

IDŹ DO

PRZYKŁADOWY ROZDZIAŁ



SPIS TREŚCI

KATALOG KSIĄŻEK

KATALOG ONLINE

ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK

DODAJ DO KOSZYKA

CENNIK I INFORMACJE

ZAMÓW INFORMACJE
O NOWOŚCIACH

ZAMÓW CENNIK

CZYTELNIA

FRAGMENTY KSIĄŻEK ONLINE

TCP/IP. Biblia

Autorzy: Rob Scrimger, Paul LaSalle, Clay Leitzke,
Mridula Parihar, Meeta Gupta

Tłumaczenie: Adam Jarczyk

ISBN: 83-7197-668-2

Tytuł oryginału: [TCP/IP Bible](#)

Format: B5, stron: 576



Niniejsza książka, wypełniona przejrzystymi objaśnieniami i praktycznymi rozwiązaniami sieciowymi, jest doskonałym przewodnikiem po TCP/IP zarówno dla doświadczonych administratorów potrzebujących wszechstronnej publikacji informacyjnej, jak i dla osób szukających materiałów pomocnych w przygotowaniach do egzaminów. Dwaj eksperci w dziedzinie TCP/IP wraz z profesjonalistami z NIIT – wiodącej informatycznej firmy szkoleniowej, prowadzą Czytelnika krok po kroku przez szczegóły tego niezastąpionego protokołu sieciowego i internetowego, zaczynając od architektury i konfiguracji, a na aplikacjach i implementacji kończąc. Czytelnik znajdzie tu wszystko, co potrzebne do uruchomienia i wyregulowania sieci TCP/IP oraz do najbardziej wydajnego wykorzystania aplikacji TCP/IP.

- Model odniesienia OSI, topologie sieci i inne podstawy techniki sieciowej
- Funkcjonowanie każdej warstwy architektury TCP/IP
- Instalacja i konfiguracja TCP/IP w systemach Unix, Linux i Windows
- Rozwiązywanie nazw, obejmujące nazwy hostów, FQDN i NetBIOS
- Szczegóły narzędzi służących do zdalnego wykonywania poleceń, serwerów WWW, usług informacyjnych dla przedsiębiorstw i innych aplikacji TCP/IP
- Wybór schematu adresowania i projekty trasowania dla sieci TCP/IP
- Planowanie rozmieszczenia serwerów sieciowych i zdalnego dostępu
- Zabezpieczanie, monitorowanie i rozwiązywanie problemów z sieciami TCP/IP



Rzut oka na książkę

O Autorach.....	15
Wstęp	17
Część I Wprowadzenie do transmisji TCP/IP	19
Rozdział 1. Podstawy działania sieci komputerowych	21
Rozdział 2. Architektura protokołu TCP/IP.....	45
Rozdział 3. Warstwa fizyczna.....	65
Rozdział 4. Warstwa interfejsu sieciowego	85
Rozdział 5. Warstwa internetowa	99
Rozdział 6. Warstwa transportowa	125
Rozdział 7. Warstwa aplikacji	143
Część II Praca z TCP/IP	157
Rozdział 8. Instalacja i konfiguracja TCP/IP.....	159
Rozdział 9. Konfiguracja automatyczna	179
Rozdział 10. Znajdowanie hostów w sieci IP	195
Część III Popularne aplikacje TCP/IP	223
Rozdział 11. Dostęp do Internetu.....	225
Rozdział 12. Narzędzia do obsługi plików	255
Rozdział 13. Narzędzia zdalnego wykonywania poleceń.....	271
Rozdział 14. Drukowanie przez sieć.....	291
Rozdział 15. Aplikacje i protokoły WWW.....	305
Rozdział 16. Dostęp do poczty elektronicznej i grup dyskusyjnych	329
Rozdział 17. Usługi informacyjne dla przedsiębiorstw	345
Część IV Tworzenie i utrzymanie sieci TCP/IP.....	363
Rozdział 18. Wybór schematu adresowania	365
Rozdział 19. Projektowanie trasowania dla sieci.....	383
Rozdział 20. Planowanie rozmieszczenia serwerów	411
Rozdział 21. Wprowadzenie do łączności	429
Rozdział 22. Planowanie bezpieczeństwa sieci	445
Rozdział 23. Rozwiązywanie problemów z siecią i łącznością.....	463
Rozdział 24. Monitorowanie sieci TCP/IP	481
Rozdział 25. Plany na przyszłość.....	505
Dodatki	515
Dodatek A Domeny DNS najwyższego poziomu.....	517
Skorowidz	557

Spis treści

O Autorach	15
Wstęp.....	17
Część I Wprowadzenie do transmisji TCP/IP	19
Rozdział 1. Podstawy działania sieci komputerowych.....	21
Co to jest sieć komputerowa?	21
Elementy składowe sieci	22
Rodzaje konfiguracji sieci	22
Sieci zdecentralizowane	22
Sieci scentralizowane	23
Model odniesienia OSI	24
Warstwa aplikacji	26
Warstwa prezentacji	26
Warstwa sesji.....	27
Warstwa transportowa.....	28
Warstwa sieciowa.....	28
Warstwa łącza danych.....	29
Warstwa fizyczna	29
Podział sieci według zasięgu	30
Sieci lokalne	30
Sieci rozległe	30
Model z projektu IEEE 802	31
Topologie sieci	32
Topologia magistrali.....	32
Topologia gwiazdy	33
Topologia pierścienia	33
Topologia oczkowa	34
Topologie hybrydowe.....	34
Infrastruktura sieciowa	35
Regeneratory	36
Karta interfejsu sieciowego.....	36
Koncentrator	36
Przełącznik	37
Most.....	37
Ruter	37
Bruter.....	37
Brama	38

Wprowadzenie do TCP/IP	38
Request for Comments	38
Model odniesienia TCP/IP	40
Przegląd adresowania IP	42
Aplikacje TCP/IP	43
Rozdział 2. Architektura protokołu TCP/IP	45
Pięciowarstwowa architektura TCP/IP	45
Warstwa fizyczna	47
Warstwa interfejsu sieciowego	53
Warstwa internetowa	56
Warstwa transportowa	57
Warstwa aplikacji	59
Łączność pomiędzy warstwami	60
Format nagłówka warstwy transportowej	62
Format nagłówka warstwy internetowej	63
Rozdział 3. Warstwa fizyczna	65
W jaki sposób sygnał przesyłany jest kablem	65
Metody transmisji (metody sygnalizacji)	66
Technologie i mechanizmy transmisji	67
Nośniki fizyczne	70
Modemy	74
Nośniki bezprzewodowe	75
Najczęściej stosowane topologie	77
Magistrala	77
Token Ring	79
Gwiazda	80
FDDI	81
Sieci ATM	82
Rozdział 4. Warstwa interfejsu sieciowego	85
Warstwa interfejsu sieciowego — omówienie	85
Zawartość ramki Ethernet	86
Typowe składniki pakietu sieciowego	88
Standardy sterowania dostępem do nośnika	89
Ethernet	89
ARCnet	91
Token Ring	91
ATM	92
Odwzorowanie adresów fizycznych na adresy IP	94
ARP i RARP	94
ATMARP	97
Rozdział 5. Warstwa internetowa	99
Przeznaczenie warstwy internetowej	99
Ustalenie, czy adres docelowy jest lokalny czy odległy	100
Wprowadzenie do trasowania	101
Adresy IP	101
Notacja dwójkowa i dziesiętna	102
Identyfikatory sieci i hostów	104

Klasy adresów IPv4	105
O czym informuje adres IP	106
Jak stosuje się maskę podsieci	107
Brama domyślna	107
Ustalenie czy adres docelowy jest lokalny, czy zdalny	108
Podstawy trasowania	109
Rutery sprzętowe i programowe	110
Typy tras	110
Zawartość datagramu IP	115
Nagłówek IP	115
Ładunek IP	116
Protokół ICMP	116
Przeznaczenie ICMP	116
Pakiety ICMP	117
Protokół IGMP	119
Wprowadzenie do transmisji grupowych	120
Do czego służy adresowanie grupowe	122
Pakiety IGMP	122
Rozdział 6. Warstwa transportowa	125
Typy przesyłu danych	125
Dostawy wiarygodne i dostawy nie gwarantowane	128
Dostawy stanowe i bezstanowe	128
Bezpołączeniowe przesyłanie danych	130
Połączeniowe przesyłanie danych	132
Inicjacja sesji	133
Maksymalny rozmiar segmentu	137
Okna nadawania i odbioru TCP	137
Okno przeciążenia	138
Algorytm powolnego startu	139
Nagłówek TCP	139
Rozdział 7. Warstwa aplikacji	143
Przegląd portów	143
Dobrze znane numery portów	144
Gniazda — wprowadzenie	147
Dwukierunkowa łączność oparta na gniazdach	147
RPC	153
Część II Praca z TCP/IP	157
Rozdział 8. Instalacja i konfiguracja TCP/IP	159
Konfiguracja TCP/IP	159
Informacje potrzebne zawsze	159
Informacje potrzebne czasami	160
Konfiguracja TCP/IP w świecie Linuksa	161
Instalacja i konfiguracja TCP/IP w świecie Microsoftu	169
Instalacja TCP/IP w systemach operacyjnych Microsoftu	169
Ręczna konfiguracja TCP/IP	172
Kontrola konfiguracji IP	177

