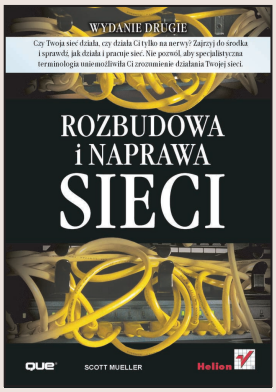
Rozbudowa i naprawa sieci. Wydanie II



Autor: Scott Mueller
Tłumaczenie: Piotr Pilch (rozdz. 1 – 11, 55 – 63),
Mikołaj Szczepaniak (rozdz. 12 – 24, 49),
Paweł Gonera (rozdz. 25 – 30, 48, 50 – 52, dod. A – G),
Adam Jarczyk (rozdz. 31 – 47, 53, 54)
ISBN: 83-7361-376-5
Tytuł oryginału: Upgrading and Repairing Networks, 4th Edition
Format: B5, stron: 1448

Jak działa i pracuje sieć ?
Zajrzyj do środka i sprawdź !

Nawet jeżeli nie jesteś maniakiem komputerowym (oficjalnie nazywanym inżynierem sieciowym), książka „Rozbudowa i naprawa sieci. Wydanie II" omawia skomplikowane zagadnienia w sposób, który nie spowoduje, że sięgniesz po aspirynę lub rewolwer.

W drugim wydaniu tego klasycznego przewodnika po sieciach omówiono skomplikowane topologie sieciowe oraz protokoły, jak również sposoby śledzenia i poprawienia błędów, które narażają Ciebie lub Twoją firmę na znaczne koszty. Dokładne objaśnienia poparte przykładami pozwalają poznać sposoby działania protokołów, architekturę i sprzęt wykorzystywane w sieciach oraz metody ich naprawy, gdy przestają działać.

Poznaj:

- Topologie sieci komputerowych
- Projektowanie sieci
- Fizyczne elementy sieci: okablowanie, karty sieciowe, przełączniki, routery
- Urządzenia NAS i sieci SAN
- Przyjęte przez IEEE standardy sieci LAN i MAN
- Protokoły ARCNet, Ethernet
- Protokoły używane w sieciach WAN
- Technologie DSL i sieci kablowe
- Sieci bezprzewodowe
- Omówienie protokołów TCP/IP
- Podstawowe usługi i aplikacje TCP/IP
- Protokoły związane z pocztą elektroniczną
- Protokoły BOOTP i DHCP
- System DNS i WINS, ActiveDirectory
- Systemy z rodziny Novell NetWare
- Sieć WWW i protokół HTTP, SSL
- Omówienie standardu IPv6
- Zarządzanie użytkownikami i ich uprawnieniami
- Zabezpieczanie sieci i szyfrowanie
- Praktyczne metody modernizacji sieci
- Migracja do nowszych systemów operacyjnych

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

O Autorach **27**

Wprowadzenie **29**
Dla kogo jest ta książka? 30
Co zawiera książka? 30
Nowości w aktualnej edycji książki 34

Część I Początek: planowanie i projektowanie sieci **35**

Rozdział 1. Historia sieci komputerowych w pigułce **37**

Rozdział 2. Przegląd topologii sieciowych **41**
Topologie stosowane w sieciach lokalnych 41
Topologia magistrali 42
Topologia gwiazdy 43
Topologia pierścienia 45
Topologia siatki 47
Topologia hybrydowa 48
Topologie sieciowe oparte na współdzielonym i nieudostępnionym nośniku danych 51
Porównanie topologii opartych na mostach i routerach 52
Tworzenie sieci wielosegmentowej i stosowane topologie 54
Łączenie segmentów sieci w obrębie budynku — sieć szkieletowa 54
Aspekty projektowania sieci wielosegmentowej 56
Skalowalność 56
Nadmiarowość 57
Odporność na awarie 57
Topologia sieci wielowarstwowej 58
Skalowalność 59
Nadmiarowość 59
Odporność na awarie 59

Rozdział 3. Strategie projektowania sieci **61**
Planowanie struktury logicznej sieci 62
Kim są Twoi klienci? 64
Jakie typu usługi lub aplikacje powinny być udostępnione w sieci? 64
Jaki stopień niezawodności jest wymagany dla każdego połączenia sieciowego? 65
Dobór protokołu sieci lokalnej 66
Instrumenty planowania i projektowania 70
Pełna dokumentacja 71
Nigdy dosyć testowania 72
Tworzenie zasad i procedur używania sieci 72
Szkolenie personelu technicznego 74
Nie zapominaj o budżecie (chyba że możesz sobie na to pozwolić) 74
Struktura fizyczna sieci 75
Planowanie zasobów 75

Rozdział 4. Zarządzanie projektem i strategie modernizacji sieci 77
Od czego zacząć? 77
Analiza — stwierdzenie konieczności przeprowadzenia modernizacji 80
Określanie wymagań i oczekiwań użytkowników 83
Obsługa starszych aplikacji 84
Zasoby wymagane do przeprowadzenia modernizacji 85
Planowanie modernizacji 86
Dokumentowanie planu 87
Określenie stopnia zgodności planu z firmowymi zasadami i procedurami 87
Określanie celów 88
Planowanie czasu przestoju sieci 88
„Kamienie milowe" i kryteria 89
Procedury wycofywania 89
Testowanie planu 90
Sprawdzanie konkurencyjnych produktów 90
Projekt pilotażowy 91
Wdrażanie 91
Członkowie zespołu 91
Informowanie użytkowników 92
Śledzenie postępu prac 92
Szkolenie użytkowników 93
Na zakończenie: spisz, co zostało wykonane i dlaczego 93
Inne zagadnienia dotyczące modernizacji 94

Rozdział 5. Ochrona sieci: metody zapobiegania zagrożeniom 95
Stabilizacja napięcia i zasilacze awaryjne UPS (Uninterruptible Power Supplies) 95
Energia to pieniądze 96
Interfejs ACPI (Advanced Configuration and Power Interface) i niezależne systemy zasilaczy awaryjnych UPS 98
Urządzenia sieciowe 100
Monitorowanie sieci 100
Kopie zapasowe stacji roboczych i serwerów 101
Nośniki archiwizujące — taśmy, dyski optyczne i CD-R 103
Harmonogram wykonywania kopii zapasowych 105
Przechowywanie kopii zapasowej w innej fizycznej lokalizacji 106
Regularna konserwacja 108
Tworzenie nadmiarowości w sieci 109
Planowanie przywracania pracy sieci 109
Szacowanie kosztu metod ochrony 110

Część II Fizyczne komponenty sieci 111

Rozdział 6. Okablowanie sieciowe: kable, złącza, koncentratory i inne komponenty sieciowe 113
Okablowanie strukturalne 113
Obszar roboczy 114
Struktura okablowania szkieletowego 115
Struktura okablowania poziomego 116
Szafa telekomunikacyjna 117
Ważne definicje 117
Typy kabli 122
Skrętka 122
Kable koncentryczne 126
Światłowody 130
Terminatory i połączenia 135
Zaciskanie 136
Styk uzyskany poprzez zdjęcie izolacji 136

Modularne gniazda i wtyczki ... 136
Konfiguracje par wtyczek modularnych ... 137
Typy powszechnie stosowanych gniazdek ... 137
Krosownice ... 139
Końcówki światłowodów ... 140
Łączenie światłowodów ... 142
Krosownice światłowodowe ... 143
Ogólne zalecenia dotyczące światłowodów ... 143
Złącza SFF (Small Form Factor) ... 144
Pomieszczenia telekomunikacyjne ... 144
Okablowanie „przenośnych" biur ... 144
Punkty konsolidacyjne ... 145
Ogólne specyfikacje podsystemu okablowania poziomego ... 145
Dokumentowanie i zarządzanie instalacją ... 145
Rekordy ... 146
Rysunki ... 146
Zlecenia ... 146
Raporty ... 147

Rozdział 7. Karty sieciowe ... 149

Wybór typu magistrali sprzętowej ... 149
ISA ... 151
PCI ... 152
PCMCIA ... 153
CardBus ... 154
Różne karty, inne szybkości ... 155
Terminatory i złącza kabli sieciowych ... 156
Założenia WfM (Wired for Management) i technologia WOL (Wake on LAN) ... 156
Universal Network Boot ... 157
Asset Management ... 157
Power Management ... 158
Remote Wake-Up ... 158
Czy warto stosować karty sieciowe zgodne z technologią WOL? ... 160
Systemy z wieloma kartami ... 161
Równoważenie obciążenia i nadmiarowe kontrolery sieci ... 161
Sterowniki programowe ... 162
Packet Driver ... 163
ODI (Open Data-Link Interface) ... 163
NDIS (Network Driver Interface Specification) ... 164
Sygnały IRQ i porty wejścia-wyjścia ... 165
Sygnały IRQ ... 165
Podstawowe porty I/O (wejścia-wyjścia) ... 167
Rozwiązywanie problemów z kartami sieciowymi ... 168
Sprawdzanie konfiguracji karty sieciowej w systemie Linux ... 169
Monitorowanie diod karty sieciowej — diody aktywności i diody połączenia ... 171
Zastosowanie programu diagnostycznego karty ... 172
Konflikty konfiguracji ... 173
Sprawdzanie konfiguracji sieciowej komputera ... 174
Konieczne kroki zapobiegawcze ... 175

Rozdział 8. Przełączniki sieciowe ... 177

Zasada działania przełączników ... 178
Dzielenie domeny kolizyjnej ... 180
Przełączniki sieci Ethernet działające w trybie pełnego dupleksu ... 181
Tworzenie sieci szkieletowych przy użyciu przełączników ... 183
Rodzaje przełączników ... 185
Przełączniki bezzwłoczne ... 186
Przełączniki buforujące ... 186

Przełączniki warstwy trzeciej 186
Zastosowanie przełącznika w niewielkim biurze 188
Przełączniki piętrowe i modularne 188
Diagnostyka i zarządzanie przełącznikami 189

Rozdział 9. Sieci wirtualne VLAN 191
Sieci wirtualne VLAN i topologie sieci 191
Przełączanie oparte na ramkach sieciowych 193
Sieci wirtualne oparte na portach 194
Znakowanie niejawne i jawne 195
Znakowanie niejawne 195
Znakowanie jawne 196
Sieci wirtualne VLAN oparte na adresach MAC 197
Sieci wirtualne VLAN oparte na typie protokołu 197
Zastosowanie znakowania jawnego w sieciach szkieletowych 198
Standardy przełączania organizacji IEEE 200
Jakiego typu przełącznik zastosować? 202

Rozdział 10. Routery 205
Do czego służą routery? 205
Hierarchiczna organizacja sieci 206
Zastosowanie zabezpieczeń 207
Różnica pomiędzy protokołami routowalnymi i protokołami trasowania 208
Kiedy jest konieczne zastosowanie routera? 209
Zwiększanie rozmiarów sieci lokalnych 210
Delegowanie uprawnień administracyjnych dla sieci lokalnych 214
Łączenie oddziałów firmy 215
Zastosowanie routera do ochrony sieci — translacja adresów i filtrowanie pakietów 216
Porty routerów i połączenia z nimi 216
Konfigurowanie routerów 218
Różnorodność routerów 219
Zastosowanie routerów w sieciach rozległych WAN 221
Routery jako urządzenia łączące z internetem 222

Rozdział 11. Urządzenia NAS i sieci SAN 225
Porównanie lokalnych i sieciowych urządzeń masowych 226
Zastosowanie technologii NAS (Network Attached Storage) 227
Zastosowanie sieci SAN (Storage Area Network) 228
Urządzenia NAS 229
Gotowe urządzenia sieciowe 230
Protokoły technologii NAS 230
Ograniczenia pojemnościowe technologii NAS — przepustowość i przestrzeń dyskowa 231
Sieci SAN 232
Technologie SAN i NAS — ich połączenie i podobieństwa 233
Zastosowanie protokołu Fibre Channel w roli protokołu transportowego 234
Rodzaje kodowania danych w sieciach opartych na protokole Fibre Channel 234
Podstawowe sieci SAN: pętla z arbitrażem 237
Inicjalizacja pętli 238
Arbitraż dostępu do pętli 241
Zastosowanie w sieciach SAN przełączników strukturalnych (ang. *Fabric Switches*) 241
Połączona topologia pętli i przełączników 244
Sieci IP SAN i ich przyszłość 246
Jakiego typu urządzenia NAS i sieci SAN powinno się stosować? 247

Część III Protokoły sieciowe niskiego poziomu 251

Rozdział 12. Przyjęte przez IEEE standardy sieci LAN i MAN 253

Czym jest komitet standardów sieci LAN i MAN? 254
Standardy IEEE 802: ogólne pojęcia i architektura 255
IEEE 802.1: mostkowanie i zarządzanie 257
IEEE 802.2: sterowanie łączem logicznym 258
IEEE 802.3: metoda dostępu CSMA/CD 258
IEEE 802.4: metoda dostępu Token-Bus oraz IEEE 802.5: metoda dostępu Token-Ring 259
IEEE 802.7: zalecane praktyki w szerokopasmowych sieciach lokalnych 260
IEEE 802.10: bezpieczeństwo 260
IEEE 802.11: sieci bezprzewodowe 260
Pozyskiwanie dokumentacji standardów IEEE 802 za darmo 261

Rozdział 13. Starszy, ale nadal używany protokół sieci lokalnej: ARCnet 263

Przegląd technologii ARCnet 264
Przydzielanie adresów i przesyłanie komunikatów w sieci ARCnet 265
Koncentratory i okablowanie sieciowe 271
Topologie magistrali i gwiazdy 272
Karty sieciowe ARCnet 274
Łączenie sieci lokalnych ARCnet z sieciami lokalnymi Ethernet 275
Rozwiązywanie problemów w sieciach ARCnet 275

Rozdział 14. Ethernet, uniwersalny standard 277

Krótka historia Ethernetu 277
Ile różnych rodzajów Ethernetu istnieje? 278
Kolizje: czym są CSMA/CA i CSMA/CD? 282
Algorytm oczekiwania 285
Definiowanie domen kolizyjnych — magistrale, koncentratory i przełączniki 285
Ograniczenia tradycyjnych topologii sieci Ethernet 286
Czynniki ograniczające możliwości technologii ethernetowych 287
Urządzenia połączeń międzysieciowych i długości segmentów przewodów 287
Reguła 5-4-3 288
Stosowanie topologii magistrali 288
Stosowanie topologii gwiazdy 289
Hybrydowe topologie sieci LAN 291
Drzewo 291
Gwiazda hierarchiczna 292
Stosowanie sieci szkieletowych na poziomie korporacji 293
Ramki sieci Ethernet 293
XEROX PARC Ethernet i Ethernet II 294
Standard 802.3 295
Standard sterowania łączem logicznym (LLC), 802.2 296
Standardy Fast Ethernet (IEEE 802.3u) i Gigabit Ethernet (IEEE 802.3z) 299
Fast Ethernet 299
Gigabit Ethernet 301
Standard 10Gigabit Ethernet (IEEE 802.3ae) 303
Problemy w sieciach Ethernet 304
Wskaźniki liczby kolizji 304
Typy kolizji 305
Odstępy próbkowania 307
Ograniczanie liczby kolizji 307
Błędy w sieci Ethernet 308
Wykrywanie prostych błędów 309
Zła wartość FCS lub niedopasowana ramka 309
Krótkie ramki 310

Olbrzymie i niezrozumiałe ramki 311
Błędy wielokrotne....312
Fala rozgłaszań 312
Monitorowanie wystąpień błędów 313

Część IV Połączenia wydzielone i protokoły sieci WAN 315

Rozdział 15. Połączenia telefoniczne....317
Protokół punkt-punkt (PPP) oraz protokół IP dla łączy szeregowych (SLIP)....318
Protokół IP dla łączy szeregowych (SLIP) 319
Protokół punkt-punkt (PPP)....322
Ustanawianie połączenia: protokół sterowania łączem (LCP) 324
Protokoły kontroli sieci (NCP) 327
Przykład: konfigurowanie klienta Windows XP Professional....328
Kiedy połączenie telefoniczne jest zbyt wolne 330

Rozdział 16. Połączenia wydzielone 331
Linie dzierżawione....332
System T-carrier 334
Częściowe T1....335
Diagnozowanie problemów w usługach T-carrier....335
Sieci ATM....337
Ramki ATM....338
Połączenia ATM 340
Model architektury ATM (model B-ISDN/ATM)....341
Emulacja sieci LAN (LANE) 343
Kategorie usług ATM 345
Znaczenie interfejsów Frame Relay i X.25....346
Nagłówek w sieci Frame Relay 348
Sygnalizacja przeciążenia sieci....350
Mechanizm sygnalizacji lokalnego interfejsu zarządzającego (LMI) 351
Stosowanie wirtualnych obwodów komutowanych (SVC)....351
Możliwe problemy w sieciach Frame Relay....352

Rozdział 17. Technologie cyfrowych linii abonenckich (DSL)....355
Modemy DSL i modemy kablowe....356
Różnice topologiczne pomiędzy technologiami sieci kablowych i DSL....357
Krótkie wprowadzenie do publicznych komutowanych sieci telefonicznych....360
xDSL....361
Przyszłość technologii DSL....368

Rozdział 18. Stosowanie modemów kablowych 369
Działanie modemów kablowych....370
Przekazywanie adresów IP dla modemów kablowych....371
Systemy modemów kablowych pierwszej generacji 373
Różnice w działaniu modemów kablowych i szerokopasmowych modemów dostępowych xDSL....373
Specyfikacja DOCSIS (Data Over Cable Service and Interface Specification)....375
Co powinieneś wybrać — modem kablowy czy modem DSL? 376

Część V Protokoły sieci bezprzewodowych....377

Rozdział 19. Wprowadzenie do sieci bezprzewodowych....379
Dlaczego rozwój sieci bezprzewodowej jest nieuchronny?....381
Punkty dostępowe i sieci ad hoc 383
Sieci ad hoc....383
Stosowanie punktów dostępowych jako elementów pośredniczących w komunikacji bezprzewodowej....385

Technologie fizycznego przesyłania danych 387
Kluczowanie częstotliwości kontra widmo rozproszone 387
Standard sieci bezprzewodowych IEEE 802.11 389
Warstwa fizyczna 390
Warstwa MAC 390
Inne usługi realizowane w warstwie fizycznej 392
Źródła zakłóceń w sieciach bezprzewodowych 392

Rozdział 20. Dostępny i niedrogi standard: IEEE 802.11b 395
Dlaczego technologia Wi-Fi? 395
Na co należy zwracać uwagę, korzystając z sieci 802.11b 396
Ograniczenia zasięgu 398
Firewalle 398
Czy potrzebujesz sieci bezprzewodowej? 399
Łączenie sieci bezprzewodowej z przewodową siecią LAN 399
Punkty dostępowe pracujące w trybie dualnym 400

Rozdział 21. Szybsza usługa: standard IEEE 802.11a 401
Przegląd standardu IEEE 802.11a 402
Zakłócenia powodowane przez inne urządzenia 402
Zwiększona przepustowość w paśmie 5,4 GHz 403
Stosowanie sieci bezprzewodowych w miejscach publicznych 404
Problem bezpieczeństwa 405

Rozdział 22. Standard IEEE 802.11g 407
Przegląd standardu 802.11g 408
Zwiększanie przepustowości w paśmie 2,4 GHz 409
Instalacja routera Linksys Wireless-G Broadband Router (model nr WRT54G) 410
Instalacja i konfiguracja karty sieci bezprzewodowej 420
Który protokół bezprzewodowy jest przeznaczony dla Ciebie? 423

Rozdział 23. Bezprzewodowa technologia Bluetooth 425
Grupa Bluetooth SIG (Special Interest Group) 427
Ogólny przegląd technologii Bluetooth 428
Sieci piconet i scatternet 430
Sieci piconet 430
Sieci scatternet 431
Tryby pracy urządzeń Bluetooth 433
Łącza SCO i ACL 434
Łącza SCO 434
Łącza ACL 434
Pakiety Bluetooth 435
Czym są profile Bluetooth? 437
Profil podstawowy GAP 437
Profil Service Discovery Application 439
Profile telefonów bezprzewodowych oraz komunikacji wewnętrznej 440
Profil portu szeregowego 440
Profil słuchawki 441
Profil połączeń telefonicznych 441
Inne profile Bluetooth 441
Bluetooth to więcej niż protokół komunikacji bezprzewodowej 443

Rozdział 24. Inne technologie bezprzewodowe 445
Urządzenia przenośne 445
Palmtopy 445
Telefony komórkowe trzeciej generacji 446

Bezpieczeństwo komunikacji bezprzewodowej....447
WEP....448
WEP drugiej generacji: klucz 128-bitowy....449
Mechanizm Wired Protected Access (WPA) i standard 802.11i....450
Jak dobrze znasz użytkowników swojej sieci?....451
Sieci osobiste (PAN)....452

Część VI Sieci LAN i WAN, usługi, protokoły i aplikacje....455

Rozdział 25. Przegląd zestawu protokołów TCP/IP....457
TCP/IP i referencyjny model OSI....458
TCP/IP: zbiór protokołów, usług i aplikacji....459
TCP/IP, IP i UDP....460
Inne protokoły pomocnicze....461
Internet Protocol (IP)....462
IP jest bezpołączeniowym protokołem transportowym....463
IP jest protokołem bez potwierdzeń....463
IP nie zapewnia niezawodności....464
IP zapewnia przestrzeń adresową dla sieci....464
Jakie funkcje realizuje IP?....464
Nagłówek datagramu IP....465
Adresowanie IP....468
Address Resolution Protocol — zamiana adresów IP na adresy sprzętowe....480
Proxy ARP....485
Reverse Address Resolution Protocol (RARP)....486
Transmission Control Protocol (TCP)....486
TCP tworzy niezawodne sesje połączeniowe....486
Zawartość nagłówka TCP....487
Sesje TCP....489
Problemy z bezpieczeństwem sesji TCP....496
User Datagram Protocol (UDP)....497
Dane nagłówka UDP....497
Współpraca pomiędzy UDP i ICMP....498
Porty, usługi i aplikacje....499
Porty zarezerwowane....500
Porty zarejestrowane....500
Internet Control Message Protocol (ICMP)....500
Typy komunikatów ICMP....501

Rozdział 26. Podstawowe usługi i aplikacje TCP/IP....505
File Transfer Protocol (FTP)....506
Porty i procesy FTP....507
Przesyłanie danych....508
Polecenia protokołu FTP....509
Odpowiedzi serwera na polecenia FTP....511
Użycie klienta FTP z wierszem poleceń w Windows....512
Użycie FTP w Red Hat Linux....518
Zastosowanie klienta FTP z wierszem poleceń w Red Hat Linux....519
Trivial File Transfer Protocol (TFTP)....521
Protokół Telnet....523
Czym jest wirtualny terminal sieciowy i NVT ASCII?....524
Polecenia protokołu Telnet i negocjacja opcji....525
Telnet a autoryzacja....527
Korzystanie z protokołów Telnet i FTP za firewallem....527
R-utilities....530
Sposób autoryzacji tradycyjnych R-utilities przy dostępie do zasobów sieciowych....530
Narzędzie rlogin....531

