helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

IDŹ DO
PRZYKŁADOWY ROZDZIAŁ
SPIS TREŚCI

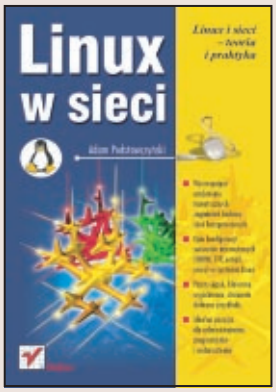
KATALOG KSIĄŻEK
KATALOG ONLINE
ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK
DODAJ DO KOSZYKA

CENNIK I INFORMACJE
ZAMÓW INFORMACJE O NOWOŚCIACH
ZAMÓW CENNIK

CZYTELNIA
FRAGMENTY KSIĄŻEK ONLINE

Linux w sieci



Autor: Adam Podstawczyński
ISBN: 83-7197-834-0
Format: B5, stron: 224

Linux to jeden z najlepiej przystosowanych do pracy w sieci systemów operacyjnych. Doskonale nadaje się na sieciową stację roboczą, serwer rozmaitych usług (WWW, FTP, e-mail, news), może również służyć jako oprogramowanie komputera spełniającego funkcje routera. Ocenia się, że ponad 1/3 serwerów WWW oparta jest na Linuksie, co sprawia, że osoby znające sieciowe zastosowania tego systemu operacyjnego są szczególnie poszukiwane na rynku pracy.

Adam Podstawczyński, autor bestsellerowego poradnika „Linux. Praktyczne rozwiązania", tym razem przedstawia wyczerpujący, dokładny a zarazem przystępny opis obsługi sieci przez Linuksa. Książka rozszerzy Twoją wiedzę nie tylko na temat systemu Linux, poznasz wiele niezależnych od systemu operacyjnego zagadnień pozwalających lepiej zrozumieć funkcjonowanie Internetu.

Mimo, iż książka nie ma charakteru przewodnika opisującego krok po kroku konfigurowanie Linuksa, to z pewnością pomocna będzie przy rozwiązywaniu problemów z tym systemem. Od rozważań teoretycznych na temat modelu OSI do opisu budowy kabla sieciowego – to wszystko znajdziesz w tej doskonałej książce. Jest to idealna pozycja dla administratorów, programistów i webmasterów.

Opisano w niej między innymi:

- Model OSI – teoretyczny model sieci
- Obsługę kart sieciowych przez system Linux
- Konfigurowanie połączeń PPP
- Instalację sieci bezprzewodowych
- Warstwę sieciową: ARP, IP, ICMP
- Warstwę transportową
- Konfigurowanie zapór sieciowych
- Obsługę DNS w Linuksie
- Bezpieczne połączenia przez SSH
- Teoretyczne zagadnienia budowy sieci komputerowych
- Opis konfiguracji serwerów internetowych (WWW, FTP, e-mail, news) w systemie Linux

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

Spis treści

Wprowadzenie 7

Rozdział 1. Model OSI 13

Komunikacja w warstwach — uproszczony opis 15
Warstwy OSI — co mówi teoria 17
Warstwa 1 fizyczna 18
Warstwa 2 łącza danych 18
Warstwa 3 sieciowa 19
Warstwa 4 transportowa 19
Warstwa 5 sesji 20
Warstwa 6 prezentacji 20
Warstwa 7 aplikacji 20
OSI a TCP/IP 20
Systemy końcowe a systemy pośrednie 21

Rozdział 2. Warstwa fizyczna i warstwa łącza danych 25

Topologie 25
Ethernet 26
Historia 26
Ogólna zasada działania 27
Typy Ethernetu i okablowanie 29
Karty sieciowe 32
Wtórniki, koncentratory, przełączniki... 34
Instalacja karty sieciowej w Linuksie 35
Format ramki ethernetowej 40
Podglądanie pakietów 43
Tryb bezładny 46
PPP 47
Port szeregowy 47
Połączenie kablem szeregowym 49
Połączenie z usługodawcą 66
Komunikacja bezprzewodowa — przykładowe rozwiązanie 71

Rozdział 3. Warstwa sieciowa 75

ARP 75
Pakiet ARP 76
IP 81
Pakiet IP 82
Adres IP 89
Routing 99
IPsec 102

ICMP ... 108
Typy ICMP 0 i 8 oraz program ping ... 108
Typ ICMP 3 — Host Unreachable ... 111
Typ ICMP 5 i przekierowanie w routingu ... 114
Typy ICMP 9 i 10 oraz wykrywanie routerów ... 115
Typ ICMP 11 i program traceroute ... 115

Rozdział 4. Warstwa transportowa ... 119
Klient, serwer ... 119
Własny serwer w 3 minuty ... 121
Protokół TCP ... 124
Pakiet TCP ... 124
Trójfazowe uzgadnianie połączenia ... 125
Połączenie TCP w trakcie ... 128
Opcje TCP ... 132
Kończenie połączenia TCP ... 136
Stany połączenia TCP ... 137
TCP a UDP ... 142
Porty i usługi ... 143
Pośrednik w usługach: inetd i tcpd ... 145
Zapory sieciowe ... 149
Ogólna zasada działania ... 150
Zapora w Linuksie 2.2 — ipchains ... 150
Zapora w Linuksie 2.4 — iptables ... 165

