# Spis treści

# Wstęp

Podręcznik *Kwalifikacja E.13. Projektowanie lokalnych sieci komputerowych i administrowanie sieciami. Podręcznik do nauki zawodu technik informatyk. Część 1* omawia treści ujęte w nowej podstawie programowej. Jest przeznaczony dla szkół kształcących uczniów i słuchaczy w zawodzie technik informatyk. Treści zawarte w podręczniku mogą być z powodzeniem wykorzystywane również w przypadku innych kierunków kształcenia, a także przez osoby, które samodzielnie poszerzają swoją wiedzę z zakresu systemów operacyjnych z grupy Windows, Linux oraz sieci komputerowych.

W podręczniku duży nacisk został położony na praktyczne stosowanie zdobywanej wiedzy, co przekłada się na dużą liczbę opisanych instrukcji postępowania, które czytelnik może w łatwy sposób wykorzystać, pracując w systemie komputerowym.

Pierwszy tom podręcznika składa się z 6 rozdziałów. Ich budowa umożliwia realizację treści programowych w sposób wybrany przez nauczyciela.

Rozdział 1. „Sieć komputerowa" omawia podstawowe pojęcia związane z sieciami komputerowymi.

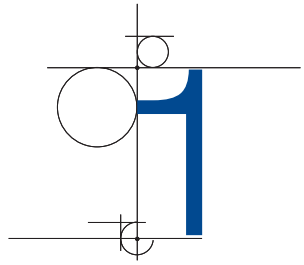
Rozdział 2. „Topologie sieci" prezentuje topologie fizyczne i logiczne wykorzystywane przy budowie sieci komputerowych.

Rozdział 3. „Medium transmisyjne" zawiera opis używanych w sieciach komputerowych mediów transmisyjnych, zarówno przewodowych, jak i bezprzewodowych.

Rozdział 4. „Protokoły sieciowe" omawia używane w sieciach protokoły transmisji danych oraz narzędzia pozwalające na diagnostykę zestawu protokołów TCP/IP.

Rozdział 5. „Urządzenia sieciowe" przedstawia urządzenia używane w sieciach komputerowych, które umożliwiają prawidłowe wykorzystanie zasobów sieciowych.

Rozdział 6. „Konfiguracja sieciowa systemów Windows" omawia sieciowe wykorzystanie systemów Windows zarówno jako stacji roboczej, jak i serwera.



# Sieć komputerowa

Siecią komputerową nazywa się grupę komputerów lub innych urządzeń połączonych ze sobą za pomocą dowolnego medium transmisyjnego w celu wymiany danych lub współdzielenia zasobów, np.:

- korzystania ze wspólnych urządzeń peryferyjnych i sieciowych (skanera, drukarki),
- korzystania ze wspólnego oprogramowania,
- korzystania z centralnej bazy danych,
- przesyłania danych (jak poczta elektroniczna, pliki itp.).

## 1.1. Rodzaje sieci

Sieci komputerowe mogą być sklasyfikowane w zależności od sposobu dostępu do zasobów oraz ze względu na obszar działania.

**DEFINICJA**

W zależności od sposobu dostępu do zasobów rozróżnia się dwa rodzaje sieci:

*Klient-serwer* — sieć, w której znajduje się jeden centralny serwer udostępniający dane.

*Peer-to-peer* (sieć równoprawna) — sieć, w której wszystkie urządzenia są równoprawne.

Przykładem sieci typu *klient-serwer* może być sieć oparta na domenie Active Directory. W sieci znajduje się centralny serwer (kontroler domeny) zarządzający uprawnieniami, który może pracować jako serwer plików (udostępniający dane) lub serwer wydruku (udostępniający drukarki).

Transmisja typu klient-serwer jest wykorzystywana także w przypadku wielu usług w internecie — np. strony WWW są umieszczane na serwerach, z których są pobierane za pomocą przeglądarki internetowej.

Komputery pracujące w sieci *peer-to-peer* są równorzędne wobec siebie, tak jak ma to miejsce w przypadku *grupy roboczej* w systemie Windows. Każdy z komputerów pełni

zarówno rolę klienta (pobierając dane z innego urządzenia), jak i serwera (dla innych urządzeń korzystających z udostępnionych zasobów).

**DEFINICJA**

Ze względu na obszar działania sieci komputerowej rozróżniane są sieci:

*LAN (ang. Local Area Network)* — sieć lokalna działająca na niewielkim, ograniczonym obszarze.

*MAN (ang. Metropolitan Area Network)* — sieć działająca na większym obszarze, np. miasta — LODMAN.

*WAN (ang. Wide Area Network)* — sieć rozległa działająca na dużym obszarze, np. polpak.

Przykładem sieci lokalnej LAN jest sieć obejmująca swoim zasięgiem budynek szkoły. Najczęściej spotyka się sieci zbudowane z wykorzystaniem technologii *Ethernet*.

Sieciami rozległymi można nazwać sieci dużych firm łączące oddziały na terenie całego kraju. Mianem sieci rozległej określamy również internet, który swoim zasięgiem obejmuje cały świat. Tego rodzaju sieci korzystają z wielu technologii transmisji na dalekie odległości, takich jak *Frame Relay*, *ATM*, *DSL*.

# 2

# Topologie sieci

***Topologie sieci*** lokalnych mogą być opisane zarówno na płaszczyźnie fizycznej, jak i logicznej. ***Topologia fizyczna*** określa organizację okablowania strukturalnego, ***topologia logiczna*** opisuje dostęp do medium fizycznego oraz reguły komunikacji, z których korzystają podłączone do sieci urządzenia. Obie płaszczyzny topologii są ściśle ze sobą powiązane.

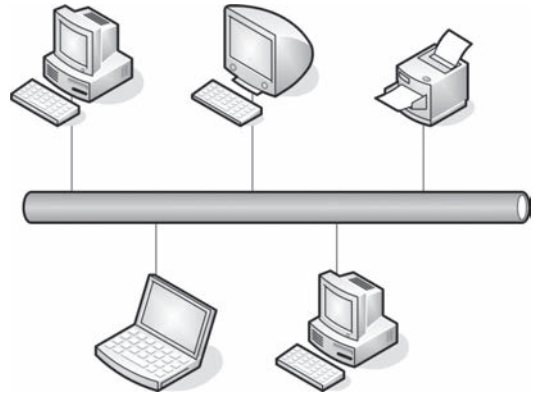
## 2.1. Topologie fizyczne

### 2.1.1. Topologia magistrali

**DEFINICJA**

W sieci zbudowanej w **topologii magistrali** (ang. *bus*) wszystkie elementy podłączone są do jednej wspólnej magistrali (zazwyczaj kabla koncentrycznego). Sieć umożliwia tylko jedną transmisję w danym momencie — sygnał nadany przez jedną ze stacji jest odbierany przez wszystkie pozostałe, lecz tylko adresat go interpretuje (rysunek 2.1).

**Rysunek 2.1.**
Topologia magistrali



Końce magistrali są wyposażone w tzw. terminatory (rysunek 2.2), których zadaniem jest wyeliminowanie odbicia sygnału od końca kabla. Odbicia te zakłócają, a nawet uniemożliwiają komunikację w sieci.

**Rysunek 2.2.**
Terminator

Maksymalna długość segmentu:

- cienki koncentryk (10Base2) — 185 m,
- gruby koncentryk (10Base5) — 500 m.

Maksymalna przepustowość łącza to 10 Mb/s.

Do zalet sieci budowanych w topologii magistrali należą: brak dodatkowych urządzeń sieciowych, takich jak koncentratory i przełączniki, spora odległość pomiędzy węzłami oraz użycie niewielkiej ilości kabla i niska cena instalacji sieci (węzły łączy pojedynczy kabel). Wśród wad trzeba wymienić często występujące kolizje, kłopotliwość lokalizacji usterek, możliwość przeprowadzenia tylko jednej transmisji w danym momencie oraz zagrożenie potencjalnym unieruchomieniem całej sieci za sprawą awarii głównego kabla lub nawet rozpięcia dowolnego złącza.

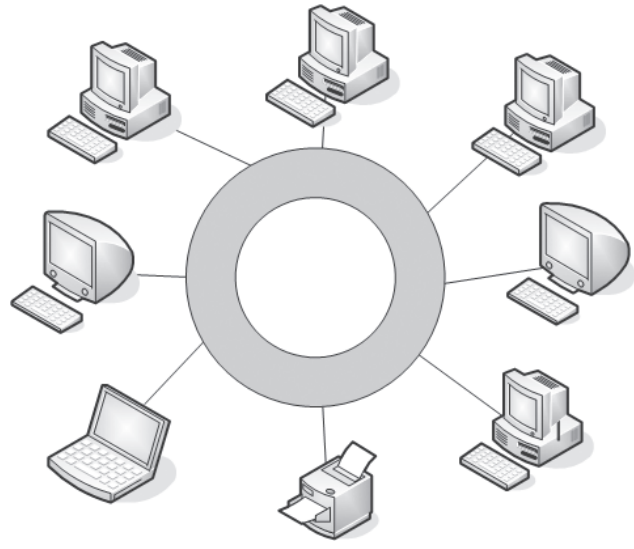
## 2.1.2. Topologia pierścienia

**DEFINICJA**

W sieci zbudowanej w **topologii pierścienia** (ang. *ring*) wszystkie węzły lub elementy połączone są za pomocą jednego nośnika w układzie zamkniętym — okablowanie tworzy krąg, nie występują zakończenia okablowania (rysunek 2.3). Stosowane są też metody podwójnych pierścieni (główny i dublujący). Sygnał wędruje w pętli między komputerami. Każdy komputer pełni funkcję wzmacniacza regenerującego sygnał i wysyłającego go dalej. Sieć w topologii pierścienia tworzona jest za pomocą kabla koncentrycznego lub światłowodu.

Zaletami sieci w topologii pierścienia są: użycie niewielkiej ilości przewodów, elastyczność w zakresie odległości pomiędzy węzłami sieci (w zależności od rodzaju wybranego medium). Wadą jest łatwość uszkodzenia sieci (uszkodzenie jednego węzła powoduje zatrzymanie transmisji w całej sieci), trudności w lokalizacji uszkodzeń, a także utrudniona rozbudowa sieci.

**Rysunek 2.3.**
Topologia pierścienia

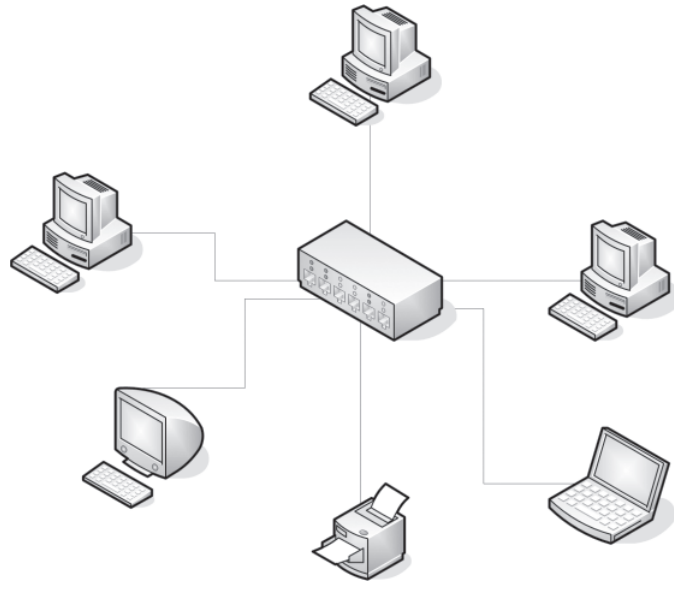


## 2.1.3. Topologia gwiazdy i gwiazdy rozszerzonej

**DEFINICJA**

**Topologia gwiazdy** (ang. *star*) charakteryzuje się tym, że okablowanie sieciowe (skrętka) łączy elementy sieci w centralnym punkcie, którym jest koncentrator lub przełącznik (rysunek 2.4).

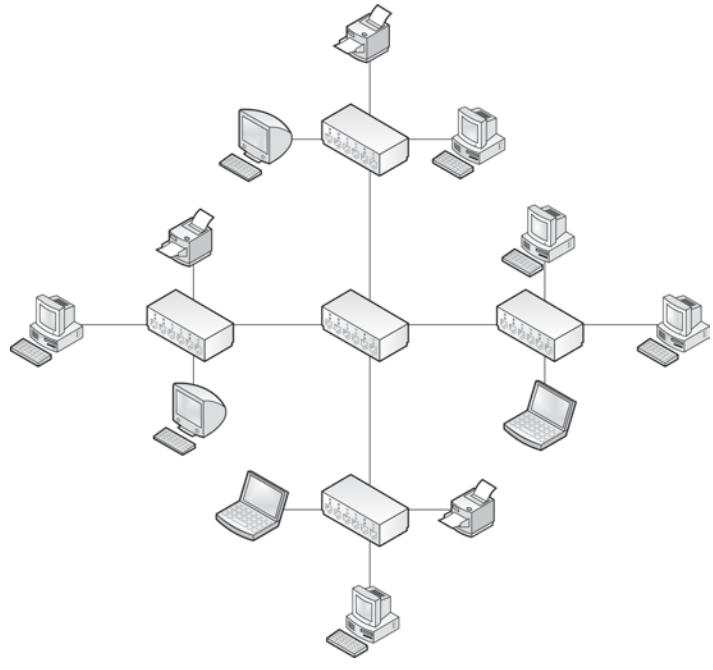
**Rysunek 2.4.**
Topologia gwiazdy



**DEFINICJA**

**Topologia gwiazdy rozszerzonej** jest oparta na topologii gwiazdy, w której gwiazdy połączone są między sobą za pomocą przełączników lub koncentratorów (rysunek 2.5). Ten rodzaj topologii pozwala na rozszerzenie zasięgu sieci i wzmocnienie sygnału między segmentami. Wadą takiej topologii jest wyższy koszt budowy związany z użyciem dodatkowych elementów sieciowych. Podobnie jak w topologii gwiazdy, wykorzystywana jest tutaj skrętka.

