Oficjalnie
75 - T, U	Każda prywatna usługa połączeń komutowanych	Oficjalnie
76 - T, U	Distributed External Object Store	Oficjalnie
77 - T, U	Każdy prywatny serwer RJE	Oficjalnie
78 - T, U	Vettcp	Oficjalnie
79 - T, U	Finger Protocol	Oficjalnie
80 - T, U	Hypertext Transfer Protocol (HTTP)	Oficjalnie
81 - T, U	Nieprzypisany	Oficjalnie
82 - T, U	Narzędzie XFER	Oficjalnie
83 - T, U	Urządzenie MIT ML	Oficjalnie
84 - T, U	Common Trace Facility	Oficjalnie
85 - T, U	Urządzenie MIT ML	Oficjalnie
86 - T, U	Micro Focus Cobol	Oficjalnie
87 - T, U	Każde prywatne połączenie terminalu	Oficjalnie
88 - T, U	Kerberos	Oficjalnie
90 - T, U	DNSIX Security Attribute Token Map	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
90 - T, U	PointCast	Nieoficjalnie
91 - T, U	MIT Dover Spooler	Oficjalnie
92 - T, U	Network Printing Protocol	Oficjalnie
93 - T, U	Device Control Protocol	Oficjalnie
94 - T, U	Tivoli Object Dispatcher	Oficjalnie
95 - T, U	SUPDUP	Oficjalnie
96 - T, U	Specyfikacja protokołu DIXIE	Oficjalnie
97 - T, U	Swift Remote Virtual File Protocol	Oficjalnie
98 - T, U	TAC News	Oficjalnie
99 - T, U	Metagram Relay	Oficjalnie
100 - T	Nieautoryzowane użycie	Oficjalnie
101 - T, U	NIC Host Name Server	Oficjalnie
102 - T, U	ISO Transport Service Access Point (TSAP) Class 0 Protocol	Oficjalnie
103 - T, U	Genesis Point-to-Point Trans Net	Oficjalnie
104 - T, U	ACR-NEMA Digital Imag. & Comm. 300	Oficjalnie
105 - T, U	Serwer nazw skrzynki pocztowej	Oficjalnie
106 - T, U	3COM-TSMUX	Oficjalnie
106 - T, U	Insecure poppassd Protocol	Nieautoryzowany
107 - T, U	Remote Telnet Service Protocol	Oficjalnie
108 - T, U	SNA Gateway Access Server	Oficjalnie
109 - T, U	Post Office Protocol 2 (POP2)	Oficjalnie
110 - T, U	Post Office Protocol 3 (POP3)	Oficjalnie
111 - T, U	Zdalne wywoływanie procedur Sun	Oficjalnie
112 - T, U	McIDAS Data Transmission Protocol	Oficjalnie
113 - T, U	Usługa uwierzytelniania	Oficjalnie
114 - T, U	Nieużywany od czerwca 2004 roku	Oficjalnie
115 - T, U	Simple File Transfer Protocol (SFTP)	Oficjalnie
116 - T, U	ANSA REX Notify	Oficjalnie
117 - T, U	Usługa UUCP	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
118 - T, U	Usługi Structured Query Language (SQL)	Oficjalnie
119 - T, U	Network News Transfer Protocol (NNTP)	Oficjalnie
120 - T, U	CFDPTKT	Oficjalnie
121 - T, U	Encore Expedited Remote Pro.Call	Oficjalnie
122 - T, U	SMAKYNET	Oficjalnie
123 - T, U	Network Time Protocol (NTP)	Oficjalnie
124 - T, U	ANSA REX Trader	Oficjalnie
125 - T, U	Locus PC-Interface Net Map Ser	Oficjalnie
126 - T, U	NxEdit	Poprzednio przypisane do Unisys Unitary Login
127 - T, U	Locus PC-Interface Conn Server	Oficjalnie
128 - T, U	GSS X License Verification	Oficjalnie
129 - T, U	Protokół Password Generator Protocol	Oficjalnie
130 - T, U	Cisco FNATIVE	Oficjalnie
131 - T, U	Cisco TNATIVE	Oficjalnie
132 - T, U	Cisco SYSMAINT	Oficjalnie
133 - T, U	Usługi danych statystycznych	Oficjalnie
134 - T, U	Usługa INGRES-NET	Oficjalnie
135 - T, U	DCE	Oficjalnie
135 - T, U	Usługi Microsoft End Point Mapper (EPMAP), AKA DCE/RPC Locator	Nieoficjalnie
137 - T, U	NetBIOS Name Service	Oficjalnie
138 - T, U	NetBIOS Datagram Service	Oficjalnie
139 - T, U	NetBIOS Session Service	Oficjalnie
140 - T, U	EMFIS Data Service	Oficjalnie
141 - T, U	EMFIS Control Service	Oficjalnie
142 - T, U	Britton-Lee IDM	Oficjalnie
143 - T, U	Internet Message Access Protocol (IMAP)	Oficjalnie
152 - T, U	Background File Transfer Program (BFTP)	Oficjalnie
153 - T, U	Simple Gateway Monitoring Protocol (SGMP)	Oficjalnie
156 - T, U	Usługa SQL	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
158 - T, U	Distributed Mail Service Protocol (DMSP)	Nieoficjalnie
161 - T, U	Simple Network Management Protocol (SNMP)	Oficjalnie
162 - T, U	Simple Network Management Protocol Trap (SNMPTRAP)	Oficjalnie
170 - T	Print-srv, Network PostScript	Oficjalnie
177 - T, U	X Display Manager Control Protocol (XDMCP)	Oficjalnie
179 - T	Border Gateway Protocol (BGP)	Oficjalnie
194 - T	Internet Relay Chat (IRC)	Oficjalnie
201 - T, U	Obsługa routingu AppleTalk	Oficjalnie
209 - T, U	The Quick Mail Transfer Protocol	Oficjalnie
213 - T, U	IPX	Oficjalnie
218 - T, U	Message Posting Protocol (MPP)	Oficjalnie
220 - T, U	Interactive Mail Access Protocol (IMAP) wersja 3	Oficjalnie
259 - T, U	Efficient Short Remote Operations (ESRO)	Oficjalnie
264 - T, U	Border Gateway Multicast Protocol (BGMP)	Oficjalnie
311 - T	Mac OS X Server Admin (oficjalna administracja AppleShare IP)	Oficjalnie
318 - T, U	PKIX Time Stamp Protocol (TSP)	Oficjalnie
323 - T, U	Internet Message Mapping Protocol (IMMP)	Nieoficjalnie
366 - T, U	On-Demand Mail Relay (ODMR)	Oficjalnie
369 - T, U	Rpc2portmap	Oficjalnie
387 - T, U	AppleTalk Update-based Routing Protocol (AURP)	Oficjalnie
389 - T, U	Lightweight Directory Access Protocol (LDAP)	Oficjalnie
401 - T, U	Uninterruptible Power Supply (UPS)	Oficjalnie
402 - T	Altiris Deployment Client	Nieoficjalnie
411 - T	Direct Connect Hub	Nieoficjalnie
412 - T	Direct Connect Client-to-Client	Nieoficjalnie
427 - T, U	Service Location Protocol (SLP)	Oficjalnie
443 - T	Hypertext Transfer Protocol over TLS/SSL (HTTPS)	Oficjalnie
444 - T, U	Simple Network Paging Protocol (SNPP) (RFC 1568)	Oficjalnie
445 - T	Microsoft-DS Active Directory, udziały Windows	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
445 - U	Współdzielenie plików Microsoft-DS SMB	Oficjalnie
464 - T, U	Kerberos zmiana/ustawienie hasła	Oficjalnie
465 - T	Protokół Cisco	Nieoficjalnie
465 - T	SMTP poprzez SSL	Nieoficjalnie
500 - U	Internet Security Association and Key Management Protocol (ISAKMP)	Oficjalnie
502 - T, U	Protokół Modbus	Nieoficjalnie
513 - T	Login	Oficjalnie
513 - U	Who	Oficjalnie
514 - T	Shell	Oficjalnie
514 - U	Syslog	Oficjalnie
515 - T	Line Printer Daemon (usługa wydruku)	Oficjalnie
517 - U	Talk	Oficjalnie
518 - U	Ntalk	Oficjalnie
520 - T	Extended Filename Server (EFS)	Oficjalnie
520 - U	Routing Internet Protocol (RIP)	Oficjalnie
524 - T, U	NetWare Core Protocol (NCP)	Oficjalnie
525 - U	Serwer Timed, Timeserver	Oficjalnie
530 - T, U	RPC	Oficjalnie
531 - T, U	AOL Instant Messenger, IRC	Nieoficjalnie
540 - T	Unix-to-Unix Copy Protocol (UUCP)	Oficjalnie
542 - T, U	Commerce (aplikacje komercyjne)	Oficjalnie
543 - T	Kerberos login (klogin)	Oficjalnie
544 - T	Zdalna powłoka Kerberos (kshell)	Oficjalnie
546 - T, U	Klient DHCPv6	Oficjalnie
547 - T, U	Serwer DHCPv6	Oficjalnie
548 - T	Apple Filing Protocol (AFP) poprzez TCP	Oficjalnie
550 - U	new-rwho, new-who	Oficjalnie
554 - T, U	Real Time Streaming Protocol (RTSP)	Oficjalnie
556 - T	Remotefs, RFS, rfs_server	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
560 - U	Remote Monitor (rmonitor)	Oficjalnie
561 - U	Monitor	Oficjalnie
563 - T, U	NNTP poprzez TLS/SSL (NNTPS)	Oficjalnie
587 - T	Simple Mail Transfer Protocol (wysyłanie wiadomości)	Oficjalnie
591 - T	FileMaker 6.0 (i późniejsze) Web Sharing (alternatywa dla HTTP, zobacz również port 80)	Oficjalnie
593 - T, U	HTTP RPC Ep Map, R	Oficjalnie
631 - T, U	Internet Printing Protocol (IPP)	Oficjalnie
636 - T, U	Lightweight Directory Access Protocol poprzez TLS/SSL (LDAPS)	Oficjalnie
639 - T, U	Multicast Source Discovery Protocol (MSDP)	Oficjalnie
646 - T, U	Label Distribution Protocol (LDP), protokół routingu używany w sieciach MPLS	Oficjalnie
647 - T	Dynamic Host Configuration Protocol (DHCP) Failover	Oficjalnie
648 - T	Registry Registrar Protocol (RRP)	Oficjalnie
652 - T	Dynamic Tunnel Configuration Protocol (DTCP)	Nieoficjalnie
654 - T	Ad-hoc On-demand Distance Vector (AODV)	Oficjalnie
655 - T	IEEE Media Management System (IEEE MMS)	Oficjalnie
657 - T, U	IBM Remote Monitoring and Control (RMC) Protocol	Oficjalnie
660 - T	Administracja systemem Mac OS X Server	Oficjalnie
666 - U	Doom	Oficjalnie
674 - T	Application Configuration Access Protocol (ACAP)	Oficjalnie
691 - T	MS Exchange Routing	Oficjalnie
694 - U	Linux-HA High Availability Heartbeat	Nieoficjalnie
695 - T	IEEE Media Management System poprzez SSL (IEEE-MMS-SSL)	Oficjalnie
698 - U	Optimized Link State Routing (OLSR)	Oficjalnie
700 - T	Extensible Provisioning Protocol (EPP)	Oficjalnie
701 - T	Link Management Protocol (LMP)	Oficjalnie
702 - T	Internet Registry Information Service (IRIS) poprzez Blocks Extensible Exchange Protocol (BEEP)	Oficjalnie
706 - T	Secure Internet Live Conferencing (SILC)	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
712 - T	Topologia rozgłaszania bazująca na protokole routingu Reverse-Path Forwarding (TBRPF)	Oficjalnie
749 - T, U	Administracja Kerberos	Oficjalnie
750 - T	RFile	Oficjalnie
750 - U	Loadav	Oficjalnie
750 - U	Kerberos wersja IV (Kerberos IV)	Oficjalnie
751 - T, U	Pump	Oficjalnie
751 - T, U	Uwierzytelnianie Kerberos (kerberos_master)	Nieoficjalnie
752 - T	qrh	Oficjalnie
752 - U	qrh	Oficjalnie
752 - U	userreg_server, serwer Kerberos Password (kpasswd) Server	Nieoficjalnie
753 - T	Reverse Routing Header (RRH)	Oficjalnie
753 - U	Reverse Routing Header (RRH)	Oficjalnie
753 - U	Serwer Kerberos userreg server (passwd_server)	Nieoficjalnie
754 - T	tell send	Oficjalnie
754 - T	Propagowanie Kerberos v5 (krb5_prop)	Nieoficjalnie
754 - U	tell send	Oficjalnie
760 - T, U	ns	Oficjalnie
783 - T	Demon spamd filtru SpamAssassin	Nieoficjalnie
829 - T	Certificate Management Protocol (CMP)	Nieoficjalnie
860 - T	iSCSI	Oficjalnie
873 - T	Protokół synchronizacji plików rsync	Oficjalnie
901 - T	Samba Web Administration Tool (SWAT)	Nieoficjalnie
901 - T, U	VMware Virtual Infrastructure Client	Nieoficjalnie
902 - T	VMware Server Console	Nieoficjalnie
904 - T	VMware Server Alternate	Nieoficjalnie
953 - T, U	Domain Name System (DNS) RDNC Service	Oficjalnie
989 - T, U	FTPS (dane): FTP poprzez TLS/SSL	Oficjalnie
990 - T, U	FTPS (polecenia kontrolne): FTP poprzez TLS/SSL	Oficjalnie
992 - T, U	TELNET poprzez TLS/SSL	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
993 - T	Internet Message Access Protocol poprzez SSL (IMAPS)	Oficjalnie
995 - T	Post Office Protocol 3 poprzez TLS/SSL (POP3S)	Oficjalnie
1025 - T	NFS-or-IIS	Nieoficjalnie
1026 - T	Usługi Microsoft DCOM	Nieoficjalnie
1029 - T	Usługi Microsoft DCOM	Nieoficjalnie
1058 - T, U	nim, IBM AIX Network Installation Manager (NIM)	Oficjalnie
1059 - T, U	nimreg, IBM AIX Network Installation Manager (NIM)	Oficjalnie
1080 - T	SOCKS proxy	Oficjalnie
1085 - T, U	WebObjects	Oficjalnie
1098 - T, U	RMI Activation (rmiactivation)	Oficjalnie
1099 - T, U	RMI Registry (rmiregistry)	Oficjalnie
1109 - T	Kerberos Post Office Protocol (KPOP)	Nieoficjalnie
1140 - T, U	AutoNOC Network Operations	Oficjalnie
1167 - U	Telefon, połączenie konferencyjne	Nieoficjalnie
1194 - T, U	OpenVPN	Oficjalnie
1214 - T	Kazaa	Oficjalnie
1220 - T	Administracja serwerem QuickTime Streaming Server	Oficjalnie
1223 - T, U	TrulyGlobal Protocol (TGP)	Oficjalnie
1234 - U	Domyślny port odtwarzacza multimedialnych VLC dla strumieni UDP/RTP	Nieoficjalnie
1270 - T, U	Agent Microsoft System Center Operations Manager (SCOM; AKAMS MOM)	Oficjalnie
1293 - T, U	Internet Protocol Security (IPSec)	Oficjalnie
1311 - T	Dell Open Manage HTTPS	Nieoficjalnie
1352 - T	Protokół zdalnego wywoływania procedur (RPC) IBM Lotus Notes/Domino	Oficjalnie
1387 - T, U	cadsi-lm, LMS International (poprzednio Computer Aided Design Software, Inc. [CADSI]) LM	Oficjalnie
1414 - T	IBM WebSphere MQ (poprzednio znane jako MQSeries)	Oficjalnie
1417 - T, U	Timbuktu Service 1 Port	Oficjalnie
1418 - T, U	Timbuktu Service 2 Port	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
1419 - T, U	Timbaktu Service 3 Port	Oficjalnie
1420 - T, U	Timbaktu Service 4 Port	Oficjalnie
1433 - T, U	Microsoft SQL Server	Oficjalnie
1434 - T, U	Microsoft SQL Monitor	Oficjalnie
1494 - T	Protokół cienkiego klienta Citrix XenApp Independent Computing Architecture (ICA)	Oficjalnie
1512 - T, U	Microsoft Windows Internet Name Service (WINS)	Oficjalnie
1521 - T	Domyślny port nasłuchiwania w bazie danych Oracle, w przyszłości będzie nim oficjalny port 2483	Nieoficjalnie
1524 - T, U	ingreslock, ingres	Oficjalnie
1526 - T	Powszechnie stosowana alternatywa dla portu nasłuchiwania dla bazy danych Oracle	Nieoficjalnie
1533 - T	IBM Sametime IM — Virtual Places Chat SQL Server	Oficjalnie
1547 - T, U	Laplink	Oficjalnie
1581 - U	MIL STD 2045-47001 VMF	Oficjalnie
1589 - U	Protokół Cisco VLAN Query Protocol (VQP) / VMPS	Nieoficjalnie
1645 - T, U	radius, protokół uwierzytelniania RADIUS (domyślny dla serwerów RADIUS firm Cisco oraz Juniper Networks)	Nieoficjalnie
1646 - T, U	radaccT, protokół rozliczeń RADIUS (domyślny dla serwerów RADIUS firm Cisco oraz Juniper Networks)	Nieoficjalnie
1677 - T, U	Klienci Novell GroupWise	Oficjalnie
1701 - U	Layer 2 Forwarding (L2F) oraz Layer 2 Tunneling (L2TP)	Oficjalnie
1723 - T, U	Microsoft Point-to-Point Tunneling Protocol (PPTP)	Oficjalnie
1725 - U	Klient Valve Steam	Nieoficjalnie
1755 - T, U	Microsoft Media Services (MMS, ms-streaming)	Oficjalnie
1761 - T, U	cft-0	Oficjalnie
1761 - T	Narzędzie Novell ZENworks Remote Control	Nieoficjalnie
1762-1768 - T, U	cft-1 to cft-7	Oficjalnie
1812 - T, U	radius, protokół uwierzytelniania RADIUS	Oficjalnie
1813 - T, U	radaccT, protokół rozliczeń RADIUS	Oficjalnie
1863 - T	Microsoft Notification Protocol (MSNP)	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
1900 - U	Microsoft SSDP dla urządzeń UPnP	Oficjalnie
1935 - T	Adobe Flash Real Time Messaging Protocol (RTMP)	Oficjalnie
1975-1977 - U	Cisco TCO (dokumentacja)	Oficjalnie
1985 - U	Cisco HSRP	Oficjalnie
1994 - T, U	Cisco Serial Tunneling — Synchronous Data Link Control (STUN-SDLC)	Oficjalnie
1998 - T, U	Usługa Cisco X.25 poprzez TCP (XOT)	Oficjalnie
2000 - T, U	Cisco SCCP (Skinny)	Oficjalnie
2002 - T	Secure Access Control Server (ACS) dla Windows	Nieoficjalnie
2030	Oracle Services dla Microsoft Transaction Server	Nieoficjalnie
2049 - U	Network File System	Oficjalnie
2053 - T	knetd Kerberos de-multiplexor	Nieoficjalnie
2083 - T	Secure Radius Service (RadSec)	Oficjalnie
2083 - T	CPanel default SSL	Nieoficjalnie
2086 - T	GNUnet	Oficjalnie
2086 - T	WebHost Manager (domyślny)	Nieoficjalnie
2087 - T	WebHost Manager (domyślny dla SSL)	Nieoficjalnie
2105 - T, U	IBM MiniPay	Oficjalnie
2105 - T, U	Szyfrowane, zdalne logowanie eklogin Kerberos (rlogin)	Nieoficjalnie
2161 - T	Agent APC	Oficjalnie
2181 - T, U	EForward - system transportu dokumentacji	Oficjalnie
2190 - U	TiVoConnect Beacon	Nieoficjalnie
2219 - T, U	NetIQ NCAP	Oficjalnie
2220 - T, U	NetIQ End2End	Oficjalnie
2222 - T	DirectAdmin (domyślny)	Nieoficjalnie
2302 - U	Halo	Nieoficjalnie
2369 - T	Agent konfiguracji BMC Software CONTROL-M/Server	Nieoficjalnie
2370 - T	BMC Software CONTROL-M/Server	Nieoficjalnie
2404 - T	IEC 60870-5-104	Oficjalnie
2427 - U	Cisco MGCP	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
2447 - T, U	Ovwdb — demon OpenView Network Node Manager (NNM)	Oficjalnie
2483 - T, U	Nasłuchiwanie w bazie danych Oracle (zastąpi port 1521)	Oficjalnie
2484 - T, U	Nasłuchiwanie w bazie danych Oracle dla połączeń SSL	Oficjalnie
2598 - T	Nowy ICA — kiedy funkcja Session Reliability jest włączona, port TCP 2598 zastępuje port 1494	Nieoficjalnie
2710 - T	XBT BitTorrent Tracker	Nieoficjalnie
2710 - U	XBT BitTorrent Tracker eksperymentalne rozszerzenie UDP Tracker	Nieoficjalnie
2735 - T, U	NetIQ Monitor Console	Oficjalnie
2809 - T	IBM WebSphere Application Server (WAS) Bootstrap/rmi (domyślny)	Nieoficjalnie
2948 - T, U	WAP-push Multimedia Messaging Service (MMS)	Oficjalnie
2949 - T, U	WAP-pushsecure Multimedia Messaging Service (MMS)	Oficjalnie
2967 - T	Symantec AntiVirus Corporate Edition	Nieoficjalnie
3025 - T	netpd.org	Nieoficjalnie
3074 - T, U	Xbox Live	Oficjalnie
3260 - T, U	iSCSI target	Oficjalnie
3268 - T, U	msft-gc, Microsoft Global Catalog (usługa LDAP)	Oficjalnie
3269 - T, U	msft-gc-ssl, Microsoft Global Catalog poprzez SSL	Oficjalnie
3283 - T	Apple Remote Desktop reporting (oficjalnie Net Assistant)	Oficjalnie
3306 - T, U	System bazy danych MySQL	Oficjalnie
3389 - T	Microsoft Terminal Server (RDP) oficjalnie zarejestrowany jako Windows Based Terminal (WBT)	Nieoficjalnie
3396 - T, U	Agent Novell NDPS Printer	Oficjalnie
3455 - T, U	Reservation Protocol (RSVP)	Oficjalnie
3689 - T	Digital Audio Access Protocol (DAAP) dla programu iTunes oraz tak zwanej stacji bazowej (router bezprzewodowego) AirPort Express firmy Apple	Oficjalnie
3702 - T, U	Web Services Dynamic Discovery (WS-Discovery), używane przez różne komponenty systemu Windows Vista	Oficjalnie
3868 - T, Stream Control Transfer Protocol (SCTP)	Podstawowy protokół Diameter (dokument RFC 3588)	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
3872 - T	Oracle Management Remote Agent	Nieoficjalnie
3899 - T	Remote Administrator	Nieoficjalnie
3900 - T	udt_os, IBM UniData UDT OS[30]	Oficjalnie
4100	WatchGuard Authentication Applet — (domyślny)	Nieoficjalnie
4125 - T	Administracja Microsoft Remote Web Workplace	Nieoficjalnie
4224 - T	Cisco Discovery Protocol (CDP)	Nieoficjalnie
4500 - U	IPsec NAT traversal	Oficjalnie
4664 - T	Google Desktop Search	Nieoficjalnie
4899 - T, U	Zdalne narzędzie administracyjne Radmin (czasami używany jako koń trojański)	Oficjalnie
4993 - T, U	Home FTP Server Web Interface Default Port	Nieoficjalnie
5000 - T	Współpraca urządzeń sieciowych UPnP–Windows	Nieoficjalnie
5001 - T, U	Iperf (narzędzie służące do pomiaru przepustowości i wydajności TCP oraz UDP)	Nieoficjalnie
5001 - T	Slingbox i SlingPlayer	Nieoficjalnie
5003 - T, U	FileMaker	Oficjalnie
5004 - T, U, Datagram Congestion Control Protocol (DCCP)	Dane multimedialne protokołu Real-time Transport Protocol (RTP)	Oficjalnie
5005 - T, U, DCCP	Polecenia kontrolne dla protokołu Real-time Transport Protocol (RTP)	Oficjalnie
5050 - T	Yahoo! Messenger	Nieoficjalnie
5060 - T, U	Session Initiation Protocol (SIP)	Oficjalnie
5061 - T	Session Initiation Protocol (SIP) poprzez TLS	Oficjalnie
5093 - U	Statistical Package for the Social Sciences (SPSS) License Administrator	Nieoficjalnie
5104 - T	IBM Tivoli Framework NetCOOL/Impact HTTP Service	Nieoficjalnie
5190 - T	ICQ i AOL Instant Messenger	Oficjalnie
5351 - T, U	NAT Port Mapping Protocol	Oficjalnie
5353 - U	Multicast DNS (mDNS)	Oficjalnie
5355 - T, U	Link-Local Multicast Name Resolution (LLMNR)	Oficjalnie
5432 - T, U	System bazy danych PostgreSQL	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
5445 - U	Cisco Unified Video Advantage	Nieoficjalnie
5500 - T	Protokół komputera zdalnego VNC	Nieoficjalnie
5517 - T	KLient serwera SETIQueue Proxy dla projektu SETI@Home	Nieoficjalnie
5631 - T	pcANYWHERE — (dane)	Oficjalnie
5632 - U	pcANYWHERE	Oficjalnie
5800 - T	Protokół pulpitu zdalnego VNC do użycia poprzez HTTP	Nieoficjalnie
5814 - T, U	Hewlett-Packard Support Automation (HP OpenView Self-Healing Services)	Oficjalnie
5900 - T, U	Virtual Network Computing (VNC) protokół pulpitu zdalnego (używany przez oprogramowanie Apple Remote Desktop i inne)	Oficjalnie
6000 - T	X11	Oficjalnie
6001 - U	X11	Oficjalnie
6005 - T	BMC Software CONTROL-M/Server	Nieoficjalnie
6346 - T, U	gnutella-svc, Gnutella (FrostWire, LimeWire, Shareaza itd.)	Oficjalnie
6347 - T, U	gnutella-rtr, Gnutella (alternatywa)	Oficjalnie
6444 - T, U	Sun Grid Engine — Qmaster Service	Oficjalnie
6445 - T, U	Sun Grid Engine — Execution Service	Oficjalnie
6571	Klient Windows Live FolderShare	Nieoficjalnie
6600 - T	Music Playing Daemon (MPD)	Nieoficjalnie
6660-6664 - T	Internet Relay Chat	Nieoficjalnie
6665-6669 -T	Internet Relay Chat	Oficjalnie
6679 - T	IRC SSL (Secure Internet Relay Chat)	Nieoficjalnie
6697 - T	IRC SSL (Secure Internet Relay Chat)	Nieoficjalnie
6771 - U	Polycom server broadcast	Nieoficjalnie
6881-6887 - T, U	BitTorrent	Nieoficjalnie
6888 - T, U	MUSE	Oficjalnie
6888 - T, U	BitTorrent	Nieoficjalnie
6889-6890 - T, U	BitTorrent	Nieoficjalnie
6891-6900 - T, U	BitTorrent	Nieoficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
6891-6900 - T, U	Windows Live Messenger (transfer plików)	Nieoficjalnie
6901 - T, U	Windows Live Messenger (głos)	Nieoficjalnie
6901 - T, U	BitTorrent	Nieoficjalnie
6902-6968 - T, U	BitTorrent	Nieoficjalnie
6969 - T	BitTorrent tracker	Nieoficjalnie
6970 - 6999 - T	BitTorrent	Nieoficjalnie
7001 - T	Serwer BEA WebLogic Server's HTTP	Nieoficjalnie
7002 - T	Serwer BEA WebLogic Server's HTTPS	Nieoficjalnie
7005 - T, U	BMC Software CONTROL-M/Server oraz CONTROL-M/Agent	Nieoficjalnie
7006 - T, U	BMC Software CONTROL-M/Server oraz CONTROL-M/Agent	Nieoficjalnie
7010 - T	Cisco AON AMC (konsola zarządzania AON)	Nieoficjalnie
7400 - T, U	Real Time Publish Subscribe (RTPS) DDS — wykrywanie	Oficjalnie
7401 - T, U	Real Time Publish Subscribe (RTPS) DDS — ruch sieciowy użytkownika	Oficjalnie
7402 - T, U	RTPS (Real Time Publish Subscribe) DDS — metadane	Oficjalnie
7777 - T	Proxy serwera plików iChat	Nieoficjalnie
7777 - T	Domyślnie używany przez program tini.exe pozwalający dostać się do systemu Windows tylnymi drzwiami	Nieoficjalnie
8000 - T, U	Intel Remote Desktop Management Interface (iRDMI)	Oficjalnie
8000-8001 - T	Strumieniowanie radia w internecie, na przykład SHOUTcast	Nieoficjalnie
8002 - T	Cisco Systems Unified CallManager Intercluster	Nieoficjalnie
8008 - T	Alternatywa dla HTTP	Oficjalnie
8008 - T	Domyślny port dla administracji serwerem IBM HTTP Server	Nieoficjalnie
8080 - T	Alternatywa dla HTTP (http_alt) — powszechnie używany przez serwery proxy oraz buforujące, a także do uruchamiania serwera WWW jako użytkownik inny niż root	Oficjalnie
8080 - T	Apache Tomcat	Nieoficjalnie
8081 - T	Alternatywa dla HTTP, na przykład McAfee ePolicy Orchestrator (ePO)	Nieoficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
8086 - T	Kaspersky AntiVirus Control Center	Nieoficjalnie
8087 - U	Kaspersky AntiVirus Control Center	Nieoficjalnie
8090 - T	Alternatywa dla HTTP (http_alt_alt) — używany jako alternatywa dla port 8080	Nieoficjalnie
8192 - T	Sophos Remote Management System	Nieoficjalnie
8193 - T	Sophos Remote Management System	Nieoficjalnie
8194 - T	Sophos Remote Management System	Nieoficjalnie
8200 - T	GoToMyPC	Nieoficjalnie
8220 - T	Bloomberg	Nieoficjalnie
8222 - T	VMware Server Management User Interface (niezabezpieczony interfejs sieciowy)	Nieoficjalnie
8243 - T, U	Nasłuchiwanie HTTPS dla Apache Synapse	Oficjalnie
8280 - T, U	Nasłuchiwanie HTTP dla Apache Synapse	Oficjalnie
8294 - T	Bloomberg	Nieoficjalnie
8333 - T	VMware Server Management User Interface (bezpieczny interfejs sieciowy)	Nieoficjalnie
8400 - T, U	cvp, CommVault Unified Data Management	Oficjalnie
8500 - T	ColdFusion Macromedia/Adobe ColdFusion (domyślny)	Nieoficjalnie
8880 - U	cddbp-al - T, Protokół CD DataBase (CDDb) Protocol (CDDbP) — alternatywa	Oficjalnie
8880 - T	cddbp-al - T, Protokół CD DataBase (CDDb) Protocol (CDDbP) — alternatywa	Oficjalnie
8880 - T	WebSphere Application Server SOAP connector (domyślny)	Nieoficjalnie
8888 - T	Sun AnswerBook dwhttpd server (przestarzały według <a href="http://docs.sun.com">http://docs.sun.com</a> )	Nieoficjalnie
8888 - T	GNUmp3d HTTP — strumieniowanie muzyki i interfejs sieciowy	Nieoficjalnie
9000 - T	Buffalo LinkSystem — dostęp sieciowy	Nieoficjalnie
9000 - U	UDPCast	Nieoficjalnie
9001	cisco-xremote (konfiguracja routera)	Nieoficjalnie
9001	Tor (domyślny)	Nieoficjalnie
9030 - T	Tor (często używany)	Nieoficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
9043 - T	WebSphere Application Server Administration Console (bezpieczna konsola)	Nieoficjalnie
9050 - T	Tor	Nieoficjalnie
9051 - T	Tor	Nieoficjalnie
9060 - T	WebSphere Application Server Administration Console (konsola)	Nieoficjalnie
9080 - U	glrpc, Groove Collaboration software GLRPC	Oficjalnie
9080 - T	glrpc, Groove Collaboration software GLRPC	Oficjalnie
9080 - T	WebSphere Application Server HTTP Transport (port 1) — domyślny	Nieoficjalnie
9110 - U	Protokół SSMP Message Protocol	Nieoficjalnie
9443 - T	Transport WSO2 Web Services Application Server HTTPS (oficjalnie WSO2 Tungsten HTTPS)	Oficjalnie
9443 - T	WebSphere Application Server HTTP Transport (port 2) — domyślny	Nieoficjalnie
9535 - T	mngsuite, LANDesk Management Suite Remote Control	Oficjalnie
9535 - T	BBOS001, IBM WebSphere Application Server (WAS) High Availability Manager Communications	Nieoficjalnie
9535 - U	mngsuite, LANDesk Management Suite Remote Control	Oficjalnie
9800 - T, U	WebDAV Source	Nieoficjalnie
9800	WebCT e-learning portal	Nieoficjalnie
9898 - T	Tripwire — File Integrity Monitoring Software	Nieoficjalnie
9999 - T	Lantronix UDS-10/UDS100[43] RS-485 to Ethernet Converter TELNET control	Nieoficjalnie
10000	Webmin — bazujące na przeglądarce internetowej narzędzie do zarządzania systemem Linux	Nieoficjalnie
10000	Backup Exec	Nieoficjalnie
10001 - T	Lantronix UDS-10/UDS100[44] RS-485 to Ethernet Converter (domyślny)	Nieoficjalnie
10017	AIX, NeXT, HP-UX — rexd daemon control	Nieoficjalnie
10113 - T, U	NetIQ Endpoint	Oficjalnie
10114 - T, U	NetIQ QCheck	Oficjalnie
10115 - T, U	NetIQ Endpoint	Oficjalnie
10116 - T, U	NetIQ VoIP Assessor	Oficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
11211	memcached	Nieoficjalnie
11371	OpenPGP HTTP — serwer kluczy	Oficjalnie
11576	Serwer zarządzania komunikacją IPStor	Nieoficjalnie
12035 - U	Linden Lab	Nieoficjalnie
12345	NetBus — narzędzie zdalnej administracji (często koń trojański)	Nieoficjalnie
12975 - T	LogMeIn Hamachi (oprogramowania do tworzenia tuneli VPN)	Nieoficjalnie
13000-13050 - U	Linden Lab	Nieoficjalnie
13720 - T, U	Symantec NetBackup — bprd	Oficjalnie
13721 - T, U	Symantec NetBackup — bpdbrm	Oficjalnie
13724 - T, U	Symantec Network Utility — vnetd	Oficjalnie
13782 - T, U	Symantec NetBackup — bpcd	Oficjalnie
13783 - T, U	Protokół Symantec VOPIED	Oficjalnie
13785 - T, U	Symantec NetBackup Database — nbdb	Oficjalnie
13786 - T, U	Symantec nomdb	Oficjalnie
14576 - U	Battlefield 1942 oraz mods	Nieoficjalnie
16000 - T	shroudBNC	Nieoficjalnie
16080 - T	Usługa Mac OS X Server Web (HTTP) wraz z buforem wydajności	Nieoficjalnie
16384 - U	Tworzenie kopii zapasowej online Iron Mountain Digital	Nieoficjalnie
18180 - T	Serwer raportowania DART	Nieoficjalnie
19226 - T	Panda Software AdminSecure Communication Agent	Nieoficjalnie
19638 - T	Ensim Control Panel	Nieoficjalnie
19771 - T, U	Softros LAN Messenger	Nieoficjalnie
19813 - T	4D Database Client Server Communication	Nieoficjalnie
19880 - T	Softros LAN Messenger	Nieoficjalnie
20000	Distributed Network Protocol (DNP), używany w SCADA	Oficjalnie
20000	Usermin, bazujące na przeglądarce internetowej narzędzie użytkownika	Nieoficjalnie
20014 - T	Serwer raportowania DART	Nieoficjalnie
20720 - T	Symantec i3 Web GUI Server	Nieoficjalnie