Rozdział 5. To, co nie mieści się w warstwach ... 179
DNS ... 179
DNS z punktu widzenia klienta — resolver ... 181
Przykładowy serwer DNS — buforujący ... 182
Wysyłanie żądań DNS „z palca” ... 193
SSH ... 195
Klucze publiczne i prywatne ... 196
Komunikacja SSH „na żywo” ... 196
Przekierowywanie portów przez SSH ... 199

Dodatek A Opcje konfiguracyjne jądra 2.4 i zmienne sysctl ... 205
Zmienne sysctl ... 206

Dodatek B Bibliografia ... 207
Książki ... 207
Źródła online ... 208
HOWTO ... 209
Dokumenty RFC ... 211

Skorowidz ... 213

Rozdział 1.
Model OSI

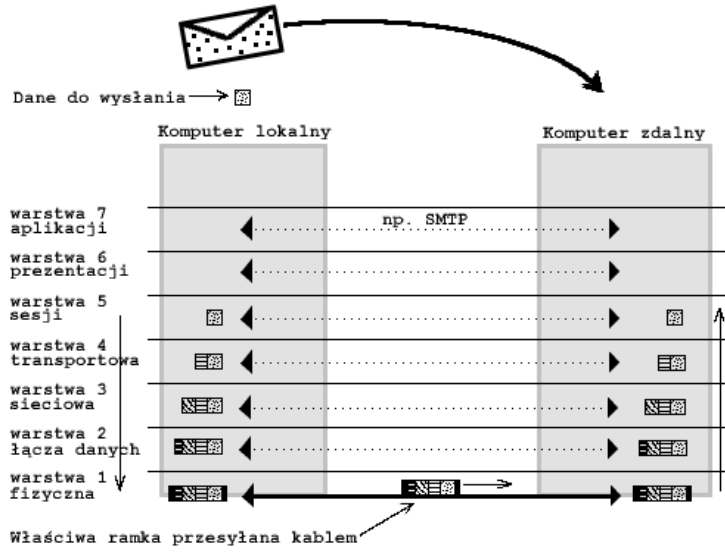
Kiedy oglądamy pełną zdjęć i animacji stronę WWW, rzadko zastanawiamy się nad tym, w jaki sposób wszystkie te dane docierają do okna naszej przeglądarki. A już na pewno mało kto słyszał o abstrakcyjnym modelu OSI, który opisuje sposób komunikacji w sieciach komputerowych. To właśnie przez kolejne warstwy modelu OSI „przedostają się" dane pobierane i wysyłane przez przeglądarkę, program pocztowy, program do chatowania itd. Wszystko to dzieje się w sposób „przezroczysty" dla użytkownika, dlatego poza osobami zainteresowanymi samym działaniem sieci — takimi jak Czytelnik tej książki — mało kto zaprząta sobie głowę całym tym mechanizmem.

Tak naprawdę nawet użytkownicy z zacięciem technicznym mogą sporo dowiedzieć się o funkcjonowaniu sieci w ogóle nie zaprzątając sobie głów nieciekawie brzmiącym skrótem „OSI". Model OSI nie jest związany z żadnym konkretnym rozwiązaniem sprzętowym czy oprogramowaniem, nie opisuje również żadnej konkretnej implementacji sieci. Ponieważ jednak poszczególne warstwy tego modelu względnie dobrze odpowiadają podziałowi na różne mechanizmy, jakie rzeczywiście biorą udział w komunikacji sieciowej, oraz ponieważ na pewnym etapie Czytelnik może spotkać się z takimi pojęciami, jak „przełącznik warstwy 2" czy „protokoły warstwy 3", autor postanowił rozpocząć właśnie od opisania modelu OSI. Zaznajomienie Czytelnika z warstwami modelu OSI umożliwi również bardziej przejrzyste przedstawienie pozostałego materiału książki — trzy najważniejsze rozdziały (2., 3. i 4.) „pną się" po warstwach sieci, rozpoczynając od dwóch najniższych.

W modelu OSI zdefiniowano siedem warstw, z których każda opisuje inną część komunikacji sieciowej. Najogólniej można powiedzieć, że im wyższa warstwa, tym „bliżej użytkownika", a im niższa warstwa, tym „bliżej kabla". Spójrzmy na rysunek 1.1.

Z punktu widzenia użytkownika informacje przesyłane są między jego aplikacją (np. przeglądarką czy programem pocztowym) a aplikacją zdalną (np. serwerem WWW czy programem pocztowym innego użytkownika). Tak jakby komunikacja była dwustronna: aplikacja-aplikacja, użytkownik-użytkownik. W rzeczywistości w wymianie danych uczestniczy o wiele więcej mechanizmów. Porcja danych wysyłana przez program użytkownika przekazywana jest kolejnym, coraz niższym warstwom. Dopiero w najniższej warstwie zamieniana jest na impulsy elektryczne i fizycznie przesyłana

Rysunek 1.1.



przez kabel sieciowy (albo inny nośnik). Po dotarciu do komputera docelowego znów wędruje przez kolejne warstwy, ale tym razem w odwrotnym kierunku — bity i bajty przekazywane są „ku górze", aż zostaną odebrane przez właściwą aplikację i użytkownika.