Użycie rsh 534
Użycie rcp 535
Użycie rwho 536
Użycie ruptime 537
Program finger 537
Inne usługi i aplikacje korzystające z TCP/IP 540
Bezpieczne usługi sieciowe 540

Rozdział 27. Protokoły poczty internetowej: POP3, SMTP oraz IMAP 541

Jak działa SMTP 542
Model SMTP 543
Rozszerzenia usługi SMTP 544
Polecenia SMTP i kody odpowiedzi 545
Kody odpowiedzi SMTP 547
Łączymy wszystko razem 549
Post Office Protocol (POP3) 549
Stan AUTORYZACJA 550
Stan TRANSAKCJA 551
Stan AKTUALIZACJA 551
Internet Message Access Protocol w wersji 4 (IMAP4) 552
Protokoły transportowe 553
Polecenia klienta 553
Znaczniki systemowe 553
Pobieranie nagłówka i treści przesyłki 554
Formatowanie danych 554
Nazwa skrzynki odbiorczej użytkownika i innych skrzynek 554
Polecenia uniwersalne 555
Pozostałe polecenia IMAP 555

Rozdział 28. Narzędzia diagnostyczne dla sieci TCP/IP 557

Sprawdzanie konfiguracji systemu komputera 557
Użycie polecenia hostname i poleceń pokrewnych 558
Kontrola konfiguracji za pomocą poleceń ipconfig i ifconfig 559
Użycie narzędzi ping i traceroute do sprawdzenia połączenia 563
Polecenie ping 563
Polecenie traceroute 568
Polecenia netstat i route 572
Polecenie arp 577
Polecenie tcpdump 578
Program WinDump 580
Użycie polecenia nslookup do wyszukiwania problemów z tłumaczeniem nazw 582
Inne użyteczne polecenia 583

Rozdział 29. Protokoły BOOTP i Dynamic Host Configuration Protocol (DHCP) 585

Czym jest BOOTP? 585
Format pakietu BOOTP 586
Mechanizm żądań i odpowiedzi BOOTP 589
Informacje BOOTP specyficzne dla producenta 590
Pobieranie systemu operacyjnego 593
Krok dalej niż BOOTP — DHCP 593
Format pakietu DHCP oraz opcje dodatkowe 596
Wymiana komunikatów między klientem i serwerem DHCP 598
Przykład: instalacja i konfiguracja serwera DHCP w Windows 2000/2003 603
Instalacja usługi serwera DHCP w Windows 2000 lub Server 2003 603
Autoryzacja serwera 604
Użycie menu Akcja w MMC 605

Konfiguracja serwera DHCP i opcji zakresu ... 612
Obsługa klientów BOOTP ... 615
Uaktywnianie agenta pośredniczącego DHCP ... 615
Czym jest klaster DHCP ... 618
Rozważania na temat DHCP w dużych sieciach lub w sieciach korzystających z routingu ... 619
Jak DHCP współpracuje z Microsoft Dynamic Domain Name Service (DNS) ... 619
Rezerwacje i wykluczenia ... 622
Co to jest APIPA? ... 623
Rozwiązywanie problemów z Microsoft DHCP ... 623
Zarządzanie rejestrowaniem ... 624
Użycie DHCP w Red Hat Linux ... 625
Demon serwera DHCP ... 626
Agent przekazujący DHCP ... 627

Rozdział 30. Wyszukiwanie nazw sieciowych ... 629

Sprzęt a adresy protokołu ... 630
NetBIOS ... 631
Plik lmhosts ... 631
Windows Internet Name Service ... 635
Instalacja i konfiguracja WINS w Windows 2000 i 2003 Server ... 641
Zarządzanie serwerem WINS w Windows 2000 ... 642
Zarządzanie usługą WINS w Windows Server 2003 ... 647
Korzystanie z polecenia netsh do zarządzania serwerem WINS ... 647
Nazwy IP ... 649
Plik hosts ... 651
Domain Name System ... 652
Konfigurowanie klienta DNS ... 659
Wykorzystanie nslookup ... 660
Dynamiczny DNS ... 660
Instalowanie DNS w Windows 2000 lub 2003 Server ... 662
Network Information Service ... 663

Rozdział 31. Praca z Active Directory ... 665

Początki usług katalogowych ... 666
Różnice pomiędzy katalogiem i usługą katalogową ... 666
Interesujące obiekty ... 667
Co umożliwia usługa Active Directory? ... 668
Od X.500 i DAP do protokołu Lightweight Directory Access Protocol ... 669
Schemat Active Directory ... 672
Obiekty i atrybuty ... 673
Standardowe obiekty Active Directory ... 674
Czym jest drzewo domen, a czym las? ... 676
Modele domen — niech spoczywają w pokoju ... 676
Podział Active Directory na domeny ... 677
Domena wciąż jest domeną ... 678
Drzewa i lasy Active Directory ... 678
Active Directory i dynamiczny DNS ... 679
Dynamiczny DNS ... 679
Jak Active Directory korzysta z DNS? ... 680
Zarządzanie dużymi sieciami przedsiębiorstw za pomocą lokacji ... 681
Replikacja katalogu ... 682
Podsumowanie danych katalogowych w wykazie globalnym ... 683
Active Directory Service Interfaces (ADSI) ... 684
Programowanie aplikacji współpracujących z katalogiem ... 684
Zostały tylko kontrolery domen i serwery członkowskie ... 685
Schemat Active Directory ... 686
Modyfikacje schematu Active Directory ... 686

Znajdowanie obiektów w Active Directory 695
Znajdowanie konta użytkownika 696
Wyszukiwanie drukarki w Active Directory 698
Funkcja Wyszukaj w menu Start 699
Windows Server 2003: nowe funkcje Active Directory 700
Instalacja Active Directory na komputerze z systemem Windows Server 2003 701

Rozdział 32. Przegląd protokołów IPX/SPX w systemie Novell NetWare 709
Praca z protokołami firmy Novell 710
Pakiet protokołów NetWare 711
Usługi i protokoły bezpołączeniowe 712
Usługi i protokoły połączeniowe 713
Protokół IPX 713
Przesyłanie pakietów w IPX 715
Struktura pakietu IPX 716
Typy ramek IPX 716
Protokół SPX 717
Przesyłanie pakietów w SPX 718
Struktura pakietu SPX 719
Protokół SPXII 719
Protokół NCP 720
Opcje podpisywania pakietów NCP 721
Poziomy podpisywania dla serwera 722
Poziomy podpisywania dla klienta 722
Podpisywanie pakietów i serwery zadań 723
Wypadkowe poziomy podpisywania pakietów 724
Rozwiązywanie problemów z konfliktami w podpisach pakietów 724
Wytyczne bezpieczeństwa dla NetWare 725
Niezależność NCP od protokołu 725

Rozdział 33. Przegląd Novell Bindery i Novell Directory Services 727
Wprowadzenie do struktur katalogowych NetWare 727
Struktura bindery 727
Struktura usługi NDS 728
Usługi bindery 733
Zestawienie usług bindery i NDS 735
Praca z usługą Novell Directory Services 739
Praca z NWADMN32 739
Tworzenie i usuwanie obiektów 740
Przenoszenie i zmiany nazw obiektów 743
Przydzielanie praw i ustawianie uprawnień 743
Zastosowanie narzędzia NDS Manager 750
Konfiguracja usług bindery 754

Rozdział 34. Rozbudowa i rozszerzenie NDS: eDirectory w systemie NetWare 755
Podstawy eDirectory 755
eDirectory można instalować w wielu różnych systemach operacyjnych 756
Opcje, które należy rozważyć przy instalowaniu eDirectory 756
Wymogi sprzętowe 757
Instalowanie eDirectory na obsługiwanych platformach 759
Nowe możliwości eDirectory 759
TLS i SSL 759
iMonitor 760
Protokół SNMP 761
Dopasowania wieloznaczne 761
Kopie zapasowe 761

Rozdział 35. Protokoły serwera plików 765
Co umożliwi Ci lektura tego rozdziału? 765
Server Message Block (SMB) i Common Internet File System (CIFS) 767
Typy komunikatów SMB 767
Mechanizmy zabezpieczeń w SMB 768
Negocjacja protokołu i nawiązanie sesji 770
Dostęp do plików 771
Polecenia NET 774
Monitorowanie i rozwiązywanie problemów z SMB 777
Protokół SMB/CIFS w klientach innych niż produkowanych przez Microsoft: Samba 780
Protokół CIFS 781
NetWare Core Protocol (NCP) 782
Ogólne żądania i odpowiedzi 783
Tryb strumieniowy 783
Trwa przetwarzanie żądania 784
Zakończenie połączenia 784
Network File System (NFS) w systemach Unix 784
Komponenty protokołu: protokół RPC 785
External Data Representation (XDR) 786
Protokoły NFS i Mount 787
Konfiguracja serwerów i klientów NFS 789
Demony klientów NFS 789
Demony serwerowe 792
Rozwiązywanie problemów z NFS 798
Rozproszony system plików DFS Microsoftu: Windows 2000 i Windows Server 2003 800
Tworzenie katalogu głównego DFS 801
Dodawanie łączy do katalogu głównego DFS 802

Rozdział 36. Protokół HTTP 805
Wszystko zaczęło się od World Wide Web Consortium (W3C) w CERN 806
Co to jest HTTP? 807
Mechanika HTTP 807
Pola nagłówka HTTP 808
URL, URI i URN 808

Rozdział 37. Protokoły routingu 813
Podstawowe typy protokołów routingu 813
Protokół RIP 814
Protokół OSPF (Open Shortest Path First) 820
Multi-Protocol Label Switching 821
Połączenie routingu i przełączania 822
Etykietowanie 822
Współpraca Frame Relay i ATM z MPLS 823

Rozdział 38. Protokół SSL 825
Szyfrowanie symetryczne i asymetryczne 826
Certyfikaty cyfrowe 827
Procedura wymiany potwierdzeń SSL 827
Ochrona przed przechwyceniem dzięki certyfikatom 828
Co oznaczają prefiksy http:// i https://? 829
Dodatkowa warstwa w stosie protokołów sieciowych 829
Czy SSL zapewnia wystarczające bezpieczeństwo transakcji internetowych? 830
Otwarte wersje SSL 830

Rozdział 39. Wprowadzenie do protokołu IPv6 831
Czym różnią się protokoły IPv4 i IPv6? 832
Nagłówki IPv6 833
Nagłówki dodatkowe IPv6 834
Pole „Typ opcji" dla nagłówków „Skok po skoku" i „Opcje odbiorcy" 836
Inne zagadnienia związane z IPv6 837
Przyszłość IPv6 837

Część VII Zarządzanie zasobami sieciowymi i użytkownikami 839

Rozdział 40. Domeny Windows NT 841
Grupy robocze i domeny 842
Międzydomenowe relacje zaufania 844
Kontrolery domen 847
Modele domen Windows NT 848
Grupy użytkowników Windows NT 851
Wbudowane grupy użytkowników 851
Tworzenie grup użytkowników 852
Specjalne grupy użytkowników 854
Zarządzanie kontami użytkowników 854
Dodawanie użytkownika do grupy 855
Profile użytkowników 856
Ograniczenie godzin logowania użytkownika 856
Ograniczanie stacji roboczych, do których użytkownik może się logować 857
Dane konta 858
Dopuszczenie dostępu przez łącza telefoniczne 858
Replikacja pomiędzy kontrolerami domen 859
Hasła i zasady 861
Wykrywanie nieudanych prób zalogowania 862
Strategie minimalizacji problemów z logowaniem 863

Rozdział 41. Narzędzia do zarządzania użytkownikami i komputerami w systemach Windows 2000 i Windows Server 2003 865
Microsoft Management Console 865
Zarządzanie użytkownikami 866
Tworzenie nowych kont użytkowników w Active Directory 866
Zarządzanie innymi informacjami w kontach użytkowników 869
Menu Action 872
Zarządzanie komputerami 873
Dodawanie komputera do domeny 874
Zarządzanie innymi danymi kont komputerów 875
Grupy użytkowników Windows 2000 877
Wybór grupy na podstawie zasięgu grupy 877
Grupy wbudowane 879
Tworzenie nowej grupy użytkowników 882
Co jeszcze można zrobić z przystawką Użytkownicy i komputery usługi Active Directory? 883

Rozdział 42. Zarządzanie użytkownikami systemów Unix i Linux 885
Zarządzanie użytkownikami 885
Plik /etc/passwd 886
Chroniony plik haseł 888
Plik /etc/groups 889
Dodawanie i usuwanie kont użytkowników 889
Zarządzanie użytkownikami w systemie Linux z GUI 892

Network Information Service (NIS) 897
Główne i podrzędne serwery NIS 897
Mapy NIS 897
Demon ypserve serwera NIS i lokalizacja map 899
Ustawienie nazwy domeny NIS za pomocą polecenia domainname 899
Uruchomienie NIS: ypinit, ypserve i ypxfrd 900
Serwery podrzędne NIS 901
Zmiany w mapach NIS 902
Wysyłanie modyfikacji do serwerów podrzędnych NIS 902
Inne przydatne polecenia YP usługi NIS 902
Klienty NIS 903
Najczęściej spotykane problemy z logowaniem 903

Rozdział 43. Prawa i uprawnienia 905

Zabezpieczenia na poziomie użytkownika i udziału 906
Zabezpieczenia na poziomie udziału w systemach Microsoft Windows 907
Przyznawanie praw użytkownika w Windows 2000, Server 2003 i XP 909
Zarządzanie zasadami haseł użytkowników 916
Standardowe i specjalne uprawnienia NTFS w Windows NT, 2000 i 2003 918
Uprawnienia w systemie Windows są kumulatywne 922
Grupy użytkowników ułatwiają zarządzanie prawami użytkowników 922
Grupy użytkowników w Windows 2000 i 2003 923
Grupy w Active Directory 924
NetWare 926
Dysponenci 927
Prawa w systemie plików 927
Prawa do obiektów i właściwości 928
Różnice pomiędzy prawami w NDS i prawami do systemu plików i katalogów 928
Dziedziczenie praw 929
Grupy Everyone i [Public] 931
Unix i Linux 932
Przeglądanie uprawnień do plików 933
Uprawnienia do plików SUID i SGID 934
Polecenie su 936

Rozdział 44. Sieciowe protokoły drukowania 937

Protokoły drukowania i języki drukowania 938
Korzystanie z lpr, lpd i protokołów strumieniowych TCP 939
Data Link Control Protocol (DLC) 939
Internet Printing Protocol (IPP) 940
Typy obiektów IPP 941
Operacje IPP 942
Co nas czeka w wersji 1.1? 943
Gdzie można znaleźć IPP? 944

Rozdział 45. Serwery druku 945

Drukowanie w systemach Unix i Linux 945
System kolejkowania BSD 946
System drukowania SVR4 956
Konfiguracja serwerów druku Windows 962
Drukarki i urządzenia drukujące 962
Instalowanie i konfiguracja drukarek w serwerach Windows 964
Windows NT 4.0 964
Dodawanie drukarki w systemie Windows 2000 Server 972
Instalacja i konfiguracja drukowania w komputerze z systemem Windows XP 986
Drukowanie w NetWare 990
Właściwości obiektu Print Queue 992
Właściwości obiektu Printer 993

Właściwości obiektu Print Server ... 994
PSERVER.NLM i NPRINTER.NLM ... 995
Narzędzie NetWare 6.x iPrint ... 995
Sprzętowe serwery drukarek ... 996

Część VIII Zabezpieczenia systemów i sieci ... 999

Rozdział 46. Podstawowe środki bezpieczeństwa, które każdy administrator sieci znać powinien ... 1001
Zasady i procedury ... 1001
Zasady podłączania do sieci ... 1002
Dopuszczalne zastosowania i wytyczne użytkowania ... 1003
Procedury reagowania ... 1006
Co powinno zostać uwzględnione w zasadach bezpieczeństwa ... 1007
Zabezpieczenia fizyczne ... 1009
Zamykanie drzwi ... 1009
Zasilacze awaryjne (UPS) ... 1010
Bezpieczna likwidacja sprzętu i nośników ... 1010
Bezpieczeństwo z dwóch stron ... 1011
Przed faktem: kontrola dostępu ... 1011
Po fakcie: kontrole użytkowania ... 1013
Hasła ... 1014
Demony i usługi systemowe ... 1017
Usuwanie zbędnego balastu ... 1018
Delegowanie uprawnień ... 1019
Konta użytkowników ... 1019
Serwery aplikacji, serwery druku i serwery WWW ... 1019
Nie zapominaj o firewallach ... 1020

Rozdział 47. Inspekcje i inne środki monitorowania ... 1021
Systemy Unix i Linux ... 1022
Praca z narzędziem syslog ... 1023
Pliki dziennika systemowego ... 1026
Konfiguracja zasad inspekcji w Windows NT 4.0 ... 1027
Wybór zdarzeń do kontroli ... 1027
Windows NT 4.0 Event Viewer ... 1030
Konfiguracja zasad inspekcji w Windows 2000 i Windows 2003 ... 1031
Włączenie inspekcji dla plików i folderów ... 1033
Inspekcje drukarek ... 1036
Rejestrowanie zdarzeń zamknięcia i uruchomienia systemu Windows Server 2003 ... 1037
Podgląd zdarzeń w systemach Windows 2000 i 2003 ... 1037
Inspekcje komputerów Windows XP Professional ... 1040
Zabezpieczenia w systemach Novella ... 1042
SYSCON i AUDITCON ... 1042
Advanced Audit Service w NetWare 6 ... 1044

Rozdział 48. Zagadnienia bezpieczeństwa w sieciach rozległych ... 1047
Zostałeś namierzony! ... 1049
Wirusy komputerowe, konie trojańskie i inne niszczące programy ... 1050
Konie trojańskie ... 1051
Wirusy ... 1052
Jak dochodzi do infekcji ... 1053
Sieć pod ostrzałem — najczęstsze ataki ... 1054
Ataki typu „odmowa usługi” ... 1055
Rozproszony atak typu „odmowa usługi” ... 1055
Atak typu SYN flooding ... 1057
Przekierowania ICMP ... 1058

Ping of Death ... 1059
Fałszywe przesyłki pocztowe ... 1059
Ochrona haseł, SecurID oraz karty elektroniczne ... 1060
„Furtki" w sieci ... 1061
Sondy sieciowe ... 1062
Podszywanie i naśladownictwo ... 1063
Jeżeli coś jest zbyt dobre, aby było prawdziwe, na pewno takie nie jest ... 1063
Działania prewencyjne ... 1064
Zabezpieczanie routerów ... 1064
Sieć jako cel ... 1064
Zabezpieczanie komputerów — szyfrowanie i oprogramowanie antywirusowe ... 1065
Wykorzystanie Tripwire ... 1066
Świadomość i wyszkolenie użytkowników ... 1067
Stałe poznawanie zagadnień bezpieczeństwa ... 1068

Rozdział 49. Firewalle ... 1069
Czym jest firewall? ... 1069
Filtrowanie pakietów ... 1071
Filtrowanie adresów IP ... 1072
Filtrowanie w oparciu o protokoły ... 1072
Filtrowanie oparte na numerach portów ... 1074
Filtrowanie stanowe ... 1076
Serwery pośredniczące ... 1077
Standardowe zastosowania serwera pośredniczącego ... 1081
Ukrywanie użytkowników końcowych:
mechanizm translacji adresów sieciowych (NAT) ... 1083
Zalety i wady serwera pośredniczącego ... 1085
Rozbudowane firewalle ... 1085
Czego należy oczekiwać od firewalla? ... 1088
Tanie firewalle dla małych firm ... 1090
Rozwiązania sprzętowe ... 1090
Rozwiązania programowe ... 1091
Jednoczesne stosowanie firewalli sprzętowych i programowych ... 1092
Skąd wiadomo, że dany firewall jest bezpieczny? ... 1093

Rozdział 50. Wirtualne sieci prywatne (VPN) i tunelowanie ... 1095
Co to jest VPN? ... 1095
Mobilna siła robocza ... 1096
Protokoły, protokoły, jeszcze więcej protokołów! ... 1097
Protokoły IPSec ... 1097
Internet Key Exchange (IKE) ... 1098
Authentication Header (AH) ... 1100
Encapsulation Security Payload (ESP) ... 1101
Point-to-Point Tunneling Protocol (PPTP) ... 1102
Layer Two Tunneling Protocol (L2TP) ... 1103
Wbudowywanie pakietów L2TP ... 1104

Rozdział 51. Technologie szyfrowania ... 1105
Komputery i prywatność ... 1105
Co to jest szyfrowanie? ... 1106
Szyfrowanie pojedynczym kluczem — szyfrowanie symetryczne ... 1106
Szyfrowanie kluczem publicznym ... 1108
Kryptografia klucza publicznego RSA ... 1110
Certyfikaty cyfrowe ... 1110
Pretty Good Privacy (PGP) ... 1112

Część IX Rozwiązywanie problemów z siecią 1113

Rozdział 52. Strategie rozwiązywania problemów w sieciach 1115
Dokumentacja sieci przydaje się przy rozwiązywaniu problemów 1115
Utrzymanie aktualności dokumentacji 1118
Techniki rozwiązywania problemów 1121
Cykl rozwiązywania problemu 1121
Monitorowanie sieci w celu lokalizacji źródeł problemów 1124
Pułapki przy rozwiązywaniu problemów 1125

Rozdział 53. Narzędzia do testowania i analizowania sieci 1127
Podstawy: testowanie kabli 1127
Ręczne testery połączeń 1128
Testery kabli 1129
Testery bitowej stopy błędów 1129
Reflektometria w domenie czasu 1130
Impedancja 1131
Szerokość impulsu 1131
Prędkość 1132
Analizatory sieci i protokołów 1132
Ustalenie poziomu odniesienia 1133
Dane statystyczne 1135
Dekodowanie protokołów 1135
Filtrowanie 1135
Analizatory programowe 1136
Inne programowe analizatory sieci 1140
Analizatory sprzętowe 1141
Protokół SNMP 1142
Operacje elementarne SNMP 1143
Obiekty sieciowe: baza MIB 1143
Agenty pośredniczące 1145
Wyboista droga do SNMPv2 i SNMPv3 1146
RMON 1147

