Sieci Komputerowe
UG 2013/2014

Spis treści

Sieciowy system operacyjny

to taki, który ma wbudowane mechanizmy komunikacji z innymi komputerami o takim samym systemie (lub posiadającymi kompatybilne oprogramowanie). Programy użytkowe oparte na funkcjach komunikacyjnych systemu operacyjnego oferują różnego rodzaju usługi - np. umożliwiają korzystanie z systemu plików na innym komputerze, mogą zlecać wykonanie na nim pojedynczych procedur lub nawiązywać z nim trwałą łączność (otwierać sesję).
Klasycznym przykładem systemu sieciowego jest Unix (udostępnia wszystkie w/w usługi).
System oferujący jedynie zdalny dostęp do swojego systemu plików nazywany jest **serwerem plików**.

Rozproszony system operacyjny

to taki sieciowy system operacyjny, który działając w pewnej liczbie komputerów połączonych w sieć sprawia na ich użytkownikach wrażenie, że pracują na jednym (dużym, wielodostępnym) komputerze.
Własność uwalniania użytkowników systemu sieciowego od potrzeby świadomości (szczegółów technicznych) aspektów komunikacji wewnątrz sieci nazywamy **przezroczystością** (transparency).
Istnieją różne rodzaje przezroczystości, np.:

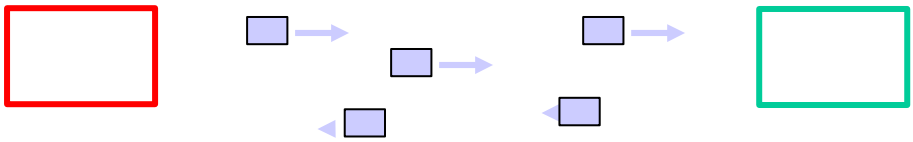
- **przezroczystość położenia zasobów**
- **przezroczystość zwielokrotniania**
- **prezroczystość awarii**
- **przezroczystość działań równoległych**

Ostatni rodzaj przezroczystości (dotyczący programistów, a nie zwykłych użytkowników komputerów) jest algorytmicznie najtrudniejszy do uzyskania.

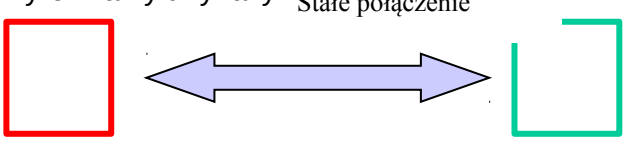
3. MODELE TEORETYCZNE ZWIĄZANE Z KOMUNIKACJĄ SIECIOWĄ

1) Modele rodzajów komunikacji
a) komunikacja bezpołączeniowa i połączeniowa

Komunikacja bezpołączeniowa polega na przesyłaniu ciągu oddzielnych porcji informacji. Każda z nich jest zaopatrzona w adres odbiorcy i może wędrować do celu niezależnie od pozostałych. Drogi przebywane przez poszczególne przesyłki mogą być różne, czasy osiągania celu też mogą być różne (przesyłki mogą docierać do odbiorcy w innej kolejności, niż zostały wysłane).



Komunikacja połączeniowa polega na przesyłaniu strumienia informacji o (teoretycznie) nieograniczonej długości przez otwarty przedtem **kanał komunikacyjny**. W przypadku takiej komunikacji elementy informacji docierają do odbiorcy w niezmienionej kolejności.
W komunikacji połączeniowej wyróżniamy trzy fazy:
1) nawiązania połączenia;
2) przesyłania informacji;
3) rozwiązania połączenia.



b) komunikacja zawodna i niezawodna

O komunikacji połączeniowej zazwyczaj zakładamy, że jest niezawodna (dopóki trwa, zapewnia przekazywanie informacji bez zniekształceń).
Komunikacja bezpołączeniowa czasem jest zawodna (przesyłki mogą być gubione na trasie, duplikowane lub mogą przychodzić w zmienionej kolejności). Sposób, aby komunikację bezpołączeniową uczynić niezawodną:
a) przesyłki muszą być opatrywane unikalnymi oznaczeniami (np. numerowane);
b) odbiorca musi **potwierdzić** otrzymanie każdej przesyłki - jeśli nadawca nie otrzyma potwierdzenia w określonym czasie (timeout), wysyła duplikat przesyłki;
c) odbiorca układa przesyłki według ich numeracji, eliminując jednocześnie niepotrzebne duplikaty.
Jeśli odbiorca zna kolejność numerowania przesyłek, możliwe jest rozwiązanie, w którym zamiast wysyłania **pozytywnych zawiadomień** o odebraniu przesyłki (positive acknowledgement), odbiorca wysyła jedynie **zawiadomienia negatywne** (negative acknowledgement), tj. zawiadomienia o brakujących przesyłkach.

c) komunikacja dwukierunkowa, naprzemienna i jednokierunkowa

W przypadku komunikacji dwukierunkowej **(full-duplex, duplex)** łącze jest dwutorowe i obie strony są w stanie przekazywać sobie informacje jednocześnie.
Przykład: rozmowa telefoniczna.
W przypadku komunikacji naprzemiennej **(half-duplex)** łącze jest jednotorowe dwukierunkowe - informacje mogą być przekazywane w obu kierunkach, ale nie jednocześnie.
Przykład: rozmowa przez krótkofalówkę.
W przypadku komunikacji jednokierunkowej **(simplex)** łącze jest jednokierunkowe - jedna ze stron pełni wyłącznie rolę nadawcy, a druga odbiorcy.
Przykład: odbiór audycji radiowej.

2) Modele relacji pomiędzy uczestnikami procesu komunikacji

a) Ze względu na grono adresatów informacji wyróżniamy komunikację:

- ***indywidualną (unicast, individual)* -** informacja kierowana jest do dokładnie jednego wybranego

adresata;

- **rozsyłanie grupowe (multicast)** - informacja rozsyłana jest do z góry określonej grupy odbiorców

(według posiadanej listy adresowej);

- **rozgłaszanie (broadcast)** - informacja rozsyłana jest do nieokreślonej, dowolnie szerokiej grupy

odbiorców (analogia: podawanie „do publicznej wiadomości”).

b) model klient-serwer (client-server)

Założenia:

- adres (identyfikator) serwera jest **powszechnie znany** (well-known) dla wszystkich potencjalnych

klientów;

- serwer funkcjonuje w sposób ciągły i jest zawsze dostępny (w skończonym czasie) dla każdego

klienta;

- adresy (identyfikatory) klientów nie są znane serwerowi i aby uzyskać odpowiedź, klienci muszą

podawać serwerowi swój **adres zwrotny** (return address) lub tworzyć połączenie.
Uwaga: 1) Żądania wobec serwera muszą być formułowane przez klientów w sposób zrozumiały dla
serwera (tj. przy użyciu protokołu komunikacyjnego, którym dysponuje serwer).
2) Niekiedy za przeciwieństwo modelu klient-serwer uważany jest model równy-z-równym
(peer-to-peer)

3) Organizacja komunikacji

Z dotychczasowych rozważań wynika, że aby przekazać pewną porcję informacji, trzeba zazwyczaj wykonać pewną liczbę czynności dodatkowych (np. nawiązać połączenie, wysłać potwierdzenia odbioru, zasygnalizować koniec połączenia itp.). Sumę tych wszystkich czynności, nie będących samym przekazywaniem informacji, nazywamy **narzutem** (overhead).
Protokołem komunikacyjnym nazywamy zbiór reguł określających ciąg czynności, jakie trzeba wykonać, aby przekazać porcję informacji.
W sieciach komputerowych stosowanych jest bardzo wiele różnych protokołów komunikacyjnych, organizują one różne rodzaje komunikacji dla konkretnych celów, bądź do ogólnego użytku.