**Tabela A.1.** Porty przypisane na stałe: od 1 do 1023, porty zarejestrowane: od 1024 do 49191, porty przypisywane dynamicznie bądź do użytku prywatnego: od 49192 do 65535 (nieprzypisane) — ciąg dalszy

Port	Przypisanie	Uwagi
22347 - T, U	WibuKey, WIBU-SYSTEMS AG Software — system ochrony	Oficjalnie
22350 - T, U	CodeMeter, WIBU-SYSTEMS AG Software — system ochrony	Oficjalnie
24444	NetBeans — zintegrowane środowisko programistyczne	Nieoficjalnie
24800	Synergy: oprogramowanie do współdzielenia klawiatury i myszy	Nieoficjalnie
25999 - T	Xfire	Nieoficjalnie
26000 - T, U	Serwer id Software Quake	Oficjalnie
27000 - U	(Do portu 27006) główny serwer id Software QuakeWorld	Nieoficjalnie
27010	Half-Life i jego mods, na przykład Counter-Strike	Nieoficjalnie
27015	Half-Life i jego mods, na przykład Counter-Strike	Nieoficjalnie
27374	Sub7 (domyślny).	Nieoficjalnie
27500 - U	(Do portu 27900) id Software QuakeWorld	Nieoficjalnie
27900	(Do portu 27901) połączenie Nintendo Wi-Fi	Nieoficjalnie
28910	Połączenie Nintendo Wi-Fi	Nieoficjalnie
29900	(Do portu 29901) połączenie Nintendo Wi-Fi	Nieoficjalnie
29920	Połączenie Nintendo Wi-Fi	Nieoficjalnie
30564 - T	Multiplicity: oprogramowanie do współdzielenia klawiatury, myszy i schowka	Nieoficjalnie
31337 - T	Back Orifice — narzędzie zdalnej administracji (często koń trojański)	Nieoficjalnie
32976 - T	LogMeIn Hamachi (oprogramowanie do tworzenia tuneli VPN; alternatywa dla portu 12975)	Nieoficjalnie
33434 - T, U	Traceroute	Oficjalnie
34443	Serwer wydruku Linksys PSUS4	Nieoficjalnie
36963	Counter-Strike 2D multiplayer (klon 2D popularnej gry komputerowej Counter-Strike)	Nieoficjalnie
37777 - T	Sprzęt Digital Video Recorder	Nieoficjalnie
40000 - T, U	SafetyNET Real-time Industrial Ethernet Protocol	Oficjalnie
47808 - T, U	BACnet Building Automation and Control Networks	Oficjalnie

Źródło: <http://www.iana.org/assignments/port-numbers>. Przedstawiona powyżej lista została edytowana i nie zawiera pełnej listy portów, którą można znaleźć na oficjalnej stronie. Ponadto, oficjalna lista jest na bieżąco aktualizowana.



# Skorowidz

.NET, 459, 623  
.NET Control, 624  
.NET Remoting, 79  
10 GbE, 443  
100 GbE, 443  
100 Giga Ethernet, 443  
1000Base-LX, 301  
1000Base-T, 186  
1000Base-X, 308  
100Base-T, 184, 186  
100Base-TX, 185, 186  
10Base2, 70, 185, 187  
10Base5, 70, 185, 187  
10Base-F, 194  
10Base-T, 185, 186, 301  
10GBase-T, 443, 445  
10GbE, 441  
10GFC Parallel, 426  
10GFC Serial, 426  
10PASS-TS, 258  
16QAM, 375  
1BASE5, 301  
1GFC, 426  
20GFC, 426  
2BASE-TL, 258  
2GFC, 426  
3+Share, 594  
3Com 3Server, 594  
3-etapowy proces negocjacji, 469  
40 GbE, 443  
40 Gigabit Ethernet, 443  
4GFC, 426  
4-PSK, 374  
4-QAM, 374  
64QAM, 375  
802.1, 296  
802.10, 297  
802.11, 28, 297, 365, 366, 370, 372, 380  
    ramki, 382  
802.11a, 265, 369, 371, 372, 375  
802.11b, 371, 372  
802.11g, 29, 265, 371, 372  
802.11n, 369, 371, 372  
802.11s, 394

802.11x, 93, 254  
802.11y, 372  
802.12, 297  
802.13, 297  
802.14, 297  
802.15, 297  
802.16, 297, 342  
802.17, 298  
802.18, 298  
802.19, 298  
802.1P, 672  
802.2, 296  
802.20, 298  
802.21, 298  
802.22, 298  
802.3, 185, 254, 296, 300, 301  
802.3a, 301  
802.3af, 262  
802.3b, 301  
802.3c, 301  
802.4, 296, 314  
802.5, 37, 296  
802.6, 296  
802.7, 296  
802.8, 296  
802.9, 296  
8GFC, 426  
8-PSK, 374

## A

A (DNS), 541, 542  
AAA, 103, 746, 778, 834  
AAAA, 542  
ABR, 125, 358  
ac, 795  
Access Control List, 572, 599  
Access Point, 366  
ACID, 81, 574  
ACK, 53, 381, 466, 467, 469, 470  
ACL, 572  
ACO, 290  
ACT, 776, 777

- Active Directory, 544, 567, 584, 587
  - ADAM, 590
  - BDC, 590
  - DN, 587
  - domena główna, 588
  - domeny, 588
  - GUID, 587
  - jednostka organizacyjna, 587, 588
  - kolejność grup polityki, 579
  - kontrolery domen, 590
  - LDAP, 587
  - nazwa wyróżniająca, 586, 587
  - obiekty, 587, 588, 589
  - OU, 587
  - partycje, 590
  - PDC, 590
  - przestrzeń nazw katalogu, 576
  - relacje zbiorów, 589
  - replikacja, 590
  - RODC, 591
  - UPN, 587
  - zasady polityki, 577
  - zbiory domen, 588
- Active Monitor, 313
- AD, 567
- ad hoc, 30
- Ad Hoc On Demand Distance Vector, 394
- ADAM, 590
- adaptacyjne przełączanie, 213
- adaptacyjne skakanie po częstotliwościach, 378
- adaptacyjny algorytm RED, 219
- adapter ATA, 672
- Adaptive Frequency Hopping, 378
- Add-Drop Multiplexer, 118
- Address, 541
- Address Resolution Protocol, 61, 93, 524
- Address Restricted Cone NAT, 734
- ADM, 118
- administracja, 778
- Adobe Flash, 644, 661, 662
- Adobe Flash Media Streaming Server 4, 658
- Adobe Shockwave, 662
- adres bloku logicznego, 412
- adres dynamiczny, 161
- adres fizyczny, 161
- adres IP, 31, 392, 485
  - dynamiczny adres IP, 508
  - klasy adresów, 489
  - NAT, 732
  - statyczny adres IP, 507
  - ustawianie, 505
- adres IPv4, 487
  - adresy zarezerwowane, 493
  - regionalni administratorzy numerów IP, 492
- adres IPv6, 516
  - adres globalny, 520
  - adres lokalny węzła, 520
  - adres unikalny lokalnie, 520
  - adresy podwójnego stosu IPv6/IPv4, 519
  - automatyczna konfiguracja adresów, 523
  - GA, 520
  - kalkulatory IPv6, 518
  - LLA, 520
  - multimisja, 521
  - notacja skompresowana, 517
  - strefy, 520
  - ULA, 520
  - zakresy adresów, 520, 522
- adres MAC, 40, 59, 61, 71, 89, 161, 213, 300
- adres pętli zwrotnej, 159
- adres sieciowy, 161
- adres statyczny, 161
- adres URL, 612
- adres URN, 613
- adresowanie, 31
  - IPv4, 488
  - IPv6, 516
  - MAC, 61
  - zero configuration, 495
- adresy zarezerwowane IANA, 494
- ADSI, 586
- ADSL, 256, 261, 343, 345
- ADSL Lite, 343, 345
- ADSL Terminal Unit-Remote, 343
- ADSL2, 345
- ADSL2+, 345
- ADU, 329
- Advanced Encryption Standard, 708
- Advanced Intelligent Network, 679
- AES, 706, 708
- AFH, 378
- AFRINIC, 492
- AFS, 599
- AFS Database, 542
- AFSDB, 542
- agent przesyłania poczty, 626
- agent SNMP, 96, 97, 98
- agregacja, 421
- AH, 699
- AIM, 681
- AIN, 679
- AIRCRACK-PTW, 709
- AIX, 553
- Akamai, 457, 598
- aktualizacja routera, 392
- aktywne rozpoznawanie elementów sieciowych, 103
- aktywny algorytm RED, 219
- aktywny koncentrator, 210
- alarmy, 766
- algorytm asymetryczny, 711
- algorytm Bellmana-Forda, 222
- algorytm ciekącego wiadra, 121, 122, 123
- algorytm CRC, 48
- algorytm Dijkstry, 227
- algorytm FDMA, 117
- algorytm GCRA, 121
- algorytm klucza publicznego, 711
- algorytm klucza symetrycznego, 708
- algorytm Nagle'a, 482
- algorytm odrzucania ostatnich pakietów, 218
- algorytm przeszukiwania wszecz, 285

- ul>
- algorytm RED, 218
- algorytm stanu łączy, 226, 227
- algorytm STP, 232
- algorytm wektora odległości, 221
- algorytm wektora odległości z numerami sekwencyjnymi, 226
- algorytm wektora ścieżki, 229
- algorytm wiadra z żetonami, 121, 123, 124
- algorytmy kryptograficzne, 705
- Alias, 542
- alokacja tonów, 265
- AL-PA, 432
- Altiris SVS, 649
- AM, 110, 199
- American National Standard Institute, 45
- amplituda sygnału, 111
- Amplitude Modulation, 199
- analiza Fouriera, 108
- analiza MVA, 151
- analiza przyczyn źródłowych, 768
- Analog Telephone Adapter, 665, 672
- Andrew File System, 599
- anonimowe sieci P2P, 280
- anonimowość w przesyłaniu danych, 243
- anonymous proxy, 737
- ANSI, 44, 45
- ANSI X3T12, 314
- anteny, 397
  - anteny inteligentne, 398
  - anteny izotropowe, 396
  - anteny kierunkowe, 396
  - anteny wielokierunkowe, 395, 396
  - charakterystyka anteny, 395, 396
  - EIRP, 398
  - F/B, 396
  - MIMO, 398
  - polaryzacja, 397
  - położenie anteny, 397
  - poziom promieniowania wstecznego, 396
  - skuteczność anteny, 396
  - SNR, 398
  - szerokość wiązki anteny, 398
  - Yagi, 396
  - zakłócenia, 396
  - zysk anteny, 396
- Antheil George, 119
- anycast, 59, 76, 219, 485
- AODV, 226, 394
- AOL Instant Messenger, 681
- AOL mail, 637
- AP, 366, 385
- ApacheDS, 584
- API, 48, 174, 556, 784
- APIPA, 495
- aplikacje klient-serwer, 79
- aplikacje P2P, 78
- aplikacje X Window, 83
- aplikacje zorientowane plikowo pamięci masowej, 424
- APNIC, 493
- APOP, 637
- Apple LocalTalk, 259
- Apple Open Directory, 584
- Apple QuickTime, 647, 661
- Apple QuickTime Streaming Server, 658
- AppleTalk, 30, 77, 550
- Application Compatibility Toolkit, 776
- Application Data Unit, 329
- Application Programming Interface, 48
- Application Specific Integrated Circuit, 94, 157
- Arbitrated Loop Physical Addresses, 432
- architektura BitTorrent, 279
- architektura dwuwarstwowa, 81
- architektura Fabric, 409
- architektura Infiniband, 451
- architektura n-warstwowa, 80
- architektura oparta na usługach, 612, 622
- architektura POSIX, 556
- architektura sieci, 59, 60
- architektura STREAMS, 557
- architektura systemów sieciowych, 56
- architektura TCP/IP, 61, 62
- architektura trójwarstwowa, 81
- architektura VIA, 450
- architektura wielowarstwowa, 78, 80
- ARCNET, 37, 311
- ARIN, 492
- arp, 533, 795
- ARP, 61, 89, 93, 214, 524, 531
  - przeglądanie bufora, 533
  - ramki, 532
  - zadania, 531
- ARPAnet, 528
- ARQ, 381
- AS, 221, 362
- ASCII, 109
- ASIC, 94, 157, 158, 448, 455, 595
- ASK, 193
- ASN, 486, 487
- ASN.1, 99
- Asterisk, 668
- asymetryczne DSL, 343
- Asynchronous Transfer Mode, 357
- AT&T, 339, 340, 554
- ATA, 665, 672
- ataki, 688, 692
  - ataki DDoS, 693
  - ataki DoS, 481, 692, 729
  - ataki man-in-the-middle, 481
  - ataki powtórzeniowe, 712
  - ataki przejścia komunikacji, 243
  - ataki siłowe, 706, 707
  - ataki smerfów, 692
  - ataki z osobą pośrodku, 693, 712
- ATM, 93, 194, 206, 355, 357
  - ABR, 358
  - CBR, 358
  - GCRA, 121
  - implementacja, 357
  - jakość usługi, 125
  - klasy usług, 125
  - komórki, 357, 358
  - kontrakt ruchowy, 358