Rozdział 9. Konfiguracja automatyczna	179
Wprowadzenie do konfiguracji automatycznej	179
Korzyści z konfiguracji automatycznej	180
Konfiguracja w sieciach wielosegmentowych	181
Protokół BOOTP	181
Proces ładowania początkowego BOOTP	182
Zawartość pakietu BOOTP	182
Rutery obsługujące protokół BOOTP	184
Wady protokołu BOOTP	185
DHCP	185
Dzierżawy DHCP	186
Opcje zakresu i serwera	189
Pakiet DHCP	190
Opcje serwera DHCP	191
Trasowanie DHCP	192
Rozdział 10. Znajdowanie hostów w sieci IP	195
Przegląd nazw hostów	195
Podstawowe nazwy hostów	197
Pełne złożone nazwy domen	197
Nazwy kanoniczne i aliasy	197
Lokalny plik HOSTS	199
Format pliku HOSTS	199
Rozwiązywanie nazw	200
Wykorzystanie usługi DNS do rozwiązywania nazw hostów	200
Czym jest domena?	202
Serwery nazw	202
Resolwery	202
Przestrzeń nazw	202
Strefy w obrębie przestrzeni nazw	205
Tworzenie pliku strefy	207
Zapytania iteracyjne i rekurencyjne	210
Konfiguracja DNS-u z wykorzystaniem programu BIND	211
Konfiguracja Windows 2000	212
Rozwiązywanie nazw NetBIOS	214
Nazwy NetBIOS — co to jest?	214
Składniki sieciowe Microsoftu	215
Rozwiązywanie nazw NetBIOS przed Windows 2000	216
Rozwiązywanie nazw NetBIOS w Windows 2000	220
Część III Popularne aplikacje TCP/IP	223
Rozdział 11. Dostęp do Internetu	225
Przegląd międzysieci prywatnych i publicznych	226
Adresowanie w sieciach prywatnych	227
Ograniczenia IPv4	229
Łączenie się z Internetem	231
Dostawcy usług internetowych	233
Wykorzystanie zapór firewall	234
Rola zapór firewall	234
Typy zapór firewall	236
Najczęściej stosowane konfiguracje sieci z zaporami firewall	239

Stosowanie NAT.....	242
Korzyści ze stosowania NAT	245
Przezroczysty czy nieprzezroczysty	246
Wykorzystanie serwera proxy	246
Udostępnianie połączenia internetowego Microsoftu	247
Wirtualne sieci prywatne	248
PPTP	251
Layer-2 Tunneling Protocol	253
Rozdział 12. Narzędzia do obsługi plików	255
NFS	255
Wprowadzenie do NFS	255
Usługi NFS	257
Zagadnienia bezpieczeństwa w NFS	258
Wersje NFS	258
Konfiguracja serwera NFS	260
DFS	263
Wprowadzenie do DFS	263
Katalogi główne DFS: autonomiczny i domeny	264
Konfiguracja DFS w Windows 2000	264
Narzędzia do przesyłania plików	266
FTP	266
TFTP	268
Remote Copy Protocol	268
Rozdział 13. Narzędzia zdalnego wykonywania poleceń.....	271
Przegląd narzędzi zdalnego wykonywania poleceń	271
Telnet.....	272
Remote login	278
Remote shell (rsh)	280
Secure shell (ssh).....	281
Remote execute (rexec).....	284
Serwery terminali	284
Sun Ray	285
Microsoft Terminal Server	287
Citrix.....	289
Rozdział 14. Drukowanie przez sieć.....	291
Wprowadzenie do drukowania	291
Drukowanie w środowisku linuksowym	292
Drukowanie w systemach Microsoftu.....	294
Drukowanie z klienta.....	295
Konfiguracja serwera lpd.....	296
Zdalne drukarki w systemach Unix i Linux	296
Narzędzie printtool	297
Łączenie z lokalną drukarką.....	297
Łączenie ze zdalną drukarką	299
Polecenia związane z drukowaniem.....	301
Internet Printing Protocol Microsoftu.....	304
Administratorzy.....	304
Pozostali użytkownicy.....	304

Rozdział 15. Aplikacje i protokoły WWW	305
Podstawy WWW	305
Internet — wprowadzenie	305
Ewolucja WWW.....	306
Jak funkcjonuje WWW	307
HTML.....	308
HTTP.....	310
World Wide Web Consortium.....	311
Aplikacje WWW	313
Serwery WWW	313
Aplikacje w Internecie.....	314
Języki.....	316
Bezpieczeństwo w Sieci	322
Handel elektroniczny w Internecie.....	324
Wideo i inne zaawansowane typy danych.....	325
Potokowa transmisja audio i wideo.....	325
Co trzeba brać pod uwagę przy transmisji potokowej	327
Rozdział 16. Dostęp do poczty elektronicznej i grup dyskusyjnych.....	329
Wprowadzenie do poczty elektronicznej.....	329
SMTP	331
POP.....	332
IMAP.....	333
Czytanie poczty	334
MIME i S/MIME.....	336
PGP.....	339
Grupy dyskusyjne — wprowadzenie.....	339
Serwery i koncentratory	341
NNTP	342
Netykieta	343
Rozdział 17. Usługi informacyjne dla przedsiębiorstw.....	345
Wprowadzenie do sieciowych usług katalogowych	345
Standard X.500	347
LDAP	350
NIS	353
NIS+	355
STDS	356
Network Directory Service Novella	357
Active Directory	360
Część IV Tworzenie i utrzymanie sieci TCP/IP	363
Rozdział 18. Wybór schematu adresowania.....	365
Szacowanie potrzeb dotyczących adresów	365
Fizyczna konfiguracja sieci.....	365
Lokalizacje obsługiwane przez sieć	366
Wymogi wydajności.....	367
Adresy publiczne i prywatne	369
Uzyskanie adresu i połączenia z Internetem.....	369
Obliczanie potrzeb adresowych.....	370

Podział na podsieci	375
Obliczanie ID lokalizacji	375
Obliczanie ID podsieci	379
Ustalenie adresów hostów	380
Rzut oka na nadsieci	381
Rozdział 19. Projektowanie trasowania dla sieci.....	383
Podstawy trasowania	383
Tablica tras	384
Budowanie tablicy tras	386
Statyczny wybór trasy	388
Tworzenie struktury trasowania	389
Łączenie podsieci	390
Maski podsieci o zmiennej długości	392
Podłączanie odległych biur	395
Dynamiczny wybór tras.....	396
ICMP Router Discovery.....	397
Protokół RIP	398
Protokół IGRP	403
OSPF	405
Rozdział 20. Planowanie rozmieszczenia serwerów.....	411
Ustalenie usług potrzebnych w sieci	411
Instalowanie usług w sieci.....	413
Łączenie usług	415
Planowanie równoważenia obciążenia i nadmiarowości	419
Dodawanie kolejnych systemów	419
Systemy wieloadresowe	421
Serwery hierarchiczne	422
Stosowanie grupowania.....	425
Rozdział 21. Wprowadzenie do łączności	429
Podstawy łączności.....	430
Łączenie lokalizacji	430
Budowanie własnej sieci WAN.....	437
Planowanie dostępu zdalnego.....	441
Wybór strategii połączeń telefonicznych	441
Praca zdalna.....	442
Rozdział 22. Planowanie bezpieczeństwa sieci.....	445
Szacowanie ryzyka	445
Równoważenie bezpieczeństwa i użyteczności.....	448
Zabezpieczanie sieci	449
Szyfrowanie transmisji danych	449
Uwierzytelnianie użytkowników.....	451
Jednoczesne stosowanie szyfrowania i uwierzytelniania.....	457
Rozdział 23. Rozwiązywanie problemów z siecią i łącznością	463
Proces rozwiązywania problemów	464
Sprawdzenie konfiguracji IP	465
Kontrola konfiguracji IP dla Microsoft Windows.....	465
Kontrola konfiguracji IP w systemach uniksowych.....	467

Testowanie łączności	468
Znajdowanie problemów z rozwiązywaniem nazw	474
Znajdowanie problemów z rozwiązywaniem nazw hostów	474
Znajdowanie problemów w rozwiązywaniu nazw NetBIOS	477
Weryfikacja klienta i serwera	480
Rozdział 24. Monitorowanie sieci TCP/IP	481
Monitorowanie sprzętu	482
Wymogi dla serwerów uwierzytelniających	482
Wymogi dla serwerów plików i drukowania	483
Wymogi dla serwerów aplikacji	483
Narzędzia monitorujące	484
Narzędzia do monitorowania sieci	487
Monitorowanie sieci za pomocą polecenia ping	487
Monitorowanie sieci za pomocą polecenia netstat	488
Monitorowanie sesji NetBIOS za pomocą narzędzia nbtstat	493
Przechwytywanie ruchu sieciowego za pomocą analizatorów pakietów	494
SNMP	498
Community name	499
System zarządzania SNMP	499
Agent SNMP	500
Baza informacji zarządzania	500
Regulacja rozmiaru okna TCP/IP	501
Rozdział 25. Plany na przyszłość	505
Wprowadzenie do IPv6	506
Zmiany w porównaniu z IPv4	507
Adresowanie IPv6	508
Bezprzewodowy Internet	508
Wireless Datagram Protocol	510
Wireless Transport Layer Security	510
Wireless Transaction Protocol	511
Wireless Session Protocol	511
Wireless Application Environment	511
Inteligentne urządzenia domowe	512
Planowanie na przyszłość	514
Dodatki	515
Dodatek A Domeny DNS najwyższego poziomu	517
Ogólne domeny najwyższego poziomu	517
Specjalne domeny najwyższego poziomu	517
Narodowe domeny najwyższego poziomu z poddomenami	518
Skorowidz	557

Rozdział 2.

Architektura protokołu TCP/IP

W tym rozdziale:

- ◆ Pięciowarstwowa architektura TCP/IP
- ◆ Łączność pomiędzy warstwami

To, co znamy obecnie pod nazwą „Internet”, zaistniało w roku 1968 jako projekt sponsorowany przez Departament Obrony (*Department of Defense*) rządu USA. Projekt ten usiłował połączyć różne centra badawcze wspierane przez Departament Obrony siecią o nazwie ARPANET (*Advanced Research Projects Agency Network*). Na początku funkcję standardowego protokołu połączeniowego pełnił *Network Control Protocol* (NCP). Jednak protokół ten okazał się niewystarczający dla sieci ARPANET, której rozmiary rosły w olbrzymim tempie, wobec tego w roku 1974 opracowany został TCP/IP. Nazwa TCP/IP (*Transmission Control Protocol and Internet Protocol*) w rzeczywistości odnosi się do dwóch protokołów, z których żaden nie jest używany samodzielnie. Tworzą one *pakiet protokołów* (ang. *protocol suite*), co oznacza hierarchiczny zbiór powiązanych protokołów. Z uwagi na rewolucyjną rolę, jaką TCP oraz IP odegrały w rozwoju sieci komputerowych, cały pakiet nosi nazwę pakietu protokołów TCP/IP.