Rozdział 54. Rozwiązywanie problemów w małych sieciach biurowych i domowych 1151
Kłopoty z zasilaniem 1152
Problemy z konfiguracją komputerów 1153
Problemy z komponentami 1157
Chroń kable! 1158
Problemy z firewallami 1158
Higiena sieci 1159
Problemy z sieciami bezprzewodowymi 1159
Gdy nic innego nie pomoże… 1160

Część X Modernizacja sprzętu sieciowego 1163

Rozdział 55. Przejście z technologii ARCnet na technologię Ethernet lub Token-Ring 1165
Technologia ARCnet 1165
Przejście na technologię Ethernet lub Token-Ring 1166
Tworzenie nowej sieci 1168
Rozwiązywanie problemów z wydajnością 1171

Rozdział 56. Przejście z technologii Token-Ring na technologię Ethernet 1173
Przyszłość technologii Token-Ring 1173
Współpraca sieci Ethernet i Token-Ring 1175
Różnice utrudniające translację 1175
Bity i ramki 1176
Potwierdzenie dostarczenia 1176
Informacje dotyczące routingu 1177
Wymiana wszystkich komponentów sieci Token-Ring 1178
Przełączniki i routery 1178
Okablowanie sieciowe i złącza 1179
Karty sieciowe 1179

Rozdział 57. Modernizacja starszych sieci Ethernet 1181
Przejście z technologii 10BASE-2 lub 10BASE-T 1182
Elementy sprzętowe i programowe powiązane z technologiami 10BASE-2, 10BASE-T i 100BASE-T 1183
Kable sieciowe 1185
Karty sieciowe 1187
Złącza kabli sieciowych 1188
Mosty, koncentratory, repeatery i przełączniki 1188
Łączenie sieci opartych na różnym okablowaniu lub topologiach 1190
Inne rozwiązania 1190
Zastosowanie w sieci szkieletowej technologii Gigabit Ethernet 1191
Umieszczenie zaawansowanych serwerów w sieci Gigabit Ethernet 1191
Połączenie ze stacjami roboczymi oparte na technologii Gigabit Ethernet 1192
Zastosowanie technologii Gigabit Ethernet na dużych odległościach 1193
Technologia 10Gigabit Ethernet pod względem finansowym staje się coraz bardziej przystępna 1193

Rozdział 58. Zamiana mostów i koncentratorów na routery i przełączniki 1195
Zwiększanie rozmiaru sieci lokalnej 1196
Segmentacja sieci może zwiększyć jej wydajność 1198
Łączenie zdalnych lokacji 1199
Zamiana mostów na routery 1200
Zagadnienia dotyczące protokołu sieciowego 1201
Zagadnienia dotyczące adresów sieciowych 1201
Inne zagadnienia dotyczące zarządzania routerem 1202
Zastosowanie routera do segmentacji sieci 1203
Połączenie z większą siecią rozległą lub internetem 1204
Zamiana mostów na przełączniki 1205

Rozdział 59. Zastosowanie bezprzewodowych sieci lokalnych 1209
Dlaczego warto zastosować technologię sieci bezprzewodowych? 1210
Wybieranie lokalizacji dla punktów dostępowych 1212
Kwestie bezpieczeństwa 1213

Część XI Migracja i integracja 1215

Rozdział 60. Migracja z systemu NetWare do systemu Windows 2000 lub Windows Server 2003 1217
Protokoły i usługi systemu Windows 1218
Client Services for NetWare (CSNW) 1219
Gateway Services for NetWare (GSNW) 1220
Oprogramowanie Services for NetWare Version 5.0 (SFN) 1225
Porównanie uprawnień plików systemów Windows 2000/2003 Server i NetWare 1226
Instalacja narzędzia File and Print Services for NetWare Version 5.0 (FPNW 5.0) 1228
Microsoft Directory Synchronization Services (MSDSS) 1232
Narzędzie File Migration Utility (FMU) 1237

Rozdział 61. Migracja między systemami Windows NT, Windows 2000, Windows Server 2003, Unix i Linux oraz integracja tych systemów 1245
Protokoły i narzędzia systemu Unix obsługiwane przez systemy Windows 2000/2003 1246
Protokoły TCP/IP 1247
Usługa Telnet 1248
Usługa FTP (File Transfer Protocol) 1256
Zarządzanie usługą FTP w systemie Windows Server 2003 1258
Protokoły DHCP (Dynamic Host Configuration Protocol) i BOOTP 1261
Usługa DNS 1263
Aplikacje 1264
Windows Services for Unix 3.0 firmy Microsoft 1265
Instalacja pakietu SFU 3.0 1267
Usługa NFS (Network File System) 1270
Powłoka Korn Shell 1271
Komponent Password Synchronization 1274
Komponent User Name Mapping 1275
Nowy serwer i klient usługi Telnet 1276
Komponent ActiveState ActivePerl 5.6 1277
Samba 1278
Network Information System 1278

Rozdział 62. Migracja z systemu Windows NT 4.0 do systemów Windows 2000, Windows Server 2003 i Windows XP 1281
Czy konieczna jest aktualizacja systemu operacyjnego lub aplikacji? 1282
Aktualizacja do systemu Windows 2000 Server 1285
Zanim zaczniesz 1287
Kontrolery domeny Windows NT i serwery członkowskie 1288
Modelowanie struktury usługi katalogowej przy uwzględnieniu organizacji firmy 1290
Domeny będące partycjami usługi Active Directory 1290
Aspekty związane z migracją — porównanie administracji scentralizowanej ze zdecentralizowaną 1292
Wdrażanie usługi Active Directory 1294
Aktualizacja podstawowego kontrolera domeny 1294
Dodawanie innych domen do struktury usługi Active Directory 1296
Najpierw uaktualnij domenę główną 1297
Aktualizacja kolejnych zapasowych kontrolerów domeny 1300
Migracja z systemu Windows NT 4.0 lub systemu Windows 2000 do systemu Windows Server 2003 1301
Wymagania sprzętowe związane z aktualizacją do systemu Windows Server 2003 1302
Zestaw aplikacji sprawdzający zgodność oprogramowania 1303
Jaką rolę będzie spełniał serwer? 1304
Przykład aktualizacji systemu Windows 2000 Server do systemu Windows Server 2003 Enterprise Edition 1305
Czy powinno się używać systemu Windows 2000 Server czy Windows Server 2003? 1308
Aktualizacja klientów stosowanych w małych biurach 1309

Rozdział 63. Migracja między systemami NetWare, Unix i Linux oraz integracja tych systemów 1311
Dlaczego warto użyć systemu Unix lub Linux? 1311
Kluczowe różnice pomiędzy systemami Unix/Linux i NetWare 1312
Udostępnianie plików 1313
Udostępnianie drukarek 1313
Autoryzacja użytkowników 1314
Przenoszenie kont użytkowników 1314
Protokoły sieciowe 1315
Aplikacje 1315

Dodatki 1319

Dodatek A Siedmiowarstwowy referencyjny model sieci OSI 1321
To tylko model! 1321
Kapsułkowanie 1322
Warstwa fizyczna 1323
Warstwa łącza danych 1323
Warstwa sieci 1323
Warstwa transportowa 1324
Warstwa sesji 1324
Warstwa prezentacji 1324
Warstwa aplikacji 1325

Dodatek B Słownik terminów sieciowych 1327

Dodatek C Zasoby internetu przydatne administratorom sieci 1359
Organizacje standaryzujące 1359
Producenci sprzętu i oprogramowania sieciowego 1360
Sieci bezprzewodowe 1363
Bezpieczeństwo 1364

Dodatek D Protokół Lightweight Directory Access Protocol 1367
Wprowadzenie do LDAP 1367
Protokoły i standardy X.500 1368
Skróty, skróty, skróty! 1369
Schemat 1371
Lightweight Directory Access Protocol 1371
Protokół LDAP 1372
Podłączanie do serwera 1372
Przeszukiwanie bazy danych 1373
Dodawanie, modyfikowanie lub usuwanie informacji z katalogu 1373
Porównywanie danych w katalogu 1374
Katalogi LDAP 1374
Windows 2000 i NetWare nie są jedynymi produktami do wyboru 1374
Zgodność ze standardem: współpraca między katalogami 1375

Dodatek E Wprowadzenie do budowania sieci w małym biurze 1377
Definiowanie wymagań: czego potrzebujesz? 1378
Zakup sprzętu dla aplikacji 1380
Topologie małych sieci 1385
Archiwizacja dla małych firm 1387

Dodatek F Tabele masek podsieci 1389
Maski podsieci dla sieci klasy A 1389
Maski podsieci dla sieci klasy B 1390
Maski podsieci dla sieci klasy C 1390

Dodatek G Specyfikacje okablowania 1393
Specyfikacje sieci Ethernet 802.x 1393
Specyfikacje sieci 100VG-ANYLAN 1393
Specyfikacje sieci Token-Ring 1394
Specyfikacje sieci ARCnet 1394

Skorowidz 1395

Rozdział 14.

Ethernet, uniwersalny standard

Niemal wszystkie używane dzisiaj w firmach komputery PC i stacje robocze są podłączone do jakiejś lokalnej sieci komputerowej, zwykle sieci Ethernet. Mimo że inne technologie sieci lokalnych, jak Token-Ring czy oryginalny IPX/SPX firmy Novell, nadal są stosowane, popularność sieci Ethernet znacznie przewyższa popularność wszystkich pozostałych. Przekonasz się, że możliwości sieci Ethernet nie ograniczają się do łączenia wyłącznie komputerów, ale łączone mogą być także serwery, drukarki i inne urządzenia sieciowe. Standard stał się na tyle wszechobecny, że wszyscy więksi producenci sprzętu sieciowego projektują swoje urządzenia w taki sposób, by prawidłowo współpracowały właśnie z ethernetowymi sieciami LAN.

Zanim przejdziemy do analizy protokołów transportowych oraz usług i aplikacji sieciowych, powinniśmy dobrze zrozumieć, czym jest Ethernet i jak faktycznie działa. Ważne jest także zrozumienie tego, że istnieje więcej niż jeden standard Ethernet. To, co początkowo było prostą technologią sieci lokalnych, stało się z czasem standardem, który można stosować także do budowy rozległych sieci komputerowych. Technologia Ethernet umożliwia rozwiązywanie większości problemów sieciowych, z którymi możesz mieć do czynienia — od pierwszej komercyjnej wersji, przesyłającej dane z szybkością 10 Mb/s, do najnowszego standardu — Ethernetu 10-gigabitowego. Wszystkie te technologie możesz z łatwością wdrożyć na swoim biurku lub w szafce kablowej.

W tym rozdziale zajmiemy się najpierw początkami istnienia Ethernetu. Następnie opiszemy różne wersje tej technologii, których oficjalne standardy opublikowano i które są dostępne na rynku. Po dogłębnym przeanalizowaniu technologii sieci Ethernet zajmiemy się technikami wykorzystywanymi do rozwiązywania problemów w tego typu sieciach.

Krótka historia Ethernetu

Oryginalna technologia Ethernet została opracowana w laboratoriach Xerox PARC (Palo Alto Research Center) w latach siedemdziesiątych. Zadaniem Roberta Metcalfe'a było połączenie grupy komputerów w taki sposób, by mogły współużytkować opracowywaną wówczas przez firmę Xerox nową drukarkę laserową. Prawdopodobnie także w firmie Xerox po raz pierwszy skonstruowano osobistą stację roboczą i połączono ze sobą więcej niż dwa lub trzy komputery w jednym budynku (co było w owym czasie nie lada osiągnięciem).

Standard Ethernet był tworzony przez kilka kolejnych lat, a efektem tych prac było opublikowanie przez Metcalfe'a i Davida Boggsa artykułu „Ethernet: Distributed Packet-Switching for Local Computer Networks" (*Communications of the ACM*, tom 19, nr 5, lipiec 1976, strony 395 – 404). Autorzy publikacji wierzyli w pomyślne zakończenie prac nad tworzonym na Hawajach projektem ALOHA, który polegał na radiowym transmitowaniu pakietu danych w „eter" (ang. *ether*) — nazwa „eter" jest używana przez naukowców do określania przestrzeni, w której są przenoszone elektromagnetyczne sygnały radiowe. Pierwsza opisana eksperymentalna sieć Ethernet mogła mieć maksymalnie 1 kilometr długości, umożliwiała przesyłanie danych z maksymalną szybkością 3 Mb/s i zezwalała na podłączenie maksymalnie 256 stacji. W tamtym czasie było to znaczne osiągnięcie.

Publikacja Metcalfe'a i Boggsa przyspieszyła prace nad wieloma rozwiązaniami pojawiającymi się przez kilka kolejnych lat w obszarze sieci komputerowych. Jej autorzy przewidzieli ograniczenia związane z wykorzystywaniem w sieciach lokalnych współdzielonego nośnika. Metcalfe i Boggs zdawali sobie sprawę także z konieczności stosowania w przyszłości mostów (repeaterów z filtrowaniem pakietów) i protokołów wysokiego poziomu, które będą oferowały rozszerzoną przestrzeń pamięciową, zawierającą pola umożliwiające realizację routingu. Kolejną istotną kwestią, o której warto pamiętać, jest to, że autorzy specyfikacji sieci Ethernet — analogicznie do firmy IBM, twórcy popularnych dzisiaj komputerów osobistych, które stały się standardem — zdecydowali się na zastosowanie najbardziej dostępnego nośnika sieciowego: zwykłego przewodu koncentrycznego ze zwykłymi końcówkami i złączami. Ten ruch spowodował, że technologia sieciowa Ethernet okazała się w praktyce stosunkowo tania. Elektroniczna kopia publikacji Metcalfe'a i Boggsa jest dostępna w internecie pod adresem *http://www.acm.org/classics/apr96*.

Nieco później powstało konsorcjum trzech firm (Digital Equipment Corporation, Intel i Xerox), które opracowało standard nazwany Ethernet II, nazywany niekiedy w literaturze standardem DIX — od pierwszych liter nazw trzech firm, które go stworzyły. Wymienione firmy wykorzystywały nową technologię do zwiększenia możliwości sieciowych swoich produktów. Przykładowo firma Digital Equipment Corporation stworzyła w tym czasie największą komercyjną sieć komputerową na świecie, wykorzystując do łączenia ethernetowych sieci lokalnych swoje protokoły DECnet. Dzisiaj protokołami dominującymi w tego typu zastosowaniach są TCP/IP i (w znacznie mniejszym stopniu) IPX/SPX.

Idea łączenia setek lub tysięcy komputerów osobistych w biznesowe sieci lokalne mogła brzmieć dość nieprawdopodobnie w czasach, gdy po raz pierwszy podjęto prace nad technologią sieciową Ethernet. Głównie za sprawą swojej prostoty oraz dostępności urządzeń, oferowanych przez bardzo wielu producentów, Ethernet nie tylko przetrwał wiele lat jako standard sieci lokalnych, ale także doczekał się wielu udoskonaleń — nowszych i lepszych urządzeń oraz nośników sieciowych. Sieć Ethernet możesz teraz zbudować za pomocą przewodów koncentrycznych, ekranowanej lub nieekranowanej skrętki lub światłowodu.

Ile różnych rodzajów Ethernetu istnieje?

W roku 1985 opublikowano standard IEEE 802.3: „Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications". Publikacja tych specyfikacji ułatwiła producentom wytwarzanie sprzętu (od okablowania po karty sieciowe) umożliwiającego poprawne współdziałanie różnych urządzeń. Wszystkie

spośród wielu różnych standardów sieci Ethernet (które zostaną omówione w dalszej części tego rozdziału) są identyfikowane nazwą rozpoczynającą się od „IEEE 802." i uzupełnione liczbą oraz (opcjonalnie) jedną lub dwiema literami.

Za tworzenie standardów dla sieci lokalnych i rozległych odpowiada komitet IEEE 802 do spraw sieci LAN i MAN (*IEEE 802 LAN/MAN Standards Committee*). Komitet ten został utworzony w roku 1980 i pierwotnie nosił nazwę komitetu ds. standardów sieci lokalnych (*Local Network Standards Committee*). Oryginalna nazwa została zmieniona celem uwzględnienia ujawniających się w czasie prac możliwości stosowania tych standardów w sieciach MAN (sieciach metropolitalnych). W rozdziale 12., „Przyjęte przez IEEE standardy sieci LAN i MAN", znajdziesz krótkie opisy ważniejszych standardów zdefiniowanych dla sieci LAN/MAN.

Każdy, kto choć trochę zna się na sieciach komputerowych, wie, że skrót LAN odnosi się do sieci lokalnych (ang. *Local Area Network*). Innym popularnym akronimem jest WAN, który odnosi się do sieci rozległych (ang. *Wide Area Network*). Co więc oznacza skrót MAN? Oznacza sieć metropolitalną (ang. *Metropolitan Area Network*) — mniejszą od sieci WAN, ale większą od sieci LAN — która jest wykorzystywana przede wszystkim do łączenia grupy mniejszych sieci, znajdujących się na terenie miasta lub na określonym obszarze geograficznym.

Więcej informacji na temat działalności komitetu organizacji IEEE do spraw standardów sieci LAN i MAN oraz wydzielonych w nim różnych grup roboczych (pracujących nad szczegółowymi specyfikacjami standardów) znajdziesz w witrynie internetowej *http://ieee802.org/*. Możesz także pobrać ze wspomnianej witryny wiele z opracowanych przez ten komitet standardów, chociaż ich wydrukowanie zajęłoby Ci sporo czasu i wymagałoby zużycia mnóstwa papieru.

Komitet stworzył wiele różnych grup roboczych i grup doradztwa technicznego. Przykładowo grupa robocza pracująca nad standardem IEEE 802.3 w rzeczywistości tworzyła technologię CSMA/CD dla sieci Ethernet, a grupa IEEE 802.3z odpowiadała za standard Gigabit Ethernet, który jest szybszą wersją oryginalnej technologii 802.3.

Różne wersje Ethernetu są także nazywane zgodnie ze schematem, którego elementami są: oferowana przez daną wersję przepustowość, słowo „BASE" (od ang. *baseband signaling*, czyli sygnalizacji w paśmie podstawowym) oraz symbol określający wykorzystywany nośnik sieciowy. Przykładem takiego oznaczenia jest nazwa standardu 10BASE-T, którą można rozbić na trzy składowe:

- 10 — Ethernet, przepustowość na poziomie 10 Mb/s,
- BASE — sygnalizacja w paśmie podstawowym,
- T — okablowanie oparte na skrętce (ang. *Twisted pair — T*).

Wybór dostępnych na rynku rozwiązań opartych na technologii Ethernet jest bardzo szeroki. Oryginalna specyfikacja standardu Ethernet przewidywała zastosowanie grubego przewodu koncentrycznego (10BASE-5), w który należało wbijać odpowiednie złącza w celu podłączenia stacji roboczych. Nieco później opracowano tzw. „cienki" Ethernet (10BASE-2), które przewidywał łatwiejsze konstruowanie sieci z bardziej elastycznych

przewodów. Wraz z nowymi przewodami wprowadzono złącza BNC, które wyeliminowały konieczność wbijania złącza w przewód. W najnowszych wersjach Ethernetu wykorzystuje się tzw. skrętkę i światłowody, a do łączenia komputerów powszechnie stosowane są koncentratory i przełączniki.

Oryginalna technologia Ethernet II przewidywała pracę z szokującą wówczas szybkością 10 Mb/s. Najnowszym standardem, które prawdopodobnie już niebawem podbije rynek technologii sieciowych, jest Gigabit Ethernet, będący aktualnie przedmiotem standaryzacji. Jakby tego było mało, ukończono już prace nad rozwiązaniem 10Gigabit Ethernet, którego urządzenia są już dostępne na rynku (w segmencie przeznaczonym dla szczególnie wymagających użytkowników).

Oto najbardziej popularne standardy sieci Ethernet (w kolejności ich powstawania):

- **10BASE-5** — w standardzie tym, zwanym często „grubym" Ethernetem, wykorzystywane są grube przewody koncentryczne. „10" w nazwie oznacza maksymalną przepustowość sieci tego typu, czyli 10 megabitów na sekundę (Mb/s). Użyta w nazwie liczba „5" oznacza, że maksymalna długość segmentu w tej topologii wynosi 500 metrów. W sieciach 10BASE-5 stosuje się grube przewody koncentryczne. Aby zainstalować nowy węzeł w sieci, należy użyć tzw. wampira, który jest podłączany do okablowania szkieletowego przez wbicie go w gruby przewód koncentryczny. Tak podłączany przewód prowadzi się do stacji roboczej. Jeśli nadal wykorzystujesz tę technologię, najwyższy czas pomyśleć o unowocześnieniu swojej sieci.
- **10BASE-2** — standard ten, zwany często „cienkim" Ethernetem, przewiduje pracę sieci z taką samą maksymalną szybkością, jak w przypadku sieci 10BASE-5 (10 Mb/s), jednak wykorzystuje cieńsze, łatwiejsze w instalacji przewody. Liczba „2" w nazwie oznacza maksymalną długość segmentu tego typu sieci, która wynosi 200 metrów. Oznaczenie to jest nieco mylące, ponieważ rzeczywista maksymalna długość segmentu wynosi 185 metrów, jednak ewentualna nazwa 10BASE-1.85 odbiegałaby od przyjętej konwencji. Często spotyka się starsze sieci, łączone za pomocą wieloportowych repeaterów, gdzie każdy port łączy się za pomocą cienkich przewodów z jednym lub większą liczbą komputerów. Same repeatery są natomiast połączone ze sobą za pomocą grubych przewodów standardu 10BASE-5. Tworzenie prostych magistral w technologii 10BASE-2 jest możliwe dzięki stosowaniu złącza BNC w kształcie T. Jeśli jednak nadal stosujesz tę technologię, powinieneś zainteresować się bardziej współczesnymi rozwiązaniami.
- **10BASE-36** — ten rzadko stosowany standard sieci Ethernet wykorzystuje, zamiast sygnalizacji w paśmie podstawowym, sygnalizację szerokopasmową. Technologia przewiduje stosowanie przewodu koncentrycznego zawierającego trzy zestawy przewodów, każdy w oddzielnym kanale, z których każdy działa z szybkością 10 Mb/s i może mieć długość do 3 600 metrów.
- **10BASE-T** — połączenia sieciowe są prowadzone od stacji roboczych do centralnego koncentratora lub przełącznika, tworząc fizyczną topologię gwiazdy. Zastosowanie okablowania nieekranowanej skrętki (stąd „T" w nazwie standardu) sprawia, że sieć jest tańsza i znacznie łatwiejsza w instalacji niż sieci wykorzystujące mało elastyczne przewody koncentryczne. Ponadto centralizacja sieci umożliwia jej łatwe testowanie w poszukiwaniu błędów, izolowanie

wadliwych portów oraz przenoszenie użytkowników pomiędzy segmentami. Jeśli nadal stosujesz tę technologię, nie ma w tym nic złego; możesz jednak stwierdzić, że Twoja praca byłaby znacznie przyjemniejsza, gdybyś zaktualizował swoją sieć przynajmniej do standardu 100BASE-T.