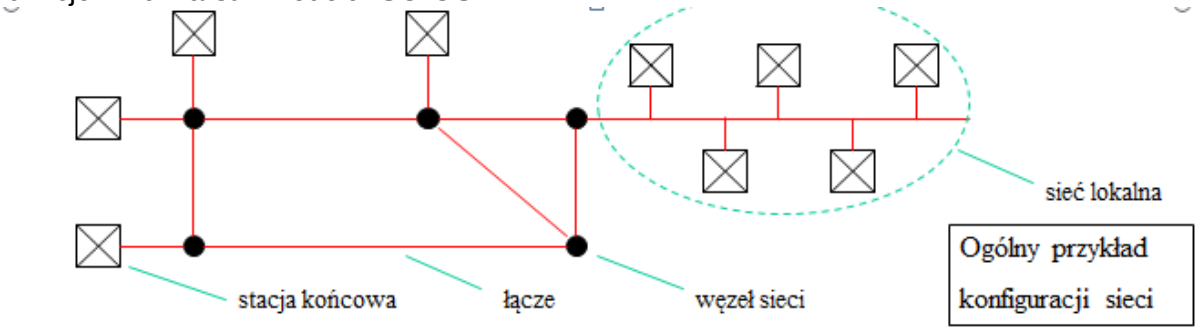
4) Warstwowość oprogramowania

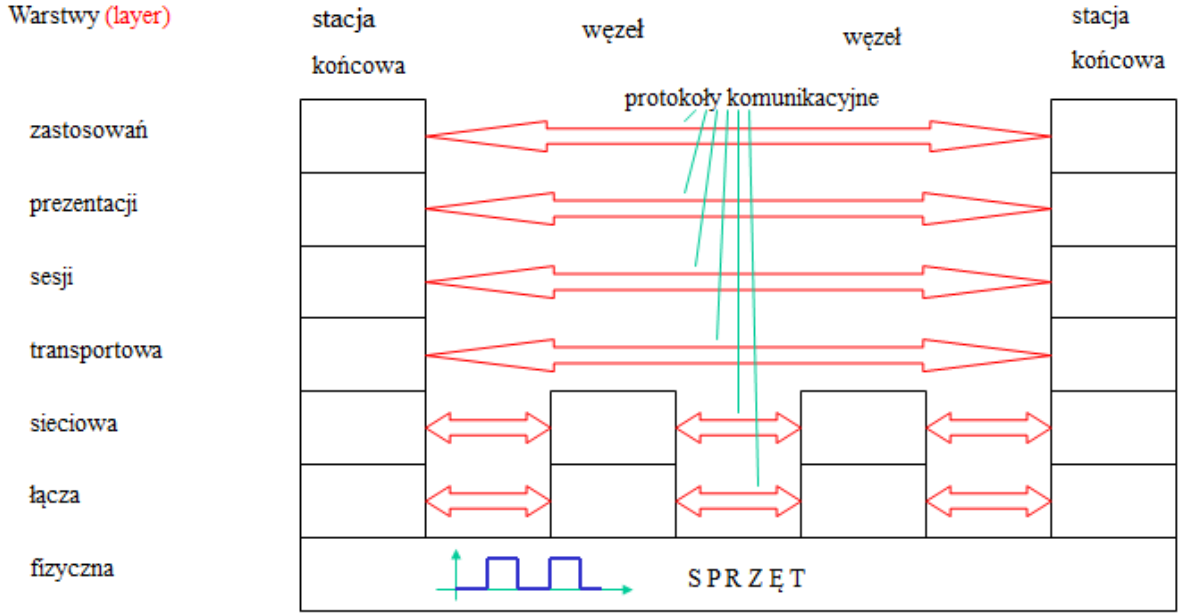
Współczesne programy komputerowe są na tyle skomplikowane, że często jest praktycznie niemożliwe zorganizowanie ich w postaci jednego zbioru podprogramów zarządzanych przez program główny. Duże programy mają **strukturę warstwową**, przy czym najniższa warstwa podprogramów operuje na **danych fizycznych** (lokatach w pamięci, portach wejścia/wyjścia), a wyższe warstwy - na **danych abstrakcyjnych** (logicznych) zdefiniowanych przy użyciu danych niższego poziomu.
Z punktu widzenia metodologii programowania istotne jest, aby:

- obiekty (abstrakcyjne typy danych) *n*-tej warstwy były definiowane na bazie obiektów *n-1*-szej warstwy (ale nie niższych);
- procedury *n*-tej warstwy (wykonujące operacje na obiektach *n*-tej warstwy) były definiowane na bazie procedur *n-1*-szej warstwy (ale nie niższych).

Dziedzina protokołów komunikacyjnych jest obecnie najbardziej sztandarowym przykładem warstwowości oprogramowania.
Międzynarodowa organizacja standaryzacyjna ISO opracowała specyfikację warstwowego modelu komunikacji OSI (Open Standard Interconnection) nazwanego **modelem otwartym**. Model ten składa się z 7 warstw i nie zawiera dokładnych specyfikacji struktur danych i procedur dla

poszczególnych warstw, a jedynie ogólne wytyczne. Specyfikacje obecnie używanych protokołów komunikacyjnych zwykle stanowią uściślenia tych wytycznych.
Uwaga: istniejące protokoły komunikacyjne (szczególnie wyższych poziomów) czasem łączą funkcje kilku warstw modelu ISO-OSI.





Zbiór współpracujących ze sobą protokołów obejmujący wszystkie warstwy - od fizycznej do zastosowań - nazywamy **stosem protokołów** (protocol stack) lub **zestawem protokołów** (protocol suit).

Ogólne zadania kolejnych warstw stosu protokołów:

1) Warstwa fizyczna

umożliwia przesyłanie **bitów**. Specyfikuje elektryczne i mechaniczne własności
łącz, reprezentacje bitów w postaci przebiegów elektrycznych, dopuszczalne częstotliwości
i opóźnienia sygnałów elektrycznych w łączach oraz charakterystyki i sposoby sterowania

nadajnikami i odbiornikami sygnałów w stacjach końcowych lub węzłach sieci. Wykrywa

i sygnalizuje wyższym warstwom uszkodzenia bitów i awarie łącza.

2) Warstwa łącza

umożliwia przesyłanie ciągów bitów nazywanych zwykle **ramkami** pomiędzy urządzeniami przyłączonymi do tego samego łącza fizycznego. Koryguje błędy zasygnalizowane przez warstwę fizyczną i rozwiązuje **kolizje** (próby nadawania przez więcej, niż jedno urządzenie jednocześnie). Operuje na unikalnych oznaczeniach sprzętu sieciowego, tzw. **adresach fizycznych**.

3) Warstwa sieciowa

umożliwia przesyłanie ciągów bitów zwanych **pakietami** (pakiety są opakowane w ramki) na większą odległość, niż tylko pomiędzy bezpośrednio połączonymi urządzeniami. Operuje na systemie adresów logicznych mającym hierarchiczną strukturę i obejmującym większy fragment sieci. Wyznacza trasę przesyłu pakietów przez kolejne węzły sieci.