**Rysunek 2.5.**
Topologia
gwiazdy rozszerzonej



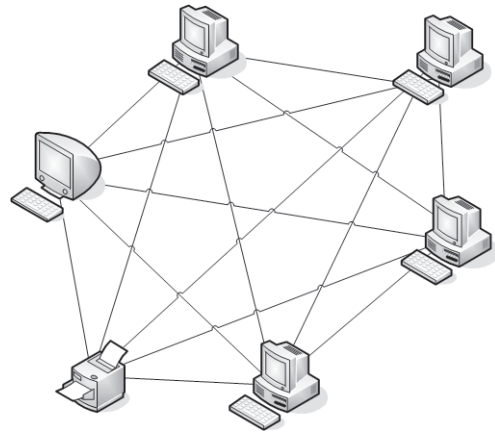
## 2.1.4. Topologia siatki

**DEFINICJA**

**Topologia siatki** polega na zapewnieniu wszystkim urządzeniom połączeń ze wszystkimi pozostałymi urządzeniami w sieci (rysunek 2.6). Oznacza to, że każdy host ma własne połączenie z pozostałymi.

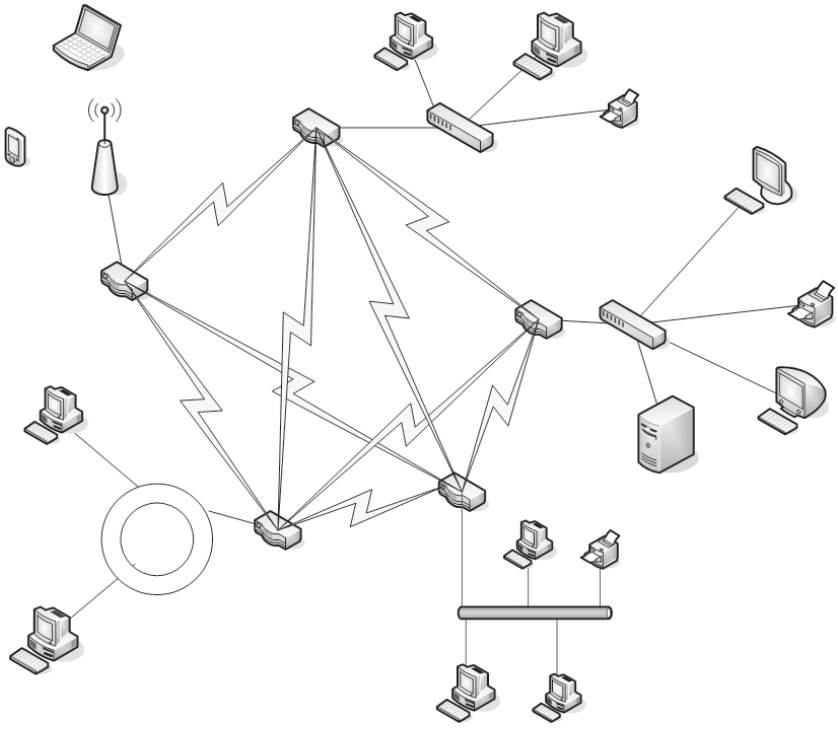
Rozwiązanie topologii siatki jest bardziej złożone. Projekt takiej sieci polega na łączeniu ze sobą urządzeń w ten sposób, że każde z nich połączone jest z więcej niż jednym urządzeniem sieciowym. Zalety tego rozwiązania to wysoka prędkość transmisji oraz odporność na uszkodzenia. Wadami tego rozwiązania są wysokie koszty urządzeń sieciowych oraz okablowania, a także kłopotliwa rozbudowa.

**Rysunek 2.6.**
Topologia siatki



## 2.1.5. Topologia siatki mieszanej

Topologia siatki mieszanej łączy w sobie różne rozwiązania — jest połączeniem co najmniej dwóch innych topologii z różnym rodzajem medium transmisyjnego (rysunek 2.7). Topologia sieci komputerowej tego typu jest stosowana w sieciach metropolitalnych oraz w sieciach rozległych (WAN).



**Rysunek 2.7.** Topologia siatki mieszanej

## 2.2. Topologie logiczne

Topologia logiczna opisuje metodę dostępu urządzeń sieciowych do medium transmisyjnego. Generalnie topologie logiczne są podzielone na:

- topologie rozgłaszania,
- topologie przekazywania żetonu (ang. *token*).

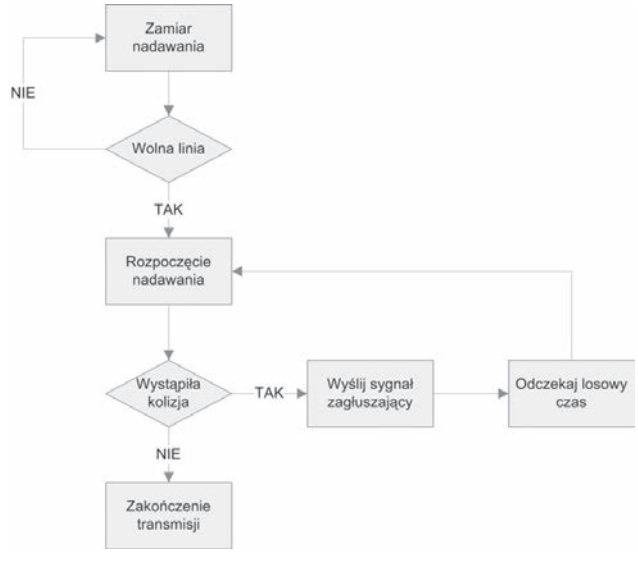
### 2.2.1. CSMA/CD

Dostęp do medium transmisyjnego w przypadku sieci Ethernet realizowany jest najczęściej przez protokół CSMA/CD (ang. *Carrier Sense Multiple Access/Collision Detection*), który jest przykładem topologii rozgłaszania. Protokół ten wykrywa, czy łącze jest dostępne, a także reaguje na występujące kolizje.

**DEFINICJA**

W sieci z protokołem CSMA/CD urządzenia przed nadawaniem sprawdzają, czy medium sieciowe nie jest zajęte. Jeśli węzeł wykryje, że sieć jest zajęta, będzie oczekiwał przez losowo wybrany czas przed ponowieniem próby. Jeśli węzeł wykryje, że medium nie jest zajęte, rozpocznie nadawanie i nasłuchiwanie. Celem nasłuchiwania jest upewnienie się, że żadna inna stacja nie nadaje w tym samym czasie. Po zakończeniu transmisji danych urządzenie powróci do trybu nasłuchiwania.

Jeśli dwa urządzenia rozpoczęły nadawanie w tym samym czasie, występuje kolizja, która jest wykrywana przez urządzenia nadawcze. Transmisja danych zostaje wówczas przerwana. Węzły zatrzymują nadawanie na losowo wybrany czas, po którym jest podejmowana kolejna próba uzyskania dostępu do medium (rysunek 2.8).




**Rysunek 2.8.** Algorytm blokowy działania mechanizmu CSMA/CD

Ta metoda transmisji jest wykorzystywana w sieciach Ethernet zbudowanych na bazie fizycznej topologii magistrali, gwiazdy, drzewa oraz siatki.

## 2.2.2. Token

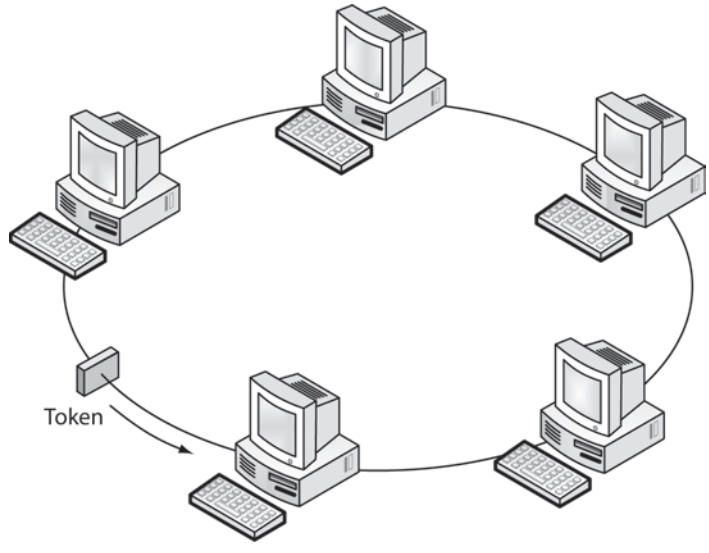
**DEFINICJA**

Dostęp do medium transmisyjnego jest realizowany przez przekazywanie żetonu. Żeton (ang. *token*) dostępu jest określoną sekwencją bitów zawierających informację kontrolną. Przejęcie żetonu przez urządzenie sieciowe zezwala na rozpoczęcie transmisji danych.

Każda sieć ma tylko jeden żeton dostępu przekazywany między kolejnymi węzłami sieci. Jeśli komputer ma dane do wysłania, usuwa żeton z pierścienia i rozpoczyna transmisję.

Dane wędrują po kolejnych węzłach sieci aż trafią do adresata. Komputer odbierający wysyła do komputera nadającego komunikat o odebraniu danych. Po weryfikacji komputer wysyłający tworzy nowy żeton dostępu i wysyła go do sieci (rysunek 2.9).

**Rysunek 2.9.** Działanie mechanizmu tokenu




Ta metoda transmisji jest wykorzystywana m.in. w sieciach Token Ring oraz FDDI.

**ĆWICZENIA**

1. Sprawdź, jaka topologia jest zastosowana w pracowni komputerowej.

## PYTANIA

1. Jak nazywa się punkt styku sieci kablowej i bezprzewodowej?
2. Opisz topologię magistrali. W jaki sposób uzyskuje się w niej dostęp do medium transmisyjnego?
3. W jakich sieciach wykorzystywany jest mechanizm przekazywania żetonu (tokenu)?
4. Scharakteryzuj topologię gwiazdy.

# 3

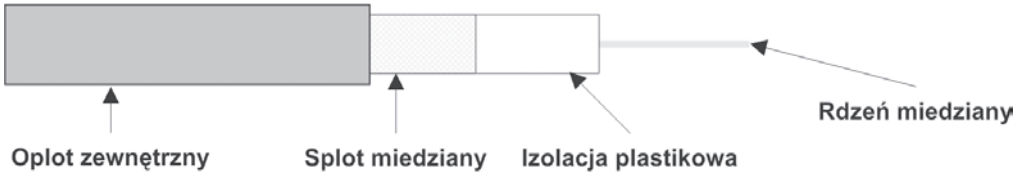
# Medium transmisyjne

Medium transmisyjne w sieciach komputerowych to nośnik informacji w postaci sygnałów określonego typu. Parametry transmisji zależą od parametrów użytego medium. Wyróżnia się media przewodowe i bezprzewodowe.

## 3.1. Media przewodowe

### 3.1.1. Kabel koncentryczny

Kabel koncentryczny składa się z miedzianego przewodnika (rdzenia) otoczonego warstwą elastycznej izolacji, która z kolei otoczona jest splecioną miedzianą taśmą lub folią metalową działającą jak drugi przewód oraz ekran dla znajdującego się wewnątrz przewodnika. Ta druga warstwa lub ekran zmniejsza także liczbę zewnętrznych zakłóceń elektromagnetycznych (rysunek 3.1).




**Rysunek 3.1.** Budowa kabla koncentrycznego

Podłączenie urządzeń do sieci komputerowej zbudowanej przy użyciu kabla koncentrycznego umożliwiają łącza typu BNC (rysunek 3.2). Ten rodzaj okablowania jest wykorzystywany w sieciach budowanych w topologii pierścienia lub magistrali. Obecnie praktycznie nie stosuje się go w sieciach komputerowych. Maksymalna prędkość transmisji dla kabla koncentrycznego wynosi 10 Mb/s, a maksymalna długość sieci to 500 m.

**Rysunek 3.2.**
Wtyk typu BNC

W przypadku sieci komputerowych używane są dwa rodzaje kabli koncentrycznych:

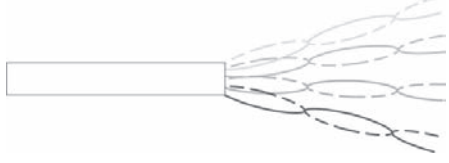
- gruby kabel koncentryczny 10Base5 (maksymalna długość segmentu 500 m),
- cienki kabel koncentryczny 10Base2 (maksymalna długość segmentu 185 m).

## 3.1.2. Kabel skręcany (Base-T)

Kabel skręcany (skrętka) składa się z zestawu 4 par żył miedzianych skręconych ze sobą. Skręcenie przewodów pozwala na wyeliminowanie zakłóceń elektromagnetycznych. Jest stosowany w topologii gwiazdy.

W skrętce każda żyła oznaczona jest osobnym kolorem: zielonym, pomarańczowym, niebieskim, brązowym oraz biało-zielonym, biało-pomarańczowym, biało-niebieskim, biało-brązowym (rysunek 3.3).