**ATM**

- kontrola ruchu, 358
- kształtowanie ruchu, 358
- NNI, 357
- ogólny algorytm wyznaczania szybkości komórek, 121
- polityka ruchu, 358
- poziom transferu, 358
- QoS, 358
- sterowanie przepływem, 120
- styki, 357
- UBR, 358
- umowy dotyczące jakości usług, 125
- UNI, 357
- VBR, 358

ATM Address, 542

ATMA, 542

atmadm, 795

AToM, 742

ATU-R, 343

AUI, 187

Austin Common Standards Revision Group, 559

Authenticated POP, 637

Authentication, Authorization, Accounting, 103

Automatic Private IP Address, 495

automatyczna konfiguracja adresów IP, 508

- adresy IPv6, 523

automatyka domowa, 319

- sieci, 325

Auto-MDI-X, 186

Autonomous System, 221, 362

Autonomous System Number, 486

autoryzacja, 835

Auto-Uplink, 186

Available Bit Rate, 125

AX.25, 355

**B**

backplane, 217

Backup Domain Controller, 573, 590

BACnet, 330

badanie stanu kanału, 299

Banyan VINES, 569

Barix Instreamer, 657

Base16, 634

Base32, 634

Base64, 629, 633

baseband, 301

bash, 791, 795

Basic Rate Interface, 342

Basic Service Set, 366

baza danych informacji o trasach, 88, 217

baza danych informacji zarządzania, 96, 98

baza danych NVD, 691

baza danych przełączania, 217

BBRAS, 831

BCV, 411, 694

BDC, 590

BDD, 138

beacon, 366

Beaconing, 314

BeanShell, 792

BearShare, 274

Berkeley Sockets, 558

best effort, 66

bezpieczeństwo, 142, 297, 687

- bezpieczeństwo sieci, 688
- CVSS, 689
- HomePlug, 267
- HTTPS, 687, 703
- IPsec, 687, 698, 699
- luki w zabezpieczeniach sieci, 688
- miejsca ataku, 691
- minimalizacja obszaru ataku, 694
- NAP, 687, 696, 697
- NLA, 687, 696
- NVD, 691
- odpowiedź na wykrycie włamania, 694
- określanie podatności systemu komputerowego na luki w zabezpieczeniach, 689
- oprogramowanie, 695
- polityka bezpieczeństwa, 696
- protokoły, 698
- reguły tworzenia bezpiecznej sieci, 694
- serwer proxy, 735
- sieć bezprzewodowa, 402
- SSL, 702
- STRIDE, 693
- szyfrowanie, 705
- TLS, 702
- zalecenia, 695
- zapora sieciowa, 717, 718
- zarządzanie bezpieczeństwem, 782

bezpieczny VPN, 743

bezprzewodowa sieć kratowa, 393

bezprzewodowy punkt dostępowy, 385

bezstanowość, 475

BFS, 285

BGP, 221, 231, 362, 486

- CIDR, 232
- trasy, 231

biały szum, 377

biblioteki taśmowe, 415

BIG-IP, 456

BIND, 536

B-ISDN, 342

bit, 46

bit dopełniający, 303

bitrate, 655

BitTorrent, 42, 78, 121, 277, 515

Biz Talk Server, 564

blokowe urządzenia pamięci masowej, 422

BLSR, 350

BlueCore Serial Protocol, 830

Bluetooth, 30, 254, 287, 325

- ACO, 290
- asynchroniczne bezpołączeniowe, 290
- DUN, 290
- komponent nadrzędny, 288
- LAP, 290
- master, 288

PAN, 290  
 pikosieć, 288, 289  
 połączenia, 288, 289  
 profile, 290  
 przyłączanie jednostki, 288  
 sieć, 288  
 sieć rozproszona, 288  
 slave, 288  
 synchroniczne połączeniowe, 290  
 urządzenia podrzędne, 288  
 zakres częstotliwości, 287  
 Bluetooth Special Interest Group, 287  
 BNC, 70, 185  
 bod, 112  
 BOINC, 458  
 Bonjour, 735  
 BOOTP, 86, 91, 510  
 Bootstrap, 510  
 Border Gateway Protocol, 221, 362  
 BPDU, 236  
 BPSK, 374, 375  
 brama, 77, 247, 385, 736  
 brama bezpieczeństwa, 724  
 brama bezprzewodowa, 390  
 bramka VoIP, 672  
 BRAS, 831  
 Breadth First Search, 285  
 BRI, 342  
 bridge, 211  
 Bridge Protocol Data Units, 236  
 Broadband ISDN, 342  
 broadcast, 59, 76, 219, 299  
 broadcasting, 298  
 brouter, 216  
 brute force, 707  
 brzegowa zaporą sieciową, 725  
 BSD, 553, 562, 595  
 BSS, 366  
 bufor ARP, 533  
 buforowanie, 121, 593  
 buforowanie brzegowe, 598  
 buforowanie plików, 597, 598  
 bursts, 319  
 burza żądań RARP, 533  
 Business Continiance Volumes, 411

## C

Cable Data Link Protocol, 257  
 call center, 666  
 Campus Area Network, 31, 336  
 CAN, 31, 336  
 Canonical Name, 541  
 CAP, 343, 344  
 Carrier Sense Multiple Access with Collision Avoidance, 73, 267  
 Carrier Sense Multiple Access with Collision Detection, 73  
 CASE, 624  
 CAT 1, 181  
 CAT 5, 51, 182, 185

CAT 5e, 181, 182, 258  
 CAT 6, 51, 182, 185, 258  
 CAT 6e, 182  
 CBP, 372  
 CBPDU, 237  
 CBR, 125, 358, 656, 657  
 CCITT, 348  
 CCK, 373  
 CCM, 676  
 CDB, 435  
 CDDI, 315  
 CDE, 559  
 CDLP, 257  
 CDMA, 119, 377  
 CDTV, 126  
 CDV, 126  
 Cell Delay Variation, 126  
 Cell Delay Variation Tolerance, 126  
 Cell Error Rate, 125  
 Cell Loss Rate, 125  
 Cell Misinsertion Rate, 126  
 Cell Transfer Delay, 126  
 centrala sterowana programowo, 667  
 Centrex, 667  
 centrum dystrybucji kluczy, 714  
 CER, 125, 839  
 certyfikaty klucza publicznego, 705  
 CGI, 619  
 CHAD, 323  
 Challenge and Response Protocol, 435  
 Challenge Handshake Authentication System, 742  
 CHAP, 435, 742  
 charakterystyka anteny, 395  
 chdir, 795  
 Cheops, 103  
 chkds, 796  
 chmura, 442, 459  
 ciagle udoskonalanie usług, 136  
 CIDR, 232, 488, 490, 504  
 ciekące wiadro, 121, 122  
 cienki Ethernet, 184, 187  
 cienki klient, 532  
 CIFS, 593, 595, 599, 601  
 CIM, 90, 438  
 CIR, 359  
 Cisco Systems, 552  
 Citrix NetScaler MX, 456  
 Citrix XenApp, 82, 649  
 cLAN, 450  
 Class of Service, 672  
 Classless Inter-Domain Routing, 490  
 CLEAN, 472  
 Clear to Send, 120, 382  
 CLI, 165, 791  
 cloud computing, 442  
 CLR, 125  
 cmd.com, 791  
 cmdlet, 816, 817  
 CMIP, 763  
 CMR, 126

cmstp, 796  
CN, 585, 586  
CNAME, 541, 542  
Code Division Multiple Access, 119  
Coherent Phase Shift Keying, 373  
Command-Line Interface, 165  
Commerce Server, 564  
Committed Information Rate, 359  
Common Gateway Interface, 619  
Common Information Model, 90, 438, 764  
Common Internet File System, 600  
Common Name, 585, 586  
Common Vulnerabilities and Exposures, 690  
Common Vulnerability Scoring System, 689  
comp, 796  
compact, 796  
Complementary Code Keying, 373  
compress, 796  
Computer Telephony Integration, 666, 678  
Configuration BPDUs, 237  
CONNECT, 615  
Constant Bit Rate, 125, 656  
Content-Disposition, 634  
Content-Type, 634  
Continual Service Improvement, 136  
Copper Data Distribution Interface, 315  
copy, 796  
CORBA, 79  
CoS, 672  
COSE, 559  
Coyote Point Systems Equalizer, 456  
cp, 796  
CPSK, 373  
CRC, 48, 467, 734  
CRC-32, 48  
crontab, 796  
csh, 791, 796  
CSI, 136  
CSMA/CA, 73, 267  
CSMA/CD, 73, 293, 296, 300, 307, 381  
    odstęp IFG, 309  
    stany sieci, 308  
    transmisja ramki, 308  
CSTA, 679  
CSU, 338  
CTD, 126  
CTI, 666, 678  
    usługi, 678  
CTS, 120, 382  
CUCM, 669, 676  
cut through, 213  
CVE, 690  
CVSS, 689  
CVSS FIRST, 689  
CVSS Special Interest Group, 689  
CWR, 467  
cyfrowa linia abonencka, 256, 342  
cyfrowe sygnały, 108  
czas odpowiedzi, 140  
czas życia pakietu, 207

czasowy wielodostęp do łącza, 299  
częstotliwość fali, 196  
częstotliwość odcięcia, 111  
częstotliwość próbkowania, 112  
częstotliwość próbkowania Nyquista, 113  
częstotliwość sygnału, 109  
częściowo połączona sieć siatkowa, 38  
człowiek pośrodku, 481  
czyste sieci P2P, 273

## D

DA, 305, 383  
DAAP, 474  
DAC, 315, 828  
DAP, 582  
Darknet, 276  
Darwin Streaming Server, 658  
DAS, 315, 409, 410, 424  
Data Circuit-terminating Equipment, 119  
Data Encryption Standard, 267, 705, 708  
Data Over Cable Service Interface Specification, 346  
Data Set Ready, 120  
Data Terminal Equipment, 119  
Data Terminal Ready, 120  
data vault, 437  
datagramy, 46, 69, 70, 355, 475, 476  
    IP, 496  
    IPv6, 523  
DBPSK, 265  
DC, 586  
DCE, 119, 300  
DCF, 381  
DCOM, 102  
dcpromo, 588  
DCS, 324, 325  
DDI, 671  
DDoS, 693  
DDP, 451  
DD-WRT, 392  
DEC STP, 232  
dedykowana sieć z komutacją obwodów, 338  
Deep Packet Inspection, 717, 720  
Deep Packet Inspection Firewall, 730  
definiowanie poziomów usług, 139  
definiowanie sieci komputerowej, 28  
dekady, 198  
DELETE, 615  
Demilitarized Zone, 725  
demultiplexer, 115  
DEMUX, 115  
Denial of Service, 481, 692  
Dependent Station Enablement, 372  
Depta First Search, 285  
DES, 267, 705, 707, 708, 714  
designated port, 234  
Desktop Management Interface, 101  
Destination NAT, 735  
Destination-Sequenced Distance Vector, 394  
Destination-Sequenced Distance Vector Routing, 226

- DF, 497
- DF1, 327
- DFIR, 370
- DFS, 594, 599, 606
  - hierarchia nazw, 608
  - mapowanie przestrzeni nazw, 608
  - przestrzeni nazw, 608
  - serwer, 608
- dhclient, 797
- DHCP, 91, 476, 508
  - alokacja statyczna, 509
  - implementacje, 509
  - konfiguracja, 509
  - przyznawanie adresu, 509
  - zabezpieczanie, 510
- DHT, 276
- diagnostyka sieci, 789, 790
- diagram czasowy, 79
- diagram sekwencji, 79
- diagram zdarzeń, 79
- dial-up, 341
- Dial-Up Networking, 290
- Diameter, 778, 838
  - aplikacje, 839
- DID, 671
- dielektryk, 183
- Differential Binary Phase-Shift Keying, 265
- Differential Phase Shift Keying, 373
- Differential Quadrature Phase-Shift Keying, 265
- Diffie-Hellman Key Agreement, 706
- Diffie-Hellman-Merkel, 712
- DiffServe, 497
- Diffuse Infrared, 370
- dig, 797
- Digital Audio Access Protocol, 474
- Digital Rights Management, 645
- Digital Subscriber Line, 256, 341
- diody LED, 193
- dircmp, 797
- Direct Attached Storage, 424
- Direct Data Protocol, 451
- Direct Sequence Spread Spectrum, 371
- directed broadcast, 485
- Directory Access Protocol, 582
- Directory Information Shadowing Protocol, 582
- Directory Operational Bindings Management Protocol, 583
- Directory Server, 584
- Directory System Agent, 582
- Directory System Protocol, 583
- diskcopy, 797
- DISP, 582
- Distance Vector, 221
- Distinguished Name, 585, 586
- Distributed Control System, 324
- Distributed Coordination Function, 381
- Distributed Denial of Service, 693
- Distributed File System, 594, 599, 606
- Distributed Hash Table, 276
- Distributed Management Task Force, 438
- Distributed Queue Dual Bus, 356
- Distribution System, 366
- DIX, 295
- DLCI, 359
- dławienie przepływności, 122
- długość fali, 196
- DMA, 447
- DMB, 604
- DMI, 101, 764
- DMT, 343, 344
- DMTF, 438
- DMZ, 725
- DN, 585, 586, 587
- DNAT, 735
- DNS, 85, 93, 476, 527, 536
  - A, 541, 542
  - AAAA, 542
  - AFSDB, 542
  - architektura klient-serwer, 538
  - ATMA, 542
  - BIND, 536
  - bufor lokalny, 538
  - CNAME, 541, 542
  - domeny, 537
  - domeny najwyższego poziomu, 536
  - glue record, 539
  - HINFO, 542
  - ISDN, 542
  - KEY, 543
  - MB, 543
  - MG, 543
  - MINFO, 543
  - MR, 543
  - MX, 541, 542
  - NS, 541
  - NXT, 543
  - oprogramowanie, 536
  - poczta elektroniczna, 627
  - przestrzeń nazw, 539, 540
  - PTR, 541, 543
  - rekord zasobów, 538, 539, 540
  - rekordy, 536
  - resolver, 538
  - root servers, 536
  - RP, 543
  - RR, 538
  - RT, 543
  - serwer, 538
  - SIG, 544
  - SOA, 539, 541
  - SRV, 543
  - strefy wpływów, 539
  - struktura domen, 537
  - TLD, 536
  - topologia, 539
  - TXT, 544
  - WKS, 544
  - X.25, 544
  - zapytanie o adres IP, 538
  - zadania, 537
- DNS SRV, 839
- dobrze znane porty, 477
- DOCSIS, 257, 346

dom inteligentny, 319  
Domain Component, 586  
Domain Master Browser, 604  
Domain Name System, 86, 527, 536  
domena kolizyjna, 71, 72, 209, 214, 215  
domena pamięci masowej, 420  
    warstwa pliku, 420  
domena rozgłoszeniowa, 71, 72  
domeny, 78, 537, 568, 570  
domeny najwyższego poziomu, 536  
domeny Windows, 30, 604  
Don't Fragment, 497  
DOP, 583  
DoS, 481, 692, 719, 729  
dostarczanie pakietów, 53  
dostawca sieci, 166  
dostawca usług, 49  
dostawca usług internetowych, 486  
dostawca usług zarządzanych, 787  
dostęp do kanału, 299  
dostęp do kanału z detekcją kolizji, 299  
dostęp negocjowany, 67  
dostęp przez sieć B-ISDN, 342  
dostęp zdalny, 827, 828  
    protokoły połączenia zdalnego, 829  
    pulpit zdalny, 831  
    RAC, 828  
    RADIUS, 834  
    RAS, 828, 831  
    serwer, 828  
    usługi, 830  
dostępna przepustowość, 125  
dostępność, 142  
DPA, 839  
DPR, 839  
DPSK, 373  
DQDB, 296, 356  
DQPSK, 265  
Draft-Martini, 742  
DRM, 459, 645, 656  
drop cable, 39  
drzewo, 33, 38, 39  
drzewo rozpinające, 233  
DS, 366  
DSA, 582  
DSDV, 226, 394  
DSE, 372  
DSL, 256, 341, 342, 667  
    ADSL, 343  
    ATU-R, 343  
    charakterystyka usług, 345  
    modem, 343  
    modulacja CAP, 344  
    modulacja DMT, 344  
    odległość, 343  
    pętla abonencka, 343  
    prędkość pobierania, 343  
    rozdzielacz sygnałów, 343  
    splitter, 343  
DSLAM, 831  
DSML, 586

DSP, 583  
DSR, 120  
DSSS, 365, 371, 375, 377  
DSU, 338  
DTE, 119, 120, 300  
DTR, 120  
DTrace, 563  
Dual Homed, 316  
Dual-Attachment Concentrator, 315  
Dual-Attachment Station, 315  
DUN, 290  
dupleks, 53  
DV, 221  
DWA, 839  
DWR, 839  
Dynamic Host Configuration Protocol, 476, 508  
Dynamic Tracing, 563  
dynamiczne strony internetowe, 619  
dynamiczny adres IP, 508  
dyspersja, 188  
dystrybucje systemu Linux, 560  
działanie w chmurach, 458  
dzielony horyzont, 225  
dziennik zdarzeń, 765

## **E**

EAP, 755  
Early Token Release, 313  
eBGP, 231  
ECE, 467  
ECMA, 679  
ECN, 497  
ECSA, 372  
edge-caching, 598  
EDI, 628  
eDirectory, 544, 584, 585  
    protokoły, 585  
efekt wielodrogowości, 396  
efi, 791  
EFM, 258  
EFMCu, 258  
EGP, 221, 487  
EHCI, 283  
EHLO, 631  
EIA/TIA, 181  
EIGRP, 225  
EIR, 359  
EIRP, 398  
EJB, 624  
ekranowanie, 180  
EKS, 267  
Eksploatacja usług, 136  
Electromagnetic Interference, 180  
Electronic Data Interaction, 628  
Electronic Software Distribution, 771  
eliminowanie zatorów, 148  
e-mail, 625  
EMC Celerra, 411  
EMF over Copper, 258

EMI, 180, 181  
emisja dowolna, 76, 219  
emisja pojedyncza, 76, 485, 487, 648  
emisja rozgłoszeniowa, 76  
encje, 49  
Encryption Key Select, 267  
enkapsulacja, 47  
Enterprise Resource Planning, 571  
Enterprise Single Sign On, 574  
EPON, 259  
ERP, 571  
ERWin, 624  
eSATA, 409  
ESD, 771  
ESMTP, 631  
ESP, 700, 701  
ESS, 367  
E-SSO, 574  
eth0, 163  
Ethernet, 34, 44, 61, 251, 254, 258, 293, 300, 325  
    adres MAC, 300  
    CSMA/CD, 300, 307  
    DCE, 300  
    długość łącza, 308, 309  
    DTE, 300  
    format ramki, 306  
    IEEE 802.3, 301  
    IFG, 307  
    kolizje, 308  
    kontrola błędów, 304  
    media fizyczne, 258  
    okablowanie, 184  
    połączenia, 258  
    PRE, 305  
    ramki, 300, 303  
    rozmiary ramek, 309  
    skrętka, 184  
    stacje końcowe, 300  
    standardy, 301, 443  
    standardy łączenia przewodów, 185  
    struktura ramki, 305  
    transmisja ramki, 308  
    tryb pełnoduplexowy, 310  
    tryb wiązkowy, 307  
    warstwy, 304  
    węzły, 300  
    wiązka, 307  
Ethernet I.0, 300  
Ethernet II, 301  
Ethernet in the First Mile, 258  
Ethernet over Passive Optical Networks, 259  
ETR, 313  
etykiety MPLS, 360  
Eudora, 640  
EUI, 435  
EuroDOCSIS, 257, 346  
EVDO, 681  
Examination Institute for Information Science, 137  
Excess Information Rate, 359  
Exchange, 638  
Exchange Server, 564

Exclusive OR, 709  
Exim, 638  
EXIN, 137  
expand, 797  
Experimental Ethernet, 301  
exploity, 688  
EXT, 306  
Extended Services Set, 367  
Extended Simple Mail Transfer Protocol, 631  
Extensible Authentication Protocol, 755  
Exterior Gateway Protocol, 221  
External Data Representation, 599  
Extranet Publishing, 738

## F

F/B, 396  
F2F, 271, 281  
F4A, 663  
F4B, 663  
F4P, 663  
F4V, 663  
Fabric, 409  
Failover, 723  
fale radiowe, 396  
Far End Crosstalk, 181  
FAS, 595  
Fast Fourier Transform, 379  
FastCGI, 620  
faza sygnału okresowego, 110  
FC, 383  
FC/IP, 433  
FC-0, 428  
FC-1, 428  
FC-2, 428  
FC-3, 428  
FC-4, 429  
FC-AL, 410, 430  
FCAPS, 761, 762  
    obszary, 763  
FCC, 681  
FCIA, 410  
FCIP, 414, 433, 436  
FCoIB, 452  
FCP, 410, 414, 425, 428  
FC-P2P, 409, 410  
FCS, 306  
FC-SW, 408, 410, 429, 431  
FDDI, 37, 77, 194, 294, 314  
    DAC, 315, 316  
    DAS, 315  
    dodawanie węzłów, 316  
    drzewo koncentratorów, 317  
    Dual Homed, 316  
    koncentrator, 315  
    LLC, 315  
    MAC, 315  
    model OSI, 315  
    pierścienie, 317  
    połączenia, 315  
    SAC, 316

- FDDI
  - SAS, 315
  - sieci szkieletowe, 316
  - stacje, 315
  - topologie, 316
  - urządzenia, 315
- FDDI-II, 316
- FDM, 117, 298, 346, 347
- FDMA, 117
- FEC, 265, 303
- FEXT, 181
- FFT, 379
- FHSS, 119, 365, 370, 376, 378
- FIB, 217
- Fiber Distributed Data Interface, 314
- Fibre Channel, 100, 408, 409, 425
  - FC-AL, 430
  - FCP, 425, 428
  - FC-SW, 429, 431
  - klasy sieci, 425
  - kontrola przepływu, 429
  - oznaczenia portów, 427
  - porty, 427
  - ramki, 429
  - standardy sieci, 426
  - warstwy protokołu FC, 428
  - zarządzanie ruchem sieciowym, 429
- Fibre Channel Arbitrated Loop, 410, 430
- Fibre Channel Industry Association, 410
- Fibre Channel over InfiniBand, 452
- Fibre Channel over IP, 414, 433, 436
  - data vault, 437
  - przyrostowe tworzenie kopii zapasowej, 437
- Fibre Channel Point-to-Point, 409
- Fibre Channel Protocol, 414, 425, 428
- Fibre Channel Switched fabric, 408, 410, 429, 431
  - adresowanie, 432
  - adresy fizyczne pętli arbitrażowej, 432
  - adresy portów, 432
  - AL-PA, 432
  - OUI, 432
  - podział na strefy, 432
  - WWN, 432
- Fibre Channel z pętlą arbitrażową, 430
- Fibre Connectivity, 414
- FICON, 414
- FIFO, 146
- File Transfer Protocol, 55
- filer NAS, 594, 595
- filtr dolnoprzepustowy, 111
- filtrowanie aplikacji, 720
- filtrowanie pakietów, 719, 727
- filtrowanie spamu, 641
- FIN, 467
- finger, 797
- FireEngine, 562
- FireWire, 285
  - BFS, 285
  - DFS, 285
  - identyfikatory IEEE EUI-64, 285
  - mechanizm przeszukiwania w głąb, 285
  - urządzenia, 285
- FireWire 400, 285, 286
- FireWire 800, 286
- fizyczne interfejsy sieciowe, 158
- fizyczne medium transmisyjne, 28
- fizyczne połączenia punkt-punkt, 63
- flagi TCP, 466
- Flash, 662
- Flash Video, 662
- FLOGI, 431
- FLOPS, 455
- FM, 110, 199
- FMP, 445
- FMSS, 658
- Foil Twisted Pair, 181
- Folding@Home, 442, 458
- forced flow law, 145
- forward delay, 237
- Forward Error Correction, 265
- Forwarding Information Base, 217
- Forwarding Table, 213
- fragment free, 213
- Frame Relay, 52, 206, 359
  - CIR, 359
  - DCE, 359
  - DLCI, 359
  - DTE, 359
  - EIR, 359
  - gwarantowana przepływność, 359
  - łącza wirtualne, 359
  - ramki, 359
  - sterowanie przepływem, 120
  - wydajność łącza, 359
- FreeNAS, 595
- Freenet, 271, 276
- FreeRADIUS, 837
- Frequency Division Multiple Access, 117
- Frequency Division Multiplexing, 117, 298
- Frequency Hopping Spread Spectrum, 119, 370, 378
- Frequency Modulation, 199
- Friend-to-Friend, 271, 281
- Front-to-Back, 396
- FRS, 607
- FSK, 193
- ftp, 797
- FTP, 55, 181
- Full Cone NAT, 734
- Functional Multiprocessing, 445
- funkcja haszująca, 710
- funkcja skrótu, 710