Dlaczego tak ważne było stworzenie modelu precyzyjnie rozdzielającego między poszczególne warstwy różne zadania związane z komunikacją? Chodzi o przezroczystość i niezależność. Użytkownik — szczególnie ten mało interesujący się komputerami — widzi tylko, że informacje są przesyłane, np. że e-mail dotarł albo że znajomy odesłał odpowiedź. W ogóle nic nie wie o wszystkich tych warstwach i mechanizmach biorących udział w przesyłaniu danych — są one dla niego „przezroczyste".

Za to wysłany e-mail może być przesyłany nie tylko między różnymi programami pocztowymi, systemami operacyjnymi i typami sieci (np. rozległymi i lokalnymi), ale także za pośrednictwem najróżnorodniejszych łączy fizycznych — w tym różnych rodzajów kabli — a nawet w sposób bezprzewodowy. Ponieważ role poszczególnych warstw zostały dokładnie określone w modelu OSI i ponieważ każda warstwa „spodziewa się" otrzymania danych w ściśle określonym formacie, możliwe jest zupełne rozdzielenie mechanizmów, oprogramowania i sprzętu odpowiedzialnych za realizację tych warstw. Tak więc twórcy programu pocztowego nie obchodzi np. to, jak przebiega trójfazowe nawiązywanie połączenia TCP między klientem a serwerem, zaś programista funkcji sieciowych systemu operacyjnego nie musi nic wiedzieć o tym, na czym polega przesyłanie fal świetlnych w światłowodzie. Producenci sprzętu, programiści, administratorzy sieci, twórcy programów użytkowych — wszyscy oni mogą pracować niezależnie i zajmować się „swoimi działkami". Muszą wiedzieć tylko, według jakich zasad dane wymieniane są z warstwami sąsiadującymi. Zasady te opisane są odpowiednimi specyfikacjami i protokołami.

O tym, co dzieje się w poszczególnych warstwach — szczególnie w najniższych czterech — jest właściwie cała ta książka. Żeby jednak uzyskać ogólny pogląd na całość i wstępnie zrozumieć, na czym polega wymiana danych w sieci komputerowej, przyjrzyjmy się teraz w skrócie poszczególnym warstwom oraz roli, jaką odgrywają w komunikacji.

Komunikacja w warstwach — uproszczony opis

Zacznijmy od samej góry. Np. po kliknięciu w programie pocztowym przycisku „Wyślij" rozpoczyna się komunikacja między naszym komputerem a docelowym serwerem pocztowym. Przesyłanie e-maili najczęściej odbywa się za pośrednictwem protokołu SMTP, w którym obie strony wymieniają między sobą najpierw wstępne informacje (np. adresy źródłowy i docelowy), a potem właściwą treść wiadomości. Ta tekstowa wymiana informacji przypomina nieco dialog między ludźmi (— Cześć, mam e-mail do przesłania. — Cześć, rozumiem. — To będzie e-mail od adam@english.w3.pl. — OK, zrozumiałem... itd.), ale oczywiście wszystkie „zawołania" i „odpowiedzi" mają ściśle standardowy format. Program pocztowy, nawiązując tego typu komunikację, korzysta właśnie z najwyższej warstwy modelu OSI — warstwy aplikacji. Warstwa aplikacji (w tym przypadku protokół SMTP) systemu lokalnego komunikuje się z warstwą aplikacji systemu zdalnego. Komunikacja na tej abstrakcyjnej warstwie może sprawnie przebiegać bez znajomości wszystkich niższych warstw. I choć w rzeczywistości nie przebiega żaden „kabel" pomiędzy lokalną a zdalną warstwą aplikacji, to nawiązane zostało wirtualne połączenie (na rysunku oznaczone przerywaną linią), za pośrednictwem którego zostanie przesłany nasz e-mail.

Aby aplikacje mogły ze sobą „rozmawiać" za pomocą protokołu SMTP, tak jak to pokazano na rysunku 1.1, musi istnieć kanał komunikacyjny między odpowiednimi dwoma systemami komputerowymi. Kanał, który zapewni niezawodne dostarczanie poszczególnych porcji danych do punktu przeznaczenia, będzie odpowiadał za sterowanie przepływem danych i umożliwi ponowienie transmisji, gdyby poszczególne pakiety IP gdzieś po drodze „zgubiły się". W sieciach TCP/IP za te wszystkie funkcje odpowiada protokół TCP, funkcjonujący na innym poziomie — w innej warstwie niż opisywana wyżej „konwersacja" SMTP. Tym razem wirtualne połączenie (znów przerywana linia) odbywa się w warstwie... transportowej. Zaraz, a gdzie podziały się warstwa 6 i 5? Wszystko wyjaśni się już wkrótce, gdy powiemy o rozbieżnościach pomiędzy protokołami TCP/IP a modelem OSI. Tymczasem jednak rozumiemy, że na poziomie warstwy 4 — transportowej — tworzony jest kanał komunikacyjny, którego zadaniem jest przede wszystkim zapewnienie, że przesyłane informacje docierają na miejsce oraz że dotrą tam we właściwej kolejności (zapewnia niezawodność przesyłania danych).