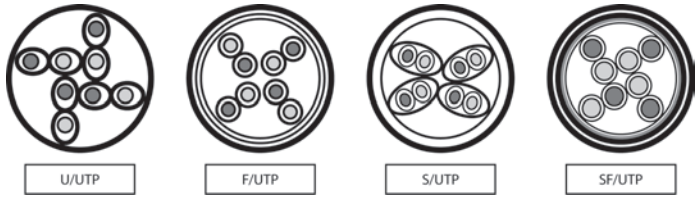
**Rysunek 3.3.**
Kabel typu skrętka



Ze względu na rodzaje stosowanego ekranowania wyróżnia się następujące kable typu skrętka (rysunek 3.4):

- U/UTP (ang. *Unshielded /Unshielded Twisted Pair*) — kabel skręcany nieekranowany. Stanowi najpopularniejszy środek transmisji danych, jest stosowany w pomieszczeniach.
- F/UTP (ang. *Foiled/Unshielded Twisted Pair*) — kabel skręcany ekranowany folią z przewodem uziemiającym. Stosuje się go na korytarzach lub na zewnątrz budynków.
- S/FTP (ang. *Shielded/ Foiled Twisted Pair*) — kabel skręcany z ekranem wykonanym w postaci foliowego oplotu każdej pojedynczej pary i dodatkowo zewnętrznej siatki.
- SF/UTP (ang. *Shielded/Foiled Twisted Pair*) — kabel skręcany z podwójnym zewnętrznym ekranem w postaci foliowego oplotu i siatki.

**Rysunek 3.4.**
Rodzaje okablowania typu skrętka



Kabel typu skrętka podłączany jest do gniazd i końcówek typu RJ45 (złącze 8P8C, rysunek 3.5). Dodatkowe informacje na temat okablowania strukturalnego znajdują się w rozdziale 3. tomu II — „Projektowanie i wykonanie sieci komputerowych".

**Rysunek 3.5.**
Końcówka RJ45.

Maksymalna długość połączenia za pomocą kabla typu skrętka pomiędzy dwoma urządzeniami wynosi 100 m. Po przekroczeniu tej odległości należy użyć aktywnych urządzeń sieciowych w celu wzmocnienia sygnału.

## 3.1.3. Światłowód

Coraz większą popularność jako typ okablowania zdobywa światłowód. Jest to spowodowane przede wszystkim jego dużą przepustowością, odpornością na zakłócenia, możliwością transmisji na dalekie odległości (dla standardu 100-BaseFX do 2000 m).

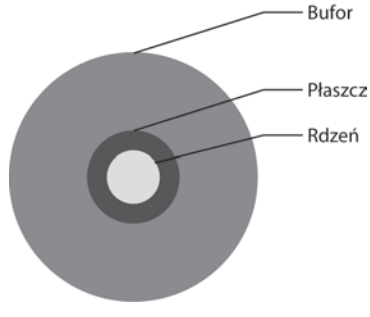
**DEFINICJA**

Najważniejszym elementem systemu światłowodowej transmisji danych jest światło, które może być emitowane przez:

- diody laserowe (ang. *Laser Diode* — LD),
- diody elektroluminescencyjne (ang. *Light Emitted Diode* — LED).

Światłowód składa się z płaszcza zewnętrznego (ochronnego), zbioru włókien, natomiast każde włókno to zbiór trzech elementów (rysunek 3.6):

- bufora,
- płaszcza,
- rdzenia.




**Rysunek 3.6.** Budowa światłowodu

**WAŻNE**

Promień świetlny, który trafia do rdzenia pod odpowiednim kątem, jest określany jako mod światłowodowy. Ze względu na liczbę równocześnie transmitowanych modów rozróżnia się światłowody:

- jednomodowe — transmitujące jeden mod (promień) światła,
- wielomodowe — transmitujące wiele modów (promieni) światła.

Poniżej prezentowane są przykładowe standardy sieci Ethernet wykorzystującej łącza światłowodowe:

- 100Base-FX — światłowód wielomodowy, maksymalna prędkość transmisji 100 Mb/s, maksymalna długość segmentu — 2000 m,
- 1000Base-LX — światłowód jednomodowy, maksymalna prędkość transmisji 1000 Mb/s, maksymalna długość segmentu — 10 km,
- 1000Base-SX — światłowód wielomodowy, maksymalna prędkość transmisji 1000 Mb/s, maksymalna długość segmentu — 550 m,
- 10GBase-LR — światłowód jednomodowy, maksymalna prędkość transmisji 10 GB/s, maksymalna długość segmentu — 10 km.

## 3.2. Media bezprzewodowe

W sieciach komputerowych wykorzystuje się dwa rodzaje bezprzewodowego medium transmisyjnego WLAN (*Wireless Local Area Network*):

- fale z zakresu podczerwieni — są stosowane na otwartym terenie bądź wewnątrz budynków. Jako źródła promieniowania fal elektromagnetycznych wykorzystuje się diody elektroluminescencyjne LED (*Light Emitting Diode*) lub diody laserowe.
- fale radiowe — do transmisji wymagają planowania przydziału częstotliwości z uwzględnieniem maksymalnej dopuszczalnej mocy nadajników, rodzaju modulacji oraz innych zaleceń Międzynarodowej Unii Telekomunikacji (ITU).

Standardy dotyczące sieci bezprzewodowych opisują m.in. prędkość transmisji i pasmo częstotliwości (tabela 3.1).

**Tabela 3.1.** Standardy sieci bezprzewodowych

| Nazwa | Szybkości (Mb/s) | Pasmo częstotliwości (GHz) |
|---|---|---|
| 802.11 | 1; 2 | 2,4 |
| 802.11a | 6; 9; 12; 18; 24; 36; 48; 54 | 5 |
| 802.11b | 1; 2; 5,5; 11 | 2,4 |
| 802.11g | 1; 2; 5,5; 6; 9; 11; 12; 18; 24; 36; 48; 54 | 2,4 |

| Nazwa | Szybkości (Mb/s) | Pasmo częstotliwości (GHz) |
|---|---|---|
| 802.11n | 100; 150; 300; 450; 600 | 2,4 lub 5 |
| 802.11ac | 100; 150; 300; 450; 600; 1024 | 5 |
| 802.15.1 (bluetooth) | 1; 2 | 2,4 |

Podstawową zaletą sieci bezprzewodowej jest mobilność rozwiązania — aby podłączyć urządzenie sieciowe, nie trzeba prowadzić przewodów, wystarczy jedynie umieścić urządzenie w zasięgu działania sieci i odpowiednio skonfigurować. Pozwala to na szybką i łatwą rozbudowę sieci.

Do wad sieci bezprzewodowych należy zaliczyć możliwość zakłócenia fal radiowych przez przeszkody znajdujące się na drodze fali niosącej sygnał lub przez warunki atmosferyczne, a także mniejsze niż w przypadku sieci kablowych bezpieczeństwo transmitowanych danych (brak kontroli nad dostępem do medium transmisyjnego).

Na infrastrukturę sieci bezprzewodowej składają się:

- karty sieciowe,
- punkty dostępowe,
- anteny wraz z okablowaniem.

Sieci WLAN mogą pracować w dwóch trybach:

- ad-hoc, w którym urządzenia łączą się bezpośrednio ze sobą,
- w trybie infrastruktury z wykorzystaniem punktów dostępowych (ang. *access point*).

Punkt dostępowy to centralny punkt sieci bezprzewodowej. Przekazuje dane pomiędzy urządzeniami, pozwala także na podłączenie sieci bezprzewodowej do sieci kablowej. Punkty dostępowe mają dwa interfejsy sieciowe: interfejs bezprzewodowy (gniazdo do podłączenia anteny) oraz interfejs sieci kablowej (najczęściej gniazdo RJ45 do podłączenia sieci Ethernet).

Punkty dostępowe mogą komunikować się między sobą, co pozwala na budowę złożonej infrastruktury łączącej urządzenia znacznie od siebie oddalone.

Punkty dostępowe pozwalają na budowę dwóch rodzajów sieci:

- BSS (ang. *Basic Service Set* — podstawowy zestaw usługowy) — cała transmisja w danej sieci przeprowadzana jest z wykorzystaniem jednego punktu dostępowego.
- ESS (ang. *Extended Service Set* — rozszerzony zestaw usług) — sieć zbudowana z kilku punktów dostępowych, które komunikują się ze sobą za pomocą protokołu IAPP (ang. *Inter-Access Point Protocol*), tworząc sieć szkieletową. W tego rodzaju sieci urządzenia podłączane są do dowolnego z punktów dostępowych i mogą przemieszczać się między nimi. Tego rodzaju sieci są stosowane m.in. przy budowie hot-spotów — publicznych punktów dostępu do internetu.

W przypadku sieci bezprzewodowych ogromne znaczenie ma bezpieczeństwo danych. Ogólnodostępne medium transmisyjne powoduje, że każde urządzenie znajdujące się w zasięgu sieci mogłoby korzystać z jej zasobów. Punkty dostępowe pozwalają na implementację procedur bezpieczeństwa polegających na filtrowaniu adresów MAC lub IP, a także na zabezpieczenie dostępu do sieci kluczem szyfrującym.

Urządzenia bezprzewodowe mogą pracować bez szyfrowania danych (tryb niezalecany ze względów bezpieczeństwa) lub w jednym z następujących trybów szyfrowania danych:

- WEP (ang. *Wired Equivalent Privacy*) — pozwalający na używanie kluczy 64-bitowych lub 128-bitowych. Szyfrowanie WEP zostało złamane i nie jest uznawane za bezpieczne.
- WPA (ang. *WiFi Protected Access*) — zabezpieczenie wykorzystujące cykliczne zmiany klucza szyfrującego podczas transmisji, może działać w dwóch trybach: *Enterprise* (klucze przydzielane są przez serwer Radius dla każdego użytkownika sieci) lub *Personal* (wszyscy użytkownicy sieci korzystają z dzielonego klucza — ang. *Pre-Shared Key* — PSK).
- WPA2 — poprawiona wersja protokołu WPA, zalecana do zabezpieczeń sieci bezprzewodowych.

Konfiguracja urządzeń bezprzewodowych zostanie omówiona w rozdziale 2. tomu II — „Konfigurowanie urządzeń sieciowych".

## ĆWICZENIA

1. Sprawdź konstrukcję sieci, do której jesteś podłączony. Z jakiego medium korzysta? W jakiej topologii jest zbudowana?

## PYTANIA

1. Opisz kabel koncentryczny.
2. Opisz kabel światłowodowy.
3. Dlaczego przewody w kablu UTP są skręcone?
4. Czym różni się kabel prosty od kabla skrosowanego? Jakie urządzenia można połączyć każdym z nich?
5. Jakie medium transmisyjne umożliwia transmisje na duże odległości?
6. Czym się różni światłowód jednomodowy od wielomodowego?
7. Omów transmisję bezprzewodową.
8. Jakie rodzaje zabezpieczeń są stosowane w sieciach bezprzewodowych?

# 4

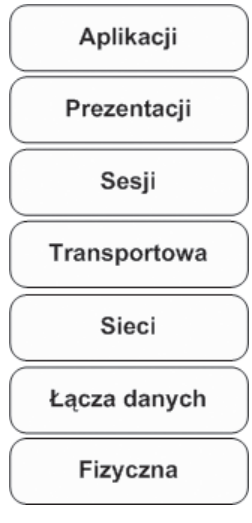
# Protokoły sieciowe

Protokoły sieciowe to zestaw reguł, które umożliwiają komunikację w sieci komputerowej.

## 4.1. Model ISO/OSI

**DEFINICJA**

**Model odniesienia OSI** (ang. *Open System Interconnection Reference Model*) to wzorcowy model transmisji danych w sieciach komputerowych. Model składa się z 7 warstw (ang. *layers*) współpracujących ze sobą w określony sposób (rysunek 4.1). Został on przyjęty przez Międzynarodową Organizację Standaryzacji ISO w 1984 roku.




**Rysunek 4.1.**
Warstwy w modelu OSI

Model odniesienia OSI jest wzorcem używanym do reprezentowania mechanizmów przesyłania informacji w sieci. Pozwala wyjaśnić, w jaki sposób dane pokonują różne warstwy w drodze do innego urządzenia w sieci, nawet jeśli nadawca i odbiorca

dysponują różnymi typami medium sieciowego. Podział sieci na warstwy przynosi następujące korzyści:

- dzieli proces komunikacji sieciowej na mniejsze, łatwiejsze do zarządzania procesy składowe,
- tworzy standardy składników sieci, dzięki czemu składniki te mogą być rozwijane niezależnie i obsługiwane przez różnych producentów,
- umożliwia wzajemną komunikację sprzętu i oprogramowania sieciowego różnych rodzajów,
- zmiany wprowadzone w jednej warstwie nie dotyczą innych warstw.

Trzy górne warstwy, czyli warstwa aplikacji, prezentacji i sesji, zajmują się współpracą z oprogramowaniem wykonującym zadania zlecane przez użytkownika systemu komputerowego. Tworzą one interfejs, który pozwala na komunikację z warstwami niższymi.

**Warstwa aplikacji** (ang. *application layer*) zajmuje się zapewnieniem dostępu do sieci aplikacjom użytkownika. W warstwie tej są zdefiniowane protokoły usług sieciowych takich jak HTTP, FTP, SMTP.

**Warstwa prezentacji** (ang. *presentation layer*) odpowiada za reprezentację danych — obsługę znaków narodowych, formatów graficznych oraz kompresję i szyfrowanie.

**Warstwa sesji** (ang. *session layer*) zapewnia aplikacjom komunikację między różnymi systemami. Zarządza sesjami transmisyjnymi poprzez nawiązywanie i zrywanie połączeń między aplikacjami.