- **10BASE-FL** — ta wersja Ethernetu także działa z szybkością 10 Mb/s, jednak wykorzystuje, zamiast przewodów miedzianych, przewody światłowodowe, a w szczególności światłowód wielomodowy (ang. *multimode fiber cable — MMF*) z rdzeniem o średnicy 62,5 mikrona i płaszczem o średnicy 125 mikronów. Do wysyłania i odbierania danych wykorzystywane są w nich dwa osobne włókna, co umożliwia komunikację w pełnym dupleksie. Ta technologia, tak jak wiele innych, należy już do historii.
- **100BASE-TX** — w tej wersji Ethernetu wykorzystywane są przewody kategorii 5 (patrz rozdział 6. — „Okablowanie sieciowe: kable, złącza, koncentratory i inne komponenty sieciowe"), co umożliwia zwiększenie odległości dzielącej stację roboczą i koncentrator do 100 metrów. Do przesyłania danych są wykorzystywane cztery żyły (dwie pary) w przewodzie. Technologia 100BASE-TX jest nadal powszechnie wykorzystywana i prawdopodobnie nie straci na popularności do czasu, kiedy nowe aplikacje wygenerują takie obciążenia w sieci, które sprawią, że konieczna będzie instalacja Ethernetu gigabitowego.
- **100BASE-T4** — wykorzystuje przewody kategorii 3 lub 5, co powoduje, że maksymalna odległość pomiędzy stacją roboczą a koncentratorem wynosi 100 metrów. Także w tej technologii komunikacja odbywa się za pomocą czterech żył (dwóch par) w przewodzie. 100BASE-T4 jest kolejnym standardem umożliwiającym przesyłanie danych z szybkością 100 Mb/s, która ma tę zaletę, że umożliwia wykorzystanie starszego okablowania, opartego na przewodach kategorii 3 (aktualizacja sieci nie wymaga instalowania przewodów kategorii 5 lub lepszych). Jeśli nadal używasz tego typu sieci i stwierdzasz jej przeciążenie i nadmierną liczbę błędów, czas rozważyć jej modernizację.
- **100BASE-FX** — wykorzystuje wielomodowe przewody światłowodowe, dzięki czemu maksymalna odległość dzieląca stację roboczą i koncentrator może wynosić nawet 412 metrów. Jedno włókno światłowodu jest wykorzystywane do nadawania, a drugie do odbierania danych.
- **1000BASE-SX** — dokument opisujący standardy IEEE 802.3z został zatwierdzony w roku 1998 i definiuje kilka technologii sieciowych z rodziny nazwanej Gigabit Ethernet. Standard 1000BASE-SX został zaprojektowany z myślą o pracy z wielomodowymi przewodami światłowodowymi, wykorzystującymi fale świetlne o długości około 850 nanometrów (nm). „S" w nazwie standardu oznacza mniejszą długość (ang. *short*) generowanych fal świetlnych. Maksymalna długość segmentu sieci 1000BASE-SX wynosi 550 metrów.
- **1000BASE-LX** — kolejny standard gigabitowego Ethernetu, zakładający pracę sieci z wykorzystaniem jednomodowego lub wielomodowego okablowania światłowodowego. Litera „L" w nazwie standardu oznacza większą długość fal świetlnych, od 1 270 do 1 335 nanometrów. Maksymalna długość segmentu sieci 1000BASE-SX wynosi 550 metrów w przypadku stosowania przewodów wielomodowych i 5 000 metrów w przypadku wykorzystania przewodów jednomodowych.

- **1000BASE-CX** — ten standard umożliwia wykorzystanie przez gigabitowy Ethernet ekranowanych przewodów miedzianych. Technologia została zaprojektowana z myślą o łączeniu urządzeń znajdujących się w niewielkich odległościach (do 25 metrów).
- **1000BASE-T** — standard IEEE 802.3ab dodano do warstwy fizycznej technologii Gigabit Ethernet, wykorzystującej nieekranowaną skrętkę kategorii 5. Maksymalna długość segmentu sieci 1000BASE-T wynosi 100 metrów.

Kolizje: czym są CSMA/CA i CSMA/CD?

W oryginalnym standardzie Ethernet (opracowanym w laboratoriach PARC) wykorzystywano metodę przesyłania danych za pomocą współdzielonego nośnika sieciowego, nazwaną *Carrier Sense Multiple Access* (*CSMA*). W specyfikacji technologii Ethernet II dodano do tej techniki mechanizm wykrywania błędów (ang. *Collision Detect — CD*) — tak powstała nowa nazwa metody, czyli CSMA/CD. Kolizja występuje w momencie, gdy dwie stacje robocze jednocześnie stwierdzą, że nośnik sieciowy jest dostępny i mniej więcej w tym samym czasie rozpoczną nadawanie danych, powodując tym samym zniekształcenia obu transmisji. Samo pojęcie *kolizji* oznacza, że pewne działania spowodowały jakiś błąd. W literaturze technicznej tego typu sytuację określa się czasami mianem *zdarzeń przyznania jednoczesnego dostępu* (ang. *stochastic arbitration event — SAE*) — taki termin w znacznie mniejszym stopniu niż określenie *kolizja* kojarzy się z błędem. Tego typu zdarzenia mają miejsce najczęściej w starszych sieciach Ethernet. Wystąpienie kolizji nie oznacza, że sieć uległa awarii. W sieciach o współdzielonym nośniku są to zdarzenia normalne (choć niepożądane). Dopiero gdy kolizje występują zbyt często, co znacząco ogranicza wydajność sieci, warto znaleźć ich źródła i ponownie rozmieścić stacje robocze lub urządzenia sieciowe, tak by działały właściwie.

Pojęcie domeny kolizyjnej przechodzi powoli do historii. Co prawda koncentratory i łącza półdupleksowe nadal wykorzystują mechanizm CSMA/CD, jednak w sieciach Ethernet wykorzystujących przełączniki pracujące w pełnym dupleksie rozwiązanie to jest już niepotrzebne. Zamiast tego mechanizmu urządzenia pełnodupleksowe wykorzystują osobne pary żył w przewodach, dzięki czemu przełącznik może jednocześnie wykorzystywać jedną parę do wysyłania danych do komputera i drugą do odbierania danych z tego samego komputera (wszystkie operacje są wykonywane za pomocą jednego portu przełącznika). Tworząc dzisiaj sieć komputerową, warto rozważyć zastosowanie niedrogich kart sieciowych i przełączników działających w trybie pełnego dupleksu. Technologię CSMA/CD omówimy w tym rozdziale tylko po to, by umożliwić Ci lepsze zrozumienie ewolucji, jakiej przez lata poddany był standard Ethernet oraz by dostarczyć niezbędnej wiedzy tym użytkownikom, którzy odziedziczyli starszy sprzęt sieciowy.

Używany we wczesnych implementacjach Ethernetu schemat kodowania Manchester wykorzystywał sygnały elektryczne o napięciu od –1,85 V do 1,85 V. Kolizje były wówczas wykrywane za pomocą pomiarów napięcia, które w przypadku wystąpienia kolizji wykraczało poza dopuszczalny przedział.

Wiesz już więc, że reguły wykorzystywane podczas tworzenia sieci Ethernet nie wynikają wprost z arbitralnych decyzji podejmowanych przez jakieś komisje — są raczej związane z właściwościami stosowanych w danej sieci fizycznych urządzeń. Urządzenie stosujące

mechanizm wykrywania kolizji, zapewniający właściwy dostęp do wspólnego nośnika sieciowego, oraz transmitujące sygnał musi dysponować informacją, jak długo potrwa transmisja, czyli (w najgorszym przypadku) jak długo potrwa przesyłanie danych do najbardziej oddalonego urządzenia w tym samym segmencie.

Dlaczego tak jest? Przypuśćmy, że dane urządzenie zaczyna transmisję danych. Ponieważ sygnał jest przenoszony w przewodzie ze zmienną szybkością, wykrycie przez wszystkie pozostałe węzły danego segmentu aktywności naszego urządzenia może zająć trochę czasu. Istnieje możliwość, że urządzenie najbardziej oddalone od węzła nadającego w danym segmencie nie otrzyma na czas informacji o rozpoczęciu transmisji i wcześniej rozpocznie nadawanie w sieci własnych danych. Efektem będzie oczywiście kolizja. Węzeł, który rozpoczął nadawanie jako pierwszy, nie wykryje kolizji do momentu, w którym otrzyma z powrotem uszkodzony sygnał, czyli po upływie czasu propagacji pakietu w sieci.

W sieciach zgodnych ze standardem Ethernet 10 Mb/s dane są przesyłane z szybkością 10 milionów bitów na sekundę. Specyfikacja standardu określa, że czas propagacji pakietu w sieci nie przekracza 51,2 milisekund — jest to czas zbliżony do czasu potrzebnego do przesłania 64 bajtów przy szybkości 10 Mb/s. Oznacza to, że — zgodnie ze specyfikacją — urządzenie powinno kontynuować przesyłanie swoich danych w czasie, który jest potrzebny do dotarcia jego sygnału do najbardziej oddalonego punktu w sieci i powrotu sygnału z tego punktu, czyli właśnie w tzw. czasie propagacji pakietu w sieci.

Innymi słowy, stacja robocza nie może rozpocząć transmisji nowego pakietu, dopóki nie minie czas potrzebny do przesłania pakietu pomiędzy dwoma najbardziej oddalonymi węzłami w danej topologii sieci zgodnej ze standardem Ethernet.

Jeśli urządzenie nie będzie nadawało w czasie propagacji pakietu w sieci, straci możliwość wykrycia kolizji, zanim jeszcze przystąpi do nadawania następnej ramki.

Jeśli rozmiar ramki, która wymaga ponownego przesłania, jest mniejszy niż 64 bajty, węzeł nadawczy wypełni ją zerami, by spełnić warunek minimalnej długości ramki.

W specyfikacji standardu Ethernet II zdefiniowano także maksymalny rozmiar ramki — ramka o minimalnej długości 64 bajtów może mieć maksymalnie 1 500 bajtów.

Wykorzystywane w tym rozdziale do określania długości pola w ramce ethernetowej pojęcie „bajta” w rzeczywistości nie jest dokładnie tym terminem, którym posługują się twórcy specyfikacji tego standardu. Zamiast tego w większości dokumentów stosowane jest pojęcie „oktetu”, czyli 8 bitów. Wykorzystuję pojęcie „bajta” przede wszystkim dlatego, że większość Czytelników znacznie lepiej wie o jego znaczeniu, dzięki czemu jest ono mniej mylące. Jeśli planujesz ubiegać się o przyznanie certyfikatu firmy Cisco, zapamiętaj dobrze słowo *oktet*!

Metodę wykorzystywaną przez urządzenia do komunikowania się przez sieć można opisać za pomocą następujących sześciu etapów:

1. Nasłuchuj sieć, by określić, czy którekolwiek inne urządzenie aktualnie nie transmituje swoich danych (ang. *Carrier Sense — CS*).
2. Jeśli żadne inne urządzenie nie nadaje swoich danych (linia jest wolna), rozpocznij transmisję.

3. Jeśli więcej niż jedno urządzenie wykryje w danym momencie brak transmisji, mogą one jednocześnie rozpocząć nadawanie. Fizyczne połączenie sieciowe jest przecież współdzielonym nośnikiem (ang. *Multiple Access — MA*).
4. Kiedy dwa urządzenia rozpoczynają nadawanie swoich danych w tym samym momencie, wysyłany przez nie sygnał jest zniekształcony, co transmitujące urządzenia powinny wykryć (ang. *Collision Detect — CD*).
5. Po nadaniu danych w sieci urządzenie przez chwilę nasłuchuje sieć, by określić, czy transmisja zakończyła się pomyślnie, czy też nastąpiła kolizja. Pierwsze urządzenie, które wykryje kolizję, rozsyła sygnał blokujący z kilkoma bajtami przypadkowych danych, by poinformować o zaistniałej sytuacji pozostałe urządzenia w sieci.
6. Każde urządzenie, którego działalność miała związek z wykrytą kolizją, wstrzymuje na krótko (kilka milisekund) swoją pracę i nasłuchuje sieć, by określić, czy nośnik sieciowy jest używany, a następnie próbuje wznowić transmisję. Każdy węzeł powodujący kolizję wykorzystuje algorytm losowo generujący czas oczekiwania, ograniczając tym samym możliwość ponownego wystąpienia kolizji. Ten mechanizm zakłada oczywiście, że dany segment sieci nie jest przeciążony, co mogłoby oznaczać niekończące się problemy z kolizjami i konieczność reorganizacji tej części sieci.

Zbyt częste kolizje mogą ograniczyć przepustowość w sieci. W dalszej części tego rozdziału zajmiemy się rozwiązaniami, które należy stosować w momencie, gdy obciążenie naszej sieci (nośnika) przekracza 40 – 50%.

Ponieważ standard Ethernet dopuszcza wykorzystanie tego samego nośnika sieciowego przez więcej niż jedno urządzenie (bez centralnego urządzenia sterującego ani mechanizmu przekazywania tokenów), kolizje nie tylko mogą wystąpić, ale są wręcz oczekiwanymi zdarzeniami w sieci. Kiedy to nastąpi, każdy węzeł „oczekuje" przez pewien (losowy) czas, by ograniczyć prawdopodobieństwo wystąpienia kolejnej kolizji przed wznowieniem transmisji (patrz kolejny podrozdział).

W przeciwieństwie do sieci Ethernet problem kolizji nie istnieje w sieciach Token-Ring. Zamiast obsługi wspólnego dostępu do nośnika i wykrywania kolizji prawo do nadawania sygnału w sieci jest w sieciach Token-Ring przydzielane za pomocą przekazywanej z węzła do węzła specjalnej ramki (tokenu). Stacja, która musi rozpocząć transmisję swoich danych, zawsze oczekuje na otrzymanie tokenu. Kiedy skończy nadawanie, przekazuje tę ramkę kolejnej stacji w sieci. Oznacza to, że Token-Ring jest siecią deterministyczną, która gwarantuje każdej stacji pierścienia możliwość transmisji danych w określonym czasie. Standard Ethernet przewiduje większą konkurencyjność węzłów sieci — każdy węzeł w sieci lokalnej musi współzawodniczyć o dostęp do nośnika sieciowego ze wszystkimi urządzeniami planującymi w danym momencie rozpoczęcie nadawania swoich danych. Można więc powiedzieć, że technologia Token-Ring posiada mechanizmy zapobiegania kolizjom, natomiast sieci Ethernet radzą sobie z kolizjami dopiero wtedy, kiedy one wystąpią.

Algorytm oczekiwania

Bez algorytmów oczekiwania urządzenie wykrywające kolizję natychmiast ponawiałoby próbę transmisji danych w sieci. Jeśli kolizja jest efektem jednoczesnej próby przesłania danych przez dwie stacje, takie rozwiązanie mogłoby spowodować ciągłe generowanie kolizji, ponieważ oba węzły mogłyby wznawiać nadawanie w tym samym czasie. Rozwiązaniem tego problemu jest zastosowanie algorytmu oczekiwania.

Algorytm oczekiwania jest jednym z podstawowych elementów mechanizmu CSMA/CD. Urządzenie sieciowe wstrzymuje swoją pracę i przestaje nadawać dane, a następnie obliczana jest losowa wartość, którą urządzenie wykorzystuje do wyznaczenia liczby milisekund, po upłynięciu których wznowi transmisję.

Wykorzystywany do wyznaczania tego czasu mechanizm obliczeń nosi nazwę skróconego binarnego algorytmu odczekiwania wykładniczego (ang. *Truncated Binary Exponential Backoff Algorithm*). Za każdym razem, gdy z powodu próby wysłania danej ramki w sieci następuje kolizja, urządzenie nadające wstrzymuje pracę na pewien czas, który przy każdej kolejnej kolizji jest dłuższy. Podejmowane jest maksymalnie 16 prób transmitowania danych. Jeśli po ich wykonaniu urządzenie stwierdzi, że przesłanie tych informacji za pomocą nośnika sieciowego jest niemożliwe, pomija daną ramkę i informuje o zaistniałej sytuacji składową wyższego poziomu stosu protokołów, która albo wznawia transmisję, albo przekazuje raport o błędzie użytkownikowi aplikacji.

Istnieje metoda dostępu podobna do *CSMA/CD*, nazywana *CSMA/CA*, w której dwie ostatnie litery (*CA*) oznaczają unikanie (a nie wykrywanie) kolizji (ang. *Collision Avoidance*). W sieciach wykorzystujących tę technikę (np. AppleTalk) urządzenia chcące uzyskać dostęp do fizycznego nośnika w pierwszej kolejności nasłuchują go, celem sprawdzenia jego wykorzystania. Zanim jednak rozpoczną transmisję ramki, wysyłają najpierw niewielki pakiet, sygnalizujący innym stacjom zamiar rozpoczęcia nadawania. Metoda ta pozwala znacznie ograniczyć liczbę kolizji, nie jest jednak zbyt popularna ze względu na dodatkowe obciążenie sieci związane z przesyłaniem tego typu pakietów. Pewna forma metody CSMA/CA jest wykorzystywana w sieciach bezprzewodowych zgodnych ze standardem IEEE 802.11.

Definiowanie domen kolizyjnych — magistrale, koncentratory i przełączniki

W rozdziale 8. — „Przełączniki sieciowe” — dogłębnie przeanalizowaliśmy zagadnienia ograniczania domeny kolizyjnej; ponieważ tradycyjne sieci Ethernet wykorzystują współdzielony nośnik sieciowy, konieczny jest mechanizm kontrolowania dostępu do tego nośnika oraz wykrywania i korygowania błędów wynikających ze zbyt częstego występowania kolizji.

W przypadku małych sieci lokalnych, łączących jedynie kilka komputerów, w zupełności powinien wystarczyć pracujący z szybkością 10 Mb/s koncentrator ethernetowy, który można kupić już za około 100 złotych. Z kolei mały, 5- lub 10-portowy przełącznik można zwykle kupić za 100 – 300 złotych (w zależności od producenta i liczby portów).

Zastosowanie małego koncentratora powoduje stworzenie domeny kolizyjnej, składającej się zazwyczaj z 5 do 10 komputerów. Chociaż urządzenie tego typu tworzy fizyczną sieć o topologii przypominającej gwiazdę, komputery podłączone do koncentratora formują w rzeczywistości logiczną magistralę, w której wszystkie łącza są współdzielone przez wszystkie węzły. Ramka wysyłana przez jedną ze stacji roboczych podłączonych do koncentratora będzie dostarczona do wszystkich pozostałych stacji roboczych podłączonych do tego samego koncentratora.

Koncentratory były zwykle wykorzystywane do łączenia niewielkich segmentów należących do większej sieci. Ponieważ dostępne obecnie na rynku przełączniki kosztują mniej więcej tyle samo, co koncentratory, wybór bardziej zaawansowanych i inteligentnych przełączników jest oczywisty. Wynika to przede wszystkim z faktu, że przełączniki ograniczają domenę kolizyjną jedynie do dwóch węzłów — samego przełącznika i komputera podłączonego do danego portu. W przypadku stosowania pełnego dupleksu problem domen kolizyjnych (podobnie jak samych kolizji) przestaje istnieć. Działanie przełącznika polega na przekazywaniu ramek sieciowych wyłącznie do portów, do których są adresowane. Jeśli większość danych w Twojej sieci jest przesyłana wewnątrz jednego segmentu sieci LAN, zastosowanie w tej sieci przełącznika może znacząco zwiększyć przepustowość.

Znacząca część obciążenia sieci jest związana z komunikacją z serwerami znajdującymi się poza daną siecią lokalną — zastosowanie przełącznika dysponującego szybkim połączeniem z przełącznikiem segmentu serwera może w takim przypadku znacznie przyspieszyć połączenia użytkowników końcowych. Ponieważ przełączniki eliminują domeny kolizyjne, efektem ich wykorzystania jest między innymi zwiększenie przepustowości w sieci Ethernet.

W kolejnych kilku podrozdziałach zajmiemy się podstawami wczesnych technologii wykorzystania współdzielonego nośnika sieci Ethernet — od architektury magistrali po koncentratory. Zrozumienie tych technologii jest ważne, jeśli chcesz uzasadnić konieczność unowocześnienia swojej sieci poprzez zastosowanie technologii przełączników ethernetowych.

Ograniczenia tradycyjnych topologii sieci Ethernet

Topologię sieci lokalnej (LAN) można opisać na dwa sposoby:

- Pierwszy to *topologia fizyczna*, która opisuje fizyczne rozmieszczenie nośnika sieciowego i połączonych za jego pomocą urządzeń.
- Drugi to *topologia logiczna*, która nie jest związana z rzeczywistymi połączeniami fizycznymi, a jedynie z logiczną ścieżką, jaką przebywają dane przesyłane z jednego węzła do drugiego.

W sieciach Ethernet wykorzystuje się wiele różnych technologii, z których każda charakteryzuje się innymi maksymalnymi długościami segmentów, odległościami pomiędzy węzłami itd. Przez pierwsze kilka lat prac nad standardem Ethernet stosowano wyłącznie

topologię magistrali. Kiedy zaczęło się pojawiać coraz więcej korporacyjnych sieci lokalnych, wprowadzono nowe standardy okablowania, umożliwiające konstruowanie sieci w topologii gwiazdy.

Czynniki ograniczające możliwości technologii ethernetowych

Magistrala i *gwiazda* są dwiema najbardziej popularnymi topologiami wykorzystywanymi do tworzenia lokalnych sieci zgodnych ze standardem Ethernet. Zastosowanie urządzeń służących do połączeń międzysieciowych — routerów i przełączników — umożliwia konstruowanie większych sieci o bardziej skomplikowanych topologiach.

Ogólnie rzecz biorąc, ograniczenia narzucane przez poszczególne topologie są pochodnymi następujących czynników:

- **Nośnik sieciowy** — narzuca ograniczenia długości segmentu i szybkości przesyłania danych.
- **Urządzenia połączeń międzysieciowych** — wykorzystywane do łączenia różnych fizycznych segmentów.
- **Liczba urządzeń w sieci** — ponieważ wymiana danych w sieciach Ethernet odbywa się przez rozgłaszanie, zbyt duża liczba urządzeń w tym samym segmencie rozgłaszania może spowodować problem przeciążenia sieci i tym samym spadek wydajności.
- **Mechanizmy dostępu do nośnika** — definiują sposób, w jaki pojedyncze urządzenia uzyskują dostęp do nośnika sieciowego; w sieciach zgodnych ze standardem Ethernet każda stacja robocza ma równe szanse w konkurowaniu o dostęp do lokalnego nośnika.