**G**

- G. Lite, 343
- GA, 520
- Galileo, 378
- GAN, 680
- GbE, 443
- GCRA, 121
- Generic Cell Rate Algorithm, 121

GET, 98, 615  
GETBULK, 98  
getfacl, 797  
getInetAddresses(), 160  
Getmac, 798  
GETNEXT, 98  
GHO, 772  
Gigabit Ethernet, 307, 308, 443  
GigaLAN, 450  
GigE, 443  
Global Address, 520  
Globally Unique Identifier, 587  
glue record, 539  
głęboka analiza pakietów, 717, 720  
główna przeglądarka, 87  
Gmail, 637  
gniazda, 79, 557  
    gniazda do przesyłania datagramów, 475  
    gniazda internetowe, 557  
    gniazda sieciowe, 557  
GNU, 560  
GNU Radius, 837  
Gnucleus, 274  
Gnutella, 271, 274  
Google Maps Microwave Link Planning Tool, 202  
Google Search Appliance, 131  
GoS, 124  
GoToAssist, 833  
GoToMeeting, 833  
GoToMyPC, 833  
GoToMyPC Broker, 833  
gotowość do nadawania, 120  
gotowość terminalu danych, 120  
gotowość zbioru danych, 120  
gpresult, 798  
GPS, 355  
Grade of Service, 124  
gradientowy światłowód wielomodowy, 189  
GRE, 754  
grid computing, 442  
grid network, 42  
Group Policies, 576  
Group Policy Object Editor, 579  
gruby Ethernet, 184, 187  
Grupa ds. Radiokomunikacji, 45  
Grupa ds. Telekomunikacji, 45  
grupa robocza, 30, 78, 272  
Grupa Rozwoju Telefonii, 45  
GSM, 680, 681  
GUI, 79  
GUID, 587  
gwarantowana jakość usługi, 67, 124  
gwiazda, 33, 35  
gwiazda — magistrala, 39  
gwiazda — pierścień, 40

## H

H.323, 669, 675, 677  
Hamachi VPN, 496  
harmoniczne, 105

hasła, 695, 706  
HBA, 101, 410, 412  
HCA, 452  
HDSL, 345  
HEAD, 615  
Helix Server, 658  
HELLO, 230  
Hewlett-Packard NAS, 596  
HFC, 346  
hierarchiczna gwiazda, 39  
High Performance Parallel Interface, 425  
High-performance computing, 442  
HINFO, 542  
HLEN, 532  
HMI, 294, 318  
HomePlug, 251, 255, 262, 325  
    alokacja tonów, 265  
    bezpieczeństwo, 267  
    CSMA/CA, 267  
    DBPSK, 265  
    DQPSK, 265  
    FEC, 265  
    kontrola dostępu do medium, 266  
    korekcja błędów, 265  
    MAC, 266  
    modulacja, 265  
    OFDM, 265  
    poziomy jakości usługi, 267  
    przepływność kanałów, 265  
    ramki, 266  
    ROBO, 265  
    sekwencje danych, 266  
    sposoby dostarczania zasilania, 263  
    sterowanie przepływem, 267  
    szyfrowanie, 267  
    transmisja danych, 264  
    warstwa MAC, 266  
HomePlug 1.0, 262  
HomePlug AV, 262  
HomePNA, 251, 255, 259, 260, 325  
HomePNA 3.1, 260  
host, 798  
Host Address, 542  
Host Bus Adapter, 101, 410  
Host Channel Adapter, 452  
Host Information, 542  
hostname, 798  
HOSTS, 85, 93, 528  
hot swap, 171  
Hotmail, 637  
HPC, 442  
HPPI, 425  
HSDA, 681  
HTML, 611  
HTTP, 55, 79, 96, 98, 611, 612  
    CONNECT, 615  
    DELETE, 615  
    GET, 613, 615  
    HEAD, 615  
    Keep-Alive, 614

## HTTP

- kody stanów, 615
  - metody, 615
  - nagłówki, 614
  - OPTIONS, 615
  - POST, 615
  - PUT, 615
  - TRACE, 615
  - zadania, 613
- HTTP 1.1, 612
- HTTPS, 619, 687, 696, 703
- HTYPE, 532
- hub, 210
- Human Machine Interface, 294
- HVAC, 318
- HWMP, 394
- Hybrid fibre-coaxial, 346
- Hybrid Wireless Mesh Protocol, 394
- hybrydowa siatka, 40
- hybrydowa sieć peer-to-peer, 276
- hybrydowe sieci oparte na kablach światłowodowych
- i koncentrycznych, 346
- hybrydowy VPN, 743
- HyperText Transfer Protocol, 55, 611
- HyperText Transfer Protocol Secure, 703
- Hypervisor XEN, 563

**I**

- i.LINK, 285
- IAC, 620
- IANA, 492, 572
- IANA ASN, 486
- IAS, 830
- IAX, 672, 675, 677
- iBGP, 231
- IBM Tivoli Directory Server, 584
- IBSS, 366
- ICA, 83, 832
- ICE, 677
- Icecast Streaming Media Server, 658
- ICI, 380
- IcM, 768
- ICMP, 70, 511, 524
- nagłówki, 511
  - typy, 512
  - wiadomości, 511
- ICMPv6, 525
- IDA, 581
- Identity and Access, 581
- Identity Lifecycle Management, 582
- identyfikatory
- DLCI, 359
  - ESSID, 367
  - SSI, 389
  - SSID, 366
  - UUID, 587
- IDLE Push-IMAP, 628
- IDS, 694
- IDSL, 345
- IDU, 49
- IEEE, 45, 161, 295
- IEEE 1394, 285
- IEEE 1394-1995, 285
- IEEE 1394a-2000, 285
- IEEE 802.11, 368
- IEEE 802.1D, 211, 212
- IEEE 802.1Q, 217
- IEEE 802.3ah, 258
- IEEE 802.5, 311
- IEEE EUI-64, 285
- IETF, 45, 96, 612
- ifconfig, 163, 164, 798
- iFCP, 433, 438
- ifdown, 798
- IFG, 307, 309
- ifup, 798
- IGP, 91, 221, 487
- IGRP, 91, 221, 225
- IKE, 700
- ILM, 413
- IMAP, 625, 636, 637
- IN, 679
- Incident Management, 768
- Independent Computing Architecture, 83, 832
- InfiniBand, 442, 450, 451
- HCA, 452
  - połączenia, 452
  - TCA, 452
- Infoblox-2000 Network Service Appliance, 131
- informacje o sieci, 85
- oprzyrządowanie do zarządzania systemem Windows, 101
  - WMI, 101
- Information Lifecycle Management, 413
- Information Systems Examination Board, 137
- Information Technology Infrastructure Library, 135
- infrastruktura klucza publicznego, 702
- inicjacja połączenia, 50
- Input/Output Operations per Second, 145
- inSSIDer, 401
- instalacja elektryczna, 262
- Instant Messaging, 666
- INSTEON, 325
- Institute of Electrical and Electronics Engineers, 45
- Integrated IS-IS, 229
- Integrated Services Digital Network, 542
- Inter-Application Communication, 620
- Inter-Asterisk eXchange, 677
- InterCarrier Interference, 380
- Interface Data Unit, 49
- interfejs API, 174
- interfejs HMI, 318
- interfejs pętli zwrotnej, 159
- interfejs sieciowy, 157, 174
- adres fizyczny, 161
  - adres MAC, 161
  - adres sieciowy, 161
  - dostawcy, 165
  - fizyczne interfejsy sieciowe, 158
  - instalacja większej liczby kart sieciowych, 168
  - interfejs API, 174

- interfejs pętli zwrotnej, 159
- izolacja, 159, 168
- izolacja aplikacji, 160
- izolacja fizyczna, 168
- karta sieciowa, 158, 172
- kolejność dostawców, 167
- kolejność powiązań, 165
- konfiguracja, 162
- lista wykorzystywanych adresów IP, 160
- logiczne interfejsy sieciowe, 159
- magistrale komunikacyjne, 170
- nadmiarowość, 159
- nazwa interfejsu logicznego, 160
- NIU, 158
- numer interfejsu logicznego, 160
- odporność na awarie, 168
- powiązania, 165
- routing, 168
- sterowniki sieciowe, 173
- tworzenie interfejsów sieciowych, 163
- UDI, 174
- ujednolicony interfejs sterownika, 174
- wielokrotne wirtualne interfejsy sieciowe, 160
- wysoka wydajność, 159
- zmiana kolejności powiązań, 166
- zwiększona wydajność, 168
- interfejs wiersza poleceń, 165
- interfejs zależny od medium transmisyjnego, 186
- interfejs zarządzania stacją roboczą, 101
- interferometr Fabry-Perota, 118
- Interframe Gap, 307
- Interior Gateway Protocol, 91, 221
- Interior Gateway Routing Protocol, 91, 221
- Intermediate System to Intermediate System, 221
- Internet, 31, 206, 361, 725
  - IXP, 361, 362
  - punkty wymiany ruchu, 361
  - TCP, 464
  - UDP, 475
- Internet Assigned Numbers Authority, 492
- Internet Control Message Protocol, 511, 524
- Internet Engineering Task Force, 45
- Internet eXchange Point, 361
- Internet Fibre Channel Protocol, 438
- Internet Information Server, 564
- Internet Protocol, 55, 61, 463, 485
- Internet Protocol Automatic Configuration, 495
- Internet Protocol Security, 699
- Internet Protocol Suite, 61
- Internet Protocol Version 6, 514
- Internet Security and Acceleration Server, 170
- Internet Service Provider, 486
- Internet Storage Name Service, 439
- Internet Wide Area RDMA Protocol, 450, 451
- Internet2, 336, 363
- internetowy protokół transportowy, 463
- interpreter wiersza poleceń, 790
- Inter-Process Communication, 556
- intersieć, 31
- InterSymbol Interference, 380
- Intrusion Detection System, 694
- inżynieria ruchu, 121, 122
  - algorytm ciekącego wiadra, 122
  - algorytm wiadra z żetonami, 123
  - buforowanie, 121
  - kształtowanie ruchu, 121
  - mechanizm kontroli dostępu, 122
  - zapisz i przekaz, 121
- IOPS, 145
- IOS, 552, 553
- IP, 55, 61, 463, 485, 486
  - DHCP, 508
  - ICMP, 511
  - interfejs pętli zwrotnej, 159
  - kształtowanie ruchu, 122
  - routing, 485, 487
  - system autonomiczny, 486
  - ustawianie adresu IP, 505
- IP PBX, 667
- IP spoofing, 719
- IPAC, 495
- IPBX, 667
- IPC, 556
- ipconfig, 162, 163, 506, 537, 793, 798
  - /release, 793
  - /renew, 793
- IPLS, 746
- IP-PBX, 668, 672
- IPsec, 266, 687, 698, 699, 723, 743
  - AH, 699
  - ESP, 700, 701
  - IKE, 700
  - tryby pracy, 699
  - tunelowanie, 754
- Ipseccmd, 799
- IPv4, 485, 487
  - adres, 487
  - adresowanie, 488
  - adresowanie statyczne, 507
  - adresowanie zero configuration, 495
  - adresy zarezerwowane, 493
  - CIDR, 490
  - klasy adresów, 489
  - maska podsieci, 504
  - nagłówek IP, 496
  - NAT, 494, 498
  - numery protokołów, 499
  - opcje protokołu IP, 498
  - podsieci, 504
  - podział przestrzeni nazw, 489
  - prefiksy bloków CIDR, 491
  - protokoły, 499
  - przestrzeń adresowa, 488
  - regionalni administratorzy numerów IP, 492
  - routing, 487, 488
  - rozszerzenia adresowania, 488
  - VLSM, 490
- IPv4 Link-Local, 495
- IPv4LL, 495
- IPv6, 485, 514
  - adresowanie, 516
  - automatyczna konfiguracja adresów, 515

IPv6  
  CIDR, 516  
  datagramy, 523  
  nagłówki, 515, 523  
  ND, 515, 524  
  podsieci, 516  
  przestrzeń adresowa, 485  
  zakresy adresów, 520, 522  
IPv6 Neighbor Discovery, 524  
IPX, 77  
IPX/SPX, 170  
ipxroute, 799  
IQN, 435  
IRC, 273  
IRDA, 325  
irftp, 799  
ISA, 170, 466, 695  
ISA Server, 170, 564, 748  
ISCAMP, 700  
iSCSI, 433, 435  
  CDB, 435  
  inicjator, 435  
  konwencje nazw, 435  
  LUN, 436  
  polecenia SCSI, 435  
  urządzenia HBA, 436  
  uwierzytelnianie, 435  
iSCSI HBA, 446  
ISDN, 206, 256, 341, 542, 667  
  dostęp do Internetu, 341  
  dostęp przez sieć B-ISDN, 342  
  kanały B, 342  
  kanały H, 342  
  pierwotny PRI, 342  
  podstawowy BRI, 342  
  rodzaje dostępu, 342  
  TA, 341  
  terminal adapter, 341  
  urządzenia, 341  
ISDN-BRI, 256  
ISDN-PRI, 256  
ISEB, 137  
ISI, 380  
IS-IS, 221, 225, 227, 229  
ISM, 368  
ISM-C, 371  
iSNS, 439  
ISO, 43, 45  
ISP, 486  
iStumbler, 401  
IT Service Management Forum International, 137  
ITIL, 135  
  certyfikaty, 137  
  części, 135  
  lista zespołów, 136  
ITIL Certification Management Board, 137  
itSMF, 137  
ITU, 196, 679  
iTunes, 644  
ITU-R, 45  
ITU-T, 45, 347, 763

iWARP, 450, 451  
IX, 361  
IXP, 336, 361, 362  
izolacja, 168  
izolacja aplikacji, 160  
izolacja fizyczna, 168  
izolacja protokołów, 170

## **J**

jakość usługi, 124  
  ABR, 125  
  CBR, 125  
  klasy usług ATM, 125  
  NRT-VBR, 125  
  QoS, 124  
  RT-VBR, 125  
  UBR, 125  
  umowy dotyczące jakości usług, 125  
Java 2 Enterprise Edition, 80  
Java EE, 623  
Java RMI, 79  
Java Telephony API, 666  
java.net.NetworkInterface, 159  
java.nio.channels.FileChannel, 448  
JavaScript, 792  
JDBC, 586  
jeden do dowolnego, 76  
jeden do jednego, 76  
jeden do wielu, 76  
jeden do wszystkich, 76  
jednokrotne logowanie, 574  
jednostka danych protokołu, 49  
jednostka danych usługi, 49  
jednostka dostępowa dla wielu stacji, 77  
jednostka MAU, 311  
jednostka organizacyjna, 577  
język HTML, 611  
język SMIL, 654  
język UML, 79  
język WSDA, 620  
język zapytań WQL, 101  
JMX, 764  
JNDI, 586  
JTAPI, 666  
JUNOS, 552

## **K**

kabel odgałęziający, 39  
kable, 177  
  kable koncentryczne, 177, 182  
  kable optyczne, 187  
  kable światłowodowe, 60, 192  
  kable współosiowe, 177, 182, 183  
  STP, 182  
  USB, 284  
  UTP, 181  
kalkulatory IPv6, 518  
kamery internetowe, 681

kamery sieciowe, 681  
kampusowa sieć komputerowa, 336  
kanał bezszumowy, 114  
kanał kablowy, 180  
kanał MIMO, 118  
kanał wirtualny, 115  
kanały, 346  
kanały komunikacyjne, 49  
kanały rozgłoszeniowe, 298  
karta PC, 171  
karta PCMCIA, 171  
karta sieciowa, 157, 158, 172  
    adres MAC, 161  
    magistrale komunikacyjne, 170  
katalog, 568  
kategorie CAT, 185  
kategorie usług ATM, 126  
kategoryzacja sieci, 30  
Kazaa, 78  
KDC, 714  
Kerberos, 599, 688, 712  
    bilety, 714  
    centrum dystrybucji kluczy, 714  
    infrastruktura, 713  
    KDC, 714  
    Public Key Protocol, 714  
    Symmetric Key Protocol, 714  
    szyfrowanie, 714  
    uwierzytelnianie, 712  
KEY, 543  
Key Distribution Center, 714  
keystream, 709  
Kismet, 401  
klastry sieciowe, 453  
    odporność na uszkodzenia, 453  
    poziom wykorzystania, 453  
    równoważenie obciążenia, 455  
    Stratus Lockstep, 455  
    systemy przetwarzania sieciowego, 457  
klasy adresów IPv4, 489  
klasy sieci Fibre Channel, 425  
klasy usług ATM, 125  
klient, 79  
klient DHCP, 508  
klient poczty, 639  
klient VPN, 750  
klient-serwer, 60, 78, 79  
kluczowanie amplitudy, 193  
kluczowanie częstotliwości, 193  
kluczowanie fazy, 193  
kluczowanie kodem komplementarnym, 373  
kod Manchester, 313  
kod Morse'a, 107  
kodek, 115  
kodowanie, 199, 655  
    Base64, 633  
    CBR, 656, 657  
    Manchester, 313  
    MBR, 656  
    VBR, 656, 657

kody stanów HTTP, 616  
kolejkowanie żądań, 146  
kolejność dostawców, 167  
kolejność powiązań, 165  
kolizje, 72, 209, 299, 308  
komórki, 32, 357, 358  
komunikacja, 59  
komunikacja między warstwami, 46  
komunikacja P2P, 272  
komunikacja punkt-punkt, 31, 61  
    poprawność połączenia, 32  
komunikacja rozgłoszeniowa, 32  
komunikacja simpleksowa, 49  
komunikatory, 666  
komunikaty, 69  
    ICMP, 70  
    pakietyzacja, 69  
    XON/XOFF, 120  
koncentrator, 37, 75, 209, 210, 282, 315  
    koncentrator aktywny, 210  
    koncentrator pasywny, 209  
koncepcja BCV, 411  
konferencje wideo, 680  
konfiguracja  
    interfejs sieciowy, 162  
    router bezprzewodowy, 391  
konfigurowalne optyczne multipleksery dołączająco-  
    odłączające, 118  
konie trojańskie, 693  
konsola SMC, 580  
konsola zarządzania, 97  
konsolidacja serwerów, 154  
kontrola błędów, 304  
kontrola dostępu, 121  
kontrola dostępu bazująca na roli, 580  
kontrola dostępu do medium, 40  
kontrola przeciążenia sieci, 473  
kontrola przeciążeń przez zmianę szybkości, 121  
kontrola przepływu TCP, 473  
kontrola przepływu w sieci Fibre Channel, 429  
kontroler PLC, 327  
konwersja DAC, 671  
konwerter Ethernet-PNA, 259  
korekcja błędów, 265  
korelacja zdarzeń, 767  
koszt trasy, 221  
krosownica, 35  
kryptografia, 705  
ksh, 791, 799  
kształtowanie ruchu, 121, 358  
    dławienie przepływności, 122  
    polityka ruchu, 122  
    sieć IP, 122

## L

L2F, 756  
L2TP, 756, 830  
    pakiety, 756  
L2TP Access Concentrator, 756  
L2TP over IPsec, 743, 748

- LA CNIC, 492
- Label Edge Router, 360
- LAC, 756
- LAMP, 560
- LAN, 27, 30, 293
- LAN Access Profile, 290
- LANcity, 257
- LANTastic, 550
- LAP, 290
- LAPS, 350
- laptop XO, 394
- lasery półprzewodnikowe, 193
- LAST-ACK, 470
- LastFM, 644
- Layer 2 Tunneling Protocol, 756
- LBA, 412
- LBM, 604
- LC, 194
- LDAP, 528, 544, 567, 582, 584, 585
  - atrybuty, 586
  - CN, 585
  - DN, 585
  - drzewo katalogu, 586
  - LDIF, 584
  - nazwa wyróżniająca, 586
  - RDN, 586
  - serwer, 584
  - usługi katalogowe, 584
  - węzły, 586
  - wpisy, 586
- LDAP Data Interchange Format, 584
- LDIF, 584
- LED, 193, 348
- lekka licencja, 372
- Lemarr Hedy, 119
- LER, 360
- LIB, 360
- liczba połączeń punkt-punkt, 34
- liczenie do nieskończoności, 224
- liczniki wydajności, 779
- Lightweight Directory Access Protocol, 528
- LILO, 146
- LimeWire, 274
- linia transmisyjna z kablami współosiowymi, 184
- linie telefoniczne, 259
- liniowy łańcuch, 40
- Link Local Address, 520
- Link State Advertisement, 226, 227
- Linux, 559
  - dystrybucje systemu, 560
- Linux Standard Base, 561
- lista przeglądania, 87
- listy ACL, 572, 599
- Live HTTP Headers, 613
- LiveMeeting, 832
- LLA, 520
- LLC, 174, 296, 305
- LMHOSTS, 85, 93, 535
- LNP, 679
- Local Area Network, 293
- Local Browse Manager, 604
- Local Number Portability, 679
- Lockstep, 454
- lodctr, 799
- Logical Block Address, 412
- Logical Link Control, 174, 305
- Logical Unit Identifier, 412
- Logical Volume Manager, 424
- logiczna gwiazda, 41
- logiczna siatka, 42
- logiczne interfejsy sieciowe, 159
- logiczny łańcuch, 40
- logman, 799
- LogMeIn Hamachi, 748
- logo Wi-Fi, 367
- lokalne ściemnianie, 322
- lokalny bufor DNS, 538
- LonTalk, 330
- LonWorks, 325
- loopback, 530
- Lotus Domino, 638
- lpq, 799
- lpr, 800
- LSA, 226, 227
- LSB, 561
- LSR, 360
- LT, 305
- luki w zabezpieczeniach, 688, 691
- LUN, 412, 436
- LVM, 413, 424

**Ł**

- łamanie szyfrów, 706
- łańcuch Markowa, 151
- łącza, 64
  - DSL, 256
  - E, 346, 347
  - ISDN, 256
  - łącza mikrofalowe, 202
  - łącza radiowe, 201
  - łącza satelitarne, 257
  - łącza szkieletowe, 31, 34
  - łącza trunkowe, 34
  - PRI, 256
  - T, 346, 347
  - VPN, 743
  - WDM, 118
  - łącza zbiorcze, 34
- łącza o dużej szybkości, 31, 441
  - 10GBase-T, 445
- Gigabitowy Ethernet, 443
- klastry sieciowe, 453
- TOE, 445
- Zero Copy Network, 448
- łączenie segmentów sieci, 212
- łączenie sieci, 77
- łączność bezprzewodowa, 196