Historia TCP/IP została opisana w rozdziale 1.

W niniejszym rozdziale poznamy pięć warstw, składających się na architekturę TCP/IP: fizyczną, sieciową, internetową, transportową i aplikacji. Czytelnik zapozna się z rolą, jaką te warstwy odgrywają w pomyślnym przesyłaniu danych z jednego komputera do drugiego. Przedstawimy również proces komunikacji pomiędzy warstwami.

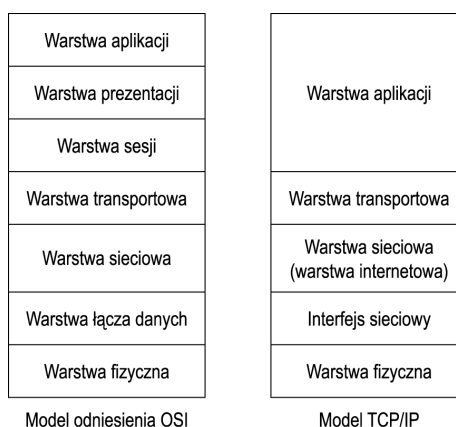
Pięciowarstwowa architektura TCP/IP

W ciągu ostatniej dekady wielu producentów sprzętu i oprogramowania dołączyło do swej oferty produkty pracujące w sieciach komputerowych. Aby uniknąć niezgodności pomiędzy rozlicznymi produktami sieciowymi wprowadzonymi na rynek, opracowane zostały standardy otwartych systemów komputerowych (ang. *open computing*). Rozwój

TCP/IP od zawsze odbywał się w środowisku otwartym, wobec tego TCP/IP nadal uznawany jest za prawdziwy protokół połączeniowy systemów otwartych, pomimo prób popularyzacji przez rząd USA protokołów *Open Systems Interconnection* (OSI). Z upływem lat, w odpowiedzi na istniejący siedmiowarstwowy model odniesienia OSI, rozwinął się współczesny pięciowarstwowy model architektury TCP/IP. Podstawowym zadaniem tego modelu jest zdefiniowanie zbioru otwartych standardów dla wszelkich obecnych lub przyszłych zmian rozwojowych w dziedzinie TCP/IP. Rysunek 2.1 przedstawia poglądowe porównanie modeli odniesienia OSI oraz TCP/IP.

Rysunek 2.1.

Modele odniesienia
OSI i TCP/IP
— porównanie



Czasami można natknąć się na czterowarstwowy model architektury TCP/IP. W uproszczonej wersji dwie pierwsze warstwy — fizyczna i interfejsu sieciowego — zostały połączone w jedną, nazywaną warstwą dostępu do sieci (*Network layer*) lub po prostu warstwą fizyczną (*Physical layer*). Zdarzają się również przypadki, gdy warstwa internetowa nazywana jest warstwą sieciową (*Network layer*).

Model odniesienia pełni funkcję wytycznych funkcjonalnych w podziale procesów i zadań łączności sieciowej:

- ♦ pozwala producentom tworzyć produkty zgodne z pozostałymi,
- ♦ ułatwia zrozumienie złożonych operacji,
- ♦ dzieli na kategorie technologie sieciowe i implementacje ich protokołów, co pozwala na wyspecjalizowane tworzenie projektów funkcji modułowych.

Podobnie jak model odniesienia OSI, model architektury TCP/IP składa się ze zbioru warstw, z których każda reprezentuje grupę określonych zadań i aspektów procesu łączności. Ponieważ model TCP/IP jest teoretyczny, warstwy te nie istnieją fizycznie, ani nie wykonują w rzeczywistości żadnych funkcji. Dopiero implementacje protokołu, stanowiące połączenie sprzętu i oprogramowania, wykonują funkcje przypisane do odpowiadających im warstw. Model TCP/IP składa się z następujących pięciu warstw:

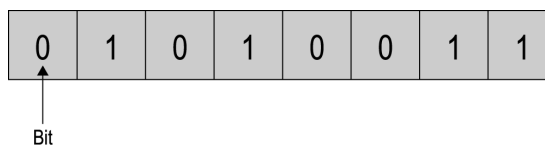
- ♦ *Warstwa fizyczna* — udostępnia nośnik fizyczny (np. przewody), służące do transmisji danych z jednego komputera do drugiego.
- ♦ *Warstwa interfejsu sieciowego* — odpowiada za identyfikację urządzeń w sieci w celu kontroli przepływu danych, na podstawie ich adresów sieciowych, oraz za organizację bitów z warstwy fizycznej w ramki.

- ♦ *Warstwa internetowa (inaczej międzysieciowa)* — odpowiada za przesyłanie (trasowanie) danych pomiędzy różnymi sieciami.
- ♦ *Warstwa transportowa* — odpowiada za organizację w segmenty komunikatów odebranych z wyższych warstw, za kontrolę błędów oraz za kontrolę przepływu między dwoma punktami końcowymi.
- ♦ *Warstwa aplikacji* — udostępnia interfejs w postaci aplikacji i usług sieciowych pomiędzy siecią a użytkownikiem.

Warstwa fizyczna

Warstwa fizyczna jest najniższą warstwą modelu TCP/IP i odpowiada za fizyczną transmisję danych przez *nośnik transmisji*. Nazwą nośnika transmisji określana jest ścieżka fizyczna (przewód elektryczny, światłowód, fale radiowe itp.), którą przesyłane są dane w postaci sygnałów elektrycznych lub fal elektromagnetycznych. Warstwa fizyczna odbiera dane od wyższych warstw i przetwarza je w ciąg bitów, który można z powodzeniem przesłać nośnikiem transmisji. Bit, przedstawiony na rysunku 2.2, jest podstawową jednostką komunikacji pomiędzy komputerami i urządzeniami sieciowymi i może przyjąć tylko jedną z dwóch wartości: 0 lub 1. 0 reprezentuje nieobecność sygnału w nośniku transmisji, zaś 1 oznacza obecność tego sygnału.

Rysunek 2.2.
Bit w ciągu sygnałów

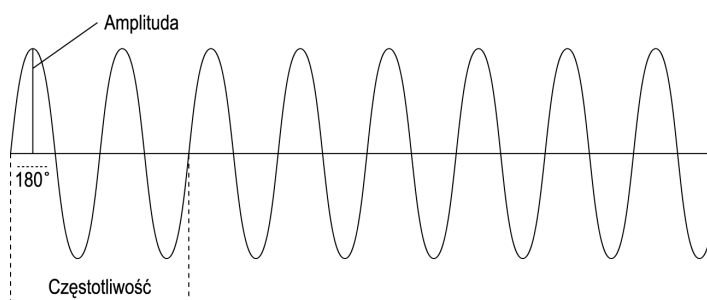


Przesyłanie sygnałów

Dane w sieci przesyłane są z jednego komputera do drugiego w postaci sygnałów. W zależności od użytego nośnika transmisji, sygnały dzieli się na dwie kategorie:

- ♦ *Sygnały analogowe* — przypominają ciąg fal sinusoidalnych, w którym stan fali ulega ciągłym zmianom i przechodzi przez wszystkie wartości z dozwolonego zakresu. Rysunek 2.3 przedstawia sygnał analogowy.

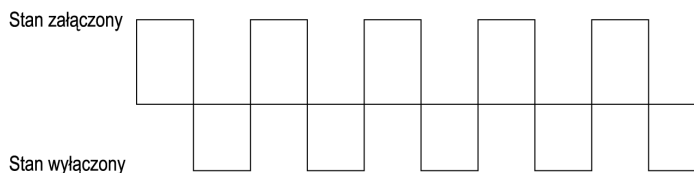
Rysunek 2.3.
Sygnał analogowy



- ♦ *Sygnały cyfrowe* — posiadają tylko dwa stany: obecność danych (1) i nieobecność danych (0). „1” powszechnie nazywa się stanem załączonym (ON), zaś „0” stanem wyłączonym (OFF). Rysunek 2.4 przedstawia sygnał cyfrowy.

Rysunek 2.4.

Sygnał cyfrowy



W sygnałach analogowych mierzone są: amplituda, częstotliwość i faza. Amplituda oznacza wartość maksymalną sygnału, mierzona w woltach (jeśli mierzymy amplitudę napięcia), watach (jeśli mierzymy moc sygnału) lub decybelach (jeśli mierzymy stosunek mocy dwóch sygnałów). Częstotliwość oznacza liczbę pełnych okresów sygnału w jednostce czasu i mierzona jest w hercach (okresach na sekundę). Faza oznacza stan względny sygnału w chwili pomiaru i podawana jest w stopniach lub radianach.



Szczegółowe informacje o nośnikach transmisji i sposobach przechodzenia przez nie sygnał zawiera rozdział 3.

Typy połączeń fizycznych

Istnieją następujące sposoby łączenia komputerów w sieci przez nośnik transmisji:

- ♦ *Połączenie dwupunktowe* — w połączeniu tego typu jeden nośnik transmisji tworzy bezpośrednie łącze pomiędzy dwoma komunikującymi się urządzeniami (patrz rysunek 2.5). Połączenie dwupunktowe jest szybsze, lecz droższe od wielopunktowego. Przykładem połączenia dwupunktowego jest linia dzierżawiona, łącząca bezpośrednio organizację z jej dostawcą usług internetowych (ISP — *Internet Service Provider*).

