

WYDANIE V

Hellon



SIECI KOMPUTEROWE



TANENBAUM | WETHERALL

Najpopularniejsze na świecie wprowadzenie do sieci komputerowych
— w pełni zaktualizowane i przygotowane na technologie przyszłości

Tytuł oryginału: Computer Networks (5th Edition)

Tłumaczenie: Przemysław Szeremiota na podstawie „Sieci komputerowe” w tłumaczeniu Andrzej Grażyńskiego i Adama Jarczyka

ISBN: 978-83-246-3079-0

Polish edition copyright © 2012 by Helion S.A.

All rights reserved.

Authorized translation from the English language edition, entitled: COMPUTER NETWORKS, Fifth Edition; ISBN 0132126958; by Andrew S. Tanenbaum; and David J. Wetherall; published by Pearson Education, Inc, publishing as Prentice Hall. Copyright © 2011, 2003, 1996, 1989, 1981 by Pearson Education, Inc.

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

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

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

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

Wydawnictwo HELION

ul. Kościuszki 1c, 44-100 GLIWICE

tel. 32 231 22 19, 32 230 98 63

e-mail: helion@helion.pl

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

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<http://helion.pl/user/opinie?gimpbi>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

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

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

SPIS TREŚCI

Wstęp	17
1. Wprowadzenie	21
1.1. Zastosowania sieci komputerowych	23
1.1.1. Zastosowania w biznesie	23
1.1.2. Zastosowania domowe	26
1.1.3. Użytkownicy mobilni	31
1.1.4. Kwestie społeczne	34
1.2. Sprzęt sieciowy	38
1.2.1. Sieci osobiste	39
1.2.2. Sieci lokalne	40
1.2.3. Sieci miejskie	44
1.2.4. Sieci rozległe	46
1.2.5. Sieci złożone	49
1.3. Oprogramowanie sieciowe	50
1.3.1. Hierarchie protokołów	51
1.3.2. Zagadnienia projektowania warstw	55
1.3.3. Usługi połączeniowe i bezpołączeniowe	57
1.3.4. Funkcje podstawowe usług	60
1.3.5. Związki usług z protokołami	62

1.4.	Modele odniesienia	63
1.4.1.	Model odniesienia OSI	63
1.4.2.	Model odniesienia TCP/IP	67
1.4.3.	Model omawiany w książce	70
1.4.4.	Porównanie modeli odniesienia OSI i TCP/IP*	71
1.4.5.	Krytyka modelu i protokołów OSI*	73
1.4.6.	Krytyka modelu odniesienia TCP/IP*	75
1.5.	Przykłady sieci	76
1.5.1.	Internet	76
1.5.2.	Sieci komórkowe trzeciej generacji*	87
1.5.3.	Bezprzewodowe sieci lokalne — 802.11*	92
1.5.4.	RFID i sieci sensorowe*	96
1.6.	Standaryzacja sieci*	99
1.6.1.	Kto jest kim w świecie telekomunikacji?	100
1.6.2.	Kto jest kim w świecie standardów międzynarodowych?	102
1.6.3.	Kto jest kim w świecie standardów internetowych?	103
1.7.	Jednostki metryczne	105
1.8.	Zarys pozostałej części książki	106
1.9.	Podsumowanie	108

2. Warstwa fizyczna

113

2.1.	Teoretyczne podstawy transmisji danych	114
2.1.1.	Analiza Fouriera	114
2.1.2.	Sygnały z ograniczonym pasmem	114
2.1.3.	Maksymalna przepływność kanału	118
2.2.	Kierowane nośniki transmisji	119
2.2.1.	Nośniki magnetyczne	119
2.2.2.	Skrętka	120
2.2.3.	Kabel koncentryczny	122
2.2.4.	Linie zasilające	123
2.2.5.	Światłowody	124
2.3.	Transmisja bezprzewodowa	130
2.3.1.	Widmo elektromagnetyczne	130
2.3.2.	Transmisja radiowa	133
2.3.3.	Transmisja mikrofalowa	135
2.3.4.	Fale milimetrowe i podczerwień	138
2.3.5.	Transmisja optyczna	139

2.4.	Satelity telekomunikacyjne*	141
2.4.1.	Satelity geostacjonarne	142
2.4.2.	Satelity na orbitach średnich	146
2.4.3.	Satelity na orbitach niskich	146
2.4.4.	Satelity kontra światłowod	148
2.5.	Modulacja cyfrowa i multipleksacja	150
2.5.1.	Transmisja w paśmie podstawowym	150
2.5.2.	Transmisja w paśmie przepustowym	156
2.5.3.	Multipleksacja z podziałem częstotliwości	158
2.5.4.	Multipleksacja z podziałem czasu	161
2.5.5.	Multipleksacja na bazie sekwencji rozpraszających	161
2.6.	Publiczna komutowana sieć telefoniczna	165
2.6.1.	Struktura systemu telefonicznego	166
2.6.2.	Pętla lokalna — modemy, ADSL i światłowody	168
2.6.3.	Łączy dalekosiężne i multipleksacja	177
2.6.4.	Komutacja	186
2.7.	Systemy telefonii mobilnej*	190
2.7.1.	Telefony mobilne pierwszej generacji (1G) — głosowe analogowe	192
2.7.2.	Telefony mobilne drugiej generacji (2G) — głosowe cyfrowe	195
2.7.3.	Telefony mobilne trzeciej generacji (3G) — cyfrowy głos i dane	200
2.8.	Telewizja kablowa*	206
2.8.1.	Telewizja i anteny zbiorcze	206
2.8.2.	Internet w kablówce	207
2.8.3.	Przydziały pasma	208
2.8.4.	Modemy kablówce	210
2.8.5.	ADSL czy kabel?	212
2.9.	Podsumowanie	213

3. Warstwa łącza danych

221

3.1.	Problemy projektowe warstwy łącza danych	222
3.1.1.	Usługi świadczone dla warstwy sieciowej	222
3.1.2.	Ramkowanie	225
3.1.3.	Kontrola błędów	229
3.1.4.	Sterowanie przepływem	230
3.2.	Wykrywanie i korekcja błędów	231
3.2.1.	Kody korekcyjne	233
3.2.2.	Kody detekcyjne	239

3.3.	Podstawowe protokoły łącza danych	245
3.3.1.	Przykładowy protokół simpleksowy	250
3.3.2.	Simpleksowy protokół stop-and-wait dla kanału wolnego od błędów	251
3.3.3.	Protokół simpleksowy dla kanału z zakłóceniami	253
3.4.	Protokoły z oknem przesuwным	257
3.4.1.	Protokół z jednobitowym oknem przesuwным	260
3.4.2.	Protokół używający techniki „wróć do n”	262
3.4.3.	Protokół używający powtórzeń selektywnych	269
3.5.	Przykładowe protokoły łącza danych	275
3.5.1.	Pakiety w sieci SONET	275
3.5.2.	ADSL (Asymmetric Digital Subscriber Loop)	279
3.6.	Podsumowanie	282

4. Podwarstwa kontroli dostępu do nośnika 287

4.1.	Problem przydzielania kanału	288
4.1.1.	Statyczne przydzielanie kanałów	288
4.1.2.	Założenia dla dynamicznego przydzielania kanału w sieciach	290
4.2.	Protokoły dostępu wielokrotnego	292
4.2.1.	ALOHA	292
4.2.2.	Protokoły dostępu wielokrotnego z wykrywaniem nośnej	297
4.2.3.	Protokoły bezkolizyjne	300
4.2.4.	Protokoły z ograniczoną rywalizacją	304
4.2.5.	Protokoły bezprzewodowych sieci LAN	308
4.3.	Ethernet	311
4.3.1.	Warstwa fizyczna klasycznego Ethernetu	312
4.3.2.	Protokół podwarstwy MAC klasycznego Ethernetu	313
4.3.3.	Wydajność sieci Ethernet	317
4.3.4.	Przełączany Ethernet	319
4.3.5.	Fast Ethernet	322
4.3.6.	Gigabit Ethernet	325
4.3.7.	Ethernet 10-gigabitowy	329
4.3.8.	Ethernet z perspektywy czasu	330
4.4.	Bezprzewodowe sieci lokalne	332
4.4.1.	Architektura i stos protokołów 802.11	332
4.4.2.	Warstwa fizyczna 802.11	334
4.4.3.	Protokół podwarstwy MAC w 802.11	336
4.4.4.	Struktura ramki 802.11	343
4.4.5.	Usługi	345

4.5.	Szerokopasmowe łącza bezprzewodowe*	347
4.5.1.	Porównanie 802.16, 802.11 i telefonii komórkowej 3G	348
4.5.2.	Architektura i stos protokołów 802.16	349
4.5.3.	Warstwa fizyczna 802.16	350
4.5.4.	Protokół podwarstwy MAC 802.16	352
4.5.5.	Struktura ramki 802.16	354
4.6.	Bluetooth*	355
4.6.1.	Architektura Bluetooth	355
4.6.2.	Zastosowania Bluetooth	356
4.6.3.	Stos protokołów Bluetooth	358
4.6.4.	Warstwa radiowa w Bluetooth	359
4.6.5.	Warstwy łącza Bluetooth	359
4.6.6.	Struktura ramki Bluetooth	361
4.7.	RFID*	363
4.7.1.	Architektura EPC Gen 2	363
4.7.2.	Warstwa fizyczna EPC Gen 2	364
4.7.3.	Warstwa identyfikacji znacznika EPC Gen 2	365
4.7.4.	Formaty komunikatów identyfikacji znaczników	367
4.8.	Przełączanie w warstwie łącza danych	368
4.8.1.	Zastosowania mostów	369
4.8.2.	Podstawy działania mostów	370
4.8.3.	Drzewa częściowe mostów	374
4.8.4.	Wzmacniaki, koncentratory, mosty, przełączniki, routery i bramy	377
4.8.5.	Wirtualne sieci LAN	380
4.9.	Podsumowanie	387

5. Warstwa sieciowa

393

5.1.	Problemy projektowe warstwy sieciowej	393
5.1.1.	Komutacja pakietów z buforowaniem	394
5.1.2.	Usługi świadczone na rzecz warstwy transportowej	394
5.1.3.	Implementacja usługi bezpołączeniowej	396
5.1.4.	Implementacja usługi połączeniowej	397
5.1.5.	Porównanie sieci obwodów wirtualnych i datagramowych	398
5.2.	Algorytmy routingu	400
5.2.1.	Zasada optymalności	402
5.2.2.	Algorytm z wyborem najkrótszej ścieżki	403
5.2.3.	Routing rozpiływowy	406
5.2.4.	Routing z użyciem wektorów odległości	408
5.2.5.	Routing z użyciem stanów połączeń	411

5.2.6. Routing hierarchiczny	416
5.2.7. Routing rozgłoszeniowy	418
5.2.8. Routing rozsyłania grupowego	420
5.2.9. Rozprowadzanie do najbliższego węzła (anycast)	424
5.2.10. Routing dla hostów mobilnych	425
5.2.11. Routing w sieciach ad hoc	427
5.3. Algorytmy kontroli przeciążeń	431
5.3.1. Metody kontroli przeciążeń	433
5.3.2. Routing z uwzględnieniem warunków ruchu	435
5.3.3. Kontrola dopuszczenia do sieci	436
5.3.4. Dławienie ruchu	437
5.3.5. Zrzut obciążenia	442
5.4. Jakość obsługi	444
5.4.1. Wymogi	445
5.4.2. Kształtowanie ruchu	447
5.4.3. Szeregowanie pakietów	451
5.4.4. Kontrola dopuszczenia	455
5.4.5. Usługi zintegrowane	459
5.4.6. Usługi zróżnicowane	462
5.5. Sieci złożone	465
5.5.1. Różnice między sieciami	467
5.5.2. Łączenie sieci	468
5.5.3. Tunelowanie	471
5.5.4. Routing w sieciach złożonych	473
5.5.5. Fragmentacja pakietów	474
5.6. Warstwa sieciowa w Internecie	478
5.6.1. Protokół IPv4	481
5.6.2. Adresy IP	485
5.6.3. IPv6	498
5.6.4. Internetowe protokoły sterujące	508
5.6.5. Etykietowanie i MPLS	514
5.6.6. OSPF — protokół bram wewnętrznych	517
5.6.7. Protokół bram zewnętrznych BGP	522
5.6.8. Rozsyłanie grupowe w Internecie	528
5.6.9. Mobilny IP	529
5.7. Podsumowanie	533

6. Warstwa transportowa

539

6.1. Usługa transportowa	539
6.1.1. Usługi świadczone na rzecz wyższych warstw	540

6.1.2. Prymitywy usług transportowych	542
6.1.3. Gniazda Berkeley Sockets	546
6.1.4. Przykład programowania — internetowy serwer plików	548
6.2. Elementy protokołów transportowych	553
6.2.1. Adresowanie	555
6.2.2. Ustanawianie połączenia	558
6.2.3. Zwalnianie połączenia	564
6.2.4. Kontrola błędów i sterowanie przepływem	569
6.2.5. Multipleksacja	575
6.2.6. Odtwarzanie po awarii	576
6.3. Kontrola przeciążeń	579
6.3.1. Skuteczna alokacja przepustowości	579
6.3.2. Regulacja prędkości wysyłania danych	584
6.3.3. Kwestie dotyczące sieci bezprzewodowych	589
6.4. Internetowe protokoły transportowe — UDP	592
6.4.1. Wprowadzenie do protokołu UDP	592
6.4.2. Zdalne wywołania procedur	594
6.4.3. Protokoły transportowe czasu rzeczywistego	598
6.5. Internetowe protokoły transportowe — TCP	605
6.5.1. Wprowadzenie do TCP	605
6.5.2. Model usługi TCP	606
6.5.3. Protokół TCP	609
6.5.4. Nagłówki segmentu TCP	611
6.5.5. Nawiązywanie połączenia TCP	615
6.5.6. Zwalnianie połączenia TCP	616
6.5.7. Model TCP zarządzania połączeniami	617
6.5.8. Okna przesuwne	620
6.5.9. Zarządzanie czasem przez TCP	624
6.5.10. Kontrola przeciążeń w TCP	627
6.5.11. Przyszłość protokołu TCP	638
6.6. Wydajność sieci*	639
6.6.1. Problemy związane z wydajnością sieci komputerowych	640
6.6.2. Pomiar wydajności sieci	641
6.6.3. Projektowanie hostów dla szybkich sieci	645
6.6.4. Szybkie przetwarzanie segmentów	649
6.6.5. Kompresja nagłówków	652
6.6.6. Protokoły dla szybkich sieci długodystansowych	655
6.7. Sieci niewrażliwe na opóźnienia*	660
6.7.1. Architektura sieci DTN	661
6.7.2. Protokół paczki	664
6.8. Podsumowanie	667

7. Warstwa aplikacji 673

7.1.	DNS — system nazw domen	673
7.1.1.	Przestrzeń nazw DNS	675
7.1.2.	Rekordy zasobów domenowych	678
7.1.3.	Serwery nazw	682
7.2.	Poczta elektroniczna*	686
7.2.1.	Architektura i usługi	688
7.2.2.	Agent użytkownika	690
7.2.3.	Formaty wiadomości	695
7.2.4.	Transfer wiadomości	704
7.2.5.	Protokoły dostarczania końcowego	710
7.3.	WWW	714
7.3.1.	Przegląd architektury WWW	715
7.3.2.	Statyczne dokumenty WWW	733
7.3.3.	Strony dynamiczne i aplikacje WWW	744
7.3.4.	HTTP — protokół przesyłu hipertekstu	757
7.3.5.	Mobilne WWW	769
7.3.6.	Wyszukiwanie w sieci WWW	772
7.4.	Strumieniowe transmisje wideo i dźwięku	774
7.4.1.	Dźwięk cyfrowy	776
7.4.2.	Cyfrowe wideo	782
7.4.3.	Strumieniowanie z dysku	792
7.4.4.	Strumieniowanie na żywo	801
7.4.5.	Telekonferencje	805
7.5.	Dystrybucja treści	816
7.5.1.	Treści a ruch w Internecie	818
7.5.2.	Farmy serwerów i serwery pośredniczące WWW	821
7.5.3.	Sieci dystrybucji treści	826
7.5.4.	Sieci równorzędne P2P	832
7.6.	Podsumowanie	843

8. Bezpieczeństwo w sieciach komputerowych 849

8.1.	Kryptografia	853
8.1.1.	Wprowadzenie do kryptografii	853
8.1.2.	Szyfry podstawieniowe	856
8.1.3.	Szyfry przestawieniowe	858

8.1.4. Systemy kluczy jednokrotnych	859
8.1.5. Dwie fundamentalne zasady kryptografii	864
8.2. Algorytmy szyfrowania z kluczami symetrycznymi	867
8.2.1. DES	869
8.2.2. AES	872
8.2.3. Tryby szyfrowania	876
8.2.4. Inne przykłady szyfrów	881
8.2.5. Kryptoanaliza	882
8.3. Algorytmy z kluczami publicznymi	883
8.3.1. RSA	884
8.3.2. Inne algorytmy szyfrowania z kluczem publicznym	886
8.4. Podpis cyfrowy	887
8.4.1. Podpisy oparte na kluczach symetrycznych	888
8.4.2. Podpisy oparte na kluczach publicznych	889
8.4.3. Skróty komunikatów	891
8.4.4. Atak urodzinowy	895
8.5. Zarządzanie kluczami publicznymi	898
8.5.1. Certyfikaty	898
8.5.2. X.509	900
8.5.3. Infrastruktura kluczy publicznych	901
8.6. Bezpieczeństwo komunikacji	904
8.6.1. IPsec	905
8.6.2. Zapory sieciowe	909
8.6.3. Prywatne sieci wirtualne	913
8.6.4. Bezpieczeństwo w sieciach bezprzewodowych	915
8.7. Protokoły uwierzytelniania	920
8.7.1. Uwierzytelnianie w oparciu o współdzielony tajny klucz	921
8.7.2. Ustanawianie dzielonego klucza: metoda Diffiego-Hellmana wymiany kluczy	926
8.7.3. Uwierzytelnianie z udziałem centrum dystrybucji kluczy	928
8.7.4. Uwierzytelnianie w oparciu o Kerberos	931
8.7.5. Uwierzytelnianie z użyciem kluczy publicznych	933
8.8. Bezpieczeństwo poczty elektronicznej*	934
8.8.1. PGP	935
8.8.2. S/MIME	939
8.9. Bezpieczeństwo WWW	940
8.9.1. Zagrożenia	940
8.9.2. Bezpieczne nazewnictwo	941
8.9.3. SSL	947
8.9.4. Bezpieczeństwo ruchomego kodu	951

8.10.	Spoleczne aspekty sieci komputerowych	955
8.10.1.	Ochrona prywatności	955
8.10.2.	Wolność słowa	958
8.10.3.	Prawa autorskie	962
8.11.	Podsumowanie	965
9.	Bibliografia i literatura uzupełniająca	973
9.1.	Zalecana literatura uzupełniająca*	973
9.1.1.	Wprowadzenie i zagadnienia ogólne	974
9.1.2.	Warstwa fizyczna	975
9.1.3.	Warstwa łączy danych	976
9.1.4.	Podwarstwa sterowania dostępem do nośnika	976
9.1.5.	Warstwa sieciowa	977
9.1.6.	Warstwa transportowa	978
9.1.7.	Warstwa aplikacji	978
9.1.8.	Bezpieczeństwo sieciowe	979
9.2.	Bibliografia w układzie alfabetycznym*	981
	Skorowidz	999
	O autorach	1023

5.3. ALGORYTMY KONTROLI PRZECIĄŻEŃ

Nadmierna liczba pakietów obecna w sieci albo w jej części doprowadza do opóźnienia rozprowadzania pakietów i w efekcie do utraty wydajności. Sytuacja taka nosi nazwę **przeciążenia**. Odpowiedzialność za radzenie sobie z przeciążeniami ruchu jest podzielona pomiędzy warstwę sieciową i transportową. Skoro do przeciążeń dochodzi w sieci, doświadcza ich przede wszystkim warstwa sieciowa i to ona ostatecznie musi zaradzić powstałemu problemowi nadmiaru pakietów. Z drugiej strony, obciążenie wynika z natężenia ruchu przenoszonego przez warstwę transportową. Dlatego dla skutecznego unikania i eliminowania przeciążeń konieczna jest współpraca warstwy sieciowej i transportowej. W tym rozdziale przyjrzymy się aspektom przeciążeń w warstwie sieciowej. Temat przeciążeń dokończymy, omawiając aspekty warstwy transportowej w rozdziale 6.