4) Warstwa transportowa

organizuje komunikację połączeniową (tworzy **łącze logiczne**) lub bezpołączeniową (przesyła **datagramy**) pomiędzy **procesami** w dwóch dowolnie oddalonych stacjach końcowych. Może zapewniać łączność niezawodną poprzez obsługę błędów popełnianych w warstwie sieciowej (gubienie, zmianę kolejności lub duplikowanie pakietów).

5) Warstwa sesji

organizuje wymianę informacji (dialog) pomiędzy dwoma procesami. Umożliwia otwarcie i zamknięcie sesji, określa tryb pracy (half-duplex lub full-duplex), może też wprowadzać limity czasu poszczególnych transmisji.

6) Warstwa prezentacji

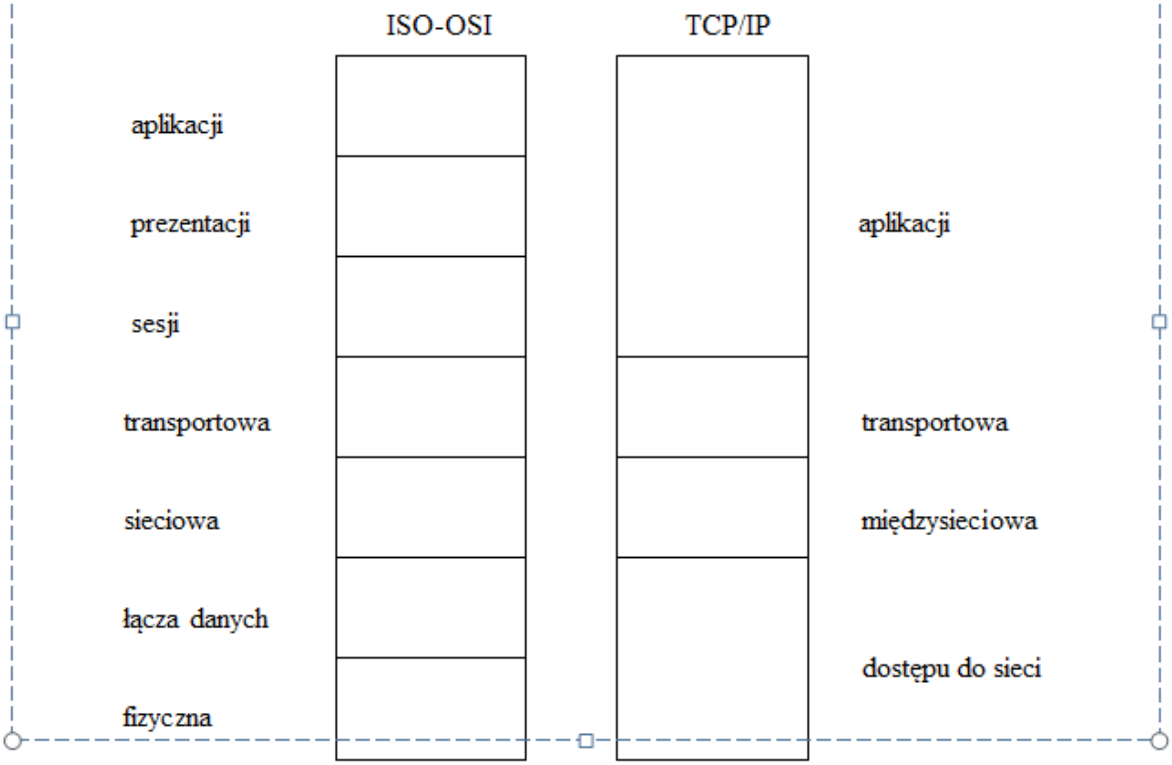
zawiaduje postacią przesyłanych informacji. Ustala sposoby kodowania (np. format liczb lub łańcuchów), w razie potrzeby dokonuje konwersji. Może też stosować szyfrowanie i deszyfrowanie oraz kompresję (upakowanie) przesyłanych danych.

7) Warstwa zastosowań

dostarcza podprogramów wchodzących bezpośrednio w skład programów użytkowych. Ich typowe zadania to transmisja plików, zdalne wywoływanie procedur, emulacja

działania zdalnego terminala, odczyt poczty elektronicznej itp.
Uwaga: oprogramowanie sieciowe istniejące obecnie tylko w przybliżeniu (często dość grubym)
jest dopasowane do modelu ISO-OSI. Duża jego część powstała jeszcze przed opracowaniem
tego modelu. Na ogół stosy protokołów mają mniej, niż siedem warstw.
Poszczególne stosy protokołów zazwyczaj nie są rozłączne - często na wcześniej skonstruowanym protokole *n*-tej warstwy oparty jest więcej niż jeden protokół warstwy
n+1-szej (klasyczny przykład: protokoły warstwy transportowej TCP i UDP oparte na protokole warstwy sieciowej IP).

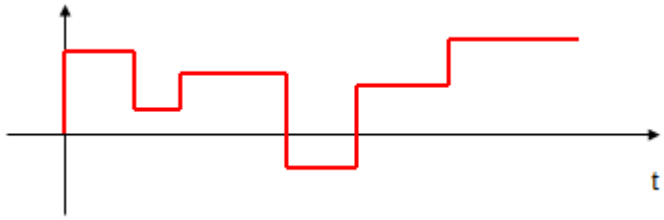
Porównanie istniejącego stosu protokołów TCP/IP z wzorcowym stosem ISO-OSI:



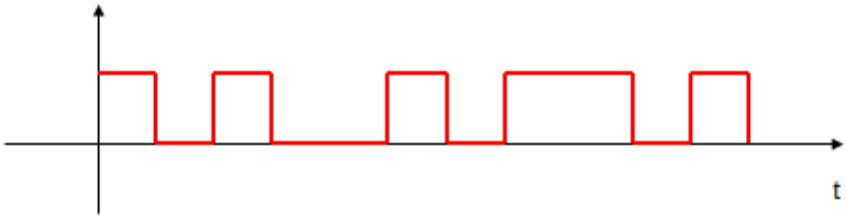
4. WARSTWA FIZYCZNA SIECI KOMPUTEROWYCH

Za **sygnał** może być uważana każda funkcja, której zmienną niezależną jest czas. Poniżej będziemy
rozważali tylko sygnały elektryczne, czyli takie, że poziom napięcia elektrycznego na wyjściu pewnego urządzenia jest funkcją czasu.
Sygnał może być **analogowy** (będący ciągłą funkcją czasu)

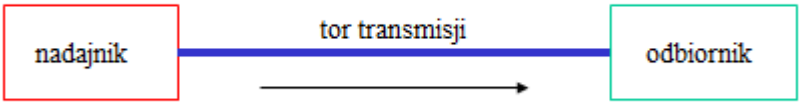
lub **dyskretny** (przyjmujący co najwyżej przeliczalny zbiór wartości).



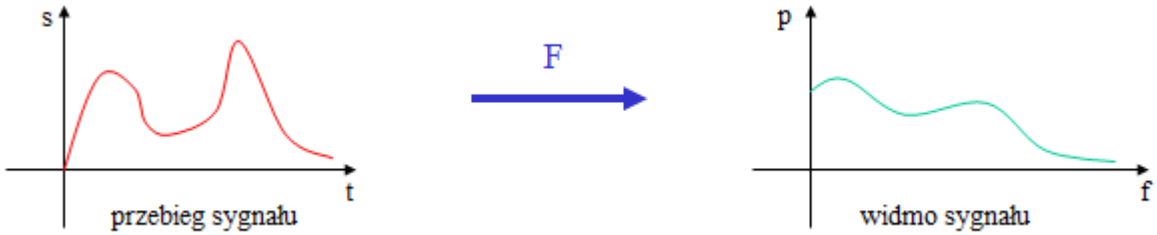
Szczególnym przypadkiem sygnału dyskretnego jest sygnał **binarny**, mogący przyjmować jedynie
dwie wartości (zazwyczaj jedną z nich jest 0).