Urządzenia połączeń międzysieciowych i długości segmentów przewodów

Urządzenia połączeń międzysieciowych i długości segmentów przewodów to najbardziej podstawowe czynniki ograniczające lokalne sieci komputerowe. Im dłuższy przewód, tym słabszy sygnał — po przebyciu pewnej odległości sygnał ulega takiemu osłabieniu, że staje się niezrozumiały dla urządzeń podłączonych do nośnika. Nawet jeśli w regularnych odstępach podłączymy do sieci urządzenia wzmacniające lub regenerujące sygnał (jak w publicznych sieciach telefonicznych — PSTN), długość przewodu nadal będzie stanowiła problem z powodu określonego *czasu propagacji pakietu* w sieci, na podstawie którego określa się, czy pakiet został prawidłowo dostarczony adresatowi. Stacja wysyłająca pakiet nie może przecież czekać w nieskończoność na informację, czy w sieci wystąpiła kolizja lub czy z jakiegoś innego powodu transmitowany przez nią sygnał został zakłócony.

Długość segmentu przewodu zależy od typu tego przewodu:

- Segment sieci 10BASE-2 (tzw. cienki Ethernet), w którym wykorzystujemy cienkie przewody koncentryczne, może mieć maksymalnie 185 metrów długości. Jeśli zastosujemy repeatery, łączna długość przewodów sieci lokalnej 10BASE-2 może wynosić nawet 925 metrów.

- W przypadku sieci Ethernet 10BASE-T, w której wykorzystujemy nieekranowaną skrętkę, stacja robocza musi się znajdować nie dalej niż 100 metrów od koncentratora lub przełącznika.
- W środowiskach sieciowych zgodnych ze standardem Fast Ethernet możemy stosować różne rodzaje okablowania, od nieekranowanej skrętki po światłowody — każda ze specyfikacji Fast Ethernet definiuje różne ograniczenia długości przewodów. Przykładowo ograniczenie długości segmentu do 100 metrów obowiązuje, poza sieciami 10BASE-T, także w sieciach 100BASE-TX i 100BASE-T4.
- Długość segmentu w standardzie 100BASE-FX (okablowanie światłowodowe) wynosi około 2 kilometrów. Przewaga sieci zgodnych z tym standardem nad pozostałymi (wykorzystującymi inne rodzaje okablowania) czyni z 100BASE-FX dobrą technologię dla szybkich sieci szkieletowych. Na rynku istnieją jednak karty sieciowe, które umożliwiają łączenie zwykłych komputerów z okablowaniem światłowodowym — jeśli możesz sobie na nie pozwolić i potrzebujesz szybkiego połączenia, warto rozważyć ich zakup. Podłączanie pojedynczych stacji roboczych do światłowodu w większości przypadków jest przesadą, chyba że pracujesz w środowisku graficznym o znaczących wymaganiach dotyczących sieci.

Reguła 5-4-3

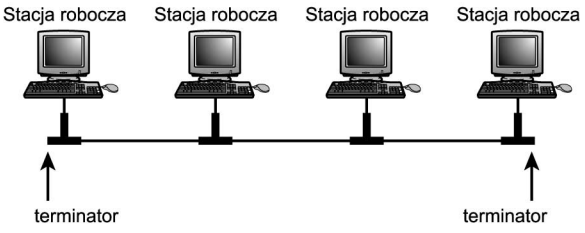
Istnieje prosty sposób zapamiętania, jakie elementy sieci możemy umieścić pomiędzy dwoma węzłami tradycyjnej lokalnej sieci Ethernet. *Reguła 5-4-3* oznacza, że możemy w tym miejscu podłączyć:

- maksymalnie pięć segmentów sieci LAN,
- maksymalnie cztery repeatery lub koncentratory,
- tylko trzy segmenty zawierające przewód z podłączonymi węzłami.

Jest to ogólna reguła, o której powinieneś pamiętać, planując topologię swojej sieci. Zauważ jednak, że ostatnia część tej reguły ma zastosowanie tylko w przypadku sieci opartych na przewodach koncentrycznych, np. 10BASE-2 lub 10BASE-5. Jeśli węzły są łączone za pomocą koncentratora lub przełącznika i skrętki, każdy węzeł ma swój własny przewód i łączy się — wraz z niewielką grupą roboczą lub tylko kilkoma komputerami — z większą siecią za pomocą tworzących właściwą strukturę koncentratorów i (lub) przełączników.

Stosowanie topologii magistrali

Topologia magistrali była wykorzystywana w pierwszych sieciach Ethernet. Jest to po prostu szereg komputerów lub urządzeń, połączonych pojedynczym przewodem (patrz rysunek 14.1). Układ stacji roboczych połączonych za pomocą pojedynczego wspólnego przewodu nazywa się niekiedy *układem łańcuchowym*. Tego typu topologię stosowano w konstruowanych za pomocą przewodów koncentrycznych sieciach 10BASE-2 i 10BASE-5.



Rysunek 14.1. *Topologia magistrali jest tworzona przez wiele urządzeń podłączonych do pojedynczego przewodu*

Topologia magistrali jest bardzo prosta w realizacji, związane z nią jest jednak kilka istotnych problemów:

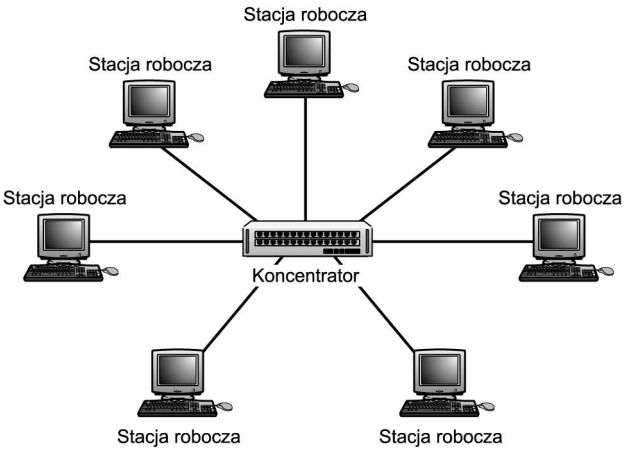
- Najsłabszym elementem tak skonstruowanych sieci lokalnych jest okablowanie. Na obu końcach magistrali muszą być podłączone odpowiednie końcówki (tzw. *terminatory*). Wadliwe działanie lub brak jednego terminatora może całkowicie uniemożliwić komunikację.
- Ponieważ wszystkie stacje robocze lub urządzenia współdzielą jeden przewód, znalezienie węzła będącego źródłem problemów może wymagać sporo czasu. Przykładowo niepoprawne podłączenie terminatora lub złącza przy jednej ze stacji roboczych może zakłócać pracę całej sieci lokalnej, a sprawdzenie złączy przy kolejnych stacjach roboczych może Ci zająć wiele godzin.
- Topologie magistrali w sieciach Ethernet buduje się zwykle za pomocą przewodów koncentrycznych (10BASE-2 oraz 10BASE-5). Chociaż topologia magistrali wymaga użycia znacznie mniejszego metrażu przewodu niż np. topologia gwiazdy, przewód koncentryczny jest droższy od prostej, nieekranowanej skrętki. W przypadku sieci 10BASE-5 wymagane przewody koncentryczne są mało elastyczne, co utrudnia kładzenie ich w budynkach.

Z uwagi na ograniczenia magistrali dotyczące łączenia w sieci lokalnej pojedynczych stacji roboczych topologie tego typu są zwykle wykorzystywane do łączenia mniejszych grup stacji, połączonych w sieć w kształcie gwiazdy. Przykładowo zanim opracowano wykorzystujące światłowody standardy Fast Ethernet i Gigabit Ethernet, do łączenia koncentratorów i przełączników stosowano właśnie przewody koncentryczne.

Stosowanie topologii gwiazdy

Zamiast łączyć stacje robocze w jednej linii za pomocą pojedynczego przewodu, możemy wykorzystać będący centralnym punktem sieci koncentrator, za pośrednictwem którego połączone będą wszystkie jej węzły. Rysunek 14.2 przedstawia prostą sieć lokalną o topologii gwiazdy, w której elementem centralnym jest właśnie koncentrator.

Wszystkie dane przesyłane z jednego węzła do drugiego muszą przejść przez koncentrator. Najprostsze koncentratory jedynie wzmacniają przekazywany do wszystkich portów sygnał; urządzenia bardziej skomplikowane mogą nie tylko wzmacniać przekazywany sygnał, ale także rozwiązywać drobne problemy w komunikacji.



Rysunek 14.2. *Stacje robocze łączą się z centralnym koncentratorem, tworząc gwiazdę*

Rozwój i popularność topologii gwiazdy wynika także z wprowadzenia przełączników na rynek urządzeń sieciowych. Przełącznik z zewnątrz niczym nie różni się od koncentratora, jednak znacząco ogranicza liczbę kolizji w sieci lokalnej. Przełączniki (patrz rozdział 8.) ograniczają liczbę kolizji, ponieważ nie rozgłaszają ponownie otrzymanej ramki we wszystkich portach. Przekazują ramkę wyłącznie do portu odpowiadającego jej adresatowi.

W porównaniu z topologią magistrali topologia gwiazdy jest rozwiązaniem korzystnym — ma jedynie kilka, stosunkowo mało istotnych, wad: wymaga więcej okablowania, a awaria centralnego koncentratora uniemożliwia pracę całej sieci. A oto korzyści płynące ze stosowania topologii gwiazdy:

- Instalacja okablowania dla tego typu sieci (podobnego do telefonicznego, ale wyższej jakości) jest łatwiejsza od instalacji przewodów koncentrycznych dla magistrali. Wymagana jest co prawda większa liczba i łączna długość przewodów, jednak przewody typu skrętka są tańsze i znacznie bardziej elastyczne.
- Znacznie prostsze jest wykrywanie błędów w sieci lokalnej dzięki diodom na obudowie koncentratora lub przełącznika. Do niektórych urządzeń tego typu dołączane jest także oprogramowanie zarządzające, które także pozwala na precyzyjne lokalizowanie awarii.
- Uszkodzenie pojedynczej stacji roboczej lub przewodu nie powoduje awarii całej sieci.
- Dodanie i usuwanie węzłów z tego typu sieci lokalnych jest bardzo proste — wystarczy włożyć końcówkę do wolnego gniazda koncentratora. Współczesne koncentratory nie wymagają umieszczania terminatorów w niewykorzystywanych portach.
- Jeśli koncentrator ulegnie awarii, można go szybko zastąpić, odłączając wszystkie przewody i podłączając je do nowego koncentratora lub przełącznika. Jeśli pozwala na to zasięg okablowania i używasz wielu koncentratorów lub przełączników, możesz (na czas naprawy) zwyczajnie przenieść użytkowników z wyłączonej jednostki do wolnych portów innej jednostki (lub innych jednostek).

Przez lata produkowane koncentratory stawały się coraz bardziej inteligentne, aż pojawiły się na rynku przełączniki dla sieci lokalnych. Przełącznik działa podobnie, jak koncentrator, ponieważ jest centralnym elementem okablowania sieci LAN. Główna różnica polega jednak na tym, że kiedy przełącznik „nauczy się", gdzie znajdują się poszczególne komputery, nie rozsyła wszystkich otrzymanych ramek do wszystkich swoich portów. Działanie przełącznika przypomina działanie wielu mostów umieszczonych w jednym urządzeniu. Kiedy przełącznik pozna już lokalizacje wszystkich połączonych ze sobą komputerów, ruch w sieci lokalnej może być bardzo szybko przełączany pomiędzy portami, co eliminuje zjawisko kolizji, nagminnie występujące w obciążonych sieciach z koncentratorem.

We współczesnych sieciach przełączniki są chętniej stosowane niż zwykłe koncentratory. Jeśli jednak niewielka sieć w Twoim domu lub biurze nie jest zbytnio obciążona, być może koncentrator będzie rozwiązaniem w zupełności wystarczającym (i bardzo tanim). Prawdopodobnie jednak nadejdzie dzień, kiedy nie będziesz w stanie znaleźć tego typu urządzenia w swoim ulubionym sklepie komputerowym, w którym półki będą się uginały od przełączników. Koncentratory omawiamy w tym rozdziale głównie po to, by pokazać Ci, jak przez lata ewoluowała technologia sieci Ethernet.

Hybrydowe topologie sieci LAN

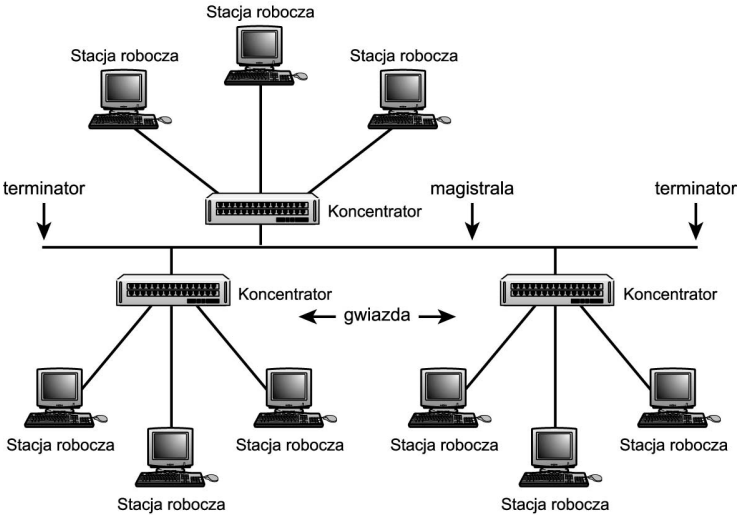
Przełączniki i koncentratory sprawiają, że tworzenie sieci lokalnych dla małych grup roboczych jest bardzo łatwe. Wykorzystując metody łączenia strukturalnego, możemy łatwo połączyć te koncentratory i przełączniki celem stworzenia większych sieci LAN. Istnieją dwie najbardziej popularne metody (topologie) dla tego typu sieci: *drzewo* i *gwiazda hierarchiczna*.

Drzewo

Rysunek 14.3 przedstawia złożoną topologię, grupującą stacje robocze w gwiazdy i łączącą tak pogrupowane węzły za pomocą liniowej magistrali. Takie rozwiązanie eliminuje większość problemów związanych z topologią magistrali, ponieważ pojedyncza stacja robocza nie może wstrzymać pracy całej sieci lokalnej. W sieci tego typu nadal mamy możliwość dodawania lub wymiany stacji roboczych przez proste przełączanie ich do portów koncentratora, przełącznika lub innego urządzenia. Inteligentne koncentratory i przełączniki oferują ponadto możliwość izolowania wadliwych portów (niektóre wykonują to automatycznie, inne wymagają interwencji za pomocą interfejsu zarządzania).

Drzewo jest niedrogą metodą łączenia np. wielu różnych działów firmy w jednym budynku. Każda lokalna grupa robocza może zatrudniać osobę administrującą siecią, która odpowiada za zarządzanie połączeniami z lokalnym koncentratorem lub przełącznikiem. Administrator całej sieci może decydować, kiedy i gdzie nowe urządzenia koncentrujące różne grupy będą dołączane do sieci.

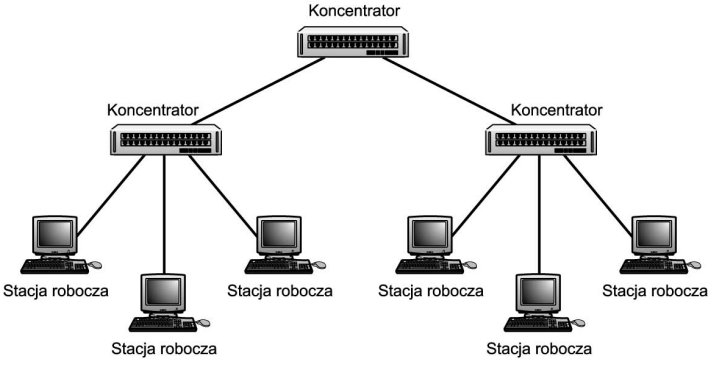
Głównym problemem tego typu hybrydowej topologii jest możliwość awarii przewodu szkieletowej magistrali — sieć jest wówczas dzielona na pojedyncze sieci (gwiazdy), skupione wokół koncentratorów lub przełączników. Stacje robocze mogą się komunikować wyłącznie z pozostałymi stacjami należącymi do tej samej grupy (przynajmniej do czasu znalezienia problemu z magistralą i rozwiązania go).



Rysunek 14.3. *W topologii drzewa poszczególne gwiazdy są łączone za pomocą magistrali*

Gwiazda hierarchiczna

Kolejną metodą łączenia koncentratorów i (lub) przełączników jest gwiazda hierarchiczna. Przykład tak skonstruowanej sieci przedstawia rysunek 14.4 — wykorzystujemy tam koncentrator lub przełącznik, który łączy inne urządzenia tego typu, będące centralnymi elementami sieci, łączącymi grupy stacji roboczych.



Rysunek 14.4. *Koncentratory i przełączniki mogą tworzyć hierarchię sieci w kształcie gwiazd*

Metodę tę możemy wykorzystywać do łączenia z centralnym koncentratorem maksymalnie 12 koncentratorów, tworząc tym samym ogromną sieć lokalną. Stosując tę metodę, możemy — bez stosowania mostów — połączyć maksymalnie 1 024 stacje robocze w jedną sieć lokalną. Pamiętajmy przy tym o regule 5-4-3 — na ścieżce pomiędzy dwoma węzłami może istnieć maksymalnie pięć segmentów przewodów, z maksymalnie czterema koncentratorami (lub repeaterami). Tylko trzy z pięciu segmentów przewodów mogą być wykorzystane do łączenia komputerów; dwa pozostałe muszą być wykorzystane do łączenia koncentratorów lub repeaterów.

Jeśli stosujesz przełączniki zamiast koncentratorów, możesz oczywiście znacznie rozbudować swoją sieć lokalną. Reguła 5-4-3 dotyczy tradycyjnych koncentratorów, tworzących domeny kolizyjne, obejmujące wszystkie łączone komputery. Przełączniki ograniczają

domenę kolizyjną, dzięki czemu w poszczególnych segmentach sieci nie istnieje problem współzawodniczenia węzłów o dostęp do nośnika sieciowego. Pamiętaj jednak, że źródłem ograniczeń mogą być połączenia pomiędzy samymi przełącznikami, ponieważ tego typu łącza są współdzielone przez wszystkie porty połączonych przełączników. Komputery połączone z przełącznikami mogą przesyłać dane z maksymalną szybkością wykorzystywanego standardu sieci Ethernet, np. 10 Mb/s lub 100 Mb/s. Jeśli jednak pomiędzy węzłami znajdują się dwa lub większa liczba węzłów, ograniczeniem może być szerokość pasma połączenia między przełącznikami, ponieważ w tym samym czasie pomiędzy przełącznikami może mieć miejsce więcej niż jedna sesja komunikacyjna.

Stosowanie sieci szkieletowych na poziomie korporacji

Do tej pory omawialiśmy sposoby łączenia w sieci lokalne pojedynczych stacji roboczych. Sieć LAN oparta na koncentratorze tworzy domenę rozgłaszania, w której wszystkie połączone stacje otrzymują dane transmitowane przez wszystkie pozostałe stacje robocze — jest to efekt zastosowania w sieci koncentratora. Przełączniki umożliwiają znaczne ograniczenie liczby kolizji w sieci — pod warunkiem, że albo komunikacja w sieci LAN ma głównie charakter lokalnej wymiany danych (wewnątrz jednego segmentu), albo przełącznik dysponuje szybkim łączem nadrzędnym z resztą sieci LAN.

Gdyby nie były dostępne inne technologie, umożliwiające łączenie różnorodnych domen rozgłaszania (sieci LAN), nie byłoby możliwe stworzenie internetu, który nie jest niczym innym, jak tylko połączeniem setek tysięcy mniejszych sieci.

W rozdziale 10. — „Routery” — przeanalizowaliśmy działanie routerów i możliwości ich stosowania do konstruowania większych sieci złożonych z wielu sieci LAN. Najkrócej mówiąc, urządzenia tego typu mogą służyć do tworzenia większych sieci, ponieważ każdy segment podłączony do routera jest traktowany jak osobna sieć LAN, podlegająca ograniczeniom związanym z okablowaniem i stosowanym protokołem. Domeny rozgłaszania należą do poziomu 2. modelu sieci OSI. Routery działają w 3. warstwie sieci i umożliwiają organizowanie w hierarchię wszystkich sieci podłączonych do internetu. To właśnie routery podejmują decyzje dotyczące przesyłania pakietów do innych sieci i mogą stosować wiele rodzajów szybkich protokołów dla połączeń typu LAN-LAN lub LAN-WAN.

Ramki sieci Ethernet

Kiedy mówimy o danych przesyłanych w sieci, używamy zwykle pojęcia „pakietu” w odniesieniu do jednostek danych. Wykorzystywana obecnie terminologia pojemników danych wprowadza jednak pewne rozróżnienie w nazewnictwie danych przesyłanych pomiędzy systemami — w zależności od poziomu siedmiowarstwowego modelu referencyjnego OSI, do którego się w danym momencie odwołujemy (patrz rysunek 14.5). Przykładowo jednostka danych w warstwie sieci jest nazywana *pakietem* lub *datagramem*. Pojęcie *datagramu* odnosi się zwykle do jednostek danych w usługach bezpołączeniowych, natomiast termin *pakiet* dotyczy zazwyczaj jednostek danych w usługach

Rysunek 14.5. *Nazwa jednostki danych zmienia się, kiedy ta jednostka jest przenoszona w górę i w dół stosu modelu referencyjnego OSI*

połączeniowych. Przekonasz się, że oba terminy są często stosowane w literaturze poświęconej protokołowi IP (ang. *Internet Protocol*). W warstwie łącza danych te datagramy nazywamy *ramkami*. Każda ramka zawiera zarówno informacje wymagane do dostarczenia jej do odpowiedniego adresata przez nośnik sieciowy, jak i wymieniane za jej pomocą właściwe dane. W warstwie fizycznej ramka jest transmitowana w postaci ciągu bitów, który jest uzależniony od konkretnej technologii, wykorzystywanej do kodowania danych w nośniku sieciowym.

►► Dobre wyjaśnienie znaczenia poszczególnych warstw modelu referencyjnego sieci OSI znajdziesz w dodatku A — „Siedmiowarstwowy referencyjny model sieci OSI".

Porcja danych w ramce składa się zwykle z bajtów zawierających informacje, które zostały tam umieszczone przez protokół wyższego poziomu i dostarczone do warstwy łącza danych, która odpowiada za transmisję ramki ethernetowej do węzła docelowego. Przykładowo protokół IP określa zarówno wykorzystywane przez siebie informacje w nagłówku, jak i dane przenoszone za pomocą datagramu IP. Kiedy datagram IP przechodzi w dół do warstwy łącza danych, wszystkie potrzebne informacje znajdują się nadal w jednostce danych ramki Ethernetu.