Rysunek 5.19 ilustruje rozwój przeciążenia sieciowego. Kiedy liczba pakietów wysyłanych do sieci przez stację mieści się w zakresie zdolności przenoszenia sieci, liczba pakietów dostarczonych jest wprost proporcjonalna do liczby pakietów wysłanych. Kiedy host wysyła dwukrotnie więcej pakietów, odbiorca też dostanie ich dwa razy więcej.



Rysunek 5.19. Przy nadmiernym ruchu efektywność sieci zaczyna maleć

Ale kiedy liczba ta będzie zbliżać się do granicznej przepustowości sieci, serie pakietów mogą momentami doprowadzać do wysycenia buforów w routerach rozprawiających pakiety, co z kolei oznacza utratę niektórych pakietów. Utracone pakiety zużywały pewną część przepustowości, więc liczba pakietów dostarczonych zaczyna być mniejsza od liczby pakietów wysłanych — krzywa dostarczania zaczyna odbiegać od prostej. Mówimy wtedy o przeciążeniu sieci.

Jeśli sieć jest słabo zaprojektowana, może w niej dojść do zapaści, gdy liczba wysyłanych pakietów przekroczy przepustowość sieci. Może to być wynikiem choćby tego, że opóźnienie rozprawiania pakietów może je unieważniać w miejscu przeznaczenia. Na przykład we wczesnej fazie rozwoju Internetu czas, jaki pakiet spędzał w oczekiwaniu na rozprawienie na powolnym, 56-kilobitowym łączu, mógł przekraczać czas, po którym nadawca decyduje się na ponowne wysłanie pakietu z powodu braku potwierdzenia odebrania. Dochodzi wtedy do powielania pakietów wysyłanych do sieci, co niewątpliwie zwiększa przeciążenie i zmniejsza jej wydajność. Na osi y na rysunku 5.19 zaznaczono więc wartość skutecznego dostarczania, to znaczy liczbę przydatnych pakietów przenoszonych przez sieć.

Pożądana jest sieć, w której do przeciążeń nie dochodzi, a już na pewno nie dochodzi do zapaści w wyniku przeciążenia. Niestety, przeciążenia nie zawsze da się uniknąć. Jeśli nagle strumień pakietów zaczął przychodzić na trzech lub czterech liniach wejściowych i wszystkie będą wymagały tej samej linii wyjściowej, powstanie kolejka. Jeżeli w pamięci braknie miejsca na wszystkie te dane, pakiety zaczną się gubić. Rozbudowa pamięci może pomóc do pewnego punktu, lecz Nagle (1987) uzmysłowił nam, że gdyby routery miały nieskończoną pojemność pamięci, przeciążenia stałyby się większe, a nie mniejsze, ponieważ do czasu dotarcia do początku kolejki pakiety traciłyby ważność (raz za razem) i źródło wysyłałoby duplikaty, co nie poprawia sytuacji, tylko ją pogarsza — prowadzi bowiem wprost do zapaści.

Źródłem przeciążeń sieci są również łącza o niskiej przepustowości albo routery, które przetwarzają pakiety wolniej, niż one napływają. W takim przypadku sytuację można poprawić poprzez kierowanie części ruchu poza wąskie gardła sieci; ostatecznie

jednak przy stałym wzroście ruchu przeciążenie musi objąć wszystkie regiony sieci. W takiej sytuacji nie ma wyjścia: trzeba albo okroić ruch, albo zbudować szybszą sieć.

Warto tu wyjaśnić różnicę pomiędzy kontrolą przeciążeń i sterowaniem przepływem, ponieważ ich związek jest bardzo subtelny. Kontrola przeciążeń ma gwarantować, że sieć będzie w stanie przenieść cały wprowadzany do niej ruch. Jest to problem globalny, obejmujący zachowanie wszystkich hostów i wszystkich routerów. Z kolei sterowanie przepływem odnosi się do ruchu pomiędzy konkretnymi nadawcami i odbiorcami. Jego zadaniem jest gwarantowanie, że szybki nadajnik nie będzie stale wysyłał danych szybciej, niż odbiornik będzie mógł je przyjmować.

Aby zrozumieć różnicę pomiędzy tymi dwoma mechanizmami, wyobraźmy sobie sieć złożoną ze 100-gigabitowych łączy optycznych, w której superkomputer usiłuje wtłoczyć duży plik do komputera osobistego, którego interfejs działa z prędkością zaledwie 1 Gb/s. Wprawdzie przeciążenie nie wystąpi (sieć nie ma kłopotów), lecz potrzebne będzie sterowanie przepływem, aby zmuszać superkomputer do częstych postojów, dających komputerowi osobistemu szansę odetchnąć.

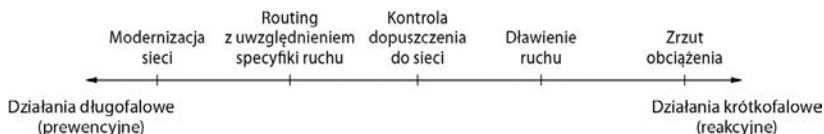
Drugą skrajnością może być na przykład sieć z buforowaniem mająca łącza 1 Mb/s i 1000 dużych komputerów, z których połowa usiłuje przysyłać pliki z szybkością 100 kb/s do drugiej połowy. Tutaj problem nie polega na przytłaczaniu odbiornika przez szybki nadajnik, lecz na przekroczeniu przez całkowity oferowany ruch możliwości sieci.

Powodem częstego mylenia sterowania przepływem i kontroli przeciążeń jest fakt, że najlepszym rozwiązaniem obu jest spowolnienie nadawców pakietów. Wobec tego host może otrzymać komunikat „zwolnij” albo dlatego, że z obciążeniem nie radzi sobie odbiornik, albo dlatego, że nie radzi sobie sieć. Wrócimy do tej kwestii w rozdziale 6.

Zacniemy analizę kontroli przeciążeń od spojrzenia na podejścia, które stosuje się w różnych skalach czasowych. Potem zajmiemy się zapobieganiem przeciążeniom, a następnie sposobom postępowania, kiedy jednak się pojawiają.

5.3.1. Metody kontroli przeciążeń

Obecność przeciążenia oznacza, że obciążenie sieci (czasowo) przekracza zasoby sieciowe (albo przynajmniej zasoby któregoś regionu sieci). Przyszedłoby wtedy na myśl dwa rozwiązania: zwiększenie zasobów albo zmniejszenie obciążenia. Na rysunku 5.20 widać, że rozwiązania te są zazwyczaj realizowane łącznie, ale w różnych horyzontach czasowych, aby z jednej strony reagować na obecne przeciążenia, a z drugiej unikać przyszłych.



Rysunek 5.20. Krótko- i długofalowe działania eliminujące przeciążenia

Najprostszym sposobem unikania przeciążenia jest zbudowanie sieci, która dokładnie odpowiada specyfice przenoszonego w niej ruchu. Jeśli na linii, którą idzie większość pakietów, znajduje się powolne łącze, przeciążenie sieci jest więcej niż prawdopodobne. Niekiedy w obliczu poważnego przeciążenia można zasilać sieć nowymi zasobami, na przykład włączając rezerwowe routery czy też dołączając łącza, które normalnie służą wyłącznie do zabezpieczenia redundancji (na wypadek fizycznych awarii łączy podstawowych). Można też na szybko nabywać przepustowość oferowaną na wolnym rynku przez innych operatorów. Zwykle te routery i łącza, które są najczęściej przeciążone, są modernizowane w najbliższym możliwym terminie. Odbyna się to już jednak w horyzoncie co najmniej miesięcy i wyłącznie po potwierdzeniu długofalowego trendu w ruchu sieciowym.

Aby możliwie dobrze wykorzystać dostępną pojemność sieci, routery powinny być przystosowane do wzorców obsługiwanego ruchu i do ich ewentualnych zmian w czasie (np. do zmian dobowego obciążenia poszczególnych łączy). Można na przykład na routerach odciągać ruch z najbardziej obciążonych tras poprzez tymczasową zmianę wag poszczególnych ścieżek. W niektórych stacjach radiowych i telewizyjnych stosuje się napowietrzną obserwację stanu dróg w mieście, umożliwiającą podawanie kierowcom informacji o korkach. Analogiczne obserwacje i dostosowania można prowadzić w sieciach komputerowych — mówimy wtedy o **routingu z uwzględnieniem warunków ruchu** (ang. *traffic-aware routing*). Pomocny bywa również rozdział ruchu pomiędzy alternatywne ścieżki dostarczania.

Niekiedy jednak zwiększenie (choćby tymczasowe) pojemności sieci jest niemożliwe; wtedy przeciążenie można zatrzymać wyłącznie poprzez zmniejszenie obciążenia ze strony nadawców pakietów. W sieciach z obwodami wirtualnymi odrzuca się wtedy nowe połączenia, bo doprowadziłyby do zapaści wydajności sieci. Takie działania noszą miano **sterowania dopuszczeniem do sieci** (ang. *admission control*).

Na niższym poziomie w obliczu przeciążenia sieć sama może dostarczać nadawcom pakietów wskazówki, aby ci zmniejszyli prędkość swoich transmisji. Można wtedy mówić o dławieniu ruchu ze strony nadawców albo o zrzucie obciążenia ze strony samej sieci.

Problemem jest tutaj samo wykrycie zbliżającego się przeciążenia oraz sposoby informowania nadawców o konieczności spowolnienia transmisji. Pierwszą kwestię rozwiązuje się mechanizmami monitorowania na routerach sieciowych, rejestrujących średnie opóźnienia kolejkovania pakietów, średnie obciążenie przetwarzaniem i stopień utraty pakietów. We wszystkich przypadkach rosnące wartości wskazują na rosnące przeciążenie.

Co do drugiego problemu konieczne jest uczestnictwo routerów w pętli zwrotnej informacji nadawców pakietów. Aby taka metoda działała poprawnie, zależności czasowe muszą być dokładnie regulowane. Gdyby po każdym dotarciu dwóch pakietów pod rząd router krzyczał: „Stop!”, a po każdym okresie bezczynności routera wynoszącym 20 μs krzyczał: „Dalej!”, system oscylowałby gwałtownie i nigdy się nie ustabilizował. Gdyby z drugiej strony czekał 30 minut na nabranie pewności przed powiedzeniem czegokol-

wiek, mechanizm kontroli przeciążeń reagowałby zbyt ślamazarnie, aby do czegokolwiek się nadawać. Dostarczanie na czas wskazówek co do dopuszczalnej prędkości transmisji nie jest wcale proste; do tego routery niefrasobliwie dostarczające takie powiadomienia same z siebie przyczyniają się do wzrostu obciążenia sieci. Ostatecznie kiedy wszystko inne zawiedzie, sieć jest zmuszona do odrzucania pakietów, których nie jest w stanie dostarczyć. Mówi się wtedy o **zrzucie obciążenia** (ang. *load shedding*). Tutaj dla zapobiegania przeciążeniom i eliminowania ich istotna jest wyważona polityka wyboru odrzucanych pakietów.

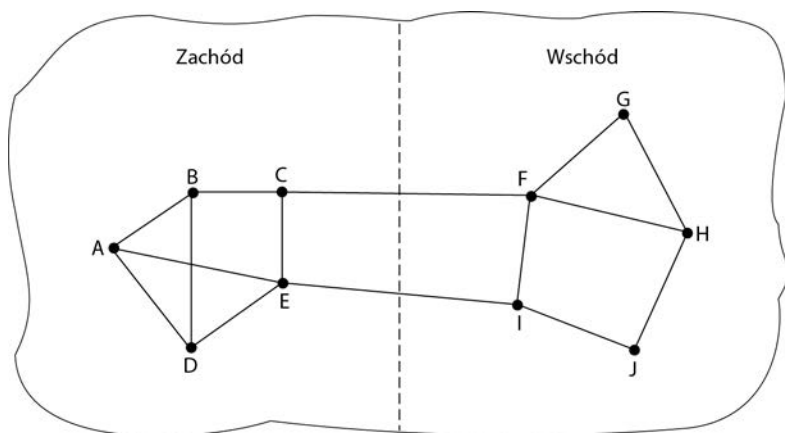
5.3.2. Routing z uwzględnieniem warunków ruchu

W pierwszej kolejności zajmiemy się routingiem z uwzględnieniem warunków ruchu. Metody routingu omawiane w podrozdziale 5.2 wykorzystywały stałe, predefiniowane wagi dla poszczególnych łączy. Adaptowały się do zmian w topologii sieci, ale nie do zmian w jej obciążeniu. Kiedy mówimy o wyznaczaniu tras z uwzględnieniem obciążenia poszczególnych fragmentów sieci, chcemy wyznaczać trasy tak, aby oddalać ruch od wąskich gardeł, które będą pierwszymi miejscami narażonymi na przeciążenia.

Najbardziej czytelnym sposobem na to jest zdefiniowanie wagi łącza jako funkcji (stałej) przepustowości łącza oraz opóźnienia propagacji sygnału plus (zmiennej) mierzonego obecnie obciążenia przetwarzania albo średniego opóźnienia kolejkovania pakietów. Podobne pod względem innych kosztów ścieżki są wtedy różnicowane za pomocą wydajności, a algorytm routingu powinien dobierać te, które mają mniejszą wartość funkcji wagi.

Routing z uwzględnieniem warunków ruchu był w takim wydaniu stosowany już we wczesnej sieci Internet (Khanna i Zinky, 1989), ale nie bez kłopotów — weźmy sieć z rysunku 5.21, podzieloną na dwie części: Wschód i Zachód, spięte dwoma łączami: *CF* i *EI*. Załóżmy, że większość ruchu pomiędzy wschodem i zachodem odbywa się za pośrednictwem łącza *CF*, w efekcie czego łącze to jest mocno obciążone i cechuje się dużymi opóźnieniami. Uwzględnienie opóźnienia kolejkovania w wadze używanej do wyznaczania najkrótszej ścieżki sprawi, że łącze *EI* zyska priorytet. Po zainstalowaniu nowych tabel routingu większość ruchu między wschodem i zachodem będzie się odbywać łączem *EI*, mocno je obciążając. W efekcie po następnej aktualizacji tablic routingu lepszym łączem okaże się ponownie *CF*. Ostatecznie dojdzie do oscylacji tabel routingu, co będzie destabilizowało routing i prowokowało liczne inne problemy.

Jeśli w wyznaczaniu najkrótszej trasy zignorujemy parametr obciążenia i uwzględnimy tylko opóźnienia propagacji pakietów, powyższy problem nie zaistnieje. Z kolei próby uwzględniania obciążenia, ale przy ograniczonym współczynniku owocują jedynie zmniejszeniem częstotliwości oscylacji routingu. Skuteczne rozwiązanie wymaga zastosowania jednej z dwóch technik. Pierwsza z nich to routing wielościeżkowy, dopuszczający obecność w tablicach routingu wielu tras do danego odbiorcy. W naszym przykładzie oznaczałoby to rozłożenie obciążenia pomiędzy oba łącza: Wschód – Zachód. Druga



Rysunek 5.21. Sieć, w której Zachód i Wschód są spięte dwoma łączami

technika to stopniowe przełączanie ruchu pomiędzy routerami, na tyle powolne, aby mogły one w międzyczasie aktualizować parametry łączy i ostatecznie osiągnąć stabilność tablic routingu, jak w metodzie Gallaghery (1977).