Urządzenie wytwarzające sygnał nazywamy **nadajnikiem**, a urządzenie wykorzystujące sygnał
odbiornikiem. Sygnał przebywa drogę od nadajnika do odbiornika poprzez **tor transmisji**.



Transmisja (przekazywanie sygnału) przebiega w pewnym **ośrodku** (medium) **transmisyjnym**,
który może być ośrodkiem materialnym (np. kabel metalowy, światłowód, powietrze) lub próżnią.
W każdym rzeczywistym ośrodku prędkość rozchodzenia się sygnału jest skończona (ograniczona
przez prędkość światła w próżni), a ponadto mają miejsce straty energii sygnału i zakłócenia.
Mówimy, że w czasie transmisji sygnał podlega **opóźnieniu** i **zniekształceniu**.
Zamiast przebiegu czasowego sygnału można rozpatrywać jego reprezentację w dziedzinie częstotliwości uzyskaną przez zastosowanie ciągłej transformaty Fouriera.



W przypadku sygnału o skończonej mocy jego widmo powyżej pewnej częstotliwości staje się już pomijalnie małe. Zakres częstotliwości, w jakim widmo uważamy za niezerowe, nazywamy
pasmem sygnału, a jego długość nazywamy **szerokością pasma**.

Każdy tor transmisji posiada swoją **charakterystykę częstotliwościową**, czyli zależność przewodzenia składowej sygnału od częstotliwości tej składowej. Charakterystyka częstotliwościowa zależna jest od:
a) rodzaju ośrodka; b) kształtu i rozmiarów toru transmisji. Dla rzeczywistych ośrodków ich charakterystyki częstotliwościowe powyżej pewnej częstotliwości stają się bliskie zeru (czyli składowe sygnałów o wyższych częstotliwościach są prawie całkowicie tłumione), możemy więc
mówić o **paśmie przenoszenia** danego toru transmisji.
W przypadku idealnym, gdy pasmo sygnału zawiera się w paśmie przenoszenia toru transmisji,
a ponadto pasmo przenoszenia jest funkcją stałą w zakresie pasma sygnału, sygnał po przebiegu przez
tor transmisji jest stłumiony i opóźniony, ale jego kształt nie ulega zmianie.

$$s(t) \xrightarrow[\text{tor transmisji}]{} a \cdot s(t-\tau)$$

W rzeczywistych ośrodkach zawsze jednak następują pewne zniekształcenia.

Sygnał możemy traktować jako zakodowaną postać pewnej **informacji**. Jeżeli informacja jest
zakodowana w postaci sygnału analogowego, to po przepuszczeniu tego sygnału przez łącze nieidealne
dokładne odzyskanie z niego informacji (odkodowanie) jest praktycznie niemożliwe.
Jeżeli informacja jest zakodowana binarnie (czyli dana jest w postaci ciągu bitów), to po przejściu
sygnału cyfrowego przez łącze nieidealne jest możliwe (jeśli zniekształcenia nie są zbyt duże)
całkowite odtworzenie tej informacji. Jest to podstawowa zaleta sygnału cyfrowego.

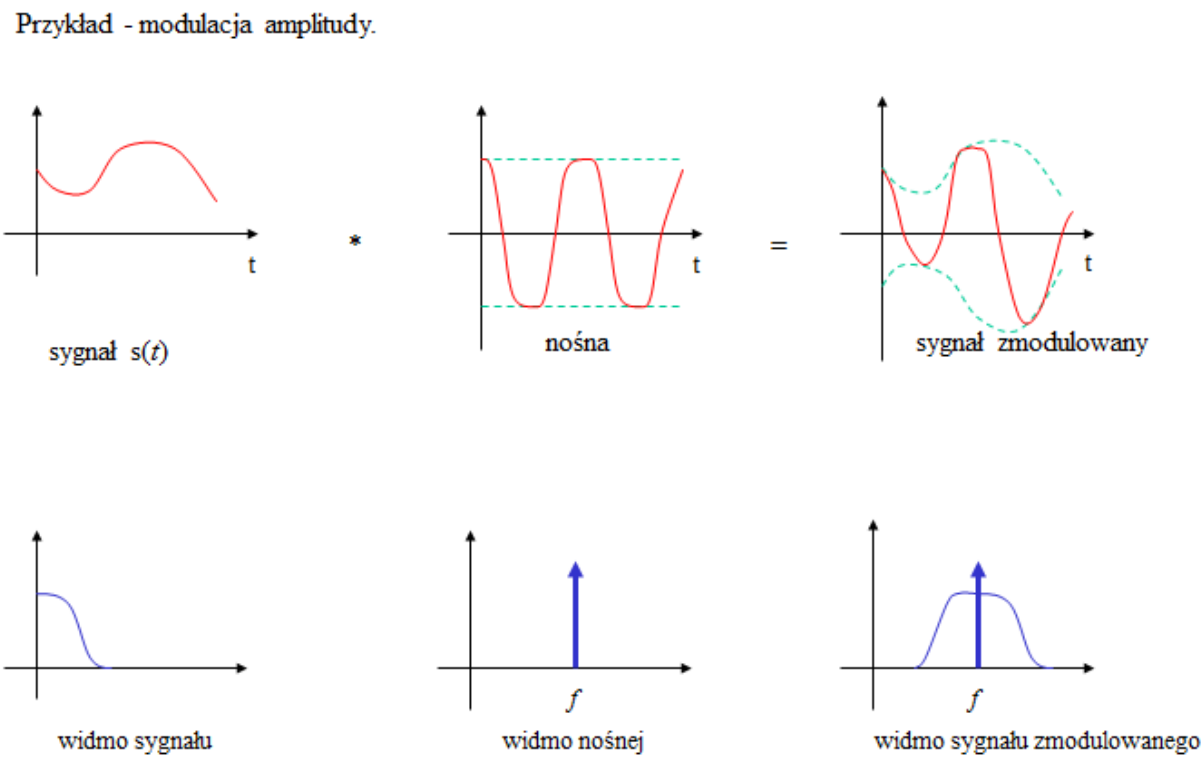
Modulacja i zwielokrotnianie

Jeżeli pasmo przenoszenia pewnego toru transmisji jest dużo szersze, niż pasmo wykorzystywane
przez pojedynczy sygnał, można przez ten tor transmisji przesyłać wiele sygnałów jednocześnie.
Możliwość taka jest uzyskiwana poprzez **modulację**:

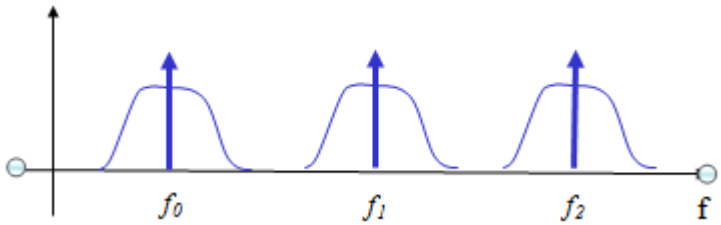
A·*cos*(2p*ft* – j) - ogólna postać równania fali nośnej

A - amplituda
***f* - częstotliwość**
j - faza

Uzmienniając jeden z powyższych parametrów tak, aby zmieniał się w czasie proporcjonalnie do
sygnału s(*t*), uzyskujemy odpowiednio modulację amplitudy, częstotliwości lub fazy.
Przykładowo s(*t*)·*cos*(2*p f t* – *j*) jest równaniem przebiegu o zmodulowanej amplitudzie.