Skład ramki zależy od typu sieci. Format ramki oryginalnego Ethernetu i format ramki Ethernetu II w niewielkim stopniu różnią się od formatu ramki IEEE 802.3. Standard IEEE 802.5 (Token-Ring) definiuje natomiast ramkę, która różni się zasadniczo od wymienionych ramek sieci Ethernet. Wynika to z faktu, że sieci Ethernet i Token-Ring stosują inne metody uzyskiwania dostępu do nośnika sieciowego i wymiany danych pomiędzy węzłami sieci.

W tym rozdziale omówimy kilka różnych typów ramek oraz ewolucję tej technologii. Kiedy będziesz próbował rozwiązywać poważne problemy, stwierdzisz, że konieczne jest poznanie tego rodzaju szczegółowych informacji, aby dobrze zrozumieć, co naprawdę dzieje się w Twoich przewodach sieciowych.

XEROX PARC Ethernet i Ethernet II

Ramka oryginalnego standardu Ethernet definiuje kilka pól, które wykorzystano później także w specyfikacji ramki standardu Ethernet II:

- **Preambuła** — 8-bajtowa sekwencja zer i jedynek, wykorzystywana do oznaczania początku ramki i ułatwiająca synchronizację transmisji.
- **Docelowy adres MAC (Media Access Control)** — 6-bajtowy adres, wyrażany zwykle w formacie liczby szesnastkowej.
- **Adres MAC nadawcy** — kolejne 6-bajtowe pole, reprezentujące adres stacji roboczej, która wygenerowała ramkę.
- **Pole typu** — 2-bajtowe pole, oznaczające protokół klienta (np. IPX, IP lub DECnet), wykorzystywany w polu danych.
- **Pole danych** — pole o nieokreślonej długości, w którym znajdują się właściwe dane.

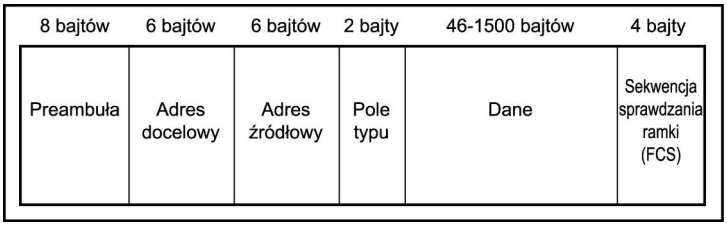
Określenie długości ramki pozostawiono protokołowi wyższego poziomu. Pole typu jest z tego powodu bardzo ważną częścią ramki.

Pojęcie *adresu MAC* oznacza adres warstwy Media Access Control (podwarstwy warstwy łącza danych modelu OSI). Jest to 48-bitowy adres, fizycznie przypisywany karcie sieciowej podczas jej produkcji. Adres MAC (nazywany czasem adresem sprzętowym lub adresem fizycznym) jest zwykle wyrażany w formie łańcucha 6 liczb szesnastkowych — po dwie cyfry dla każdego bajta — oddzielonych myślnikami, np. 08-00-2B-EA-77-AE. Pierwsze trzy bajty w unikalny sposób identyfikują producenta danego urządzenia sieci Ethernet, natomiast ostatnie trzy są unikalnym identyfikatorem, przypisanym przez tego producenta do danego urządzenia. Znajomość puli adresów MAC producenta może się przydać podczas rozwiązywania problemów w naszej sieci.

Adres sprzętowy FF-FF-FF-FF-FF-FF jest wykorzystywany do rozgłaszania, czyli przesyłania pojedynczego komunikatu do wszystkich węzłów w sieci lokalnej.

Na rysunku 14.6 widać rozmieszczenie poszczególnych pól w ramce oryginalnego standardu Ethernet.

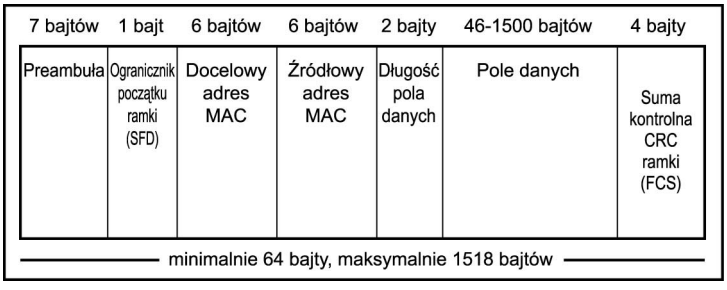
Rysunek 14.6. *Rozmieszczenie pól w ramce oryginalnego standardu Ethernet*



Standard 802.3

Kiedy w projekcie IEEE 802 zdefiniowano format ramki, okazało się, że zachowano większość cech ramki standardu Ethernet II. Istnieje jednak kilka istotnych różnic. Rozmieszczenie pól w ramce standardu Ethernet 802.3 zostało przedstawione na rysunku 14.7.

Podstawowa zmiana polega na wprowadzeniu nowego pola w miejsce wykorzystywanego wcześniej pola typu. Te 2 bajty są w standardzie 802.3 wykorzystywane do określania długości następującego po nich pola danych. Kiedy wartość w tym polu nie przekracza 1 500, możemy powiedzieć, że jest to pole długości. Jeśli omawiane pole zawiera wartość 1 536 lub większą, oznacza to, że jest wykorzystywane do definiowania typu protokołu.



Rysunek 14.7. *Format ramki standardu IEEE 802.3*

Dodatkowo ograniczono rozmiar preambuły z 8 do 7 bajtów, natomiast zaraz po niej umieszczony jest 1-bajtowy ogranicznik początku ramki (ang. *Start of Frame Delimiter — SFD*). Pole SFD zawiera ciąg bitów 10101011 (ostatni bajt stosowanej wcześniej 8-bajtowej preambuły zawierał w ostatnich dwóch bitach cyfry 1 i 0).

Ostatnią częścią ramki jest 4-bajtowa suma kontrolna ramki (ang. *Frame Check Sequence — FCS*), która służy do przechowywania obliczanej dla ramki sumy kontrolnej CRC. Stacja nadająca ramkę oblicza tę wartość na podstawie pozostałych bitów tej ramki. Stacja odbiorcza także oblicza wartość CRC według otrzymanych bitów i porównuje ją z liczbą otrzymaną w polu FCS. Jeśli obie wartości nie są identyczne, wiadomo, że ramka uległa uszkodzeniu podczas przesyłania i musi zostać nadana ponownie.

Standard sterowania łączem logicznym (LLC), 802.2

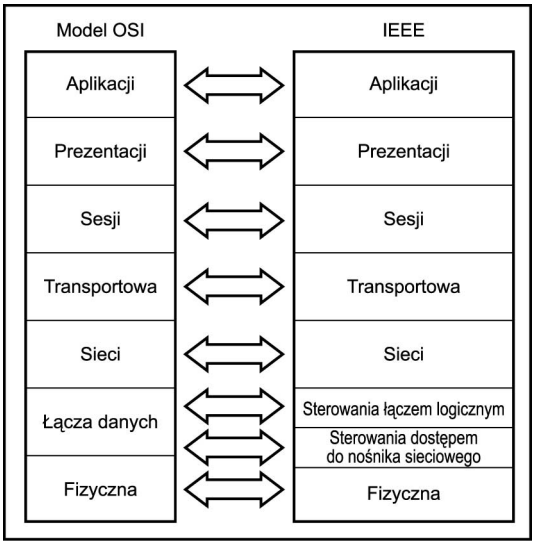
W siedmiowarstwowym referencyjnym modelu sieci OSI dwie najniższe warstwy to warstwa fizyczna i warstwa łącza danych. Kiedy w IEEE projektowano model referencyjny, przyjęto nieco inne założenia. Na rysunku 14.8 widać, że wersja opracowana przez IEEE zawiera — ponad warstwą fizyczną — podwarstwy sterowania łączem logicznym (ang. *Logical Link Control — LLC*) i sterowania dostępem do nośnika sieciowego (ang. *Media Access Control — MAC*). Zaproponowana przez IEEE podwarstwa sterowania dostępem do nośnika sieciowego znajduje się pomiędzy przyjętymi w modelu OSI warstwą fizyczną i warstwą łącza danych.

►► Więcej informacji na temat siedmiowarstwowego modelu referencyjnego sieci OSI znajdziesz w dodatku A.

Istnieje racjonalne uzasadnienie przekazania części funkcjonalności warstwy fizycznej modelu OSI podwarstwie sterowania dostępem do nośnika sieciowego i wydzielenia z warstwy łącza danych podwarstwy sterowania łączem logicznym: dzięki temu możliwe jest korzystanie w jednej sieci z różnych rodzajów nośników transmisyjnych i różnych metod uzyskiwania dostępu do tych nośników.

Nagłówek LLC

Podwarstwa sterowania dostępem do nośnika sieciowego odpowiada za właściwe wykorzystanie usług udostępnianych przez warstwę fizyczną i obsługi danych przesyłanych do i od zdalnych stacji roboczych w sieci. Do zadań podwarstwy LLC należy więc wykrywanie błędów i lokalne adresowanie (z wykorzystaniem adresów fizycznych, czyli adresów MAC).



Rysunek 14.8. *Model IEEE różni się od modelu referencyjnego OSI*

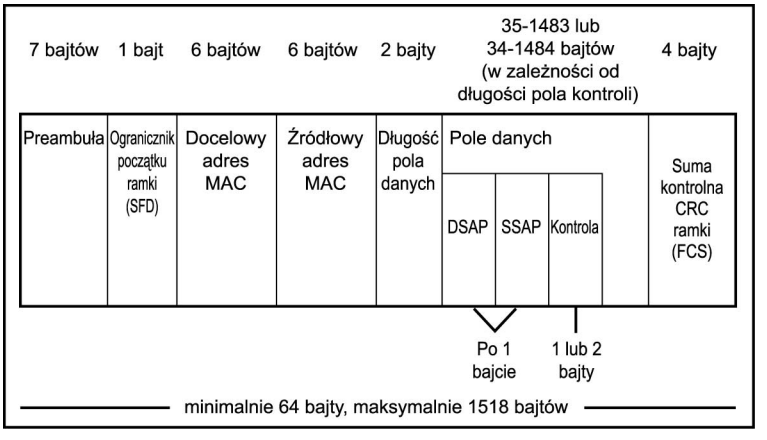
Podwarstwa LLC udostępnia wyższym warstwom usługi, które można podzielić na następujące trzy typy:

- **Usługa bezpołączeniowa bez potwierdzeń** — niektóre protokoły wyższego poziomu (np. TCP) udostępniają już funkcje sterowania przepływem i potwierdzania odbiorów, które umożliwiają weryfikację prawidłowego dostarczania pakietów. Nie ma potrzeby powielania tych funkcji w podwarstwie LLC.
- **Usługa połączeniowa** — ten rodzaj usługi utrzymuje aktywne połączenia i może być wykorzystywany w urządzeniach należących do sieci, których protokoły nie implementują pełnego modelu OSI.
- **Usługa bezpołączeniowa z potwierdzeniami** — ta usługa jest kombinacją dwóch pozostałych. Oferuje mechanizm potwierdzania faktu otrzymania pakietu, ale nie utrzymuje połączeń pomiędzy stacjami w sieci.

Aby umożliwić implementację tych funkcji podwarstwy LLC, w standardzie IEEE 802.2 zdefiniowano umieszczany w ramce „podnagłówek", który znajduje się bezpośrednio przed polem danych. Pole nagłówka LLC ma długość 3 bajtów. Pierwszy bajt reprezentuje punkt dostępu usługi docelowej (ang. *Destination Service Access Point — DSAP*), drugi reprezentuje punkt dostępu usługi źródłowej (ang. *Source Service Access Point — SSAP*), a ostatni to pole kontroli.

Ramka LLC sieci Ethernet

Na rysunku 14.9 przedstawiono kombinację podnagłówka LLC z ramką standardu 802.3 — łączny rozmiar ramki się nie zmienia, ograniczany jest jednak rozmiar danych przesyłanych za pomocą ramki (podnagłówek LLC wykorzystuje część pola danych).



Rysunek 14.9. *Ramka 802.3 z podnagłówkiem LLC*

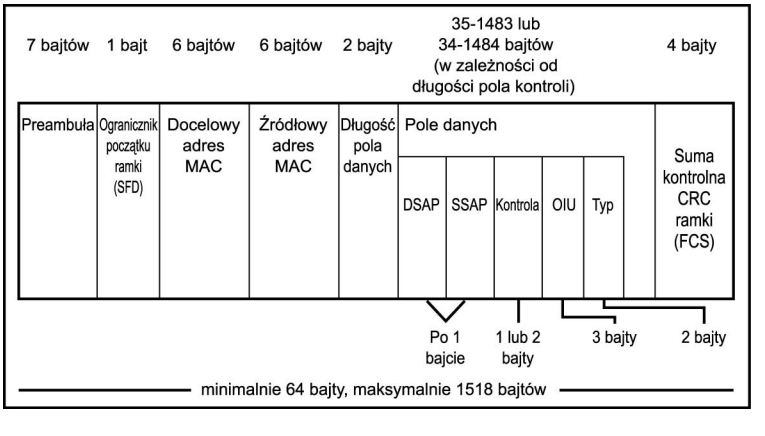
Standard ramki SNAP, 802.3

We wczesnych formatach ramek Xerox PARC i Ethernet II do określania protokołu wyższego poziomu, dla którego wygenerowano ramkę, wykorzystywano 2-bajtowe pole typu. W specyfikacji ramki standardu 802.3 zastąpiono to pole polem długości, które określa długość pola danych.

Aby zapewnić zgodność z wcześniejszymi technologiami sieciowymi, które ciągle wymagały, by ramki identyfikowały używany protokół, wprowadzono podramkę SNAP (od ang. *Sub-Network Access Protocol*). Konstruuje się ją, dodając dwa nowe pola do podnagłówka LLC zaraz po właściwych polach LLC:

- 3-bajtowy unikalny identyfikator OUI (od ang. *Organizationally Unique Identifier*),
- 2-bajtowe pole typu protokołu.

Rozszerzenia SNAP muszą się znajdować w polach nagłówka LLC, ponieważ ich istnienie w ramce nagłówka SNAP nie ma sensu, jeśli nie zawiera ona nagłówka LLC. Pełną postać ramki standardu 802.3 (włącznie z polami SNAP) przedstawiono na rysunku 14.10.



Rysunek 14.10. *Ramka standardu 802.3, zawierająca podnagłówek LLC i rozszerzenia SNAP*

Specyfikacja 802.5 definiuje format ramki wykorzystywany w sieciach Token-Ring. Sieci tego typu zasadniczo różnią się od sieci Ethernet — nie dotyczy to wyłącznie formatów ramek, ale także metod wykorzystywanych do uzyskiwania dostępu do nośnika sieciowego.

Standardy Fast Ethernet (IEEE 802.3u) i Gigabit Ethernet (IEEE 802.3z)

We wczesnych latach dziewięćdziesiątych opracowano szybszą wersję Ethernetu, której nadano nazwę Fast Ethernet (czyli szybki Ethernet). Ten standard (802.3u) umożliwia komunikację zarówno za pomocą przewodów miedzianych, jak i światłowodów z szybkością 100 Mb/s. Różne standardy zgodne z Fast Ethernet są nazywane w tradycyjny sposób — nazwa składa się z przepustowości, metody przesyłania sygnałów i typu nośnika (ten schemat nazewnictwa omówiliśmy wcześniej w tym rozdziale).

Standardy Fast Ethernet obejmują klasę sieci Ethernet, których nazwy rozpoczynają się od 100BASE-, podczas gdy nazwy rozpoczynające się od 1000BASE- odnoszą się do standardów zgodnych z technologią Gigabit Ethernet. Urządzenia Gigabit Ethernet już są dostępne na rynku. Specyfikację standardu 10Gigabit Ethernet ukończono w lipcu 2002 roku; niektórzy producenci (np. Cisco) już wprowadzają na rynek urządzenia pracujące zgodnie z tym standardem.

Fast Ethernet

Technologia Fast Ethernet została zaprojektowana w taki sposób, by zapewnić zgodność z istniejącymi sieciami 10BASE-T. Wykorzystuje ten sam format ramki i nadal stosuje zdefiniowaną w standardzie 802.3 metodę dostępu do nośnika CSMA/CD. Jedną z zalet tej technologii jest więc możliwość łatwej rozbudowy sieci (polegającej np. na sukcesywnej wymianie urządzeń) z wykorzystaniem okablowania istniejącej sieci 10BASE-T. Oznacza to, że dysponując inteligentnym koncentratorem (lub przełącznikiem), który ma możliwość wykrywania szybkości transmisji obsługiwanych przez karty sieciowe poszczególnych stacji roboczych, możesz wykorzystywać w swojej sieci urządzenia obu typów, które mogą bez problemu wzajemnie się komunikować. Koncentrator (lub przełącznik) zapewnia buforowanie danych wymienianych pomiędzy portami pracującymi z różnymi szybkościami. Jeśli Twoja sieć nadal zawiera komputery łączące się za pomocą sieci standardu 10BASE-T, powinieneś pamiętać o możliwości jej modernizacji do standardu Fast Ethernet. Jeśli przyjmiesz odpowiedni harmonogram, możesz tę modernizację wykonywać stopniowo, ponieważ porty z funkcją automatycznego wykrywania i karty sieciowe umożliwiają współpracę węzłów 10BASE-T i 100BASE-T w jednej sieci LAN.

100BASE-T

Jedną z zalet sieci 100BASE-T jest możliwość przejścia na tę technologię bez konieczności zmiany istniejącego w budynku okablowania kategorii 3. Specyfikacja standardu 100BASE-T przewiduje pracę albo ze skrętką (100BASE-TX i 100BASE-T4), albo ze światłowodami (100BASE-FX). Jedynym standardem umożliwiającym wykorzystanie okablowania kategorii 3 jest 100BASE-T4, zatem właśnie ta technologia powinna być

rozważana w sytuacjach, gdy nie można sobie pozwolić na dodatkowe koszty związane z wymianą okablowania sieciowego. Wymiana przewodów jest jednym z najdroższych elementów w procesie modernizacji istniejącej sieci. Jeśli jednak nadal używasz przewodów gorszych niż przewody kategorii 5, powinieneś już teraz poważnie zastanowić się nad ich wymianą i poniesieniem związanych z tym kosztów. Przepustowość 10 Mb/s jest po prostu zbyt niska dla większości dzisiejszych zastosowań w dużych sieciach korporacyjnych. Rozmiary aplikacji i plików z danymi nieprzerwanie rosną i szerokość pasma na poziomie 100 Mb/s jest obecnie uważana za rozsądne minimum dla większości przewodowych sieci lokalnych.

Istnieje ważna różnica pomiędzy standardami 100BASE-T4 i 100BASE-TX: w przewodach do nadawania i odbierania danych nie są używane te same pary żył. W standardzie 100BASE-T4 do komunikacji wykorzystywane są wszystkie cztery pary żył i stosowana jest zupełnie inna technika przesyłania sygnałów.

W przypadku sieci, które zostały — mimo stosowania technologii 10BASE-T (o niewielkich wymaganiach w tym zakresie) — przezornie skonstruowane w oparciu o okablowanie kategorii 5, przejście do standardu o przepustowości 100 Mb/s będzie najlepszym dowodem trafności tamtej inwestycji. Specyfikacja standardu 100BASE-T, w której przewidziano wykorzystanie skrętki, może być stosowana zarówno z tego typu przewodami nieekranowanymi, jak i ekranowanymi (STP), które są zwykle używane w sieciach Token-Ring. Standard 100BASE-TX oparto na specyfikacji ANSI TP-PMD (od ang. *Twisted-Pair Physical Medium Dependent*). Maksymalna długość segmentu wynosi 100 metrów, powinieneś jednak pamiętać o dodaniu do tej odległości dystansu, jaki dzieli gniazdko użytkownika od jego stacji roboczej.

Łączna długość okablowania w sieci lokalnej zawierającej do dwóch koncentratorów może wynosić maksymalnie 200 metrów. Istnieją dwie klasy koncentratorów: klasa I oraz klasa II. Pamiętaj, że koncentratory są obecnie uważane za urządzenia przestarzałe i można je spotkać tylko w starszych (dawno nie modernizowanych) sieciach. Na rynku znajduje się coraz mniej urządzeń tego typu. Jeśli jednak Twoja sieć nie była od jakiegoś czasu modernizowana, poniższe informacje mogą Ci się przydać. Oto krótki opis klas koncentratorów:

- **Koncentratory klasy I** — standardowy koncentrator sieci 10BASE-T otrzymuje dane z pewnego segmentu i przekazuje niezmieniony sygnał do innych segmentów podłączonych do swoich portów. Ponieważ istnieją trzy odmiany sieci 100BASE-T, standardowy koncentrator wprowadza dla łączonych przez siebie pojedynczych segmentów sieci LAN ograniczenie, polegające na wykorzystywaniu tylko jednego standardu 100BASE-T. Koncentratory klasy I rozwiązują ten problem, „tłumacząc" (przed przesłaniem do innych portów) przychodzące sygnały z jednego formatu na drugi. Ze względu na obciążenia związane z przetwarzaniem sygnału specyfikacja standardu ogranicza stosowanie tego typu koncentratorów, zezwalając na używanie tylko jednego takiego urządzenia w sieci.
- **Koncentratory klasy II** — koncentrator klasy II działa tylko z jednym typem nośnika — 100BASE-TX. Oznacza to, że nie jest konieczne specjalne przetwarzanie sygnału — wystarczy działanie na zasadzie wieloportowego repeatera. W jednej domenie kolizyjnej mogą istnieć maksymalnie dwa koncentratory klasy II.

100BASE-T4

W przypadku sieci opartych na okablowaniu kategorii 3 i 4 jedynym sposobem na przeprowadzenie ich modernizacji bez wymiany przewodów jest zastosowanie urządzeń technologii 100BASE-T. Standard ten wykorzystuje metodę przesyłania sygnałów w trybie półdupleksowym za pomocą czterech par żył (inaczej niż w przypadku dwóch par, wykorzystywanych do komunikacji w sieciach 10BASE-T i 100BASE-TX). Trzy z tych par żył są wykorzystywane do przesyłania właściwych danych, natomiast czwarta służy wykrywaniu kolizji. Każda z tych trzech par umożliwia transmisję danych z szybkością 33,3 Mb/s, co daje razem 100 Mb/s (ten rodzaj sygnalizacji nosi nazwę 4T+). Ponadto w przewodach stosuje się trzypoziomowy schemat kodowania, zamiast używanego w większości innych nośników schematu dwupoziomowego. Ponieważ standard 100BASE-T4 wymaga specjalnego sprzętu (kart sieciowych i koncentratorów) i działa w trybie półdupleksowym, nie powinien być rozważany jako technologia dla nowych sieci, a jedynie jako możliwy sposób ulepszenia istniejącego rozwiązania (kiedy inne opcje są niemożliwe).