**M**

- M2M VPN, 746
- MAC, 40, 59, 61, 71, 89, 161, 174, 266, 298, 304, 703, 711
- Mac OS X, 553
- macierz RAID, 421
- MAE, 361
- magistrala, 33, 34, 70
  - domena kolizyjna, 72
  - kolizje, 72
  - segmenty, 71
  - unikanie kolizji, 73
  - wykrywanie kolizji, 73
  - wyłumianie sygnału, 74
- magistrala komputerowa, 281
- magistrala liniowa, 34
- magistrala rozproszona, 35
- magistrale komunikacyjne kart sieciowych, 170
- Mail Delivery Agent, 626
- Mail Exchange, 541, 542
- Mail Group, 543
- Mail Submission Agent, 626
- Mail Transfer Agent, 626, 638
- Mail User Agent, 626, 639
- Mail2Web, 637
- Mailbox, 543
- Mailbox Information, 543
- maksymalna częstotliwość sygnału, 112
- maksymalna przepustowość zaszumionego kanału, 114
- MAN, 31, 164
- Managed Beans, 764
- Managed Service Provider, 787
- Management Information Base, 90
- MANET, 226, 393
- man-in-the-middle, 481, 693, 712
- mapa sieci, 86, 102
  - narzędzia aktywnego rozpoznawania elementów sieciowych, 103
  - oprogramowanie, 103
  - techniki sporządzania map sieci, 103
- maska podsieci, 504
- maskowanie podsieci, 489
- master-slave, 120
- MAU, 77, 311
- Maximum Segment Size, 473
- Maximum Transmission Unit, 468, 473
- MB, 543
- MBeans, 764
- MBR, 656
- MBSA, 689
- MCR, 125
- MCU, 677
- MD4, 711
- MD5, 711
- MDA, 626
- MDI, 186, 305
- MDI-X, 186
- mDNS, 495
- mechanizm drogowaskazu, 314
- mechanizm Failover, 723
- mechanizm kontroli dostępu, 122
- mechanizm PXE, 174
- mechanizm skakania po częstotliwościach, 119
- mechanizm sterowania przepływem, 52
- mechanizm TCP offload, 158
- mechanizm zbierania informacji o sieci, 85
- Media Access Control, 40, 174
- Media Gateway Control, 669
- Media Gateway Control Protocol, 678
- Medium Access Control, 266, 304
- Medium Dependent Interface, 186
- medium transmisyjne, 28, 51, 106, 177
  - ekranowanie, 180
  - kable, 177
    - kable koncentryczne, 177, 182
    - kable optyczne, 187
    - kable współosiowe, 177, 182
  - oznaczenia przewodów ethernetowych
    - w standardach TIA/EIA, 185
  - przygotowanie okablowania, 178
  - skrętka, 180
  - skrętka ekranowana, 177
  - skrętka nieekranowana, 178, 181
  - standardy łączenia przewodów, 185
  - światłowody, 187
  - układanie kabli sieciowych, 179
  - włókno optyczne, 178
- Memory Management Unit, 448
- mesh computing, 442
- mesh network, 432
- Mesh Point, 394
- Message Authentication Code, 703, 711
- messages, 766
- metadane, 47
- Metcalfe Rober, 34
- metoda wielościeżkowa, 299
- metody HTTP, 615
- Metropolitan Area Exchanges, 361
- Metropolitan Area Network, 31
- metryki przepustowości, 141
- MG, 543
- MGCP, 672, 675, 676, 678
- MIB, 90, 96, 98
  - ASN.1, 99
- Microsoft .NET Framework, 160
- Microsoft Active Directory, 587
- Microsoft Baseline Security Analyzer, 689
- Microsoft Deployment Toolkit, 773, 775
- Microsoft Exchange, 638
- Microsoft File Replication Service, 607
- Microsoft Home Server, 268
- Microsoft Internet Security and Acceleration, 695
- Microsoft Live Meeting, 832
- Microsoft Management Console, 785
- Microsoft Network Monitor, 782
- Microsoft Operations Framework, 137
- Microsoft Remote Procedure Call, 602
- Microsoft Response Point, 669
- Microsoft Security Account Manager, 587
- Microsoft Server, 564
- Microsoft Small Business Server, 571

- Microsoft Solution Accelerator for Business Desktop Deployment 2007, 138
- Microsoft Solutions Framework, 137
- Microsoft System Center Operations Manager, 777
- Microsoft Windows Media Player, 661
- Międzynarodowa Organizacja Normalizacyjna, 45
- Międzynarodowa Unia Telekomunikacyjna, 45
- miękki podział na strefy, 432
- MIIS, 582
- mii-tool, 800
- mikrofale, 202
- MIME, 612, 629, 631, 632
- MIMO, 118, 371, 398
- MINFO, 543
- minimalna szybkość przesyłania komórek, 125
- Minimum Cell Rate, 125
- MiniStumbler, 400
- MIPS, 141
- MISTP, 242
- MITRE, 690
- mkdir, 800
- MMC, 766, 770, 785
- MMU, 448
- Mobile Ad hoc Network, 226
- Mobile VoIP, 680
- mod, 190
- Modbus, 294, 327, 328
  - ADU, 329
  - implementacja standardu, 328
  - PDU, 329
  - ramki, 329
  - transmisja danych, 329
  - typy danych, 330
- Modbus +, 328
- Modbus ASCII, 328
- Modbus RTU, 328
- Modbus/TCP, 328
- model ACID, 81
- model internetowy, 43
- model jednostek równorzędnych, 273
- model łączenia systemów otwartych, 45
- model Markowa, 151, 152, 153
- model operacyjny serwera sieciowego, 132
- model OSI, 45, 56
  - komunikacja między poszczególnymi warstwami, 49
  - protokoły, 48
  - protokoły warstwy n, 48
  - transport danych, 47
  - urządzenia sieciowe, 48
  - usługi, 49
  - warstwa aplikacji, 54
  - warstwa fizyczna, 50
  - warstwa łącza danych, 51
  - warstwa prezentacji, 54
  - warstwa sesji, 53
  - warstwa sieciowa, 52
  - warstwa transportowa, 53
  - warstwy, 46, 49
- model SNIA, 414
- model sterowników Windows, 101
- model TCP/IP, 43, 49, 55, 56, 61
  - IP, 55
  - TCP, 55
  - UDP, 55
  - warstwa dostępu do sieci, 55
  - warstwa transportowa, 55
  - warstwy, 55
- model współdzielonej sieci pamięci masowej, 414
  - agregacja, 421
  - domena pamięci masowej, 420
  - modele urządzeń, 422
  - serwery zorientowane plikowo, 423
  - taśmy, 415
  - warstwa aplikacji/systemu operacyjnego, 422
  - warstwa bloku/urządzenia pamięci masowej, 422
  - warstwa pliku/bloku, 422
  - warstwa systemu operacyjnego/pliku i rekordu, 422
- model żądanie-odpowiedź, 146
- modelowanie sieci, 151
- modem, 119
  - modem ADSL, 343
  - modem kablowy, 257
- modulacja
  - AM, 199
  - BPSK, 374
  - CAP, 343, 344
  - CCK, 373
  - DMT, 343, 344
  - DSSS, 375
  - FM, 199
  - modulacja amplitudy, 110, 199
  - modulacja amplitudy impulsu, 115
  - modulacja częstotliwości, 110, 199
  - modulacja delta, 117
  - modulacja fazy, 110
  - modulacja impulsowa, 199
  - modulacja impulsowo-kodowa, 115
  - modulacja intensywności światła, 193
  - modulacja polaryzacji, 193
  - modulacja położenia impulsu, 115
  - modulacja szerokości impulsu, 115
  - OFDM, 265, 379
  - PM, 199
  - PSK, 373
  - QAM, 343
  - QPSK, 374, 375
  - ROBO, 265
- moduł interfejsu sieciowego, 158
- moduł NIU, 158
- moduły kształtowania ruchu, 122
- modyfikacja adresu MAC, 89
- MOF, 137
- monitor aktywny, 313
- Monitor niezawodności i wydajności, 781
- Monitor wydajności, 779
- monitorowanie zasobów, 143
- Morpheus, 274
- most, 211, 212, 386, 388
  - adaptacyjne przełączanie, 213
  - cechy, 214

mostkowanie na podstawie trasy źródłowej, 213  
 programowy most sieciowy, 214  
 sieć Token Ring, 213  
 STP, 213  
 most bezprzewodowy, 388  
 mostkowanie, 215  
 mostkowanie na podstawie trasy źródłowej, 213  
 mount, 800  
 mountvol, 800  
 move, 800  
 MPLS, 206, 355, 360, 742  
     etykiety, 360  
     LER, 360  
     LIB, 360  
     LSR, 360  
 MPPE, 755  
 MR, 543  
 mrowie, 278  
 MSA, 626  
 MS-CHAP, 755  
 MSF, 137  
     zasady, 139  
 MSP, 787  
 MSRPC, 602  
 MSS, 473  
 MSTP, 242  
 MTA, 626, 638  
 MTU, 468, 473  
 MUA, 626, 639  
 Multi Protocol Label Switching, 360  
 multicast, 59, 76, 219, 485  
 Multicast DNS/DNS-SD, 495  
 multicasting, 32  
 multiemisja, 32, 76, 219, 485, 487, 648  
 Multihomed, 486  
 multimedia, 643  
 multipath, 299  
 Multiple Access Unit, 311  
 Multiple Bit Rate, 656  
 Multiple Instances Spanning Tree Protocol, 242  
 Multiple Spanning Tree Protocol, 242  
 Multiple-Input Multiple-Output, 398  
 multipleksacja, 105, 115, 474  
     FDM, 117  
     multipleksacja z podziałem czasu, 115, 116  
     multipleksacja z podziałem częstotliwości, 116, 117  
     multipleksacja z podziałem długości fali, 117, 118  
     proces, 115  
     WDM, 117, 118  
 multiplekser, 115  
 multiplekser ADM, 118  
 multiplekser dołączająco-odłączający, 118  
 Multistation Access Unit, 37, 77  
 MUX, 115  
 mv, 800  
 MVA, 151  
 MX, 541, 542, 626, 627

## N

NIGE, 459  
 NAA, 435  
 nadmiarowość, 159  
 nagłówek ICMP, 511  
 nagłówek IP, 496  
 nagłówek IPv6, 515, 523  
 nagłówek RTP, 652  
 najlepszy z możliwych, 66  
 NAK, 381  
 Name Server, 541  
 NAP, 361, 687, 696, 697, 725  
 Napster, 276  
 NAPT, 734  
 NAPTR, 839  
 narrowcasting, 648  
 NAS, 407, 410, 424, 593, 594, 597, 598  
     elementy, 595  
     filer, 595  
     FreeNAS, 595  
     implementacja, 594  
     system operacyjny, 595  
     urządzenia, 595  
     Windows Storage Server 2003 R2, 596  
 NAS Head, 411, 424  
 NAT, 170, 212, 253, 494, 498, 515, 676, 717, 719, 732  
     oprogramowanie, 733  
     schematy mapowania, 734  
     trwałe przypisanie mapowania, 734  
 National LambdaRail, 363  
 National Science Foundation, 361  
 National Vulnerability Database, 690  
 NAT-PMP, 735  
 nazwa wyróżniająca, 586  
     Active Directory, 587  
 nazwy, 527  
 nazwy interfejsów sieciowych, 160  
 nazwy NetBIOS, 534  
 NBF/IPX, 272  
 NBMA, 37  
 NBNS, 603, 604  
 NBT, 89, 602  
 nbstat, 801  
 NCP, 599  
 ND, 515, 524  
 NDIS, 174  
 NDMP, 420  
 NDP, 506  
 Near End Crosstalk, 181  
 negocjacja, 50  
 negocjowanie parametrów wzajemnego połączenia, 119  
 Neighbor Discovery, 486  
 NetApp, 424, 595  
 NetApp Fabric Attached Storage, 595  
 NetBEUI, 86, 170  
 NetBIOS, 85, 89, 93, 272, 527, 534  
     nazwy, 534  
     określanie nazw, 535  
 NetBIOS Name Server, 603

NetBIOS over TCP/IP, 89  
 NETCONF, 764  
 Netcraft, 559  
 NetMeeting, 832  
 netsh, 401, 808  
 NetShell, 807  
     polecenia, 808, 809  
 netstat, 557, 801  
 NetStumbler, 400, 401  
 NetWare, 30, 31, 550, 553  
 NetWare 4, 550  
 NetWare Core Protocol, 599  
 NetWare Loadable Modules, 564  
 Network Access Point, 361  
 Network Access Policy, 725  
 Network Access Protection, 687, 697  
 Network Address Port Translation, 734  
 Network Address Translation, 170, 212, 253, 676, 717  
 Network Attached Storage, 407, 410, 423, 594  
 Network Basic Input/Output System, 534  
 Network Data Management Protocol, 420  
 Network File System, 599  
 Network Information Service, 544, 583  
 Network Interface Card, 158  
 Network Interface Unit, 158  
 Network Location Awareness, 687, 696, 697  
 Network Management Systems, 782  
 Network Monitor, 782  
 Network Operating System, 549, 566  
 Network Stumbler, 400  
 Next, 543  
 NEXT, 181  
 NFS, 562, 593, 595, 599  
     implementacja, 599  
     instalacja, 600  
     usługa zdalnego wywoływania procedur, 600  
 NIC, 158  
 Nicecast, 657  
 nierozgłoszeniowe sieci wielodostępne, 37  
 nieustalona przepustowość, 125  
 niezarządzalny przełącznik, 214  
 niezawodna usługa pakietowa, 70  
 niezawodność, 142  
 NIS, 583  
     klient, 583  
     serwer główny, 583  
     serwer zapasowy, 583  
 N-ISDN, 342  
 NIU, 158  
 NLA, 687, 696  
 NLM, 564  
 NLR, 363  
 NLSP, 227  
 nmbd, 92  
 nmdb, 603  
 NMS, 782  
 NNI, 357  
 non-broadcast multi-access, 37  
 Non-Real Time Variable Bit Rate, 125  
 notacja skompresowana IPv6, 517  
 Novell eDirectory, 585

Novell NetWare, 550, 563  
 NPS, 830  
 NRT-VBR, 125  
 NS, 541  
 NSF, 361  
 nslookup, 801  
 Nullsoft SHOUTcast, 659  
 NUMA, 551  
 numery protokołów, 499  
 NVD, 691  
 NX, 832  
 NX Technology, 832  
 NXT, 543  
 Nyquist Harry, 113

## O

OASIS, 621  
 obiekty OID, 99  
 obiekty sieciowe, 96  
 obliczenia „w chmurach”, 459  
 obraz taśmy, 415  
 obsługa żądania HTTP, 145  
 obszarowe punkty dostępu, 361  
 obszary ataków, 692  
 obwód, 94, 207, 338  
 obwód transmisyjny, 338  
 obwód wirtualny, 95  
 OC-12, 352  
 OC-192, 352  
 ochrona przed zagrożeniem, 694  
 ODBC, 586  
 ODI, 174  
 ODM, 346  
 odmowa usług, 692  
 odporność na awarie, 37, 168, 453, 723  
 odpowiedź, 50  
 odpytywanie, 88, 93  
 odstęp IFG, 309  
 odświeżanie ustawień DHCP, 793  
 odtwarzacze multimedialnych, 661  
 odwrotne proxy, 738  
 odwzorowanie adresu, 93  
 OES, 563  
 OES 2, 564  
 OFDM, 265, 379  
 OGC, 135, 137  
 ogłoszenie o stanie łącza, 226  
 ogólny algorytm wyznaczania szybkości komórek, 121  
 OID, 99  
 OidView Professional, 99  
 okablowanie, 177  
     sieć Ethernet, 184  
 oktawy, 198  
 oktet, 304  
 OLE for Process Control, 294  
 OLPC, 393  
 OLPC XS, 394  
 OLTP, 141  
 OmniPeek, 782  
 One Laptop Per Child, 393

OOB, 474  
OPC, 294, 331, 332  
    sieć, 332  
OPC Alarm & Events, 331  
OPC Batch, 331  
OPC Commands, 331  
OPC Complex Data, 331  
OPC Data Access, 331  
OPC Data eXchange, 331  
OPC Foundation, 331  
OPC Historical Data Access, 331  
OPC Security, 331  
OPC Unified Architecture, 331  
OPC XML-DA, 331  
OPC-AE, 331  
OPC-DA, 331  
OPC-HDA, 331  
opcje protokołu IP, 498  
OPC-UA, 332  
OPEN, 472  
Open Enterprise Server, 553, 563  
Open Shortest Fast First, 221  
Open System Interconnection, 43, 45  
OpenDS, 584  
OpenRADIUS, 837  
OpenVPN, 553, 747  
OPER, 532  
opóźnienie przekazywania, 237  
opóźnienie w dostarczaniu komórek, 125  
oprogramowanie do zarządzania konfiguracją, 761  
oprogramowanie do zarządzania usterkami, 761  
oprogramowanie komunikacyjne, 28  
oprogramowanie warstwy aplikacji, 54  
oprogramowanie wspierające sieci bezprzewodowe, 399  
oprzyrządowanie do zarządzania systemem Windows, 101  
OPTIONS, 615  
optymalizacja tras, 75  
OQPSK, 375  
Oracle, 131, 561  
Oracle Directory Server Service Plus, 584  
organizacje standaryzacyjne, 44, 45  
Organizational Unit, 577, 585, 586, 587  
Orthogonal Frequency Division Multiplexing, 265, 379  
ortogonalna multipleksacja w dziedzinie częstotliwości, 265  
OS/2, 550  
OSI, 43, 45  
osobista sieć LAN, 27, 271  
osobista zaporą sieciowa, 720  
OSPF, 221, 225, 227  
    grupy obszarów, 228  
    LSA, 227  
    pakiety, 228  
    powiadomienia o stanie łącza, 227  
    router wyznaczony, 227  
    sieć szkieletowa, 228  
    system autonomiczny, 227  
OU, 579, 585, 586, 587  
OUI, 432

out-of-band, 474  
oznaczenia przewodów ethernetowych  
w standardach TIA/EIA, 185

## P

P2MP, 259  
P2P, 77, 271, 272  
Packet over SONET/SDH, 353  
PacketTrap, 103  
PAD, 306, 356  
PAE, 402  
Pakiet projektowania usług, 135  
pakiety, 46, 69, 354  
    L2TP, 756  
    pakiet rozgłoszeniowy, 32  
    PoS, 353  
    PTTP, 756  
    RTCP, 654  
    RTP, 652, 653  
    TCP, 465  
PAM, 115, 186, 835  
pamięć masowa, 409  
PAN, 30, 290  
panel krosowy, 178, 179  
PAR, 470  
paradoks Braessa, 219, 220  
Parallel Stack Offload, 446  
parametry medium transmisyjnego, 106  
pasywna gwiazda, 195  
PAT, 734  
patch panel, 178  
path vector, 229, 362  
pathping, 802  
PBX, 665, 667  
    Asterisk, 668  
    CUCM, 669  
    Microsoft Response Point, 669  
    telefon wewnętrzny, 667  
PCF, 381  
PCI, 170  
PCI Express, 172  
PCI-E, 172  
PCI-X, 170, 171, 172  
PCM, 115  
PCMCIA, 171  
PCR, 125  
PCS, 187, 267, 324, 445  
PCSM, 381  
PD, 262  
PDA, 463  
PDU, 49, 329, 652  
Peak Cell Rate, 125  
peer-to-peer, 27, 30, 60, 64, 77, 253, 271  
pełny dwupłask, 49  
perfmon, 802  
Personal Area Networking, 290  
Personal Data Assistant, 463  
personal LAN, 27  
Per-VLAN Spanning Tree, 242

- pętla arbitrażowa, 410, 430
- PFLOPS, 455
- Phase Shift Keying, 365, 373
- phishing, 641
- phpsh, 792
- PHY, 445
- Physical Carrier Sense, 267
- Physical Carrier Sense Method, 381
- Physical Coding Sublayer, 445
- Physical Layer Convergence Protocol, 380
- Physical Medium Dependent, 381
- Physical Medium Dependent Layer, 445
- pięścić, 33, 37, 77, 195, 311
- pierwotny PRI, 342
- pikosieć, 288
- ping, 70, 71, 102, 140, 159, 465, 792, 793, 802
- PKI, 702
- Plain Old Telephone Service, 667
- pLAN, 27, 30, 271, 282
- planowanie pojemności systemu, 133
- Plastic-Clad Silica, 187
- platforma .NET, 459
- platforma zarządzania siecią, 783
- platformy sieciowych systemów operacyjnych, 553
- PLC, 319, 326, 327
- PLCP, 380
- PLEN, 532
- pliki
  - HOSTS, 85, 93, 528
  - LMHOSTS, 85, 93, 535
  - MIB, 99
  - SMIL, 648, 654
  - TORRENT, 277
- plaszcz, 191
- PM, 199
- PMD, 381
- PMDL, 445
- PNA, 259
- PnP, 173
- pobieranie progresywne, 643, 644, 645, 647
- poczta elektroniczna, 625
  - DNS, 627
  - filtrowanie spamu, 641
  - generowanie MIME, 634
  - IMAP, 625, 637
  - klient poczty, 639
  - klient poczty Webmail, 637
  - kodowanie Base64, 633
  - konfiguracja klienta poczty, 639
  - MIME, 629, 631
  - MSA, 626
  - MTA, 626, 638
  - MUA, 626, 639
  - MX, 627
  - nagłówki wiadomości e-mail, 628
  - numery portów, 627
  - POP3, 625, 626
  - protokoły, 626
  - push e-mail, 628
  - routing poczty, 627
  - sendmail, 639
  - serwer poczty, 638
  - SMTP, 625, 626, 630
  - wiadomości w częściach, 628
  - wiadomość e-mail, 625
  - wysyłanie wiadomości e-mail, 626
  - X.400, 628
- Podgląd zdarzeń, 765
- podpis cyfrowy, 712
- podsieci, 504, 695
  - IPv6, 516
- podstawowy BRI, 342
- podstawowy system wejścia-wyjścia sieci, 534
- podwarstwa sterowania dostępem do medium, 174
- podwarstwa sterowania łączem logicznym, 174
- podział czasu, 67
- podział na strefy nazw, 433
- podział na strefy portów, 433
- podziela sygnału na składowe, 108
- PoE, 262
  - IEEE, 262
- Point Coordination Function, 381
- Pointer, 541, 543
- point-to-point connection, 409
- Point-to-Point Protocol, 755
- Point-to-Point Tunneling Protocol, 755
- pojemność serwera sieciowego, 133
- pojemność systemu, 106
- polaryzacja sygnału, 118
- polecenia powłoki NetShell, 809, 817
- polecenia sieciowe, 790, 795
- polityka bezpieczeństwa, 696
- polityka ruchu, 122
- polityka zarządzania cyklem życia informacji, 413
- połączenia, 94, 95, 106, 207, 472
  - Bluetooth, 30, 289
  - HomePlug, 265
  - InfiniBand, 452
  - połączenia asymetryczne, 256
  - połączenia bezprzewodowe, 201, 257, 384
  - połączenia bezstanowe, 66, 95, 96
  - połączenia kablowe, 177
  - połączenia równorzędne, 27
  - połączenia stałe, 258
  - połączenia stanowe, 66, 95
  - połączenia szerokopasmowe, 253, 256
  - połączenia światłowodowe, 257
  - połączenia trwałe, 94, 95
  - połączenia tymczasowe, 65, 94, 95
  - połączenia typu T, 194
  - PPP, 74
  - SONET/SDH, 349
  - TCP, 464, 469
  - UTP, 180
  - VPN, 95, 749
  - WDS, 389
- połączenia przełączane, 67
  - dostęp do obwodu, 68
  - dostęp negocjowany, 67
  - negocjowanie dostępu do sieci, 68