Zwielokrotnianie przesyłu w łączu polega na generowaniu wielu nośnych odległych od siebie na
osi częstotliwości o więcej, niż podwojona szerokość pasma sygnału użytecznego, i modulowaniu
każdej z nośnych innym sygnałem użytecznym. Suma zmodulowanych sygnałów jest przepuszczana
przez łącze, a następnie poszczególne sygnały użyteczne są **odfiltrowane** i rozdzielone.



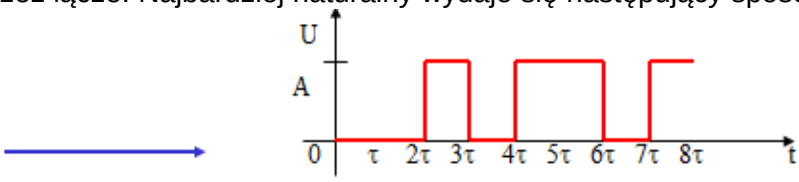
Przesyłanie samego sygnału użytecznego (bez żadnej modulacji) nazywamy przesyłaniem
w **paśmie podstawowym**. Zazwyczaj w lokalnych sieciach komputerowych stosowane jest przesyłanie w paśmie podstawowym, natomiast w sieciach rozległych stosowane jest zwielokrotnianie.

Przesyłanie informacji binarnej

Jeżeli informacja dana jest w postaci ciągu bitów, wystarczy zareprezentować ją sygnałem cyfrowym,
żeby mogła być przesłana przez łącze. Najbardziej naturalny wydaje się następujący sposób:

Przykład:

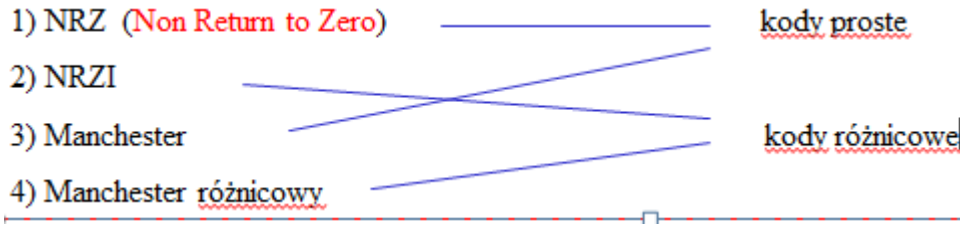
0 0 1 0 1 1 0 1



Taki sposób wydaje się bardzo prosty, ale wyłaniają się różne problemy techniczne.
Problemy:
1) Jak dobrać amplitudę A i okres t, żeby w wyniku przejścia przez łącze sygnał był na tyle mało
zniekształcony, aby można było odtworzyć z niego pierwotny ciąg bitów, a jednocześnie żeby
przesłać jak najwięcej informacji w jednostce czasu ?
2) Jak poinformować odbiornik, kiedy sygnał użyteczny zaczyna się, a kiedy kończy (ciąg zer też
może być sygnałem użytecznym) ?
3) Jak spowodować, żeby w przypadku przesyłania długiego ciągu bitów nie nastąpiło **rozsynchronizowanie** nadajnika i odbiornika (częstotliwości wzorcowe nadajnika i odbiornika
mogą się minimalnie różnić) ?
4) W komputerze najmniejszą adresowalną jednostką jest 1 bajt (8 bitów) - jak dokonać **serializacji** informacji równoległej, a potem **deserializacji** informacji szeregowej (czy np. przyjąć, że najwcześniejszy jest bit najbardziej znaczący, czy najmniej znaczący) ?

Jest stosowanych co najmniej kilka różnych systemów kodowania bitów - każdy z nich ma swoje wady i zalety, i jest stosowany w innych sytuacjach.

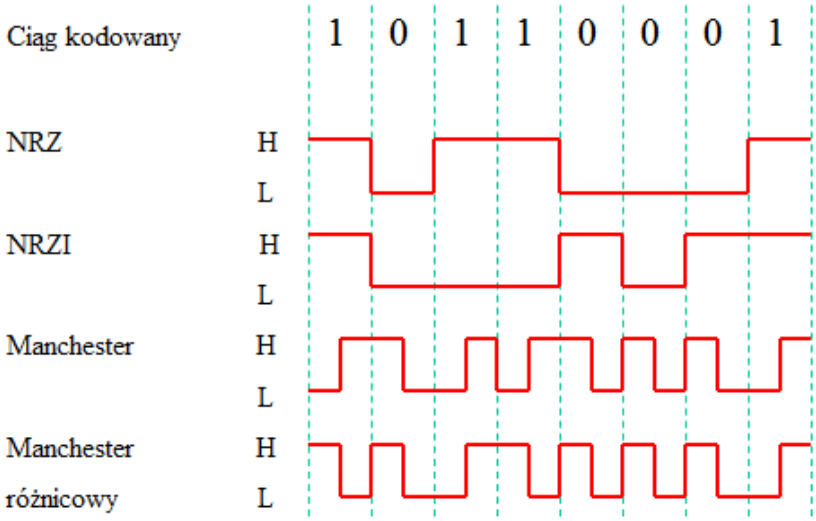
Cztery najczęściej stosowane kodowania:



	Dane	Szukane	
Kod	Informacja źródłowa	Poziom sygnału zakodowanego w czasie	
		od -0.5T do 0	od 0 do 0.5T	od 0.5T do T
NRZ (prosty)	1	nieistotny	H	H
	0	nieistotny	L	L
NRZI (różnicowy)	1	H	H	H
		L	L	L
	0	H	L	L
		L	H	H
Manchester (prosty)	1	nieistotny	L	H
	0	nieistotny	H	L
Manchester różnicowy	1	H	H	L
		L	L	H
	0	H	L	H
		L	H	L

H - wysoki poziom napięcia (High) L - niski poziom napięcia (Low)

Przykład



Uwaga: dla kodów różnicowych przyjęto, że przed pierwszym okresem sygnalizacji poziom sygnału był H.

Własności powyższych kodów:

1) Kody NRZ i NRZI zachowują stały poziom napięcia w ciągu jednego okresu sygnalizacji, kody Manchester i Manchester różnicowy zawsze zmieniają poziom napięcia w połowie okresu.

2) W widmach sygnałów w kodzie Manchester i Manchester różnicowy częstotliwości dominujących składowych są przeciętnie dwukrotnie wyższe, niż w widmach sygnałów w kodzie NRZ i NRZI, zatem sygnały w kodzie Manchester i Manchester różnicowy są przeciętnie silniej tłumione, niż sygnały w kodzie NRZ i NRZI.