Rysunek 2.5.

Połączenie dwupunktowe



Dodatkowe informacje o dostawcach usług internetowych zawiera rozdział 11.

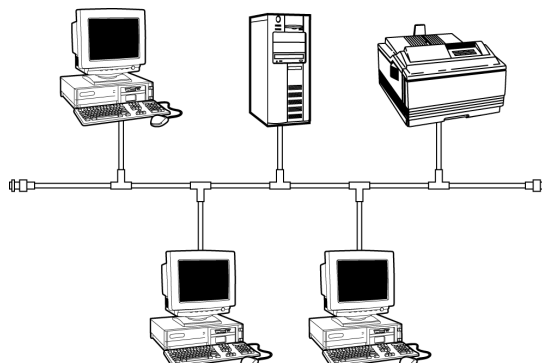
- ♦ *Połączenie wielopunktowe* — w połączeniu tego typu pojedynczy nośnik transmisji jest użytkowany wspólnie przez trzy lub więcej urządzeń sieciowych (patrz rysunek 2.6). W rezultacie połączenie jest stosunkowo wolniejsze, lecz tańsze od połączeń dwupunktowych. Na przykład, możemy wiele urządzeń sieciowych połączyć z serwerem za pomocą pojedynczego kabla.

Topologie fizyczne

Fizyczny układ nośnika transmisji w sieci nazywany jest *topologią fizyczną sieci*. Do najpopularniejszych obecnie topologii sieci lokalnych (LAN) zaliczają się:

Rysunek 2.6.

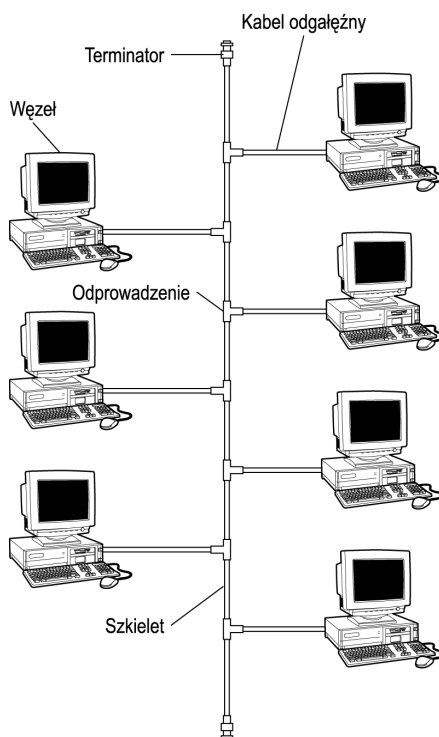
Połączenie wielopunktowe



- ♦ *Topologia magistrali* — w tej topologii (przedstawionej na rysunku 2.7) wszystkie urządzenia sieciowe podłączone są do głównego kabla, zwanego szkieletem (ang. *backbone*), albo za pomocą krótkich kabli zwanych odgałęźnymi, albo bezpośrednio przez trójniki. Aby zapobiec odbiciom sygnału od końców magistrali, kabel szkieletowy musi być zakończony z obu stron terminatorami. Z wszystkich stosowanych topologii magistrala uznawana jest za najłatwiejszą i najtańszą w implementacji. Jednakże topologia ta jest wolniejsza od pozostałych.

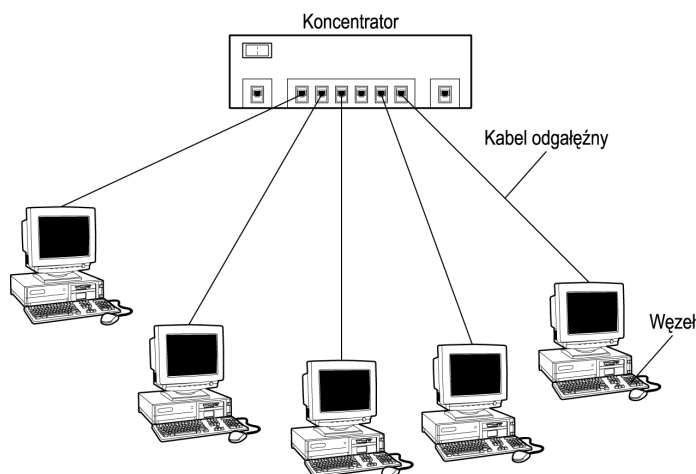
Rysunek 2.7.

Topologia magistrali

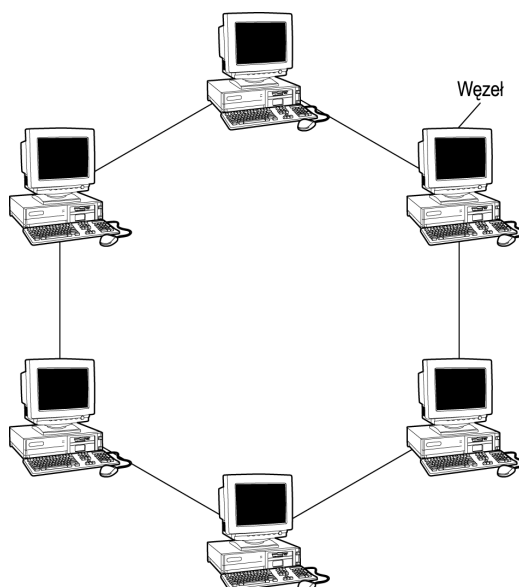


- ♦ *Topologia gwiazdy* — w tej topologii (przedstawionej na rysunku 2.8) wszystkie urządzenia sieciowe podłączone są za pomocą kabli odgałęźnych do urządzenia centralnego, zwanego koncentrატorem. W wyniku tego każde urządzenie posiada

dwupunktowe połączenie z koncentratorem. Topologią tą łatwo zarządzać, łatwo ją rozbudowywać i znajdować w niej problemy. Jednakże w przypadku awarii koncentratora cała sieć przestaje działać.

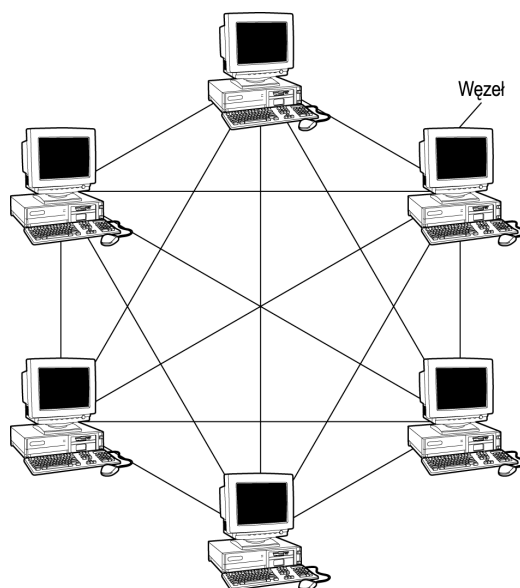
Rysunek 2.8.*Topologia gwiazdy*

- ♦ *Topologia pierścienia* — w tej topologii (przedstawionej na rysunku 2.9) każde urządzenie sieciowe połączone jest z następnym tak, iż tworzą zamkniętą pętlę (pierścień). Łatwo nią zarządzać i rozwiązywać problemy, jednakże jest bardzo droga w implementacji, a zmiany konfiguracji są w niej trudne.

Rysunek 2.9.*Topologia pierścienia*

- ♦ *Topologia oczkowa* — w tej topologii (przedstawionej na rysunku 2.10) każdy węzeł połączony jest bezpośrednio z wszystkimi pozostałymi węzłami sieci za pomocą połączeń dwupunktowych. Topologia ta jest zarówno wyjątkowo odporna na uszkodzenia, jak i wyjątkowo kosztowna w implementacji.

Rysunek 2.10.
Topologia oczkowa



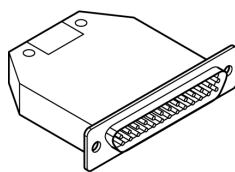
Rozdział 3. zawiera więcej informacji o różnych topologiach.

Urządzenia sieciowe warstwy fizycznej

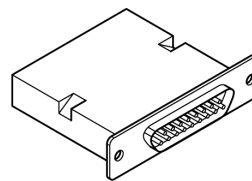
Aby zbudować sieć i połączyć każdy komputer z nośnikiem transmisji, potrzebujemy szeregu urządzeń sieciowych. Do sprzętu zwykle kojarzonego z warstwą fizyczną modelu TCP/IP należą:

- ♦ *Złącza* — złącza nośnika transmisji zapewniają połączenie pomiędzy urządzeniami sieciowymi i nośnikiem transmisji. Dla każdego nośnika transmisji istnieje jeden lub kilka typów złączy, które mogą posłużyć do przyłączenia urządzenia. Do najczęściej używanych złączy fizycznych należą (przedstawione na rysunku 2.11):

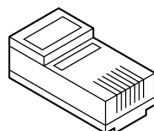
Rysunek 2.11.
Najczęściej stosowane złącza



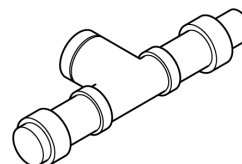
DB-25



DB-15

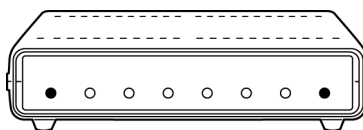


RJ-45



Trójnik (ze złączem BNC)

- ♦ Trójniki i złącza BNC
- ♦ Złącza RJ-45
- ♦ Złącza DB-25 (inaczej RS-232)
- ♦ Złącza DB-15
- ♦ *Regeneratory* — im dłuższą drogę ma do przebycia sygnał, tym bardziej jest tłumiony, wobec czego każdy nośnik transmisji może być użyty na ograniczonej odległości. Nośnik można jednakże przedłużyć za pomocą regeneratorów. Urządzenia te po prostu wzmacniają sygnały do oryginalnego poziomu. Regenerator przedstawiony jest na rysunku 2.12.