- podział czasu, 67
- symulowanie przełączanych połączeń, 68
- tabela stanów, 68
- połączenia punkt-punkt, 35, 61
  - fizyczne połączenia punkt-punkt, 63
  - połączenia bezstanowe, 66
  - połączenia przełączane, 67
  - połączenia stanowe, 66
  - połączenia tymczasowe, 65, 66
  - przełączanie pakietów, 65
  - stan połączenia, 62
  - szybkość transmisji, 63
  - tabela stanów, 63
  - wirtualne interfejsy sieciowe, 64
  - wirtualne połączenia punkt-punkt, 64
- POP, 55
- POP3, 466, 625, 626, 636
  - identyfikacja wiadomości, 636
  - UIDL, 636
  - żądanie poczty, 636
- poprawność połączenia w komunikacji punkt-punkt, 32
- Port Access Entity, 402
- Port Address Translation, 734
- port główny, 234
- port MDI, 186
- port MDI-X, 187
- port mirroring, 211
- Port Restricted Cone NAT, 734
- port uplink, 39, 210
- port wyznaczony, 234
- porty, 477
  - porty dynamiczne, 477
  - porty prywatne, 477
  - porty przypisane na stałe, 477
  - porty TCP, 466
  - porty ulotne, 477
  - porty zarejestrowane, 477
- Pos, 353
- Positive Acknowledgement with Retransmission, 470
- POSIX, 556
- POSIX.1, 558
- POST, 615
- Post Office Protocol, 55, 636
- Post Office Protocol 3, 466
- potoki, 282
- POTS, 339, 667
- potwierdzenie, 50, 53
- potwierdzenie skumulowane, 470
- Power over Ethernet, 251, 262
- PoweredUSB, 282
- PowerShell, 791, 815
  - cmdlet, 816, 817
  - get-process, 825
  - get-psprovider, 816
  - get-service, 825
  - get-service-computername, 825
  - get-wmiobject, 826
  - set-location, 825
  - uruchamianie powłoki, 816
- PowerShell Drive, 825
- powłoka poleceń, 790
- powłoka sieciowa, 807
- powódz pakietów SYN, 729
- poziom usługi, 124, 139
- poziom zwrotu z inwestycji, 153
- poziomy ostrożnościowe stopnia
  - wykorzystania zasobu, 149
- półdupleks, 49, 53
- PPM, 115
- PPP, 74, 509, 755, 829
- PPPoE, 829
- PPTP, 748, 755, 830
- prawo Metcalfa, 34
- prawo Plancka, 111
- PRE, 305
- preambuła PRE, 305
- prefiksy bloków CIDR, 491
- PRI, 256, 342
- Primary Domain Controller, 573, 590
- Primary Rate Interface, 342
- print, 802
- Private Branch Exchange, 667
- Privoxy, 244
- problem przepływu danych, 119
- proces enkapsulacji, 47
- proces multipleksacji, 115
- proces negocjacji, 50
- proces standaryzowania technologii, 44
- Process Control System, 324
- profile Bluetooth, 290
- Programmable Logic Controller, 319
- programowa kontrola przepływu, 120
- programy automatyki domowej, 323
- projekt GNU, 560
- projekt rozbudowy sieci, 153
- projekt SETI, 458
- projektowanie sieci, 59, 94
- Projektowanie usług, 135
- promieniowanie elektromagnetyczne, 196, 198
- propagacja fal, 198
- prośba o komentarze, 44
- prośba o propozycje, 44
- Protocol Data Unit, 49, 652
- protokoły, 46, 48, 55, 497
  - 802.11, 380
  - AODV, 226, 394
  - ARP, 61, 93, 524, 531
  - BACnet, 330
  - BGP, 221, 231, 362, 486
  - BitTorrent, 277
  - BOOTP, 86, 510
  - CBP, 372
  - CMIP, 763
  - CSMA/CD, 307
  - DAAP, 474
  - DDP, 451
  - DHCP, 508
  - Diameter, 838
  - DNS, 527
  - DSDV, 394
  - EGP, 221
  - ESMTP, 631

## protokoły

- FCP, 410, 414, 425, 428
- FLOGI, 431
- GRE, 754
- H.323, 677
- HTTP, 96, 611, 612
- HTTPS, 619, 696, 703
- HWMP, 394
- IAX, 677
- ICMP, 511, 524
- ICMPv6, 525
- iFCP, 438
- IGP, 91, 221
- IGRP, 91, 221
- IMAP, 637
- IP, 55, 61, 485, 486
- IPsec, 699, 754
- IPv4, 487
- IPv6, 514
- iSCSI, 435
- IS-IS, 221, 229
- iSNS, 439
- iWARP, 451
- Kerberos, 712
- L2F, 756
- L2TP, 756
- LonTalk, 330
- MGCP, 678
- MPLS, 360
- ND, 524
- NDP, 506
- NetBIOS, 527
- NFS, 599
- numery protokołów, 499
- OSPF, 221, 227
- PLCP, 380
- POP3, 626, 636
- PoS, 353
- PPP, 74
- PPTP, 755
- protokoły bezstanowe, 612
- protokoły routingu, 91, 221
- protokoły warstwy n, 48
- protokół datagramów użytkownika, 55
- protokół internetowy, 55, 61
- protokół odwzorowywania adresów, 61
- protokół sterowania transmisją, 55, 61
- protokół zdalnego pulpitu, 83
- RADIUS, 402
- RARP, 532
- RDP, 83
- RIP, 221, 224
- RSTP, 238
- RTCP, 645, 653
- RTP, 651, 676
- RTSP, 645, 650
- SCCP, 669, 676
- SIP, 669, 675
- SMB, 89, 600
- SMTP, 626, 630
- SNMP, 86, 90, 96
- SOAP, 620
- SRTP, 653
- SSL, 702
- sterowanie przepływem, 120
- STP, 213, 232
- STUN, 677
- TCP, 55, 61, 70, 464
- TLS, 702, 755
- UDP, 55, 70, 475
- UPnP, 495
- X.500, 582
- X10, 323
- X11, 83
- XNS, 569
- proxy, 717, 723, 735
- proxy transparentne, 738
- ProxySG, 598
- próbkowanie, 105, 112
  - PCM, 115
  - próbkowanie sygnału sinusoidalnego, 113
- przechowaj i przekaz, 32
- przechwytywanie ruchu sieciowego, 781
- przeciążony NAT, 734
- przeglądanie bufora ARP, 533
- przeglądanie sieci, 91
- przejęcie komunikacji, 243
- przekazywanie informacji, 32
- przekazywanie znacznika, 77
- przekierowywanie usług reklamowych, 530
- przełączane połączenia punkt-punkt, 67
- przełączanie, 205
- przełączanie obwodów, 34, 69, 205, 207
- przełączanie pakietów, 32, 34, 65, 69, 205, 207
  - tabela stanów, 66
- przełącznik, 75, 211
  - cechy, 211
- przepływ danych, 119
- przepustowość, 105, 107
- przepustowość systemu, 141
- przepustowość zmienna nie w czasie rzeczywistym, 125
- przepustowość zmienna w czasie rzeczywistym, 125
- przesłuchy, 181
  - przesłuch zbliżny, 181
  - przesłuch zdalny, 181
- przestrzenie nazw, 575
  - DNS, 540
- przesuwne okno, 473
- przetwarzanie bez granic, 442
- przetwarzanie sieciowe, 442, 458
- przetwarzanie stosu TCP bez użycia procesora, 445
- przetwarzanie sygnału, 105
- przetwarzanie w chmurze, 442, 458
- przezroczyste serwery proxy, 738
- przybliżenie przebiegu prostokątnego, 109
- przygotowanie okablowania, 178, 179
- przynęty, 738
- przypisania portów, 841
- PSD, 262
- PSH, 467

PSK, 193, 373  
 PSTN, 67, 206, 212, 221, 335, 339, 665, 827  
 PTR, 541, 543  
 PTYPE, 532  
 Public Key, 543  
 Public Key Infrastructure, 702  
 Public Switched Telephone Network, 67, 206, 335  
 publiczna sieć telefoniczna, 67, 206, 335  
 publiczna sieć telefoniczna z komutacją obwodów, 339  
 publikowanie informacji o węźle, 90  
 pulpit zdalny, 831  
     GoToMyPC, 833  
     oprogramowanie, 833  
     protokoły, 832  
     RDP, 832  
     Windows, 832  
 Pulse Amplitude Modulation, 115  
 Pulse Code Modulation, 115  
 Pulse Modulation, 199  
 Pulse Position Modulation, 115  
 Pulse Width Modulation, 115  
 pułapki SNMP, 98  
 punkt dostępu, 366, 385  
 punkt-punkt, 31, 61  
 punkty dostępu do sieci, 361  
 punkty dostępu do usługi, 49  
 punkty końcowe, 85, 94  
 punkty przyłączeniowe, 74  
 punkty wymiany ruchu internetowego, 361  
 push e-mail, 628  
 PUT, 615  
 PuTTY, 815  
 PWM, 115  
 PXE, 174, 697, 775  
 python, 792

## Q

QAM, 343, 375  
 gmail, 638  
 QoS, 67, 106, 121, 124, 139, 218, 358, 360, 447, 481, 524  
 QPSK, 374, 375  
 QRT, 275  
 QTSS, 658  
 Quadrature Amplitude Modulation, 375  
 Quagga, 216  
 Quality of Service, 67, 106, 447, 481, 672  
 Query Routing Table, 275  
 QuickTime, 660  
 QuickTime Broadcaster, 657  
 QuickTime Player, 660  
 Qwest, 341

## R

RA, 383  
 RAC, 828  
 Radio Frequency Communication, 290  
 Radio Frequency Interference, 180  
 Radio-Frequency Identification, 536

RADIUS, 103, 402, 406, 778, 827, 828, 830, 834  
     autoryzacja, 835  
     Diameter, 838  
     dołączalne moduły uwierzytelniania, 835  
     dynamiczne odkrywanie węzłów, 839  
     oprogramowanie, 837  
     PAM, 835  
     roaming RADIUS, 837  
     rozliczanie, 835  
     sesja, 836  
     sesja Diameter, 839  
     strefy, 837  
     uwierzytelnienie, 834  
 RAID, 143, 421  
 RAID-Z, 563  
 ramki, 46, 51, 69, 300  
     802.11, 382  
     ARP, 532  
     BPDU, 237  
     Fibre Channel, 429  
     Frame Relay, 359  
     HomePlug, 266  
     Modbus, 329  
     PoS, 353  
     ramki potwierdzeń, 52  
     SONET, 351, 352  
     Token Ring, 314  
     VLAN, 307  
     X10, 319  
 ramki Ethernet, 303  
     struktura, 305  
 ramkowanie, 69  
 Random Early Detection, 218  
 raport o stanie połączenia, 50  
 RARP, 532, 533  
 RAS, 828, 831  
 rasdial, 803  
 RBAC, 580  
 RC4, 402, 709  
 RCA, 768  
 rcp, 803  
 RCP, 645  
 RDBMS, 569  
 RDMA, 449  
 RDN, 586  
 RDP, 83, 832  
 Read Only Domain Controller, 591  
 Real Control Packets, 645  
 Real Time Variable Bit Rate, 125  
 RealMedia, 660  
 RealPlayer, 661  
 RealProducer, 657  
 Real-Time Control Protocol, 643, 645, 653  
 Real-Time Media Flow Protocol, 663  
 Real-Time Messaging Protocol, 663  
 Real-Time Operating System, 82  
 Real-Time Streaming Protocol, 643, 645  
 Real-Time Transfer Control, 676  
 Real-Time Transport Protocol, 643, 651, 666, 676  
 RECEIVE, 472  
 Reconfigurable Optical Add-Drop Multiplexer, 118

- RED, 218, 219
- Red Hat Linux, 553
- regenerator, 209, 210, 386
  - regenerator bezprzewodowy, 388
- Regional Internet Registries, 492
- regionalni administratorzy numerów IP, 492
- reguła czasu interaktywnej odpowiedzi, 147
- reguła Little'a, 145, 146, 147, 149
- reguła wykorzystania, 144, 147
- reguła wymuszonego przepływu, 145, 147
- reguła zapotrzebowania na usługę, 145, 147, 148
- rekordy LDIF, 585
- rekordy zasobów, 538, 539, 540
- Relational Database Management Systems, 569
- Relative Distinguished Node, 586
- relog, 803
- Remote Access Client, 828
- Remote Access Server, 828
- Remote Authentication Dial-In User Service, 834
- Remote Desktop, 831
- Remote Desktop Protocol, 83, 832
- Remote Procedure Call, 600, 620
- remsh, 803
- ren, 803
- rename, 803
- Rename Mailbox, 543
- repeater, 211
- replace, 803
- replay attack, 712
- replikacja, 573
- replikacja Active Directory, 590
- repozytorium CIM, 101
- repozytorium wspólnego modelu informacji, 90, 101
- Representational State Transfer, 622
- Request For Comments, 44
- Request For Proposal, 44
- Request to Send, 120, 382
- Research in Motion, 628
- resolver, 538
- Response Point, 669
- Responsible Person, 543
- REST, 622
- Return of Investment, 153, 762
- Reverse Address Resolution Protocol, 532
- rexec, 803
- rexx, 792
- rezerwacja zasobów, 121
- RFC, 44
- RFC 1122, 61
- RFC 2453, 224
- RFC 793, 465
- RFCOMM, 290
- RFI, 180
- RFID, 536
- RFP, 44
- RG-11, 183
- RG-58 A/U, 183
- RG-58 C/U, 183
- RG-58/U, 183
- RG-59, 183
- RG-6, 183
- RG-62, 183
- RG-8, 183
- RIB, 88, 217
- RIM, 628
- RIP, 91, 221, 224, 476
- RIPE NCC, 493
- RIPEMD, 711
- RIPng, 225
- RIR, 492
- RJ-11, 261
- RJ-45, 180, 181
- rm, 803
- rmdir, 803
- ROADM, 118
- roaming RADIUS, 837
- robaki, 693
- ROBO, 265
- RODC, 591
- rodzaje sieci, 30
- rodzaje transmisji danych, 31
- ROI, 153, 762
- Role-Based Access Control, 580
- Root Cause Analysis, 768
- root port, 234
- root servers, 536
- RootDirectoryDAP, 101
- RootMicrosoftIISv2, 101
- RootSNMP, 101
- route, 804
- Route Through, 543
- router, 75, 215
  - backplane, 217
  - baza danych przełączania, 217
  - plyty montażowe, 217
  - QoS, 218
  - RIB, 217
  - routing, 219
    - warstwa danych, 217
    - warstwa przełączania, 217
    - warstwa sterująca, 217
    - wirtualne sieci LAN, 217
  - wybór pakietów do odrzucenia, 218
  - zapora sieciowa, 721
- Router Advertisement, 523
- router bezprzewodowy, 390
  - aktualizacja, 392
  - konfiguracja, 391
  - Tomato, 392
- router cebulowy, 242
  - anonimowość w przesyłaniu danych, 243
  - jednostki klienckie Tor, 244
  - klient Tor, 245
  - komponent proxy sieci Tor, 244
  - ruch Tor, 244
  - ukryte usługi, 245
  - zasada działania systemu, 243
- routing, 52, 76, 91, 168, 215, 216, 219, 438, 485
  - algorytm Bellmana-Forda, 222
  - algorytm stanu łącza, 226
  - algorytm wektora odległości, 221

- algorytm wektora odległości z numerami sekwencyjnymi, 226
- algorytm wektora ścieżki, 229
- BGP, 221, 231
- drzewo rozpinające, 233
- DSDV, 226
- DV, 221
- dzielony horyzont, 225
- EGP, 221
- emisja dowolna, 219
- emisja pojedyncza, 219
- HWMP, 394
- IGP, 221
- IGRP, 221
- IPv4, 488
- IS-IS, 221, 229
- koszt trasy, 221
- liczenie do nieskończoności, 224
- metody optymalizacji, 221
- metody wysyłania pakietów, 219
- multiemisja, 219
- oprogramowanie, 216
- OSPF, 221, 227
- paradoks Braessa, 219, 220
- protokoły, 91, 221, 487
- protokoły stanu łącza, 226
- protokół drzewa rozpinającego, 232
- RIP, 221, 224
- rozgłaszanie, 219
- STP, 232
- tablica routingu, 223
- technika dzielonego horyzontu z zatrzymywaniem wstecznym, 225
- topologie routing, 219
- wektor odległości, 221
- wektor ścieżki, 229
- wyznaczanie najkrótszej trasy w grafie, 222
- Routing Information Base, 88, 217
- Routing Information Protocol, 91, 221, 476
- rozbudowa serwerów, 153
  - charakterystyka aplikacji, 153
  - konsolidacja serwerów, 154
  - maksymalne obciążenie, 153
  - oddzielenie funkcji serwera i pamięci masowej, 153
  - poziom zwrotu z inwestycji, 153
  - wydajność dysku, 153
  - wydajność sieci, 153
- rozdzielanie wiązek światła w systemie WDM, 118
- rozgłęźniki światłowodowe, 194
- rozgłaszanie, 32, 219, 298, 485, 487
  - sieci IP, 89
- rozgłaszanie kierunkowe, 485, 487
- rozgłoszeniowe sieci wielodostępne, 37
- rozkład prawdopodobieństwa, 134
- rozległa sieć komputerowa, 335
- rozliczanie, 835
- rozpraszanie widma przez skakanie po częstotliwościach, 119
- rozproszona gwiazda, 36
- rozproszona tabela skrótów, 276
- rozszerzenia adresowania IP, 488
- rozszerzona gwiazda, 36
- równoważenie obciążenia, 455
  - oprogramowanie, 456
  - rozwiązania sprzętowe, 456
  - równoważenie obciążenia w mostku, 456
  - równoważenie obciążenia w routerze, 456
  - szeregowanie cykliczne, 456
- różnicowa modulacja bifazowa, 313
- różnicowa modulacja impulsowo-kodowa, 116
- różnicowe binarne kluczowanie fazy, 265
- różnicowe kodowanie Manchester, 313
- różnicowe kwadraturowe kluczowanie fazy, 265
- RP, 543
- RPC, 600, 620
- R-PVST, 242
- RR, 538
- RS 232, 120, 329
- RS 485, 329
- RSA, 706, 712
- rsh, 803, 804
- RST, 467
- RSTP, 238
  - jednostki BPDU, 239
  - rekonfiguracja w przypadku awarii, 240
  - technika szybkiej zmiany stanu portu, 240
  - wprowadzanie nowych łączy, 241
- RT, 543
- RTCP, 645, 653
- RTMFP, 663
- RTMP, 663
- RTOS, 82
- RTP, 651, 665, 675, 676
  - nagłówki, 652
  - pakiety, 653
  - zadania, 651
- RTS, 120, 382
- RTSP, 645, 650, 660
  - polecenia, 650
- RT-VBR, 125
- ruch w sieci, 106

**S**

- S/N, 114
- SA, 305, 383, 700
- SaaS, 459
- SABRE, 21
- SACK, 468, 474
- SAM, 657
- Samba, 92, 602
  - autoryzacja użytkowników, 605
  - bezpieczeństwo, 603
  - DMB, 604
  - instalacja, 604
  - NBNS, 603, 604
  - nmbd, 603
  - określanie nazw, 603
  - przeglądanie udziałów, 603
  - smb.conf, 606
  - smbd, 603
  - smbusers, 605
  - system plików SMB, 602

- Samba
  - tryby bezpieczeństwa, 603
  - Ubuntu, 604
  - WINS, 604
- Samba Web Administration Tool, 602
- SAN, 100, 407, 408, 410, 438, 451, 593, 597, 598
- SAP, 49
- SAS, 315
- SATA, 409
- SBC, 341
- SBS, 571
- SC, 194
- SCA, 623
- SCADA, 294, 319, 325
- scatternet, 288
- SCCP, 665, 669, 674, 675, 676
- SCGI, 620
- schemat Markowa, 152
- schemat PAR, 470
- schematy mapowania NAT, 734
- SCO, 290
- SCO Open Server 6, 553
- SCOM, 777
- SCR, 125
- SCSI, 281, 409
- SDH, 118, 317, 335, 348
- SDH STM-1, 350
- SDO, 623
- SDP, 135, 660
- SDSL, 345
- SDU, 49, 652
- SECBR, 126
- Secure Real-Time Transport Protocol, 653
- Secure Socket Layer, 702, 738
- Secure VPN, 743
- Security Account Manager, 587
- seeder, 278
- segmentacja danych, 51
- segmenty, 46, 59, 70, 71
- SEND, 472
- sendfile(), 448
- sendfile64(), 448
- sendmail, 638, 639
- separator zakresu, 416
- Sequence Diagram Editor, 79
- Serial ATA, 409
- Serial Port Profile, 290
- server appliance, 131
- Server Message Block, 600
- Server-Free Backup, 419
- Service Access Point, 49
- Service Component Architecture, 623
- Service Data Unit, 49, 652
- service demand, 145
- service demand law, 145
- Service Design, 135
- Service Design Package, 135
- Service Level Agreement, 125, 778
- Service Location, 543
- Service Location Protocol, 495
- Service Operation, 136
- Service Oriented Architecture, 459, 612, 622
- Service Set Identifier, 366, 389
- Service Strategy, 135
- Service Switching Point, 679
- Service Transition, 135
- serwer, 79, 129, 130
  - emulacja programowa, 132
  - kolejka wejściowa, 132
  - metodologia prac projektowych, 134
  - model operacyjny serwera sieciowego, 132
  - planowanie pojemności, 133
  - pojemność, 133
  - przyczyny niepowodzenia przedsięwzięcia, 134
  - skalowanie, 139
  - system operacyjny, 130
  - urządzenia serwerowe, 131
- serwer AAA, 834
- serwer anonimizujący, 737
- serwer aplikacji, 130
- serwer BOOTP, 91
- serwer DHCP, 91, 508
- serwer DNS, 538
- serwer domen, 131, 571
- serwer dostępu zdalnego, 828
- serwer ISA, 695
- serwer kopii zapasowych, 130
- serwer LDAP, 584
- serwer nazw, 527
- serwer ogólnego przeznaczenia, 130
- serwer plików, 130, 597
- serwer poczty, 638
- serwer pośredniczący, 170
- serwer proxy, 170, 717, 726, 735
  - odwrotne proxy, 738
  - oprogramowanie, 737
  - proxy otwarte, 737
  - przezroczysty serwer proxy, 738
  - przynęty, 738
  - serwer anonimizujący, 737
  - web proxy, 737
- serwer RADIUS, 406, 834
- serwer RARP, 533
- serwer Samba, 602
- serwer sieci domowych, 268
- serwer sieciowy, 131
- serwer strumieniowania, 643, 647, 658
- serwer STUN, 651
- serwer śledzący, 277
- serwer terminali, 82
- serwer uwierzytelniania, 402
- serwer WINS, 536
- serwer wydruku, 130
- serwer X Window System, 83
- sesja, 52, 96
- sesja Diameter, 839
- sesja RADIUS, 836
- sesja Telnet, 814
- sesja terminalowa, 54
- Session Initiation Protocol, 665, 669, 674

- Session Traversal Utilities for NAT, 676
- SETI@home, 442, 458
- Severely Errored Cell Block Ratio, 126
- SFD, 305
- SGE, 459
- sh, 791, 804
- SHA, 532, 711
- Shannon Cladue, 114
- Shielded Twisted Pair, 180
- shutdown, 804
- siatka, 33, 37
- sieci rozległe geograficznie, 31
- sieciowy bufor plików, 597
- sieciowy dostęp do plików, 593
- sieciowy system operacyjny, 130, 549, 550, 566, 593
  - gniazda, 557
  - IOS, 552
  - Linux, 559
  - NetWare, 563
  - ogólny sieciowy system operacyjny, 551
  - Open Enterprise Server, 563
  - oprogramowanie, 552
  - platformy, 549, 553
  - POSIX, 556
  - protokoły, 551
  - sieciowy system operacyjny specjalnego przeznaczenia, 551
  - Single UNIX Specification, 558
  - Solaris, 561
  - STREAMS, 557
  - Unix, 554
  - usługi, 551
  - Windows Server, 564
- sieciowy system plików, 598
  - DFS, 606
  - NFS, 599
  - Samba, 602
  - SMB, 600
- sieć, 21, 27, 28
  - architektura sieci, 60
  - ATM, 120
  - bezpieczeństwo, 687
  - Bluetooth, 30
  - CAN, 31, 336
  - CDDI, 315
  - definiowanie sieci, 28
  - Ethernet, 61
  - F2F, 271, 281
  - FC-AL, 430
  - FC-SW, 429, 431
  - Fibre Channel, 408, 425
  - Frame Relay, 359
  - HomePNA, 260
  - ISDN, 341
  - LAN, 27, 30, 293
  - MAN, 31
  - NAS, 410
  - OPC, 332
  - P2P, 77
  - PAN, 30
  - peer-to-peer, 30
  - pLAN, 27, 30, 271
  - proces modelowania, 151
  - PSTN, 335, 339, 667
  - rodzaje sieci, 30
  - SAN, 100, 407, 410, 438
  - SDH, 317
  - SONET, 195, 348
  - TCP/IP, 463
  - topologia, 33, 60
  - topologia fizyczna, 33
  - VINES, 569
  - VLAN, 217
  - VPN, 67, 741
  - VSAN, 414
  - WAN, 27, 31, 335, 336
  - Wi-Fi, 365
  - X.25, 355
  - zasieg, 27
  - Zero Copy Network, 448
- sieć ad hoc, 30, 42, 366
- sieć bezprzewodowa, 196, 365, 366
  - 802.11, 366, 368, 370, 372, 380
  - anten, 395
  - AP, 366, 385
  - beacon, 366
  - bezpieczeństwo, 402
  - BPSK, 374
  - brama, 385, 390
  - BSS, 366
  - CBP, 372
  - częstotliwości kanałów, 369
  - DCF, 381
  - DFIR, 370
  - DPSK, 373
  - DS, 366
  - DSE, 372
  - DSSS, 371, 375, 377
  - ECSA, 372
  - ESS, 367
  - ESSID, 367
  - FHSS, 370, 376, 378
  - IBSS, 366
  - informacja, 199
  - kanały, 369
  - kodowanie informacji, 199
  - konfiguracja routera, 391
  - logo Wi-Fi, 367
  - łącza mikrofalowe, 202
  - łącza radiowe, 201
  - MIMO, 118, 371
  - modulacja, 199, 373
  - most, 386, 388
  - OFDM, 379
  - oprogramowanie, 399
  - OQPSK, 375
  - PCF, 381
  - PCSM, 381
  - planowanie dostępu, 387
  - PLCP, 380