Dalej komunikacja odbywa się już zgodnie z rysunkiem 1.1. Żeby opisany wyżej kanał komunikacyjny mógł być utworzony, musi istnieć sposób na „znalezienie się" dwóch końców tego kanału. Przecież w Internecie rzadko jest tak, że dwa komunikujące się komputery połączone są jednym, bezpośrednim łączem. Zazwyczaj informacja, zanim dotrze na miejsce, przechodzi przez wiele systemów pośrednich (patrz także podrozdział „Systemy końcowe a systemy pośrednie"). Trzeba więc zapewnić mechanizm, który umożliwi określonej porcji danych odnalezienie drogi do punktu przeznaczenia w gąszczu komputerów i sieci. To „odnajdywanie drogi" nazywa się *routingiem* i odbywa się na poziomie warstwy 3, sieciowej. Żeby możliwe było odnalezienie właściwej trasy, najpierw musi być oczywiście znany adres docelowy. Dlatego również tutaj, w warstwie 3, realizowane jest adresowanie internetowe — czyli to tu następuje obsługa adresów IP. To właśnie protokół IP i warstwa sieciowa odpowiadają za całą „magię"

Internetu — za to, że informacje docierają z jednego końca świata na drugi oraz za to, że w wyjątkowych przypadkach pakiet z Wrocławia do Łodzi może podróżować... przez ocean!

No dobrze, w warstwie 3 wszystko wygląda bardzo przejrzyście: jest adres źródłowy IP i jest adres docelowy, a pakiet dociera tam gdzie trzeba optymalną (choć nie zawsze!) trasą. Ale przecież każdy wie, że Internet to „sieć sieci", a więc trasa pakietu może przebiegać przez bardzo różne obszary. Stacja wysyłająca może się znajdować np. w ethernetowej sieci lokalnej (LAN). Po wyjściu z tej sieci pakiet może być przesyłany przez łącze typu „punkt-punkt" z usługodawcą — np. po zwykłym kablu telefonicznym. Stamtąd może biec łączem światłowodowym aż do innej sieci lokalnej, w której z kolei odbierany jest przez stację sieci lokalnej typu Token Ring. Na poziomie warstwy 3 różnice między tymi sieciami nie mają znaczenia. Za to w warstwie 2, czyli łącza danych — owszem! To właśnie tutaj obsługiwane są takie technologie sieciowe, jak Ethernet, Token Ring i inne. To tu do pakietu IP (w którym jest informacja o dwóch adresach, np. 192.168.0.1 i 192.168.3.2, i niewiele więcej) dodawane są nagłówki specyficzne dla konkretnego typu sieci — np. zawierające adresy sprzętowe kart sieciowych. Pakiet w tej postaci (często nazywany „ramką"), gotowy do przesłania, przekazywany jest następnie najniższej warstwie — fizycznej.

I dopiero tutaj kolejne bity porcji danych zamieniane są na impulsy elektryczne (lub świetlne, ew. radiowe) i przesyłane w fizycznym nośniku. W warstwie fizycznej zaczynają mieć znaczenie takie pojęcia, jak RJ45, BNC czy ST (typy złączy), skrętka i światłowód wielomodowy (typy kabli) czy „baseband" i „broadband" (typy modulacji). Ta warstwa jest zazwyczaj realizowana całkowicie sprzętowo. „Zazwyczaj", bo istnieją przecież programowe emulatory złączy szeregowych, portów USB czy nawet całych komputerów.

A potem? Potem wszystko dzieje się odwrotnie. Pakiet, który dotarł do miejsca przeznaczenia, wędruje „w górę" stosu warstw: impulsy zamieniane są na bity, potem na ramki, z ramki konkretnej sieci „obcinane" są informacje sterujące i „powstaje" pakiet IP, warstwa czwarta „widzi" już tylko kanał komunikacyjny, protokół SMTP „rozmawia" z drugą stroną połączenia, a odbiorca e-maila... widzi nową wiadomość w skrzynce. Gdyby nie istniał standardowy podział na warstwy, program pocztowy musiałby umieć zrobić wszystkie opisane wyżej czynności! To oczywiście ograniczałoby jego zastosowanie tylko do bardzo konkretnej sieci i to pewnie opartej na konkretnym rodzaju okablowania — mniej popularne typy sieci nie byłyby na pewno obsługiwane. Dzięki spójnemu modelowi warstw programista praktycznie nie musi myśleć w ogóle o warstwach niższych niż 4, a program będzie działał zarówno w Ethernecie, jak i przez łącza PPP, w sieci bezprzewodowej czy choćby przez łącze na podczerwień.

To tylko przykładowy i uproszczony opis. Nie tylko warstwy zostały omówione pobieżnie, ale niektóre z nich w ogóle pominięto. Poza tym wzięto tutaj pod uwagę wyłącznie sytuację rzadko spotykaną — taką, w której komputer-nadawca jest połączony bezpośrednio kablem z komputerem-odbiorcą. Szczegółowy, teoretyczny opis wszystkich warstw OSI znajduje się poniżej („Warstwy OSI — co mówi teoria"). O tym, dlaczego pominięto niektóre warstwy, mówi podrozdział „OSI a TCP/IP". Natomiast o tym, jak to wszystko ma się do rzeczywistej komunikacji sieciowej — gdy informacje przebiegają przez wiele komputerów pośrednich — można przeczytać w podrozdziale „Systemy końcowe a systemy pośrednie".