3) Sygnały w kodzie NRZ i NRZI mogą zachowywać stały poziom napięcia przez dowolnie długi czas (co grozi rozsynchronizowaniem nadajnika i odbiornika), sygnały w kodzie Manchester i Manchester różnicowy mogą zachowywać stały poziom przez co najwyżej długość jednego **okresu (są to tzw. kody samosynchronizujące).**

4) Sygnały w **kodzie NRZ i NRZI** w przypadku przewagi zer nad jedynkami (lub na odwrót) wprowadzają składową stałą sygnału (tzn. średni poziom napięcia w łączu może odbiegać od

średniej arytmetycznej H i L), co może być niekorzystne w przypadku niektórych rozwiązań technicznych, dla sygnałów w kodzie Manchester i Manchester różnicowy średnia wartość napięcia zawsze wynosi (H + L) / 2.

5) Kody różnicowe są bardziej odporne na przypadkowe zakłócenia i przypadkową zmianę polaryzacji sygnału (zamianę końcówek kabli).

Uwaga

Aby zapobiec pojawianiu sie dowolnie długich ciągów zer i jedynek w informacji kodowanej przy użyciu NRZ lub NRZI, stosowane jest wstępne przekodowanie ciągów bitów poprzez umieszczenie w nich **bitów nadmiarowych** (usuwanych później po stronie nadajnika), które przerywają nazbyt długie utrzymywanie stałego poziomu napięcia. Szczególnie popularnym rozwiązaniem w przypadku kodu NRZI (gdzie groźne są tylko długie ciągi jedynek) jest szpikowanie zerami (zero stuffing), polegające na zliczaniu w informacji jedynek modulo 5 i dodawaniu „sztucznego zera” po co piątej jedynce (uwaga: każde pojawienie się „prawdziwego zera” zeruje licznik jedynek).

Problem **synchronizacji** polega na umożliwieniu odbiornikowi stwierdzenia, kiedy sygnał użyteczny zaczyna się, a kiedy kończy (żeby był w stanie prawidłowo go zdekodować). Ze względu na sposób rozwiązania tego problemu transmisje dzielimy na **asynchroniczne** i **synchroniczne**.

W przypadku transmisji asynchronicznej, w stanie bezczynnym (brak przesyłu) łącze jest w stanie L.

Nadajnik rozpoczyna transmisję od **bitu startu** (jednego bitu H). Odbiornik wykrywa moment zmiany napięcia z L na H i pobiera próbki sygnału w chwilach 3/2 T, 5/2 T, 7/2 T ... określoną liczbę razy (przy założeniu, że okres T jest taki sam w nadajniku, jak i w odbiorniku). Nadajnik po zakończeniu nadawania pozostawia łącze w stanie L. W ten sposób mogą być przesyłane niezbyt długie ciągi bitów z niezbyt dużą częstotliwością (ale za to może być stosowany kod NRZ lub NRZI).

W przypadku transmisji synchronicznej przed wysłaniem właściwego kodu informacji wysyłana jest **preambuła**, zazwyczaj będąca ciągiem bitów 101010... o określonej długości, pozwalająca nie tylko wyznaczyć moment rozpoczęcia nadawania, ale i dokładnie zestroić fazy nadajnika i odbiornika. Ta metoda z założenia służy do przesyłania dłuższych ciągów bitów z dużą częstotliwością, więc i w trakcie

przekazywania informacji potrzebne jest sukcesywne korygowanie dostrojenia nadajnika i odbiornika.

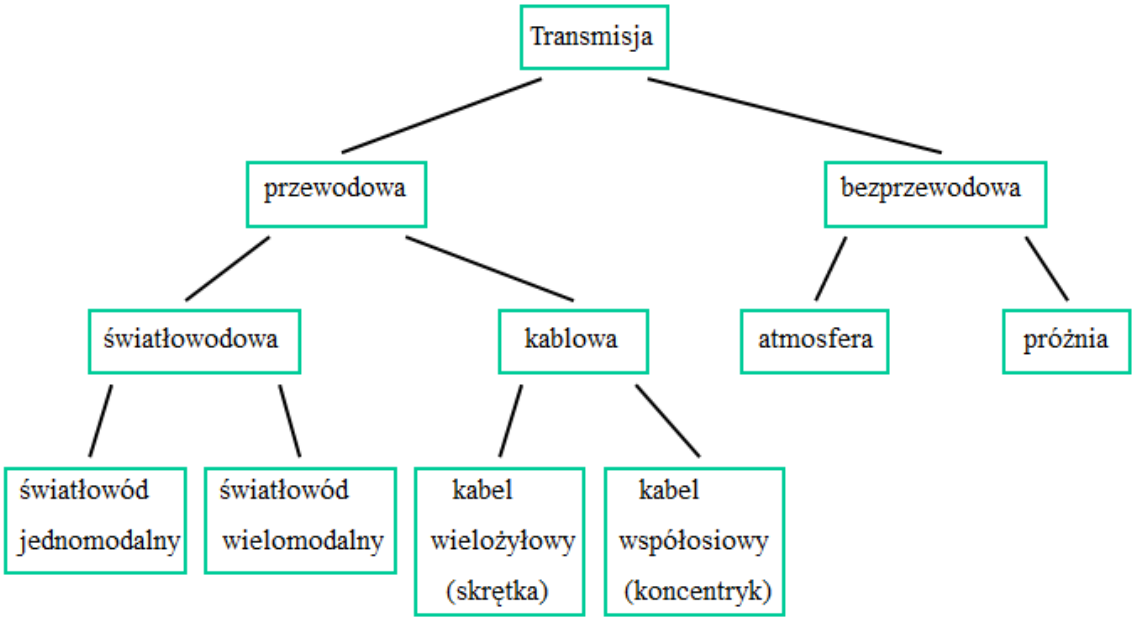
Może to być osiągane przez:
1) stosowanie kodów Manchester i Manchester różnicowy lub **kodów wielopoziomowych**, np. MLT-3 lub PAM-5 (kody samosynchronizujące);
2) stosowanie **kodowania nadmiarowego** (kodowania z bitami nadmiarowymi), żeby nie było zbyt długich okresów czasu bez zmiany napięcia;
3) przesyłanie dodatkowego **sygnału taktującego** przez dodatkowe, poprowadzone równolegle łącze (jest to drogie rozwiązanie).

Uwaga
1) Do oznaczenia początku i końca nadawanego ciągu bitów są czasem stosowane **symbole specjalne** (sygnały o kształcie nie odpowiadającym ani zeru, ani jedynce).
2) Inną metodą jest utrzymywanie łącza w stanie **ciągłej aktywności**, tj. nadawanie pewnych sygnałów przez cały czas, nawet jeśli nie ma w danej chwili żadnej informacji do przesłania.

Parametry eksploatacyjne sieci

Parametry eksploatacyjne należy rozpatrywać w odniesieniu do konkretnej warstwy w stosie protokołów (może to być warstwa fizyczna lub wyższa).
Opóźnienie wprowadzane przez sieć jest sumą czasu transmisji w łączu i czasów, jakie potrzebuje oprogramowanie po stronie nadawcy i po stronie odbiorcy, żeby przesłać jednostkę informacji stosowaną w danej warstwie (bit, ramkę, pakiet ...). W równoważny sposób może być zdefiniowane jako czas potrzebny do przesłania pustej informacji.
Szybkość przesyłania danych jest to liczba bitów użytecznej informacji, jaka może być przesłana przez pojedynczy kanał transmisyjny w ciągu jednej sekundy.
Do użytecznej informacji każda warstwa stosu protokołów dodaje pewną liczbę bitów służącą do zorganizowania łączności w danej warstwie. Ogólną liczbę bitów dodatkowych potrzebną do przesłania jednostki informacji w danej warstwie nazywamy **narzutem** (overhead). Narzut jest często wyrażany jako procent ogólnej liczby przesłanych bitów.