**Warstwa transportowa** (ang. *transport layer*) zapewnia połączenie między aplikacjami w różnych systemach komputerowych, dba o kontrolę poprawności przesyłanych danych. Tutaj następuje podział danych na segmenty, które są kolejno numerowane i wysyłane do stacji docelowej. Stacja docelowa po odebraniu segmentu może wysłać potwierdzenie odbioru, co pozwala zapewnić prawidłowość transmisji.

**Warstwa sieciowa** (ang. *network layer*) zapewnia metody łączności. W tej warstwie obsługiwane są routing i adresacja logiczna.

**Warstwa łącza danych** (ang. *data link*) odpowiada za poprawną transmisję danych przez konkretne media transmisyjne. Warstwa ta operuje na fizycznych adresach interfejsów sieciowych (MAC), zapewniając łączność między dwoma bezpośrednio połączonymi urządzeniami.

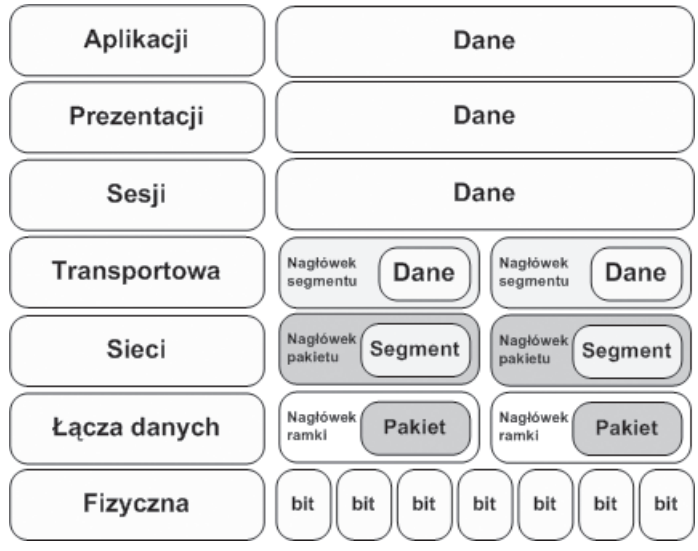
**Warstwa fizyczna** odbiera dane z warstwy łącza danych i przesyła je w medium transmisyjnym jako bity reprezentowane w konkretny sposób (sygnały elektryczne, impulsy świetlne).

Model OSI opisuje drogę danych przesyłanych między aplikacjami, które zostały uruchomione w różnych systemach komputerowych. W przypadku większości usług w internecie transmisja między systemami jest realizowana według modelu klient-serwer, a komunikują się aplikacje klienckie (np. przeglądarka internetowa) z aplikacją serwerową (np. serwer stron WWW).

**DEFINICJA**

Transmisja w modelu OSI jest przeprowadzana w dół kolejnych warstw (na urządzeniu źródłowym), a następnie w górę (na serwerze lub urządzeniu docelowym). Proces przekazywania danych między warstwami protokołu jest nazywany **enkapsulacją** lub kapsułkowaniem (rysunek 4.2).

**Rysunek 4.2.**
Model enkapsulacji




W procesie enkapsulacji dane użytkownika (z warstwy aplikacji) są dzielone w warstwie transportu na **segmenty** i opatrywane nagłówkiem zawierającym m.in. numery portów. Tak przygotowane porcje danych wędrują do warstwy trzeciej, gdzie jest dodawany nagłówek zawierający adresy logiczne nadawcy i odbiorcy. Powstaje **pakiet**. Do pakietów w warstwie łącza danych są dodawane adresy fizyczne — tworzona jest **ramka**. Ostatnia warstwa — fizyczna — przekształca ramkę z poprzedniej warstwy do postaci pozwalającej przesłać informację medium transmisyjnym. Dane wędrują do stacji docelowej i tam są ponownie przekształcane, najpierw z bitów na ramki, następnie na pakiety i segmenty, po czym zostają zinterpretowane przez aplikację na komputerze docelowym.

# 4.2. Protokoły używane w sieciach LAN

## 4.2.1. Protokół TCP/IP

Najpopularniejszym spośród protokołów komunikacyjnych jest **protokół IP**, powszechnie używany w sieciach LAN, a także w internecie. W sieciach IP dane są wysyłane w formie bloków określanych mianem pakietów. W przypadku transmisji z wykorzystaniem protokołu IP przed rozpoczęciem transmisji nie jest zestawiana wirtualna sesja komunikacyjna między dwoma urządzeniami.

Protokół IP jest protokołem zawodnym — nie gwarantuje, że pakiety dotrą do adresata, że nie zostaną pofragmentowane czy też zdublowane. Ponadto dane mogą dotrzeć do odbiorcy w innej kolejności niż ta, w jakiej zostały nadane. Niezawodność transmisji danych zapewniają protokoły warstw wyższych (np. protokół warstwy transportowej — TCP).

### 4.2.2. Protokół IPX/SPX

Dla sieci pracujących w środowisku Novell Netware został opracowany protokół **IPX** (ang. *Internet Packet Exchange*). Nie został on wyposażony w mechanizmy kontroli transmisji i nie gwarantuje, że wszystkie pakiety dotrą na miejsce. Podobnie jak w przypadku protokołu IP, niezawodność transmisji zapewnia protokół warstwy czwartej — **SPX** (ang. *Sequenced Packet Exchange*).

Adresacja w protokole IPX składa się z dwóch części: adresu sieci i adresu hosta. Pierwszy z nich jest liczbą 32-bitową, drugi — 48-bitową i odpowiada adresowi MAC karty sieciowej.

Obecnie protokoły IPX/SPX praktycznie nie są stosowane, ponieważ zostały wyparte przez stos protokołów TCP/IP.

### 4.2.3. AppleTalk

AppleTalk jest protokołem opracowanym przez firmę Apple, stosowanym w sieciach komputerowych opartych na systemie operacyjnym MacOS. Protokół ten wykorzystują proste sieci równorzędne. Aktualnie protokół AppleTalk nie jest rozwijany, został zastąpiony przez protokół TCP/IP.

Protokoły IP, IPX i AppleTalk są **protokołami rutowalnymi** (ang. *routed protocol*). Oznacza to, że mogą być obsługiwane przez routery, a więc mogą przenosić dane między różnymi sieciami.

### 4.2.4. NetBEUI

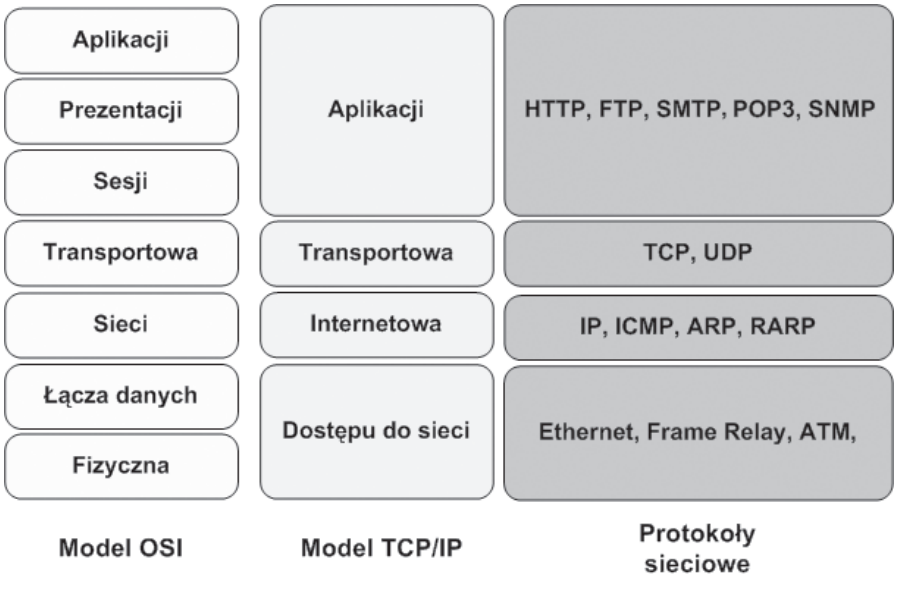
**NetBEUI** to prosty protokół opracowany przez IBM i wykorzystywany jedynie w systemach operacyjnych firmy Microsoft. Protokół ten cechuje się minimalnymi wymaganiami i dużą odpornością na błędy. Sprawdza się jednak tylko w małych sieciach lokalnych — nie może być używany w internecie, gdyż nie jest protokołem rutowalnym. W najnowszych wersjach systemów Windows protokół ten został zastąpiony przez TCP/IP.

## 4.3. Model TCP/IP

**Warstwa aplikacji** (ang. *application layer*) to najwyższy poziom, w którym pracują aplikacje, na przykład serwer WWW czy przeglądarka internetowa. Warstwa ta obejmuje zestaw gotowych protokołów, które są wykorzystywane przez aplikacje do przesyłania w sieci różnego typu informacji.

**DEFINICJA**

**Model TCP/IP** (ang. *Transmission Control Protocol/Internet Protocol*) to teoretyczny model warstwowej struktury komunikacji sieciowej. Opiera się on na szeregu współpracujących ze sobą warstw (ang. *layers*). Założenia modelu TCP/IP są pod względem organizacji warstw zbliżone do założeń modelu OSI, jednak liczba warstw jest mniejsza i lepiej odzwierciedla prawdziwą strukturę internetu (rysunek 4.3).




**Rysunek 4.3.** Porównanie modeli OSI i TCP/IP

**Warstwa transportowa** (ang. *transport layer*) odpowiada za przesyłanie danych i kieruje właściwe informacje do odpowiednich aplikacji, wykorzystując porty określane dla każdego połączenia. Warstwa transportowa nawiązuje i zrywa połączenia między komputerami. W tej warstwie działa protokół TCP (przesyłający potwierdzenia odbioru porcji danych, co gwarantuje pewność transmisji) oraz protokół UDP (bez potwierdzeń odbioru).

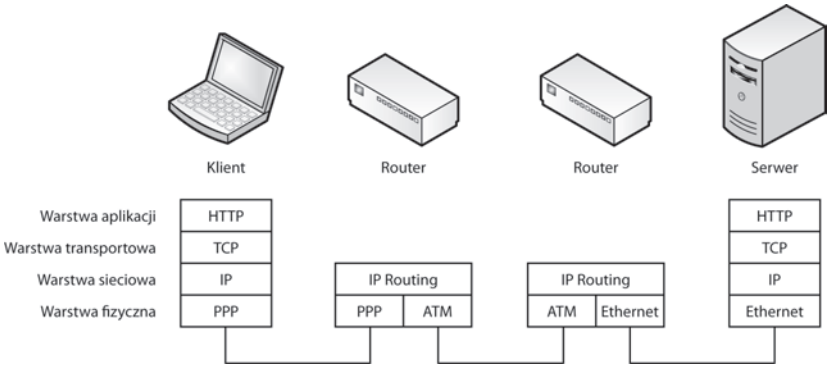
**Warstwa internetowa** (ang. *internet layer*) ma za zadanie podzielenie segmentów na pakiety i przesłanie ich dowolną siecią. Pakiety trafiają do sieci docelowej niezależnie od przebytej drogi. Tą warstwą zarządza protokół IP. Tutaj jest określana najlepsza ścieżka i następuje przełączanie pakietów.

**UWAGA**

Związek między protokołem IP i protokołem TCP jest bardzo istotny. Protokół IP określa drogę dla pakietów, a protokół TCP zapewnia niezawodny transport.

**Warstwa dostępu do sieci** (ang. *network access layer*) zajmuje się przekazywaniem danych przez fizyczne połączenia między urządzeniami sieciowymi (np. karty sieciowe lub modemy). Dodatkowo warstwa ta jest wyposażona w protokoły służące do dynamicznego określania adresów IP.

Przykład komunikacji z wykorzystaniem protokołu TCP/IP (rysunek 4.4).




**Rysunek 4.4.** Przykład transmisji w TCP/IP

## 4.3.1. Protokoły w warstwie dostępu do sieci

Warstwa dostępu do sieci jest odpowiedzialna za wszystkie zagadnienia związane z zestawieniem łącza fizycznego służącego do przekazywania pakietu IP do medium transmisyjnego. Odpowiada między innymi za odwzorowywanie adresów IP na adresy sprzętowe i za enkapsulację pakietów IP w ramki. Określa połączenie z fizycznym medium sieci w zależności od rodzaju sprzętu i interfejsu sieciowego.

Warstwa dostępu do sieci w modelu TCP/IP definiuje funkcje umożliwiające korzystanie ze sprzętu sieciowego i dostęp do medium transmisyjnego. W sieciach lokalnych protokołem dostępu do sieci jest Ethernet, w sieciach rozległych są to m.in. protokoły ATM i Frame Relay.

### Ethernet

**DEFINICJA**

**Standard Ethernet** został opublikowany w latach 80. ubiegłego wieku. Transmisja osiągała szybkość do 10 Mb/s i była realizowana przez gruby kabel koncentryczny na odległościach do 500 m. Pierwotny standard technologii Ethernet był wielokrotnie poprawiany w celu dostosowania go do potrzeb nowych mediów transmisyjnych i większych prędkości transmisji. Obecnie rodzina technologii Ethernet obejmuje następujące standardy: Ethernet (prędkość 10 Mb/s), Fast Ethernet (100 Mb/s), Gigabit Ethernet (1000 Mb/s), 10 Gigabit Ethernet (10 Gb/s), 40 Gigabit Ethernet (40 Gb/s) oraz 100 Gigabit Ethernet (100 Gb/s).