- sieć bezprzewodowa
  - PMD, 381
  - połączenia, 257, 384
  - połączenia bezprzewodowe, 201
  - połączenia WDS, 389
  - PSK, 373
  - punkt dostępu, 366, 385
  - punkt-punkt, 388
  - QPSK, 375
  - ramki, 380
  - ramki 802.11, 382
  - regenerator, 386
  - router, 390
  - rozmieszczanie punktów dostępowych, 370
  - sieć ad hoc, 366, 367
  - sieć infrastrukturalna, 367
  - skaner sieciowy, 400
  - SSID, 366
  - STA, 366, 372
  - standardy, 365, 368
  - system dystrybucji, 366
  - szyfrowanie, 402
  - topologia wielopunktowa, 388
  - topologie, 388
  - transmisja, 199, 380
  - tryb wzmacniaka, 386
  - typy połączeń, 370
  - unikanie kolizji, 381
  - uwierzytelnianie, 385, 402
  - WAP, 385
  - wardriving, 400
  - WDS, 388
  - WEP, 385, 402
  - Wi-Fi, 367
  - WPA, 385, 404
  - WPA2, 404
  - zakres częstotliwości, 201
- sieć bezprzewodowa laptopów XO, 393
  - HWMP, 394
  - routing, 394
  - węzeł kraty MP, 394
- sieć Bluetooth, 288
- sieć brzegowa, 725
- sieć buforowania brzegowego, 598
- sieć cyfrową z integracją usług, 341
- sieć domowa, 251
  - elementy sieci, 252
  - Ethernet, 258
  - HomePlug, 262
  - HomePNA, 259
  - PoE, 262
  - połączenia, 253
  - połączenia bezprzewodowe, 257
  - połączenia stałe, 258
  - serwer, 268
  - technologie, 254
  - zasoby sieciowe, 253
  - zastosowanie, 252
- sieć elektryczna, 264
- sieć gwiazdista, 35, 41
- sieć heterogeniczna, 100
- sieć jednostek równorzędnych, 77
- sieć kampusowa, 31
- sieć klient-serwer, 79
  - klient, 79
  - serwer, 79
- sieć komputerowa, *Patrz sieć*
- sieć kratowa, 42, 432
- sieć lokalna, 27, 30, 293
  - dostęp do kanału z wykorzystaniem tokenu, 299
  - dostęp sekwencyjny do kanału, 299
  - Ethernet, 293, 300
  - FDDI, 314
  - FDM, 299
  - kanały rozgłoszeniowe, 298
  - komunikacja rozgłoszeniowa, 299
  - sieci wykorzystywane w automatyce, 318
  - standardy, 294, 295
  - ścieżka transmisji, 299
  - Token Ring, 293, 295, 310
  - wielodostęp, 299
  - X10, 294, 319
- sieć małego świata, 273
- sieć mesh, 458
- sieć metropolitarna, 31
- sieć nakładkowa, 281
- sieć o przełączanych obwodach, 206
- sieć o topologii drzewiastej, 39
- sieć o topologii liniowego łańcucha, 40
- sieć o topologii łańcucha połączona w pierścień, 41
- sieć oparta na łączach dzierżawionych, 337
- sieć optyczna, 194
- sieć pakietowa, 32, 69, 206, 354
  - datagramy, 355
  - pakiety, 354
- sieć pamięci masowej, 100, 407, 410
  - adres bloku logicznego, 412
  - brama NAS, 411
  - DAS, 409, 410
  - dysk wirtualny, 412
  - FC-AL, 410
  - FCP, 410
  - FC-P2P, 410
  - FC-SW, 410
  - Fibre Channel, 408, 409, 425
  - Fibre Channel over IP, 436
  - Fibre Channel Point-to-Point, 409
  - HBA, 410, 412
  - identyfikator jednostki logicznej, 412
  - iFCP, 438
  - iSCSI, 435
  - iSNS, 439
  - kontroler pamięci masowej, 412
  - LUN, 412
  - model współdzielonej sieci pamięci masowej, 414
  - oprogramowanie wirtualizacji pamięci masowej, 413
  - pętla arbitrażowa, 410
  - polityka zarządzania cyklem życia informacji, 413
  - SAN, 408
  - SNIA, 414
  - taśmy, 415
  - technologie pamięci masowej z zastosowaniem IP, 433

- thin provisioning, 413
- topologia sieci, 407
- typy sieci, 409
- urządzenia, 408, 410
- urządzenia wirtualizacyjne, 414
- wiele kart interfejsu sieciowego, 410
- wirtualizacja, 412
- współdzielone taśmy, 415
- zarządzanie siecią SAN, 438
- sieć peer-to-peer, 64, 77, 78, 271, 272
- czyste sieci P2P, 273
- Freenet, 276
- Gnutella, 274
- konfiguracje sieci, 271
- Napster, 276
- sieci małego świata, 273
- systemy hybrydowe, 276
- Torrent, 277
- sieć pierścieniowa, 37
- sieć pLAN, 282
- sieć prywatna, 726
- sieć przełączana, 34, 69
- sieć przyjacielska, 271, 280
- uwierzytelnianie, 281
- sieć rozległa, 27, 31, 335, 336
- ATM, 357
- Frame Relay, 359
- Internet, 361
- Internet2, 363
- kategorie, 337
- łącza, 336
- media transmisyjne, 336
- SMDS, 356
- X.25, 355
- sieć rozproszona, 288
- sieć siatkowa, 38
- sieć szkieletowa, 335, 336
- sieć szkieletowa VPLS, 747
- sieć telefoniczna, 665
- sieć telefonii cyfrowej, 206
- sieć telewizji kablowej, 346
- sieć Tor, 243, 244
- sieć ustrukturyzowana, 276
- sieć wielowarstwowa, 80
- model ACID, 81
- transakcje, 81
- sieć wirtualna, 307
- sieć z komutacją komórek, 337
- sieć z komutacją obwodów, 336, 337
- DSL, 342
- ISDN, 341
- łącze dedykowane, 338
- obwody, 338
- połączenia wirtualne, 338
- PSTN, 339
- sieć telewizji kablowej, 346
- sieć z komutacją pakietów, 336, 337
- SIG, 254, 544
- Signature, 544
- Silly Window Syndrome, 481
- Silverlight, 663
- Silverlight 2.0, 664
- Silverlight Streaming Service, 664
- Simple Mail Transfer Protocol, 55
- Simple Network Management Protocol, 86, 90, 476
- Simple Object Access Protocol, 620
- Simple Service Discovery Protocol, 495
- simpleks, 49
- Single Attached Stations, 315
- Single Sign On, 574
- Single UNIX Specification, 554, 558
- SIP, 515, 665, 669, 674, 675, 680
- Site Local Address, 520
- skakanie po częstotliwościach, 30, 376
- skakanie po częstotliwościach w odstępach czasu, 378
- skalowalność, 142
- skalowanie okna, 473
- skalowanie serwerów, 139
- skalowanie systemów sieciowych, 139
- skalowanie w górę, 154, 155
- skalowanie wszerek, 154
- skaner sieciowy, 400
- skanowanie sieci, 102
- SKEME, 701
- Skinny Call Control Protocol, 665, 669, 674, 676
- skoki, 75
- skrętka, 60, 180, 184
- kategorie, 182, 185
- oznaczenia przewodów ethernetowych w standardach
- TIA/EIA, 185
- skrętka ekranowana, 177, 180
- skrętka foliowana, 181
- skrętka nieekranowana, 178, 181
- standardy łączenia przewodów, 185
- skrypty CGI, 619
- skuteczność anteny, 396
- Skype, 671, 680, 681
- SLA, 125, 778
- SLAAC, 523
- SLIP, 829, 830
- SLP, 495
- SMA, 194
- Small Office/Home Office, 269, 722
- smart metering, 378
- SMASH, 764
- SMB, 89, 272, 593, 599, 600
- CIFS, 601
- smbclient, 602
- smbfs, 602
- SMC, 580
- SMDS, 356
- SMI, 99
- SMIL, 648, 654
- SMO, 763
- SmoothWall, 216
- SMP, 455, 551
- SMTP, 55, 625, 626, 630
- polecenia, 630
- POP3, 636
- przesyłanie wiadomości e-mail, 630
- typy MIME, 631

- SMTP-AUTH, 631
- Smurf Attack, 692
- SNA, 56
- SNAT, 735
- sneakernet, 29
- SNIA, 45, 410, 414
- sniffer pakietów, 781
- SNMP, 79, 86, 90, 91, 96, 438, 465, 476
  - agent, 96, 98
  - ASN.1, 99
  - baza danych informacji zarządzania, 96, 98
  - Ethernet, 100
  - Fibre Channel, 100
  - GET, 98
  - GETBULK, 98
  - GETNEXT, 98
  - interakcje między poszczególnymi elementami, 97
  - konsola zarządzania, 97, 100
  - MIB, 96, 98, 99
  - odpowiedzi, 97
  - odpytywanie, 98
  - OID, 99
  - polecenia, 97
  - protokół, 96
  - przeglądanie plików MIB, 99
  - pułapki, 98
  - SMI, 99
  - stan urządzenia, 98
  - TRAP, 98
  - wykrywanie urządzeń, 97
  - zapytania, 98
  - zarządzane obiekty, 96
  - zarządzanie siecią, 97
  - żądania, 98
- SNMPPutil, 103
- SNMPWalk, 103
- SNP, 455
- SNR, 398
- SOA, 459, 539, 541, 612, 622
  - architektura, 623
  - dane, 623
  - klient, 622
  - komponenty, 623
  - platformy, 623
  - SDO, 623
- SOAP, 102, 586, 620, 621
- SOCKS, 244
- SoftGrid, 649
- SoftGrid Sequencer, 649
- Software as a Service, 459
- Software Virtualization Solution, 649
- SOHO, 269, 722, 828
- Solaris, 553, 561
- Solaris Management Console, 580, 581
- Solaris Resource Manager, 576
- solitony, 191
- SOMF, 624
- SONET, 118, 195, 335, 348
- SONET STS-1, 350
- SONET/SDH, 349
  - agregacja ruchu ATM w routerach PoS, 354
  - architektura, 349
  - ATM, 353
  - BLSR, 350
  - LAPS, 350
  - łącza, 349
  - połączenia, 349
  - PoS, 353
  - ramki, 352
  - ramki PoS, 353
  - ramkowanie, 350
  - router PoS, 353
  - sekcje, 349
  - ścieżki, 349
  - TDM, 353
  - topologie sieci, 350
  - transmisja danych, 350
  - UPSR, 350
  - zwielokrotnienie łączy, 352
- Source NAT, 735
- source route bridging, 213
- SPA, 532
- SPA3102, 673
- spam, 641
- Spanning Tree Protocol, 213, 232
- SPC, 667
- speaker node, 230
- SPI, 721, 727
- splitter, 343
- sporządzanie mapy sieci, 102
- SPP, 290
- sprzętowa kontrola przepływu, 120
- sprzętowe zapory sieciowe, 722
- SQL Server, 564
- SRB, 213
- SRI, 528
- SRM, 439, 576
- SRTP, 653, 673
- SRV, 543
- SSD, 421
- SSH, 243, 815
- SSI, 389
- SSID, 366, 386, 392
- SSL, 702, 743
- SSO, 574
- SSP, 455, 679
- ST, 194
- STA, 366, 372
- stacje, 315
- stacje końcowe, 300
- stała przepustowość, 125
- stała szybkość przesyłania komórek, 125
- stan fizyczny, 62
- stan logiczny, 62
- stan połączenia, 62
- stan serwera DHCP, 793
- standard X10, 319
- standardy, 44
- standardy łączenia przewodów, 185
- standardy sieci Fibre Channel, 426

- ul style="list-style-type: none; padding-left: 0;">
- standardy sieci LAN, 295
- Stanford Research Institute, 528
- StarLAN, 301
- Start of Authority, 541
- Stateful Inspection, 719
- Stateful Packet Inspection, 721, 727
- statefull, 66
- stateless, 66
- STATUS, 472
- statyczne strony internetowe, 619
- statyczny adres IP, 507
- Steel Belted Radius, 837
- sterowanie dostępem do nośnika, 304
- sterowanie łączem logicznym, 305
- sterowanie oświetleniem, 322
- sterowanie przepływem, 51, 119
  - ATM, 120
  - Frame Relay, 120
  - negocjowanie parametrów wzajemnego połączenia, 119
  - programowa kontrola przepływu, 120
  - protokoły, 120
  - sprzętowa kontrola przepływu, 120
  - TCP, 120
- sterowniki PLC, 326
- sterowniki sieciowe, 173
- STM-256, 352
- STM-64, 352
- stopa błędnie przesłanych komórek, 126
- stopa błędnych komórek, 125
- stopa poważnie uszkodzonych bloków komórek, 126
- stopa utraty komórek, 125
- Storage Area Network, 100, 407, 408, 422, 451
- Storage Networking Industry Association, 45, 410
- Storage Resource Management, 439
- store and forward, 32, 213
- Stored Program Control, 667
- stos protokołów sieciowych, 43
- stos sieciowy, 165
- stos TCP/IP, 165
- stosunek sygnału do szumu, 114
- STP, 180, 181, 182, 213, 232
  - BPDU, 236
    - drzewo rozpinające, 233
    - dynamiczna optymalizacja, 236
    - hierarchia węzeł-most, 233
    - jednostki BPDU, 237
    - koszt segmentu, 236
    - koszt węzła, 234
    - obliczanie ścieżek o najniższym koszcie, 234
    - opóźnienie przekazywania, 237
    - porty główne, 234
    - porty wyznaczone, 234
    - ramka BPDU, 237
    - RSTP, 238
    - szybki protokół drzewa rozpinającego, 238
    - ścieżki o najniższym koszcie, 233
    - tryby pracy port mostu, 238
    - waga węzła, 234
- Strategia zarządzania usługami, 135
- Stratus FT, 454
- Stratus Lockstep, 455
- Stratus South PCI, 455
- STREAMS, 557, 558
- StreetTalk, 569
- strefa zdemilitaryzowana, 725
- STRIDE, 693
- strona MAN, 164
- strongly collision-free, 710
- strony internetowe, 619
- Structure of Management Information, 99
- strumieniowanie danych, 28
- strumieniowanie HTTP, 647
- strumieniowanie multimediów, 70, 643, 644, 647
  - bitrate, 655
  - emisja pojedyncza, 648
  - formaty strumieniowanych plików, 659
  - kodowanie, 655
  - multiemisja, 648
  - narrowcasting, 648
  - odtwarzacze, 661
  - platformy, 644
  - protokoły, 650
  - przepustowość serwera, 660
  - RTCP, 653
  - RTP, 651
  - RTSP, 650
  - serwer strumieniowania, 658
  - SMIL, 654
  - SRTP, 653
- strumień kluczy, 709
- Stub, 486
- STUN, 651, 666, 674, 675, 676, 677, 735
- subst, 804
- sugarcane, 738
- suma kontrolna, 467
- Sun, 561
- Sun Grid Engine, 459
- Sun N1 Grid Engine, 459
- Supervisory Control And Data Acquisition, 294
- SUS, 554, 558
- Sustained Cell Rate, 125
- SVS, 649
- swarm, 278
- SWAT, 602
- switch, 211
- Switched Multimegabit Data Service, 356
- SWS, 481
- sygnał cyfrowy, 106
- sygnał transmisyjny, 28
- sygnały, 62, 105, 107
  - amplituda sygnału, 111
  - częstotliwość sygnału, 109
  - faza sygnału okresowego, 110
  - kodowanie danych, 110
  - maksymalna częstotliwość sygnału, 112
  - podział sygnału na składowe, 108
  - polaryzacja sygnału, 118
  - przybliżanie przebiegu prostokątnego, 109
- sygnały harmoniczne, 105
- Symantec, 833

Symmetric Key Protocol, 714  
 Symmetric NAT, 734  
 SYN, 466, 467, 469, 729  
 synchroniczna hierarchia systemów cyfrowych, 317  
 Synchronized Markup Integration Language, 648, 654  
 Synchronous Digital Hierarchy, 317, 348  
 syndrom głupiego okna, 481  
 synteza Fouriera, 108  
 syslog, 766  
 System Area Network, 451  
 system autonomiczny, 221, 227, 362, 486  
 system integracji telefonu z komputerem, 678  
 system magistrali liniowej, 34  
 system nazw domenowych, 86  
 system operacyjny czasu rzeczywistego, 82  
 system operacyjny serwera, 130  
 system oprzyrządowania do zarządzania, 90, 97  
 system PBX, 667  
 system przetwarzania sieciowego, 457  
 system routerów cebulowych, 243  
 system sieciowy, 129  
 system sterowania procesami, 324  
 system telefoniczny, 667  
 system wykrywania zagrożeń, 694  
 system zarządzania siecią, 782  
 system zarządzania siecią WBEM, 101  
 Systems Network Architecture, 56  
 szacowanie wydajności, 143  
   dane wydajnościowe, 144  
   eliminowanie zatorów, 148  
   modelowanie sieci, 151  
   monitorowanie zasobów, 143  
   poziomy graniczne przepustowości, 150  
   poziomy ostrożnościowe stopnia  
     wykorzystania zasobu, 149  
   reguła czasu interaktywnej odpowiedzi, 147  
   reguła Little'a, 145, 146, 147, 149  
   reguła wykorzystania, 144, 147  
   reguła wymuszonego przepływu, 145, 147  
   reguła zapotrzebowania na usługę, 145, 147, 148  
   reguły operacyjne, 147  
   sekundy, 145  
   system typu klient-serwer, 146  
   własność Markowa, 151  
   zależności wydajnościowe, 143  
   zapotrzebowanie na usługę, 145  
 szczytowa szybkość przesyłania komórek, 125  
 szerokość pasma, 105, 106, 107, 111  
 szerokość wiązki anteny, 398  
 szum, 106, 114  
 szybka transformata Fouriera, 379  
 szybki protokół drzewa rozpinającego, 238  
 szybkie uwalnianie tokenu, 313  
 szybkość próbkowania Nyquista, 113  
 szybkość transmisji danych, 52  
 szyfr blokowy, 708  
 szyfr strumieniowy, 709  
 szyfrowanie, 267, 705, 706, 782  
   WEP, 402, 403  
   WPA, 404

## Ś

ścieżka, 94  
 światłowody, 187  
   diody LED, 193  
   dyspersja, 188  
   gradientowa zmiana współczynnika odbicia, 189  
   gradientowy światłowód wielomodowy, 189  
   kabel, 192  
   lasery półprzewodnikowe, 193  
   mod światła, 190  
   modulacja impulsów świetlnych, 193  
   odbicie światła, 189  
   parametry fizyczne, 191  
   płaszcz, 191  
   połączenia typu T, 194  
   przyłączanie światłowodów, 194  
   PSK, 193  
   rozgałęźniki, 194  
   rozgałęźniki aktywne, 194  
   system transmisyjny, 187  
   ścieżki propagacji światła, 189  
   światłowody jednomodowe, 187  
   światłowody wielomodowe, 187  
   tłumienie, 188  
   topologia sieci optycznej, 194  
   transmisja, 190  
   transmisja w światłowodzie wielomodowym, 189  
   włókna, 192  
   zakresy fal świetlnych, 190  
   złącza, 194  
   zmiana współczynnika załamania, 192

## T

T1, 347  
 TA, 383  
 tabela ARP, 531  
 tablica mostowania, 213  
 tablica routingu, 88, 223  
 tablica routingu żądań, 275  
 TACACS, 778, 835  
 TACACS+, 835  
 tail drop, 218  
 tape image, 415  
 TAPI, 666  
 Target Channel Adapter, 452  
 taskkill, 804  
 tasklist, 804  
 taśmy, 415  
   model współdzielonej pamięci masowej, 417  
   nagłówki, 416  
   przenoszenie danych taśmy, 419  
   separator zakresu, 416  
   struktura logiczna, 416  
   tworzenie kopii zapasowej, 416, 417  
   tworzenie kopii zapasowej bez udziału serwera, 419  
   wirtualizacja, 418  
 TCA, 237, 452  
 TCB, 472  
 TCI, 305

tcsh, 791  
 tcmsetup, 804  
 TCN, 237  
 TCP, 55, 61, 69, 70, 79, 355, 463, 464, 729  
   3-etapowy proces negocjacji, 469, 729  
   ACK, 466, 467, 469, 470  
   algorytm Nagle'a, 482  
   CWR, 467  
   Cyclic Redundancy Check, 467  
   ECE, 467  
   FIN, 467  
   flagi, 466  
   implementacja, 465  
   kontrola przeciążenia sieci, 473  
   kontrola przepływu, 473  
   LAST-ACK, 470  
   MSS, 473  
   MTU, 468, 473  
   multipleksowanie, 474  
   nagłówki IP, 496  
   niezawodność, 465  
   OPEN, 472  
   operacje protokołu, 469  
   pakiety, 465  
   pola kontrolne, 468  
   pole danych, 468  
   pole sumy kontrolnej, 467  
   połączenia, 464, 469, 472  
   połączenia jednokierunkowe, 469  
   porty, 466  
   potwierdzenie skumulowane, 470  
   problemy, 481  
   przesuwne okno, 473  
   PSH, 467  
   QoS, 481  
   RST, 467  
   SACK, 468, 474  
   schemat PAR, 470  
   skalowanie okna, 473  
   stany punktów końcowych, 471  
   sterowanie przepływem, 120  
   SYN, 466, 467, 469  
   three-way handshake, 469, 729  
   transfer danych, 469, 472  
   URG, 467, 468  
   wielkość okna, 465, 473  
   wskaźnik pilności, 468  
   zamykanie połączenia, 470  
 TCP Chimney Offload, 446  
 TCP offload, 158  
 TCP Offload Engine, 158, 441, 445, 460  
 TCP/IP, 21, 46, 49, 55, 61, 463  
 TCP\_NODELAY, 482  
 TDM, 115, 117, 299, 348  
 TDMA, 115  
 technika dzielonego horyzontu  
   z zatrzymywaniem wstecznym, 225  
 techniki multipleksacji, 118  
 techniki routingu, 76  
 technologia HomePlug, 262

technologia WMI, 101  
 technologie pamięci masowej z zastosowaniem IP, 433  
 technologie szerokopasmowe, 256  
 telefon wewnętrzny, 667  
 telefonia bezprzewodowa, 32  
 telefonia cyfrowa, 665, 666  
   aplikacje telefoniczne, 666  
   PBX, 667  
 telefony VoIP, 674  
 Telephony API, 666  
 Telestream Agility, 659  
 telnet, 805  
 Telnet, 814  
 teoria próbkowania, 112  
 teoria sygnałów, 107  
 terminal danych, 119  
 terminal X Window, 83  
 Terminate and Stay Resident, 550  
 terminator, 35  
 Text, 544  
 tftp, 805  
 THA, 532  
 The Onion Router, 243, 244  
 thin client, 82, 532  
 thin provisioning, 413  
 three-way handshake, 469, 729  
 TIA/EIA, 185  
 Time Division Multiple Access, 115  
 Time Division Multiplexing, 115, 299  
 Time To Live, 497, 511  
 TINC, 748  
 TKIP, 404  
 TLD, 536, 537  
 TLS, 702  
   algorytmy kryptograficzne, 703  
   tunelowanie, 755  
   uwierzytelnianie, 702  
 TLS 1.0, 619  
 tłumaczenie adresów IP na nazwy, 536  
 tłumaczenie adresów portów, 734  
 tłumaczenie adresów portów sieciowych, 734  
 tłumaczenie adresów sieciowych, 717, 719, 732  
 tłumaczenie zapytań DNS, 793  
 tłumienie, 74, 188  
 TOE, 158, 441, 442, 445, 460, 465  
   implementacja, 446  
   Zero Copy Network, 448  
 token, 37, 310  
 Token Bus, 296  
 token passing, 77  
 Token Ring, 37, 77, 293, 295, 296, 310  
   ARCNET, 311  
   Beaconing, 314  
   ETR, 313  
   kontrola ruchu, 313  
   MAU, 311, 312  
   mechanizm drogowskazu, 314  
   monitor aktywny, 313  
   most, 213  
   prawo do transmisji danych, 310