100BASE-FX

Przewody światłowodowe umożliwiają konstruowanie dłuższych segmentów sieci Fast Ethernet. Sieć 100BASE-FX wykorzystuje przewody z dwiema wiązkami (jedna do nadawania, druga do odbierania danych) i może mieć nawet 2 kilometry długości.

Światłowody są dobrym rozwiązaniem dla sieci szkieletowych. W przeciwieństwie do przewodów miedzianych, które wykorzystują do komunikacji impulsy elektryczne, w przewodach światłowodowych stosowane są impulsy świetlne. To sprawia, że przewody światłowodowe znacznie lepiej sprawdzają się w środowiskach charakteryzujących się dużymi zakłóceniami elektrycznymi. Przewody tego typu są także znacznie bezpieczniejsze, ponieważ nie emitują sygnałów elektrycznych, które mogłyby być przechwytywane przez specjalistyczne urządzenia podsłuchowe. Z uwagi na możliwości oferowane przez światłowody z pewnością będą one w przyszłości (po opracowaniu nowych standardów) umożliwiały przesyłanie danych z jeszcze większymi szybkościami.

Gigabit Ethernet

W roku 1998 ukończono prace nad specyfikacją technologii 802.3z, nazwanej Gigabit Ethernet (gigabitowym Ethernetem), na którą składają się następujące standardy:

- **1000BASE-SX** — wykorzystuje światłowody wielomodowe do łączenia na niewielkie odległości. W przypadku przewodów o średnicy rdzenia 50 mikronów maksymalna długość przewodu wynosi 300 metrów, a w przypadku przewodów o średnicy rdzenia 62,5 mikronów maksymalna długość wynosi 550 metrów.
- **1000BASE-LX** — wykorzystuje światłowody jednomodowe o maksymalnej długości 3 000 metrów lub wielomodowe o maksymalnej długości 550 metrów.
- **1000BASE-CX** — wykorzystuje przewody miedziane, czyli skrętkę, zapewniającą dużą wydajność na odległości maksymalnie 25 metrów. Standard ten został zaprojektowany z myślą o szafach kablowych.
- **1000BASE-T** — wykorzystuje przewody skrętki kategorii 5 o maksymalnej długości 100 metrów.

Wersja technologii Gigabit Ethernet wykorzystująca okablowanie UTP jest znana jako standard 802.3ab. Z uwagi na niewielki zasięg (do 25 metrów) jest przeznaczona przede wszystkim do łączenia urządzeń rozmieszczonych na małej przestrzeni.

Oczekuje się, że standard Gigabit Ethernet będzie prawidłowo współpracował z sieciami działającymi z szybkościami 10 i 100 Mb/s. Wykorzystywany będzie ten sam protokół dostępu do nośnika sieciowego (CSMA/CD) oraz ten sam format i rozmiar ramek. Gigabitowy Ethernet będzie doskonałym rozwiązaniem dla szkieletów sieci, które będą łączone za pomocą routerów i koncentratorów (a także innych typów repeaterów) — zarówno dzięki zgodności z istniejącymi technologiami, jak i z powodu uzyskiwanych szybkości transmisji. Użyteczność technologii Gigabit Ethernet jako rozwiązania dla sieci szkieletowej wynika na przykład z możliwości komunikacji w trybie pełnego dupleksu na wydzielonych łączach. W tym trybie do przesyłania danych wykorzystywane są dwa połączenia (jedno do wysyłania, drugie do odbierania danych), co oznacza, że nie jest potrzebny mechanizm wykrywania kolizji — to z kolei umożliwia szybsze przesyłanie danych pomiędzy przełącznikami wykorzystywanymi do łączenia sieci lokalnych.

Definiujący tzw. gigabitowy Ethernet standard IEEE 802.3z przewiduje dodanie nowego pola do podstawowej ramki 802.3: jest to pole *rozszerzenia*. Pole to zostało dodane do ramki bezpośrednio za polem sekwencji sprawdzania ramki i jest wykorzystywane do zwiększenia minimalnego rozmiaru ramki do 512 bajtów (zamiast wykorzystywanych w wolniejszych sieciach 64 bajtów). Zwiększony minimalny rozmiar ramki jest potrzebny tylko w sytuacjach, gdy sieć standardu Gigabit Ethernet działa w trybie półdupleksowym i nadal wykorzystuje mechanizm wykrywania kolizji. Wspomniane pole jest zbędne w pełnym dupleksie.

Kolejną metodą zwiększenia szybkości przesyłania danych w sieciach Gigabit Ethernet jest ograniczenie kosztów związanych z wykorzystywaniem mechanizmu CSMA/CD dla każdej ramki przesyłanej w sieci. Do standardu 802.3z dodano tzw. tryb wiązkowy (ang. *burst mode*), który umożliwia kolejne przesyłanie wielu ramek zaraz po otrzymaniu dostępu do nośnika sieciowego. Jest to możliwe dzięki specjalnym tzw. *bitom rozszerzającym*, wstawianym w wolnych przestrzeniach pomiędzy normalnymi ramkami. Te bity utrzymują aktywność nośnika, dzięki czemu pozostałe stacje nie mogą wykryć jego bezczynności i próbować transmitować swoich danych.

Kolejną, rozważaną przez wiele firm propozycją jest stosowanie tzw. ramek Jumbo. Pomysł (opracowany przez firmę Alteon Networks) polega na zwiększeniu długości ramki ethernetowej (w trybie pełnego dupleksu) do 9 018 bajtów. Dalsze zwiększenie rozmiaru ramki byłoby niepraktyczne, ponieważ wykorzystywany w sieciach Ethernet mechanizm wykrywania błędów CRC nie mógłby działać wystarczająco precyzyjnie. Mimo to zwiększenie maksymalnego rozmiaru ramki z 1 500 bajtów (w sieciach Ethernet) do 9 018 bajtów jest posunięciem radykalnym.

Standard Gigabit Ethernet jest obecnie powszechnie stosowany w szkieletowych sieciach lokalnych, łączących mocno obciążone usługi lub przełączniki. Tego typu funkcje były wcześniej realizowane przez sieci standardu Fast Ethernet (jeszcze wcześniej był to oczywiście Ethernet, działający z szybkością 10 Mb/s). Kiedy jedna technologia wkracza na rynek stacji roboczych, kolejna zastępuje istniejący standard sieci szkieletowych. W obszarze szybkich protokołów transportowych standard Gigabit Ethernet może teraz konkurować z technologiami ATM i Frame Relay, które wcześniej miały niemal monopol na tym rynku.

Chociaż w sieciach MAN dość powszechnie wykorzystuje się obecnie standard SONET, to im szybsze będą kolejne technologie Ethernetu, tym trudniejsze będzie utrzymać w roli protokołów transportowych starszych standardów sieciowych.

Kiedy protokół IP osiągnie i przekroczy ograniczenie szybkości 10 gigabitów, bez wątpienia stanie się istotnym elementem rynku sieci szkieletowych. Ponieważ Ethernet pozostaje Ethernetem (przynajmniej dopóki podłączasz właściwe przełączniki), zarządzanie pojedynczym protokołem jest prostsze niż próba zarządzania odwzorowaniem jednego protokołu na drugi. Standard Gigabit Ethernet jest z pewnością technologią przyszłości dla Twojej sieci lokalnej; na rynku są już dostępne urządzenia standardu 10Gigabit Ethernet, jednak ich cena na razie uniemożliwia ich powszechne stosowanie.

Standard 10Gigabit Ethernet (IEEE 802.3ae)

Jeśli znasz inne protokoły sieci WAN, stosowane w rozległych sieciach szkieletowych i internecie, być może uważasz, że nie ma potrzeby rozwijania technologii ethernetowych (czyli — z natury protokołu — sieci LAN) przekraczających wymagania stawiane typowym sieciom lokalnym. Dzięki możliwościom stosowania przełączników, zwiększanym szybkościom przesyłania danych i łączom pełnodupleksowym Ethernet okazał się znacznie lepszym rozwiązaniem od wszystkich innych technologii, zaproponowanych przez ostatnie 30 lat. Wystarczy, że porównasz te parametry np. ze standardem Token-Ring. Nie ma jednak powodu, by wstrzymywać dalszy rozwój standardu Ethernetu, który może przynieść wiele korzyści.

W standardzie 10Gigabit Ethernet utrzymano format ramki 802.3 oraz znane z wcześniejszych wersji Ethernetu minimalne i maksymalne rozmiary ramek. Nowa technologia wyklucza jednak możliwość komunikacji w trybie półdupleksowym oraz stosowania mechanizmów współdzielonego dostępu do nośnika sieciowego (zakłada więc wykorzystanie wyłącznie przełączników, a nie koncentratorów). Rezygnacja z trybu półdupleksu i — tym samym — potrzeby stosowania mechanizmu CSMA/CD sprawia, że zasięg segmentów w nowej technologii sieci Ethernet jest ograniczany wyłącznie przez fizyczne własności nośników sieciowych i metod przesyłania sygnałów. Kolejnym ważnym powodem rezygnacji z trybu półdupleksu jest fakt, iż mimo że standard Gigabit Ethernet umożliwia pracę w obu trybach (pełny dupleks i półdupleks), użytkownicy niemal jednomyślnie wybierali urządzenia pracujące w trybie pełnego dupleksu.

Specyfikacja standardu 802.3ae przewiduje istnienie dwóch typów warstwy fizycznej (ang. *Physical layer — PHY*): warstwy sieci LAN i warstwy sieci WAN. Warstwa PHY jest dalej dzielona na dwie podwarstwy: podwarstwę zależną od fizycznego nośnika (ang. *Physical Media Dependent — PMD*) oraz podwarstwę fizycznego kodowania (ang. *Physical Coding Sublayer — PCS*). Podwarstwa PCS odpowiada za sposób kodowania danych w fizycznym nośniku sieciowym. Podwarstwa PMD reprezentuje parametry fizyczne, np. stosowaną długość fal laserowych lub świetlnych.

Warstwy LAN PHY i WAN PHY obsługują te same podwarstwy PMD. Podwarstwy PMD sieci 10Gigabit Ethernet wykorzystują zakres od lasera 850 nm w wielomodowych światłowodach (50,0 mikronów) dla mniejszych odległości (do 65 metrów) do lasera 1 550 nm w jednomodowych światłowodach (9,0 mikronów) dla sieci o długości nawet 40 kilometrów. Warstwa LAN PHY będzie przeznaczona do działania z istniejącym kodowaniem sieci lokalnych standardu Gigabit Ethernet, jednak z większą szybkością przesyłania danych.

Warstwa LAN PHY jest osobnym fizycznym interfejsem, umożliwiającym komunikację na większe odległości z opcjonalnym (rozważanym obecnie) interfejsem, umożliwiającym wykorzystanie przez sieci 10Gigabit Ethernet sieci SONET/SDH. SONET OC-192 oferuje przepustowość zbliżoną do proponowanej w standardzie 10Gigabit Ethernet. Potrzebny jest jedynie prosty mechanizm buforujący, który umożliwi połączenie urządzeń obu standardów. Ponieważ technologia SONET/SDH jest dosyć popularna, takie rozwiązanie nie będzie wymagało od operatorów sieci WAN ogromnych inwestycji związanych z wymianą okablowania na takie, które będzie w stanie obsłużyć przesyłanie danych z sieci standardu 10Gigabit Ethernet. Zamiast tego będą oni mogli niewielkim kosztem rozszerzyć ofertę proponowaną swoim użytkownikom. Połączenie sieci Ethernet za pomocą sieci rozległych, bez konieczności czasochłonnej konwersji formatów ramek, znacznie ułatwi zarządzanie sieciami WAN, ponieważ ograniczy liczbę czynników będących źródłem potencjalnych awarii.

Obecnie standard 10Gigabit Ethernet jest jednak powszechnie uważany za protokół sieci WAN. Szacuje się, że implementacja usług sieci 10Gigabit Ethernet będzie tańsza niż konstrukcja podobnych rozwiązań T3 dla środowisk MAN i WAN.

Istnieje oczywiście grupa krytyków, którzy twierdzą, że sieci Ethernet nigdy nie będą posiadały mechanizmów gwarancji jakości usługi (ang. *Quality of Service — QoS*), oferowanych przez sieci ATM. Poza tym, w porównaniu z technologią SONET i innymi szybkimi protokołami transmisyjnymi, Ethernet oferuje stosunkowo niewiele narzędzi administracyjnych. Prostota standardu Ethernet i fakt, że kosztuje on znacznie mniej niż inne rozwiązania sieci WAN, czyni z niego jednak atrakcyjnego konkurenta na tym rynku.

Problemy w sieciach Ethernet

Ponieważ w tradycyjnym standardzie Ethernet wykorzystywany jest współdzielony nośnik sieciowy, wykrywanie i lokalizowanie błędów może niekiedy być stosunkowo trudne. Problemy mogą wynikać zarówno z zagięcia lub przerwania przewodów, jak i awarii kart sieciowych. Najczęściej spotykanym źródłem problemów jest jednak nadmierna liczba kolizji, wynikająca z rozbudowy sieci.

Wskaźniki liczby kolizji

Utrzymanie właściwie działającej sieci wymaga zapewnienia normalnego funkcjonowania wszystkich jej składników fizycznych i optymalnego poziomu wydajności. Nie zwalnia Cię to jednak z obowiązku monitorowania swojej sieci, które pozwala Ci upewnić się, że pozostałe czynniki nie ograniczają rzeczywistej ilości przesyłanych danych.

Chociaż w tradycyjnych sieciach Ethernet kolizje są zjawiskiem naturalnym (są wręcz zdarzeniami oczekiwanymi), zawsze istnieje możliwość wystąpienia nadmiernej liczby kolizji, które powodują zauważalny dla końcowych użytkowników spadek wydajności.

Kolizje i obciążenie sieci

Kiedy jakieś urządzenie zacznie generować kolizje stanowiące 1% łącznego obciążenia sieci, może to oznaczać pewien problem. Jest to jeden ze wskaźników, o którym warto pamiętać podczas monitorowania obciążenia sieci lokalnej. Teoretycznie możemy oczekiwać,

że sieć przesyłająca w ciągu sekundy 10 milionów bitów umożliwia ciągłe przesyłanie właśnie takiej ilości danych. Tak jednak nie jest — w większości sieci Ethernet rzeczywiste obciążenie nie powodujące znacznego spadku wydajności wynosi około 40%. Przekroczenie tego wskaźnika nieuchronnie prowadzi do pojawienia się nadmiernej liczby kolizji.

Pamiętaj, że ten podrozdział jest poświęcony kolizjom, które występują wyłącznie w sieciach wykorzystujących współdzielony nośnik sieciowy. Jeśli używasz przełączników (pracujących w pełnym dupleksie), kolizje w Twojej sieci nie wystąpią. Jeśli stosujesz koncentratory, najprostszym rozwiązaniem zwiększającym przepustowość sieci jest zastąpienie koncentratorów przełącznikami.

Jeśli Twoja sieć spełnia założenia zastosowanej topologii oraz jej obciążenie jest na niskim poziomie, nadmierna liczba kolizji może wynikać z niewłaściwie działającej karty sieciowej, która nie nasłuchuje sieci przed podjęciem próby transmisji danych. Więcej informacji na ten temat znajdziesz nieco dalej, w podrozdziale „Wadliwe karty sieciowe".

Wykrywanie kolizji

Najprostszą metodą określenia liczby kolizji w sieci lokalnej jest obserwacja odpowiednich diod koncentratora lub przełącznika. Większość koncentratorów ma diodę zapalającą się w momencie wykrycia kolizji. Jeśli stwierdzisz, że taka dioda świeci się niemal ciągle lub miga bardzo często, powinieneś zbadać to zjawisko dokładniej, aby określić, czy liczba kolizji przekracza dopuszczalny limit. Jeśli tak jest, spróbuj temu zaradzić. Stosując oprogramowanie monitorujące sieć, możesz określić jej obciążenie — jeśli przekracza ono 30 – 40%, czas rozważyć podzielenie Twojej sieci LAN na segmenty (mniejsze domeny kolizyjne).

Analizatory sieci lokalnych i narzędzia monitorujące mogą Ci pomóc w wyznaczeniu liczby występujących w Twojej sieci kolizji. Specjalne pulpity zarządzania, wykorzystujące protokół SNMP i sondy RMON, mogą przydać się do zebrania informacji statystycznych, wartościowych w przypadku lokalizowania segmentów sieci o najwyższych wskaźnikach występowania kolizji. Utrzymywane przez RMON dane historyczne można poddać analizie, która pozwoli wyjaśnić przyczyny takiej, a nie innej wydajności sieci. Jeśli masz zamiar kupić nowy przełącznik lub koncentrator, sprawdź w dokumentacji interesującego Cię urządzenia, czy obsługuje ono sesje zdalnego zarządzania. Tego typu funkcjonalność jest obecnie oferowana nawet przez stosunkowo niedrogie koncentratory. W przypadku małych sieci lokalnych, zawierających tylko kilka przełączników, zastosowanie wbudowanego oprogramowania zarządzającego jest znacznie tańszym rozwiązaniem niż inwestycja w zaawansowane oprogramowanie zarządzania siecią, np. SMS lub HP OpenView.

Typy kolizji

Dobre analizatory sieci oferują mnóstwo informacji statystycznych. W przypadku poszukiwania przez Ciebie przyczyn kolizji oprogramowanie tego typu dostarcza zwykle więcej niż jeden rodzaj danych, który ułatwia znalezienie ich przyczyny.

Kolizje lokalne

Z *kolizją lokalną* (nazywaną także *wczesną kolizją*) mamy do czynienia w sytuacji, gdy kolizja wystąpi w lokalnym segmencie już w trakcie nadawania pierwszych 64 bajtów ramki. Jest to najbardziej popularny rodzaj kolizji, z którym będziesz się spotykał w segmencie sieci — zwykle nie ma ona związku z problemami sprzętowymi. Do wystąpienia tego typu kolizji dochodzi w momencie, gdy dwie różne stacje sieci LAN wykryją brak transmisji w nośniku sieciowym i jednocześnie rozpoczną nadawanie swoich danych. Efektem jest tzw. krótka ramka (ang. *runt*), ponieważ przed wystąpieniem zdarzenia kolizji została pomyślnie wysłana tylko mała część ramki. Specyfikacja standardu Ethernet przewiduje tego typu sytuacje — obie stacje wykorzystują algorytm wyczekiwania, który opóźnia wznowienie transmisji.

Kiedy stwierdzisz, że wskaźnik występowania wczesnych kolizji jest wysoki, sprawdź, czy obciążenie segmentu sieci nie zbliża się do 40% (lub nie przekracza tego progu). Jeśli tak jest, w większości przypadków oznacza to, że sieć jest po prostu przeciążona. Powinieneś wówczas rozważyć zainstalowanie dodatkowego przełącznika, który pozwoli ograniczyć liczbę kolizji. Jeśli jesteś w stanie wskazać konkretny węzeł, w którym dochodzi do największej liczby kolizji lokalnych, może to oznaczać jakiś problem sprzętowy tej stacji. Dokładnie sprawdź wszystkie połączenia sieciowe węzła; jeśli problem nadal będzie się pojawiał, spróbuj wymienić kartę sieciową, by sprawdzić, czy to nie ona powoduje zwiększoną liczbę kolizji.

Późne kolizje

Późne kolizje występują w momencie, gdy dwa urządzenia sieciowe rozpoczynają nadawanie danych w tym samym czasie, ale nie wykrywają zaistniałej kolizji natychmiast. Przyczyną występowania tego typu kolizji są zwykle zbyt długie segmenty sieci. Jeśli czas nadania ramki w sieci jest krótszy od czasu potrzebnego na dostarczenie tej ramki do najbardziej oddalonego węzła, żaden z transmitujących dane węzłów nie zostanie poinformowany o rozpoczęciu transmisji przez inny węzeł w trakcie nadawania pierwszych 64 bajtów ramki (64 bajty to rozmiar najmniejszej ramki).

Dla przykładu przypuśćmy, że stacja robocza A rozpoczyna i kończy transmisję ramki zanim odpowiedni sygnał dotrze do stacji roboczej B, która znajduje się w większej odległości od stacji A niż dopuszcza to specyfikacja używanego standardu. Stacja robocza B — przy założeniu, że nośnik sieciowy jest bezczynny — rozpoczyna nadawanie swojej ramki bezpośrednio przed otrzymaniem sygnału od stacji roboczej A. Ponieważ stacja robocza B znajduje się najbliżej zdarzenia kolizji, oczywiście to ona to zjawisko wykrywa. Ponieważ jednak stacja robocza A zakończyła już transmitowanie ramki, zakończyła także nasłuchiwanie nośnika sieciowego celem wykrycia ewentualnej kolizji. W efekcie stacja robocza A zakłada, że jej ramka została pomyślnie przesłana do adresata i nic „nie wie" o zaistniałej kolizji.

Późne kolizje nie powodują wznawiania transmisji ramki, ponieważ jej nadawca po prostu „nie ma pojęcia" o wystąpieniu kolizji. Odpowiedzialność za wykrycie i obsłużenie błędu (zażądanie ponownej transmisji) spoczywa w takim przypadku na protokole wyższego poziomu.

Jeśli masz do czynienia z wieloma późnymi kolizjami występującymi w danej sieci lokalnej, sprawdź, czy problem nie wynika ze złej topologii. Nie chodzi wyłącznie o przekroczenie dopuszczalnych długości przewodów, ale także o wykorzystywanie zbyt wielu koncentratorów i innych urządzeń. Jeśli nie stwierdzisz niezgodności ze specyfikacją stosowanej technologii, problem wynika prawdopodobnie z awarii sprzętu. Spróbuj zlokalizować wadliwą kartę sieciową lub przewód, analizując dekodowane za pomocą analizatora sieciowego informacje o adresach.

Odstępy próbkowania

Monitorując sieć w poszukiwaniu kolizji, nie wyciągaj pochopnych wniosków na podstawie obserwowanych chwilowych wzrostów częstotliwości ich wystąpień. Sprawdzaj sieć kilka razy w ciągu dnia i spróbuj skojarzyć kolizje z zadaniami realizowanymi w danych momentach przez użytkowników sieci. Pamiętaj, że niekiedy znaczenie może mieć wybór konkretnego dnia, a nie godziny. Przykładowo na końcu miesiąca lub kwartału w systemie są często wykonywane różne funkcje biznesowe — np. przygotowywanie raportów — które generują znaczące dodatkowe obciążenie sieci. Określenie, które z tego typu zadań powinny być wykonywane jako pierwsze, a które w dalszej kolejności, jest zwykle dosyć proste. Niekiedy rozwiązaniem problemu przeciążenia sieci jest opracowanie odpowiedniego harmonogramu.

