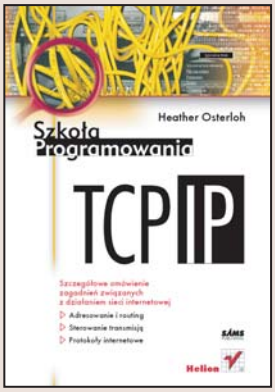
TCP/IP. Szkoła programowania



Autor: Heather Osterloh
Tłumaczenie: Maciej Gołębiewski, Grzegorz Kowalski
ISBN: 83-246-0293-3
Tytuł oryginału: TCP/IP Primer Plus
Format: B5, stron: 544

Szczegółowe omówienie zagadnień związanych z działaniem sieci internetowej

- Adresowanie i routing
- Sterowanie transmisją
- Protokoły internetowe

TCP/IP to podstawa działania sieci komputerowych. Protokoły wchodzące w skład zestawu TCP/IP odpowiadają za poprawne funkcjonowanie wszystkiego, z czego korzystamy we współczesnych sieciach, szczególnie w internecie, czyli stron WWW, poczty elektronicznej, przesyłania plików, adresów IP i wielu innych elementów. Znajomość zasad stosowania i konfigurowania tych protokołów w różnych systemach operacyjnych jest jedną z kluczowych umiejętności administratora sieci spotykającego się w swojej pracy z problemami, których rozwiązanie wymaga takiej wiedzy.

„TCP/IP. Szkoła programowania" to podręcznik gruntownie opisujący zagadnienia związane z TCP/IP. Czytając go, poznasz podstawy modeli OSI i DoD, ze szczególnym uwzględnieniem warstw łącza danych i fizycznej. Znajdziesz w nim bardzo dokładne omówienie różnych protokołów umieszczonych w kolejnych warstwach modelu OSI. Każde zagadnienie przedstawione jest w sposób praktyczny, bez zbędnego wgłębiania się w teorię, a zatem wiedzę zdobytą dzięki tej książce z łatwością wykorzystasz w swojej pracy.

- Warstwy modelu OSI
- Adresowanie IP
- Protokoły routingu
- Protokoły warstwy transportowej
- Przesyłanie plików
- Protokół HTTP
- Poczta elektroniczna

Ta książka powinna znaleźć się w biblioteczce każdego administratora sieci

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

SPIS TREŚCI

O autorce ... 15

wstęp ... 17

Rozdział 1. Omówienie modeli i standardów branżowych ... 19
- Omówienie modelu referencyjnego OSI ... 19
- Omówienie modelu Departamentu Obrony ... 22
- Zalety warstwowej konstrukcji OSI ... 22
  - Jasne sprecyzowanie funkcji warstw ... 23
  - Dobrze określony schemat dla dostawców ... 23
  - Mniejsza złożoność pracy w sieci ... 23
  - Popieranie specjalizacji ... 24
- Opis ogólny warstw OSI ... 24
  - Warstwa aplikacji ... 26
  - Warstwa prezentacji ... 27
  - Warstwa sesji ... 27
  - Warstwa transportowa ... 28
  - Warstwa sieciowa ... 29
  - Warstwa łącza danych ... 30
  - Warstwa fizyczna ... 31
- Architektura i topologie łącza danych ... 31
  - Ethernet i IEEE 802.3 ... 31
  - Powolny Ethernet ... 38
  - Szybki Ethernet ... 39
  - Gigabitowy Ethernet ... 40
  - Token-Ring i IEEE 802.5 ... 40
  - FDDI i ANSI X3T9.5 ... 42
- Technologie sieci rozległych (WAN) ... 43
  - Protokoły hermetyzacji WAN ... 46
- Dokumenty RFC ... 47
- Internet kontra intranet ... 48
- Grupy odpowiedzialne za technologię Internetu ... 49
- Podsumowanie ... 49
- Pytania sprawdzające ... 49

Rozdział 2. Adresowanie IP ... 51
Istota konwersji dwójkowo-dziesiętnej ... 51
Adresowanie IP ... 52
Klasy adresów ... 53
Maski sieci i podsieci ... 58
Podział na podsieci. Przykłady ... 61
Tłumaczenie adresów sieciowych (NAT) ... 73
Statyczne ... 74
Dynamiczne ... 74
Podsumowanie ... 75
Pytania sprawdzające ... 76

Rozdział 3. Protokoły internetowe i warstwa sieciowa ... 77
Protokół IP ... 77
Nagłówek IP ... 79
Protokół ICMP ... 90
Format nagłówków i komunikatów ICMP ... 91
Kod komunikatów ICMP a ich rodzaje ... 92
Suma kontrolna ... 93
Typ komunikatu ICMP ... 94
Ping: żądanie i odpowiedź echa — typy 8 i 0 ... 94
Odbiorca nieosiągalny — typ 3 ... 96
Tłumienie nadawcy — typ 4 ... 100
Przekierowanie — typ 5 ... 100
Ogłaszanie i poszukiwanie routera — typy 9 i 10 ... 101
Przekroczony czas — typ 11 ... 101
Problem z parametrami — typ 12 ... 103
Żądanie i odpowiedź znacznika czasu — typy 13 i 14 ... 103
Żądanie i odpowiedź informacji — typy 15 i 16 ... 103
Żądanie i odpowiedź maski adresu — typy 17 i 18 ... 104
Podsumowanie ... 104
Pytania sprawdzające ... 104

Rozdział 4. Zamiana adresów ... 105
Protokół ARP ... 107
Działanie protokołu ARP ... 107
Mechanizmy bufora ARP ... 110
Proxy ARP ... 111
Działanie proxy ARP ... 111
Nagłówek ARP ... 113
Typ sprzętu (Hardware Type) ... 114
Typ protokołu (Protocol Type) ... 114
Długość adresu sprzętowego (Hardware address Length, HLen) ... 115
Długość adresu protokolarnego (Protocol address Length, PLen) ... 115
Kod operacji (Operation code, Opcode) ... 115
HA nadawcy (Sender's HA) ... 115

PA nadawcy (Sender's PA) ... 115
HA odbiorcy (Target HA) ... 115
PA odbiorcy (Target PA) ... 116
Protokół RARP ... 116
Działanie protokołu RARP ... 116
Działanie ARP a działanie RARP ... 117
Wady protokołu RARP ... 119
Nagłówek RARP ... 119
Typ sprzętu ... 119
Typ protokołu ... 119
Długość adresu sprzętowego (HLen) ... 120
Długość adresu protokolarnego (PLen) ... 120
Kod operacji (Opcode) ... 120
HA nadawcy ... 120
PA nadawcy ... 120
HA odbiorcy ... 121
PA odbiorcy ... 121
Protokół BOOTP ... 121
Nagłówek BOOTP ... 122
Żądanie i odpowiedź BOOTP ... 126
Protokół DHCP ... 127
Przydzielanie informacji konfiguracyjnych ... 128
Komunikaty DHCP ... 128
Wymiany komunikatów DHCP ... 129
Nagłówek DHCP ... 136
Podsumowanie ... 139
Pytania sprawdzające ... 140

Rozdział 5. Routing IP ... 141
Podstawy routingu IP ... 141
Interfejs podłączony bezpośrednio ... 142
Routing statyczny ... 142
Routing domyślny ... 143
Routing dynamiczny ... 144
Protokoły routingu i najlepsza ścieżka ... 145
Protokoły wektora odległości ... 145
Protokoły stanu łącza ... 148
Protokoły hybrydowe ... 149
Podsumowanie ... 151
Pytania sprawdzające ... 151

Rozdział 6. Protokoły routingu ... 153
Wprowadzenie ... 153
Protokół RIP ... 154
RIP w.1 ... 155
Nagłówek RIP w.1 ... 158

Wady protokołu RIP w.1 ... 160
Czasomierze RIP ... 163
Protokół RIP a obwody tworzone na żądanie ... 164
RIP w.2 ... 167
Protokół OSPF ... 169
Charakterystyka OSPF ... 170
Bazy danych OSPF ... 171
Działanie OSPF ... 172
Nagłówek LSA ... 176
Stany routera OSPF ... 178
Typy routerów OSPF ... 183
Działanie OSPF w różnych architekturach łącza danych ... 184
Typy obszarów ... 187
Standardowe pola pakietu OSPF ... 190
Nagłówki dodatkowe ... 192
Protokół IGRP ... 199
Sieci IGRP ... 200
Protokół EIGRP ... 202
Działanie EIGRP ... 202
Typy pakietów EIGRP ... 205
Protokół BGP ... 205
Protokoły IGP versus protokoły EGP ... 206
Routery BGP ... 207
Działanie BGP ... 209
Nagłówek BGP ... 209
Atrybuty ścieżki ... 214
BGP w.3 a BGP w.4 ... 217
Podsumowanie ... 217
Pytania sprawdzające ... 218

Rozdział 7. Warstwa transportowa ... 221
Protokoły warstwy transportowej ... 221
Protokoły połączeniowe ... 223
Protokoły bezpołączeniowe ... 225
Protokoły bezpołączeniowe a protokoły połączeniowe ... 225
Porty i gniazda ... 226
Podsumowanie ... 228
Pytania sprawdzające ... 229

Rozdział 8. Protokół sterowania transmisją (TCP) ... 231
Wprowadzenie ... 231
Nagłówek TCP ... 232
Port źródłowy (Source Port) ... 233
Port docelowy (Destination Port) ... 233
Numer kolejny (Sequence Number) ... 234

Numer potwierdzenia (Acknowledgement Number) ... 234
Przesunięcie danych (Data Offset) ... 236
Zarezerwowane (Reserved) ... 236
Flagi (Flags) ... 236
Okno (Window) ... 237
Suma kontrolna (Checksum) ... 237
Wskaźnik pilności (Urgent Pointer) ... 237
Opcje (Options) ... 238
Podstawowe zasady działania TCP ... 238
Ustanawianie i zrywanie połączenia ... 239
Zwielokrotnianie ... 240
Przesył danych ... 241
Sterowanie przepływem ... 241
Niezawodność ... 242
Priorytety i zabezpieczenia ... 242
Cechy charakterystyczne połączeniowości ... 244
Ustanawianie sesji ... 244
Zrywanie sesji ... 249
Sekwencjonowanie i potwierdzenia ... 250
Komunikaty utrzymywania przy życiu ... 255
Sterowanie przepływem ... 255
Porty TCP ... 258
Podsumowanie ... 259
Pytania sprawdzające ... 259

Rozdział 9. Protokół datagramów użytkownika (UDP) ... 261
Działanie UDP ... 262
Aplikacje UDP ... 263
Porty UDP ... 263
Nagłówek UDP ... 264
Port źródłowy (Source Port) ... 265
Port docelowy (Destination Port) ... 265
Długość (Length) ... 265
Suma kontrolna (Checksum) ... 266
Podsumowanie ... 267
Pytania sprawdzające ... 267

Rozdział 10. Protokoły górnej warstwy ... 269
Wprowadzenie do protokołów górnej warstwy ... 269
Warstwa aplikacji ... 270
World Wide Web (sieć WWW) i HTTP (protokół przesyłania hipertekstu) ... 271
Poczta elektroniczna oraz SMTP
(prosty protokół przesyłania poczty elektronicznej) ... 272
Telnet (sieć telekomunikacyjna) ... 272
Przesyłanie plików ... 273

Warstwa prezentacji ... 273
Warstwa sesji ... 274
NetBIOS (Network Basic Input Output System) — interfejs programowy aplikacji ... 275
Sieciowy system plików NFS (Network File System) oraz protokoły ONC ... 275
Podsumowanie ... 275
Pytania sprawdzające ... 276

Rozdział 11. Telnet ... 277
Komunikacja zewnętrzna ... 277
Usługi podstawowe ... 279
Wirtualny terminal sieciowy ... 280
NVT ASCII (American Standard Code for Information Interchange — standardowy amerykański kod wymiany informacji) ... 280
Polecenia protokołu Telnet ... 281
Negocjacja opcji ... 283
Opcje protokołu Telnet ... 284
Negocjacje subopcji ... 287
Podsumowanie ... 288
Pytania sprawdzające ... 288

Rozdział 12. Protokół przesyłu plików (FTP) ... 289
Wprowadzenie do przesyłania plików ... 289
Sesja FTP ... 291
Reprezentacja danych ... 294
Typy danych FTP ... 295
Kontrola formatu ... 296
Struktury danych FTP ... 297
Tryby transmisji FTP ... 298
Polecenia FTP ... 298
Odpowiedzi FTP ... 301
Działanie FTP oraz przykłady ... 302
Anonimowy FTP ... 303
Podsumowanie ... 304
Pytania sprawdzające ... 305

Rozdział 13. Prosty Protokół Przesyłania Poczty Elektronicznej (SMTP) ... 307
Model nazewniczy X.400 ... 310
Agenci Transferu Wiadomości (MTA) ... 311
Format SMTP ... 311
Polecenia SMTP ... 313
Odpowiedzi SMTP ... 314
MIME ... 316
Podsumowanie ... 317
Pytania sprawdzające ... 317