Z uwagi na powyższe trudności w protokołach routingu w Internecie unika się dostosowywania tras na podstawie obciążenia. Ewentualne dostosowania odbywają się za to poza protokołem routingu — zmieniane są więc jego dane wejściowe, a nie algorytm. Mówimy wtedy o **inżynierii ruchu**.

5.3.3. Kontrola dopuszczenia do sieci

W sieciach z obwodami wirtualnymi powszechnie stosowaną techniką unikania przeciążeń jest **kontrola dopuszczenia do sieci**. Pomysł jest prosty: nie wolno dopuszczać do tworzenia nowych obwodów wirtualnych, jeśli sieć nie będzie w stanie obsłużyć ruchu w tych obwodach. Próba zestawienia obwodu wirtualnego w takich warunkach powinna zostać zablokowana. To znacznie lepsze rozwiązanie niż dopuszczenie do sieci już obciążonej, a wkrótce przeciążonej. Analogicznie w systemie telefonicznym, kiedy centrala jest przeciążona, blokada dopuszczenia do sieci odbywa się poprzez brak emisji dźwięków wywołania.

Sztuką jest tu wytypowanie momentu, od którego dodawanie nowych obwodów wirtualnych naraża sieć na przeciążenie. W sieci telefonicznej jest to proste, ponieważ operuje ona na obwodach o z góry określonej prędkości transmisji (64 kb/s w przypadku nieskompresowanych danych dźwiękowych). Ale w sieciach komputerowych obwody wirtualne mogą definiować kanały o najróżniejszym zapotrzebowaniu na przepustowość. Każdy obwód powinien mieć więc przypisaną jakąś charakterystykę przenoszonego ruchu, inaczej trudno zarządzać dopuszczeniem do sieci.

Ruch jest często opisywany miarami prędkości i rozkładu. Sęk w dobraniu takiego opisu, który w prosty, ale znaczący sposób scharakteryzuje ruch w danym obwodzie — jest to problematyczne, ponieważ ruch pojawia się zazwyczaj w seriach mocno odbie-

gających od wartości średnich. Na przykład ruch związany z przeglądaniem strony WWW jest zupełnie inny niż ruch obsługujący strumieniowanie wideo i ten pierwszy trudniej scharakteryzować w długim okresie, ponieważ skumulowane serie ruchu WWW mogą łatwo doprowadzić do przeciążenia routerów w sieci. Powszechnie stosowaną miarą, która uwzględnia ten efekt, jest tzw. **cieknące wiadro** bądź **wiadro żetonów**. Operuje ona na dwóch parametrach, które reprezentują prędkość średnią ruchu i zwiększoną prędkość chwilową. Więcej o tych miarach powiemy w podrozdziale 5.4, przy okazji omawiania metod zapewniania jakości obsługi.

Uzbrojeni w deskryptory ruchu możemy w sieci decydować, czy dopuścić zestawienie nowego obwodu wirtualnego, czy nie. Sieć może na przykład rezerwować określoną pojemność wzdłuż ścieżek wykorzystywanych przez istniejące już obwody wirtualne, tak aby nie dopuścić do ich przeciążenia. W takim układzie deskryptor ruchu jest swego rodzaju umową świadczenia usługi — taką zarezerwowaną pojemność gwarantuje sieć. Przeciążenie jest wtedy niemożliwe. Zagłębiliśmy się jednak zanadto w temat jakości obsługi — wrócimy do niego w następnym podrozdziale.

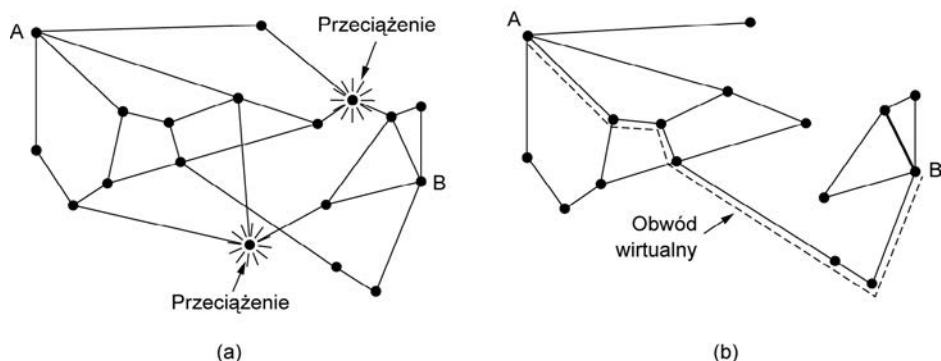
Nawet w przypadku braku gwarancji co do obwodu wirtualnego sieć wciąż może korzystać z danych zawartych w deskrypcji ruchu i decydować o dopuszczeniu do niej. Wystarczy oszacować, ile obwodów pomieści się w sieci bez ryzyka przeciążenia. Załóżmy, że obwody wirtualne przepychają ruch o szczytowej prędkości do 10 Mb/s wzdłuż tego samego 100-megabitowego łącza fizycznego. Ile takich obwodów można dopuścić? 10 obwodów na pewno nie przeciąży sieci, ale z drugiej strony tak mała ich liczba oznacza marnotrawstwo, ponieważ rzadko kiedy szczytowe natężenia ruchu dotyczą wszystkich obwodów w tym samym momencie. W faktycznych sieciach zbiera się statystyki opisujące dane typy transmisji i na ich podstawie szacuje się liczbę obsługiwanych obwodów wirtualnych — dzięki temu zyskujemy na efektywności sieci, jednak kosztem zwiększonego (ale wciąż akceptowalnego) ryzyka przeciążenia.

Dopuszczanie można też połączyć z routingiem z uwzględnieniem warunków ruchu, a więc z ustawieniem tras dla danego ruchu z pominięciem wąskich gardeł. Spójrzmy na przykład na sieć z rysunku 5.22 (a), w której przeciążone są dwa routery (oznaczone na rysunku).

Założmy, że host podłączony do routera *A* chce nawiązać połączenie z hostem podłączonym do routera *B*. Zwykle połączenie to przechodziłoby przez jeden z przeciążonych routerów. Aby uniknąć takiej sytuacji, możemy narysować sieć na nowo, jak na rysunku 5.22 (b), pomijając przeciążone routery i wszystkie ich linie. Linia przerywana przedstawia możliwą trasę dla obwodu wirtualnego, unikającą przeciążonych routerów. Tego rodzaju routing wrażliwy na obciążenie opisywał Shaikh i inni (1999).

5.3.4. Dławienie ruchu

W Internecie i w wielu innych sieciach komputerowych nadawcy dostosowują prędkość transmisji, tak aby wysłać możliwie dużą ilość danych, do maksimum dopuszczalnego pojemnością sieci. W takim układzie sieć z założenia pracuje w warunkach tuż



Rysunek 5.22. (a) Sieć z przeciążeniami, (b) Fragment sieci wolny od przeciążenia.
W punkcie (b) został pokazany dodatkowo obwód wirtualny z A do B

poniżej punktu przeciążenia. Jeśli to przeciążenie jest już bardzo bliskie, sieć musi powiadomić nadawców o konieczności zdławienia ich transmisji i spowolnienia tempa wysyłania pakietów. Owa wskazówka jest traktowana jako sytuacja zwyczajna, nie zaś jako sytuacja wyjątkowa. Do opisu tego zachowania sieci stosuje się pojęcie **unikania przeciążenia** (ang. *congestion avoidance*) — dla odróżnienia tego momentu od stanu faktycznego przeciążenia sieci.

Przyjrzyjmy się kilku podejściom do realizacji pomysłu dławienia ruchu, nadającym się do stosowania zarówno w sieciach datagramowych, jak i w sieciach z obwodami wirtualnymi. Każde z opisywanych podejść łączy się z dwoma problemami. Przede wszystkim routery muszą potrafić określić moment zbliżającego się przeciążenia, najlepiej jeszcze zanim ono faktycznie nastąpi. W tym celu router musi stale monitorować zasoby używane do rozprowadzania ruchu. Dostępными tu miarami są zajętość łączy wyjściowych, rozmiar wewnętrznych buforów oczekujących na przetworzenie oraz liczba pakietów, które zostały utracone z powodu braku miejsca w buforach. Z tych trzech najbardziej istotny jest parametr drugi. Średnia zajętość łączy nie odpowiada wprost obciążeniu z powodu charakterystyki wielu transmisji (np. chwilowe szczyty transmisji): zużycie na poziomie 50% może oznaczać wartość niską przy gładkim ruchu o stałym natężeniu albo już zbyt wysoką dla ruchu o dużej zmienności natężenia. Z kolei liczba pakietów utraconych jest miarą dostępną zbyt późno — gdy dochodzi do tracenia pakietów na wejściu do routera, już można mówić o przeciążeniu sieci.

Tymczasem dobrym opisem przeciążenia jest opóźnienie kolejkowania pakietów do przetworzenia w routerach; przez większość czasu rozmiar kolejki powinien być mały, ale w przypadku pojawienia się chwilowych skoków natężenia ruchu od razu widać jej wydłużenie. Do wyznaczenia porządnej estymaty opóźnienia kolejkowania d można uokresować próbkę chwilowej długości kolejki s i odpowiednio dostosowywać d — według wzoru:

$$d_{\text{nowe}} = d_{\text{stare}} + (1 - \alpha)s$$

gdzie stała α opisuje szybkość, z jaką router zapomina miary historyczne. Jest to tak zwana miara **EWMA** (*Exponentially Weighted Moving Average*), czyli krocząca średnia ważona wykładniczo. Wygładza ona fluktuacje i odpowiada działaniu dolnoprzepustowego filtra częstotliwości. Kiedy d przekracza wartość progową, router wykrywa stan bliski przeciążeniu.

Drugi problem do rozwiązania to potrzeba dostarczenia do odpowiednich nadawców powiadomień o konieczności zdławienia transmisji w momencie, kiedy jeszcze można zapobiec przeciążeniu. Samo przeciążenie jest odczuwalne w całej sieci, natomiast prewencja wymaga działań po stronie nadawców używających tej sieci. Dostarczenie zalecenia spowolnienia transmisji wymaga od routerów identyfikowania właściwych nadawców. Same ostrzeżenia powinny być też stosowane oszczędnie, bez zalewania pakietami ostrzegawczymi sieci stojącej u progu przeciążenia. Rozwiązań jest kilka.

Pakiety tłumienia

Najbardziej oczywistym sposobem powiadomienia nadawcy o rychłym przeciążeniu jest komunikacja bezpośrednia. W tej metodzie router wybiera nadawcę pakietów przeciążających i wysyła **pakiet tłumienia** (ang. *choke packet*) z powrotem do hosta źródłowego, podając mu cel transmisji znaleziony w pakiecie. Pierwotny pakiet może być oznaczony przez włączenie bitu w nagłówku, aby nie generował kolejnych pakietów tłumienia po drodze, a następnie zostaje przekazany dalej jak zwykle. W celu uniknięcia zwiększenia obciążenia sieci w czasie przeciążenia router może wysyłać pakiety tłumiące z małą prędkością.

Gdy host źródłowy otrzymuje pakiet tłumienia, wymaga się od niego redukcji ruchu wysyłanego do wskazanego celu, na przykład o 50%. W sieci datagramowej wybór nadawcy pakietów do zdławienia jest prosty — zwyczajne losowe próbkowanie oczekujących pakietów daje dużą szansę natrafienia na szybkiego nadawcę (jego pakietów jest stosunkowo dużo). Jest też równie prawdopodobne, że pakiety tłumiące trafią wtedy do tego samego nadawcy wielokrotnie. W takim przypadku powinien on ignorować kolejno spływające pakiety, póki odstęp między nimi mieści się w jakimś określonym przedziale czasu — tak aby mieć szansę doczekać efektów pierwszego zmniejszenia prędkości transmisji. Jeśli po tym okresie pakiety tłumiące wciąż spływają, nadawca powinien ponownie zmniejszyć prędkość transmisji, bo sieć wciąż jest przeciążona.

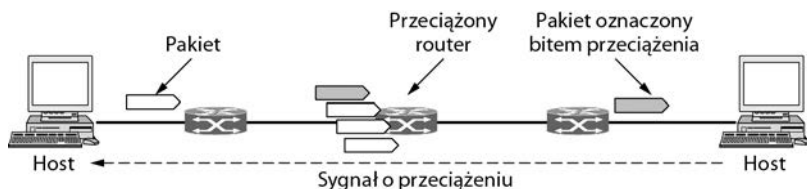
Przykładem pakietu tłumiącego z wczesnej fazy rozwoju sieci Internet jest komunikat SOURCEQUENCH (Postel, 1981). Nie przyjął się on jednak, po części z powodu braku jasnego określenia okoliczności, w których miał być generowany, i oczekiwanych działań po stronie odbiorcy pakietu. We współczesnym Internecie stosuje się alternatywne powiadomienia.

Jawne powiadamianie o przeciążeniach

Zamiast generować dodatkowe pakiety ostrzegające przed przeciążeniem, router może oznaczyć takim komunikatem dowolny rozprowadzany pakiet (odbywa się to poprzez ustawienie bitu w nagłówku pakietu). Kiedy sieć dostarczy pakiet, jego adresat może

zorientować się w sytuacji i poinformować o niej nadawcę w jednym z pakietów odpowiedzi (bądź potwierdzenia odbioru). Tak powiadomiony nadawca może wtedy przejść do dławienia swojej transmisji.

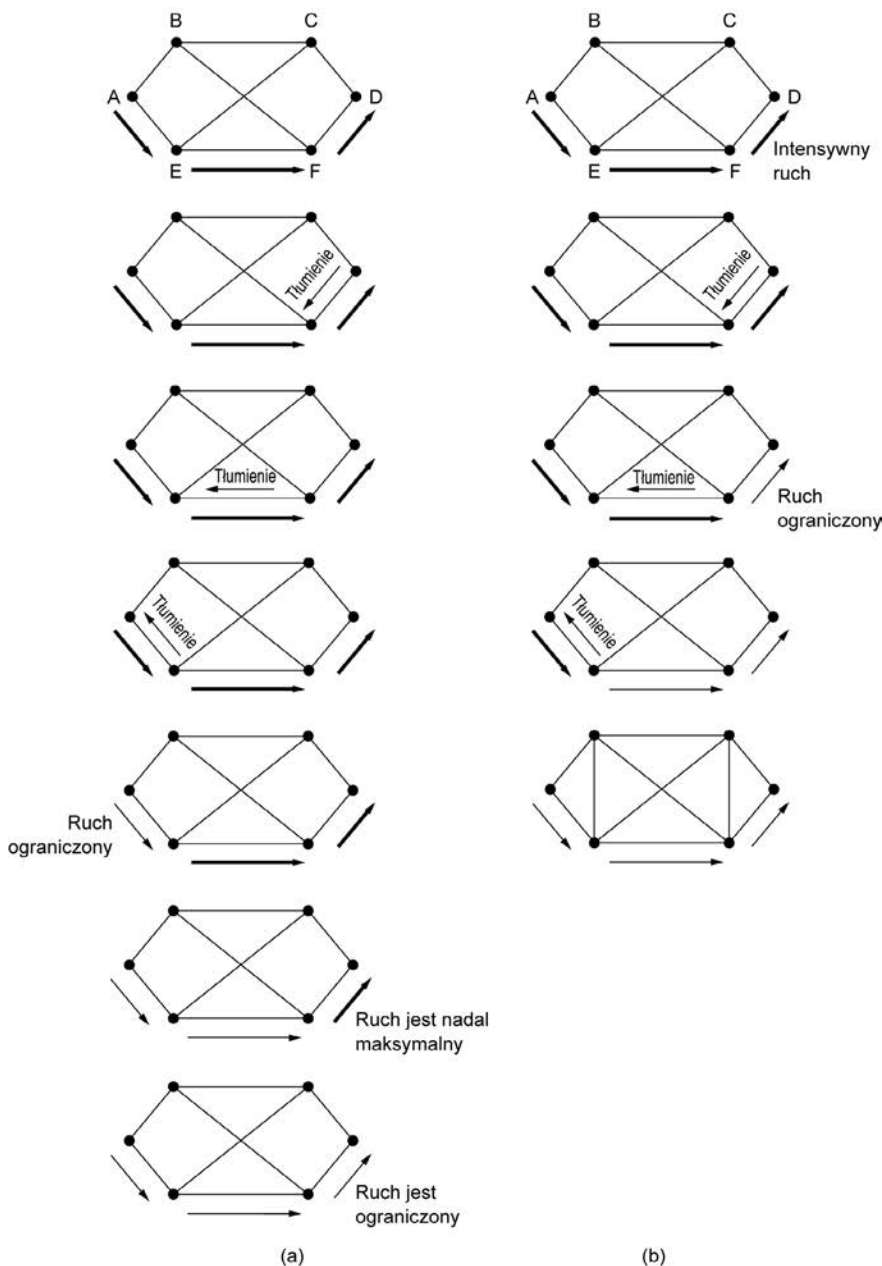
Schemat ten nosi miano *jawnego powiadamiania o przeciążeniu*, w skrócie **ECN** (od *Explicit Congestion Notification*), i jest stosowany w sieci Internet (Ramakrishnan i inni, 2001). Jest to udoskonalona wersja wczesnych protokołów sygnalizacji przeciążeń, przede wszystkim metody powiadamiania binarnego opracowanej przez Ramakrishnana i Jaina (1988), która była stosowana w architekturze sieci DECNET. W nagłówku pakietu IP zarezerwowano dwa bity przeznaczone do oznaczania pakietu pod przeciążeniem. Nadawca wysyła pakiety z bitami wyzerowanymi (jak na rysunku 5.23). Jeśli którykolwiek z routerów po drodze jest przeciążony, oznaczy pakiet bitem przeciążenia i rozprowadzi go do odbiorcy. Obowiązkiem adresata jest odpowiadać nadawcy z zachowaniem bitów odebranych z sieci, więc nadawca dowie się o przeciążeniu wraz z najbliższą odpowiedzią odbiorcy (np. wraz z pakietem potwierdzającym odebranie transmisji). Na rysunku sygnał o przeciążeniu jest zaznaczony linią przerywaną, ponieważ pojawia się na poziomie protokołu i pakietów IP (np. w transmisji TCP), a nie na poziomie właściwych danych wymienianych przez strony komunikacji. Nadawca transmisji po odebraniu od odbiorcy pakietów z ustawionymi bitami sygnalizacji przeciążenia powinien zareagować tak jak na pakiety tłumiące, czyli zdławić swoją transmisję.