Technologie Ethernet określają sposoby ustalania przepustowości łącza sieciowego nazywane **autonegocjacją**. Interfejsy sieciowe mogą pracować w wielu trybach, w zależności od rodzaju wykorzystywanego w sieci medium (tabela 4.1). Celem autonegocjacji jest umożliwienie współpracy różnych urządzeń w trybie o najwyższej prędkości akceptowalnej przez wszystkie urządzenia w sieci.

Format ramki przyjmuje postać przedstawioną na rysunku 4.5.


**Rysunek 4.5.** Ramka Ethernet

Poszczególne elementy oznaczają:

- **Preambuła** — składa się z 7 bajtów złożonych z naprzemiennych jedynek i zer.
- **SFD** (ang. *start frame delimiter*), czyli znacznik początkowy ramki w postaci sekwencji 8 bitów (1 bajt).
- **Adres MAC odbiorcy** (6 bajtów).
- **Adres MAC nadawcy** (6 bajtów).
- **Typ ramki** (2 bajty).
- **Dane** (46 – 1500 bajtów) — jeżeli dane są mniejsze niż 46 bajtów, to są uzupełniane zerami.
- **Suma kontrolna** (4 bajty).

**Tabela 4.1.** Standardy Ethernet

| | |
|---|---|
| IEEE 802.3 | standard protokołu CSMA/CD |
| IEEE 802.3u | Fast Ethernet 100BASE-T |
| IEEE 802.3z | Gigabit Ethernet |
| IEEE 802.3ab | Gigabit Ethernet, 1000BASE-T |
| IEEE 802.11 | bezprzewodowy Ethernet |
| IEEE 802.3ae | 10 Gigabit Ethernet |
| IEEE 802.3bg | 40 Gigabit Ethernet |
| IEEE 802.3bj | 100 Gigabit Ethernet |

### Frame Relay

**DEFINICJA**

**Frame Relay** zapewnia komunikację połączeniową o przepływności do 45 Mb/s. Funkcjonuje na telekomunikacyjnych łączach cyfrowych odznaczających się niskim wskaźnikiem błędów. Frame Relay pozwala na łączenie sieci LAN, transmisję danych i głosu, wideo- i telekonferencje.

Sieć Frame Relay składa się z wielu urządzeń sieciowych połączonych kanałami fizycznymi, na których są tworzone połączenia wirtualne (logiczne). Mogą być one zestawiane na stałe (ang. *Permanent Virtual Circuits — PVC*) i tymczasowo (ang. *Switched Virtual Circuits — SVC*).

Frame Relay zapewnia gwarantowaną szybkość transmisji (ang. *Committed Information Rate — CIR*).

### ATM

**DEFINICJA**

**ATM** jest technologią telekomunikacyjną, która umożliwia przesyłanie głosu, obrazów wideo i danych przez sieci prywatne i publiczne. Podstawową porcją danych w sieciach ATM jest komórka, która ma stałą długość 53 bajtów. Tworzy ją 5-bajtowy nagłówek ATM i 48 bajtów treści zasadniczej. Małe komórki o stałej długości doskonale nadają się do przesyłania głosu i obrazów wideo, ponieważ ruch ten nie toleruje opóźnień. Ruch zawierający obrazy wideo i głos nie musi czekać na przesłanie większego pakietu danych.

## 4.3.2. Protokoły warstwy internetowej

Zadaniem warstwy internetowej jest wybranie najlepszej ścieżki dla pakietów przesyłanych w sieci. Podstawowym protokołem działającym w tej warstwie jest **protokół IP** (ang. *Internet Protocol*). Tutaj następuje określenie najlepszej ścieżki i przełączanie pakietów.

Protokół IP spełnia następujące zadania:

- definiuje format pakietu i schemat adresowania,
- kieruje pakiety do zdalnych hostów.

**DEFINICJA**

W warstwie internetowej modelu TCP/IP działają następujące protokoły:

- **Protokół IP**, który zapewnia usługę bezpołączeniowego dostarczania pakietów przy użyciu dostępnych możliwości. Protokół IP nie uwzględnia zawartości pakietu, ale wyszukuje ścieżkę do miejsca docelowego.
- **Protokół ICMP** (ang. *Internet Control Message Protocol*), który pełni funkcje kontrolne i informacyjne. Jest on używany przez polecenia sprawdzające poprawność połączenia (np. polecenie `ping`).
- **Protokół ARP** (ang. *Address Resolution Protocol*), który znajduje adres warstwy łącza danych MAC dla znanego adresu IP.
- **Protokół RARP** (ang. *Reverse Address Resolution Protocol*), który znajduje adres IP dla znanego adresu MAC.
- **Protokoły routingu** (RIP, IGRP, EIGRP, OSPF, BGP).

Postać, w jakiej dane są przesyłane przez pakiety IP, została przedstawiona na rysunku 4.6.

<table>
<tr><td>Wersja</td><td>Długość</td><td>Typ usługi (ToS)</td><td colspan="2">Rozmiar pakietu</td></tr>
<tr><td colspan="3">Identyfikator</td><td>Flagi</td><td>Przesunięcie fragmentu</td></tr>
<tr><td colspan="2">Time-to-live (TTL)</td><td>Protokół</td><td colspan="2">Suma kontrolna nagłówka</td></tr>
<tr><td colspan="5">Adres nadawcy</td></tr>
<tr><td colspan="5">Adres odbiorcy</td></tr>
<tr><td colspan="5">Opcje</td></tr>
<tr><td colspan="5">Dane</td></tr>
</table>

**Rysunek 4.6.** Format pakietu IP

Poszczególne elementy oznaczają:

- **Wersja** — wersja protokołu IP.
- **Długość nagłówka** — wartość tego pola pomnożona przez 32 bity określa długość nagłówka w bitach.

- **Typ usługi** (ang. *Type of Service — ToS*) — określa klasę usług, wykorzystywany przy zarządzaniu ruchem.
- **Rozmiar pakietu** — rozmiar całego pakietu IP podany w bajtach.
- **Identyfikator** — używany podczas łączenia fragmentów danych.
- **Flagi** — jest to 3-bitowe pole, gdzie pierwszy bit określa, czy dany pakiet może zostać podzielony na fragmenty; drugi — czy pakiet jest ostatnim fragmentem. Trzeci bit nie jest używany.
- **Przesunięcie fragmentu** — określa kolejną pozycję przesyłanych danych w oryginalnym datagramie w celu jego późniejszego odtworzenia.
- **Czas życia (TTL)** — zawiera znacznik życia pakietu. Pole to jest liczbą zmniejszaną przez każdy router, przez który przechodzi. Kiedy wartość TTL osiągnie zero, pakiet jest zatrzymywany, a nadawca zostaje poinformowany, że pakietu nie udało się dostarczyć.
- **Protokół** — oznacza kod protokołu warstwy wyższej — transportowej.
- **Suma kontrolna nagłówka** — służy do wykrywania uszkodzeń wewnątrz nagłówka.
- **Adresy źródłowy i docelowy pakietu** — adres IP nadawcy i odbiorcy pakietu.
- **Opcje** — dodatkowe informacje, nie zawsze używane, mogą dotyczyć na przykład funkcji zabezpieczeń.
- **Wypełnienie** — opcjonalne pole, które uzupełnia nagłówek pakietu zerami, aby jego wielkość była wielokrotnością 32 bitów.
- **Dane** — pole, w którym są transportowane właściwe dane.

## 4.3.3. Protokoły warstwy transportowej

**DEFINICJA**

**Warstwa transportowa** zapewnia usługi przesyłania danych z hosta źródłowego do hosta docelowego. Ustanawia logiczne połączenie między hostem wysyłającym i odbierającym. Protokoły transportowe dzielą i scalają dane wysyłane przez aplikacje wyższej warstwy w jeden strumień danych przepływający między punktami końcowymi.

Protokoły warstwy transportowej to TCP i UDP.

Protokół IP pozwala na przenoszenie pakietów między sieciami, jednak nie gwarantuje, że wysłane dane dotrą do adresata. Ta cecha powoduje, że protokół IP jest nazywany **bezpołączeniowym** — dane są wysyłane tylko w jedną stronę bez potwierdzenia.

Za niezawodność przesyłu danych jest odpowiedzialny **protokół TCP** nazywany protokołem **połączeniowym**. To on po odebraniu każdej porcji danych wysyła potwierdzenie do nadawcy, że dane zostały odebrane. W przypadku braku potwierdzenia dane są wysyłane ponownie.

Innym protokołem działającym na rzecz protokołu IP jest **UDP** (ang. *User Datagram Protocol*). Jest on bezpołączeniowym protokołem transportowym należącym do stosu protokołów TCP/IP. Służy do wysyłania datagramów bez potwierdzania czy gwarancji ich dostarczenia. Przetwarzanie błędów i retransmisja muszą być obsłużone przez protokoły warstwy aplikacji.

Protokół UDP jest zaprojektowany dla aplikacji, które nie mają potrzeby składania sekwencji segmentów. Nie przysyła on informacji o kolejności, w jakiej mają być odtworzone. Taka informacja jest zawarta w nagłówku segmentów protokołu TCP.

### 4.3.4. Protokoły warstwy aplikacji

**DEFINICJA**

**Warstwa aplikacji** zajmuje się świadczeniem usług dla użytkownika. Protokoły warstwy aplikacji definiują standardy komunikacji między aplikacjami (programami klienckimi a serwerowymi).

Najpopularniejsze protokoły warstwy aplikacji:

- **Telnet** — protokół terminala sieciowego, pozwalający na zdalną pracę z wykorzystaniem konsoli tekstowej.
- **FTP** (ang. *File Transfer Protocol*) — protokół transmisji plików.
- **SMTP** (ang. *Simple Mail Transfer Protocol*) — protokół wysyłania poczty elektronicznej.
- **POP3** (ang. *Post Office Protocol*) — protokół odbioru poczty elektronicznej.
- **HTTP** (ang. *Hypertext Transfer Protocol*) — protokół przesyłania stron WWW.
- **SSH** (ang. *Secure Shell*) — protokół terminala sieciowego zapewniający szyfrowanie połączenia.
- **DNS** (ang. *Domain Name System*) — system nazw domenowych. Odpowiada za tłumaczenie adresów domenowych na adresy IP i odwrotnie.
- **DHCP** (ang. *Dynamic Host Configuration Protocol*) — protokół dynamicznej konfiguracji urządzeń. Odpowiedzialny za przydzielanie adresów IP, adresu domyślnej bramki i adresów serwerów DNS.
- **NFS** (ang. *Network File System*) — protokół udostępniania systemów plików (dysków sieciowych).
- **SNMP** (ang. *Simple Network Management Protocol*) — prosty protokół zarządzania siecią. Pozwala na konfigurację urządzeń sieciowych i gromadzenie informacji na ich temat.

# 4.4. Narzędzia diagnostyczne protokołów TCP/IP

Poprawne skonfigurowanie protokołu IP pozwala na pracę z wykorzystaniem zasobów sieciowych. Każdy sieciowy system operacyjny oferuje narzędzia pozwalające sprawdzić poprawność konfiguracji.

## 4.4.1. Polecenie ipconfig

W systemach Windows poleceniem, które pozwala sprawdzić adresy przypisane do poszczególnych interfejsów, jest `ipconfig`. Narzędzie to pomaga przy wykrywaniu błędów w konfiguracji protokołu IP.

**WAŻNE**

Najczęściej polecenie `ipconfig` jest wykorzystywane w następujący sposób:

- `ipconfig` — pokazuje skróconą informację o połączeniu.
- `ipconfig /all` — pokazuje szczegółowe dane o konfiguracji wszystkich interfejsów.
- `ipconfig /renew` — odnawia wszystkie karty.
- `ipconfig /release` — zwalnia wszystkie połączenia.
- `ipconfig /?` — wyświetla komunikat pomocy.
- `ipconfig /flushdns` — czyści bufor programu rozpoznającego nazwy DNS.
- Odpowiednikiem polecenia `ipconfig` w systemie Linux jest `ifconfig`.

## 4.4.2. Polecenie ping

Do diagnozowania połączeń w sieciach komputerowych TCP/IP używa się polecenia `ping`. Pozwala ono na sprawdzenie, czy istnieje połączenie między dwoma urządzeniami, i umożliwia sprawdzanie jego jakości poprzez mierzenie liczby zgubionych pakietów oraz czasu ich dotarcia do celu i z powrotem. Do badania jakości połączenia `ping` korzysta z protokołu ICMP.