Rozdział 14. Przekształcanie nazw ... 319
Dlaczego potrzebujemy przekształcenia nazw? ... 319
Przestrzeń nazw ... 320
Delegacja zarządu domenami DNS ... 322
Nazwy domen internetowych ... 325
Zapytania i mapowanie ... 326
Buforowanie (caching) ... 326
Format wiadomości serwera domen ... 327
Identyfikator (ID) ... 327
QR ... 327
Opcode ... 328
Flagi ... 328
Rcode ... 329
Nagłówki pytań i odpowiedzi ... 330
Typy nazw domen ... 330
Przykłady DNS ... 331
NetBIOS ... 334
NetBIOS a TCP/IP ... 335
Typy węzłów (node types) ... 337
B-node ... 337
P-node ... 337
M-node ... 338
H-node ... 338
WINS (Windows Internet Naming Server — internetowy serwer nazewniczy Windows) ... 338
Agent proxy WINS ... 339
Przykłady działania NetBIOS ... 339
Podsumowanie ... 340
Pytania sprawdzające ... 341

Rozdział 15. Protokół przesyłania hipertekstu (HTTP) ... 343
HTTP oraz World Wide Web ... 343
Cechy HTTP ... 344
Komponenty HTTP ... 345
Widoczni i niewidoczni agenci proxy ... 345
Sesje HTTP ... 346
Format wiadomości HTTP ... 348
Wiersz startowy ... 348
Nagłówek ogólny ... 349
Kontrola bufora ... 349
Połączenie ... 349
Data ... 349
Pragma ... 350
Stopka (trailer) ... 350

Kodowanie transferu ... 350
Aktualizacja ... 350
Via ... 350
Ostrzeżenie ... 351
Nagłówki wiadomości (zapytania, odpowiedzi lub obiektu) ... 351
Nagłówek zapytania ... 351
Nagłówek odpowiedzi ... 352
Obiekt ... 352
Pusty wiersz (CRLF) ... 352
Treść wiadomości ... 352
Wiadomości odpowiedzi, stan i kody błędów HTTP ... 353
Wiadomości o błędzie HTTP ... 355
Podsumowanie ... 355
Pytania sprawdzające ... 356

Rozdział 16. Trywialny protokół przesyłania plików (TFTP) ... 357
Wprowadzenie do protokołów przesyłania plików ... 357
Typy pakietów TFTP ... 358
Pakiety RRQ i WRQ ... 360
Pakiety danych ... 360
Pakiet ACK ... 360
Pakiety błędu ... 361
Działanie TFTP ... 362
Rozszerzenia TFTP ... 364
Pakiet OACK ... 365
Podsumowanie ... 365
Pytania sprawdzające ... 366

Rozdział 17. Prosty protokół zarządzania siecią (SNMP) ... 367
Wprowadzenie do zarządzania siecią ... 367
SNMP ... 369
Menadżer SNMP ... 369
Agenci SNMP ... 370
Widoki MIB ... 370
Proxy ... 370
Format wiadomości SNMP ... 371
Wersja ... 371
Nazwa społeczności ... 372
Jednostki danych protokołu (PDU) ... 373
Pułapka PDU ... 373
Podsumowanie ... 374
Pytania sprawdzające ... 375

Rozdział 18. Protokoły otwartego przetwarzania sieciowego (ONCP) ... 377
Wprowadzenie do protokołów otwartego przetwarzania sieciowego ... 377
Cechy NFS ... 378
Działanie NFS ... 380
Klient NFS ... 381
Serwer NFS ... 383
Składniki i działanie automountera ... 383
Auto-polecenie ... 384
XDR ... 384
RPC ... 385
Wiadomość wywołująca ... 386
ID transakcji ... 387
Typ ... 387
Wersja ... 387
Program ... 387
Procedura ... 389
Rodzaj uwierzytelniania ... 390
Rozmiar uwierzytelniania w bajtach ... 390
Dane uwierzytelniania ... 390
Weryfikacja uwierzytelniania ... 390
Odpowiedź ... 391
Stan ... 391
Stan akceptacji ... 391
Przykłady działania NFS ... 391
Podsumowanie ... 393
Pytania sprawdzające ... 393
Dodatek A Dokumenty RFC wg rozdziałów ... 395
Dodatek B Skróty i akronimy ... 467
Dodatek C Numery portów TCP/UDP ... 477
Dodatek D Słowniczek ... 479
Dodatek E Odpowiedzi do pytań sprawdzających ... 521
Skorowidz ... 539

OMÓWIENIE MODELI I STANDARDÓW BRANŻOWYCH

Przegląd treści rozdziału:

- Model OSI
- Model DoD
- Architektura siedmiowarstwowa
- Architektura i topologie sieci
- Technologie sieci rozległych (WAN)
- Dokumenty RFC

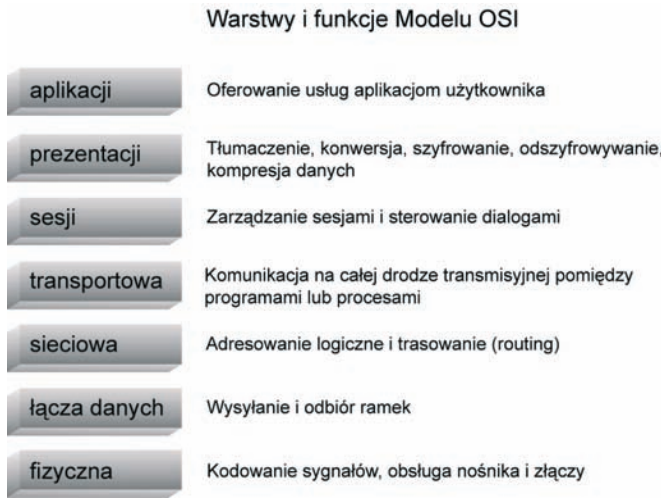
Omówienie modelu referencyjnego OSI

Na początku powstawania sieci istniały tylko systemy i protokoły wewnątrzfirmowe. Systemy operacyjne projektowane przez duże firmy, np. SNA firmy *IBM* (International Business Machines) czy DECNet firmy *DEC* (Digital Equipment Corporation), zawierały własne pakiety protokołów. Systemy te i odpowiadające im protokoły przede wszystkim umożliwiały komunikację sieciową pomiędzy komputerami klas mini- i mainframe. Firmy nie zapewniały jednak obsługi wzajemnych połączeń ani nie umożliwiały komunikacji z systemami zewnętrznymi. Kiedy IBM projektował SNA, a DEC — DECNet, nikt nie przewidywał obecnego rozpowszechnienia się mieszanych środowisk komputerowych. Komunikować się ze sobą i wymieniać dane mogły więc tylko komputery korzystające z kompatybilnych protokołów i systemów operacyjnych.

Jak nietrudno sobie wyobrazić, systemom różnych firm ciężko było komunikować się ze sobą, o ile w ogóle było to możliwe. Wkrótce okazało się konieczne stworzenie jakiegoś mechanizmu translacji protokołów, umożliwiającego firmom komunikację i współdzielenie informacji. We wczesnych latach 1970-tych amerykański Departament Obrony (*DoD, Department of Defense*) zaprojektował model komunikacji międzykomputerowej, który stał się modelem źródłowym dla pakietu protokołów TCP/IP.

Model ten został jednak w znacznym stopniu zastąpiony *modelem referencyjnym OSI* (OSI Reference Model), powstałym we wczesnych latach 80-tych . Model referencyjny OSI ma budowę (architekturę) siedmiowarstwową, określającą poszczególne funkcje sieciowe występujące w każdej z warstw (por. rysunek 1.1). W dalszym ciągu rozdziału znajduje się szersze omówienie modelu DoD wraz z jego odwzorowaniem w modelu OSI. Występujące w całej książce opisy przeznaczenia i funkcji protokołów, obecnych w pakiecie TCP/IP, zawierają odwołania do obu tych modeli.

RYSUNEK 1.1. Model referencyjny OSI definiuje siedem warstw i ich funkcje



Model referencyjny OSI umożliwia bezkonfliktową komunikację dowolnych systemów, oferując producentom i dostawcom schemat architektoniczny służący do projektowania sprzętu, protokołów i środowisk operacyjnych. Dzięki niemu inżynierowie i projektanci mogą korzystać ze standardowych specyfikacji komunikacji międzysystemowej. Pozwala on także na korzystanie z różnych protokołów w różnych architekturach sieciowych i odnoszących się do niższych warstw typach nośników. Choć nie zawsze da się osiągnąć bezkonfliktową komunikację, jest ona podstawowym celem modelu referencyjnego OSI.

Zanim powstał model OSI, istniejące protokoły nie ułatwiały wzajemnych połączeń. W większości przypadków próba zapewnienia wstecznej kompatybilności z tymi protokołami byłaby niewykonalna. Stąd większość protokołów i sprzętu, obecnie wdrażanych przez producentów i dostawców, spełnia wytyczne modelu OSI. Sprawna i szybka wymiana danych oraz bezkonfliktowa łączność wzajemna, wymagana w dzi-

siejszych mieszanych środowiskach komputerowych, zależy od zastosowania się przez producentów i dostawców do znormalizowanego modelu referencyjnego.

Model OSI jest schematem *koncepcyjnym*. Składa się na niego szereg standardów, definiujących co powinno się zdarzyć i jak należy zapakować dane, aby po okablowaniu dostały się do zdalnego hosta. Warstwy logiczne tego modelu nie definiują dokładnie czynności wykonywanych w każdej warstwie, a jedynie opisują funkcje dostępne w każdej z nich. Sposób zapewnienia zestawu funkcji określonych w poszczególnych warstwach zależy od dostawcy lub producenta, tworzącego lub wdrażającego sprzęt lub protokoły. Konkretni producenci mogą swobodnie interpretować i wybierać stopień wierności wobec specyfikacji danej warstwy. W rezultacie nie zawsze uzyskuje się całkowitą zgodność komunikacji między niepodobnymi urządzeniami, ale omawiany schemat dostarcza najlepszych możliwych wzorców do jej osiągnięcia.

Model OSI składa się z następujących siedmiu warstw (od góry do dołu):

- aplikacji,
- prezentacji,
- sesji,
- transportowej,
- sieciowej,
- łącza danych,
- fizycznej.

Mówiąc ogólnie, każda warstwa dostarcza odrębnych funkcji, które muszą zostać użyte wewnątrz niej, aby przygotować dane do wysłania przez okablowanie do zdalnej stacji. Dostawca może określać szczegóły wewnętrzne tych funkcji ogólnych. Innymi słowy, producenci lub projektanci definiują działanie szczegółów, tak, że dostawcy muszą troszczyć się tylko o swoją część układanki. Dopóki organizacja lub dostawca przestrzega zasad, ustalonych przez *ISO* (International Standards Organization) dla konkretnej warstwy, produkt końcowy łatwo integruje się z innymi produktami zgodnymi z zasadami tego modelu.

Warto pamiętać, że model OSI jest stosowany tylko podczas przygotowywania danych wysyłanych do zdalnego hosta, podobnego lub niepodobnego (tzn. korzystającego z tych samych protokołów i systemu operacyjnego lub nie). Modelu referencyjnego OSI nie stosuje się podczas lokalnego dostępu do danych systemu. Na przykład dostęp do usług plików i wydruku wymaga jedynie dostępu do twardego dysku komputera lokalnego i otwarcia lokalnej aplikacji. W takiej sytuacji dostęp do danych nie wymaga żadnej interwencji użytkownika. Jeśli jednak to samo działanie ma zostać wykonane na zdalnym hoście, trzeba jakoś wysłać do innego urządzenia komunikat o potrzebie dostępu do plików lub drukarki, zmuszający je do odpowiedzi - przesłania danych.

Aby przekierować żądanie dostępu do usług plików i wydruku, potrzebny jest *readresator* (redirector). Przekierowuje on żądanie do zdalnego hosta, celem jego przetworzenia. Zdalny host przygotowuje żądanie do transmisji przez sieć, dodając informacje *nagłówkowe* (header) i kontrolne, pozwalające stacji docelowej zrozumieć, co powinna zrobić z danymi i jak zareagować.

Omówienie modelu Departamentu Obrony

Historia modelu DoD zaczęła się na długo przed modelem OSI, który wkrótce go zastąpił. Już w 1973 roku *Agencja Zaawansowanych Projektów Badawczych Departamentu Obrony* (DARPA, DoD Advanced Research Projects Agency) rozpoczęła program mający na celu stworzenie technologii, które mogłyby łączyć między sobą różne rodzaje pakietów sieciowych. Nadano mu nazwę „Internetting Project", a jego wynikiem — czego można domyślać się na podstawie nazwy — jest dzisiejszy Internet.