Rysunek 5.23. Jawne powiadamianie o przeciążeniu

Tłumienie skok po skoku

Przy dużych szybkościach i długich dystansach po zasygnalizowaniu przeciążenia przez router nadawca może wysłać jeszcze wiele pakietów, a to z powodu opóźnienia, z jakim odbiera sygnał o przeciążeniu. Weźmy na przykład hosta z San Francisco (router A na rysunku 5.24), który wysyła transmisję do hosta w Nowym Jorku (router D z rysunku 5.24) z szybkością 155 Mb/s. Jeśli w hoście nowojorskim zacznie brakować buforów, to dotarcie pakietu tłumienia z powrotem do San Francisco, żądającego spowolnienia transmisji, zajmie około 40 milisekund. Sygnalizacja ECN zajmie jeszcze więcej czasu, ponieważ jest dostarczana do nadawcy za pośrednictwem adresata transmisji. Propagację pakietu tłumienia przedstawiają drugi, trzeci i czwarty krok z rysunku 5.24 (a). Podczas tych 40 ms zostało wysłanych kolejne 6,2 megabita danych. Nawet jeśli host w San Francisco natychmiast przestanie nadawać, te 6,2 megabita w kanale nadal będzie napływać i trzeba będzie sobie z nimi poradzić. Dopiero na siódmym schemacie z rysunku 5.24 (a) router z Nowego Jorku zauważy wolniejszy napływ danych.



Rysunek 5.24. (a) Pakiet tłumienia wpływający tylko na źródło transmisji,
 (b) Pakiet tłumienia wpływający na każdy węzeł, przez który przechodzi

Alternatywne rozwiązanie polega na tym, że pakiet tłumienia zaczyna działać już w każdym przeskoku, jak na rysunku 5.24 (b). Tutaj natychmiast po dotarciu pakietu tłumienia do *F* od tego routera żąda się redukcji przepływu do *D*. Będzie to wymagało poświęcenia przez *F* dodatkowych buforów na tę transmisję, ponieważ źródło nadal

pracuje na pełnych obrotach, lecz przynosi *D* natychmiastową ulgę (jak lekarstwo od bólu głowy z reklam telewizyjnych). W następnym kroku pakiet tłumienia dociera do *E*, co każe *E* ograniczyć przepływ do *F*. Zwiększa to zapotrzebowanie na bufor routera *E*, lecz natychmiast odciąża *F*. Na koniec pakiet tłumienia dociera do *A* i przepływ autentycznie maleje.

W sumie ten schemat tłumienia **skok po skoku** (ang. *hop-by-hop*) zapewnia szybkie odciążenie w punkcie przeciążenia kosztem zużycia dodatkowego miejsca w buforach w poprzednich węzłach na trasie transmisji. W ten sposób przeciążenie może zostać stłumione w zarodku bez tracenia jakichkolwiek pakietów. Pomysł ten opisuje Mishra i inni (1996).

5.3.5. Zrzut obciążenia

Gdy żadna z powyższych metod nie spowoduje zniknięcia przeciążenia, routery mogą wytoczyć ciężkie działa — **zrzut obciążenia** (ang. *load shedding*). To określenie jest eleganckim sposobem powiedzenia, że routery zalane pakietami, których nie są w stanie obsłużyć, po prostu wyrzucają te pakiety. Termin wziął się ze świata elektroenergetyki, gdzie oznacza rozmyślne odłączanie pewnych obszarów, aby uchronić całą sieć przed zapaścią w porach, gdy zapotrzebowanie na energię znacznie przekracza dostępne zasoby.

Zasadniczym pytaniem dla routera podlegającego przeciążeniu jest dobór odrzuconych pakietów. Wybór może być uzależniony od specyfiki aplikacji działających w danej sieci. W transferze plików stary pakiet ma większą wartość niż nowy, ponieważ odrzucenie pakietu nr 6 i zachowanie pakietów od 7 do 10 i tak wymusi po stronie odbiorcy buforowanie danych, których nijak nie może spożytkować bez odebrania brakującego pakietu. Z kolei w mediach czasu rzeczywistego nowy pakiet jest bardziej wartościowy niż stary, bo pakiety przeterminowane w aplikacjach czasu rzeczywistego są bezużyteczne.

Pierwsza zasada (starszy lepszy od nowego) nazywana jest często **winem**, a druga (świeży lepszy od starego) to **mleko** — wiadomo, że większość ludzi woli pić stare wino i świeże mleko niż na odwrót.

Bardziej inteligentne zrzucanie obciążenia wymaga współpracy z nadawcami. Przykładem mogą być pakiety przenoszące informacje dla routingu. Są one ważniejsze od zwykłych pakietów danych, bo dotyczą samych routerów, a więc i działania samej sieci. Jeśli zostaną utracone, sieć może stracić zdolność do rozprowadzania pakietów. Inny przykład to algorytmy kompresji wideo (jak MPEG), które okresowo przesyłają całą klatkę normalizującą, a następnie wysyłają kolejne klatki różnicowe względem ostatniej pełnej klatki. W tym przypadku odrzucenie pakietu niosącego informacje różnicowe będzie lepsze niż odrzucenie tego, który jest częścią pełnej klatki, gdyż przyszłe pakiety są od niego zależne.

Aby zaimplementować inteligentną zasadę odrzucania pakietów, aplikacje muszą oznaczać swoje pakiety, sygnalizując w ten sposób ich wartość. W takim układzie kiedy dojdzie do zrzutu obciążenia, routery będą w pierwszej kolejności odrzucać mniej ważne

pakiety, a pakiety ważniejsze będą odrzucane dopiero w ostateczności. Oczywiście wszyscy będą respektować zasady oznaczania pakietów i nikt nie pokusi się o oflagowanie wszystkich swoich transmisji znacznikiem: „BARDZO WAŻNY — NIE WYRZUCAĆ POD ŻADNYM POZOREM!”.

Wymuszanie bądź zachęcanie do właściwego oznaczania pakietów odbywa się często na poziomie rozliczania za usługę. Na przykład sieć może dopuszczać transmisje z większą prędkością niż ta, za którą zapłacili nadawcy, jeśli w zamian ci będą oznaczać swoje pakiety znacznikiem niskiego priorytetu. Taka strategia jest niegłupia, ponieważ pozwala znacznie skuteczniej wykorzystać beczynne zasoby. Hosty mają prawo ich używać, dopóki nikt inny nie jest nimi zainteresowany, lecz bez nabywania prawa do nich w okresach dużego obciążenia.

Random Early Detection

Wiadomo, że obsługa przeciążenia u jego zarania jest bardziej skuteczna niż wtedy, gdy pozwolimy mu narobić bigosu i dopiero wtedy będziemy próbować sobie z nim poradzić. To spostrzeżenie prowadzi do ciekawego ulepszenia metody zrzutu obciążenia, w ramach którego pakiety są odrzucane, jeszcze zanim dojdzie do wyczerpania miejsca w buforach.

Chodzi o to, że większość hostów w sieci Internet nie otrzymuje jeszcze sygnałów o przeciążeniu w postaci ECN; w wielu regionach sieci jedynym niezawodnym sygnałem przeciążenia jest utrata nadawanych pakietów. Trudno przecież zbudować taki router, który nie gubi pakietów w warunkach przeciążenia. Protokoły transportowe (takie jak TCP) są więc projektowane z założeniem, że utrata pakietów świadczy o przeciążeniu i spowalnianiu źródła transmisji. Do zastosowania takiej metody doprowadziło rozumowanie, że TCP został zaprojektowany dla sieci kablowych, które są bardzo niezawodne, więc pakiety tracą się głównie z powodu przepełnienia buforów, a nie błędów transmisji. W łączach bezprzewodowych dobra współpraca z TCP wymusza zatem odzysk błędów transmisji na poziomie warstwy łącza danych (nie są więc one widoczne w warstwie sieciowej).

Można to wykorzystać do walki z przeciążeniami. Odrzucanie przez routery pakietów, jeszcze zanim sytuacja stanie się beznadziejna, oznacza, że jest czas na podjęcie działań po stronie nadawcy, zanim będzie za późno. Popularny służący do tego algorytm nosi nazwę **RED** (*Random Early Detection* — **losowe wczesne wykrywanie**) (Floyd i Jacobson, 1993). Aby zdecydować, kiedy przychodzi pora, by zacząć odrzucać pakiety, routery rejestrują na bieżąco średnią wartość długości swoich kolejek. Gdy średnia długość kolejki dla jakiegoś łącza przekracza ustaloną granicę, uznaje się, że łącze jest przeciążone, i losowo odrzuca małą część pakietów. Losowy wybór pakietów jest optymalny, ponieważ w sieci datagramowej router nie jest w stanie wytypować źródła przeciążenia. Każdy z nadawców, którego dotyczyła utrata pakietów, dowie się o niej w wyniku braku potwierdzenia od odbiorcy, i wtedy sam spowolni swoją transmisję. Utrata pakietu jest tu więc odpowiednikiem dostarczenia pakietu tłumiącego, ale w sposób niejawny.

Routery RED cechują się lepszą wydajnością w porównaniu do routerów, które odrzucają pakiety dopiero po przepełnieniu buforów, choć uzyskanie optymalnych efektów wymaga pewnego dostrojenia. Na przykład idealna liczba pakietów do odrzucenia jest zależna od tego, ilu nadawców zamierzamy powiadomić o przeciążeniu. Mimo to preferowaną opcją jest sygnalizacja ECN (jeśli tylko jest możliwa). Działa podobnie, ale dostarcza sygnał o przeciążeniu w sposób jawny, a nie poprzez wnioskowanie z utraty pakietów; RED stosuje się tam, gdzie hosty sieci nie obsługują sygnalizacji jawnej.

SKOROWIDZ

1000Base-SX, 327
100Base-FX, 324
100Base-T4, 323
100Base-TX, 324
10GBase-T, 311, 330
3GPP, Third Generation Partnership Project, 100

A

AAC, Advanced Audio Coding, 780
AAL5, ATM Adaptation Layer 5, 281
abstrakt komunikatu, message digest, 891
ACL, Asynchronous ConnectionLess, 360
ACM, Association for Computing Machinery, 27
ActiveX, 752, 952
adaptacja szybkości, rate adaptation, 334
adaptacyjny przeskok częstotliwości, 359
ADC, Analog--Digital Converter, 777
adres
 grupowy, 313
 IP, 485, 492, 530, 942
 kontaktowy, care of address, 426
 o stałej długości, 502
 przeznaczenia, 313
 specjalny IP, 494
 URL, 718
 źródłowy, 313
adresowanie klasowe, classful addressing, 491
adresowanie specjalne, 491
ADSL, Assymetric DSL, 149, 172, 212, 213
 konfiguracja, 175
ADSL, Asymmetric Digital Subscriber Loop, 279
AES, Advanced Encryption Standard, 346, 872
agent, 426

transmisji, message transfer agent, 688
urlopowy, 693
użytkownika, 688, 690
agregacja prefiksów IP, 490
AH, Authentication Header, 907
AIFS, Arbitration InterFrame Space, 342
AIMD, Additive Increase Multiplicative Decrease, 587, 628
AJAX, Asynchronous JavaScript and XML, 752
aktualność, 866
algorytm
 1-persistent CSMA/CD, 316
AES, 882
AODV, 428
binarne oczekiwanie wykładnicze, 317
cieknącego wiadra, 448
DES, 869, 882
DHT, 835
Dijkstry, 406
drzewa częściowego, 376
dystrybucji pakietów, 414
E0, 919
fair queueing, 453
forwardingu, 49
IDEA, 935
Karna, 627
Nagle'a, 622
obliczania CRC, 243
poznawania wstecz, 372
przekazywania, 49
RC4, 882
RC5, 882
RED, 465
Rijndael, 873
routingu, 48, 397, 400, 401
RSA, 886

- algorytm
 - rywalizacji, 299
 - SAFER, 919
 - Serpent, 882
 - stanu łączy, 473
 - szeregowania pakietów, 452
 - Triple DES, 882
 - Twofish, 882
 - wiadra żetonów, 448
 - wolnego rozruchu, 631
 - wolnego startu Johnsona, 659
 - wyszukiwania najkrótszej ścieżki, 403
 - Ziva-Lempela, 936
 - algorytmy
 - adaptacyjne, 402
 - dynamiczne, 408
 - kompresji, 779
 - kompresji dźwięku, 780
 - kontroli przeciążeń, 431
 - kryptograficzne, 965
 - nieadaptacyjne, 402
 - wyznaczania tras, 416
 - z kluczem symetrycznym, 867
 - ALOHA, 95, 292
 - alokacja przepustowości, 579
 - AMI, Alternate Mark Inversion, 155
 - amplituda, 157
 - AMPS, Advanced Mobile Phone System, 87, 192
 - analiza
 - Fouriera, 114
 - nagłówków HTTP, 823
 - ruchu, traffic analysis, 35, 907
 - poczty elektronicznej, 36
 - anomalie szybkości transmisji, rate anomaly, 343
 - anonimowość, 956
 - kaskadowa, 957
 - w sieci, 826
 - ANS, Advanced Networks and Services, 82
 - ANSNET, 82
 - anteny
 - kierunkowe, 204
 - sektorowe, 204
 - anycast, 424
 - AODV, Ad hoc On-demand Distance Vector, 428
 - AP, Access Point, 41, 93, 332
 - aplet, 751
 - aplikacje
 - pomocnicze, 723
 - WWW, 24, 744
 - sieci równorzędnych, 28
 - APR z pośrednikiem, proxy ARP, 512
 - APSD, Automatic Power Save Delivery, 341
 - arbitraż, 95
 - architektura
 - Bluetooth, 355
 - EPC Gen 2, 363
 - Internetu, 83
 - RFID, 364
 - sieci, 52
 - sieci 802.16, 349
 - sieci DTN, 661
 - sieci komórkowej, 197
 - sieci niewrażliwych na opóźnienia, 662
 - sieci WWW, 715, 716
 - systemu pocztowego, 688
 - arkusze CSS, 743
 - ARP, Address Resolution Protocol, 511
 - ARPA, Advanced Research Projects Agency, 78
 - ARPANET, 67, 77–80
 - ARQ, Automatic Repeat reQuest, 255
 - AS, Authentication Server, 931
 - AS, Autonomous System, 474, 520
 - ASK, Amplitude Shift Keying, 156, 364
 - asocjacja, 345
 - ASP.NET, Active Server Pages .NET, 749
 - aspekt, 784
 - asynchroniczna komunikacja, 756
 - asynchroniczny transfer, 280
 - atak
 - brigady kubelkowej, 927
 - DDoS, 913, 940
 - Dos, 913, 940
 - keystream-reuse, 880
 - atak lustrzany, reflection attack, 923
 - powtarzający, 929
 - urodzinowy, 895
 - z osobą pośrednią, 927
 - ATM, Asynchronous Transfer Mode, 280, 331, 446
 - atrybut, 735
 - Authenticode, 952
 - autonegocjacja, 325, 326
 - AVC, Advanced Video Coding, 789
 - awaria hosta, 576
- ## B
- B2B, Business-to-business, 29
 - B2C, Business-to-consumer, 29
 - bajt
 - unikowy ESC, 227
 - znacznikowy, flag byte, 226
 - bandwidth-delay product, 263
 - baner reklamowy, 732
 - baza diagonalna, 862
 - baza prostoliniowa, 862
 - bel, 777

bezpieczeństwo, 507, 532, 850
 apletów Javy, 951
 Bluetooth, 918
 DNS, 944
 IP, 905
 komunikacji, 904
 poczty elektronicznej, 934, 939, 966
 przez ukrycie, 855
 sieci WWW, 940, 966
 sieciowe, 979
 systemów operacyjnych, 852
 w sieciach bezprzewodowych, 915
 w warstwie aplikacji, 851
 w warstwie sieciowej, 851
 w warstwie transportowej, 851, 950
bezpieczne
 nazewnictwo, 941
 połączenie SSL, 947
 HTTP, 947
bezpoległościowe warstwy sieciowe, 395
bezprowizyjna
 sieć rozległa, 49
 sieć lokalna, 92, 332
BGP, Border Gateway Protocol, 473, 522
biblioteki online, 27
biblioteki sieciowe, 27
binarny kod spłotowy, 236
bit MF, 343
bit parzystości, 240
BitTorrent, 27, 835
blok z jednobitowym błędem, 240
blokada usługi, 913
blokowanie portów, 911
Bluetooth, 39, 138, 387, 919
 profile, 356
 SIG, 356
błędy
 izolowane, 240
 seryjne, 240
 transmisji, 152, 225, 239, 254
 w pracy potokowej, 264
błyskawiczne przesyłanie wiadomości, 28
bod, baud, 152
botnet, 692
BPSK, Binary Phase Shift Keying, 156
brama, 812
 sieciowa, gateway, 50
 wejściowa, 822
bramki aplikacyjne, application-level
 gateways, 911
broadcasting, 314
BSC, Base Station Controller, 197
bufor pakietów, 415

buforowanie, 571
 danych, 643
 pakietów, 603
 ramek, 379
burza transmisyjna, broadcast storm, 382