Polecenie `ping` jest dostępne zarówno w systemie Windows, jak i Linux. Aby sprawdzić poprawność konfiguracji połączenia IP, należy użyć składni:

```
ping nazwa_lub_adres_do_sprawdzenia
```

## 4.4.3. Polecenie tracert

Komendą służącą do badania trasy pakietów IP w systemie Windows jest `tracert` (dla systemów Linux komenda `traceroute`). Sprawdza ona czasy dostępu do kolejnych routerów znajdujących się na drodze do adresu docelowego (rysunek 4.7).

```
[root@student ~]# traceroute wikiedia.org
traceroute to wikiedia.org (174.132.216.229), 30 hops max, 40 byte packets
 1  abc34.internetdsl.tpnet.pl (80.13.121.34)  1.020 ms  0.990 ms  2.161 ms
 2  abc33.internetdsl.tpnet.pl (80.13.121.33)  32.334 ms  32.324 ms  32.301 ms
 3  kat-ru5.idsl.tpnet.pl (213.25.2.203)  33.261 ms  33.243 ms  34.607 ms
 4  ge-1-1-4.20.kat-r1.tpnet.pl (212.160.0.17)  34.586 ms  35.561 ms  35.540 ms
 5  tengige0-3-0-7.ffttr1.FrankfurtAmMain.opentransit.net (193.251.255.253)  52.457 ms  54.383 ms  55.94
0 ms
 6  64.208.110.225 (64.208.110.225)  58.667 ms  32.439 ms  34.836 ms
 7  The-Planet.TenGigabitEthernet2-3.ar2.HOU1.gblx.net (64.214.196.58)  160.478 ms  164.310 ms  165.279
ms
 8  po1.car08.hstntx2.theplanet.com (74.55.252.90)  160.379 ms  164.236 ms  164.233 ms
 9  e5.d8.84ae.static.theplanet.com (174.132.216.229)  180.325 ms  180.318 ms  181.475 ms
[root@student ~]# traceroute wikiedia.org
```

**Rysunek 4.7.** Wynik działania funkcji tracert

**WAŻNE**

Często z wyników działania programu można odczytać przebieg wędrówki pakietów po sieci, ponieważ niektóre nazwy routerów zawierają ich lokalizację. W przykładzie podanym na rysunku 4.7 pakiety pokonały trasę z Katowic (z adresu **kat**-ru5.idsl.tpnet.pl), przez Frankfurt nad Menem (tengige0-3-0-7.ffttr1.**FrankfurtAmMain**.opentransit.net), do Houston (The-Planet.TenGigabitEthernet2-3.ar2.**HOU1**.gblx.net).

## 4.4.4. Polecenie netstat

Polecenie `netstat` jest jednym z najbardziej rozbudowanych poleceń, pozwalającym na sprawdzanie połączeń sieciowych (rysunek 4.8). Dostępne jest zarówno dla systemu Windows, jak i Linux. Umożliwia wyświetlanie aktywnych połączeń sieciowych TCP, a także portów, na których komputer nasłuchuje, tabeli routingu, statystyk itp.

```
[root@student root]# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.100.0   *               255.255.255.0   U         0 0          0 eth0
83.16.196.34    *               255.255.255.248  U        0 0          0 eth1
192.168.3.0     wenus           255.255.255.0   UG        0 0          0 eth2
192.168.2.0     mars            255.255.255.0   UG        0 0          0 eth3
192.168.1.0     neptun          255.255.255.0   UG        0 0          0 eth3
169.254.0.0     *               255.255.0.0     U         0 0          0 eth1
127.0.0.0       *               255.0.0.0       U         0 0          0 lo
default         gate            0.0.0.0         UG        0 0          0 eth0
[root@student root]#
```

**Rysunek 4.8.** Przykład wykorzystania polecenia netstat — tablica routingu

Polecenie `netstat` użyte bez parametrów powoduje wyświetlenie aktywnych połączeń protokołu TCP. Inne najważniejsze parametry polecenia to:

- `-a` — służy do wyświetlania wszystkich aktywnych połączeń oraz portów nasłuchu protokołów TCP i UDP.
- `-b` — służy do wyświetlania aktywnych połączeń protokołu TCP i nazw programów, które są przypisane do obsługi danego portu.
- `-e` — wyświetla statystykę sieci Ethernet.
- `-n` — wyświetla aktywne połączenia TCP (adresy i numery portów są wyrażane numerycznie).
- `-o` — wyświetla aktywne połączenia TCP i identyfikatory procesów (PID) poszczególnych połączeń.
- `-p` *protokół* — ukazuje połączenia wybranego protokołu (udp, tcpv6, tcp lub udpv6).
- `-s` — służy do wyświetlania oddzielnych statystyk dla poszczególnych protokołów.
- `-r` — służy do wyświetlania zawartości tabeli trasowania protokołu IP.

## 4.5. Zasady transmisji w sieciach TCP/IP

Urządzenia pracujące w jednej sieci mają możliwość komunikacji tylko między sobą. Aby połączyć je z inną siecią, wymagany jest **router**. Jest to urządzenie, które przekierowuje pakiet do adresata znajdującego się w innej logicznej sieci IP.

### 4.5.1. Brama domyślna

**DEFINICJA**

Komunikacja w sieciach TCP/IP pozwala na wymianę danych tylko z urządzeniami znajdującymi się w danej sieci. Aby wysłać wiadomość poza sieć, w której pracuje urządzenie, należy ustawić parametr konfiguracyjny protokołu IP — **bramę domyślną**. Adres bramy domyślnej wskazuje na router, który przechowuje informacje o tym, jak dotrzeć do wybranej sieci.

**Routery** to węzły sieci. Mają za zadanie przesyłać pakiety do adresata, a dokładnie do sieci, w której znajduje się jego adres IP. Pakiet zaadresowany do komputera znajdującego się w naszej sieci jest kierowany bezpośrednio do niego. Jeśli ma zostać wysłany poza sieć, trafia do routera, który sprawdza, czy pakiet ten jest kierowany do sieci bezpośrednio podłączonej do tego routera, czy ma być przesłany do urządzenia znajdującego się poza podłączonymi do niego sieciami. Pakiety wędrują od jednego węzła (routera) do drugiego poprzez wiele węzłów pośredniczących, często mogą też być transmitowane różnymi trasami. Zadaniem routera jest wybrać najlepszą dostępną drogę pomiędzy jednym a drugim węzłem. Decyzja o wyborze trasy jest podejmowana na podstawie

wpisów znajdujących się w tablicy routingu — spisie sieci podłączonych bezpośrednio do routera oraz sieci dostępnych na routerach sąsiadujących.

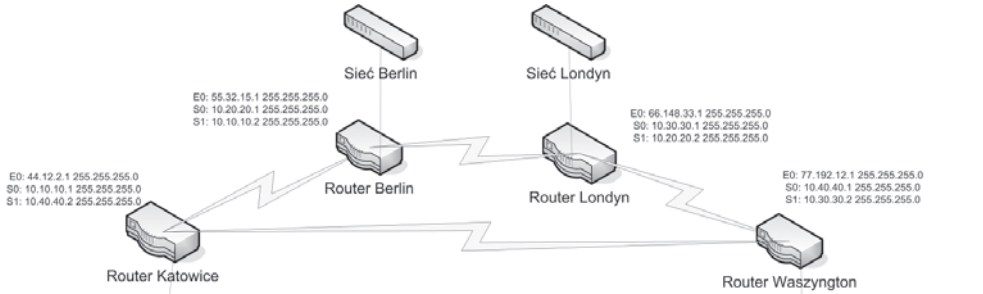
**DEFINICJA**

**Tablica routingu** może być utworzona przez administratora lub dynamicznie, przez protokoły routingu (nie mylić z protokołami rutowalnymi). **Routing** (**trasowanie**) polega na podjęciu decyzji, przez który fizyczny port lub przez którą sieć pakiety mają być wysłane, aby jak najszybciej dotarły do adresata.

Każdy wpis w tablicy routingu zawiera adres sieci docelowej oraz adres sieci lub interfejsu, przez który dana sieć docelowa jest osiągalna. Jeśli router zna więcej niż jedną trasę do sieci docelowej, wybiera trasę najkorzystniejszą na podstawie metryki — wartości określającej jakość danej trasy.

Metryki są zależne od konkretnego protokołu routingu. Mogą opierać się tylko na liczbie routerów znajdujących się na drodze do celu, ale również na chwilowym obciążeniu łącza, jego prędkości czy opóźnieniach występujących w transmisji.

**Przykład 4.1.** Rysunek 4.9 przedstawia infrastrukturę sieciową dla przykładowej sieci łączącej Katowice, Berlin, Londyn i Waszyngton. W każdym z miast do zainstalowanych routerów została podłączona sieć lokalna. Informacje o dostępnych sieciach są zapisane w tablicach routingu zamieszczonych pod rysunkiem. Kolejne wpisy w tablicach oznaczają: adres sieci, adres interfejsu (lub jego nazwę w przypadku sieci bezpośrednio podłączonych), przez który dana sieć jest osiągalna, oraz liczbę przeskoków do celu.




Router Katowice

| | | |
|---|---|---|
| 10.10.10.0 | Serial0 | 1 |
| 10.20.20.0 | 10.10.10.1 | 2 |
| 10.30.30.0 | 10.40.40.2 | 2 |
| 10.40.40.0 | Serial1 | 1 |
| 44.12.2.0 | Eth0 | 1 |
| 55.32.15.0 | 10.10.10.1 | 2 |
| 66.148.33.0 | 10.10.10.1 | 3 |
| 77.192.12.1 | 10.40.40.2 | 2 |

Router Berlin

| | | |
|---|---|---|
| 10.10.10.0 | Serial1 | 1 |
| 10.20.20.0 | Serial0 | 1 |
| 10.30.30.0 | 10.20.20.1 | 2 |
| 10.40.40.0 | 10.10.10.2 | 2 |
| 44.12.2.0 | 10.10.10.2 | 2 |
| 55.32.15.0 | Eth0 | 1 |
| 66.148.33.0 | 10.20.20.1 | 2 |
| 77.192.12.1 | 10.10.10.2 | 3 |

Router Londyn

| | | |
|---|---|---|
| 10.10.10.0 | 10.20.20.2 | 2 |
| 10.20.20.0 | Serial1 | 1 |
| 10.30.30.0 | Serial0 | 1 |
| 10.40.40.0 | 10.30.30.1 | 2 |
| 44.12.2.0 | 10.30.30.1 | 3 |
| 55.32.15.0 | 10.20.20.2 | 2 |
| 66.148.33.0 | Eth0 | 1 |
| 77.192.12.1 | 10.30.30.1 | 2 |

Router Waszyngton

| | | |
|---|---|---|
| 10.10.10.0 | 10.40.40.1 | 2 |
| 10.20.20.0 | 10.30.30.2 | 2 |
| 10.30.30.0 | Serial1 | 1 |
| 10.40.40.0 | Serial0 | 1 |
| 44.12.2.0 | 10.40.40.1 | 2 |
| 55.32.15.0 | 10.40.40.1 | 3 |
| 66.148.33.0 | 10.30.30.2 | 2 |
| 77.192.12.1 | Eth0 | 1 |

**Rysunek 4.9.** Przykładowa infrastruktura sieci

## 4.5.2. Protokoły routingu

Routery budują tablice routingu na podstawie informacji wymienionych z innymi routerami. Wymiana ta opiera się na **protokołach routingu**. Mają one za zadanie poinformować inne węzły sieci o sieciach, do których dany router ma dostęp. Takie rozwiązanie pozwala na dynamiczne budowanie struktury. Dołączenie kolejnej sieci do jednego z routerów nie wymaga rekonfiguracji pozostałych węzłów sieci. Zostaną one automatycznie „poinformowane" o zaistniałych zmianach.

Aby określić, która z dostępnych tras jest najlepsza, router wykorzystuję metrykę — wartość wyliczaną na podstawie określonych czynników zależnych od protokołu routingu, np. liczby przeskoków, szerokości pasma, opóźnienia, obciążenia czy niezawodności łącza.

Ze względu na sposoby działania rozróżnia się następujące protokoły routingu:

- protokoły wektora odległości (ang. *distance vector*) — wysyłają w określonych interwałach czasowych do sąsiednich routerów zawartość tablicy routingu wraz z metrykami. Jeśli dana trasa nie jest dostępna (nie dotarła informacja od sąsiedniego routera), wówczas wpis dotyczący trasy i sieci, które były osiągalne, zostaje usunięty z tablicy routingu i — o ile to możliwe — jest zastępowany innym wpisem (np. wcześniej odrzuconym jako mniej korzystny).
- protokoły stanu łącza (ang. *link state*) wysyłają do wszystkich routerów informację, która zawiera jedynie dane o podsieciach podłączonych do routera. Aktualizacje informacji są wysyłane okresowo lub wywoływane zmianami zachodzącymi w sieci.

Tabela 4.2 zawiera opis najpopularniejszych protokołów routingu.

**Tabela 4.2.** Opis protokołów routingu

| Nazwa protokołu | Opis |
|---|---|
| RIP (ang. *Routing Information Protocol*) | Protokół wektora odległości, używający liczby przeskoków pomiędzy routerami jako metryki. Domyślnie wysyła uaktualnienia co 30 sekund. |
| IGRP (ang. *Interior Gateway Routing Protocol*) i EIGRP (ang. *Enhanced Interior Gateway Routing Protocol*) | Protokół wektora odległości opracowany i wykorzystywany w urządzeniach CISCO. Wyliczana metryka uwzględnia przepustowość i obciążenie pasma, opóźnienie i niezawodność łącza. Uaktualnienia są wysyłane co 90 sekund lub po zmianie stanu sieci. |
| OSPF (ang. *Open Shortest Path First*) | Protokół stanu łącza, który używa algorytmu Dijkstry do wyznaczenia najkrótszej ścieżki. Uaktualnienia domyślnie są wysyłane po zmianach w topologii sieci. |
| BGP (ang. *Border Gateway Protocol*) | Służy do wyznaczania niezapętlonych tras pomiędzy systemami autonomicznymi — siecią lub grupą sieci — wykorzystującymi spójny schemat routingu. |

Dynamiczne przekazywanie informacji o stanie sieci poprawia jej działanie. Router, który utracił bezpośrednie połączenie z sąsiadującym węzłem, może połączyć się z nim inną drogą. Routery mają możliwość zdefiniowania **routingu domyślnego** — trasy określającej dostęp do wszystkich sieci, które nie są wpisane w tablicy routingu.