Model zaprojektowany przez agencję DARPA, będący wyjściowym standardem któremu podporządkowane są podstawowe protokoły internetowe, jest właśnie znany jako model DoD. Składa się on z następujących czterech warstw (od góry do dołu):

- aplikacji
- transportowej
- sieciowej
- dostępu do sieci

Jak widać na rysunku 1.2, model DoD z grubsza odpowiada modelowi OSI.

RYSUNEK 1.2. Model DoD składa się z czterech odrębnych warstw

Zalety warstwowej konstrukcji OSI

Warstwowa konstrukcja modelu referencyjnego OSI jest korzystna dla producentów sprzętu i projektantów oprogramowania oraz osób zawodowo oferujących pomoc techniczną i rozwiązywanie problemów (np. inżynierów sieciowych). Zalety tego modelu można podzielić następująco:

- Jasne sprecyzowanie ogólnych funkcji każdej warstwy.
- Zapewnienie dostawcom dobrze określonego schematu dla potrzeb pisania aplikacji i projektowania sprzętu.
- Zmniejszenie złożoności pracy w sieci dzięki skategoryzowaniu funkcji modelu.
- Zwiększenie współdziałania niepodobnych sieci i protokołów.
- Uproszczenie rozwiązywania problemów dzięki łatwiejszemu umiejscawianiu źródła problemów sieciowych.
- Przyspieszanie rozwoju branży przez ułatwienie specjalizacji.

Jasne sprecyzowanie funkcji warstw

Dzięki zawężeniu zakresu odpowiedzialności poszczególnych warstw, model OSI zmniejsza problemy na jakie napotykają producenci i inżynierowie sieciowi. Poza tym nie trzeba ponownie wymyślać wytycznych produktu lub protokołu dla konkretnych zastosowań. Dzięki jasnemu określeniu funkcji każdej z warstw dostawcy mogą projektować produkty przeznaczone dla jednej konkretnej warstwy, a nie dla wszystkich siedmiu. Pozwala im to na specjalizację w wybranych dziedzinach i zmniejsza złożoność sieci.

Dobrze określony schemat dla dostawców

Dostawcy mogą tworzyć specyfikacje przeznaczone dla jednej lub kilku warstw. Podejście warstwowe upraszcza takie tworzenie, pozwalając dostawcom koncentrować się i specjalizować we własnej, konkretnej warstwie modelu OSI. Dodatkowo zwiększa współdziałanie między systemami, tworząc otwarte środowisko umożliwiające współistnienie wielu protokołów. Na przykład dostawca tworzący *kartę sieciową* (NIC, Network Interface Card) może zajmować się tylko warstwą łącza danych modelu OSI.

Modułowa konstrukcja OSI umożliwia dostawcom tworzenie wyspecjalizowanych produktów. Ponieważ nie muszą zajmować się wszystkimi funkcjami od góry do dołu modelu, mogą skupić się na konkretnej warstwie i funkcji. Dzięki temu tworzenie sprzętu i oprogramowania oraz wprowadzanie go na rynek jest prostsze. Poza tym, bez względu na różne dostosowywanie się przez dostawców do zasad koncepcyjnych każdej warstwy, samo istnienie znormalizowanego modelu zwiększa zarówno bieżący poziom współdziałania między systemami, jak i prawdopodobieństwo harmonijnego współistnienia przyszłych protokołów i produktów w tej samej sieci.

Mniejsza złożoność pracy w sieci

Podejście warstwowe pozwala inżynierom sieciowym rozwiązywać problemy zgodnie z zasadą „dziel i rządź". Kiedy wiadomo, jakie procesy powinny zachodzić w każdej warstwie, wówczas źle działającą funkcję można zidentyfikować wiedząc, która

warstwa nie spełnia swych funkcji. Protokół lub część sprzętu powinny działać zgodnie ze specyfikacjami zdefiniowanymi dla danej warstwy.

Co chyba ważniejsze, dzięki temu modelowi umiejscawianie problemów nie wymaga zajmowania się całą strukturą, a tylko siedmioma mniejszymi jej fragmentami. Gdy konkretna warstwa nie działa poprawnie, w oparciu o model można wydzielić i zaszufladkować problem, a dzięki temu dużo łatwiej go rozwiązać. Mówiąc ogólnie, operacje sieciowe funkcjonują jako prostsze fragmenty, a nie jedna, bardziej skomplikowana całość.

Popieranie specjalizacji

Stosowanie powszechnie przyjętego, „ogólnobranżowego" zestawu zasad obsługi sieci jest inspiracją dla powstawania jeszcze szybszych i bardziej niezawodnych programów i protokołów. Dostawcy wiedząc, że mogą współzawodniczyć w ulepszaniu specyfikacji i skuteczności w dowolnej warstwie modelu referencyjnego OSI, wciąż przesuwają granice wydajności. Ponieważ wystarczy spełnianie specyficznych standardów tylko jednej warstwy, mogą specjalizować się w wytwarzaniu produktów spełniających specyficzne potrzeby klientów. Przykładem może być router działający na warstwie trzeciej, przeznaczony dla małego biura lub domu.

Opis ogólny warstw OSI

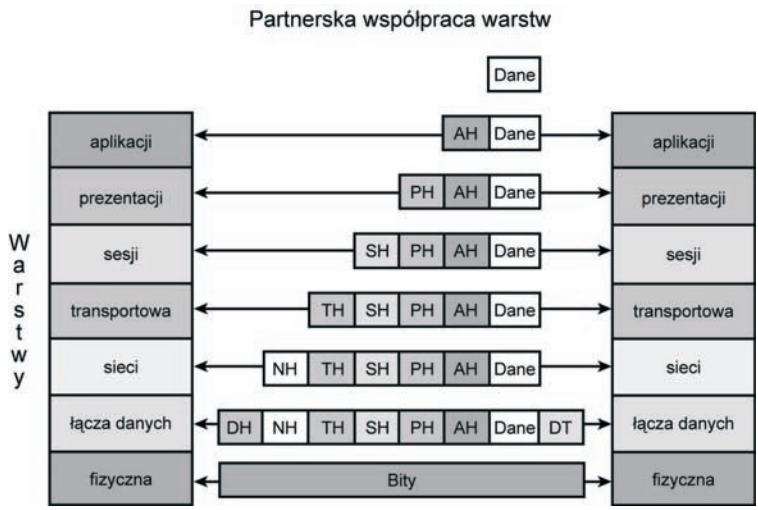
Kiedy trzeba wysłać dane (np. wiadomość poczty elektronicznej lub żądanie odczytu pliku ze zdalnego hosta), żądanie to musi zostać przekształcone w pakiet danych i przekierowane. System wysyłający musi wykonać następujące działania, oparte na poszczególnych funkcjach modelu referencyjnego OSI:

1. Zaadresować żądania.
2. Skojarzyć z nim protokoły.
3. Zmodulować go.
4. Wysłać go poprzez okablowanie.

Gdy system przygotowuje dane do wysłania przez okablowanie, najpierw readresator przechwytuje komunikat, nakłada na niego swoje informacje nagłówkowe i kontrolne, po czym przesyła go w dół do następnej warstwy. Niższe warstwy w modelu OSI obsługują warstwy wyższe, zapewniając im niezawodny transport, routing i adresowanie. Usługi te są stosowane nawet wtedy, gdy komunikat to zwykłe „Hej" przesyłane od jednego użytkownika do drugiego.

Każda warstwa w modelu OSI dołącza swoje informacje nagłówkowe i kontrolne tak, aby odpowiadająca jej warstwa na zdalnym hoście mogła je usunąć i wiedziała, co z nimi zrobić. Każda z warstw odgrywa odrębną rolę podczas przygotowywania

danych do wysłania celem komunikacji ze zdalnym hostem partnerskim (por. rysunek 1.3). Wszelkie działania właściwe dla tych ról pozostają dla użytkownika niewidoczne.



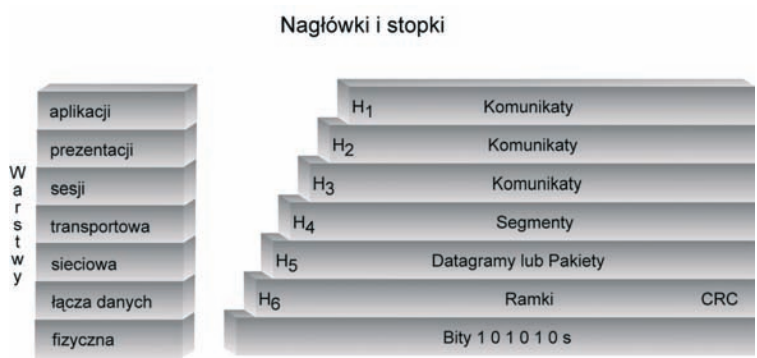
RYSUNEK 1.3. Każda warstwa modelu OSI dodaje informacje nagłówkowe i kontrolne, wykorzystywane przez odpowiadającą jej warstwę na hoście odbierającym

Gdy komputer przekazuje dane z jednej warstwy do następnej, każda kolejna warstwa dodaje do nich informacje nagłówkowe oraz kontrolne i tak dane te wędrują w dół do warstwy fizycznej i rzeczywistego nośnika fizycznego (przewodu czy też kabla sieciowego). Każda warstwa traktuje wszystko to, co przekazuje w dół, jako ogólne dane warstw wyższych. Przypomina to wkładanie w każdej warstwie jednej koperty do drugiej.

Na przykład warstwa aplikacji dodaje informacje nagłówkowe i kontrolne, przeznaczone dla odpowiadającej jej warstwy aplikacji na zdalnym hoście. Następnie przekazuje je wraz z danymi w dół, do warstwy prezentacji. Warstwa ta odczytuje informacje warstwy wyższej jako dane, nie dzieląc ich na informacje nagłówkowe i kontrolne ani dane. Warstwa prezentacji dodaje swoje informacje nagłówkowe i kontrolne, przeznaczone dla warstwy prezentacji na zdalnym hoście. Innymi słowy każda warstwa niższa (w tym przypadku prezentacji) nie zważa na informacje nagłówkowe i kontrolne ani dane warstwy wyższej, traktując to wszystko jako jedną całość — dane. Każda warstwa wykorzystuje jedynie informacje kontrolne i nagłówkowe oraz dane odpowiadającej jej warstwy partnerskiej ze zdalnego hosta. Każda kolejna warstwa dodaje swoje własne informacje nagłówkowe i kontrolne oraz wysyła dane w dół, na następny poziom.

Gdy dane osiągną poziom łącza danych, system uruchamia algorytm zwany *cykliczną kontrolą nadmiarowości* (CRC, Cyclical Redundancy Check) lub *sekwencją kontroli ramki* (FCS, Frame Check Sequence). Następnie dodaje wynik CRC jako *stopkę* (trailer) na końcu informacji, gwarantującą zgodność bitów wysyłanych z bitami odbieranymi

przez hosta końcowego. Termin ***ramka*** odnosi się do logicznego pogrupowania informacji, jakiemu ulegają dane w warstwie łącza danych. Dalej dane te wychodzą na okablowanie jako sygnały elektryczne lub świetlne — jedynki (1) i zera (0) — a zamierzony host zdalny je odbiera (por. rysunek 1.4).



RYSUNEK 1.4. Host odbierający usuwa nagłówki i stopki, po czym wysyła dane w górę, do następnej warstwy

Po odebraniu danych proces się odwraca. Każda warstwa usuwa swoje informacje nagłówkowe i kontrolne oraz przekazuje dane w górę, do następnej warstwy, odsłaniając informacje nagłówkowe i kontrolne oraz dane właśnie tej warstwy. Gdy dane wreszcie dojdą do warstwy aplikacji, ta ściąga swoje własne informacje nagłówkowe i kontrolne oraz przekazuje dane wzwyż. Dzieje się tak z każdą pojedynczą ramką przechodzącą przez okablowanie. Każda warstwa musi dołączać do danych informacje nagłówkowe i kontrolne tak, aby jej odpowiadająca jej warstwa partnerska mogła zidentyfikować warstwę wyższą, która powinna je otrzymać jako następna.

Warstwa aplikacji

Czasem mylnie uważa się, że nazwa szczytowej warstwy modelu OSI odnosi się do aplikacji użytkownika, takich jak Word, Excel, PowerPoint, itp. Nazwa ta nie wiąże się jednak z samym oprogramowaniem aplikacyjnym, ale raczej z możliwością dostępu przez sieć do danych jednej aplikacji z innej oraz z dostępem do modelu referencyjnego OSI, mającym na celu przygotowanie danych do umieszczenia ich w pakiecie i wysłania przez okablowanie.

Warstwa aplikacji umożliwia aplikacjom użytkownika wysyłanie danych przez sieć, po prostu zapewniając im dostęp do warstw niższych (dostęp do modelu OSI). Jej zadaniem jest dostarczenie interfejsu do stosu protokołów. W przeciwieństwie do innych warstw OSI, nie oferuje ona usług żadnym innym warstwom, udostępniając jedynie własne usługi.