C

C2C, Consumer-to-consumer, 29
CA, Certification Authority, 898
cacheowanie
 stron, 765
 treści, 766
CAPTCHA, 37
carrier-grade Ethernet, 331
CAT 5, 121
CBC, Cipher Block Chaining, 877, 918
CCITT, 101
CCK, Complementary Code Keying, 335
CD, Committee Draft, 102
CDM, Code Division Multiplexing, 161
CDMA, Code Division Multiple Access, 132,
 162, 196, 204
CDMA2000, 202
CDN, Content Distribution Network, 817
cechy sieci, 467
centrala
 końcowa, 167
 tandemowa, 167
 tranzytowa, toll office, 167
centrum
 autoryzacyjne CA, 898, 900
 dystrybucji kluczy, 921, 928
certyfikat, 898
 anulowany, 903
 na klucz publiczny, 899
 X.509, 102, 352, 900
CFB, Cipher FeedBack, 878
CGI, Common Gateway Interface, 746, 749
chip, 162
chrominancja, 785
ciasteczka, cookies, 36, 728
 cookie nietrwale, 730
 cookie trwałe, 730
 SYN, 616
CIDR, Classless InterDomain Routing, 488–491
cieknące wiadro, 448
cienki Ethernet, 312
click fraud, 774
CMTS, Cable Modem Termination System,
 85, 209
CND, Content Delivery Networks, 826
combing, 784
CRC, Cyclic Redundancy Check, 242
CRL, Certificate Revocation List, 904

CSMA with Collision Detection, 298
 CSMA, Carrier Sense Multiple Access, 95
 CSMA/CA, CSMA with Collision Avoidance, 336–340
 CSNET, Computer Science Network, 81
 CSS, Cascading Style Sheets, 742
 CTS, Clear to Send, 310
 cyberpunk remailer, 957
 cybersquatting, 677
 cyfrowe
 linie abonenckie, 171
 linie telefoniczne T1, 153
 wideo, 782
 wykluczenie, 101
 cykliczna suma kontrolna CRC, 242
 cykowanie drukowalne, 700
 czas
 dotarcia pakietu, 446
 oczekiwania na retransmisję, 316
 odpowiedzi, 644
 przejścia sygnału, 145
 przesyłu, 315
 przybywania potwierdzenia, 625
 RTT, 625
 transmisji, 211, 262, 316
 zakończenia obsługi pakietu, 455
 życia pakietu, 429
 czasomierz, 229, 249
 częstotliwość, 157
 fali, 130
 odcięcia, 115, 117
 transmisji, 93
 zmian sygnału, 152
 członek ISO
 AFNOR, 102
 ANSI, 102
 BSI, 102
 DIN, 102
 PKN, 102
 czynnik pseudolosowy, 154
 czytnik
 RFID, 365
 książek elektronicznych, 27

D

DAC, Digital-to-Analog Converter, 777
 DAG, Directed Acyclic Graph, 403
 DAMPS, Digital Advanced Mobile Phone System, 196
 datagram, 59, 396
 DCCP, Datagram Congestion Controlled Protocol, 548
 DCF, Distributed Coordination Function, 337
 DCMA, 35

DCS1000, 36
 DCT, Discrete Cosine Transformation, 786, 787
 DdoS, Distributed Denial of Service, 913
 decybel dB, 118
 deficit round robin, 455
 definicje w protokołach, 247
 dekodowanie, decoding, 779
 elastyczne, soft-decision, 237
 sztywne, hard-decision, 237
 z korekcją błędów, 238
 demon protokołu IMAP, 711
 DES, Data Encryption Standard, 869
 detekcja błędów, 240, 282
 detranspozycja, unmarshaling, 595
 DHCP, Dynamic Host Configuration Protocol, 513
 DHT, Distributed Hash Tables, 838–842
 diagram
 konstelacji, 158
 stanów, 545
 stanów automatu skończonego, 619
 DIFS, DCF InterFrame Spacing, 342
 digitalizacja sygnałów cyfrowych, 178
 DIS, Draft International Standard, 103
 DIX, 314
 dławienie ruchu, 437
 długość fali, 130
 długość graniczna, constraint length, 236
 długość ramki, 228
 DMT, Discrete MultiTone, 173
 DMZ, DeMilitarized Zone, 911
 DNS spoofing, 942
 DNS, Domain Name System, 70, 81, 673, 941
 DNSsec, DNS Security, 686, 944
 dobór punktu odtwarzania, 604
 DOCSIS, Data Over Cable Service Interface Specification, 210
 dokument, 905
 RFC 1323, 564
 RFC 1661, 275
 RFC 1663, 277
 RFC 1939, 712
 RFC 1958, 478
 RFC 2109, 729
 RFC 2210, 457
 RFC 2364, 281
 RFC 2440, 936
 RFC 2615, 278
 RFC 2616, 757
 RFC 2632, 939
 RFC 3501, 711
 RFC 3550, 598
 RFC 3875, 746

RFC 4614, 606
RFC 4632, 489
RFC 5246, 950
RFC 5322, 695
XML, 754
DOM, Document Object Model, 752–756
domena, 676
domena kolizji, 321
domeny najwyższego poziomu
 narodowe, 675
 rodzajowe, 675
domeny drugiego poziomu, 676
DoS, Denial of Service, 913
dostawca
 łącza internetowego, 914
 łączy kablowych, 212
 treści, 827
 usług internetowych, 47
 usług ADSL, 212
 usług transportowych, 541
dostęp
 do nośnika, 976
 do pasma, 207
 szerokopasmowy, broadband, 85
 wielokrotny, 292
dostosowanie
 addytywne, 587
 multiplikatywne, 587
drzewo
 centrowane, 423
 częściowe, spanning tree, 420
 dystrybucji sieci CDN, 827
 ujścia, 402
DS, Differentiated Services, 808
DSAM, 281
DSL, Digital Subscriber Line, 84, 171
DSLAM, DSL Access Multiplexer, 84, 174, 279
DSR, Dynamic Source Routing, 431
DSS, Digital Signature Standard, 890
DTN, Delay-Tolerant Network, 660
dupleksacja z podziałem
 czasu, 351
 częstotliwości, 351
DVMRP, Distance Vector Multicast Routing Protocol, 422
DWDM, Dense WDM, 185
dwuznaki, 857
dynamiczna alokacja buforów, 574
dynamiczne generowanie strony, 745, 751
dynamiczny
 HTML, 749
 przydział adresów IP, 728
 wybór częstotliwości, 346

dyrektywy, directives, 734
dyskretna transformata kosinusowa, 786, 787
dyspersja chromatyczna, 126
dystrybucja, 346
dystrybucja treści, 816, 826, 830
dzielenie pakietów, 475
dzierzawa, 513
dźwięk cyfrowy, 776

E

EAP, Extensible Authentication Protocol, 916
eBGP, zewnętrzny BGP, 526
ECB, Electronic Code Book, 876
ECMP, Equal Cost MultiPath, 519
ECN, Explicit Congestion Notification, 440, 586, 612
e-commerce, electronic commerce, 26
e-mail, 25, 686, 843
EDE, Encrypt-Decrypt-Encrypt, 872
EDGE, Enhanced Data rates for GSM Evolution, 205
efektywność sieci, 432
EIFS, Extended InterFrame Spacing, 343
ekstrapolacja wyników, 644
elementy skwantowane, 788
emotikony, 687
EPC, 363
EPC Gen 2, 363
EPON, Ethernet PON, 177
ESMTP, Extended SMTP, 707
ESP, Encapsulation Security Payload, 908
Ethernet, 42, 311, 330
 10-gigabitowy, 329
 klasyczny, 42, 311
 przełączany, 42, 311
etykietowanie, 514
EuroDOCSIS, 210
EWMA, Exponentially Weighted Moving Average, 439, 625

F

Facebook, 28
fale
 milimetrowe, 138
 podczerwone, 139
 radiowe, 134
fałszywy adres źródłowy, 912
farma serwerów, 86, 821
Fast Ethernet, 311, 322
faza, 157
faza punktu, 157
FCC, Federal Communication Commission, 136
FCFS, First-Come First-Serve, 452

FDD, Frequency Division Duplex, 194, 351
 FDDI, Fiber Distributed Data Interface, 303, 331
 FDM, Frequency Division Multiplexing, 159
 FEC, Forward Error Correction, 795
 FEC, Forwarding Equivalence Class, 516
 Fibre Channel, 331
 FIFO, First-In First-Out, 452
 filtr
 analogowy, 174
 pakietów, 910
 tłumiący, 172
 filtrowanie, 115
 filtrowanie tekstu, 912
 firewall, 910, 912
 firmware, 55
 fizyczna warstwa radiowa, 358
 fluktuacja, jitter, 446, 603, 775
 format
 adresu, 694
 ramek
 Ethernet, 314
 IEEE 802.3, 314
 IEEE 802.11, 344
 PPP, 276
 w HDLC, 276
 T1, 180
 X.400, 694
 wiadomości, 695
 formularz, 738–741, 750
 forum WiMAX, 347
 foton, 861
 fragmentacja
 nieprzezroczysta, 476
 pakietów, 474
 przezroczysta, 475
 fragmenty, 340
 frame bursting, 327
 framework .NET, 749
 FSK, Frequency Shift Keying, 156
 FTP, File Transfer Protocol, 70, 497
 FttH, Fiber to the Home, 85, 125, 175
 funkcja podstawowa
 ACCEPT, 61
 CONNECT, 60
 DISCONNECT, 61
 LISTEN, 60
 RECEIVE, 61
 SEND, 61
 SEND PACKET, 63
 funkcja skrótu, 839, 894
 funkcja XOR, 154
 funkcje mieszające, 894
 fuzzball, 81

G

G.lite, 175
 G2C, Government-to-consumer, 29
 generowanie
 dynamicznych stron, 747, 757
 treści dla stron, 746
 geoznakowanie, geo-tagging, 33
 GGSN, Gateway GPRS Support Node, 90
 Gigabit Ethernet, 311, 325, 327, 328
 gigabitowa karta sieciowa, 327
 gigabitowy przełącznik, 327
 głębia WWW, 773
 GMSC, Gateway Mobile Switching Center, 90
 gniazda, sockets, 81, 606
 gniazda Berkeley Sockets, 546
 GNU Privacy Guard, 747, 936
 GPON, Gigabit-capable PON, 177
 GPRS, General Packet Radio Service, 90
 GPS, Global Positioning System, 33, 132, 146
 GPSR, Greedy Perimeter Stateless Routing, 431
 gromada, swarm, 836
 gruby Ethernet, 312
 gry komputerowe, 30
 GSM, Global System for Mobile communications, 87, 196, 198

H

H.264, 102, 789
 H.323, 809
 handel elektroniczny, 26, 29
 handel mobilny, 33
 handoff, 91, 194
 handover, 91
 handshake, 917
 hard handover, 91
 harmoniczne, 117
 HDLC, High-level Data Link Control, 227, 276
 HDTV, High Definition Television, 784
 herc Hz, 130
 HF RFID, High Frequency RFID, 97
 HF, high frequency, 131
 HFC, Hybrid Fiber Coax, 207
 HID, Human Interface Device, 357
 hierarchia DOM, 753
 hierarchiczny układ, 828
 hierarchizacja adresów, 486
 hiperłącze, 716, 736
 HLR, Home Location Register, 197
 HMAC, Hashed Message Authentication Code, 908, 917, 925
 host, 46
 host mobilny, 426, 507
 hosting, 86

hotspot, 31
 HSS, Home Subscriber Server, 91
 HTML, HyperText Markup Language, 721,
 733, 736
 wersje, 738
 HTTP, HyperText Transfer Protocol, 67, 717,
 720, 768
 HTTPS, Secure HTTP, 947
 hub, 319

I

IAB, Internet Activities Board, 103
 iBGP, wewnętrzny BGP, 526
 ICANN, Internet Corporation for Assigned
 Names and Numbers, 486, 675
 ICMP, Internet Control Message Protocol, 69,
 504
 idea steganografii, 961
 IDEA, International Data Encryption
 Algorithm, 935
 identyfikacja, 850
 klienta, 728
 znaczników, 367
 identyfikator
 URI, 721
 URN, 721
 węzła, 839
 IEEE 1394, 44
 IEEE Computer Society, 27
 IEEE, Institute of Electrical and Electronics
 Engineers, 103
 IETF, Internet Engineering Task Force, 105,
 581
 IGMP, Internet Group Management Protocol,
 529
 IKE, Internet Key Exchange, 906
 iloczyn przepustowości i opóźnienia, 263
 iloczyn skalarny, 163
 IMAP, Internet Message Access Protocol, 711
 IMP, Interface Message Processor, 78
 implementacja
 RPC, 598
 usługi, 62
 warstw, 246
 IMT, International Mobile
 Telecommunications, 201
 IMT-2000, 201
 IMTS, Improved Mobile Telephone System, 192
 inetd, internet daemon, 607
 informacja nadmiarowa, 233
 infrastruktura kluczy publicznych, 901, 902
 ingerencja intruza, 898
 ingress filtering, 532

instalacja zasilająca, 30
 integralność, 850
 integralność danych, 57
 interakcja w protokołach sieciowych, 261
 interfejs, 51
 agenta użytkownika, 691
 FireWire, 44
 napowietrzny, 89
 sieciowy, 44
 Internet, 22, 49, 76, 480
 Internet Society, 105
 Internet w kablówce, 207
 internetowa suma kontrolna, 241
 internetowe protokoły transportowe, 592
 interwały graniczne, 161
 intranet, 87
 intruz, intruder, 854
 inżynieria ruchu, 436
 IP, Internet Protocol, 69, 480
 IPsec, IP security, 905
 tryb transportowy, 906
 tryb tunelowy, 906
 IPTV, IP TeleVision, 30, 801
 IrDA, Infrared Data Association, 139
 IRTF, Internet Research Task Force, 105
 IS, International Standard, 103
 IS-IS, Intermediate-System to Intermediate-
 System, 411, 416, 518
 ISM, Industrial, Scientific, Medical, 93, 137
 ISO OSI, 63
 ISO, International Standards Organization, 63,
 102
 ISP, Internet Service Provider, 47, 84, 479
 ITU, International Telecommunication Union,
 101, 131, 809
 ITU-D, Development Sector, 101
 ITU-R, Radiocommunications Sector, 93, 101
 ITU-T, Telecommunications Standardization, 101
 IXP, Internet eXchange Points, 85, 523

J

jakość obsługi, 57
 JavaScript, 749, 752, 953
 jednolity lokalizator zasobów, 718
 jednostka państwowa, 100
 jednostka transportowa, transport entity, 540
 jednostka transportowa TCP, 606
 język
 HTML, 721
 PHP, 747
 XML, 754
 jitter, 603
 JPEG, Joint Photographic Experts Group, 785

JSP, JavaServer Pages, 749
jumbogram, 504
JVM, Java Virtual Machine, 751, 951

K

kabel
koncentryczny, 122
miedziany, 129
światłowodowy, 127

kable
kategorii 3, 121
kategorii 5, 121
kategorii 6, 121

kanal, 194
dostępu
bezpośredniego, 200
wielokrotnego, 287, 292
kontrolny rozsiewczy, 199
logiczny, 812
multipleksowany, 160
nasłuch, 338
opóźnienie, 289
o dostępie swobodnym, 287
przepustowość, 289
przydziału łącza, 200
przydzielanie
dynamiczne, 290
statyczne, 288
przywoławczy, 200
RAS, 810
sygnalizacyjny
dedykowany, 200
wspólny, 200
T2, 180
wymazujący, erasure channel, 232

karta
sieciowa z odrębnym procesorem, 659
SIM, 92, 197
WiFi, 916

kaskada, product cipher, 868
kaskadowe arkusze stylów, 742
KDC, Key Distribution Center, 921, 928
Kerberos, 932
klasa ekspedycji, 809
klasa zgodności przekazywania, 516
klasy adresów IP, 491
klient, 24, 595
usługi IMAP, 711
WWW, 717

klucz, key, 840, 854
dzielony, 926
główny, 917
grupowy, 917
prywatny, 884
publiczny, 883, 889, 898
sesji, 917, 937
sieciowy, 345
symetryczny, 882, 888
tajny, 921

klucze RSA, 937
kluczowanie z przesuwem częstotliwości, 359

kod
4B/5B, 153, 324
8B/10B liniowy, 155, 328
AMI, 155
aplikacji klienckiej, 551
blokowy, 233
Graya, 158
Hamminga, 235
internetowego serwera plików, 548
LDPC, 239
Manchester, 153, 313
NRZ, 150
NRZI, 153
parzystości, 239
PIN, 192
Reeda-Solomona, 237, 238
splotowy, convolutional code, 236
strony WWW, 734
systematyczny, 233
uwierzytelniania komunikatu, 917
Walsha, 163, 164
wielomianowy, 242

koder-dekoder, 178

kodowanie, coding, 779, 853
A-law, 778
długości serii, 788
dwubiegunowe, bipolar encoding, 155
percepcyjne, 780, 781
przy podstawie 64, 699
sekwencjami, 132
widmowe, 780
 μ -law, 778

kody detekcyjne, error-detecting code, 231, 239, 282
CRC, 242
kod parzystości, 239
suma kontrolna, 241

kody diagnostyczne serwera, 762

kody korekcyjne, error-correcting code, 231, 239, 282
Hamminga, 233
kontroli parzystości, 233
Reeda-Solomona, 233
splotowe, 233

kody liniowe, 151, 155, 328
 kolejkovanie uczciwe, fair queueing, 453
 kolizje, 42, 211, 290, 336
 kolokacja, 86
 kombinacja błędów transmisji, 254
 komórka informacji, 280
 komparator, 178
 kompresja
 audio, 779
 bezstratna, 779
 JPEG, 786
 nagłówków, 652, 654
 stratna, 779
 video, 784
 komputery do noszenia, wearable computers, 34
 komputeryzacja powszechna, 30
 komunikacja
 faktyczna, 223
 laserowa, 140
 pomiędzy warstwami, 52
 w Internecie, 480
 wirtualna, 223
 komunikaty
 ACK, 814
 ICMP, 508
 klienta, 917
 MIC, 917
 NCP, 278
 o błędzie MTU, 477
 OSPF, 522
 PGP, 938
 SOURCEQUENCH, 439
 protokołu paczki DTN, 665
 komutacja, 186
 obwodów, 186, 190
 pakietów, 186–190
 pakietów z buforowaniem, 394
 znaczników, 514
 koncentrator, hub, 144, 319
 konflikt sprawiedliwości, 401
 kontakt, contact, 662
 kontrola
 błędów, 395, 569
 dopuszczenia do sieci, 436, 455
 dostępu do nośnika, 287
 przeciążeń, 433, 579, 590
 przeciążeń w TCP, 627
 kontroler BSC, 197
 kontrolka ActiveX, 752, 952
 konwergencja, 409, 583
 konwergencja trasy, 430
 konwerter elektrooptyczny, 207
 konwerter NAT, NAT box, 495
 koordynacja satelity, station-keeping, 143

koperta, envelope, 689
 korekcja błędów, 231
 korekcja błędów bezpośrednia, 231
 korelacja, 203
 koszt łączy, 412
 kotwica zaufania, trust anchors, 903
 kryptoanaliza, cryptanalysis, 854
 linearna, 882
 różnicowa, 882
 kryptografia, 853, 965
 kwantowa, 861, 863
 z kluczami publicznymi, 884, 898
 kryptologia, cryptology, 854
 kształtowanie ruchu, 447
 kubit, 862
 kurator transferu, 665
 kwadraturowa modulacja amplitudowa, 158
 kwantowanie próbkowania, 778
 kwantyzacja, 787
 kwantyzacja współczynników DCT, 787