Warstwy OSI — co mówi teoria

Przyjrzyjmy się nieco bardziej szczegółowo — i bardziej technicznie — warstwom protokołu OSI. Cała koncepcja warstw opiera się na pojęciu **usługi**, którą pewna warstwa niższa (nazwijmy ją *n*) świadczy warstwie „o jeden wyższej" (warstwie *n+1*). Warstwa *n* odpowiedzialna jest za pewien mechanizm w komunikacji między systemami. Mechanizm ten realizowany jest za pomocą **protokołu**, przy czym sam model OSI nie definiuje ani nie wymaga stosowania określonych protokołów — opisuje jedynie ogólnie, jakie usługi mają być świadczone przez daną warstwę. Dzięki takiemu podziałowi twórcy konkretnych protokołów, aplikacji, urządzeń sieciowych itd. związanych z poszczególnymi warstwami mogą pracować niezależnie: z autorytatywnych źródeł (np. od innych producentów, z dostępnych publicznie specyfikacji) wiedzą, jaką usługę świadczy warstwa niższa (jaki „interfejs" udostępnia) i nie muszą przejmować się, w jaki sposób jest ona wewnętrznie realizowana. Podobnie producentom rozwiązań warstwy wyższej udostępniają jedynie opis funkcjonalności protokołu swojej warstwy — i to ma wystarczyć. Tak więc jakiś protokół warstwy *n* może być wykorzystywany przez wiele różnych protokołów warstwy *n+1*, a sam może korzystać z różnych protokołów warstwy *n-1* i to bez konieczności komunikowania się z twórcami tych protokołów. Hierarchiczny zbiór wszystkich warstw zaimplementowany w konkretny sposób nosi nazwę **stosu protokołów** (np. stos TCP/IP).

Tak więc w modelu OSI występują dwa aspekty komunikacji. Aspekt „poziomy" to komunikacja między tymi samymi warstwami różnych urządzeń lub systemów (na rysunku 1.1 ten aspekt został oznaczony liniami przerywanymi). Aspekt „pionowy" to komunikacja między różnymi, sąsiadującymi warstwami tego samego urządzenia lub systemu. W aspekcie poziomym komunikacja jest możliwa dzięki przyjęciu wspólnego protokołu wymiany danych. W aspekcie pionowym sąsiadujące warstwy są w stanie wymieniać informacje dzięki przyjęciu określonego interfejsu programowania (API) oraz założeniu, że dana warstwa świadczy ściśle określoną usługę.

Komunikat przesyłany w warstwie *n* składa się z **informacji sterujących** i **treści**. Informacje sterujące mają postać **nagłówka** i (opcjonalnie) **zakończenia**, którymi „opakowana" jest treść. W treści komunikatu warstwy *n* znajduje się wszystko to, co należy do warstwy *n+1*, czyli znów: informacje sterujące i treść. I tak dalej, dopóki treści nie stanowią faktyczne informacje, które mają zostać dostarczone do użytkownika lub innego systemu — np. treść e-maila. W warstwie sieciowej systemu OSI taki komunikat składający się z informacji sterujących i treści nazywa się **pakietem**; na drugiej warstwie używa się również pojęcia **ramki**. Z kolei w warstwie transportowej porcję danych często określa się mianem **datagramu**, zaś ogólnie porcję danych na różnych warstwach nazywa się także **segmentem**. Do tego dochodzi jeszcze pojęcie **oktet**, którym część autorów określa po prostu bajt, najczęściej przy okazji opisywania strumienia bitów. Rozróżnienie „oktet-bajt" wprowadzono dlatego, że dokładnie rzecz biorąc, bajt nie zawsze musi składać się z ośmiu bitów (np. w komunikacji z terminalami kiedyś często składał się z 7 bitów); natomiast oktet, jak sama nazwa wskazuje, to dokładnie 8 bitów. Ponieważ nawet autorzy specyfikacji i oprogramowania sieciowego nie są konsekwentni w zakresie opisanej w tym akapicie terminologii, w książce nie będziemy sztywno trzymali się określonych terminów w odniesieniu do porcji danych w różnych warstwach — rozróżnienie będziemy stosować tylko tam, gdzie ma to rzeczywiście znaczenie.

Jak więc przesyłany jest pakiet z systemu do systemu? Otóż w systemie „nadającym" pakiet przemieszcza się „w dół" drabiny warstw. Warstwa *n* otrzymuje pewną treść, opatruje ją swoimi informacjami sterującymi i „wysyła", korzystając z usług świadczonych przez warstwę *n-1*. Ta z kolei otrzymuje cały pakiet (dla niej widoczny jest jako „treść"), opatruje go swoimi informacjami sterującymi i znów „wysyła", korzystając z usług świadczonych przez niższą warstwę. W ten sposób komunikat, opatrzony wieloma warstwami informacji sterujących, dociera do najniższej warstwy. Tutaj jest on już rzeczywiście wysyłany przez określony nośnik (np. kabel telefoniczny), w przeciwieństwie do warstw wyższych, gdzie „wysyłanie" odbywa się po abstrakcyjnym (wirtualnym) łączu biegnącym do odpowiedniej warstwy systemu-odbiorcy.

W systemie odbierającym pakiet przemieszcza się „w górę". Coraz wyższe warstwy wycinają swoje informacje sterujące, a treść przekazują dalej. Pakiet jest tak „oskubywany" (techniczna nazwa to **demultipleksing**), aż — już jako konkretna informacja — trafi do odbiorcy. Należy przy tym zauważyć, że ani nadawca, ani odbiorca wcale nie muszą być ludźmi — mogą to być dwa systemy komputerowe (np. portal pobierający z innej witryny informacje o pogodzie).

Przyjrzyjmy się teraz bardziej szczegółowo kolejnym warstwom systemu OSI, tym razem jednak zaczynając od tej najniższej.