Usługi warstwy aplikacji obejmują m. in.:

- aplikacyjne usługi sieciowe i międzysieciowe;
- usługi plikowe i wydruku;

- *pocztę elektroniczną* (e-mail);
- dostęp do sieci *WWW* (World Wide Web) i *protokół przesyłania hipertekstu* (HTTP, HyperText Transfer Protocol);
- dostęp za pomocą protokołu Telnet ze zdalnego hosta;
- *protokół przesyłania plików* (FTP, File Transfer Protocol).

Te i inne usługi zostaną omówione w niniejszej książce.

Warstwa prezentacji

Warstwa prezentacji zapewnia różnym platformom wspólny format danych. Odpowiada ona za następujące usługi:

- konwersję i tłumaczenie (translację) danych;
- kompresję i dekompresję;
- szyfrowanie i odszyfrowywanie.

Przykładem rzeczywistego protokołu tej warstwy jest *XDR* (eXternal Data Representation), stosowany w opartym na schemacie klient-serwer systemie plików *NFS* (Network File System), stworzonym przez firmę Sun MicroSystems. Protokół ten zapewnia niezależność od platformy. Jest on w istocie włączony do kodu oprogramowania. System plików NFS i protokół XDR będą dokładnie omawiane w rozdziale 18.

Warstwa sesji

Warstwa sesji ustanawia sesje i zarządza nimi. Sesja składa się z dialogu między warstwami prezentacji w przynajmniej dwóch systemach. Warstwa ta obsługuje też żądania dostępu do różnych usług, występujące między systemami, i zarządza odpowiedziami na te żądania. Poza tym steruje dialogiem między dwoma aplikacjami na różnych hostach i zarządza strumieniami danych.

Wydajność sterowania dialogiem między hostami w warstwie sesji zależy od tego, czy komunikacja odbywa się w trybie ***połowicznie dwukierunkowym*** (***half-duplex***) czy ***całkowicie dwukierunkowym*** (***full-duplex***). W trybie połowicznie dwukierunkowym tylko jedno urządzenie może w danej chwili się komunikować (nadawać), natomiast wszystkie pozostałe oczekują na swoją kolej. Każda strona komunikacji musi czekać na koniec wysyłania przez inną, a następnie odpowiadać odrębnym potwierdzeniem. W trybie całkowicie dwukierunkowym wysyłanie i odbieranie może być jednoczesne, co zwiększa wydajność komunikacji. Wydajność w tym trybie osiąga się przez *tz.w jazdę na barana* (piggybacking) lub zawieranie danych w obrębie tej samej ramki.

Przykładem znanego protokołu warstwy sesji może być *NetBIOS* (Network Basic Input/Output System). Ustanawia on sesje między dwoma komputerami z systemem operacyjnym typu Windows (NT lub 9*x*) firmy Microsoft. Protokół ten zapewnia usługi nazewnicze i zarządzanie sesjami między dwoma urządzeniami korzystającymi z nazewnictwa prostego.

Warstwa sesji obsługuje też *zdalne wywoływanie procedur* (RPC, Remote Procedure Call), zaprojektowane przez firmę Sun, umożliwiające klientom tworzenie żądań przeznaczonych do zdalnego wykonywania. Żądania te są wysyłane do zdalnego hosta celem przetworzenia i udzielenia odpowiedzi, co pozwala na komunikację między dwoma hostami przez sieć. System plików NFS stosuje RPC do wysyłania wywołań i odbierania odpowiedzi w warstwie sesji, zaś w warstwie prezentacji wykorzystuje protokół XDR.

Warstwa transportowa

Warstwa transportowa w zasadzie ma zapewniać gwarantowane, niezawodne dostarczanie danych tylko między dwoma komunikującymi się procesami lub programami, uruchomionymi na zdalnych hostach. Jest to jednak prawdą tylko wtedy, gdy dostawca zdecyduje się zaimplementować *protokół sterowania transmisją* TCP (TCP, Transmission Control Protocol) zamiast jego mniej niezawodnego odpowiednika, *protokołu datagramów użytkownika* UDP (UDP, User Datagram Protocol). Protokoły te omówimy w rozdziałach 8 i 9.

Warstwa transportowa wykonuje następujące działania:

- Steruje komunikacją całościową („od końca do końca") między dwoma procesami uruchomionymi na różnych hostach.
- Zapewnia usługi połączeniowe i bezpołączeniowe warstwom wyższym.
- Wykorzystuje adresy portów klienta i serwera do identyfikacji procesów uruchomionych w obrębie hosta.
- Segmentuje dane dla aplikacji warstw wyższych.

Zadaniem tej warstwy jest identyfikowanie procesów komunikujących się na każdym hoście oraz zapewnianie usług połączeniowych i niezawodnego transportu, bądź szybkości dostarczania. Zarządza ona przepływem danych, a gdy sesja jest połączeniowa zajmuje się sterowaniem przepływem. W warstwie tej rezydują protokoły TCP i UDP.

Segmentuje ona dane (komunikaty) podawane w dół przez aplikacje warstw wyższych. Obsługuje adresowanie za pomocą ***portów***, zwanych też ***gniazdami*** (***sockets***), identyfikujących programy lub procesy warstw wyższych, komunikujące się na konkretnym urządzeniu. Śledzenie różnych segmentów i zarządzanie nimi zapewniają jej numery portów każdej aplikacji.

Łączenie gniazd w pary

Gdy występuje komunikacja całościowa między dwoma hostami, w której uczestniczą źródłowe i docelowe adresy IP i porty (zwane też gniazdami), wówczas w branży nazywa się to *parą gniazd* (*socket pair*).

Warstwa transportowa może zapewniać protokołom warstw wyższych zarówno obsługę połączeniową, jak i bezpołączeniową. Zawsze jednak zajmuje się portami i adresami. Adresy klienta i serwera (np. porty TCP lub UDP) służą do identyfikacji procesów uruchomionych w obrębie hosta. Warstwę transportową dokładnie omówimy w rozdziale 7.

Warstwa sieciowa

Warstwa sieciowa przede wszystkim przypisuje logiczne adresy źródłowy i docelowy oraz określa najlepszą ścieżkę routingu danych między sieciami. Warstwa ta zapewnia:

- komunikację całościową między dwoma hostami,
- adresowanie logiczne,
- dostarczanie pakietów,
- routing.

Protokoły warstwy Sieciowej zajmują się ***adresowaniem logicznym***, które należy odróżnić od adresowania *MAC* (Media Access Control) warstwy fizycznej, skojarzonego z kartami sieciowymi. W przeciwieństwie do adresów fizycznych (przypisanych na stałe), dostawcy nie umieszczają na stałe adresów logicznych w kartach. Zamiast tego administratorzy sieci przypisują je ręcznie lub dynamicznie. Adresy logiczne warstwy sieciowej będą omawiane w rozdziałach 4 – 6.

Aby zapewnić najlepszy routing danych, urządzenia warstwy sieciowej (takie, jak routery) stosują ***przełączanie pakietów*** (***packet switching***). W procesie tym router identyfikuje logiczny adres docelowy (warstwy sieciowej) ruchu sieciowego odbieranego na jednym interfejsie, po czym z innego interfejsu wysyła go do miejsca przeznaczenia.

W warstwie sieciowej działają następujące protokoły:

- **RARP**, **ARP**, **BootP**, **DHCP** — zapewniające konfigurację lub rozwiązywanie adresów;
- **ICMP** — diagnostyczny i kontrolny;
- **RIP**, **IGRP**, **EIGRP**, **OSPF** i **BGP** — trasujące.

Warstwa łącza danych

Do głównych obowiązków warstwy łącza danych modelu OSI należy wysyłanie i odbiór ramek oraz adresowanie fizyczne. Warstwa ta przed wysłaniem otrzymanych z góry danych dodaje do nich zarówno nagłówek z przodu, jak i czterobajtową stopkę na końcu, tworząc w ten sposób ***ramkę*** (***frame***) wokół tych danych. Termin ***ramkowanie pakietów*** (***packet framing***) oznacza tworzenie ciągów takich ramek. Stopki dodaje do danych tylko warstwa łącza danych.

Warstwa łącza danych ma następujące cechy i obowiązki:

- Steruje dostępem do nośnika.
- Dodaje adresy sprzętowe — źródłowy i docelowy.
- Przygotowuje ramki do transmisji, konwertując pakiety danych na ramki.
- Bierze na siebie funkcję wysyłania i odbierania danych przez okablowanie.
- Oblicza wielkości CRC lub FCS.
- Obsługuje *mosty* (*bridges*) i *przełączniki* (*switches*).

Adresy warstwy drugiej

Producenci zapisują na stałe w każdej karcie sieciowej adres warstwy łącza danych (adres MAC). Podczas produkcji kart określają ich numery seryjne. Każdy adres ma sześć bajtów długości, zgodnie z zaleceniem *IEEE*. Pierwsze trzy bajty określają konkretnego dostawcę, który z kolei w sposób niepowtarzalny przypisuje wartości ostatnim trzem bajtom. Urządzenia działające w warstwie łącza danych muszą mieć możliwość identyfikowania tych adresów.

Warstwa łącza danych dodaje do nagłówka adresy MAC — źródłowy i docelowy — celem identyfikacji karty sieciowej urządzenia wysyłającego ramkę, jak i urządzenia które powinno ją odebrać. Każdy adres MAC musi być niepowtarzalny (unikatowy) w całej sieci. Urządzenia warstwy 2 w oparciu o adres docelowy decydują, czy informacje należy przekazać dalej.

Przed transmisją nadające urządzenia stosują algorytm *cyklicznej kontroli nadmiarowości* (CRC) lub *sekwencji kontroli ramki* (FCS). W branży te dwa terminy stosowane są zamiennie. Urządzenia warstwy łącza danych dodają wynik CRC lub FCS jako stopkę na końcu danych podawanych w dół przez warstwę sieciową, obramowując w ten sposób przesyłane bity. Z tego powodu w warstwie łącza danych mówi się właśnie o „ramkach". Wartości sum kontrolnych CRC (lub FCS) nie gwarantują dostarczenia danych, a służą jedynie do sprawdzania, czy bity wysyłane zgadzają się z bitami odebranymi przez hosta docelowego. Za pomocą tego samego algorytmu hosty odbierające sprawdzają, czy w trakcie przesyłania ramka nie została uszkodzona. Gdy wielkości CRC (lub FCS) nie są zgodne, host odbierający po prostu odrzuca ramkę bez powiadamiania stacji wysyłającej. Jeżeli ramka nie jest prawidłowa, stacja docelowa nigdy nie przekaże danych do warstwy wyższej. Obowiązek ponownego wysyłania uszkodzonych ramek spoczywa na urządzeniach wysyłających.

Warstwa fizyczna

Warstwa fizyczna zajmuje się jedynkami (1) i zerami (0), czyli bitami tworzącymi ramkę. ***Bity*** kodowane są jako impulsy elektryczne lub świetlne. Warstwa ta zajmuje się też charakterystykami elektrycznymi i mechanicznymi, kodowaniem sygnałów i poziomami napięcia. Mówiąc ogólnie: dotyczy ona elementów namacalnych, czyli takich elementów fizycznych, których można dotknąć, np. okablowania czy *wtórników* (*repeaters*). Warstwa fizyczna obejmuje:

- charakterystyki elektryczne i mechaniczne;
- kodowanie sygnałów;
- jedynki (1) i zera (0);
- specyfikacje złączy fizycznych.

Architektura i topologie łącza danych

Termin ***aplikacja*** oznacza literalne zastosowanie standardów w formie architektury sieciowej i specyfikacji dotyczących głównych topologii. Standardy te obejmują specyfikacje IEEE i *ANSI* (American National Standards Institute), przeznaczone dla następujących technologii:

- Ethernet,
- *Szybki* (Fast) Ethernet,
- Gigabitowy Ethernet,
- Token-Ring,
- FDDI.

Standardy obejmują też typy ramek i metody dostępu do kanału, określane przez IEEE i ANSI. Kolejne punkty w charakterze przypomnienia zawierają ogólne omówienie tych technologii.

Ethernet i IEEE 802.3

Zaczynamy od najbardziej popularnej architektury łącza danych, mianowicie technologii ethernetowych, zdefiniowanych przez IEEE w ramach specyfikacji 802.3. Zasługę wynalezienia Ethernetu zwykle przyznaje się firmie Xerox Corporation, jednak w rzeczywistości uzyskała ona źródłową technologię o nazwie Aloha Net w latach 1970-tych od Uniwersytetu Hawajskiego. Następnie Xerox dołączył do firm DEC i Intel celem zaprojektowania najwcześniejszego standardu ethernetowego, wypuszczonego w roku 1980 jako wersja 1. W 1982 roku te trzy firmy wydały kolejny, ulepszony standard: ethernet wersja 2.

W połowie lat 1980-tych komitet 802 organizacji IEEE zaadoptował ethernet jako standard 802.3. Wszystkie aktualne i przyszłe projekty technologii ethernetowych rzekomo mają się opierać właśnie na tym standardzie bazowym. Ze względu na swoje początki Ethernet stał się najpopularniejszym, stosowanym na całym świecie standardem sieci *LAN* (Local Area Network).