L

L2CAP, Logical Link Control Adaptation Protocol, 358
 LAN, Local Area Network, 40
 laser, 139
 lasery półprzewodnikowe, 128
 LCP, Link Control Protocol, 276
 LDPC, Low-Density Parity Check, 238
 LED, diody świecące, 128
 LER, Label Edge Router, 515
 LF RFID, Low Frequency RFID, 97
 LF, low frequency, 131
 liczba
 pakietów, 646
 przeskoków, 431
 warstw, 72
 linia naturalna, voice-grade line, 117
 linie transmisyjne, 46
 linie zasilające, 123
 lista anulowanych certyfikatów, 904
 lista części, chunks, 835
 listy dystrybucyjne poczty, 689
 LLC, Logical Link Control, 314, 333
 losowe próbkowanie węzłów, 837
 losowe wczesne wykrywanie, 443
 LSR, Label Switched Router, 515
 LTE, Long Term Evolution, 92, 205, 348
 luminancja, 785

Ł

ładunek użyteczny, payload, 600
 łamanie haseł WEP, 916
 łańcuch buforów, 572

łańcuch zaufania, chain trust, 903
 łączy, links, 360, 715
 bezpołączeniowe asynchroniczne, 360
 dalekosiężne, 177
 DSL, 85
 dwupunktowe, 38
 międzycentralowe, 167
 rozgłoszeniowe, 38
 sieciowe, 287
 SONET, 47
 łączenie sieci, 468

M

MAC, Medium Access Control, 287, 333, 917
 MACA, Multiple Access with Collision Avoidance, 310
 macierz
 wagowa, weight matrix, 787
 współczynników DCT, 787
 MAHO, Mobile Assisted Handoff, 200
 makrobloki, 790
 maksymalna jednostka transmisji, 610
 maksymalny poziom wypełnienia bufora, 799
 MAN, Metropolitan Area Network, 44
 MANET, Mobile Ad hoc NETWORKS, 428
 maska podsieci, 485
 maskarada DNS, 943
 maskowanie
 bieżące, 781
 błędów transmisji, 591
 dźwięków, 780, 781
 pamięciowe, 781
 master, 40
 master-slave, 40
 maszyna, 46
 maszyna-klient, 705
 maszyna-serwer, 705
 m-commerce, mobile-commerce, 33
 MD5, 894
 mechanizm
 automatycznej reakcji, 693
 pilnych danych, urgent data, 609
 redukujący opóźnienia, 809
 RPC, 598
 RTS/CTS, 339
 usług zróżnicowanych, 808
 zabezpieczania transportu, 726
 media ciągle, 776
 medium rozgłoszeniowe, 42
 medium strumieniowe, 776
 metoda
 Diffiego-Hellmana wymiany kluczy, 926
 frame bursting, 327

Huffmana, 791
 kontroli parzystości LDPC, 282
 książki kodowej, 876
 licznikowa, 880, 918
 Robertsa, 295
 metody
 modulacji, 214
 protokołu SIP, 814
 ramkowania, 225, 228, 282
 zadań HTTP
 BYE, 814
 CONNECT, 762
 GET, 761
 HEAD, 761
 INVITE, 814
 OPTIONS, 762, 814
 POST, 761
 PUT, 761
 REGISTER, 814
 TRACE, 762
 MF, medium frequency, 131
 MGW, Media Gateway, 90
 miarowy ARP, gratuitous ARP, 512
 MIC, Message Integrity Check, 917
 miękkie przekazywanie transmisji, soft handoff, 204
 mikrokomórki, 194
 MIME, Multipurpose Internet Mail Extension, 697, 702, 937
 MIMO, Multiple Input Multiple Output, 336
 minimalizacja narzutu przetwarzania, 649
 mobilne WWW, 769
 mobilny IP, 529
 moc nadawcza, 346, 581
 mod, 126
 model
 DOM, 756
 każdy z każdym, 27
 klient-serwer, 24, 27
 odniesienia OSI, 63, 64
 interfejs, 71
 protokoły, 72
 usługi, 71
 warstwa aplikacji, 67
 warstwa fizyczna, 64
 warstwa łączy danych, 65
 warstwa prezentacji, 67
 warstwa sesji, 66
 warstwa sieciowa, 65
 warstwa transportowa, 66
 zła polityka, 75
 zła technologia, 74
 złe implementacje, 75
 zły moment, 73

- odniesienia TCP/IP, 67, 72
- krytyka modelu, 75
- warstwa aplikacji, 70
- warstwa internetowa, 68
- warstwa łącza danych, 68
- warstwa transportowa, 69
- referencyjny, 70
- szyfrowania, 854
- modele Poissona, 291
- modem, 84, 169
 - ADSL, 174
 - kablowy, 85, 210, 212
 - modem radiowy, 41
 - modem telefoniczny, 169, 170
- modulacja
 - amplitudy ASK, 156
 - cyfrowa, 150
 - częstotliwości FSK, 132, 156
 - fazy BPSK, 157
 - fazy PSK, 156
 - fazy QPSK, 157
 - NRZ, 150
 - QAM, 174
 - QAM-16, 158, 351
 - QAM-64, 351
 - QPSK, 351
- moduły robocze, processing modules, 725
- MOSPF, Multicast OSPF, 422
- most, bridge, 368, 379
 - główny, root bridge, 376
 - przezroczysty, 370
- MP3, MPEG audio layer 3, 780
- MP4, 780
- MPEG, Motion Picture Expert Group, 788, 792
- MPEG-2, 212
- MPEG-4 AVC, 102
- MPLS, MultiProtocol Label Switching, 396, 514–516, 914
- MSC, Mobile Switching Center, 90, 194
- MTSO, Mobile Telephone Switching Office, 194
- MTU, Maximum Transfer Unit, 610
- multemisja, multicasting, 38, 314, 421, 803
- multihoming, 525
- multihop network, 98
- multimedia, 776
- multipath fading, 93, 94
- multipleksacja, 150, 575
 - CDMA, 165
 - na bazie sekwencji rozpraszających DM, 161
 - odwrotna, 576
 - OFDM, 335
 - ortogonalna OFDM, 160
 - z podziałem czasu TDM, 161, 179, 180, 213

- z podziałem częstotliwości FDM, 158, 209, 288
- z podziałem długości fali WDM, 177, 184
- multiplexer DSLAM, 84, 279
- multipleksowanie, 168

N

- nadajnik, 251
- nadajnik SONET, 182
- nadmiarowe żądania ARP, 531
- nadzór
 - routingu, 474
 - ruchu, traffic policing, 447
- nagłówki, 54
 - Authorization, 764
 - Cache-Control, 765, 767
 - dodatkowy dla routingu, 505
 - ESP, 908
 - ETag, 765
 - Expires, 766
 - fragmentacji, 505
 - Host, 764, 768
 - If-Modified-Since, 764
 - If-None-Match, 764
 - IP, 651
 - IPv6, 501
 - Last-Modified, 765
 - pakietu UDP, 592
 - protokołu IPv4, 481
 - protokołu RTP, 601
 - segmentu TCP, 611
 - skok po skoku, 504
 - TCP, 651
 - Upgrade, 765
 - User-Agent, 764
 - uwierzytelniający IPsec, 907
 - uwierzytelniania, 505
 - wiadomości, 696
- nagłówki
 - Accept, 764
 - dodatkowe IPv6, 504
 - komunikatów HTTP, 763
 - odpowiedzi, response headers, 762
 - żądań, request headers, 762
- naliczanie do nieskończoności, 410
- NAP, Network Access Point, 82
- napęnianie
 - bajtami, byte stuffing, 227
 - bitami, bit stuffing, 227
- Napster, 28
- narzut rekonstrukcji, 476
- nasłuch kanału, 338
- nasłuch wirtualny, 338
- NAT, Network Address Translation, 493–495, 823

- natychmiastowe wysłanie, 612
 - NAV, Network Allocation Vector, 338
 - nawalnica rozgłoszeniowa, broadcast storm, 640
 - NCP, Network Control Protocol, 276
 - negatywne potwierdzenia, 274
 - negocjacja opcji LCP, 278
 - negocjacja parametrów, 57
 - negocjowanie trójstopniowe, 562, 564
 - neutralność sieci, 35
 - NFC, Near Field Communication, 33
 - NIC, Network Interface Card, 230, 245
 - NID, Network Interface Device, 174
 - nieparzystość, disparity, 156
 - niezaprzeczalność, 850
 - niezawodny strumień bajtowy, 547
 - NIST, National Institute of Standards and Technology, 103
 - nośna, 290
 - nośnik transmisji, 115, 214
 - E1, 180
 - T1, 179
 - nośniki
 - fizyczne, 51
 - magnetyczne, 119
 - wyższych rzędów, 181
 - notacja ASN.1, 900
 - NRZ, Non-Return-to-Zero, 150
 - NSAP, Network Service Access Point, 555
 - numer
 - hosta, 530
 - portu, 910
 - potwierdzenia, 613
 - ramki, 261
 - sekwencyjny, 561, 612
 - sieci, 530
 - numery
 - portów, 607
 - sekwencyjne ramek, 249
- O**
- obciążenie sieci, 824
 - obcinanie ogona, 452
 - obliczanie
 - sumy kontrolnej CRC, 243
 - tras, 415
 - obsługa
 - dystribucji treści, 828
 - formularza HTML, 748
 - przeciążenia, 443
 - zintegrowana, integrated services, 809
 - obszar
 - pokrycia, footprint, 144
 - szkieletu, 520
 - obszary, 519
 - obwód, circuit, 57
 - obwód wirtualny, VC, 280, 396, 400
 - ochrona
 - kluczy, 945
 - na całej drodze pakietu, 570
 - prywatności, 955
 - odbicie fali, 94
 - odbiornik, 251
 - odkrywanie trasy, 428
 - odległość Hamminga, 233
 - odliczanie binarne, 303
 - odpowiedź, 25
 - odpowiedź ROUTE REPLY, 429
 - odrzućanie pakietów, 442
 - odstęp
 - AIFS, 342
 - DIFS, 342
 - EIFS, 343
 - SIFS, 342
 - odstęp między ramkami, 342
 - odtwarzacz multimediiów, 794, 797
 - OFDM, Orthogonal Frequency Division Multiplexing, 94, 159, 334
 - OFDMA, Orthogonal Frequency Division Multiple Access, 351
 - okablowanie
 - 10-gigabit Ethernet, 330
 - Fast Ethernet, 324
 - Gigabit Ethernet, 327
 - okazja do nadawania, 343
 - okna
 - przesuwne, 259, 620
 - nadawcze, 258
 - odbiorcze, 258
 - przeciążenia, 628
 - opcje IP, 484
 - operator ISP, 915
 - opłata za tranzyt, 86
 - opóźnienie, 580
 - kolejkowania, 189
 - pakietu, 458
 - potwierdzeń, 621
 - oprogramowanie
 - podsieci, 79
 - pośredniczące, middleware, 22
 - sieciowe, 50, 108
 - sprzętowe, firmware, 55
 - szpiegowskie, spyware, 732
 - OSPF, Open Shortest Path First, 411, 416, 517
 - otwarty przekaznik poczty, 708
 - OUI, Organizationally Unique Identifier, 314

P

- P2P, Peer-to-Peer, 27, 29, 817, 832
- paczka, bundle, 661
- pakiet, 38, 58
 - parzystości, 795
 - ROUTE REQUEST, 429
 - rozgłoszeniowy, 42
 - sondujący, 621
 - SYN, 912
 - tłumienia, choke packet, 439
 - VoIP, 808
 - zakłócający, 315
- pakiety
 - ekspresowe, 464
 - o stałej wielkości, 212
- pamięć cache, 725
- pamięć cache serwera DNS, 942
- PAN, Personal Area Networks, 39
- pancerz ASCII, ASCII armor, 699
- PAR, Positive Acknowledgement with Retransmission, 255
- parowanie proste zabezpieczone, 360
- parowanie urządzeń, 355
- pasma satelitarne, 143
- pasmao
 - ISM, 138
 - kanalu transmisyjnego, 152
 - nielicencjonowane, 138
 - podstawowe, 150
 - pogranicza, 159
 - przepustowe, 115, 150
 - sieciowe, 56
 - U-NII, 138
- pasywna sieć optyczna PON, 176
- Path MTU, 475
- PAWS, Protection Against Wrapped Sequence numbers, 564, 614
- PCF, Point Coordination Function, 337
- PCM, Pulse Code Modulation, 178, 600
- PCS, Personal Communications Services, 196
- pełny duplex, full-duplex, 121
- pętla lokalna, 167, 168
- PGP, Pretty Good Privacy, 935
- phishing, 37
- PHP, 747–749
- piaskownica, sandbox, 952
- piconet, 355
- pierścień kluczy
 - prywatnych, 938
 - publicznych, 939
- pierwszorzędne serwery nazw, 684
- pięciokrotka, 611
- piggybacking, 257
- pijawki, leechers, 837
- pikosieć, 355, 919
- piksel, 783
- piłowy obraz pracy, 636
- PIM, Protocol Independent Multicast, 424, 529
- PIN, Personal Identification Number, 360
- PKI, Public Key Infrastructure, 901, 926
- platforma wiki, 29
- plik protocol.h, 247
- plik torrent, 835
- pliki host.txt, 674
- pobieranie strony, 718
- poczta
 - elektroniczna, 25, 686, 843
 - niechciana, *Patrz* spam
 - ślimacza, 687
- podcast, 801
- podnośna, 160
- podpis cyfrowy, 887–889, 926
- podpisywanie
 - kodu, code signing, 952
 - zbiorów RRSet, 945
- podsieć, 46, 49, 486
- podszycanie się, 942
- podwarstwa
 - łącza logicznego, 350
 - MAC, 288, 349
 - sterowania dostępem do nośnika, 976
 - zabezpieczeń, 349
 - zbieżności, 350
- podział max-min, 581, 582
- podział ramek, 340
- podział sieci 802.11, 95
- pojemność, 657
- poła certyfikatu X.509, 901
- pole
 - ack, 248
 - info, 248
 - kind, 248
 - potwierdzenia, 261
 - sekwencji, 344
 - seq, 248
- polecenia protokołu IMAP, 712
- polecenie RCPT, 706
- połączenia dwupunktowe, 608
- połączenia
 - międzyn sieciowe, 368
 - nadmiarowe mostów, 374
 - pełnodupleksowe, 608
 - transportowe, 555
- połączenie
 - oczekujące, 815
 - równoległe, 760

- połączenie
 - TCP, 615, 758
 - nawiązywanie, 615
 - zarządzanie, 617
 - zwalnianie, 616
- trwale, 758, 760
- VoIP, 812
- wdzwaniane, dial-up, 84
- połączeniowa
 - usługa sieciowa, 540
 - usługa transportowa, 540
- pomiar wydajności sieci, 641
- PON, Passive Optical Network, 176
- POP, Point of Presence, 85
- POP3, Post Office Protocol Version 3, 712
- port, 606
 - docelowy, 496
 - źródłowy, 496
- portmapper, 556
- porty, 555
 - przełącznika, 42
 - zarezerwowane, 607
- potok, pipe, 542
- potokowe przesyłanie ramek, 264
- POTS, Plain Old Telephone Service, 173
- potwierdzanie na całej drodze przepływu, 579
- potwierdzenia
 - odbioru, 630
 - powielone, 633
 - wybiórcze SACK, 637
- potwierdzenie
 - ACK, 339
 - skumulowane, 268
 - zbiorcze, 612, 624
- poufność, 850
- powiadomienie o przeciążeniu, 439
- powolny rozruch, 635
- powtórzenia selektywne, selective repeat, 265
- poziom hierarchii nazw, 675
- poziom usług, 447
- poziomy cacheowania, 826
- poznawanie sąsiadów, 412
- półdupleks, half-duplex, 121, 326
- PPP, Point-to-Point Protocol, 227, 275
- PPPoA, PPP over ATM, 281
- praca potokowa, pipelining, 264
- praca wielowątkowa, multithreading, 725
- prawa autorskie, copyright, 962
- prawdopodobieństwo
 - kolizji, 296
 - przejęcia kanału, 305
 - retransmisji w każdej szczelinie, 317
- prawo
 - Metcalfe'a, 26
 - Zipfa, 819
- preambuła, preamble, 228
- prefiks, 485
- prefiksy metryczne, 106
- prędkość
 - przesyłu symboli, 152
 - światła, 130
 - transmisji, 94
 - wysyłania danych, 584
- problem
 - dwóch armii, 565
 - odkrytej końcówki, 309, 338
 - ostatniego kilometra, 165
 - trzech misiów, 492
 - ukrytej końcówki, 309, 338
 - wybranego tekstu otwartego, 856
 - złamania szyfru, 856
 - znanego tekstu otwartego, 856
- proces odwzorowujący nazwy, 674
- profil
 - HID, 357
 - interkomu, 357
 - połączenia wdzwanianego, 357
 - sieci osobistej, 357
- profile
 - do strumieniowania dźwięku, 357
 - zestawu głośnomówiącego, 357
 - zestawu słuchawkowego, 357
- profilowanie użytkowników, 36
- program pocztowy, 690, 704
- program telnet, 708
- programy CGI, 747
- projekt
 - Globalstar, 147
 - Iridium, 147
- projektowanie
 - hostów, 645
 - warstw, 55
- prosty ALOHA, pure ALOHA, 295
- protokoły
 - 802.11, 41, 333, 590
 - 802.16, 349
 - bezkolizyjne, 300
 - beziprzewodowych sieci LAN, 308
 - Bluetooth, 358
 - dla szybkich sieci, 655
 - dostarczania końcowego, 710
 - łącza, 282
 - łącza ADSL, 280
 - TCP/IP, 80
 - transportowe, 571
 - transportowe czasu rzeczywistego, 598
 - typu żądanie-odpowiedź, 757
 - URL, 719
 - uwierzytelniania, 920