Warstwa 1 fizyczna

Warstwa fizyczna (*Physical Layer*) opisuje właściwości elektryczne i funkcjonalne faktycznego nośnika, po którym przesyłane są dane — kabla miedzianego, światłowodu, łącza bezprzewodowego itp. Warstwa ta różni się od pozostałych tym, że na jej poziomie rozpoznawane są tylko pojedyncze bity, a nie całe ramki ani nawet pojedyncze znaki. Jest to warstwa najbliższa sprzętowi — tutaj bity (a więc logiczne „jedynki" i „zera") zamieniane są na impulsy elektryczne (np. obecność napięcia lub jego brak). Bezpośrednio od warstwy fizycznej zależy również, z jaką szybkością dane mogą być przesyłane i na jaką odległość. Przykładowym działaniem tej warstwy jest zamiana bitów otrzymywanych z warstwy łącza danych na sygnały na odpowiednich stykach złącza równoległego w połączeniu PLIP.

Z tą warstwą związane są m.in. standardy (lub niektóre części standardów): ISDN, ADSL, FDDI, RS-232C, standardy okablowania, standardy komunikowania się modemów (w tym np. modemów telewizji kablowej), specyfikacje opisujące właściwości elektryczne i długości fal, Ethernet, X.25, Token Ring, ATM, Arcnet, standardy bezprzewodowe (np. 802.11b, IrDA) itd.

Warstwa 2 łącza danych

Warstwa łącza danych (*Data Link Layer*) zapewnia kontrolę błędów i sterowanie przepływem. Jest pierwszą warstwą, w której operuje się na porcjach danych większych niż bity — na *ramkach* (*frames*). W warstwie tej fizyczne łącze „udostępniane jest" jako łącze logiczne warstwom wyższym. Ponadto do tej warstwy należy dbanie o „sprawiedliwy" dostęp wielu urządzeń do jednego nośnika. Warstwa łącza danych

dzieli się na dwie podwarstwy: sterowania dostępem do nośnika (*Media Access Control — MAC*) i sterowania logicznym łączem (*Logical Link Control — LLC*). Ramka powstaje w efekcie współpracy obu tych podwarstw.

„Niżej" jest podwarstwa MAC — odpowiada ona za dostęp do nośnika, obsługę kolizji, adresów sprzętowych urządzeń.

Podwarstwa LLC odpowiedzialna jest za część *PDU* (*Protocol Data Unit*) ramki. W tej „warstwie-nakładce" do ramki może być dodawana informacja o tym, który protokół warstwy wyższej ma być wykorzystywany (np. IP); informacja ta może jednak również występować w warstwie MAC. Tu także odbywa się logiczne sterowanie łączem, które może przybierać różne formy: bezpołączeniowe (z potwierdzaniem otrzymania pakietów i bez potwierdzania) i połączeniowe (połączenie trwa dopóki, dopóty nie zostanie zerwane przez jedną ze stron).

Przykładowe standardy (lub części standardów) i technologie warstwy łącza danych to: Ethernet (IEEE 802.3), Token Ring (IEEE 802.5), adresy MAC, ATM, HDLC, SDLC, standardy bezprzewodowe, PPP.

Warstwa 3 sieciowa

Warstwa sieciowa (*Network Layer*) zapewnia komunikację w praktycznie całym Internecie. Jest to pierwsza warstwa, ponad którą aspekty fizyczne łącza, przez które przesyłane są dane, przestają mieć istotne znaczenie. Dwie podstawowe usługi warstwy sieciowej to: znajdywanie adresów oraz dostarczanie pakietu z komputera źródłowego do docelowego. Tym razem droga pakietu nie musi już przebiegać bezpośrednio z jednego systemu do drugiego — po drodze może być wiele komputerów i wiele różnych łączy fizycznych (w tym np. bezprzewodowych, światłowodowych itd.). To ta warstwa odpowiedzialna jest za znalezienie trasy do miejsca docelowego (routing), ale *nie gwarantuje*, że wszystkie pakiety dotrą na miejsce, oraz że dotrą tam we właściwej kolejności. Komunikacja w tej warstwie jest bezpołączeniowa, tzn. hosty nie nawiązują „konwersacji" — będzie ona miała miejsce dopiero w warstwie 4. W warstwie sieciowej odbywa się również tłumaczenie adresów sprzętowych (np. adresy MAC kart sieciowych) na adresy sieciowe (np. IP).

Na poziomie warstwy sieciowej odbywa się również fragmentacja (dzielenie większych pakietów tak, aby „mieściły się" w ramkach warstwy niższej) oraz zapewnia się dodatkowe mechanizmy, np. Quality of Service.

Najbardziej znanymi protokołami tej warstwy są IP (zarówno IPv4, jak i IPv6), ARP i ICMP. Inne standardy warstwy sieciowej to IPX, DDP.

Warstwa 4 transportowa

Warstwa transportowa odpowiedzialna jest za *niezawodne* dostarczanie informacji. Między stronami połączenia nawiązywany jest dialog, a więc mamy tutaj do czynienia z komunikacją połączeniową (choć komunikacja bezpołączeniowa jest również możliwa). Jeśli część informacji nie dotrze na miejsce (np. z powodu błędnego routingu), transmisja jest ponawiana. Na tym poziomie odbywa się kontrola błędów i sterowanie

przepływem. O ile w niższych warstwach miały jeszcze znaczenie systemy pośrednie (patrz podrozdział „Systemy końcowe a systemy pośrednie"), o tyle na poziomie tej warstwy mamy do czynienia już tylko z dwoma końcami połączenia — systemami końcowymi, często pełniącymi rolę odpowiednio serwera i klienta. Z drugiej strony, między dwoma tymi samymi systemami może istnieć wiele połączeń warstwy transportowej.