**Przykład 4.2.** Wróćmy do przykładu z rysunku 4.9. Węzeł Katowice ma dostęp do węzła Waszyngton dwoma drogami — przez Berlin i Londyn oraz bezpośrednio. Na podstawie informacji zawartych w tablicy routingu wszystkie pakiety są kierowane do sieci bezpośrednio łączącej oba węzły. Jeśli połączenie pomiędzy Katowicami a Berlinem — sieć 10.10.10.0 — zostanie zerwane (nie dotrze informacja protokołu routingu lub router wykryje niedostępną trasę), wówczas w tablicy routingu wpis dotyczący bezpośredniej dostępności węzła Berlin zostanie zamieniony na trasę przez Waszyngton.

Wpisy w tablicy routera Katowice będą wyglądać następująco:

```
10.20.20.0        10.40.40.2      2
10.30.30.0        10.40.40.2      1
10.40.40.0        Serial1         0
44.12.2.0         Eth0            0
55.32.15.0        10.10.40.2      3
66.148.33.0       10.10.40.2      2
77.192.12.1       10.40.40.2      1
```

Wpis dla sieci 10.10.10.0 został usunięty — sieć ta przestała działać.

## 4.5.3. Gniazdo

**DEFINICJA**

Transmisja w sieciach TCP/IP opiera się na dwóch elementach — adresie urządzenia i numerze portu. Taka para parametrów transmisji jest nazywana **gniazdem**. Adres IP odpowiada za zidentyfikowanie pojedynczego urządzenia w sieci, a numer portu oznacza, jaka aplikacja na urządzeniu docelowym ma przetwarzać przesłane dane.

Numery portów są dodawane do segmentów na poziomie warstwy czwartej (przez protokoły TCP i UDP). Numery portów zapewniają, że dane zostaną przetworzone przez konkretną aplikację. Na przykład podczas pobierania stron WWW zapytanie ze strony przeglądarki jest wysyłane na port 80 wybranego serwera WWW. Portem nadającym jest pierwszy wolny port powyżej 1023. Dane trafiają do serwera WWW na port 80 — jest to port, za którego obsługę odpowiada serwer HTTP. Serwer WWW wysyła dane (wybraną stronę) do klienta, kierując odpowiedź na port, z którego przyszło zapytanie. Komputer odbierający na podstawie portu kieruje odebrane dane do przetworzenia przez program, który wysłał zapytanie.

Numery portów do numeru 1023 są przypisywane znanym usługom sieciowym, na przykład 21 — FTP, 23 — Telnet, 25 — SMTP, 80 — HTTP. Numery portów powyżej 1024 są przydzielane dynamicznie programom, które korzystają z połączeń sieciowych.

# 4.6. Adresacja IP

**Protokół IP** jest podstawowym protokołem sieciowym, używanym zarówno w sieciach lokalnych, jak i w internecie. Znajomość sposobu adresacji ma kluczowe znaczenie dla zrozumienia transmisji danych między sieciami.

Każde urządzenie podłączone do sieci działającej z wykorzystaniem protokołu IP powinno mieć niepowtarzalny identyfikator — **adres IP**.

## 4.6.1. IPv4

Adres IPv4 to liczba 32-bitowa przedstawiona w postaci czterech liczb dziesiętnych z zakresu 0 – 255 (cztery liczby ośmiobitowe), które są rozdzielone kropkami. Każda część odpowiada kolejnym 8 bitom adresu zapisanego w systemie binarnym. Taka postać adresu jest łatwiejsza do zapamiętania niż jedna liczba z zakresu $0 – 2^{32}$.

**Przykład 4.3.** Porównanie różnych sposobów zapisu tej samej liczby

- zapis binarny: 11000000101010000000000000000001,
- zapis dziesiętny: 3 232 235 521,
- zapis tradycyjny: 192.168.0.1.

Jak widać, zapis w postaci czterech części oddzielanych kropką jest czytelniejszy i łatwiejszy do zapamiętania.

### Klasa adresu IP

Dla adresów zgrupowanych w klasach przyjęto domyślne maski podsieci: 8-bitową dla klasy A, 16-bitową dla klasy B i 24-bitową dla klasy C. Maski podsieci (opisane dalej) określają, które bity w adresie identyfikują sieć, a które hosta.

W adresach z klasy A sieć jest identyfikowana przez pierwszych 8 bitów, tak więc w zapisie dziesiętnym identyfikator sieci jest określany przez pierwszą liczbę. Pozostałe bity identyfikują hosta pracującego w danej sieci (komputer, router, drukarkę sieciową).

W puli adresów klasy B dwa pierwsze oktety (16 bitów) identyfikują sieć, pozostała część adresu to identyfikator hosta. Z kolei w klasie C pierwsze 3 liczby dziesiętne (24 bity) identyfikują sieć, natomiast ostatnia liczba jest identyfikatorem hosta (rysunek 4.10).

**DEFINICJA**

Adres IP ma budowę hierarchiczną. Część adresu IP oznacza identyfikator sieci, a część — identyfikator hosta (urządzenia). Adresy IP zostały pogrupowane w **klasy**. Klasa to logiczny podział puli adresów IP nazywany kolejnymi literami alfabetu (od A do E).

**Klasa A** zawiera adresy, których pierwszy bit to **0**, tak więc w adresach z tej klasy pierwsza część adresu należy do zakresu 0 – 127. Nie używa się adresu 0, z kolei adresy rozpoczynające się od 127 to adresy zarezerwowane dla tzw. pętli zwrotnej i niewykorzystywane do adresowania urządzeń sieciowych.

Pierwsze dwa bity adresów IP z **klasy B** to **10**, tak więc pierwsza część adresu z klasy B zawiera się w przedziale 128 – 191.

**Klasa C** jest oznaczana przez pierwsze 3 bity o wartości **110** (zakres adresów 192 – 223).

**Klasa D** jest oznaczana przez pierwsze 4 bity o wartości **1110** (zakres adresów 224 – 239).

**Klasa E** jest oznaczana przez pierwsze 4 bity o wartości **1111** (zakres adresów 240 – 255).

W adresowaniu urządzeń sieciowych wykorzystuje się tylko adresy z klasy A, B i C. Adresy z **klasy D** pozwalają na przesyłanie informacji do grupy adresów IP, dzięki czemu pojedyncze urządzenie podłączone do sieci jest w stanie rozsyłać informacje jednocześnie do wielu odbiorców (transmisja typu *multicast*). Z kolei pula adresów należąca do **klasy E** została zarezerwowana przez Internet Engineering Task Force — organizację odpowiedzialną za ustanawianie standardów w internecie.


**Rysunek 4.10.** Podział adresów na klasy

## Adres sieci i adres rozgłoszeniowy

Dla każdego adresu IP przypisanego do konkretnego urządzenia można określić dwa specyficzne adresy — adres sieci i adres rozgłoszeniowy.

**Adres sieci** określa sieć, do której przynależy dany adres IP. **Adres rozgłoszeniowy** (ang. *broadcast*) to adres pozwalający na wysłanie informacji do wszystkich urządzeń w danej sieci.

Adres sieci jest określany jako liczba, która w części adresu IP identyfikującej hosta ma bity ustawione na 0. Adres rozgłoszeniowy dla danej sieci w części hosta ma bity ustawione na 1.

Adresy sieci są wykorzystywane w procesie przełączania pakietów IP — routery przechowują w tablicach routingu adresy sieci oraz adresy, przez które są one dostępne.

Sposób wyznaczania adresu sieci oraz adresu rozgłoszeniowego przedstawia przykład 4.4.

**Przykład 4.4.** Wyznaczanie adresu sieci oraz adresu rozgłoszeniowego

| | |
|---|---|
| Adres IP: | 77.213.126.82 |
| Postać binarna: | 01001101 11010101 01111110 01010010 |

Jest to adres z klasy A, więc część sieci jest określana przez pierwsze 8 bitów, a adres sieci uzyskuje się przez ustawienie na ostatnich 24 bitach liczby 0.

| | |
|---|---|
| Postać binarna adresu sieci: | 01001101 00000000 00000000 00000000 |
| Postać dziesiętna adresu sieci: | 77.0.0.0 |
| Postać binarna adresu rozgłoszeniowego: | 01001101 11111111 11111111 11111111 |
| Postać dziesiętna adresu rozgłoszeniowego: | 77.255.255.255 |

Podział na klasy został wprowadzony w celu rozróżnienia wielkości sieci. Komunikacja w obrębie jednej sieci nie wymaga używania routerów, które są niezbędne w przypadku komunikacji między sieciami.

W przypadku klasy A istnieje możliwość utworzenia 126 użytecznych adresów sieci — od 1 do 126 (adres 0.0.0.0 nie jest wykorzystywany, sieć 127.0.0.0 jest siecią zarezerwowaną). Dla każdej z tych sieci można utworzyć po 16 777 216 adresów. Liczba adresów IP w sieci jest wyliczana na podstawie wzoru:

$L_{IP} = 2^n$,

gdzie: $L_{IP}$ — liczba adresów IP w sieci (liczba adresów do wykorzystania wymaga odjęcia pierwszego i ostatniego adresu rozgłoszeniowego), $n$ — liczba bitów w części hosta.

Dla klasy B istnieje możliwość utworzenia 16 384 sieci. Liczba ta wynika z możliwych kombinacji w części sieci adresu — 64 kombinacje w pierwszym oktecie i 256 kombinacji w drugim. W każdej sieci należącej do klasy B istnieje możliwość zaadresowania 65 536 adresów ($2^{16}$).

W klasie C istnieje możliwość utworzenia ponad 2 mln sieci (32·256·256 = 2 097 152) po 256 adresów ($2^8$).

Tabela 4.3 prezentuje właściwości poszczególnych klas adresów.

**Tabela 4.3.** Liczba adresów dostępnych w poszczególnych klasach

| Klasa adresu | Liczba bitów części sieci | Liczba bitów części hosta | Liczba dostępnych sieci | Liczba dostępnych adresów w sieci |
|---|---|---|---|---|
| Klasa A | 8 | 24 | 127 | 16 777 216 |
| Klasa B | 16 | 16 | 16 384 | 65 536 |
| Klasa C | 24 | 8 | 2 097 152 | 256 |

## Maska podsieci

Podział adresów na klasy wprowadzono w celu zróżnicowania wielkości sieci. Niestety podział ten powodował, że wiele adresów IP pozostawało niewykorzystanych. Organizacje otrzymywały pulę adresów całej sieci, a więc w przypadku sieci klasy A ponad 16 mln adresów IP do wykorzystania. Szybki rozwój internetu w latach 90. XX wieku i ogromna liczba przyłączanych do sieci urządzeń spowodowały konieczność wprowadzenia innego podziału na część sieci i część hosta. W celu zmiany sztywnego podziału adresu IP na część sieci i część hosta wprowadzono maskę podsieci.

**DEFINICJA**

**Maska podsieci** (ang. *subnet mask*), podobnie jak adres IP, jest liczbą 32-bitową rozpoczynającą się określoną liczbą bitów o wartości 1, po których jest dopełniana bitami o wartości 0. Najczęściej przedstawiano ją jako cztery liczby dziesiętne oddzielone kropkami (np. 255.255.255.0). Alternatywnie maska podsieci jest zapisywana jako liczba bitów oznaczonych 1 po znaku / (np. /24).

Kolejny bit w masce podsieci określa przynależność do części sieci lub hosta kolejnego bitu w adresie IP. **Bit maski oznaczony 1** mówi, że ten bit w adresie IP należy do części sieci, **bit oznaczony 0** mówi, że odpowiadający mu bit w adresie IP należy do części hosta.

**Przykład 4.5.** Zapis maski podsieci

| | |
|---|---|
| Adres IP: | 77.213.62.82 |
| Postać binarna: | 01001101 11010101 01111110 01010010 |
| Maska podsieci: | 255.0.0.0 |
| Postać binarna maski: | 11111111 00000000 00000000 00000000 |

## Podział sieci na podsieci

Algorytm dzielenia sieci na podsieci polega na znajdowaniu optymalnego podziału bitów należących do części hosta adresu IP.

W zależności od założeń problemu określamy liczbę bitów:

- należących do części podsieci,
- należących do części hosta.

Gdy zadana jest liczba wymaganych adresów w nowo tworzonej podsieci (z uwzględnieniem adresu sieci i adresu rozgłoszeniowego), znajdujemy najmniejszą potęgę liczby 2, która jest większa lub równa wymaganej liczbie adresów IP. Ilustruje to wzór:

$2^n >= L_{IP} + 2$,

gdzie: $L_{IP}$ — liczba adresów IP w podsieci, $n$ — liczba bitów w masce podsieci oznaczających część hosta.

Korzystając z tego wzoru, wyznaczymy prawidłową liczbę $n$, która odpowiada liczbie bitów oznaczonych liczbą **0**. Pozostałe oznacza się liczbą **1**.

Gdy zadana jest liczba podsieci, określamy najmniejszą potęgę liczby 2, która jest większa lub równa zadanej liczbie podsieci. Ilustruje to wzór:

$2^n >= L_{SUB}$,

gdzie: $L_{SUB}$ — liczba podsieci, $n$ — liczba bitów w części hosta oryginalnej maski oznaczających część sieci.

Korzystając z tego wzoru, wyznaczymy liczbę $n$, która określa liczbę bitów oznaczonych jako **1** w masce podsieci. Pozostałe bity są oznaczane jako **0**.

**Przykład 4.6.** Podział sieci adresów klasy C na 4 podsieci

Maska podsieci dla sieci klasy C (o przykładowym adresie 199.10.20.0) składa się z 24 bitów oznaczających część sieci oraz z 8 bitów oznaczających część hosta.

Aby utworzyć nową maskę, która podzieli pulę adresów danej sieci na 4 podsieci, należy znaleźć taką liczbę bitów, by możliwe było stworzenie 4 kombinacji. Posługując się odpowiednim wzorem, wyznaczamy liczbę $n = 2$:

$2^2 >= 4$.