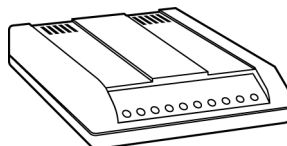
Rysunek 2.12.*Regenerator*

- ♦ *Koncentratory* — koncentrator gra rolę centralnego węzła do przyłączania wielu urządzeń sieciowych. Rysunek 2.13 przedstawia typowy koncentrator. Do warstwy fizycznej należą dwa typy koncentratorów:
 - ♦ *Koncentratory aktywne* — oprócz pełnienia funkcji centralnego punktu połączenia, regenerują sygnał.
 - ♦ *Koncentratory pasywne* — jedynie rozsyłają sygnał otrzymany od przyłączonego urządzenia, bez regeneracji sygnału.

Rysunek 2.13.*Koncentrator*

Istnieje jeszcze trzeci typ koncentratorów — *koncentratory inteligentne*. Jednakże te urządzenia funkcjonują w warstwie interfejsu sieciowego.

- ♦ *Modemy* — gdyby połączyć komputer (który używa sygnałów cyfrowych) bezpośrednio z analogową linią telefoniczną (która przenosi jedynie sygnały analogowe), łączność byłaby niemożliwa. Modem (ang. *MOdulator/DEModulator*) — taki, jak na rysunku 2.14 — przekształca odebrane z komputera sygnały cyfrowe na analogowe, które można przesłać analogową linią telefoniczną. Sygnały odebrane z analogowej linii telefonicznej są przekształcane przez modem na cyfrowe, aby komputer mógł je przetworzyć.

Rysunek 2.14.*Modem*

Warstwa interfejsu sieciowego

Do podstawowych zadań warstwy interfejsu sieciowego należą:

- ♦ unikatowa identyfikacja urządzeń w sieci lokalnej (LAN) za pomocą adresów sprzętowych MAC (*Media Access Control*),
- ♦ organizacja bitów otrzymanych z warstwy fizycznej w ramki,
- ♦ konwersja adresów IP na adresy LAN i vice versa,
- ♦ wykrywanie błędów i zgłaszanie ich do wyższych warstw,
- ♦ kontrola przepływu danych.

Urządzenia warstwy interfejsu sieciowego

Do urządzeń powszechnie kojarzonych z warstwą interfejsu sieciowego należą:

- ♦ *Karty interfejsu sieciowego (NIC — Network Interface Card)* — sprzętowe karty rozszerzeń, które po instalacji zapewniają komputerom łączność sieciową przez połączenie z nośnikiem transmisji.
- ♦ *Mosty* — w dużych sieciach (zwłaszcza o topologii magistrali) wszystkie urządzenia podłączone do szkieletu odbierają sygnały w nim obecne, co powoduje zbędny ruch w sieci. Możemy jednak użyć mostu, by podzielić dużą sieć na mniejsze segmenty, wydajnie redukując niepotrzebny ruch. Gdy most odbiera sygnał, wtedy sprawdza, czy odbiorca znajduje się w lokalnym segmencie. Jeśli tak, wówczas most rozgłasza odebrany sygnał w segmencie i nie przekazuje go do innych segmentów. Jeśli odbiorca nie należy do lokalnego segmentu, wówczas most przekazuje sygnał jedynie do segmentu, w którym mieści się adresat, co efektywnie zmniejsza ruch sieciowy. Rysunek 2.15 przedstawia funkcjonowanie typowego mostu.
- ♦ *Inteligentne koncentratory* — oprócz tego, że są centralnym punktem podłączenia w łączności sieciowej i regenerują sygnał, inteligentne koncentratory przekazują sygnały tylko do urządzeń-odbiorców, nie rozgłaszając ich do wszystkich podłączonych urządzeń.

Standardy kontroli dostępu do nośnika

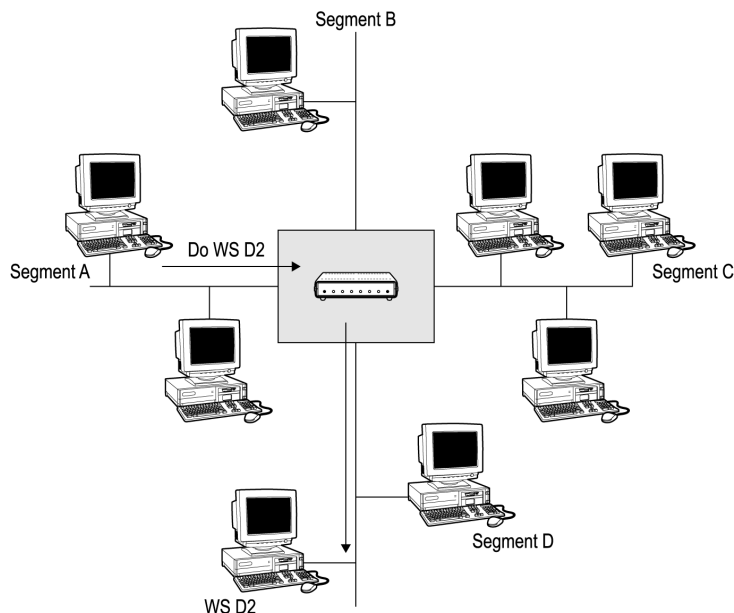
Aby zapewnić poprawne funkcjonowanie sieci, należy zminimalizować lub całkiem wyeliminować możliwość równoczesnego wysłania do nośnika transmisji dwóch lub więcej sygnałów. Sieci używają reguł kontrolujących, kiedy urządzenie sieciowe może nadawać pakiety danych. Reguły te noszą nazwę *standardów kontroli dostępu do nośnika*.

W zależności od używanej topologii fizycznej, stosowane są różne standardy kontroli dostępu do nośnika:

- ♦ *Rywalizacja* — w tej metodzie każde urządzenie w sieci rywalizuje o umieszczenie jako pierwsze swojego sygnału w nośniku transmisji. Jeśli dwa lub kilka urządzeń równocześnie umieści swoje sygnały w nośniku, zachodzi kolizja sygnałów i zostają one odrzucone (zniszczone). Metoda ta jest powszechnie stosowana w topologiach magistrali.

Rysunek 2.15.

Sposób działania mostu



- ♦ *Przekazywanie żetonu* — w tej metodzie nieustannie krąży w sieci specjalna ramka, zwana żetonem (ang. *token*). Dowolne urządzenie, które chce nadawać dane, przechwytytuje żeton i umieszcza dane w jego ramce. Po zakończeniu transmisji urządzenie zwalnia żeton. Ta metoda stosowana jest w topologiach pierścieniowych.
- ♦ *Odpytywanie* — w tej metodzie urządzenie nadrzędne odpytuje urządzenia sieciowe w regularnych odstępach czasu. Gdy określone urządzenie chce wysłać dane, wówczas urządzenie nadrzędne wysyła do niego pakiet żądania. Urządzenie umieszcza dane w ramce żądania i zwraca pakiet do urządzenia nadrzędnego, które następnie wysyła ramkę do odpowiedniego odbiorcy. Tę metodę dostępu stosują powszechnie inteligentne koncentratory w topologii gwiazdy.



Szczegółowe informacje o metodach dostępu do nośnika zawiera rozdział 4.

Sterowanie przepływem

Sieć składa się z urządzeń obsługujących różne prędkości transmisji — na przykład przełączniki są znacznie szybsze od koncentratorów. Z reguły drukarki są jednymi z najwolniejszych urządzeń sieciowych. Gdyby nadawca wysyłał ramki szybciej niż odbiorca jest w stanie je przyjmować, nadawca zarzuciłby odbiorcę ramkami. Nawet gdyby transmisje były wolne od błędów, w pewnym momencie odbiorca nie byłby w stanie ich przyjmować w miarę nadsyłania i zacząłby tracić ramki. Wobec tego ilość objętość danych, którą można wysłać jednokrotnie podczas komunikacji dwóch tożsamości sieciowych, jest bardzo ważnym zagadnieniem.

Wstępnie zdefiniowane reguły sterowania przepływem zapewniają, że szybsze urządzenia nie zalewają wolniejszych danymi podczas transakcji. Sterowanie przepływem zwalnia szybkość transmisji nadawcy do tempa, z jakim odbiorca może sobie poradzić.

W sterowaniu przepływem stosowany jest mechanizm sprzężenia zwrotnego, za pomocą którego odbiorca może poinformować nadawcę, czy jest w stanie poradzić sobie z prędkością transmisji. Na przykład, przy nawiązaniu połączenia odbiorca może poinformować nadawcę, aby po wysłaniu n ramek zatrzymał się i poczekał, aż do otrzymania od odbiorcy wyraźnej lub pośredniej zgody na kontynuację.



Sterowanie przepływem jest zasadniczo wbudowane w różne protokoły w postaci dobrze zdefiniowanych reguł i ma wpływ zarówno na urządzenia końcowe (np. stacje robocze), jak i urządzenia pośredniczące (np. rutery).

Sterowanie przepływem w warstwie interfejsu sieciowego może się odbywać według dwóch strategii:

- ♦ *Sterowanie z gwarantowaną szybkością przepływu* — w tej strategii nadawca i odbiorca negocjują akceptowalną szybkość transmisji dla całej sesji, jeszcze przed rozpoczęciem transmisji. Niezmiennność tej szybkości jest gwarantowana na okres całej sesji.
- ♦ *Sterowanie przepływem za pomocą okien* — takie sterowanie przepływem pozwala dwóm połączonym urządzeniom wynegocjować rozmiary bufora (okna), w którym można umieścić zadaną liczbę ramek. Istnieją dwa typy sterowania przepływem w oknach:
 - ♦ *Statyczne* — w chwili nawiązania połączenia tożsamości na jego końcach ustalają wspólnie rozmiary okna i używają ich przez całą sesję, aż do jej zamknięcia. Załóżmy, że na początku sesji nadawca i odbiorca umawiają się na rozmiar okna wynoszący osiem ramek. Wówczas nadawca zbiera osiem ramek danych, przydziela do każdej tymczasowy numer i umieszcza ramki w nośniku transmisji. W tym przypadku numer okna będzie z przedziału od jeden do osiem. Po odebraniu ramki odbiorca musi wysłać potwierdzenie. Jeśli nadawca wysłał wszystkie osiem ramek, musi czekać na potwierdzenie odbioru przynajmniej jednego z przydzielonych numerów, a następnie powtarza cały proces dla kolejnych ośmiu ramek. Proces ten zapewnia, iż w każdej chwili nie zalega więcej niż osiem ramek.