Dwa najbardziej znane protokoły tej warstwy to TCP (połączeniowy) i UDP (bezpołączeniowy). Na poziomie tej warstwy operują również protokoły zaawansowanego routingu, np. BGP czy OSPF.

Warstwa 5 sesji

W warstwie sesji odbywa się „konwersacja" między stronami połączenia. Ten dialog w wielu przypadkach nazywa się właśnie *sesją* i polega na utrzymywaniu przez jedną lub obie strony informacji o bieżącym stanie komunikacji. Umożliwia to np. odtworzenie sesji po czasowym zerwaniu połączenia. Na poziomie warstwy 5 *zakłada się* już, że niezawodne połączenie zostało ustanowione (przez warstwę 4).

Według różnych źródeł i sposobów rozumienia warstwy 5, zalicza się do niej częściowo protokół TCP, koncepcje „nazwanych potoków" oraz portów usług, protokół NetBIOS, AppleTalk (ADSP).

Warstwa 6 prezentacji

Warstwa ta udostępnia dane w pewien standardowy sposób na potrzeby aplikacji. W tej warstwie mogą również mieć miejsce takie procesy, jak szyfrowanie, kompresja i zmiana formatu przesyłanego tekstu (np. zmiana sposobu zapisu końca wiersza między systemami uniksowymi a Windows, przekodowanie między standardem EBDIC a ASCII).

Warstwa 7 aplikacji

Najwyższa, siódma warstwa pełni rolę interfejsu, przez który użytkownik lub aplikacja może korzystać z usług sieciowych.

Przykładowe zastosowania, standardy lub koncepcje, które można (czasem luźno) sklasyfikować na poziomie tej warstwy to: protokoły SMTP i X.400, FTP, protokoły zarządzania siecią (np. SNMP, NICE), zdalny dostęp do komputerów (np. Telnet, SSH, rlogin) itp.

OSI a TCP/IP

W dotychczasowym opisie modelu OSI łatwo zauważyć niespójności i celowe pominięcia. Wynika to z faktu, że model ten jest propozycją czysto teoretyczną. Powstał w latach 70. i 80. na biurkach pracowników komitetów normalizacyjnych CCITT (później ITU-T)

i ISO. Przy jego tworzeniu postawiono głównie na ścisłe przestrzeganie standardów — nie było wymogu zgodności z istniejącymi już implementacjami. Dlatego model OSI jest tak bardzo formalny i często... tak nieprzystający do rzeczywistości. Nad sposobem zapewnienia ujednoliconej komunikacji między sieciami (ang.: między = *inter*, sieć = *network* — *internetworking*) w rzeczywistych warunkach pracowano już wcześniej, w trakcie prac nad „prasiecią" — ARPANET-em. Już tam pojawiły się takie koncepcje, jak „warstwy" i „wirtualne połączenia", a więc to, co w OSI sformalizowano wiele lat później. Różnica między „protokołami ARPANET-u" — czyli późniejszym TCP/IP — a modelem OSI polegała na tym, że te pierwsze działały już w praktyce i zdążyły się upowszechnić. Rozwiązania zastosowane w protokołach TCP/IP wynikały z praktycznych potrzeb i poddawane były pod publiczną dyskusję w łatwo zrozumiałych dokumentach *RFC* (*Request For Comment*), które zresztą do dziś wytyczają drogę rozwoju Internetu. Przyjmowały się te standardy, które były najlepsze, które najwygodniej dało się implementować, lub które nie wymagały wprowadzania istotnych zmian w już funkcjonujących systemach. Natomiast standardy ISO dojrzewały powoli, protokoły były kłopotliwe w implementacji, a uzyskanie kopii samego standardu nie było (i wciąż nie jest) proste.

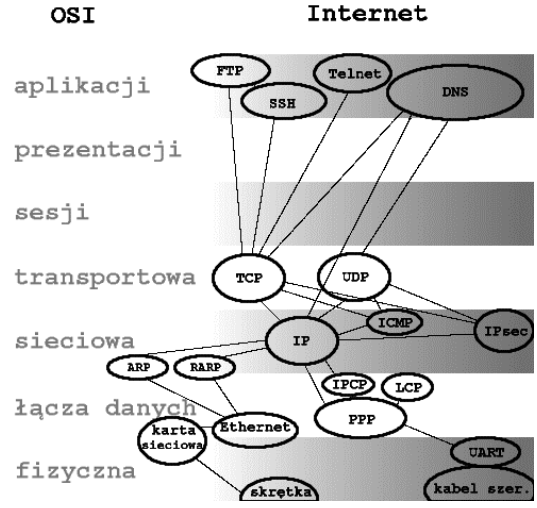
W wyniku tej sytuacji model OSI okazał się nieco spóźniony — został oficjalnie zaprezentowany wtedy, gdy większość komputerów rozwijającej się sieci globalnej korzystała już z TCP/IP. Dlatego, choć niewątpliwie OSI bardzo przejrzyście i jednoznacznie definiuje role poszczególnych warstw, rzeczywiście wykorzystywane standardy komunikacyjne nie zawsze idealnie pokrywają się z siedmioma warstwami modelu, a czasami wręcz zupełnie do niego nie przystają. Warstwy komunikacyjne Internetu są zdefiniowane luźniej; często nie mówi się wręcz o „warstwach", ale po prostu o „wyższych" lub „niższych" protokołach. W kontekście modelu OSI warstwą „graniczną" byłaby tutaj warstwa transportowa. Wszystko to, co ponad nią, określa się często mianem warstwy lub protokołów usług i aplikacji; wszystko co pod nią — warstwy lub protokołów sieci i podsieci, komunikacyjnych itp. W wielu nawet bardzo technicznych opisach zagadnień sieciowych taki rozdział zupełnie wystarcza.