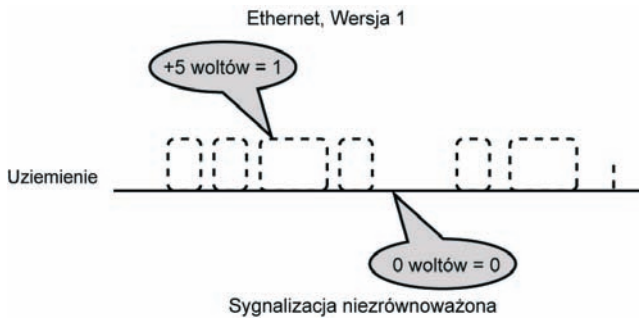
Warto pamiętać, że Ethernet to nie to samo, co implementacje IEEE 802.3, a terminów tych nie powinno się stosować zamiennie (choć czasem się tak robi). Firmy Xerox, DEC i Intel zaprojektowały wersje 1 i 2 z dość podobnymi parametrami, a komitet IEEE 802 dodał do nich szereg znormalizowanych funkcji rozszerzonych, nie współdzielonych z poprzednikami. Tabela 1.1 zawiera omówienie podobieństw i różnic między tymi implementacjami.

TABELA 1.1. Wersje 1 i 2 ethernetu oraz IEEE 802.3

Wersja 1	Wersja 2	IEEE 802.3
Architektura warstwy łącza danych.	Zawiera Ethernet_II, celem wykrywania i odrzucania wadliwych ramek (*de facto* schemat branżowy przenoszenia ruchu IP przez sieci LAN typu ethernet).	Dodaje *nadbiorniki* (transceivers) z kontrolą rozwlekania (lub pochłanianiem rozwlekania).
Dostarczała dane z szybkością 10 Mb/s w topologii *magistrali liniowej* (linear bus).	Dostarcza dane z szybkością 10 Mb/s w topologii magistrali liniowej.	Rozciąga obsługę topologii fizycznych na konfiguracje *gwiazdy* (star).
Mogła korzystać tylko z nośnika *grubego koncentrycznego* (thick coaxial).	Może korzystać tylko z nośnika grubego koncentrycznego.	Dodaje takie typy nośników, jak *cienki koncentryczny* (thin coaxial), *światłowód* (fiber) i *skrętka dwużyłowa* (twisted pair).
Stosowała *sygnalizację niezrównoważoną* (unbalanced signaling) z uziemieniem jako punktem odniesienia, wrażliwą na *szum* (noise) i *interferencje elektromagnetyczne* (EMI, Electro-Magnetic Interference).	Stosuje *sygnalizację zrównoważoną* (balanced signaling).	Rozszerzenia z 1995 roku oferują szybkości przesyłu 100 Mb/s (specyfikacja 802.3u).
Nie obsługiwała *błędu jakości sygnału* (SQE, Signal Quality Error), zwanego też *sygnałem taktowania* (heartbeat), więc wykrywanie *kolizji* (collisions) było trudniejsze.	Dodaje SQE.	Obsługuje SQE, ale jest to konieczne tylko przy nadbiornikach zewnętrznych.
Niezgodna z wersją 2.	Niezgodna z wersją 1.	Niezgodna z wersją 1.

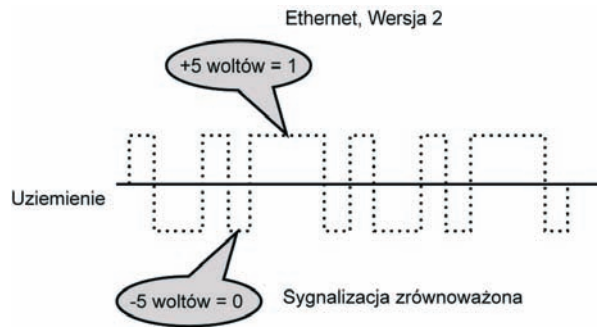
Wersja 1 specyfikacji Ethernet reprezentuje dane w oparciu o obecność lub nieobecność napięcia, co nosi nazwę ***sygnalizacji niezrównoważonej***. Ten typ transmisji jest wysoce podatny na zakłócenia zewnętrzne. Przykład takiej sygnalizacji widać na rysunku 1.5.

RYSUNEK 1.5. W sygnalizacji niezrównoważonej dane są reprezentowane przez poziomy napięcia zmieniające się od 0 (uziemienie) do +5 woltów



W wersji 2 Ethernetu wprowadzono lepszą metodę ***sygnalizacji zrównoważonej***, reprezentującej dane w oparciu o zmiany napięcia z dodatniego na ujemne, z napięciem 0 (uziemieniem) jako wspólnym punktem odniesienia (por. rysunek 1.6). Dzięki niej wpływ zakłóceń transmisji maleje, a przez to wzrasta jakość sygnału.

RYSUNEK 1.6. Sygnalizacja zrównoważona zwiększa jakość sygnału dzięki wspólnemu punktowi odniesienia, a dane reprezentuje przez dodatnie i ujemne poziomy napięcia



Specyfikacja IEEE 802.3 opisuje ogólne działanie, składniki i ograniczenia odległościowe Ethernetu:

- Definiuje wszystkie składniki, funkcje, metody dostępu do kanału i działania warstw łącza danych i fizycznej.
- Daje dostawcom reguły wdrażania i rozwijania technologii sieci LAN typu 802.3.
- Jest oparta na standardzie IEEE o nazwie 10Base5, z drobnymi odchyleniami spełnianym przez wszelkie inne standardy 802.3.

Standard IEEE 802.3 definiuje opartą na *rozgłaszaniu* (broadcast) liniową architekturę sieciową o szybkości 10 Mb/s, opartą na rywalizacyjnej metodzie dostępu do kanału, zwanej ***dostęp z nasłuchiwaniem nośnej z detekcją kolizji*** (CSMA/CD, Carrier Sense Multiple Access with Collision Detection) — por. niżej.

Metoda dostępu do kanału

Obecnie istnieją różne ***metody dostępu do kanału***, zależne od architektury sieciowej (Ethernet wykorzystuje metodę opartą na rywalizacji). Opisują one reguły dyktujące urządzeniom sposób:

- dostępu do nośnika komunikacyjnego,
- przesyłania ramek,
- zwalniania kanału dla innych urządzeń.

Urządzenia korzystające z metody CSMA/CD:

- rywalizują o prawo do transmisji;
- mogą pomyślnie transmitować tylko pojedynczo (jedno urządzenie naraz);
- muszą poczekać na dostępność kanału aby wysłać ramkę w sytuacji, gdy inne urządzenia wykorzystują kanał (działanie połowicznie dwukierunkowe).

Gdy urządzenia nadają jednocześnie na tym samym kanale, występują kolizje sygnałów i ramki ulegają uszkodzeniu. Taki dostęp oparty na rywalizacji nosi nazwę CSMA/CD. Ponieważ dla Ethernetu wskaźnikiem możliwości wysyłania jest cisza, aby ją wykryć urządzenia przeprowadzają nasłuchiwanie nośnej. Jeśli nie wykryją w przewodzie żadnej częstotliwości, uzyskują dostęp do kanału i mogą od razu zacząć transmisję. Po transmisji urządzenia zwalniają kanał, a zanim ponownie spróbują uzyskać do niego dostęp, czekają przynajmniej 9,6 μs (mikrosekund). Dzięki temu inne nadbiorniki mają szansę na wysłanie własnych ramek.

Kolizje

Kolizje to, jak sama nazwa wskazuje, właśnie kolizje. W jakiejkolwiek danej chwili w sieci o transmisji w *paśmie podstawowym* (baseband) kanał powinien być zajęty przez najwyżej jeden sygnał. Jeśli przez przewód jednocześnie przemieszcza się więcej sygnałów, wynikiem jest kolizja utrudniająca pomyślną transmisję. Podczas transmisji *nadbiornik* (nadajnik-odbiornik) koduje sygnał na nośniku i nasłuchuje kolizji. Gdy taka nastąpi, wówczas wewnętrzny zespół obwodów nadbiornika, służący do detekcji kolizji, powiadamia kartę sieciową za pomocą sygnału zmuszającego ją do przerwania transmisji. Za wykrycie i ponowne wysłanie ramek po kolizji odpowiada urządzenie nadające.

Kolizje są codziennością Ethernetu, jednak kolizje nadmierne lub spóźnione są powodem do zmartwień. Nadmierne kolizje są powodowane przez przeciążenie odcinka (segmentu) zbyt wieloma urządzeniami. Gdy każde z nich współzawodniczy o kanał, prawdopodobieństwo kolizji rośnie wskutek samej ilości sygnałów.

Specyfikacja 802.3 definiuje ***kolizje spóźnione*** (***late collisions***) jako występujące po 64-tym bajcie ramki. Ich przyczyną może być przekroczenie maksymalnego ograniczenia długości nośnika, znane jako ***opóźnienie propagacji*** (***propagation delay***) lub

awaria sprzętu (***hardware failure***). Zderzeń spóźnionych nigdy nie powinno się uważać za część normalnego działania Ethernetu.

Ramki Ethernetowe

W dziedzinie standardów Ethernetowych istnieją następujące cztery różne typy ramek, każdy zaprojektowany przez kogo innego i dla innych celów:

- Ethernet_II (DIX);
- Ethernet_802.3 (zastrzeżony przez Novella);
- IEEE 802.3;
- IEEE 802.3 SNAP (SubNetwork Access Protocol).

Pierwotną ramkę ethernetową, o nazwie Ethernet_II lub DIX, wspólnie zaprojektowały firmy *DEC, Intel i Xerox* (w skrócie właśnie DIX). Novell zaprojektował swoją własną, zastrzeżoną ramkę Ethernet_802.3, przeznaczoną wyłącznie dla ruchu IPX/SPX. Ostatnie dwie ramki zaprojektował i nazwał instytut IEEE. Mimo nazewnictwa firmowego tych typów ramek, IEEE i branża stosują nazwy odmienne. Różnice pochodzą przede wszystkim od firm, stosujących ramki we własnych architekturach i językach. Na przykład firma Cisco odwołuje się do ramki Ethernet_II jako do ARPA. Tabela 1.2 zawiera opis nazewnictwa typów ramek, a tabela 1.3 — informacje specyficzne dla każdego z nich.

Wszystkie cztery typy ramek mogą współistnieć w jednej sieci, ale nie są ze sobą zgodne. Gdy informacje chcą wymieniać stacje korzystające z niepodobnych typów *hermetyzacji* (encapsulation), muszą one komunikować się za pośrednictwem routera obsługującego oba typy. Router taki przeprowadza konwersję między hostami. Ponieważ konwersja niepotrzebnie zwiększa obciążenie i opóźnia ruch danych w sieci, wewnątrz jednej sieci najlepiej korzystać tylko z jednego typu ramek. Tabela 1.4 zawiera opis cech podstawowych i drugorzędnych, charakteryzujących ramki ethernetowe.

Na rysunkach 1.7 – 1.10 pokazano wszystkie typy ramek. Warto porównać zarówno ich reprezentacje funkcyjne, jak i faktyczny wygląd. Wszystkie ramki mają te same podstawowe cechy charakterystyczne: zaczynają się 6-bajtowym adresem docelowym MAC, po którym następuje 6-bajtowy adres źródłowy MAC, a kończą się 4-bajtowym polem CRC.

TABELA 1.2. Odwzorowanie nazw ethernetowych

IEEE	Branża
–	Ethernet_II (DIX)
–	Ethernet_802.3
802.3	Ethernet_802.2
802.3 SNAP	Ethernet_SNAP

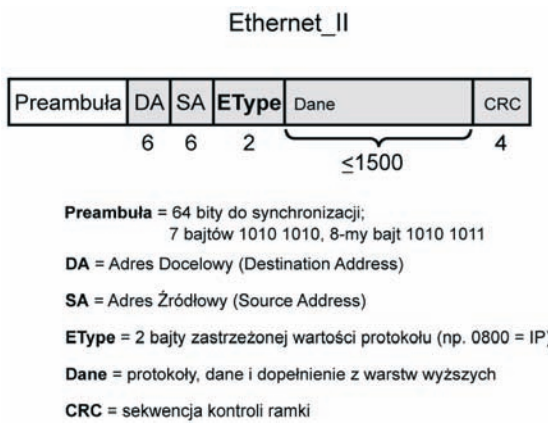
TABELA 1.3. Typy ramek ethernetowych

Ethernet_II (DIX)	Ethernet_802.3	Ethernet_802.2	Ethernet_SNAP
Służy do przenoszenia ruchu IP.	Służy do przenoszenia ruchu IPX/SPX.	Zawiera nagłówki LLC, wykorzystujące adresy DSAP i SSAP do identyfikacji protokołów warstw wyższych.	Zawiera nagłówki LLC, wykorzystujące adresy DSAP i SSAP do identyfikacji protokołów warstw wyższych.
Wykorzystuje do identyfikacji protokołów 2-bajtowe zastrzeżone wartości Ether-Type, np. 0800=IP.	Ograniczony do przenoszenia samego protokołu IPX.	Wykorzystuje zastrzeżone adresy SAP, np. E0=IPX.	Uwzględnia specjalny adres SAP AA, wskazujący na idący za nim nagłówek SNAP z dwubajtową wartością Ether-Type.
	Najczęściej obecnie stosowany typ ramki. Był faktycznym typem ramki w sieciach IPX przed powstaniem typu Ethernet_802.2.		Po nagłówku LLC dodaje pięciobajtowy nagłówek SNAP, służący do identyfikacji protokołu.