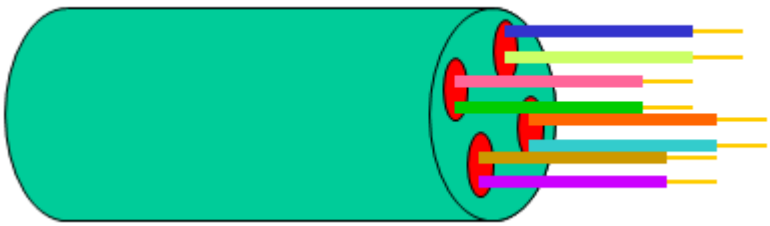
Rodzaje okablowania



Rodzaje Okablowania

1) Skrętka

Skrętka jest powszechnie stosowana w telefonii przewodowej. Pierwotnie byla to para izolowanych
przewodów, lekko skręconych i umieszczonych we wspólnej osłonie izolacyjnej. Obecnie zazwyczaj
są to cztery pary przewodów we wspólnej osłonie (zwiększenie pasma, możliwość przesyłania
sygnałów sterujących transmisją).



Skrętka jest najtańszym i najczęściej stosowanym rodzajem kabla w lokalnych sieciach komputerowych. Do podłączania najczęściej służą złączki RJ-45 (8-końcówkowe). W zależności od

jakości (która związana jest z możliwością przenoszenia sygnałów o określonych częstotliwościach)
wyróżniane są **kategorie** skrętki oznaczane symbolami liczbowymi - obecnie najbardziej rozpowszechniona jest skrętka Cat. 5.

Zalety skrętki:

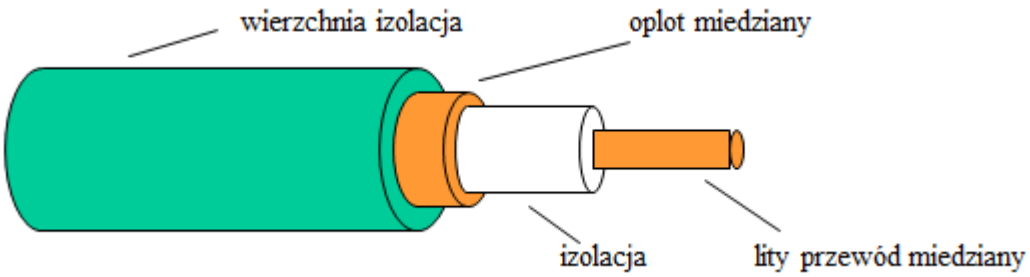
1. Szeroka stosowalność (oprogramowanie produkowane przez wiele firm uwzględnia skrętkę jako
   medium transmisyjne).
2. Niska cena.
3. Łatwość montażu (wymagana najmniejsza precyzja).
4. Możliwość pracy w trybie full-duplex.
5. Przy typowej (gwiaździstej) konfiguracji sieci odłączenie / dołączenie jednej stacji nie wpływa na
   pracę pozostałych stacji.
6. Dość duża szerokość pasma (ale do transmisji z dużymi częstotliwościami powinna być stosowana
   skrętka ekranowana, droższa od zwykłej skrętki).

Wady skrętki:

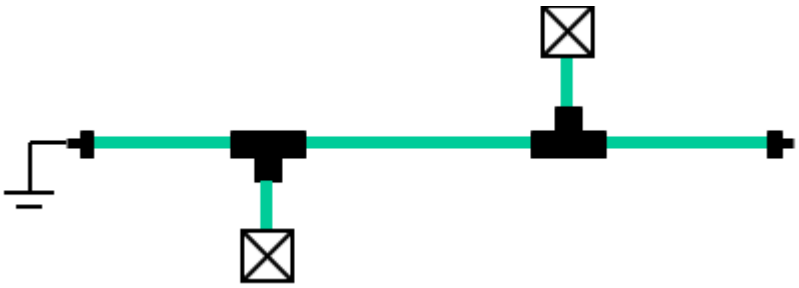
1. Dość duże straty energii w czasie transmisji (i tym samym możliwość zakłócania pracy innych
   urządzeń).
2. Nieduża maksymalna długość kabla.
3. Nieodporność na zakłócenia zewnętrzne (skrętka nieekranowana nie powinna być stosowana
   w środowiskach przemysłowych, np. w halach produkcyjnych).
4. Nieodporność na podsłuch (wystarczy analizować pole elektromagnetyczne wytwarzane przez
   kabel).

2) Kabel koncentryczny

Kabel koncentryczny jest tradycyjnie stosowany do przesyłania przebiegów o wysokiej częstotliwości
(aparatura elektroniczna, radiofonia i telewizja kablowa). Jest pojedynczym ekranowanym przewodem.
Oplot miedziany stanowi zaporę dla pola elektromagnetycznego.



Do podłączania koncentryka służą złączki BNC. Do jednego kabla może być podłączonych wiele
stacji końcowych (za pomocą trójników i kabli dystansowych). Na końcach głównego kabla zakładane
są terminatory, z których jeden powinien być uziemiony.



Zalety koncentryka:

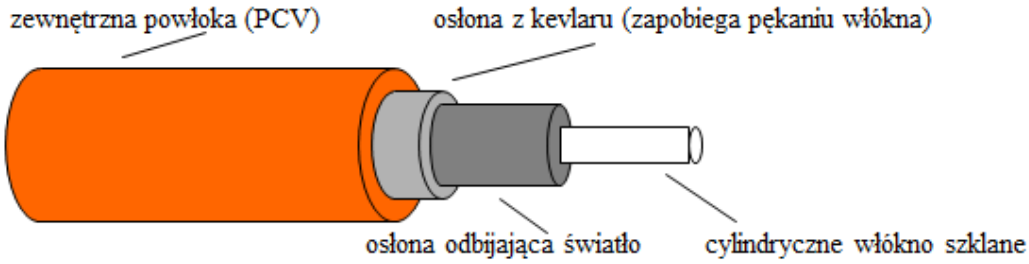
1. Odporność na zakłócenia zewnętrzne (może być stosowany w środowiskach przemysłowych).
2. Nie emituje zakłóceń.
3. Może przewodzić sygnały na dużo większą odległość, niż skrętka (rzędu kilometrów).
4. Do jednego kabla może być przypiętych wiele stacji końcowych.
5. Trudniejsze, niż w przypadku skrętki założenie podsłuchu (trzeba przebić oplot miedziany), łatwiejsze wykrycie podsłuchu.
6. Jest nieco droższy od skrętki, ale dużo tańszy od światłowodu (szczególnie uwzględniając koszty instalacji).

Wady koncentryka:

1. Jest coraz rzadziej stosowany i coraz mniej firm uwzględnia go w produkowanym oprogramowaniu.
2. Jeśli jest stosowany jako medium jednopasmowe, umożliwia pracę tylko w trybie half-duplex.
3. Podłączenie / odłączenie pojedynczej stacji powoduje przerwę w pracy całego fragmentu sieci.
4. Trudniej jest rozbudowywać sieć o nowe fragmenty (możliwość rozbudowy musi być z góry przewidziana w projekcie sieci).
5. Jest sztywniejszy od skrętki i trudniejszy w instalacji.