Mając wyznaczoną liczbę $n$, powinniśmy zwiększyć liczbę bitów oznaczonych 1 o dwa.

| | |
|---|---|
| Adres sieci do podziału: | 199.10.20.0 |
| Domyślna maska podsieci: | 255.255.255.0 |
| Domyślna maska podsieci w postaci binarnej: | 11111111 11111111 11111111 00000000 |
| Nowa postać maski podsieci w zapisie binarnym: | 11111111 11111111 11111111 11000000 |
| Nowa postać maski podsieci w zapisie dziesiętnym: | 255.255.255.192 |

Mając określoną długość maski podsieci, możemy określić zakresy adresów w poszczególnych podsieciach, a także adresy podsieci i adresy rozgłoszeniowe (tabela 4.4). W tym celu należy wykonać omówione wyżej operacje logiczne.

**Tabela 4.4.** Zakresy wyznaczonych podsieci

| Zakres adresów w podsieci (dwójkowy) | Adres dziesiętny podsieci | Numer podsieci | Adres początkowy | Adres końcowy | Adres rozgłoszeniowy |
|---|---|---|---|---|---|
| 00000000<br>00111111 | 199.10.20.0 | Podsieć 0 | 199.10.20.1 | 199.10.20.62 | 199.10.20.63 |
| 01000000<br>01111111 | 199.10.20.64 | Podsieć 1 | 199.10.20.65 | 199.10.20.126 | 199.10.20.127 |
| 10000000<br>10111111 | 199.10.20.128 | Podsieć 2 | 199.10.20.129 | 199.10.20.190 | 199.10.20.191 |
| 11000000<br>11111111 | 199.10.20.192 | Podsieć 3 | 199.10.20.193 | 199.10.20.254 | 199.10.20.255 |

Jak pokazuje tabela, poprzez zmianę maski pula adresów sieci należącej do klasy C została podzielona na cztery mniejsze podsieci po 64 adresy każda. W ramach każdej z nich zostały wyodrębnione adresy podsieci i adresy rozgłoszeniowe, które nie mogą być przypisane do urządzeń sieciowych.

**Przykład 4.7.** Podział sieci klasy B na podsieci po 1000 adresów

Mając do dyspozycji sieć adresów klasy B 129.230.0.0, spróbujmy podzielić ją na maksymalną liczbę podsieci składających się z co najmniej 1000 adresów IP.

Maska podsieci dla sieci klasy B składa się z 16 bitów oznaczających część sieci oraz z 16 bitów oznaczających część hosta. Aby utworzyć nową maskę, która podzieli pulę adresów danej sieci na podsieci składające się z co najmniej 1000 adresów, należy

znaleźć taką liczbę bitów, by możliwe było zaadresowanie wymaganej liczby hostów. Posługując się wzorem, wyznaczamy liczbę *n* = 10:

$2^{10} >= 1000$.

Wyznaczona liczba *n* oznacza liczbę najmłodszych bitów w nowej masce podsieci, oznaczonej liczbą **0**.

| | |
|---|---|
| Adres sieci do podziału: | 129.230.0.0 |
| Domyślna maska podsieci: | 255.255.0.0 |
| Domyślna maska podsieci w postaci binarnej: | 11111111 11111111 00000000 00000000 |
| Nowa postać maski podsieci w zapisie binarnym: | 11111111 11111111 11111100 00000000 |
| Nowa postać maski podsieci w zapisie dziesiętnym: | 255.255.252.0 |

## Pętla zwrotna

W puli wszystkich adresów IP istnieje zakres adresów, które zostały zarezerwowane do specyficznego wykorzystania. Jednym z takich zakresów jest **sieć 127.0.0.0**, czyli adresy IP z przedziału 127.0.0.1 – 127.255.255.254. Adresy te są wykorzystywane w celu adresowania komputera (urządzenia) lokalnego. Komunikacja z tym adresem odwołuje się do urządzenia, które tę komunikację wywołało.

**DEFINICJA**

Mechanizm tej komunikacji jest nazywany **pętlą lokalną** lub **pętlą zwrotną** (ang. *loopback*). Pętla zwrotna to wirtualne urządzenie sieciowe, które z poziomu systemu operacyjnego nie różni się od fizycznej karty sieciowej. Komunikacja z adresem pętli zwrotnej może odbywać się poprzez dowolny adres należący do sieci 127.0.0.0 lub poprzez nazwę *localhost* (w systemie operacyjnym nazwa przypisana dla adresu 127.0.0.1).

Mechanizm pętli zwrotnej może być wykorzystywany do kontroli poprawności instalacji obsługi protokołu IP w systemie operacyjnym.

## Adresy prywatne i adresy publiczne

Część adresów IP jest wykorzystywana do adresowania urządzeń w sieciach lokalnych. Sieci lokalne działają na ograniczonym obszarze. Komunikacja między urządzeniami w tej sieci nie wymaga przypisywania im tzw. adresów publicznych. **Adresy prywatne** to adresy niepowtarzalne w ramach struktury sieci lokalnej, **adresy publiczne** są unikalne w skali całego internetu. Takie same adresy prywatne mogą być używane w wielu

sieciach lokalnych. Adresy publiczne są przypisywane tylko i wyłącznie jednemu interfejsowi sieciowemu.

Zakresy adresów prywatnych:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.0.0

Jak widać, w każdej klasie zostały wyznaczone adresy prywatne do wykorzystania w sieciach lokalnych, dzięki czemu istnieje możliwość budowy dowolnej, nawet bardzo rozbudowanej struktury sieci. Dostęp do internetu dla urządzeń z prywatnymi adresami IP jest możliwy dzięki zastosowaniu technologii translacji adresów.

## Translacja adresów

Wzrost liczby komputerów w internecie spowodował, że groźba wyczerpania puli dostępnych adresów publicznych stała się całkiem realna. Aby temu zaradzić, przyjęto zasadę, że lokalne sieci komputerowe korzystające z adresów prywatnych (specjalna pula adresów tylko dla sieci lokalnych) mogą zostać podłączone do internetu przez router, mający mniej adresów publicznych, niż jest komputerów w tej sieci.

Router ten, gdy komputery z sieci lokalnej komunikują się ze światem, dynamicznie tłumaczy adresy prywatne na adresy publiczne, umożliwiając użytkowanie internetu przez większą liczbę komputerów, niż pozwalałaby na to liczba adresów zewnętrznych. Technika ta polega na zmianie adresów i portów źródłowych (dla pakietów wychodzących) lub docelowych (dla pakietów przychodzących). Adresem nadawcy pakietu staje się router z publicznym adresem IP, który również nadaje numer portu. Takie przekierowanie jest zapisywane w tablicy. Pakiety, które wracają do routera, są modyfikowane na podstawie zapisu w tablicy, otrzymując właściwy adres i port odbiorcy znajdującego się w sieci wewnętrznej (z prywatną adresacją IP).

**DEFINICJA**

**Technologia NAT** (ang. *Network Address Translation*) jest wykorzystywana przez niewielkie routery przeznaczone do użytku domowego oraz przez mechanizm udostępniania połączenia internetowego w systemie Windows.

## Przydzielanie adresów IP

Adresy IP zwane są również adresami logicznymi. W przeciwieństwie do adresów fizycznych (MAC), zapisywanych w pamięciach ROM interfejsów sieciowych, są one nadawane przez administratora sieci. Adres może być przypisany statycznie (ręczna konfiguracja urządzenia) lub dynamicznie — urządzenie otrzymuje wówczas adres z serwera działającego w sieci.

Serwerem umożliwiającym uzyskanie parametrów konfiguracyjnych takich jak adres IP, maska podsieci, adres bramy domyślnej jest **serwer DHCP** (ang. *Dynamic Host Configuration Protocol*). Jest on następcą protokołu BOOTP (ang. *BOOTstrap Protocol*). Urządzenie, które nie ma statycznie przypisanego adresu IP, wysyła do wszystkich komputerów w sieci (*broadcast*) zapytanie o parametry konfiguracyjne. Jeśli w sieci znajduje się serwer DHCP, odpowiada on na prośbę, wysyłając parametry takie jak adres IP, maska podsieci, brama domyślna i adres serwera DNS. Jeśli w sieci nie działa serwer DHCP lub nie jest on dostępny, to uruchomiony zostaje mechanizm APIPA (ang. *Automatic Private IP Addressing*). Jego zadaniem jest przypisanie adresu IP w przypadku nieotrzymania go od serwera działającego w sieci. Mechanizm APIPA przydziela adres z puli 169.254.0.1 – 169.254.255.254 (sieć 169.254.0.0, maska podsieci 255.255.0.0).

Dynamiczne konfigurowanie adresów pozwala na łatwiejsze zarządzanie siecią. Konfiguracja serwera umożliwia przypisywanie stałych adresów IP na podstawie adresów MAC, jak również przypisywanie adresów na zadany czas.

## 4.6.2. Protokół IPv6

Adresacja w sieci internet w chwili obecnej opiera się na protokole IP w wersji 4. (*IPv4*, ang. *Internet Protocol version 4*). Adres IP w wersji 4. to liczba 32-bitowa (od 0 do 4 294 967 295). Obecnie liczba publicznych adresów IP jest na wyczerpaniu. Jest to spowodowane dużym przyrostem liczby użytkowników sieci, a co za tym idzie, zwiększonym zapotrzebowaniem na usługi sieciowe, a więc także i adresy IP.

W latach 90. ubiegłego wieku podjęto prace nad zbudowaniem nowego systemu komunikacji. Stworzono protokół **IPv6 / IPNG** (ang. *Internet Protocol version 6* / *Internet Protocol Next Generation*). Protokół ten wprowadza 128-bitową adresację, a więc umożliwia zaadresowanie $2^{128}$ urządzeń. Adres IP w wersji 6. jest przedstawiany w postaci szesnastkowej, z dwukropkiem co 16 bitów (np. 32fa:a237:0000:0000:cd21:1521:1175:67af).

Specyfikacja IPv6 pozwala na pomijanie początkowych zer w bloku, a także na pomijanie kolejnych bloków składających się z samych zer i zastąpienie ich podwójnym dwukropkiem „::”. Dopuszczalny jest tylko jeden podwójny dwukropek „::” w adresie. Poniższy przykład pokazuje równoważne poprawne zapisy jednego adresu IPv6.

**Przykład 4.8.**

5423:0246:0000:0000:0000:0000:2583:fa25

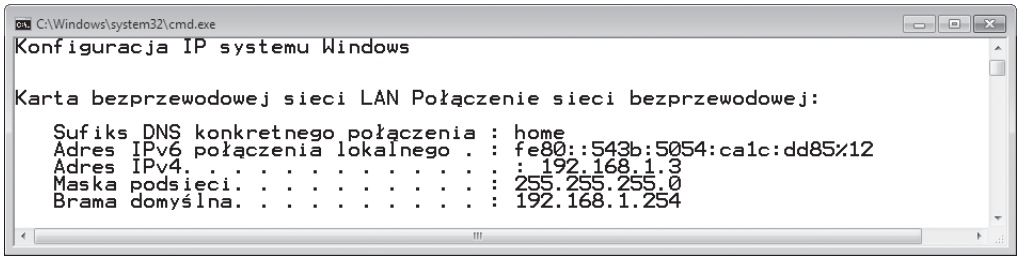
5423:0246:0:0:0:0:2583:fa25

5423:0246:0:0:0::2583:fa25

5423:0246::2583:fa25

5423:246::2583:fa25

Rysunek 4.11 przedstawia przykład adresacji IPv6 w systemie Windows 7.




**Rysunek 4.11.** Przykład adresacji w Windows 7

## Adresy zarezerwowane

W specyfikacji adresacji IPv6 występują adresy specjalne i zarezerwowane do szczególnych celów. Najważniejsze z nich zostały przedstawione poniżej:

::/128 — adres nieokreślony, zawierający same zera.

::1/128 — adres pętli zwrotnej.

::/96 — pula adresów zarezerwowana w celu zachowania kompatybilności wstecznej z aktualnie używaną wersją protokołu IP.

2001:db8::/32 — pula adresów do wykorzystania w przykładach i dokumentacji, nieużywana w produkcyjnie działających systemach.

2002::/24 — są to adresy wygenerowane na podstawie istniejących aktualnie używanych publicznych adresów IPv4.

### ĆWICZENIA

1. Wyświetl trasę routingu.
2. Sprawdź działanie poleceń: `ping`, `netstat`, `tracert`.
3. Sprawdź adres bramy domyślnej dla swojego komputera.
4. Sprawdź adres IP swojego komputera.

## PYTANIA

1. Wymień wszystkie warstwy modelu OSI. Jakie funkcje pełnią one w transmisji danych?
2. Czym różni się model TCP/IP od modelu OSI?
3. Jakie urządzenia działają w warstwie dostępu do sieci oraz w warstwie internetu?
4. Wymień protokoły warstwy sieci.
5. Wymień protokoły warstwy aplikacji.
6. Czym różni się protokół TCP od UDP?
7. Jakie wpisy zawiera tablica routingu?
8. Wymień trzy protokoły routingu. Jakie jest ich zadanie?
9. Co oznacza termin gniazdo w przypadku transmisji sieciowej?
10. W której warstwie modelu ISO pracują switche?
11. Na jakich portach pracują takie usługi jak FTP, SMTP, HTTP?
12. Wymień protokoły warstwy aplikacji.
13. Z ilu bitów składa się adres IPv4?
14. Z ilu bitów składa się adres IPv6?
15. Jak wygląda adres pętli zwrotnej w IPv4?
16. Jak wygląda adres pętli zwrotnej w IPv6?