Na przykład protokół IP stosunkowo dobrze „pasuje" do warstwy sieciowej. Jednak już protokół TCP można odwzorować na warstwę transportową i częściowo warstwę sesji OSI. Usługę DNS, bardzo powszechną w Internecie, w ogóle trudno przełożyć na model OSI; podobnie jest z mechanizmem ping (protokół ICMP) i protokołem SNMP. Z kolei np. warstwa 6, prezentacji, bardzo rzadko występuje „samodzielnie" — najczęściej implementowana jest jako część warstwy aplikacji lub sesji. Na rysunku 1.2 pokazano, jak niektóre „protokoły Internetu" — z naciskiem na te opisywane w niniejszej książce — wyglądają na tle warstw modelu OSI.

Systemy końcowe a systemy pośrednie

Dwa systemy komunikujące się w sieci komputerowej rzadko połączone są bezpośrednio. Najczęściej między systemami końcowymi (*end systems — ES*) występują dodatkowo systemy pośrednie (*intermediate systems — IS*).

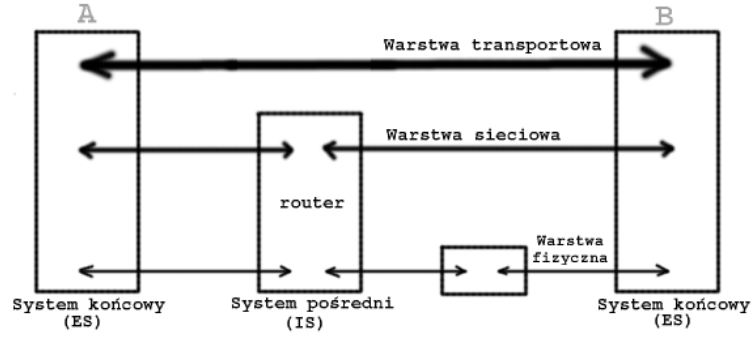
Rysunek 1.2.



Sposób rozumienia systemów końcowych i pośrednich może być różny na różnych warstwach. Np. kiedy w sieci lokalnej pakiety IP przesyłane są między dwoma komputerami, pomiędzy którymi znajduje się tylko przełącznik sieciowy, to z punktu widzenia warstwy sieciowej nie ma tutaj żadnych systemów pośrednich (administrator widzi tylko jedno połączenie między dwoma adresami IP); z punktu widzenia warstwy łącza danych i fizycznej systemem pośrednim jest przełącznik (można wyodrębnić dwa fizyczne połączenia: komputer A ↔ przełącznik oraz przełącznik ↔ komputer B).

Z kolei jeśli wziąć pod uwagę sytuację, w której komunikacja odbywa się między dwoma systemami znajdującymi się w różnych sieciach wchodzących w skład globalnego Internetu i w której pakiety przebiegają przez przynajmniej jeden router, wtedy połączenie jest typu „punkt-punkt" tylko z punktu widzenia warstwy transportowej i wyższych. Z punktu widzenia warstwy sieciowej występują tu już systemy pośrednie (routery). Ta sytuacja została zobrazowana na rysunku 1.3.

Rysunek 1.3.



Na rysunku 1.3 wyraźnie widać, że komunikacja w warstwach 4 i wyższych ma charakter „dwupunktowy" (najgrubsza strzałka) i brak tutaj systemów pośrednich. Dla tych warstw sposób realizacji komunikacji oraz obecność w nich systemów pośrednich nie ma znaczenia.

W warstwie 3, sieciowej, połączenia między routerami mają już znaczenie i są rozróżniane. Dlatego w zilustrowanym wyżej przykładzie można na tym poziomie wyróżnić dwa połączenia (pokazano komunikację z wykorzystaniem jednego routera). Router jest systemem pośrednim warstwy 3 (i niższych).

Dla urozmaicenia na rysunku wprowadzono również system pośredni warstwy łącza danych (najmniejszy prostokąt). Może to być np. przełącznik sieciowy. Warto zauważyć, że z punktu widzenia warstwy sieciowej urządzenie to nie ma znaczenia (router „widzi" bezpośrednio system końcowy B).

Jak widać, systemy pośrednie mogą występować w różnych warstwach modelu OSI. Można choćby dowodzić, że systemem pośrednim najwyższych warstw jest serwer pocztowy przekazujący nasz e-mail do innego serwera (*relaying*). Kiedy jednak mowa o systemach pośrednich w kontekście modelu OSI, bardzo często w domyśle dodaje się właśnie „warstwy trzeciej" — a więc słysząc „system pośredni" możemy przyjąć, że chodzi o router.