Dopiero gromadzone przez pewien czas średnie liczby kolizji występujących w ciągu sekundy w połączeniu z poziomem obciążenia sieci pozwalają określić, czy Twoja sieć lokalna jest przeciążona. Zebrane w ten sposób informacje na temat poziomów szczytowych mogą się okazać bardzo przydatne podczas projektowania efektywnego modelu wykorzystania sieci przez użytkowników.

Ograniczanie liczby kolizji

Istnieje kilka przyczyn występowania nadmiernej liczby kolizji. Niektóre z nich są następstwem zignorowania reguł zdefiniowanych dla topologii, wadliwie działającego sprzętu lub przeciążenia segmentu sieci (zbyt dużej liczby użytkowników).

Niepoprawna topologia sieci

Jeśli wykorzystujesz segmenty, których rozmiary przekraczają długości dopuszczane przez specyfikację stosowanej topologii sieciowej, niektóre z urządzeń sieciowych mogą nie mieć możliwości wykrycia transmisji danych przeprowadzanych przez pozostałe węzły. Sprawdź długości swoich przewodów i upewnij się, że spełniają zalecenia standardów. Kiedy stwierdzisz, że konieczna jest rozbudowa Twojej sieci, nigdy nie powinieneś w nieprzemyślany sposób dodawać nowych segmentów, dołączając do sieci nowy repeater, koncentrator czy most. Z tego właśnie powodu istotne znaczenie ma konstruowanie aktualnych map fizycznych topologii sieci, co umożliwi Ci w przyszłości właściwe planowanie rozbudowy sieci.

Pamiętaj, że w przypadku sieci 10BASE-T stacje robocze nie mogą znajdować się dalej niż 100 metrów od koncentratora. Co więcej, reguła 5-4-3 określa, że maksymalna liczba segmentów przewodowych w sieci LAN wynosi pięć, maksymalna liczba repeaterów lub

koncentratorów to cztery, a maksymalna liczba segmentów z podłączonymi węzłami jest ograniczona do trzech. W przypadku sieci zgodnych ze standardami Fast Ethernet i Gigabit Ethernet powinieneś upewnić się, że nie przekraczasz ograniczeń poszczególnych topologii wynikających z parametrów wykorzystywanego fizycznego nośnika sieciowego.

Wadliwe karty sieciowe

Problem nadmiernej liczby kolizji może wynikać ze złego funkcjonowania karty sieciowej, która nie wykrywa transmisji sygnału w nośniku sieciowym i rozpoczyna nadawanie swoich danych niezależnie od dostępności tego nośnika. W rozdziale 7. — „Karty sieciowe" — znajdziesz szczegółową analizę sposobów rozwiązywania problemów dotyczących funkcjonowania kart sieciowych. Najprostszą metodą jest jednak zastąpienie podejrzanego urządzenia innym, co do którego mamy pewność, że działa prawidłowo. Jeśli to nie rozwiąże naszego problemu, warto spróbować wykorzystać inny przewód łączący tę kartę z siecią lub przełożyć tę samą kartę do innego gniazda komputera. Wymieniając kartę lub przewód, musimy oczywiście mieć pewność, że nowy sprzęt działa właściwie. Kolejna taktyka rozwiązywania tego typu problemów polega na wykorzystaniu oprogramowania diagnostycznego, dołączanego do sprzedawanych urządzeń przez producentów kart sieciowych.

Nadawcy generujący największe obciążenie

Liczba urządzeń, które możesz połączyć w jednej domenie rozgłaszania swojej sieci komputerowej, jest ograniczona z powodu spadającej wydajności. Spadek wydajności może spowodować także stosunkowo niewielka liczba wydajnych komputerów, generujących duży ruch w sieci. Pamiętaj, że kiedy rośnie obciążenie sieci, rośnie także liczba kolizji. Kiedy więc stwierdzasz w swojej sieci nadmierną liczbę kolizji, oznacza to zwykle, że obciążenie w danym segmencie zbliżyło się lub przekroczyło poziom 40% — warto wówczas rozważyć podzielenie tej części sieci lokalnej na segmenty za pomocą przełącznika lub podobnego urządzenia. Przełącznik, który może być stosowany do zapewniania pełnodupleksowej komunikacji z wydajnymi serwerami, jest także idealnym rozwiązaniem dla lokalnych segmentów sieci, zawierających zarówno komputery użytkowników, jak i ważne serwery danych (tzw. *top-talkers*).

Błędy w sieci Ethernet

Większości z omawianych poniżej problemów można zaradzić, wprowadzając w sieciach stosunkowo niewielkie modyfikacje. Jeśli nadal korzystasz z koncentratorów, rozważ zastosowanie w ich miejsce nowocześniejszych przełączników. Jeśli decydujesz się na używanie urządzeń korzystających z mechanizmu CSMA/CD, decydujesz się tym samym na kolizje i problemy z nimi związane. Oznacza to, że wiele nowych aplikacji opierających swoje działania na wykorzystaniu szybkich połączeń z wieloma serwerami i innymi zasobami sieciowymi może powodować przeciążenie Twojej sieci. Jakość aplikacji nie ma żadnego znaczenia, jeśli nie jest ona w stanie pobrać na czas potrzebnych danych z powodu wolnego połączenia sieciowego. Zalecanym dzisiaj rozwiązaniem jest wykorzystanie centralnych serwerów zamiast instalowania ogromnych aplikacji lub baz danych na komputerach użytkowników.

Jeśli jednak nadal używasz koncentratorów i starszego sprzętu, w którym możliwe jest występowanie kolizji, treść tego podrozdziału może Ci pomóc w rozwiązywaniu niektórych problemów, z którymi możesz się spotkać.

Wykrywanie prostych błędów

Kiedy przesyłasz w swojej sieci setki tysięcy bitów za pomocą miedzianego przewodu — z nadzieją, że dotrą do miejsca przeznaczenia niezmienione i we właściwej kolejności — mnóstwo spraw może się nie udać. Im większe szybkości przesyłania danych w proponowanych nowych technologiach, tym ważniejsze jest wykrywanie pojawiających się błędów.

Najprostszą metodą wykrywania błędów jest tzw. kontrola parzystości (ang. *parity check*). Przykładem tej metody jest przesyłanie znaków za pomocą 7-bitowego zbioru znaków ASCII z dodatkowym ósmym bitem. Jeśli dany protokół sieciowy wykorzystuje mechanizm *kontroli parzystości*, ósmemu bitowi przypisuje się wartość jeden lub zero, w zależności od tego, czy liczba wartości „1" w pozostałych siedmiu bitach jest odpowiednio parzysta czy nieparzysta. Jeśli stosowany jest mechanizm *kontroli nieparzystości*, wartość „1" w ósmym bicie oznacza nieparzystą liczbę wartości „1" w pozostałych siedmiu bitach. Stacja odbiorcza może w prosty sposób sama obliczyć wartość bitu parzystości, analizując pierwsze siedem bitów, a następnie porównać wynik z otrzymaną wartością. Ten schemat wykrywania błędów może się jednak łatwo załamać, jeśli podczas transmisji uszkodzeniu uległ więcej niż jeden bit.

Taki sposób kontrolowania otrzymywanych danych może być wykorzystywany wyłącznie na poziomie pojedynczych bajtów, nie jest więc przydatny podczas weryfikacji poprawności ramki danych mającej długość 1 518 bajtów. W ramkach sieci Ethernet wykorzystuje się do wykrywania ewentualnych niespójności 4-bajtowe sumy kontrolne CRC ramki (ang. *Frame Check Sequence — FCS*). Protokoły wyższego poziomu wykorzystują do sprawdzania poprawnej kolejności i spójności otrzymywanych pakietów jeszcze inne metody. Poza błędami związanymi z uszkodzeniami ramek podczas ich przesyłania, które można wykryć za pomocą FCS, w sieciach Ethernet występują także inne popularne rodzaje błędów. W tym podrozdziale krótko omówimy najczęściej pojawiające się błędy, a także przyczyny ich występowania.

Zła wartość FCS lub niedopasowana ramka

Najbardziej oczywistym przedmiotem weryfikacji jest sekwencja sprawdzania ramki (FCS). Warstwa MAC oblicza, na podstawie zawartości ramki, wartość sumy kontrolnej CRC, którą umieszcza w polu FCS. Stacja docelowa może wykonać te same obliczenia i — porównując otrzymany wynik z wartością umieszczoną w ramce przez stację nadawczą — określić, czy ramka została uszkodzona podczas przesyłania.

Istnieje możliwość, że wartość FCS zostanie błędnie obliczona przez stację nadawczą z powodu problemów sprzętowych związanych z realizacją tej funkcji w warstwie MAC. Nie można także wykluczyć sytuacji, w której problem spowodowała karta sieciowa odpowiedzialna za transmisję ramki, czego efektem mogło być niewłaściwe przekazanie bitów do nośnika sieciowego. Jak w przypadku większości błędów, problem może także wynikać z zakłóceń, jakim podlegają miedziane przewody łączące naszą sieć komputerową.

Kiedy monitorowany przez Ciebie poziom występowania błędnych wartości FCS przekroczy 2 – 3% łącznego obciążenia pasma sieci komputerowej, powinieneś rozpocząć poszukiwanie urządzenia, które generuje tego typu błędy. Zlokalizowanie adresu źródłowego wadliwego urządzenia (celem podjęcia odpowiednich kroków zaradczych) jest zwykle możliwe przy wykorzystaniu analizatorów sieciowych.

Aby stwierdzić z całą pewnością, czy podejrzane urządzenie faktycznie jest źródłem błędów, wyłącz je i kontynuuj monitorowanie sieci. Jeśli problem będzie się powtarzał, ale analizator będzie wskazywał adres innego urządzenia generującego błędy, zaistniała sytuacja może wynikać z niewłaściwie działającego okablowania sieciowego. Jeśli natomiast po odłączeniu tego urządzenia błędy przestały występować, możesz przystąpić do dalszego, bardziej szczegółowego lokalizowania ich przyczyn. Oto elementy, które powinieneś wówczas sprawdzić:

- **Uszkodzone złącze** — sprawdź złącze przymocowane do przewodu sieciowego wykorzystywanego przez kartę sieciową danej stacji roboczej.
- **Uszkodzony port** — jeśli stacja robocza jest podłączona do koncentratora lub przełącznika, być może źródłem błędu jest port tego urządzenia. Także w tym przypadku upewnij się, że złącze na tym końcu kabla jest prawidłowo zamontowane.
- **Uszkodzony przewód** — zawsze istnieje możliwość, że wykorzystywany przewód sieciowy został uszkodzony lub rozłączony. Jeśli Twoje próby nie przynoszą rozwiązania tego problemu, wykorzystaj specjalne narzędzia diagnostyczne, np. stosujące metodę reflektometrii w domenie czasu, które pozwalają zlokalizować problemy w okablowaniu sieciowym.
- **Niesprawna karta sieciowa** — na końcu spróbuj wymienić kartę sieciową w stacji roboczej, by sprawdzić, czy takie posunięcie nie rozwiąże zauważonego problemu.

Ponieważ ramka składa się z bajtów (jednostek złożonych z 8 bitów), po dotarciu do węzła docelowego jej rozmiar powinien być zawsze podzielny przez osiem. Jeśli tak nie jest, oczywiste jest, że musiał wystąpić błąd. Ten typ błędu nosi nazwę niedopasowanej ramki (ang. *misaligned frame*) i występuje zwykle w połączeniu z błędem niewłaściwej wartości FCS. Najczęstszym powodem tego typu błędów są zakłócenia elektryczne w okablowaniu lub kolizja. Inną przyczyną może być niewłaściwa topologia sieci, w której wykorzystuje się więcej niż dwa wieloportowe repeatery połączone kaskadowo.

Możesz rozwiązywać tego rodzaju problemy, stosując tę samą metodę, co w przypadku błędów niepoprawnej wartości FCS. Jeśli problem wynika z niewłaściwej topologii, jego rozwiązanie jest oczywiście zupełnie inne.

Krótkie ramki

Rozmiar tzw. krótkiej ramki (ang. *runt*) w sieci Ethernet jest mniejszy niż 64 bajty, czyli mniejszy od rozmiaru najmniejszej dopuszczalnej ramki. Pamiętaj, że transmitujące pakiet urządzenie sieciowe nie może zakończyć nadawania w czasie krótszym niż wynosi czas propagacji tego pakietu w lokalnej domenie rozgłaszania. W przeciwnym przypadku

urządzenie to nie miałoby możliwości wykrycia ewentualnej kolizji. Maksymalny czas propagacji w segmentach sieci Ethernet wynosi 51,2 mikrosekund, czyli tyle, ile potrzeba do przesłania około 64 bajtów. Minimalny rozmiar ramki nie uwzględnia jej preambuły.

Istnieje wiele możliwych przyczyn przesyłania krótkich ramek w sieciach Ethernet. Niektóre z nich mają swoje źródło w wystąpieniu następujących sytuacji:

- kolizji,
- wadliwie działających kart sieciowych,
- błędnych topologii.

Jeśli krótka ramka ma poprawną wartość FCS, co oznacza, że jest wewnętrznie spójna, problem prawdopodobnie wynika z niewłaściwego funkcjonowania karty sieciowej, która wygenerowała tę ramkę. Jeśli natomiast wartość FCS nie jest zgodna z zawartością ramki, prawdopodobnym źródłem problemu jest kolizja lub błędna topologia.

Kolizje są normalnymi zdarzeniami w sieciach Ethernet. Niekiedy jednak skutkiem ubocznym ich występowania jest przesyłanie sygnałów interpretowanych jako krótkie ramki. Jeśli tego typu błędy pojawiają się w Twojej sieci stosunkowo często, koniecznie sprawdź wskaźniki obciążenia danego segmentu sieci. Jeśli odkryte maksymalne obciążenie jest wysokie, a średnie obciążenie jest na satysfakcjonującym poziomie, spróbuj zmienić harmonogram pracy użytkowników w taki sposób, by zadania szczególnie wymagające wykorzystania sieci były realizowane w czasie, gdy sieć jest mniej obciążona. Innym rozwiązaniem jest umieszczenie wydajnych stacji roboczych generujących duże obciążenie sieci w osobnym segmencie LAN, co zwalnia tym samym pasmo dostępne dla zwykłych stacji roboczych w dotychczasowym segmencie sieci. Rozwiązaniem problemu będzie wówczas połączenie tych segmentów za pomocą przełącznika lub routera.

Jeśli obciążenie sieci jest niskie, problem będzie być może wymagał głębszej analizy, polegającej na zidentyfikowaniu stacji roboczej lub urządzenia sieciowego generującego krótkie ramki (będzie wówczas możliwe przetestowanie podejrzanego węzła celem sprawdzenia, czy rzeczywiście działa nieprawidłowo i jest źródłem rozważanego problemu). Może to być dosyć trudne, ponieważ znaczna część błędów tego typu polega na przesyłaniu ramek tak krótkich, że niemożliwe jest określenie adresu źródłowego.

Generowanie krótkich ramek może także wynikać ze zignorowania reguł określonych w standardzie Ethernet dla stosowanej topologii. Typowym błędem jest zastosowanie więcej niż czterech repeaterów w jednej domenie kolizyjnej, co może prowadzić do częstego pojawiania się w nośniku sieciowym krótkich ramek.

Olbrzymie i niezrozumiałe ramki

Karty sieciowe generują niekiedy ramki, których rozmiar przekracza dopuszczalne maksimum. Tego typu zdarzenia są oczywiście odwrotnością zjawiska krótkich ramek i noszą nazwę błędów olbrzymich ramek (ang. *giant frame error*). Zgodnie z regułami rządzącymi komunikacją w sieciach Ethernet, maksymalny rozmiar ramki wynosi 1 518 bajtów, z wyłączeniem bitów preambuły. Potencjalnych powodów wystąpienia w nośniku sieciowym zbyt dużych ramek jest kilka:

- Wadliwe urządzenie sieciowe stale transmituje dane.
- Bity oznaczające długość ramki zostały uszkodzone podczas przesyłania i wskazują na większy rozmiar ramki niż w rzeczywistości.
- W przewodzie zaistniały zakłócenia. Rozmaite zakłócenia w niepewnym przewodzie mogą być interpretowane jako część ramki, nie jest to jednak najczęstsza przyczyna występowania błędu olbrzymich ramek.

Zlokalizowanie urządzenia generującego ramki o zbyt dużych rozmiarach może być proste, jeśli używany przez Ciebie analizator sieci LAN jest w stanie wykryć ich adres źródłowy. Możesz odłączyć zasilanie lub przewód sieciowy od podejrzanego węzła, by określić, czy jest on rzeczywistym źródłem problemu. W niektórych przypadkach nie będziesz jednak w stanie wykryć adresu wadliwego urządzenia, jeśli np. działająca nieprawidłowo karta sieciowa rozsyła w sieci z pewną częstotliwością nic nie znaczące sygnały. W takim przypadku powinieneś kolejno odłączać każdą stację roboczą danego segmentu sieci, aby sprawdzić, czy usunięcie tych węzłów nie eliminuje omawianego problemu.

Chociaż określenie *jabber* (niezrozumiała ramka) dotyczy niekiedy ramek przekraczających dopuszczalny rozmiar, w ogólności odnosi się do wszystkich sytuacji, w których urządzenie sieciowe nie działa zgodnie z regułami i transmituje do nośnika sieciowego nieprawidłowe sygnały. Wadliwe urządzenie sieciowe może zarówno rozsyłać zbyt duże ramki, jak i bez przerwy nadawać niezrozumiały sygnał.

Ten rodzaj błędu może unieruchomić nawet cały segment sieci, ponieważ karta sieciowa bez przerwy przesyłająca swoje sygnały uniemożliwia uzyskanie dostępu do współdzielonego nośnika sieciowego wszystkim innym stacjom. Stacje muszą przed rozpoczęciem transmisji sprawdzać, czy nośnik nie jest zajęty, co oznacza, że normalnie działające węzły będą po prostu czekały, aż wadliwa karta sieciowa zakończy nadawanie i zwolni nośnik sieciowy.

Błędy wielokrotne

Liczba różnych typów wykrywanych błędów może się różnić, w zależności od wykorzystywanego narzędzia monitorowania sieci. Przykładowo błędy niedopasowania ramek występują zwykle w parze z niewłaściwymi wartościami pola FCS. Niektóre analizatory zarejestrują oba błędy jako pojedyncze zdarzenie, natomiast inne zarejestrują tylko błąd należący do jednego z dwóch typów.

Sprawdź w dokumentacji swojego oprogramowania, by dowiedzieć się, jak postępować w tego typu przypadkach.

Fala rozgłaszań

Ze zjawiskiem *fali rozgłaszań* mamy zwykle do czynienia w momencie, gdy urządzenia sieciowe generują obciążenie sieci powodujące dalsze generowanie tego obciążenia. Chociaż dodatkowe obciążenie może teoretycznie wynikać z fizycznych problemów urządzeń sieciowych, zwykle jest powodowane przez protokoły wyższego poziomu. Co więcej, problem z wykryciem źródła tego typu zachowań polega na tym, że zwykle w momencie

ich wystąpienia uzyskanie dostępu do sieci jest niemożliwe. „Burze rozgłaszań" mogą znacząco ograniczyć szybkość przesyłania danych w sieci, a nawet całkowicie wstrzymać jej pracę.

Monitorując operacje rozgłaszania w swojej sieci, będziesz zwykle widział wskaźnik nie przekraczający około 100 rozgłaszanych ramek na sekundę. Jeśli wartość tego wskaźnika na stałe przekroczy 100 ramek na sekundę, może to oznaczać wadliwe działanie karty sieciowej lub konieczność podzielenia domeny kolizyjnej na mniejsze segmenty. Możesz to wykonać za pomocą routerów, ponieważ tego typu urządzenia — jeśli nie zostały specjalnie skonfigurowane — nie przekazują dalej ramek rozgłaszania. Także wiele dostępnych mostów można skonfigurować w taki sposób, by wykrywały nadmierną liczbę rozgłaszań i wstrzymywały przesyłanie rozgłaszanych ramek do momentu ustania fali.

Monitorowanie wystąpień błędów

Istnieje wiele narzędzi, które możesz wykorzystać do monitorowania swojej sieci celem wykrywania błędów. Przykładowo analizator sieciowy *Network Sniffer* firmy Network General wyświetla informacje o ramkach zwierających rozmaite błędy (włącznie ze słabymi ramkami, błędami CRC czy niewłaściwymi rozmiarami). Niektóre programowe narzędzia, np. *Monitor sieci*, dołączany m.in. do systemu Windows NT Server firmy Microsoft, umożliwiają przeglądanie statystyk na temat zgubionych ramek, błędów CRC oraz rozgłaszań. Także znacznie prostsze i mniejsze narzędzia oferują często funkcjonalność umożliwiającą wykrywanie wystąpień tego typu błędów.

W przypadku sieci wymagających centralnego zarządzania i kontroli do monitorowania sieci celem wykrywania błędów i automatycznego powiadamiania o sytuacjach alarmowych można wykorzystać aplikacje protokołu SNMP i standard RMON. Gromadzenie pojawiających się przez jakiś czas informacji o błędach ułatwia późniejszą analizę sytuacji i rozwiązywanie problemów.

►► Więcej informacji na temat protokołu SNMP, RMON oraz narzędzi monitorowania sieci znajdziesz w rozdziale 52. („Strategie rozwiązywania problemów w sieciach") oraz w rozdziale 53. („Narzędzia do testowania i analizowania sieci"). Bardziej szczegółowe informacje na temat sposobów znajdowania problemów w sieciach Ethernet przedstawiłem w rozdziałach poświęconych kartom sieciowym, przewodom, koncentratorom, przełącznikom i routerom.

Do wielu urządzeń działających w internecie (np. routerów lub inteligentnych koncentratorów) jest dołączane specjalne oprogramowanie zarządzające, którego działanie można ograniczyć do wyświetlania statystyk o błędach, jeśli oczywiście nie korzystamy z bardziej zaawansowanych funkcji (np. konsoli zarządzania). Regularne sprawdzanie informacji statystycznych i utrzymywanie odpowiedniego pliku dziennika może nam bardzo pomóc. Jeśli na bieżąco śledzisz wystąpienia błędów w swojej sieci, możesz przystępować do rozwiązywania ewentualnych problemów znacznie szybciej, ponieważ jesteś w stanie określić, czy aktualna sytuacja ma związek z problemami rozwiązanymi wcześniej.