- warstwy sieciowej, 394
- wielokrotnego dostępu, 292
- WWW, 844
- z ograniczoną rywalizacją, 304
- protokół, 51, 62
- „wróć do n”, 265
- 1-persistent CSMA, 297
- about, 720
- adaptacyjnego przejścia przez drzewo, 306
- ALOHA, 293
- ARP, 510
- BB84, 861
- binarnego odliczania wstecz, 304
- BitTorrent, 835
- Bluetooth, 355
- bram granicznych, 522
- bram wewnętrznych, 473, 517
- bram zewnętrznych, 473, 517, 522
- CCMP, 918
- CSMA/CD, 298
- DCCP, 548
- DHCP, 513
- DNS, 944
- dostępu do wiadomości internetowych, 711
- drzewa, 387
- dynamicznej konfiguracji hosta, 513
- EAP, 916
- file, 720
- ftp, 720
- G.711, 810
- H.245, 810
- H.323, 813, 809, 815
- HTTP, 717, 720
- HTTPS, 947
- ICMP, 508
- IKE, 906
- inicjowania sesji, 813
- IP, 395
- IPv4, 481
- IPv6, 498
- ISAKMP, 906
- IS-IS, 416, 517
- L2CAP, 358
- LCP, 276
- MACA, 310
- mailto, 720
- NCP, 276
- Needhama-Schroedera, 929
- nonpersistent CSMA, 298
- okna przesuwne, 610
- paczki, 664, 665
- podwarstwy MAC 802.11, 336
- podwarstwy MAC 802.16, 352
- połączenia wstępnego, 557
- potwierdzeń, 255
- p-persistent CSMA, 298
- PPP, 275, 276
- przesyłu hipertekstu, 757
- przesyłu plików, 497
- rezerwacji zasobów, 460
- RFC, 358
- rozwiązywania adresów, 511
- RTCP, 602
- RTP, 599, 600
- RTSP, 720
- rywalizacji CSMA/CD, 371
- SCTP, 548, 576
- simpleksowy, 250, 253
- SIP, 720, 813, 815
- SLIP, 276
- SMTP, 689, 707
- SOAP, 756
- SSL, 948
- transmisja danych, 950
- SST, 548
- stop-and-wait, 251
- stopujący, 570
- TCP, 564, 592, 605, 609, 638
- TKIP, 918
- token-bus, 302
- token-ring, 302
- trzystopniowego negocjowania, 667
- UDP, 592, 807
- urzędu pocztowego, 712
- uwierzytelniania
- Needhama-Schroedera, 929
- Otwaya-Reesa, 930
- używający powtórzeń selektywnych, 269
- WAP, 769
- wektora ścieżki, 525
- wykrywania usług, 358
- wyzwanie-odpowiedź, 921
- z oknem przesuwne, 258, 266, 270, 570
- z mapą bitową, 301
- z rezerwacją, 301
- z wykrywaniem nośnej, 297
- zarządzający kanałem, 349
- zarządzania grupami, 529
- zarządzania łączem, 360
- zwalniania połączenia, 567
- proxy, 826
- proxy cacheujące, 768
- proxy WWW, Web proxy, 825, 828
- próbka reprezentatywna, 642
- próbkowanie fali, 778
- próg wolnego rozruchu, 632
- prymityw, 543, 546
- prymitywy usług transportowych, 542

prywatność, 346, 955
 przebieg pilowy, 635
 przeciążenie, congestion, 57, 431, 443, 585
 przeciążeniowe załamanie sieci, 628
 przeglądarka, 727
 przeglądarka WWW, 715
 przekazywanie, forwarding, 400

- ekspresowe, expedited forwarding, 463
- gwarantowane, assured forwarding, 464
- pakietu IP, 516

 przekierowanie DNS, DNS redirection, 828, 832
 przełączanie

- cut-through, 58
- kontekstów, 647
- store-and-forward, 58
- w locie, 373

 przełączany Ethernet, 319
 przełącznik, 42, 46, 320
 przełącznik Ethernetowy, 321, 379
 przepłot, interlace, 240, 783, 796
 przepływ, flow, 445
 przepływ informacji, 54
 przepływność, 117
 przepływność maksymalna kanału, 118
 przepustowość

- efektywna, 212
- pętli lokalnej, 172
- skuteczna, 580
- transmisji, 57

 przeskakiwanie częstotliwości, frequency hopping, 919
 przestrzeń nazw

- DNS, 675
- reprezentacja drzewiasta, 677
- z podziałem na strefy, 682

 przesyłanie znaku, 114
 przeszacowanie, overprovisioning, 444
 przetwarzanie w chmurze, cloud computing, 744
 przetwarzanie w warstwach, 469
 przewidywanie nagłówka, header prediction, 651
 przezroczystość sieci, 382
 przybliżenia sygnału, 116
 przydział

- częstotliwości, 209
- przepustowości, 583
- pasma, 208
- zmienny pasma, 584

 przydzielanie kanału

- dynamiczne, 43, 290
- statyczne, 42, 288

 przyspieszanie addytywne, 633
 pseudolosowe sekwencje kodujące, 203

pseudonagłówek IPv4, 594
 PSK, Phase Shift Keying, 156
 PSTN, Public Switched Telephone Network, 90, 165
 publiczna komutowana sieć telefoniczna PSTN, 90, 165
 punkt dostępowy, access point, 31, 41, 93
 punkt zborny, rendezvous point, 423
 punkty dostępu do usługi

- sieciowej, 555
- transportowej, 555

Q

QAM, Quadrature Amplitude Modulation, 158
 QAM-128, 211
 QAM-16, 158, 351
 QAM-256, 210
 QAM-64, 158, 351
 QoS, Quality of Service, 57, 346, 445, 600
 QPSK, Quadrature Phase Shift Keying, 157, 351

R

RA, Regional Authorities, 902
 radio internetowe, 801
 radiodyfuzyjna telewizja satelitarna, 144
 ramki oczekujące, 267
 ramki, 179, 222

- długość minimalna, 315
- nagłówków, 222
- numery sekwencyjne, 229, 249
- pole ack, 248
- pole info, 248
- pole kind, 248
- pole seq, 248
- pole treści, 222
- potwierdzenie, 229
- potwierdzenie negatywne, 229
- przesyłana w jednym kierunku, 257
- stopka, 222
- wielokrotne nadawanie, 229

 ramka, frame, 248

- 802.11, 343
- 802.16, 354
- 802.1Q, 385
- 802.3, 386
- 802.5, 386
- AAL, 281
- AAL5, 281, 282
- ACK, 274
- CTS, 310, 339
- danych, 65, 343
- danych Bluetooth, 361
- Ethernetu, 313

- GSM, 199
- OFDMA, 352
- potwierdzająca, 65
- RTS, 310, 339
- sondująca, beacon frame, 341
- standardowa, 354
- sterująca, 343
- z negatywnym potwierdzeniem NAK, 274
- z żądaniem pasma, 354
- zarządzania, 343, 344
- ramki
 - filmu, 791
 - gigantów, jumbo frames, 328
- ramkowanie, 225
- real-time, 57
- reasocjacja, 345
- RED, Random Early Detection, 443
- redundancja, 864
 - czasowa, 789
 - przestrzenna, 789
 - sygnalizacji, 228
- regiony, 417
- reguła samopodobieństwa, 819
- rejestr HLR, 197
- rejestr VLR, 197
- rekord pamiętany, 683
- rekord wiarygodny, 683
- rekordy zasobów domenowych, 678
- replikowanie treści, 828
- repozycja wiadomości, 692
- retransmisja, 141
- RFC, Request For Comments, 104
- Rfcomm, Radio Frequency communication, 358
- RFID, Radio Frequency IDentification, 31, 96, 363
- Rijndael, 873
- RLE, Run-Length Encoding, 788
- RNC, Radio Network Controller, 89
- robot indeksujący, 773
- rodzajowe domeny najwyższego poziomu, 676
- ROHC, RObust Header Compression, 654
- root CA, 902, 939
- router, 46
 - bezprzewodowy, 41
 - brzegowy, 470
 - brzegowy obszaru, 520
 - brzegowy systemu autonomicznego, 520
 - docelowo, 470
 - wieloprotokołowy, 471
- rutery
 - sąsiadujące, 521
 - szkieletowe, 520
 - wewnętrzne, 519
- routing
 - Bellmana-Forda, 408
 - bezklasowy międzydomenowy, 488
 - gorącego ziemniaka, 527
 - hierarchiczny, 416, 418
 - mobilny, 426
 - partnerski, peer routing, 524
 - QoS, 456
 - rozplywowy, flooding, 406, 419
 - rozsyłania grupowego, 421
 - sesji, 400
 - statyczny, 402
 - w podsieci, 398
 - w sieci datagramowej, 397
 - w sieciach ad hoc, 427
 - w sieciach złożonych, 473
 - w trybie anycast, 424
 - wczesnego wyjścia, 527
 - wewnętrzny, 517
 - wieloadresowy, multidestination routing, 418
 - z uwzględnieniem warunków ruchu, 434, 435
 - z użyciem stanu połączeń, 408, 411
 - z użyciem wektorów odległości, 408
 - ze stanem łączy, 415
 - zewnętrzny, 517
- rozgałęźnik, 174
- rozgłaszanie, broadcasting, 314, 418
- rozkład Poissona, 295
- rozkład Zipfa, 820
- rozmiar próbki, 642
- rozpraszanie
 - widma, 133
 - wsteczne, backscatter, 97
 - zwrotne, backscatter, 365
- rozprowadzanie wzdłuż ścieżki odwrotnej, 419
- rozsyłanie grupowe, multicast routing 38, 421, 528
- rozszerzenia przeglądarek WWW, 724, 953
- rozwiązywanie nazw, name resolution, 683
- równanie Shannona, 131
- równoważenie obciążenia, 823
- różnicowanie ścieżki transmisji, 93
- RPC, Remote Procedure Call, 595
- RPR, Resilient Packet Ring, 303
- RRSets, Resource Record Sets, 944
- RSA, 885
- RSV, Resource reSerVation Protocol, 460
- RTCP, Real-time Transport Control Protocol, 602
- RTP, Real-time Transport Protocol, 70, 598
- RTS, Request to Send, 310
- RTTVAR, Round-Trip Time VARIation, 626

ruch

- długotrwały, 819
- FTP, 818
- HTTP, 911
- krótkotrwały, 819
- P2P, 818
- przekaz wideo, 818
- sieciowy, 818
- SMTP, 818
- VoIP, 818
- WWW, 818
- rywalizacja, 387

S

S/MIME, 939

SACK, Selective ACKnowledgement, 614, 637

satelity

- CubeSats, 148
- geostacjonarne, 142
- GPS, 146
- Iridium, 147
- LEO, 146
- MEO, 146
- telekomunikacyjne, 141, 144

scatternet, 355

schemat adresacji, 469

schemat blokowy DES, 870

SCO, Synchronous Connection Oriented, 360

scrambling, 154

SCT, Stream Control Transmission Protocol, 576

SCTP, Stream Control Transmission Protocol, 548

SDH, Synchronous Digital Hierarchy, 181

seed, 836

segment, 592, 609

sekwencja Barkera, 335

sekwencja kodująca, chip sequence, 162

sensory, 98

serwer, 24, 595

- biletów, 931
- lustrzany, mirror, 828
- macierzysty, 828
- nazw, 682
- plików, 548
- pocztowy, 693
- poczty anonimowej, 956
- pośredniczący, 824
- pośredniczący z buforowaniem, 825
- procesów, 557
- uwierzytelniania, 916, 931
- WWW, 724, 726
- wykonawczy, 931

sesja, 66

SGSN, Serving GPRS Support Node, 90

SHA-1, Secure Hash Algorithm 1, 892

SHA-2, 894

sieci

- 1 warstwy, Tier 1 networks, 479
- 802.11, 332
- ad hoc, 332
- bezprowadowe, 41
- brzegowe, 479
- dystribucji treści, 826
- komputerowe, 108
- lokalne, 479
- na liniach zasilających, 44
- niewrażliwe na opóźnienia, 660
- osobiste PAN, 39
- przewodowe i bezprzewodowe, 308
- sensorowe, 34
- szkieletowe, 479
- szkieletowe systemów telefonicznych, 214

sieć, 50

- 2.5G, 201
- 802.11, 469
- ad hoc, 93, 428
- ADSL, 119
- ALOHA, 312
- ARPANET, 843
- ATM, 281
- bezprowadowa, 31, 93
- BitTorrent, 834
- CDN, 817, 832
- CND, 826
- CSNET, 81
- datagramowa, 396, 399
- DECNET, 440
- domowa, 44
- dostępu radiowego, 89
- DTN, 661, 663
- internetowa, 47, 49
- internetwork, 466
- ISP, 47
- kablowa, 214
- komórkowa, 87, 88
- komputerowa, 22
- końcowa, stub network, 520, 524
- korporacyjna, 40
- logiczna, 42
- lokalna LAN, 40
 - bezprowadowa, 41
 - przewodowa, 41
- LTE, 92
- miejska MAN, 44
- NSFNET, 82
- obwodów wirtualnych, 396, 399

- operatora ISP, 474
- P2P, 83, 817, 832–834
- P2P strukturyzowana, 839
- piconet, 356
- powielonych łączy bezpośrednich, 98
- prywatna, 913
- przełączana, switched Ethernet, 42
- rdzenna, core network, 89
- RFID, 96, 363
- rozległa WAN, 46, 48
- rozrzucona, 355
- równorzędna, 27, 833
- satelitarna, 49
- scatternet, 356
- sensorowa, sensor network, 98
- społecznościowa, social networking, 28
- szkieletowa ISP, 85
- szkieletowa NSFNET, 82
- telefoniczna, 810
- token-ring, 303
- VLAN, 383
- wielodostępowa, multiaccess networks, 518
- WiMAX, 92
- wirtualna, 42
- WWW, 83, 817, 843
- z komutacją pakietów, 475
- z przeciążeniami, 438
- złożona, 49, 466
- zorientowana połączeniowo, 469
- SIFS, Short InterFrame Spacing, 342
- SIM, Subscriber Identity Module, 92, 197
- simpleks, 121
- SIP, Session Initiation Protocol, 809, 813
- SIPP, Simple Internet Protocol Plus, 499
- skalowalność sieci, 56
- składowe harmoniczne, 115
- skojarzenie bezpieczeństwa, 906
- skok po skoku, hop-by-hop, 442
- skrącanie ramek, 340
- skrętka, 120
 - kategorii 3, 323
 - kategorii 5, 121, 323
 - nieekranowana UTP, 330
- skrót SHA-1, 839
- skrypty CGI, 749
- skrypty PHP, 749
- skrzynka
 - permutacyjna, 867
 - pocztowa, 689
 - podstawieniowa, 868
- Skype, 809
- SLA, Service Level Agreement, 447
- slave, 40
- SLIP, Serial Line Internet Protocol, 276
- słowo kodowe, codeword, 233
- SMTP, Simple Mail Transfer Protocol, 70, 689, 757
 - rozszerzenia, 707
- SOAP, Simple Object Access Protocol, 756
- SoF, start of frame delimiter, 313
- soft handover, 91
- solitony, 127
- SONET, Synchronous Optical NETwork, 177, 181, 275
- spam, 687, 692, 710
- SPE, Synchronous Payload Envelope, 183
- specyfikacja przepływu, 457
- specyfikacja Q.931, 810
- spektrum nośnika, 132
- sprawcy ataków, 850
- sprzęg pojemnościowy, capacitive coupling, 155
- sprzężenia między protokołami, 659
- sprzężenie zwrotne szyfrogramu, 878
- SRTT, Smoothed Round-Trip Time, 625
- SSL, Secure Socket Layer, 947
- SST, Structured Stream Transport, 548
- stacja
 - bazowa, base station, 93, 203
 - bazowa telefonii komórkowej, 89
 - czołowa, head end, 45, 85, 206
 - radiowa, 805
- stan połączeń, 413
- stan S0, 577
- stan S1, 577
- standard
 - 802.11, 31, 99, 343–346, 915
 - 802.11a, 335
 - 802.11b, 335
 - 802.11g, 335
 - 802.11i, 96, 916
 - 802.11n, 334, 336
 - 802.16, 45, 205, 347, 387
 - 802.1D, 377
 - 802.1Q, 384, 386
 - 802.3, 42, 311, 314
 - 802.3ab, 325
 - 802.3u, 323
 - 802.5, 303
 - ADSL, 174
 - ADSL2, 174
 - ADSL2+, 174
 - DIX, 312
 - formatu certyfikatów, 900
 - IETF, 100
 - IS-95, 196
 - SMTP, 694
 - T1, 179