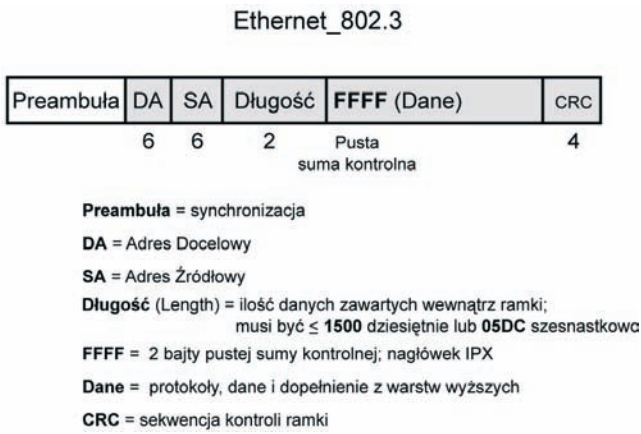
TABELA 1.4. Charakterystyki ramek ethernetowych

Podstawowe cechy charakterystyczne	Drugorzędne cechy charakterystyczne
Przed transmisją dodaje 14-bajtowy nagłówek.	Pierwsze 12 bajtów składa się z 6-bajtowego adresu docelowego MAC i 6-bajtowego adresu źródłowego (nadawcy) MAC. Po nich następuje pole 2-bajtowe, definiujące długość datagramu lub typ protokołu.
Przed transmisją dołącza 4-bajtową stopkę (CRC lub FCS).	Dodawana przez nadawcę i porównywana przez odbiorcę po to, żeby upewnić się, że ramka nie została uszkodzona
Przed transmisją każdej ramki wysyła 64-bitową preambułę celem osiągnięcia synchronizacji.	Zawiera 7 bajtów na przemian jedynek (1) i zer (0); ostatnie 2 bity 8-ego bajtu alarmują stacje o nadchodzeniu danych.
Najmniejszy dozwolony rozmiar ramki wynosi 64 bajty (ramki mniejsze muszą być dopełniane), a największy 1518 bajtów.	Zawiera 14-bajtowy nagłówek Łącza Danych, 4-bajtową doczepkę oraz maksymalnie 1500 bajtów protokołów i danych warstw wyższych.

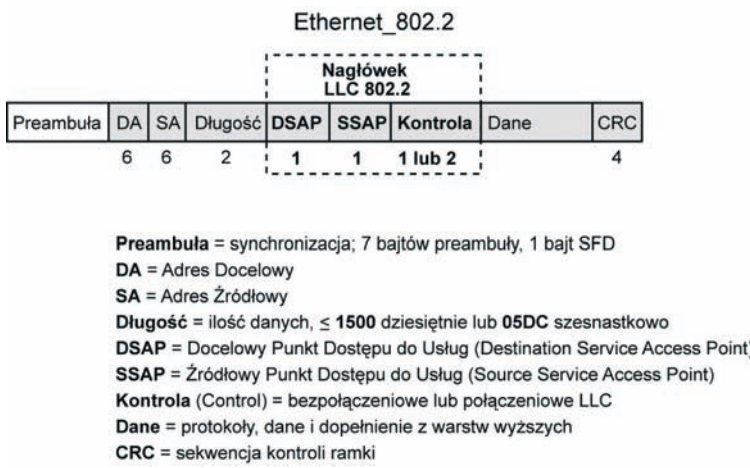
RYSUNEK 1.7. Ramka Ethernet_II jako jedyna zawiera po adresie źródłowym 2-bajtową wartość Ether-Type, służącą do identyfikacji protokołu przenoszonego wewnątrz ramki

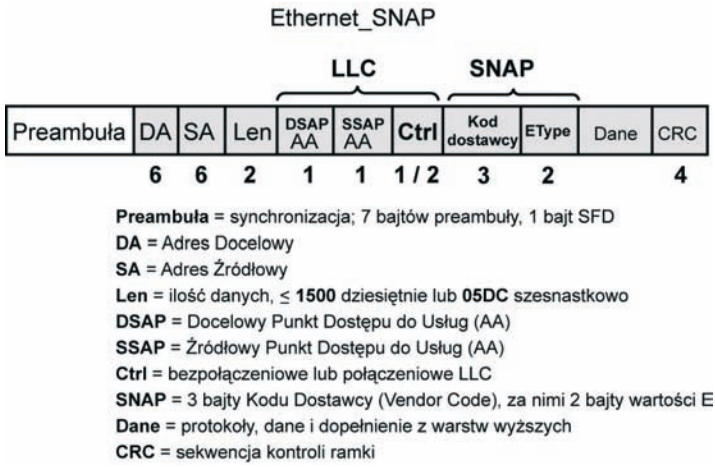


RYSUNEK 1.8. W ramkach Ethernet_802.3 za polem długości zawsze następuje pole z nagłówkiem IPX, zawierającym 2-bajtową pustą sumę kontrolną FFFF



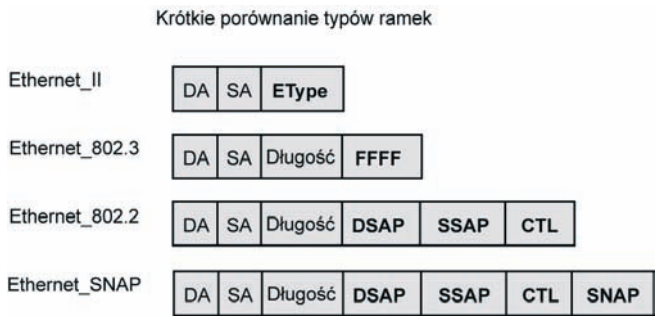
RYSUNEK 1.9. Ramka 802.3 instytutu IEEE, w branży znana jako Ethernet_802.2, zawiera nagłówek 802.2 z adresami DSAP (SAP docelowy) i SSAP (SAP źródłowy), służącymi do identyfikacji protokołu





RYSUNEK 1.10. Ramka 802.3 SNAP instytutu IEEE, w branży znana jako Ethernet_SNAP, dołącza do nagłówka 802.2 5-bajtowy nagłówek rozszerzający, obejmujący 3-bajtowy kod dostawcy i dalej 2-bajtową wartość Ether-Type, identyfikującą przenoszony protokół

Na rysunku 1.11 widać skrótowe porównanie czterech omówionych typów ramek.



RYSUNEK 1.11. Szybka identyfikacja różnic między typami ramek

Powolny Ethernet

Od pojawienia się w połowie lat 80-tych, powolny (10 Mb/s) Ethernet był oparciem dla sieci LAN. Ponieważ początki obsługiwania sieci były cokolwiek chaotyczne (dostawcy tworzyli oparte na własnych rozwiązaniach produkty i rządzące nimi reguły), warto prześledzić rozwój sieci w kierunku oficjalnych standardów branżowych i ich najnowszych udoskonaleń. Mimo wyłonienia się różnych ciał definiujących standardy, określające jasne reguły wdrażania technologii sieciowych (np. 802.3), chęć przekraczania ograniczeń prowadzi branżę do ignorowania wielu z tych reguł.

Istnieją następujące specyfikacje powolnego Ethernetu:

- **10Base5** — transmisja ma miejsce przy 10 Mb/s z wykorzystaniem grubego kabla koncentrycznego na magistrali liniowej.

- **10Base2** — transmisja ma miejsce przy 10 Mb/s z wykorzystaniem cienkiego kabla koncentrycznego na magistrali liniowej.
- **10BaseT** — transmituje 10 Mb/s przez skrętki dwużyłowe w konfiguracji gwiazdy fizycznej.

Szybki Ethernet

Szybki Ethernet spełnia dokładnie te same standardy bazowe co powolny. Różnica tkwi w dodatkowych 10 klauzulach wydanej w 1995 roku addendy IEEE 802.3u. Definiują one standard 3 różnych implementacji sieci o szybkości 100 Mb/s, ogólnie znanych jako **100BaseX**. Tabela 1.5 zawiera porównanie konfiguracji wolnego i szybkiego Ethernetu.

TABELA 1.5. Powolny Ethernet kontra Szybki Ethernet

	Szybki	Powolny
Dostęp do kanału metodą CSMA/CD	X	X
Te same minimalne/maksymalne rozmiary ramek	X	X
Obsługa tych samych typów ramek	X	X
Obsługa kat. 3, 4 i 5	X	X
Obsługa światłowodu	X	X
Obsługa gwiazdy fizycznej	X	X
Pełna/połowiczna dwukierunkowość	X	X
Obsługa topologii magistrali koncentrycznej		X
Kodowanie sygnałów sposobem Manchester		X
Wymóg sprzętu 100BaseX	X	
Zmiany składników i taktowania	X	

Standardy 100BaseX

Wszystkie trzy standardy 100BaseX opisują 100-megabitowe technologie „podstawowo-pasmowe" komunikacji przez skrętkę dwużyłową lub światłowód. Z powodu charakterystyk warstwy fizycznej, w obrębie każdego standardu występują inne odległości i ograniczenia. Istnieją trzy typy standardów 100BaseX:

- **100BaseTX** — definiuje przesył 100 Mb/s przez UTP co najmniej 5 kategorii, stosując takich samych dwóch skrętek jak 10 Mb/s Ethernet.
- **100BaseFX** — definiuje przesył 100 Mb/s przez nośnik światłowodowy.
- **100BaseT4** — wykorzystuje do transmisji 4 nieekranowane skrętki dwużyłowe, 3 do nadawania i odbierania, a 1 do wykrywania kolizji.

Gigabitowy Ethernet

Gigabitowy Ethernet (GE) pozwala na transmisję z maksymalną szybkością 1000 Mb/s za pośrednictwem okablowania UTP kategorii 5. Odpowiednia specyfikacja, o nazwie IEEE 802.3z, wykorzystuje formaty ramek ethernetowych 802.3 i metodę dostępu CSMA/CD. Dalsze korzystanie ze standardu 802.3 zapewnia wsteczną zgodność z technologiami 100BaseT i 10BaseT.

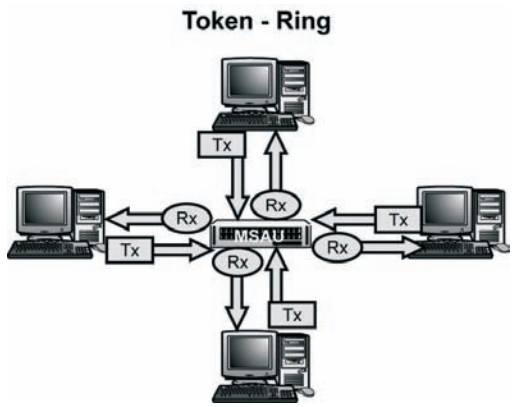
Token-Ring i IEEE 802.5

Za twórcę standardu Token-Ring sieci LAN zwykle uważa się firmę IBM, ale naprawdę opatentował go w 1967 roku dr Olaf Solderblum ze Szwecji. Firma IBM przejęła tę technologię właśnie od niego, zaś przy pomocy przedsiębiorstwa Texas Instruments rozwinęła technologię odpowiednich układów scalonych i zasady działania. Potem udostępniła technologię instytutowi IEEE, którego podkomitet 802.5 zaprojektował i opublikował w 1985 roku standard sieci Token-Ring o szybkości 4 Mb/s. Specyfikacja IEEE 802.5 zawiera szczegółowy opis podwarstwy MAC i warstwy fizycznej, do identyfikacji protokołów wykorzystując specyfikację 802.2 w warstwie LLC. W roku 1989 instytut IEEE wydał rozszerzenie standardu 802.5, definiujące działanie 16 Mb/s sieci Token-Ring.

Sieć Token-Ring opiera się na transmisji jednokierunkowej, w której każde urządzenie zawsze odbiera komunikaty od swojego sąsiada „pod prąd" (poprzedzającego), a wysyła je do swojego sąsiada „z prądem" (następującego). Wykorzystuje ona topologię *pierścienia* (ring) z *przekazywaniem żetonu* (token-passing), w której ramki przekazywane są bez narażania się na kolizje (w danej chwili może nadawać tylko jedno urządzenie). Urządzenia uzyskują dostęp do nośnika i mogą nadawać po odebraniu wolnego żetonu, czyli 3-bajtowego sygnału krążącego wokół pierścienia.