Ta strategia powoduje marnowanie przepustowości łącza, ponieważ każda wysłana ramka musi zostać potwierdzona.

- ♦ *Dynamiczne* — podczas nawiązywania połączenia ustalone zostają rozmiary okna. Jednakże ten typ sterowania przepływem pozwala urządzeniom sieciowym dostosowywać rozmiary okna do wymogów chwili, zgodnie ze statusem odbiorcy. Na początku połączenia ustalany jest maksymalny rozmiar okna. Gdy w czasie transmisji bufor odbiorcy zacznie się przepełniać, wówczas wysyła on natychmiast *pakiet tłumienia*. Pakiet ten jest dla nadawcy sygnałem, by zwolnić. Po jakimś czasie nadawca zaczyna powoli zwiększać szybkość transmisji, aż do odebrania kolejnego pakietu tłumienia. W ten sposób rozmiar okna jest nieustająco regulowany podczas samej transmisji. Dynamiczne sterowanie przepływem za pomocą okien nazywane jest również *sterowaniem z oknem pływającym* lub *przesuwaniem*.

Warstwa internetowa

Warstwa interfejsu sieciowego identyfikuje unikatowo urządzenie w sieci lokalnej za pomocą adresów fizycznych, zakodowanych na trwałe w kartach interfejsów sieciowych. Noszą one inaczej nazwę adresów sterowania dostępem do nośnika (MAC — *Media Access Control*). Jednakże ta metoda unikatowej identyfikacji urządzeń nie jest skuteczna, gdy łączność zachodzi pomiędzy dwoma urządzeniami położonymi w różnych sieciach. Do przesyłania pakietów pomiędzy sieciami warstwa internetowa używa adresów IP.

Adres IP jest 32-bitową binarną konwencją nazewniczą, która została opracowana na potrzeby globalnej komunikacji. Adresy IP, w celu łatwego zapamiętania, notowane są w postaci czterech dziesiętnych liczb całkowitych oddzielonych kropkami. Na przykład, 23.33.71.11 jest adresem IP.

W zależności od liczby hostów i sieci, które mogą być obsługiwane w danym zakresie adresów, istnieje pięć klas adresów IP:

- ♦ klasa A, obejmująca adresy IP od 0.1.0.0 do 126.0.0.0
- ♦ klasa B, obejmująca adresy IP od 128.0.0.0 do 191.255.0.0
- ♦ klasa C, obejmująca adresy IP od 192.0.1.0 do 223.255.255.0
- ♦ klasa D, obejmująca adresy IP od 224.0.0.0 do 239.255.255.255
- ♦ klasa E, obejmująca adresy IP od 240.0.0.0 do 247.255.255.255



Szczegółowe informacje o adresowaniu IP oraz klasach adresów IP zawiera rozdział 5.

Komutacja

Pomiędzy dwoma urządzeniami komunikującymi się ze sobą w sieci może istnieć więcej niż jedna łącząca je ścieżka. Aby zapewnić szybkie dostarczenie danych, sygnał może w miarę potrzeb być przełączany (komutowany) pomiędzy tymi ścieżkami, za pomocą poniższych trzech technik komutacji:

- ♦ *Komutacja obwodów* — w tej metodzie wymagany jest dedykowany kanał (obwód) łączności pomiędzy dwoma komunikującymi się urządzeniami.
- ♦ *Komutacja komunikatów* — w tej metodzie komutacji nie trzeba nawiązywać dedykowanego fizycznego połączenia pomiędzy punktami końcowymi łączności. Komunikat jest dzielony na małe części, którym zostają przydzielone numery. Część jest traktowana jak niezależna całość; wszystkie zawierają też informacje o adresie docelowym. Komunikaty są składowane w każdym przełączniku przed przesłaniem do następnego przełącznika na trasie.
- ♦ *Komutacja pakietów* — w tej metodzie komunikaty dzielone są na segmenty zwane pakietami, które następnie są przesyłane niezależnie przez sieć, własnymi trasami. Każdy pakiet zawiera oprócz właściwych danych adres źródłowy i docelowy.

**Uwaga**

Jest jedna podstawowa różnica pomiędzy dwiema ostatnimi metodami. W komutacji komunikatów nie istnieje górna granica rozmiarów bloku komunikatów, zaś w komutacji pakietów rozmiar pakietu ograniczony jest do ustalonej wartości.

Wykrywanie i wybór tras

Rutery są urządzeniami sieciowymi skojarzonymi z funkcjami warstwy internetowej. Aby zapewnić najszybsze dostarczenie danych z jednego urządzenia do drugiego, ruter musi wykryć najkrótszą i najszybszą trasę. Ta metoda ustalania tras do sieci docelowej nosi nazwę *wykrywania trasy* (ang. *route discovery*). Istnieją dwie metody wykrywania trasy:

- ♦ *Metoda wektora odległości* — w tej metodzie każdy ruter utrzymuje tablicę tras (ang. *routing table*), którą rozgłasza w regularnych odstępach czasu. Dzięki rozgłoszeniom innych ruterów, każdy ruter regularnie aktualizuje informacje o wszelkich nowych trasach. Chociaż ta metoda zapewnia każdemu ruterowi posiadanie najświeższych tablic tras, generuje bardzo wysokie obciążenie łącza.
- ♦ *Metoda stanu połączenia* — w tej metodzie rozgłoszenia generowane są tylko wtedy, gdy nastąpi dowolna zmiana w istniejącej tablicy tras rutera. Pozostałe rutery, które odbierają rozgłoszenie, odpowiednio aktualizują swoje tablice tras. W rezultacie metoda ta generuje znacznie mniejszy ruch w sieci.

**Odnosnik**

Rozdział 5. zawiera bardziej szczegółowe informacje o wyznaczaniu tras.

Ruter po zbudowaniu tablicy tras, przez wykrycie tras do sieci docelowych, wybiera właściwą trasę do sieci docelowej, obliczając najlepszą ścieżkę transmisji. Wybór może odbywać się zarówno *dynamicznie*, jak i *statycznie*:

- ♦ *Dynamiczny wybór trasy* — jeśli w dowolnej chwili dostępnych jest wiele tras do urządzenia docelowego, ruter ustala najlepszą z nich. Ten wybór odbywa się w każdym ruterze po drodze do urządzenia docelowego. Inaczej mówiąc, tablica tras jest utrzymywana automatycznie, bez ingerencji administratora sieci.
- ♦ *Stacyjny wybór trasy* — nawet jeśli dostępnych jest wiele tras do urządzenia docelowego, do przesłania pakietów użyta zostaje jedynie trasa wyznaczona przez administratora sieci. Rutery po drodze do urządzenia docelowego nie mogą podejmować decyzji o wyznaczaniu tras. Inaczej mówiąc, tablica tras jest tworzona i utrzymywana przez administratora sieci.

**Odnosnik**

Szczegółowe informacje o statycznym i dynamicznym wyborze tras zawiera rozdział 19.

Warstwa transportowa

Czwarta warstwa modelu TCP/IP — transportowa — jest przede wszystkim odpowiedzialna za:

- ♦ udostępnienie interfejsu pomiędzy warstwami niższymi (internetową, interfejsu sieciowego i fizyczną) a warstwą aplikacji,
- ♦ dostarczenie danych od nadawcy do odbiorcy.

Niższe warstwy mogą zlokalizować zamierzonego odbiorcę (w tej samej sieci lub w innych sieciach) i wysłać do niego dane. Jednakże warstwy te nie mogą zapewnić wiarygodnych usług połączeniowych. Warstwa transportowa spełnia powyższe wymagania. Używa ona do celów łączności dwóch protokołów — TCP i UDP (*User Datagram Protocol* — protokół datagramów użytkownika). TCP świadczy usługi połączeniowe, zaś UDP bezpołączeniowe.



Wiarygodność usług połączeniowych nie oznacza, iż dane zostaną przesłane bez względu na okoliczności. Pojęcie połączenia wiarygodnego (*reliable*) oznacza, iż protokoły warstwy transportowej potrafią potwierdzić pomyślny odbiór danych lub poinformować o niepowodzeniu. Jeśli dane nie dotarły do odbiorcy lub uległy uszkodzeniu w trakcie transmisji, wówczas warstwa transportowa może zainicjować retransmisję. Warstwa aplikacji również jest informowana o niepowodzeniach, dzięki czemu może zainicjować działania korekcyjne lub powiadomić użytkownika.