- standardy
 - de facto, 99
 - de iure, 100
 - IEEE, 177
 - sieci lokalnych, 93
- stanowe zapory sieciowe, stateful firewalls, 911
- stany automatu skończonego, 618
- stany zasilania, 356
- statyczne dzielenie kanału, 290
- STDM, Statistical Time Division Multiplexing, 161
- steganografia, 960, 962
- sterowanie
 - dialogiem, 66
 - dopuszczeniem do sieci, admission control, 434
 - przepływem, flow control, 56, 230, 569
 - informacje zwrotne, 230
 - szybkość transmisji, 230
- stoper
 - przetwarzania, persistence timer, 627
 - retransmisji, 624
 - żywołności, keepalive timer, 627
- stopień wykorzystania łącza, 263
- stos protokołów, 52, 56
 - 802.11, 333
 - 802.16, 349
 - ADSL, 280
 - H.323, 811
- stos warstw, 51
- stosunek sygnał/szum, 118
- strategie klienta i serwera, 578
- strażnik, gatekeeper, 810
- strefa, zone, 682, 810
- strefa zdemilitaryzowana, 911
- strona, page, 715
 - dynamiczna, 717, 744
 - HTML, 721
 - statyczna, 717
- strumieniowanie, 802
 - na żywo, 801
 - utworów, 794
 - w multimedii, 803
 - z dysku, 792
- strumień bajtów, 226
- strumień bitów, 225
- STS-1, Synchronous Transport Signal-1, 182
- stub klienta, 595
- stub serwera, 595
- suma kontrolna, checksum, 241
 - cykliczna, 242
 - Fletchera, 242
- superramka, 179
- sygnalizacja
 - kradzionym bitem, 180
 - poza kanałem, 180
 - przebiegów, 586
 - w kanale, 180
 - we wspólnym kanale, 180
- sygnał
 - 100 Mb, 323
 - binarny, 116
 - oryginalny, 116
 - przerwania, 249
 - taktujący, 153
- sygnały zrównoważone, 155
- sygnatura do wiadomości, 694
- sygnatura HMAC, 917
- SYN cookies, 616
- SYN flood, 616
- synchronizacja, 66
- synchronizacja zegarów, 346
- syndrom błędu, 236
- syndrom głupiego okna, 622
- system
 - 3G, 88
 - adresowania, 56
 - ALOHA, 292
 - GSM, 196
 - klucza jednokrotnego, 860
 - nazw, 56
 - PKI, 926
 - rywalizacyjny, 293
 - Strowgera, 186
 - telefoniczny, 77, 166, 213, 214
 - centrale telefoniczne, 168
 - łącza dalekosiężne, 168
 - pętle lokalne, 168
 - telefonii komórkowej, 191
 - telefonii stacjonarnej, 214
 - trzeciej generacji, 87
 - X.400, 694
- systemy
 - autonomiczne, 474, 524
 - rozproszone, 22
 - wieloprosesorowe, 39
- szczelina, slot, 290, 295
- szczelinowy ALOHA, slotted ALOHA, 295
- szereg Fouriera, 114
- szeregowanie ruchu, 346
- szerokość pasma, 115
- szum
 - elektryczny, 123
 - kwantyzacji, 778
 - nietermiczny, 159
- szybka retransmisja, 634
- szybka ścieżka, 650

szybki Ethernet, Fast Ethernet, 322
 szybkie przywracanie, fast recovery, 635
 szybkość
 hosta, 645
 sieci, 645
 transmisji, 117, 184, 340
 szyfr
 Cezara, 856
 podstawieniowy, 856
 przestawieniowy, 858
 Rijndael, 919
 strumieniowy, 879, 880
 szyfrogram, ciphertext, 854
 szyfrogram bez wiadomości oryginalnej, 856
 szyfrowanie, ciphering, 853
 blokowe, 867
 łącza, link encryption, 851
 PGP, 935
 ramek, 352
 transmisji, 917

Ś

ścieżka
 AS, 525
 certyfikacji, certification path, 903
 przepływu danych, 827
 śledzenie użytkownika, 36, 731
 światłowód, 85, 124, 176
 światłowód wielomodowy, 126

T

tablica
 przemieszczania, 371
 routingu, 400, 409
 wskazań, finger table, 841
 takt potwierdzeń, ack clock, 630
 Tanenbaum Andrew, 1001
 taśma Ultrium, 119
 TCG, Trusted Computing Group, 964
 TCM, Trellis Coded Modulation, 170
 TCP, Transmission Control Protocol, 69, 592, 605, 758
 TDD, Time Division Duplex, 351
 TDM, Time Division Multiplexing, 161, 198
 technika „wróc do n”, 266
 techniki uwierzytelniania, 852
 technologia 3G, 202
 tekst otwarty, 854
 telefon internetowy, 25
 telefonia
 internetowa, 775, 806
 IP, 25
 stacjonarna, 208

telefony
 komórkowe, 190
 mobilne 1G, 192
 mobilne 2G, 195
 mobilne 3G, 200
 telekonferencja, 805
 telewizja kablowa, 45, 206
 telewizja zbiorcza, 206
 TELNET, 70
 terminal, 810
 terminal zdalny, 621
 TGS, Ticket Granting Server, 931
 TLS, Transport Layer Security, 950
 tłumienie, 441
 tłumienie światła, 126, 127
 token, 302
 topologia fizyczna, 382
 topologia logiczna, 382
 torrent, 835
 TPDU, Transport Protocol Data Unit, 543
 traceroute, 509
 tracker, 835
 transfer
 danych, 222
 poczty, 709
 wiadomości, 704
 transformacja treści, 770
 transkodowanie, 770
 translacja
 adresów sieciowych, 493
 NAT, 496
 transmisja
 bezprowadowa, 130
 danych, 114
 dźwięku i wideo, 774
 mikrofalowa, 135
 obrazu, 57
 optyczna, 125, 139
 pełnodupleksowa, 257
 radiowa, 133
 światła, 126
 w czasie rzeczywistym, 774
 w paśmie podstawowym, 150
 w paśmie przepustowym, 156
 z rozpraszaniem widma, 132
 z żetonem, 302
 transponder, 141
 transpozycja, marshaling, 595
 transpozycja kolumnowa, 858
 trasowanie, 48, 56
 trasowanie cebulowe, 958
 trasy anycast, 425
 trasy BGP, 526
 triple DES, 871
 trójkątniki, 857

tryb

- nasłuchu, 322
- oszczędności energii, 341
- pełnoduplexowy, 329
- progresywny, 783

tryby rozprowadzania, 424

tryby szyfrowania, 876

TSAP, Transport Service Access Point, 555

TTL, Time to live, 429

tunelowanie pakietów, 427, 471

twierdzenie Nyquista, 170

Twitter, 28

tworzenie pakietów stanu połączeń, 413

TXOP, 343

typ MIME, 701, 721

typy

- ramek MPEG-1, 790
- rekordów zasobowych DNS, 679
- usług, 59

U

UDP, User Datagram Protocol, 69, 592

UHF RFID, Ultra- -High Frequency RFID, 97

UHF, Ultra High Frequency, 364

umacnianie prywatności, 863

UMTS 3G, 100

UMTS, Universal Mobile

Telecommunications System, 87, 202

unicast, 424

unicasting, 38

U-NII, Unlicensed National Information

Infrastructure, 137

unikanie przeciężeń, 438, 648

unikanie przeterminowań, 648

URI, Uniform Resource Identifiers, 721

URL, Uniform Resource Locator, 718

URN, Uniform Resource Names, 721

USB, Universal Serial Bus, 153, 227

usługa, 62

Akamai, 832

asocjacja, 345

bezpołączeniowa, connectionless, 58, 396

bezpołączeniowa bez potwierdzeń, 223

bezpołączeniowa z potwierdzeniami, 224

DNS, 944

dynamicznego wyboru częstotliwości, 346

dystrybucja, 346

elementarna, 539

gwarantowana, 58

maksymalizująca transfer, 354

oparta na klasach, 462

połączeniowa, 58, 395, 397

połączeniowa z potwierdzeniami, 224

potwierdzonych datagramów, 59

prywatności, 346

sterowania mocą nadawczą, 346

szeregowania ruchu, 346

TCP, 606

transportowa, 539

tranzytu, 523

QoS, 346

połączeniowa, connection-oriented, 57, 395

reasocjacja, 345

uwierzytelnienie, 345

wieczności, eternity service, 959

xDSL, 172

ze stałą szybkością transmisji, 353

ze zmienną szybkością transmisji, 353

zintegrowana IETF, 533

zintegrowana, integrated services, 459

zróżnicowana, differentiated services, 462

żądania i odpowiedzi, 59

ustanawianie połączenia, 558

ustawa DMCA, 963

usuwanie tras, 430

UTP, Unshielded Twisted Pair, 121

utrata danych, 565

utrata mocy sygnału, 134

UWB, Ultra WideBand, 133

uwierzytelnianie authentication, 345, 920, 928

dwukierunkowe, 922

protokół Needhama-Schroedera, 929

protokół Otwaya-Reesa, 930

w oparciu o Kerberos, 931

wzajemne, 352

z użyciem HMAC, 925

z użyciem kluczy publicznych, 933

za pośrednictwem KDC, 928

uzyskiwanie adresu IP, 942

V

VC, virtual circuit, 396

VLAN, Virtual LAN, 42, 382

VLR, Visitor Location Register, 197

vocoder, 779

VoD, Video on Demand, 792

VoIP, Voice over IP, 25, 58, 806

VPN, Virtual Private Network, 23, 47, 473, 906, 913

VSAT, Very Small Aperture Terminal, 144

W

W3C, World Wide Web Consortium, 105, 715, 754

waga WFQ, 458

WAN, Wide Area Network, 46

- WAP, Wireless Application Protocol, 769
- warianty kwantyzacji
 - A-law, 178
 - μ -law, 178
- warstwa
 - aplikacji, 978
 - bezpiecznych połączeń, 947
 - fizyczna, 113, 213, 975
 - fizyczna 802.11, 334
 - fizyczna 802.16, 350
 - fizyczna EPC Gen 2, 364
 - łącza danych, 221, 282, 976
 - radiowa, 359
 - równorzędna, 51
 - sieciowa, 50, 223, 393, 977
 - sieciowa Internetu, 478
 - sterowania łączem, 358, 359
 - transportowa, 539, 978
- warunkowe żądanie GET, 767
- wątek czołowy, front-end, 725
- WCDMA, Wideband CDMA, 88, 202
- WDM, Wavelength Division Multiplexing, 184
- Web crawling, 773
- Webmail, 713
- WEP, Wired Equivalent Privacy, 96, 345, 916
- weryfikacja
 - kontrolek ActiveX, 952
 - poprawności MIC, 917
 - tożsamości, 852
- Wetherall David, 1002
- węzeł
 - główny, master, 355, 423
 - nieodcięty, 837
 - odcięty, 837
 - podrzędny, slave, 355
 - sieci, 46
 - światłowodowy, 207
- węzły CDN, 828, 832
- WFQ, Weighted Fair Queueing, 454
- wiadomość
 - nagłówek, header, 690
 - treść, body, 690
- wiadomość wieloczęściowa, 703
- wiadro żetonów, 437, 448
- wiązanie bloków szyfrowanych, 877
- wiązki punktowe, spot beam, 144
- widmo elektromagnetyczne, 130, 131
- wielodrożny zanik sygnału, 135
- wielomian generujący, 242
- wieloprotokołowa komutacja etykiet, 514
- wielowątkowy serwer WWW, 725
- WiFi, 41, 93
- WiFi Alliance, 99
- WiMAX, 45, 205, 347, 351
- wirtualna
 - maszyna Javy, 951
 - sieć lokalna, 380
 - sieć prywatna, 47, 914
- wirusy, 954
- własna pętla lokalna, 207
- własność intelektualna, 962
- właściciel treści, 831
- właściwości „pamięciowe” sieci, 554
- właściwości fal radiowych, 134
- włączanie linii, 279
- włókna światłowodowe, 128
- włókno jednomodowe, 126
- wolność słowa, 958
- WPA2, WiFi Protected Access 2, 345, 915
- wrażliwość czasowa słuchu, 777
- wrzeciono czasu, timing wheel, 652
- wskaźnik pilności, 612
- współczynnik kodu, 233
- współczynnik Nyquista, 151
- współdzielenie pulpitu roboczego, 25
- współużytkowanie zasobów, 23
- współzależność warstw, 540
- wstępny klucz główny, premaster key, 949
- wtyczka, plug-in, 722
- WWW, World Wide Web, 22, 714
- wybielanie, whitening, 870
- wydajność
 - kanalu, 302, 318
 - protokołów symetrycznych, 305
 - sieci, 639, 657
 - sieci Ethernet, 317, 319
- wydziałanie podsieci, 487
- wykorzystanie kanału, 299
- wykrywanie
 - błędów, 55
 - kolizji, 308
 - MTU ścieżki, 477
- wymaganie niezaprzeczalności, 888
- wymiana kluczy, 926
- wysyłanie ramki, 337
- wysyłka poczty, mail submission, 688, 708
- wyszukiwanie
 - informacji, 36
 - nazwy zdalnej, 683
 - w sieci WWW, 772
- wyszukiwarka, 772
- wytrychy, 919
- wywołania RPC, 598
- wyznaczenie węzła sieci CDN, 829
- wyznacznik początku ramki, 313
- wzmacniak, repeater, 120, 313
- wznowienie transmisji, 66

X

X.509, 900
xDSL, 172
XHTML Basic, 770
XHTML, eXtended HyperText Markup
Language, 755
XML, eXtensible Markup Language, 752, 753
XSLT, eXtensible Stylesheet Language
Transformations, 755

Z

zabezpieczenie sieci
 bezprzewodowej, 345
 wewnętrznej, 912
zagnieżdżenie segmentów, 544
zagubione pakiety, 640
zakleszczenie, deadlock, 621
zalewanie pakietami SYN, 616
zamiana torrenta na klucz, 840
zaporą sieciową, firewall, 910, 912
zapytanie iteracyjne, iterative query, 685
zapytanie rekurencyjne, recursive query, 685
zarządca regionalny RA, 902
zarządzanie
 kluczami publicznymi, 966
 oknem, 620
 żetonem, 66
zasada
 AIMD, 588
 dozwolonego użytku, 964
 optymalności, 402
 sieci końcówek, 395
 sterująca, control law, 587
zasady
 kryptografii, 864
 projektowania sieci, 478
zasięg
 transmisji stacji, 338
 transmitera radiowego, 308

zator, 188
zatruty cache, poisoned cache, 942
zbiór rekordów zasobowych, 944
zbiór RRSet, 946
zdalna diagnostyka, 25
zdalne wywołanie procedury, 596
zdarzenia serwera, 578
zegary taktujące, 152
zestawianie
 łączy, circuit switching, 186
 połączenia 802.11i, 918
 połączenia z siecią, 917
zgłoszenie, ranging, 352
zgodność międzysieciowa, 56
złącza BNC, 312
znacznik, 368, 734
 aktywny RFID, 97
 FIN, 613
 obrazka, 735
 pasywny RFID, 97
 RFID, 97
 stanu minimalnego, 798
 UHF RFID, 364
znaczniki XHTML Basic, 771
znak pionowej kreski, 487
znak wodny, watermarking, 962
znaki ASCII, 735
znakowanie czasowe, timestamping, 600
znormalizowany iloczyn skalarny, 163
zrzut obciążenia, load shedding, 435, 442
zwalnianie połączenia, 564

Ż

żądanie, 25
 HTTP, 746, 761
 potokowe, pipelined requests, 758
żeton, 302

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**

Technika przesyłania danych rozwija się w zawrotnym tempie. Co rusz wprowadzane są nowe standardy, protokoły i narzędzia. Od czasu ukazania się na rynku czwartego wydania tej książki szczególnie mocno rozwinęły się wszystkie obszary związane z sieciami bezprzewodowymi. Mobilny dostęp do internetu jest w dzisiejszych czasach normą, dlatego znajomość nowych trendów oraz biegłość w poruszaniu się w gąszczu specjalistycznej wiedzy są konieczne potrzebne wszystkim projektantom i administratorom.



LOW-EARTH
ORBIT SATELLITE

Piąte wydanie książki **Sieci komputerowe** pozwoli Ci na błyskawiczne opanowanie najbardziej aktualnej wiedzy. Autor położył tu szczególny nacisk na sieci bezprzewodowe — standardy 802.11, 802.16, Bluetooth™ oraz dostęp przez sieć komórkową zostały dogłębnie omówione. Lektura tej pozycji umożliwi Ci również uzyskanie kompletnej wiedzy na temat tradycyjnych sieci kablowych. To medium transmisji jeszcze długo będzie wykorzystywane tam, gdzie jest wymagana najwyższa niezawodność. Ta książka jest idealnym wprowadzeniem do sieci współczesnych — *oraz tych, które dopiero powstaną.*

PRZECZYTAJ I SPRAWDŹ:

- jakie są dostępne media transmisyjne
- co warto wiedzieć o zaletach i wadach protokołów routingu
- w jaki sposób zapewnić wydajność sieci (QoS)
- jak zagwarantować bezpieczeństwo przesyłanych danych

ANDREW STUART TANENBAUM

— profesor informatyki, zdobywca prestiżowego European Research Council Advanced Grant na badania nad niezawodnością w systemach komputerowych. Autor bardzo znanych i cenionych książek informatycznych, które stanowią lekturę obowiązkową w dziedzinie komputerów.

DAVID J. WETHERALL

— profesor informatyki, od ponad dwudziestu lat zajmujący się sieciami komputerowymi. W kręgu jego zainteresowań badawczych znajdują się protokoły internetowe, sieci bezprzewodowe i bezpieczeństwo komunikacji.

OBOWIĄZKOWA LEKTURA KAŻDEGO ADMINISTRATORA I PROJEKTANTA SIECI KOMPUTEROWYCH!

Nr katalogowy: 8527



Księgarnia internetowa
http://helion.pl



Zamówienia telefoniczne:
0 801 339900



0 601 339900



Helion

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

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

helion.pl
księgarnia
internetowa

Cena 129,00 zł

ISBN 978-83-246-3079-0



9 788324 630790

Informatyka w najlepszym wydaniu