- Token Ring
    - QoS, 313
    - ramki, 314
    - różnicowe kodowanie Manchester, 313
    - szybkie uwalnianie tokenu, 313
    - token, 310, 313
    - topologia sieci, 312
  - tolerancja zmienności opóźnień komórek, 126
  - Tomato, 392
  - Top500.org, 443
  - Top-Level Domains, 537
  - topologia DNS, 539
  - topologia fizyczna, 33
    - drzewo, 33, 38
    - gwiazda, 33, 35
    - hierarchiczna, 38
    - magistrala, 33, 34
    - pierścień, 33, 37
    - rozproszona gwiazda, 36
    - rozszerzona gwiazda, 36
    - siatka, 33, 37
  - topologia hybrydowa, 39
    - gwiazda — magistrala, 39
    - gwiazda — pierścień, 40
    - hierarchiczna gwiazda, 39
    - hybrydowa siatka, 40
  - topologia logiczna, 40
    - gwiazda, 41
    - łańcuch, 40
    - siatka, 42
  - topologia routingu, 76, 220, 219
  - topologia sieci, 33, 59, 60
    - sieć optyczna, 194
    - wyznaczanie liczby połączeń między wszystkimi węzłami, 34
  - Topology Change Acknowledgement, 237
  - Topology Change Notification, 237
  - Tor, 243, 244
  - Torbutton, 244
  - Torrent, 277
  - Toshiba Magnia, 268
  - TPA, 532
  - TPC-C V5.10, 141
  - TRACE, 615
  - traceroute, 70, 465, 805
  - tracerpt, 805
  - tracert, 70, 805
  - tracker, 277
  - traffic policing, 358
  - traffic shaping, 358
  - transakcje, 81
  - Transarc, 599
  - Transit, 486
  - translacja adresów sieciowych, 170, 212, 253
  - transmisja bezpołączeniowa, 55
  - transmisja danych, 31
  - transmisja punkt-punkt, 31
  - transmisja radiowa, 119
  - transmisja rozgłoszeniowa, 29, 32
  - transmisja sygnału binarnego, 28
  - transmisja wielopunktowa, 32
  - Transmission Control Block, 472
  - Transmission Control Protocol, 55, 61, 463, 464
  - transport danych, 47
  - transport IPsec, 753
  - Transport Layer Security, 702
  - trap, 98
  - TRAP, 98
  - trasowanie, 219
  - trasy, 64, 75, 85
  - trasy wsteczne, 225
  - Traversal Using NAT, 677
  - tree, 805
  - Trinax, 183
  - triple play, 260
  - Trouble Ticket, 768
  - trójkierunkowa kopia zapasowa NDMP, 420
  - TruUnix, 553
  - trwałe połączenia fizyczne, 94
  - tryb pełnego duplexu, 49
  - tryb półdupleksowy, 49
  - TSR, 550
  - TTL, 207, 497, 511, 537
  - tunel VPN, 753
  - tunelowanie, 753
    - GRE, 754
    - IPsec, 754
    - L2F, 756
    - L2TP, 756
    - PPTP, 755
    - protokoły, 754
    - TSL, 755
    - tunelowanie punkt-punkt, 755
  - TURN, 677
  - twardy podział na strefy, 433
  - twierdzenie o próbkowaniu Nyquista-Shannona, 114
  - Twinax, 183
  - twisted-pair, 184
  - tworzenie
    - interfejs sieciowy, 163
    - łącza WDM, 118
    - model Markowa, 151
    - most sieciowy, 214
    - podsieci, 504
    - połączenia VPN, 749
  - tworzenie kopii zapasowej, 418
  - tworzenie kopii zapasowej bez udziału serwera, 419
  - TXT, 544
  - tylne drzwi, 693
  - tymczasowe połączenia, 94
  - typeperf, 806
  - typy MIME, 631
  - typy połączeń sieciowych, 95
- U**
- UBR, 125, 358
  - UDDI, 621
  - UDI, 174
  - udostępniający, 278

- UDP, 55, 69, 70, 79, 464, 475
  - datagramy, 475, 476
  - zastosowanie, 476
- udziały, 272
- UIDL, 636
- ujednolicony interfejs sterownika, 174
- układ ASIC, 158
- układanie kabli sieciowych, 179
- ukryte usługi, 245
- ULA, 520
- UML, 79
- umount, 800
- umowy dotyczące jakości usług, 125
- UMTS, 681
- UNC, 608
- UNDI, 174
- UNI, 357
- unicast, 59, 76, 219, 485
- Unicode, 109
- Unified Communications Manager, 669
- Unified Modeling Language, 79
- Uniform Driver Interface, 174
- Uniform Naming Convention, 608
- Uniform Resource Identifier, 575, 613
- Uniform Resource Name, 613
- unikanie kolizji, 73, 77, 381
- Unique Local Address, 520
- Universal ADSL, 343
- Universal Datagram Protocol, 476
- Universal Description, Discovery, and Integration, 621
- Universal Global Unique Identifier, 587
- Universal Network Device Interface, 174
- Universal Plug and Play, 495, 735
- Universal Serial Bus, 282
- uniwersalna magistrala szeregową, 282
- uniwersalny interfejs urządzenia sieciowego, 174
- Unix, 554
- UNIX, 70, 165
- unlodctr, 806
- Unreal media Server, 659
- Unshielded Twisted Pair, 178
- Unspecified Bit Rate, 125
- Untangle, 216
- uplink, 39, 186, 210
- UPN, 587
- UPnP, 495, 735
- uproszczony klient-serwer, 60, 82
  - serwer terminali, 82
  - X Window, 83
- UPSR, 350
- URG, 467, 468
- URI, 575, 613
- URL, 612
- URN, 613
- urządzenia, 48, 75, 209
  - DCE, 119, 300
  - DTE, 119, 300
  - HBA, 412
  - NAS, 424
  - PAD, 356
  - urządzenia przełączające, 208
  - urządzenia serwerowe, 131
  - urządzenia warstw 1. i 2, 209
  - urządzenie kończące obwód, 119
- USB, 30, 282, 409
  - EHCI, 283
  - grupy, 282
  - interfejsy, 283
  - kable, 284
  - komunikacja, 283
  - koncentrator, 282
  - potoki, 282
  - szybkość wymiany danych, 283
  - wtyczki, 284
  - zerowy punkt końcowy, 282
- USB 2.0, 283
- USB 3.0, 284
- User Datagram Protocol, 55, 464, 476
- User Principle Name, 587
- usługa wdzwaniana, 341
- usługi bezpołączeniowe, 50
- usługi DHCP, 91
- usługi dostępu zdalnego, 830
- usługi katalogowe, 528, 544, 567, 568, 572
  - Active Directory, 573, 587
  - Banyan VINES, 569
  - DAP, 582
  - delegowanie, 578
  - DNS, 568
  - domeny, 568, 570
  - DSA, 582
  - eDirectory, 585
  - IDA, 581
  - informacje dotyczące użytkowników, 581
  - jednokrotne logowanie, 574
  - kontrola dostępu bazująca na roli, 580
  - LDAP, 582, 584
  - listy ACL, 572
  - metadane, 572
  - migracja usługi katalogowej, 571
  - MIIS, 582
  - NIS, 583
  - organizowanie typów domen, 570
  - polityka, 576
  - przestrzenie nazw, 575
  - RBAC, 580
  - replikacja, 573
  - serwer domen, 571
  - StreetTalk, 569
  - synchronizacja, 573
  - topologie domen, 570
  - usługi tożsamości, 582
  - X.500, 582
  - zarządzanie polityką, 576
  - zarządzanie tożsamością, 581
  - zastosowanie, 572
- usługi określenia nazw, 527
  - ARP, 531
  - DNS, 527, 536
  - HOSTS, 528
  - LDAP, 528

- usługi określania nazw
  - NetBIOS, 534
  - usługi katalogowe, 544
  - WINS, 527, 535
- usługi plików, 593
  - DFS, 606
  - NFS, 599
  - Samba, 602
  - SMB, 600
- usługi połączeniowe, 50
- usługi rozgłoszeniowe, 91
- usługi rozpoznawania sieci, 90
- usługi sieciowe, 611, 620
  - architektura klient-serwer, 621
  - dane, 620
  - HTTP, 611, 612
  - rejestr, 621
  - REST, 622
  - RPC, 620, 622
  - SOA, 622
  - SOAP, 620, 621
  - UDDI, 621
  - wiadomości, 620
  - WSDA, 620
  - WSDL, 621
  - WSDM, 622
  - zdalne wywoływanie procedur, 622
- usługi warstwy aplikacji, 55
- ustawianie adresu IP, 505
  - adresowanie dynamiczne, 508
  - adresowanie statyczne, 507
- usterki, 764
- utilization law, 144
- UTP, 178, 180, 182
- uuencoding, 635
- UUID, 587
- uwierzytelnianie, 782, 834
- użytkownik usługi, 49

## **V**

- Value Added Resellers, 666
- vampire tap, 187
- VANET, 393
- VAR, 666
- Variable Bit Rate, 656
- Variable Length Subnet Mask, 490
- VBR, 358, 656, 657
- VCS, 267
- vdisk, 412
- VDSL, 261, 345
- VDSL2, 345
- Vehicular Wireless Ad Hoc Mesh Network, 393
- Verizon, 341
- VIA, 429, 441, 448, 449
  - komponenty systemu, 450
  - reguła 80/80, 450
  - VIPL, 451
- Vidalia, 244
- Video on Demand, 647
- VINES, 569
- VINES Internetwork Protocol, 569
- VIP, 569
- VIPL, 451
- Virtual Carrier Sense, 267
- virtual disk, 412
- Virtual Interface Architecture, 429, 441, 442, 448, 449, 460
- Virtual Local Area Network, 672
- Virtual Network Computing, 832
- Virtual Private LAN Service, 225
- Virtual Private Network, 67, 741
- Virtual Private Network Consortium, 746
- Virtual Server, 94
- Virtual Storage Area Networks, 414
- Vistumbler, 402
- VLAN, 212, 217, 242, 307, 672
  - ramki, 307
- VLAN ID, 307
- VLAN-ie, 242
- VLSM, 488, 490
- VMWare, 94
- VNC, 832
- VOD, 647
- Voice over IP, 121, 465, 476, 515, 665, 671
- VoIP, 121, 465, 476, 515, 665, 671
  - adapter ATA, 672
  - bramka VoIP, 672
  - H.323, 677
  - IAX, 677
  - implementacja usług, 671
  - konwersja DAC, 671
  - MGCP, 678
  - NAT, 676
  - protokoły, 675
  - RTP, 676
  - SCCP, 674, 676
  - SIP, 674, 675
  - STUN, 677
  - telefony, 674
  - zastosowanie, 673
- VPLS, 225, 746, 747
- VPN, 67, 95, 741, 827
  - AAA, 746
  - bezpieczny VPN, 743
  - ekstranetowe łącza WAN, 743
  - hybrydowy VPN, 743
  - intranetowe łącza WAN, 743
  - IPLS, 746
  - klient, 750
  - łącza, 743
  - łącze zdalnego dostępu, 743
  - M2M VPN, 746
  - metody transportowe, 743
  - oprogramowanie, 747
  - połączenia, 749
  - protokoły tunelowania, 754
  - rodzaje sieci, 742
  - site-to-site, 745, 746
  - szyfrowanie, 752
  - technologie, 742

topologie połączeń między lokacjami, 745  
 tunelowanie, 753  
 tunelowy VPN, 743  
 urządzenia, 746  
 VPLS, 746  
 wewnętrzne łącze sieci LAN, 743  
 Windows Server 2008, 749  
 VPNC, 746  
 VSAN, 414  
 VSHARE.386, 272  
 VT, 305

## W

w (polecenie), 806  
 w pełni połączona sieć siatkowa, 38  
 w32tm, 806  
 W3C, 45  
 WAFL, 424  
 WAIK, 774  
 wampir, 187  
 WAN, 27, 31, 32, 258, 335, 336  
     sieć pakietowa, 32  
 WAN PHY, 445  
 WAP, 385  
 wardriving, 400  
 warstwa aplikacji, 54  
 warstwa dostępu do sieci, 55  
 warstwa fizyczna, 50  
 warstwa łączy danych, 51, 61  
 warstwa międzysieciowa stosu TCP/IP, 61  
 warstwa prezentacji, 54  
 warstwa sesji, 53  
 warstwa sieciowa, 52  
 warstwa transportowa, 53, 55  
 warstwy modelu OSI, 46  
     warstwa aplikacji, 46, 54  
     warstwa fizyczna, 46, 50  
     warstwa łączy danych, 46, 51  
     warstwa prezentacji, 46, 54  
     warstwa sesji, 46, 53  
     warstwa sieciowa, 46, 52  
     warstwa transportowa, 46, 53  
 warstwy modelu TCP/IP, 55  
 warstwy stosu Ethernet, 304  
 wartości hash, 710  
 Wavelength Division Multiplexing, 117, 118  
 ważony algorytm RED, 219  
 WBEM, 90, 101  
 wbudowane grupy użytkowników, 580  
 WCF, 79  
 wczesne losowe wykrywanie, 218  
 WDM, 101, 117, 118, 346, 352  
 wdrażanie, 771  
 wdrażanie usług, 135  
 WDS, 388, 389  
     połączenia, 389  
     SSI, 389  
     tryby pracy, 388  
 weakly collision-free, 710  
 Web Cache Control Protocol, 738  
 web proxy, 737  
 Web Services Description Language, 620  
 Web Services Distributed Management, 622  
 Web Services Interoperability Organization, 621  
 Web Services Resource Framework, 621  
 Web2Mail, 637  
 Web-Based Enterprise Management, 90, 438  
 WEBM, 438, 764  
 Webmail, 637  
 wektor IV, 403  
 wektor odległości, 221  
 wektor ścieżki, 229, 362  
 Well-Known Services, 544  
 WEP, 385, 389, 402, 709  
     zasada działania, 403  
 wewnętrzna sieć LAN, 726  
 wewnętrzna zaporą sieciową, 726  
 wewnętrzny BGP, 231  
 węzeł centralny, 37  
 węzły dystrybucyjne, 178  
 węzły rozgłaszające, 230  
 WhatsUp Gold, 98, 103  
 whois, 806  
 wiadomości e-mail, 625  
     kodowanie Base64, 633  
     wiadomości w częściach, 628  
 wiadomości ICMP, 511  
 wiadomości SOAP, 620  
 wiadro, 122  
 wiadro z żetonami, 121, 123  
 wiązka, 307, 319  
 Wide Area Network, 31, 335  
 wideo na żądanie, 647  
 wideotelefony, 679  
     kamery internetowe, 681  
     Mobile VoIP, 680  
 widmo elektromagnetyczne, 199  
 widmo sygnału FHSS, 376  
 wielkość okna, 465  
 wielodostęp z podziałem czasu, 115  
 wielodostęp z podziałem częstotliwości, 117, 298  
 wielodostęp z wykrywaniem nośnej i detekcją kolizji, 73  
 wielodostęp z wykrywaniem nośnej i unikaniem kolizji, 73  
 wielodostęp ze zwielokrotnieniem kodowym, 119  
 wielokanałowy system rozgłoszeniowy, 300  
 wielopunktowe sieci prywatne, 746  
 wielostanowiskowa jednostka dostępową, 37  
 Wi-Fi, 28, 202, 253, 254, 325, 365, 367, 681  
 WIM, 772  
 WiMAX, 342, 681  
 Windows, 78, 553  
 Windows CE, 82  
 Windows Datacenter Edition, 564  
 Windows Driver Model, 101  
 Windows Home Server, 269, 564  
 Windows Imaging Format, 772  
 Windows Internet Name Service, 527, 535, 603  
 Windows Live, 664  
 Windows Live Messenger, 681

Windows Management Instrumentation, 90, 101, 438  
Windows Media Encoder, 657  
Windows Media Services, 658  
Windows NetShell, 807  
Windows Plug and Play, 173  
Windows Presentation Framework, 664  
Windows Script Host, 791  
Windows Server, 564  
Windows Server 2008, 82, 565  
Windows Small Business Server, 564  
Windows Storage Server, 564  
Windows Storage Server 2003 R2, 596  
Windows System Image Manager, 774  
WinMX, 274  
WINS, 93, 527, 535, 603  
Wirecast, 657  
Wired Equivalent Privacy, 402  
Wireless Distribution System, 388  
Wireless Network Connection Status, 400  
wiring closet, 178  
wirtualizacja pamięci masowej, 412  
wirtualizacja systemów, 94  
wirtualne połączenia punkt-punkt, 64  
    tabela stanów, 64  
wirtualne sieci LAN, 217  
wirtualne sieci prywatne, 67, 95, 741  
wirtualny interfejs sieciowy, 64, 94  
wirtualny punkt końcowy, 94  
wish, 791  
witryny WWW, 160  
WKS, 544  
własność Markowa, 151  
włókno optyczne, 178, 192  
    włókna jednomodowe, 187  
WMI, 90, 97, 101, 438  
    CIM, 101  
    DMI, 101  
    gromadzenie danych z węzłów SNMP, 101  
    operacje, 101  
    WQL, 101  
WMI Query Language, 101  
WMIC, 438  
WMN, 393  
World Wide Name, 414, 432  
World Wide Web Consortium, 45  
Wowza Media Server 2, 658  
WPA, 385, 404  
WPA Enterprise, 405  
WPA Personal, 405  
WPA2, 404  
WPA-PSK, 389, 405  
WPF, 664  
WPSN VPN, 746  
WQL, 101  
Write Anywhere File Layout, 424  
WSDA, 620  
WSDL, 621  
WSDM, 622  
wsh, 791  
WS-I, 621

WS-Management, 764  
współczynnik rozgałęzienia, 39  
współdzielenie plików, 602  
współdzielenie rozproszonych zasobów, 272  
współdzielone taśmy, 415  
WSRF, 621  
wstawienie, 276  
wtyczka RJ-45, 181  
wtyczki USB, 284  
WWID, 432  
WWN, 414, 432  
WWPN, 432  
wydajne systemy obliczeniowe, 442  
wydajność, 62  
wyrzebywanie CPU, 458  
wyrzebywanie cykli, 458  
wykorzystanie dysku, 143  
wykorzystanie pamięci, 143  
wykorzystanie sieci, 143  
wykorzystanie zasobów, 143  
wykrywanie kolizji, 73  
wykrywanie zagrożeń, 694  
wyprzedzająca korekcja błędów, 265  
wysoka wydajność, 159  
wysyłanie wiadomości e-mail, 626, 627  
wytlumianie sygnału, 74  
wytyczne związane z zarządzaniem zasobami IT, 135  
wyznaczanie najkrótszej trasy w grafie, 222

## X

X Window, 82, 83, 832  
X.25, 206, 355, 544  
    DCE, 356  
    DTE, 356  
    PAD, 356  
    wirtualne połączenia, 356  
X.28, 356  
X.29, 356  
X.3, 356  
X.400, 628  
X.500, 528, 544, 567, 582  
    DAP, 582  
    DISP, 582  
    DOP, 583  
    DSP, 583  
    protokoły, 582  
    shadowing, 582  
X.500 Directory Access Protocol, 582  
X.511, 582  
X10, 294, 318, 319, 325  
    adresy, 322  
    kody poleceń, 321  
    kontroler, 319  
    ramki, 319  
    sterowanie oświetleniem, 322  
    wiązki, 320  
X11, 83, 559, 832  
X-Architecture, 78  
xcopy, 806

XDR, 599  
Xen, 563  
Xerox Network Services, 550, 569  
Xerox PARC, 300, 311  
xinit, 806  
XML, 620  
XNS, 569  
XO, 393  
XoloX, 274  
XON/XOFF, 120  
XOR, 709  
XORP, 216

## Y

Yagi, 396  
Yahoo! Mail, 637  
YouTube.com, 644

## Z

zajętość procesora, 143  
zakłócenia, 396  
zakłócenia elektromagnetyczne, 180  
zakłócenia EMI, 181  
zakłócenia radiowe, 180  
zakresy częstotliwości, 197  
zależności wydajnościowe, 143  
zależność nadrzędny-podrzędny, 120  
zamiana adresów sieciowych na nazwy, 86  
zamykanie połączenia TCP, 470  
zapaść z powodu przeciążenia, 481  
zapewnianie jakości usługi, 106  
zapisz i przekaz, 121  
zapora sieciowa, 695, 717, 718  
    analiza połączeń, 719  
    brzegowa zapora sieciowa, 725  
    DMZ, 725  
    filtrowanie aplikacji, 720  
    filtrowanie pakietów, 719, 727  
    filtry aplikacji, 730  
    filtry bezstanowe, 727  
    filtry stanu, 727  
    funkcje zapory, 718  
    kategorie zapór, 718  
    NAT, 719, 732  
    osobista zapora sieciowa, 720  
    proxy, 719, 723, 726  
    router, 721  
    sieć prywatna, 726  
    SPI, 721, 727  
    sprzętowe zapory sieciowe, 722  
    stan domyślnie odmawiaj, 731  
    Stateful Inspection, 719  
    strefy sieciowe, 725  
    tłumaczenie adresów sieciowych, 732  
    wewnętrzna zapora sieciowa, 726  
Zapora systemu Windows, 720  
zapotrzebowanie na usługę, 145

zarządzanie bezpieczeństwem, 782  
zarządzanie konfiguracją, 769  
    cykl życiowy oprogramowania, 771  
    instalacja „od zera”, 776  
    konsole, 769  
    monitorowanie, 775  
    pliki obrazów, 772  
    poprawki, 776  
    systemy zinventoryzowane lub przeznaczone do implementacji, 772  
    uaktualnienia, 776  
    wdrażanie, 771  
zarządzanie polityką grupy, 576  
zarządzanie rozliczeniami, 778  
zarządzanie siecią, 761, 762  
    FCAPS, 762  
    oprogramowanie, 783, 785  
    platformy sieciowe, 784  
    sieć SAN, 438  
    standardy, 762  
zarządzanie szybkością transmisji danych, 52  
zarządzanie tożsamością, 581  
zarządzanie usterkami, 764  
    alarmy, 766  
    korelacja zdarzeń, 767  
    pliki dzienników zdarzeń, 765  
zarządzanie wydajnością, 779  
zasilanie przez Ethernet, 262  
zatory, 148  
zbieranie informacji o sieci, 85, 86  
    główna przeglądarka, 87  
    komunikacja bezpośrednia, 89  
    lista elementów sieciowych, 87  
    lista przeglądania, 87  
    mechanizm przeglądania, 88  
    mechanizm rozgłaszania dostępności urządzeń, 87  
    obwód, 94  
    odpytywanie, 88, 93  
    połączenia sieciowe, 94  
    przeglądanie sieci, 91  
    publikowanie informacji o węzle, 90  
    SNMP, 90, 96  
    usługi rozgłoszeniowe, 91  
    WMI, 90  
zdalne wywoływanie procedur, 600  
zdalny dostęp, 827  
zdolność do adaptacji, 142  
Zenmap, 102  
ZENworks, 576, 577  
Zero Configuration Networking, 495  
Zero Copy Network, 448  
    Virtual Interface Architecture, 449  
Zero Day Exploit, 688, 689  
zestaw ASCII, 109  
zestaw protokołów internetowych, 61  
Zettabyte File System, 563  
zewnętrzny BGP, 231  
ZFS, 563  
ZigBee, 325, 378  
zintegrowany protokół IS-IS, 229

## złącza

- BNC, 70, 185
- FireWire 400, 286
- typ D, 187
- typ N, 187
- złączanie wiązek światła w systemie WDM, 118
- zmiana kolejności powiązań, 166
- zmiennosc opóźnienia komórek, 126
- znacznik, 37
- znaczniki RFID, 536
- zniekształcenia, 380
- zoning, 432
- zorientowane plikowo serwery pamięci masowej, 424
- zorientowany blokowo system pamięci, 425
- Z-Wave, 325
- zwiększona wydajność, 168
- zwrot z inwestycji, 762
- zysk anteny, 396
- zysk kodowy, 377
- zysk przetwarzania, 377

**Ż**

## żądania

- ARP, 531
- DNS, 537
- HTTP, 613
- RARP, 532
- żądanie nadawania, 120
- żądanie połączenia, 50



# 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>

GRUPA WYDAWNICZA

 **Helion SA**