Usługi połączeniowe

Warstwa transportowa udostępnia dwa typy usług połączeniowych:

- ♦ *Zorientowane na połączenie (połączeniowe)* — gdy dane przesyłane są z jednego urządzenia sieciowego do innego, każda pomyślnie przesłana porcja nie uszkodzonych danych jest potwierdzana przez odbiorcę. Nadawca nie wyśle następnych danych, dopóki nie odbierze pozytywnego potwierdzenia dotyczącego ostatniej wysłanej porcji. Jeśli dane podczas transmisji ulegną zagubieniu lub uszkodzeniu, nadawca nie otrzyma od odbiorcy odpowiedniego potwierdzenia. Nadawca musi ponownie wysłać albo utracony pakiet, albo całą porcję, w zależności od implementacji protokołu. Usługi zorientowane na połączenia udostępniają również sterowanie przepływem i kontrolę błędów.
- ♦ *Bezpołączeniowe* — urządzenie nadające wysyła dane do odbiorcy i nie odpowiada za retransmisję wszelkich danych uszkodzonych lub utraconych podczas transmisji do odbiorcy. Istnieją dwa typy usług bezpołączeniowych:
 - ♦ *Potwierdzane usługi bezpołączeniowe* — komunikaty potwierdzające są wymieniane, jeśli transmisja jest dwupunktowa. Tego typu usługi również zapewniają kontrolę błędów i sterowanie przepływem, o ile transmisja odbywa się dwupunktowo.
 - ♦ *Nie potwierdzane usługi bezpołączeniowe* — transmisje nie są potwierdzane i nie są dostępne żadne metody kontroli błędów, sterowania przepływem, czy też kontroli sekwencji pakietów.



Szczegółowe informacje o usługach zorientowanych na połączenie i bezpołączeniowych zawiera rozdział 6.

Obsługa segmentów

Oprócz wiarygodnych usług połączeniowych warstwa transportowa odpowiada także za podział dużych komunikatów warstwy aplikacji na segmenty, które można przesłać nośnikiem transmisji. Proces ten nosi nazwę *fragmentacji*. Gdy urządzenie sieciowe odbiera komunikat w postaci kilku segmentów, warstwa transportowa odpowiada za poprawne złożenie tych segmentów w oryginalny komunikat — ten proces nazwany jest *defragmentacją*.

Sterowanie przepływem w warstwie transportowej

Sterowanie przepływem w warstwie transportowej nazywane jest również dwupunktowym sterowaniem przepływem (ang. *end-to-end flow control*), ponieważ zajmuje się połączeniami pomiędzy węzłami nadawcy i odbiorcy. Warstwa transportowa dokonuje sterowania przepływem za pomocą poniższych typów potwierdzeń:

- ♦ *Potwierdzenia pozytywne i negatywne* — gdy przesłane dane są odebrane bez strat i uszkodzeń, odbiorca wysyła do nadawcy potwierdzenie pozytywne. Jeśli jednak dane ulegną uszkodzeniu, odbiorca wysyła potwierdzenie negatywne. W drugim przypadku warstwa transportowa albo warstwa aplikacji, która zainicjowała transakcję, podejmuje działania korekcyjne.
- ♦ *Potwierdzenie „wróć do n”* — potwierdzenie „wróć do n” („go back n”) oznacza, iż nadawca musi ponownie przesłać część komunikatu, zaczynając od pakietu o numerze *n* z ostatniej transakcji.
- ♦ *Potwierdzenie z selektywnym powtórzeniem* — oznacza, iż ciąg pakietów został odebrany poprawnie, lecz kilka zawartych w nim pakietów zostało podczas transmisji utraconych lub uszkodzonych. Potwierdzenie takie mówi nadawcy, aby zamiast całego ciągu wysłał ponownie jedynie pakiety brakujące i uszkodzone.

Kontrola błędów

Utrata danych podczas transmisji jest niekiedy nieunikniona, a ponadto istnieje możliwość dotarcia do celu danych uszkodzonych w procesie transmisji. Warstwa transportowa naprawia te błędy w następujący sposób:

- ♦ Podczas transmisji segmentom przydzielane są unikatowe numery, aby zapobiec wystąpieniu podwójnych numerów segmentów, a co za tym idzie — utracie pakietów.
- ♦ Pakiety, których dopuszczalny czas istnienia został przekroczony (co ustala się na podstawie wartości TTL, używanej przez warstwę internetową), są odrzucane, ponieważ im dłużej pakiet danych podróżuje w sieci, tym większe jest prawdopodobieństwo jego uszkodzenia.
- ♦ Podczas sesji używana jest tylko jedna wirtualna trasa, aby zminimalizować szanse utraty pakietów danych.



Szczegółowe informacje o warstwie transportowej zawiera rozdział 6.

Warstwa aplikacji

Warstwa aplikacji mieści się na szczycie modelu architektury TCP/IP. Jest warstwą najważniejszą, ponieważ użytkownik pracuje z nią bezpośrednio. Warstwa aplikacji obsługuje wszystkie niezbędne protokoły, aby świadczyć usługi sieciowe: na przykład, usługi plikowe, przesyłanie wiadomości, usługi baz danych, czy też usługi drukowania. W istocie wszystkie pozostałe warstwy istnieją tylko po to, by obsługiwać warstwę aplikacji.



Pakiety oprogramowania, na przykład Microsoft Word, Excel i tak dalej, nie należą do warstwy aplikacji. Jedynie aplikacje inicjujące żądania, które mogą być obsługane przez inne urządzenia sieciowe — na przykład poczta elektroniczna — uznawane są za składniki warstwy aplikacji.

Do najczęściej używanych protokołów warstwy aplikacji zaliczają się:

- ♦ *FTP (File Transfer Protocol — protokół transferu plików)* — bezpieczny i niezawodny protokół, służący do przesyłania plików ze zdalnego komputera do lokalnego i odwrotnie. Aby umożliwić transfer plików, użytkownik musi nawiązać połączenie ze zdalnym komputerem.
- ♦ *TFTP (Trivial File Transfer Protocol — prosty protokół transferu plików)* — protokół, który używa UDP w roli swojego protokołu transportowego. Dzięki temu użytkownik, aby przesyłać pliki, nie musi nawiązywać połączenia z drugim urządzeniem ani logować się do zdalnego systemu.



Dodatkowe informacje o FTP i TFTP zawiera rozdział 12.

- ♦ *Telnet (TELEcommunication NETwork)* — protokół, który pozwala użytkownikom pracować ze zdalnym systemem tak, jak z lokalnym. Jest to możliwe, ponieważ Telnet przejmuje lokalną interpretację informacji wprowadzanych z klawiatury.



Dodatkowe informacje o usłudze Telnet zawiera rozdział 13.

- ♦ *SMTP (Simple Mail Transfer Protocol — prosty protokół przesyłania poczty)* — protokół, który używany z aplikacją poczty elektronicznej pozwala użytkownikom odbierać i wysyłać pocztę elektroniczną (e-mail) przez sieć.



Dodatkowe informacje o SMTP zawiera rozdział 16.

- ♦ *SNMP (Simple Network Management Protocol — prosty protokół zarządzania siecią)* — protokół służący do zarządzania siecią. SNMP przede wszystkim zbiera, analizuje i raportuje dane związane z działaniem różnych składników sieci na potrzeby aplikacji służących do zarządzania siecią.

Łączność pomiędzy warstwami

Według modelu architektury TCP/IP warstwa może w stosie komunikować się z warstwą równorzędną w innych urządzeniach. W tym celu jednak musi przesłać dane lub komunikaty przez niższe warstwy stosu, do którego należy. Warstwa może skorzystać z usług warstwy znajdującej się bezpośrednio pod nią, a zarazem musi świadczyć usługi warstwie bezpośrednio nad sobą.

Gdy warstwa przekazuje dane do niższej, dołącza do tych danych własny *nagłówek* (ang. *header*). Nagłówek zawiera informacje sterujące danej warstwy. Jedynie równorzędna warstwa w innym stosie jest w stanie przetworzyć te informacje. Ogólnie rzecz

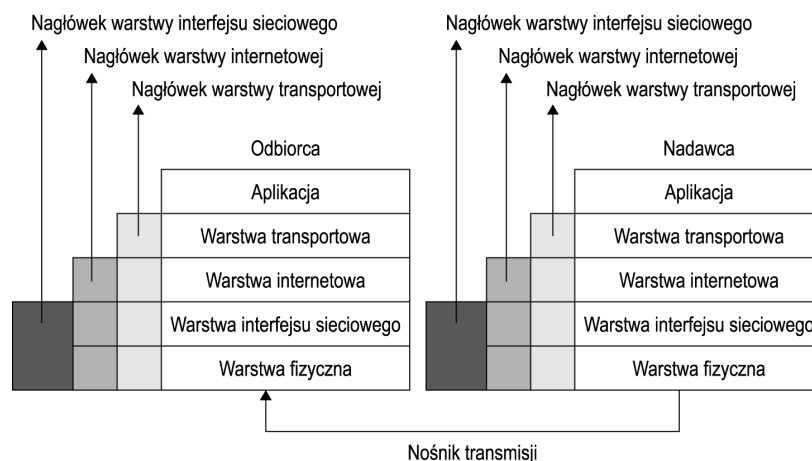
biorąc, żądania usług sieciowych pochodzą z warstwy aplikacji. W takim przypadku komunikat zostaje przesłany w dół, do warstwy transportowej, która dzieli komunikat na mniejsze segmenty, które można przesłać nośnikiem transmisji. Warstwa transportowa, podobnie jak jej poprzednik, również dodaje własny nagłówek do każdego segmentu i przesyła segmenty dalej, do warstwy internetowej. Ten proces dzielenia dużych komunikatów na segmenty nosi nazwę *fragmentacji*. Następnie warstwa internetowa dodaje swój nagłówek do każdego segmentu i przekazuje pakiet do warstwy interfejsu sieciowego. Podobnie jak wszystkie wyższe warstwy, ta dodaje własny nagłówek do datagramów otrzymanych z warstwy internetowej i wysyła ramki do warstwy fizycznej. Warstwa fizyczna dzieli każdą ramkę na sekwencję bitów i umieszcza te sygnały w nośniku transmisji.



Dane w warstwie aplikacji są określane mianem *komunikatu (message)*. W warstwie transportowej dane noszą nazwę *segmentów* lub *datagramów*. W warstwie internetowej segmenty nazywane są *pakietami*. Dane przesyłane do warstwy interfejsu sieciowego noszą nazwę *ramek*, zaś w warstwie fizycznej — *bitów* lub *sygnałów*.