Sieć Token-Ring ma następujące ważne cechy charakterystyczne:

- Wszystkie urządzenia są połączone szeregowo, transmitując sygnał w jednym kierunku.
- Przewód nadający każdego urządzenia jest pośrednio połączony z przewodem odbierającym swojego sąsiada „z prądem".
- Transmisja sygnału jest jednokierunkowa.
- Wszystkie urządzenia są bezpośrednio połączone w gwiazdę fizyczną za pomocą centralnych *koncentratorów MSAU* (MSAU, Multi-Station Access Unit), widocznych na rysunku 1.12. Koncentratory MSAU podtrzymują działanie pierścienia, elektrycznie ignorując niedziałające (wyłączone lub zepsute) urządzenia i porty.
- Karta sieciowa każdego urządzenia działa jak w pełni funkcjonalny jednokierunkowy *wtórnik* (repeater), całkowicie regenerujący sygnał i powtarzający go.
- Sieć działa z szybkością 4 Mb/s albo 16 Mb/s (nigdy z obiema naraz), wyznaczoną przez konfigurację kart sieciowych.
- Wszystkie urządzenia muszą uzgadniać szybkość pierścienia.



RYSUNEK 1.12. Działanie sieci Token-Ring

Odbijanie bitowe

Termin „bitowe powtarzanie" (bit repeating) oznacza w branży wzmocnienie (amplifikację) i odnowienie (regenerację) odebranego sygnału, powtarzanego na zewnątrz pozostałymi interfejsami.

Metoda dostępu do kanału

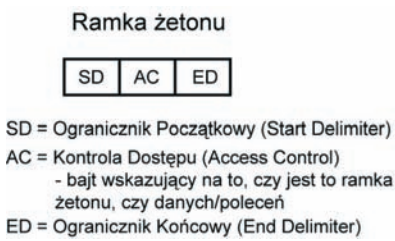
Urządzenia sieci Token-Ring uzyskują dostęp do kanału metodą przekazywania żetonu. Gdy urządzenie ma informacje do nadania, czeka na wolny żeton (3-bajtową ramkę przemieszczającą się po pierścieniu i zapewniającą dostęp do nośnika). Po otrzymaniu żetonu może przekształcić go w ramkę.

Stacje wysyłają swoje ramki wokół pierścienia z nadzieją, że odnajdą one hosta docelowego. Pozostałe urządzenia na pierścieniu sprawdzają adres docelowy tej ramki (stwierdzają w ten sposób, czy jest przeznaczona dla nich), po czym powtarzają bitowo ten sygnał. Każda karta sieciowa działa jak wtórnik, wzmacniając, ponownie taktując i powtarzając bitowo sygnały. Za usunięcie własnej ramki i wypuszczenie nowego żetonu odpowiada urządzenie wysyłające.

Ramki Token-Ring

Istnieją dwa typy ramek sieci Token-Ring: ramka żetonu i ramka danych/poleceń. Na rysunku 1.13 pokazano ramkę żetonu. Stacje rozpoznają sygnał jako wolny żeton, sprawdzając stan bitu żetonu w obrębie pola AC. Jeśli bit ten zawiera 0, jest to właśnie ramka żetonu. Wielkości SD i ED wyznaczają po prostu początek i koniec ramki. Z kolei na rysunku 1.14 widać ramkę służącą do transmisji danych i poleceń. Warto zapamiętać, że pole MAC/LLC za polem SA (Adres Źródłowy) wskazuje na to, czy ramka zawiera polecenie (MAC), czy też dane (LLC).

RYSUNEK 1.13. 3-bajtowy sygnał okrąża pierścień, zapewniając przyłączonym urządzeniom dostęp do kanału



RYSUNEK 1.14. Struktura ramki Token-Ring z opisem pól

FDDI i ANSI X3T9.5

FDDI (Fiber Distributed Data Interface — „interfejs danych rozprowadzanych światłowodem") jest to typ dostępu do nośnika, zdefiniowany przez specyfikację X3T9.5 *Amerykańskiego Instytutu Norm Krajowych* (ANSI, American National Standards Institute). Technologia ta również wykorzystuje schemat adresowania MAC, jednak istotnie różni się od technologii Ethernet i Token-Ring: do adresów MAC odwołuje się za pomocą symboli 4-bitowych, a nie w postaci 6-bajtowej.

Technologia FDDI obejmuje przekazywanie żetonu w topologii fizycznej *pierścienia podwójnego* (dual-ring), zapewniającej nadmiarowość z samonaprawianiem. Gdy dzieje się coś złego z pierścieniem podstawowym, zastępuje go pierścień drugorzędny. Po awarii dane są przekierowywane z pierścienia podstawowego w przynajmniej dwa miejsca pierścienia drugorzędnego. Jest to tzw. ***zawijanie pierścienia*** (***ring wrap***).

Kiedyś interfejs FDDI, ze względu na maksymalną szybkość transmisji 100 Mb/s oraz — w przeciwieństwie do miedzi — odporność na *interfencje elektromagnetyczne(EMI) i radiowe (RFI)*, był ulubionym standardem sieci szkieletowych. Okablowanie światłowodowe ma w istocie przewagę nad konwencjonalnym kablem miedzianym w następujących dziedzinach:

- szybkości przemieszczania się danych,
- odległości sygnału osiąganej przed tłumieniem,
- odporności na EMI i RFI,
- nadmiarowości zapewnianej przez dodatkowy pierścień.

Uwaga

Niegdyś FDDI był ulubionym standardem sieci szkieletowych, jednak w wielu miejscach zastąpiono go tańszym Szybkim lub Gigabitowym Ethernetem.

Metoda dostępu do kanału

FDDI transmituje pakiety metodą przekazywania żetonu. Dostęp do nośnika fizycznego (pierścienia) odbywa się za pośrednictwem żetonu przekazywanego wokół niego. Węzeł chcący nadawać po prostu chwyta żeton, wysyła swoją transmisję, a następnie wypuszcza na pierścień nowy żeton. W przeciwieństwie do sieci Token-Ring, umożliwiających krążenie tylko jednego żetonu naraz, sieci FDDI umożliwiają krążenie wielu żetonów w dowolnym danym czasie.

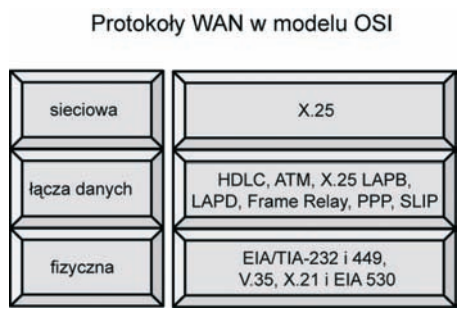
Uwaga

Dostawcy sieci Token-Ring co prawda zaimplementowali wczesne wypuszczanie żetonu (early token release), umożliwiające równoczesne występowanie wielu transmisji na pierścieniu, jednak dopuszczalny jest i tak tylko jeden żeton.

Technologie sieci rozległych (WAN)

Technologie *sieci rozległych* (WAN, Wide Area Network) wykorzystują możliwości transmisyjne, oferowane przez ogólnie dostępne nośniki (np. dostawców usług lub operatorów telefonii), do przesyłania danych na duże odległości. Technologie te dotyczą dwóch najniższych warstw modelu OSI (rysunek 1.15).

RYSUNEK 1.15. Przypisanie protokołów sieci WAN do modelu OSI



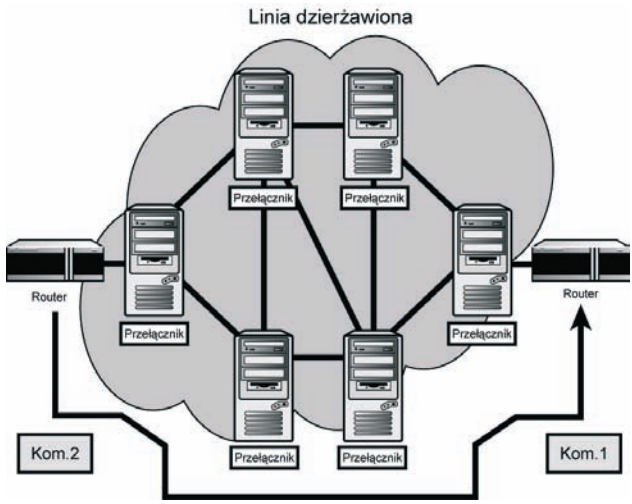
Połączenia WAN umożliwiają firmom łączenie się z oddalonymi ośrodkami i tym samym rozszerzanie własnych sieci. Większość firm, posiadających rozsiane na znacznym obszarze oddziały, musi korzystać z jakiegoś rodzaju połączeń WAN (w zależności od potrzeb firmy). Istnieją 3 typy połączeń WAN, służących do przesyłu danych za pośrednictwem sieci zewnętrznej (patrz tabela 1.6):

- **Linia dzierżawiona** (leased), **czyli dedykowana** — inaczej zwana linią „od punktu do punktu" (point-to-point), korzysta z synchronicznego połączenia szeregowego za pośrednictwem sieci dostawcy usług.
- **Z przełączaniem obwodów** (circuit-switched) — posiada dedykowaną ścieżkę obwodową, korzystając z asynchronicznego połączenia szeregowego za pośrednictwem sieci operatora telefonii.
- **Z przełączaniem pakietów** (packet-switched) — wykorzystuje synchroniczne połączenie szeregowe za pośrednictwem sieci dostawcy usług.

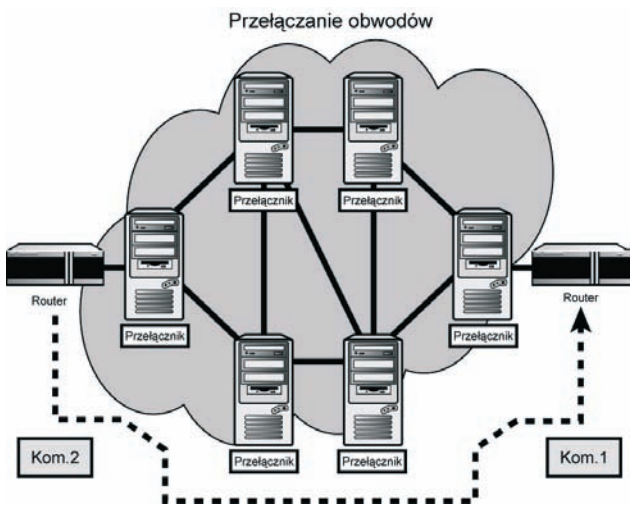
TABELA 1.6. Typy połączeń WAN

Typ połączenia	Opis
Linia dzierżawiona (czyli dedykowana lub „od punktu do punktu")	Tworzy wydzieloną ścieżkę komunikacyjną za pośrednictwem sieci dostawcy usług, prowadzącą od klienta do sieci zdalnej. Dostawcy usług rezerwują połączenie i szerokość pasma do prywatnego użytku klienta. Gwarantuje dostęp do pełnej szerokości pasma. Jego wada to kosztowność — połączenie jest zawsze aktywne (nawet gdy jest nieużywane). Wykorzystuje synchroniczne połączenia szeregowe o maksymalnej szybkości E3 (45 Mb/s). Obsługuje hermetyzację PPP, SLIP i HDLC (warstwy Łącza Danych).
Z przełączaniem obwodów (circuit--switching)	Dla każdej sesji tworzony jest „w locie" dedykowany obwód, który musi istnieć między nadawcą a odbiorcą przez cały czas trwania transmisji. Powszechnie stosowane w środowiskach wymagających jedynie minimalnego lub rzadkiego użytkowania sieci WAN. Wykorzystuje asynchroniczne połączenia szeregowe za pośrednictwem standardowych linii telefonicznych lub połączeń ISDN. Obsługuje hermetyzację PPP, SLIP i HDLC.
Z przełączaniem pakietów (packet--switching)	Urządzenia sieciowe korzystają ze wspólnych łączy „od punktu do punktu", zapewniających dostarczanie pakietów ze źródła do celu za pośrednictwem sieci usługodawcy (dostawcy usług). Połączenie źródła z celem ustanawiane jest w oparciu o tymczasowe *obwody wirtualne* (VC, Virtual Circuits). Urządzenia przełączające ustanawiają obwód wirtualny i w oparciu o urządzenia zwielokrotniające zapewniają klientom wspólny dostęp do niego. Tańsze — obwód nie jest dedykowany. Wykorzystuje połączenia synchroniczne o szybkości od 56 Kb/s do E3. Obsługuje hermetyzację X.25, ATM i Frame Relay.