Po przesłaniu sygnałów do zamierzonego odbiorcy, do czego służą nagłówki warstw internetowej i interfejsu fizycznego, proces przetwarzania sygnałów po stronie odbiorcy jest dokładnie odwrotny do procesu po stronie nadawcy. Warstwa fizyczna odbiorcy odbiera sygnały z nośnika transmisji i przekazuje je do warstwy interfejsu sieciowego. Ta z kolei, używając danych sterujących zamieszczonych przez swojego odpowiednika u nadawcy, przekształca ciągi bitów w ramki i przekazuje je do warstwy internetowej. Warstwa internetowa usuwa odpowiadający jej nagłówek i przekazuje pakiety do warstwy transportowej. Ta z kolei, używając danych sterujących zamieszczonych w nagłówku przez swojego odpowiednika u nadawcy, składa segmenty w komunikat. Proces łączenia segmentów w komunikat nosi nazwę *defragmentacji*. Następnie warstwa transportowa przesyła komunikat do warstwy aplikacji, która go przetwarza oraz, w razie potrzeby, wyświetla informacje dla użytkownika. Cały proces opakowywania i rozpakowywania został przedstawiony na rysunku 2.16.

Rysunek 2.16.
Proces opakowywania
i rozpakowywania



Format nagłówka warstwy transportowej

W zależności od typu łączności — gwarantowanej lub nie — nagłówek warstwy transportowej może należeć do jednego z dwóch typów: TCP lub UDP.

Format nagłówka TCP

Nagłówek TCP, przedstawiony na rysunku 2.17, składa się z następujących pól:

Rysunek 2.17.
Format nagłówka TCP

Port źródłowy			Port docelowy	
Numer kolejny				
Numer potwierdzenia				
HLEN	Zarezerwowane	Bity sterujące	Okno	
Suma kontrolna			Wskaźnik pilności	
Opcje (ewentualne)				Wypełnienie

- ♦ *Adres portu źródłowego* — zawiera adres portu TCP aplikacji po stronie nadawcy, która zainicjowała żądanie. Pole to ma długość dwóch bajtów.
- ♦ *Adres portu docelowego* — zawiera adres portu TCP aplikacji po stronie odbiorcy, która musi odpowiedzieć na żądanie. Pole o długości dwóch bajtów.
- ♦ *Numer kolejny* — zawiera numer porządkowy segmentu przydzielony podczas podziału komunikatu na segmenty. Pole o długości czterech bajtów.
- ♦ *Numer potwierdzenia* — zawiera numer następnego segmentu, który powinien dotrzeć do odbiorcy. Pole o długości czterech bajtów.
- ♦ *HLEN* — zawiera długość nagłówka segmentu. Pole o długości czterech bitów.
- ♦ *Zarezerwowane* — jego wartość musi być równa zero, ponieważ to pole jest zarezerwowane do wykorzystania w przyszłości. Pole o długości sześciu bitów.
- ♦ *Bity sterujące* — zawiera sześć poniższych jednobitowych pól, które wskazują, jak należy interpretować pozostałe pola nagłówka:
 - ♦ *URG* — jeśli wartość jest równa 0, pole *Wskaźnik pilności* powinno zostać zignorowane. Jeśli wartość jest równa 1, pole to jest obowiązujące.
 - ♦ *ACK* — jeśli równe 0, pole *Numer potwierdzenia* powinno zostać zignorowane. Jeśli 1, pole jest obowiązujące.
 - ♦ *PSH* — jeśli równe 0, to pole powinno zostać zignorowane. Jeśli 1, segment inicjuje funkcję *push*.
 - ♦ *RST* — jeśli równe 0, to pole powinno zostać zignorowane. Jeśli równe 1, połączenie jest zerowane.
 - ♦ *SYN* — jeśli równe 0, segment żąda nawiązania nowego połączenia.
 - ♦ *FIN* — jeśli równe 1, oznacza, iż nadawca nie ma więcej danych do wysłania i połączenie musi zostać zamknięte po bieżącym segmentcie.
- ♦ *Okno* — zawiera rozmiar bufora nadawcy i ustala liczbę bajtów, jaką nadawca segmentu jest obecnie w stanie przyjąć. Pole o długości dwóch bajtów.

- ♦ *Suma kontrolna* — zawiera sumę kontrolną, służącą do weryfikacji poprawności odebranych danych. Pole to zawiera również pseudonagłówek, który pomaga odbiorcy stwierdzić, czy segment dotarł do właściwego celu. Pole o długości dwóch bajtów.
- ♦ *Wskaźnik pilności* — zawiera informacje określające pozycję w segmencie, na której kończą się pilne dane. Pole to przetwarzane jest tylko wtedy, gdy pole URG w bitach sterujących ma wartość 1. Pole o długości dwóch bajtów.
- ♦ *Opcje* — zawiera informacje o kilku funkcjach, na przykład maksymalnym rozmiarze segmentu (MSS — *Maximum Segment Size*), jaki punkty końcowe połączeń mogą odebrać, pole końca opcji i tak dalej. Pole o zmiennej długości.
- ♦ *Wypełnienie* — zawiera ciąg zer dodanych do nagłówka, aby jego długość wynosiła 32 bajty. Pole o zmiennej długości.

Format nagłówka UDP

Nagłówek UDP, przedstawiony na rysunku 2.18, składa się z następujących pól:

Rysunek 2.18.

Format nagłówka UDP

0	16	31
Źródłowy port UDP	Docelowy port UDP	
Długość komunikatu UDP	Suma kontrolna UDP	

- ♦ *Adres portu źródłowego* — zawiera adres portu UDP aplikacji po stronie nadawcy, która zainicjowała żądanie. Pole to ma długość dwóch bajtów.
- ♦ *Adres portu docelowego* — zawiera adres portu UDP aplikacji po stronie odbiorcy, która musi odpowiedzieć na żądanie. Pole o długości dwóch bajtów.
- ♦ *Długość* — podaje długość segmentu. Pole o długości dwóch bajtów.
- ♦ *Suma kontrolna* — zawiera *pseudonagłówek*, który pomaga odbiorcy stwierdzić, czy segment dotarł do właściwego celu. Pole opcjonalne, o długości dwóch bajtów.

Format nagłówka warstwy internetowej

Nagłówek warstwy internetowej, przedstawiony na rysunku 2.19, składa się z następujących pól:

Rysunek 2.19.

Format nagłówka warstwy internetowej

Wersja	HLEN	Typ usługi	Długość całkowita	
Identyfikacja			Flagi	Przesunięcie fragmentu
Czas życia	Protokół		Suma kontrolna nagłówka	
Źródłowy adres IP				
Docelowy adres IP				
Opcje IP				Wypełnienie

- ♦ *Wersja* — określa wersję protokołu IP. Obecnie stosowana jest wersja 4 (*IPv4*). Pole o długości czterech bitów.
- ♦ *Długość* — zawiera długość nagłówka warstwy internetowej. Pole o długości czterech bitów.

- ♦ *Typ usługi* — zawiera informacje, jak należy przetwarzać datagram oraz o pożądanej jakości usług (QoS — *Quality of Service*). Pole o długości jednego bajta.
- ♦ *Długość całkowita* — zawiera całkowitą długość datagramu, łącznie z nagłówkiem i zawartymi danymi. Pole o długości dwóch bajtów.



Długość tego pola — 16 bitów wskazuje, iż maksymalna długość datagramu (pakietu) IP może wynosić 65 535 bajtów (2¹⁶). Minimalna długość pakietu IP wynosi 576 bajtów.

- ♦ *Identyfikacja* — zawiera informacje służące do ponownego złożenia datagramu z fragmentów. Pole o długości dwóch bajtów.
- ♦ *Flagi* — zawiera trzy poniższe flagi sterujące:
 - ♦ *Bit 0* — zarezerwowany; jego wartość musi zawsze wynosić 0.
 - ♦ *Bit 1* — jeśli jego wartość wynosi 0, datagram można pofragmentować. Jeśli jest równa 1, datagramu fragmentować nie wolno.
 - ♦ *Bit 2* — jeśli jego wartość wynosi 0, fragment jest ostatni w strumieniu danych i nie następują po nim żadne dalsze. Jeśli wynosi 1, po fragmencie następują kolejne.
- ♦ *Przesunięcie fragmentu* — zawiera pozycję fragmentu w datagramie, jeśli jest on podzielony na fragmenty. Pole o długości trzynastu bitów.
- ♦ *Czas życia (TTL — Time to Live)* — zawiera maksymalny czas życia (w sekundach), przez jaki datagram może istnieć. Każdy ruter, przez który datagram przechodzi po drodze do celu, zmniejsza tę wartość o 1. Gdy wartość w polu spadnie do zera, datagram zostaje odrzucony. Pole o długości jednego bajta.
- ♦ *Protokół* — zawiera informacje o protokole warstwy aplikacji, który zapoczątkował żądanie. Pole o długości jednego bajta.



Wartości odpowiadające poszczególnym protokołom wyszczególnione są w RFC 1700.

- ♦ *Suma kontrolna nagłówka* — zawiera sumę kontrolną jedynie z samego nagłówka IP. Po każdej modyfikacji nagłówka tę wartość trzeba obliczyć na nowo. Pole o długości dwóch bajtów.
- ♦ *Źródłowy adres IP* — zawiera adres IP urządzenia nadawczego. Pole o długości czterech bajtów.
- ♦ *Docelowy adres IP* — zawiera adres IP urządzenia odbiorczego. Pole o długości czterech bajtów.
- ♦ *Opcje IP* — zawiera informacje o kilku funkcjach IP. Pole ma zmienną długość.
- ♦ *Wypełnienie* — zawiera ciąg zer, dodanych do nagłówka, aby jego długość wynosiła 32 bajty. Pole o zmiennej długości.



Format nagłówka warstwy interfejsu sieciowego opisany jest w rozdziale 4.