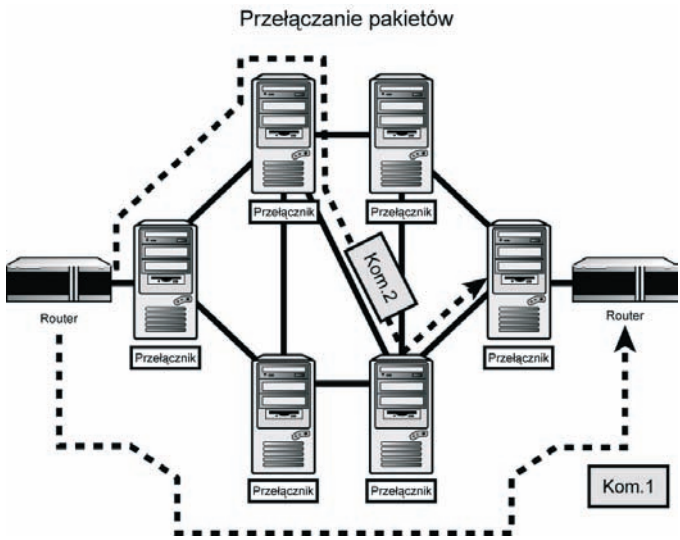
Na rysunkach 1.16 – 1.18 przedstawiono różne typy połączeń WAN. Linia dzierżawiona, inaczej ***linia dedykowana***, tworzy wydzieloną ścieżkę komunikacji WAN za pośrednictwem sieci usługodawcy — od klienta do sieci zdalnej (rysunek 1.16). Na rysunku 1.17 widać ścieżkę tworzoną „w locie" dla połączenia WAN z przełączaniem obwodów, zaś na rysunku 1.18 — przykład przełączania pakietów.



RYSUNEK 1.16. Linie dzierżawione bywają kosztowne, gdyż połączenie pozostaje aktywne nawet gdy jest nieużywane



RYSUNEK 1.17. Przełączanie obwodów wymaga ustanawiania i zrywania połączenia dla każdej sesji między nadawcą a odbiorcą



RYSUNEK 1.18. Przełączanie pakietów przekazuje pakiety od węzła do węzła, zajmując kanał tylko na czas trwania transmisji

Większość połączeń WAN jest obecnie zapewniana przez dostawców usług i operatorów telefonicznych. Dzięki routerom możliwy jest dostęp do serwerów zapewniających połączenia *komutowane* (dial-up) z przełączaniem obwodów, realizowane za pośrednictwem standardowych modemów analogowych, bądź *routing połączeń na żądanie* (DDR, Dial-on-Demand Routing) poprzez linie analogowe lub ISDN. Łącza dzierżawione (dedykowane) można skonfigurować za pomocą urządzeń CSU/DSU tak, aby spójnie obsługiwały duże ilości ruchu sieciowego przez synchroniczne złącza szeregowe. Połączenia przełączane pakietowo, np. X.25, ATM i Frame Relay, muszą korzystać ze *multiplekserów* (MUX, Multiplexer) i *demultiplekserów* (DEMUX, Demultiplexer), zapewniających urządzeniom wspólny dostęp do tego samego obwodu. Dzięki dowolnej z tych metod można dostarczać dane do ośrodków zdalnych na całym świecie za pośrednictwem sieci dowolnego usługodawcy.

Protokoły hermetyzacji WAN

Hermetyzacja WAN (***WAN encapsulation***) polega na przygotowaniu pakietu tak, aby umożliwić mu przemieszczanie się przez siatkę odległych od siebie sieci. Internet opiera się na wielu różnych typach połączeń WAN, w tym dedykowanych i niededykowanych. W każdym takim połączeniu lokalne dane sieci LAN muszą zostać przekształcone poprzez hermetyzację w ramki, a dopiero potem mogą przejść przez łącze WAN. Aby skonfigurować odpowiedni typ hermetyzacji warstwy łącza danych, trzeba znać właściwy protokół (zależny od stosowanej technologii WAN). Każdy usługodawca powinien udzielać specyficznych informacji konfiguracyjnych, pozwalających na udane podłączanie się do jego sieci WAN.

Interfejs do sieci usługodawcy mogą zapewniać różne opcje. Wszystkie one są odmianami protokołu *HDLC* (High-level Data Link Control) — szeroko stosowanego

standardu wprowadzonego przez organizację ISO, wzorowanego na protokole *SDLC* (Synchronous Data Link Control) firmy IBM. Protokoły te działają w warstwie łącza danych modelu OSI, zapewniając usługi połączeniowe i bezpołączeniowe tej warstwy aplikacjom warstw wyższych i danym użytkownika przy przechodzeniu przez sieć WAN.

Większość protokołów WAN pochodzi od potomków HDLC. Istnieje szereg implementacji tego ostatniego, pochodzących od różnych dostawców, i nie wszystkie są kompatybilne. Na przykład firma Cisco stworzyła implementację wewnątrzfirmową, niezgodną ze wszystkimi innymi. Bardzo podobnie działa protokół SDLC firmy IBM, stosowany w jej technologii sieciowej *SNA* (Systems Network Architecture), zapewniając połączeniowe, niezawodne dostarczanie danych pomiędzy komputerami mini- i mainframe IBM a ich klientami. Wszelkie inne protokoły, np. LAPB sieci X.25, LAPD sieci ISDN, a nawet LLC2, są tylko podzbiorami HDLC. Opis podstawowych protokołów hermetyzacji zawiera tabela 1.7.

Dokumenty RFC

Technologie TCP/IP nie mają właściciela, nie da się zatem uzyskać od ich dostawców informacji na ten temat w formie dokumentów, zasad, protokołów ani standardów. Tym niemniej informacje te są bezpośrednio dostępne za darmo w postaci dokumentów RFC (RFC, Request For Comments, ang. Wezwanie do komentarzy). Choć dostawcy publikują dokumentację dotyczącą własnych implementacji tych technologii, standardy leżące u ich podstaw — opisujące funkcje, reguły i metody implementacji protokołów — zawarte są w dokumentach RFC, interpretowanych właśnie przez dostawców.

Dokumenty RFC mają postać szeregu raportów technicznych, pisanych przez komitety, osoby i korporacje rozwijające protokoły, zasady, implementacje, itp. Pojawiają się w kolejności chronologicznej: poprawione RFC zajmuje miejsce swojego poprzednika i dostaje nowy numer. Należy zwracać uwagę, żeby zawsze korzystać z najnowszych RFC.

RFC mogą być różne — od dokumentacji technicznej protokołu do sugestii zmian, czy nawet propozycji nowych protokołów — a pod względem stylu od suchych i akademickich do żartobliwych. W tej książce traktujemy je jako materiały referencyjne. Poza tym w dodatku A znajduje się lista RFC podzielona na kategorie. Są one dostępne też w sieci WWW: *http://www.faqs.org/rfcs/*.

TABELA 1.7. Podstawowe protokoły hermetyzacji WAN

Typ protokołu	Opis
Frame Relay: hermetyzacja Cisco; hermetyzacja IETF (standardowe, wg RFC 1490).	Ustanawia wiele wirtualnych ścieżek logicznych lub obwodów wirtualnych. Działa w warstwach łącza danych i fizycznej. Bardziej wydajny od X.25, gdyż nie ustanawia połączeń i nie stosuje poprawiania ani usuwania błędów. Zakłada, że większość sieci jest niezawodna fizycznie i ma niską stopę błędów. W dziedzinie wykrywania i usuwania błędów polega na protokołach warstw wyższych. Obsługuje kontrolę przeciążenia sieci.
ISDN (Integrated Services Digital Network)	Transmituje dane, głos i innych ruch źródłowy poprzez istniejące linie telefoniczne. Wykorzystuje dwa typy kanałów: D i B. Kanał D przenosi informacje sygnalizacyjne i kontrolne, a kanał B dane. Istnieją dwa główne typy usług ISDN: *BRI* (Basic Rate ISDN), o całkowitej szybkości 144 Kb/s, oraz *PRI* (Primary Rate ISDN), o całkowitej szybkości 1,544 Mb/s (w USA, Kanadzie i Japonii) lub 2,048 Mb/s (w Europie).
LAPB (Link Access Protocol Balanced) sieci X.25, hermetyzacja dla kanału sygnalizacyjnego	Pochodny od HDLC protokół połączeniowy stosu X.25, zapewniający wykrywanie i usuwanie błędów w warstwie drugiej. Wyjątkowo niezawodny, choć wolny, ze względu na duży koszt ogólny utrzymywania połączeń. Warty stosowania w sieciach WAN podatnych na błędy. Generalnie zastępowany przez Frame Relay i inne standardy WAN.
HDLC (High-level Data Link Control)	Protokół połączeniowy wprowadzony przez ISO. Nie obsługuje uwierzytelniania ani kompresji danych. Ponieważ nie potrafi identyfikować typu protokołów przenoszonych wewnątrz swoich kapsuł, może przenosić tylko jeden protokół naraz. Implementacje dostawców różnią się.
PPP (Point-to-Point Protocol)	Zapewnia ścieżkę komunikacyjną od klienta poprzez ustanowione połączenie asynchroniczne WAN oraz połączenie synchroniczne poprzez sieć firmy komunikacyjnej do sieci zdalnej. Obsługuje wiele protokołów, np. IP, IPX i AppleTalk, a także uwierzytelnianie kompresji danych, wykrywanie błędów i łączenie połączeń (multilinking).
SLIP (Serial Line Internet Protocol)	Starszy protokół obsługujący połączenia szeregowe „od punktu do punktu" z wykorzystaniem TCP/IP. Zastępowany przez PPP.
ATM (Asynchronous Transfer Mode)	Międzynarodowy standard technologii przełączania i zwielokrotniania opartej na komórkach. Obsługuje wiele typów usług (głos, wideo i dane) za pośrednictwem komórek o stałej długości (53-bajtowych), zmniejszających koszt ogólny przetwarzania i opóźnienie tranzytu. Zapewnia transmisję przez linie miedziane lub światłowodowe z szybkością od 1,544 Mb/s (usługa T1) do 622 Mb/s (OC-12).

Internet kontra intranet

Jak wiadomo koniak to brandy, ale nie każda brandy to koniak. To samo dotyczy ***Internetu*** i ***intranetu***. Nazwa ***intranet*** (z małej litery) oznacza wiele sieci w obrębie firmy, połączonych ze sobą i wewnętrznie komunikujących się w oparciu o centralny

nadzór (algorytm). Z kolei ***Internet*** (z dużej litery) pozwala bardzo wielu osobom (hostom) z różnych organizacji na całym świecie porozumiewać się ze sobą za pomocą TCP/IP bez żadnej kontroli. Tak, jak brandy nie dorównuje koniakowi (choć ma podobny skład), tak samo ***intranet*** nie dorównuje ***Internetowi***.

Grupy odpowiedzialne za technologię Internetu

Branża ciągle się zmienia i może się wydawać, że nowe protokoły i standardy pojawiają się „z powietrza". Tym niemniej technologiami internetowymi rządzą cztery grupy:

- ***ISOC*** (***Internet Society***) — organizacja nie czerpiąca dochodów ze swojej działalności, popierająca zainteresowanie Internetem. Kieruje organizacją IAB (por. niżej).
- ***IAB*** (***Internet Architecture Board***) — mała grupa międzynarodowych ochotników, ustalająca zasady zwiększające jakość standardów Internetu (TCP/IP). Podlega ISOC.
- ***IETF*** (***Internet Engineering Task Force***) — mała grupa ukierunkowana na opracowywanie standardów, podzielona na grupy zajmujące się konkretnymi dziedzinami TCP/IP i Internetu. Każda dziedzina ma niezależnego kierownika i grupy robocze.
- ***IRTF*** (***Internet Research Task Force***) — grupa pracująca nad projektami badawczymi związanymi z TCP/IP i Internetem.

Podsumowanie

Model referencyjny OSI powstał po to, aby bez kłopotu mogły komunikować się ze sobą systemy podobne i niepodobne. Oferuje on producentom i dostawcom jednolity schemat architektoniczny, składający się z siedmiu warstw: aplikacji, prezentacji, sesji, transportowej, Sieciowej, łącza danych i fizycznej.

Model OSI zapewnia korzyści producentom sprzętu i projektantom oprogramowania oraz inżynierom sieciowym oferującym pomoc techniczną i rozwiązywanie problemów. Dzięki kategoryzacji funkcji poszczególnych warstw zawęża on zakres jej odpowiedzialności, tym samym ułatwiając producentom i inżynierom sieciowym projektowanie i obsługę.

Pytania sprawdzające

1. Dlaczego model OSI jest taki ważny i czemu został utworzony?
2. Która warstwa modelu OSI zarządza dialogiem komunikacyjnym (całkowicie lub połowicznie dwukierunkowym) między usługami?
3. Która warstwa zapewnia obsługę błędów i sterowanie przepływem, a także gwarantowane dostarczanie danych?

4. W której warstwie modelu OSI występuje przełączanie?
5. W której warstwie modelu OSI działają protokoły IP i ICMP?
6. Jakie są cztery warstwy modelu DoD?
7. Jakie są dwie funkcje warstwy łącza danych?
8. Jaki protokół warstwy transportowej jest bezpołączeniowy?