3) Kabel światłowodowy

Światłowód służy do przesyłania światła widzialnego (czyli przebiegu elektromagnetycznego o bardzo
dużej częstotliwości).



Ze względu na małą średnicę włókna szklanego, wejściowy promień światła powinien być możliwie
jednorodny i precyzyjnie skierowany do światłowodu. Pojedynczy światłowód zawsze służy tylko do
transmisji jednokierunkowej (simplex). Światłowody takie prowadzone są parami, aby umożliwić
łączność dwukierunkową (duplex). Obecnie światłowody wykorzystywane przez firmy telekomunika-
cyjne zawierają od kilku do kilkuset pojedynczych włókien szklanych

Światłowody dzielą się na dwie kategorie:

a) światłowody jednomodalne

(single mode) - mają średnicę włókna rzędu kilku mikrometrów,
muszą być zasilane światłem spójnym generowanym przez lasery. Wykazują bardzo małe tłumienie,
mogą przewodzić sygnały na odległość rzędu setek kilometrów. Są bardzo drogie, osprzęt do nich
i oprogramowanie również są bardzo drogie.

b) światłowody wielomodalne (multi mode)

- mają średnicę włókna rzędu kilkudziesięciu mikro-
metrów, mogą być zasilane za pomocą diod świecących LED. Sygnał w takich światłowodach ulega
silniejszemu tłumieniu, niż w światłowodach jednomodalnych, dlatego też służą one do transmisji na
odległość rzędu pojedynczych kilometrów.
Do odbioru sygnałów świetlnych służą różne rodzaje diod światłoczułych. Światłowody mają ogromne
pasmo przenoszenia (barierą są raczej własności elektryczne nadajnika i odbiornika). Do podłączania

światłowodu służą złączki SMA oraz FDDI. Zakładanie złączek na światłowód wymaga bardzo dużej
precyzji i środowiska bezpyłowego - jest wykonywane w warunkach laboratoryjnych, a światłowód
jest sprzedawany w gotowych odcinkach o zestandaryzowanych długościach.

Zalety światłowodu:

1. Całkowita odporność na zewnętrzne zakłócenia elektromagnetyczne i brak emisji takich zakłóceń.
2. Możliwość transmisji na duże i bardzo duże odległości.
3. Bardzo duża szerokość pasma (i maksymalna szybkość transmisji).
4. Praktyczna niemożliwość założenia podsłuchu.
5. Duże prawdopodobieństwo tego, że w przyszłości będzie stosowany w coraz szerszym zakresie
   (również w sieciach lokalnych).

Wady światłowodu:

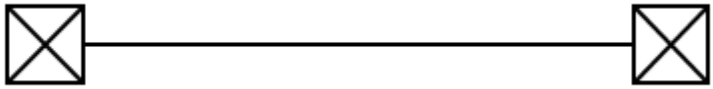
1. Wysoka cena samego światłowodu oraz towarzyszącego sprzętu i oprogramowania (ale wykazuje
   tendencję spadkową).
2. Skomplikowana i kosztowna instalacja.
3. Konieczność kupowania światłowodu w odcinkach o standardowych długościach.
4. Możliwość wykorzystania wyłącznie jako łącza od punktu do punktu (point to point).

Topologia fizyczna a topologia logiczna

Topologia jako gałąź matematyki zajmuje się własnościami zbiorów niezmienniczymi względem
homeomorfizmów (przekształceń różnowartościowych obustronnie ciągłych).
W przypadku sieci komputerowych termin **topologia fizyczna** jest rozumiany jako konfiguracja
połączeń poszczególnych elementów sieci (węzłów i łącz), przy czym nie bierzemy pod uwagę ich
kształtów ani rozmiarów (czyli rozważamy tylko sam **graf połączeń**).
Elementy występujące w sieci dzielimy na **aktywne** i **pasywne**. Elementy pasywne to takie, które
mogą wpływać jedynie na parametry sygnału (wzmacniać, korygować kształt), ale nie wpływają na
jego treść informacyjną (nie dodają, nie usuwają ani nie zmieniają bitów). Elementy aktywne to węzły
sieci i stacje końcowe.

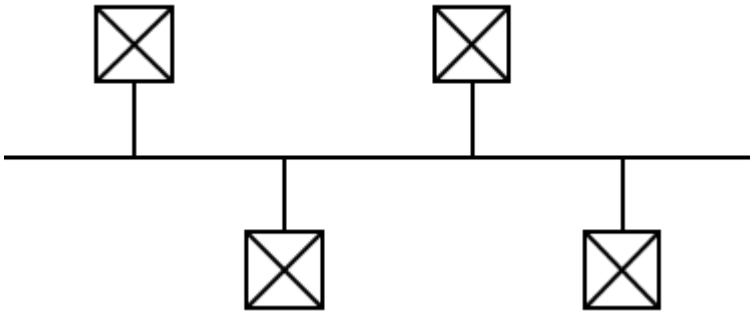
Poział łącz ze względu na ilość podłączeń:

a) dwupunktowe



(zazwyczaj służące do łączności na większą odległość), oraz

b) wielopunktowe



(typowe dla sieci lokalnych).

sW przypadku łącza wielopunktowego może się zdarzyć, że wiele stacji jednocześnie będzie chciało
wysyłać sygnały. Taką sytuację nazywamy **kolizją**, a obszar łącza, w którym mogą nakładać się na
siebie niezależnie wysyłane sygnały nazywamy **obszarem kolizji** lub **domeną kolizyjną**. Wykrywanie
kolizji i algorytm postępowania w przypadku wystąpienia kolizji muszą być uwzględnione w oprogra-
mowaniu przeznaczonym dla sieci opartej na łączu wielopunktowym.
Pojęcie **topologii logicznej** nie jest precyzyjnie zdefiniowane. Intuicyjnie jest rozumiane jako schemat
zorganizowania łączności w danej warstwie protokołów sieciowych. W szczególności w odniesieniu do
protokołów warstwy fizycznej obejmuje również rozwiązywanie kolizji.
Pojęcia topologii fizycznej i topologii logicznej są ze sobą częściowo powiązane. Poszczególne topo-
logie logiczne mogą być implementowane na niektórych topologiach fizycznych, a na niektórych nie.

Elementy pasywne sieci

Elementy pasywne funkcjonują w warstwie fizycznej sieci. Służą do przekazywania bitów i nie
mają wpływu na strukturę przekazywanej informacji.

1) Konwertery nośników (złączki, przejścia).

Służą do łączenia różnych rodzajów medium transmisyjnego (np. koncentryk - skrętka). Są stosowane,
gdy z jakiś powodów nie można wymienić od razu całego okablowania sieci. Nie powinny być
stosowane bez wyraźnej potrzeby, gdyż zawsze wprowadzają pewne tłumienie i zniekształcenie
sygnału.

2) Wzmacniaki

Są zwyczajnymi wzmacniaczami mocy sygnału nie wprowadzającymi żadnej korekty jego kształtu.
Umożliwiają pewne zwiększenie odległości, na jaką może być wysyłany sygnał, ale jednocześnie
wprowadzają pewne jego opóźnienie (a łączne opóźnienie sygnału nie może być dowolnie duże).

3) Regeneratory sygnału (repeater).

Pełnią rolę dwuportowych wzmacniaków, a ponadto korygują kształt sygnału („odszumiają"). Są więc
bardziej wskazane (choć droższe) od zwykłych wzmacniaków, szczególnie w środowiskach
wprowadzających zakłócenia.

4) Koncentratory (hub)

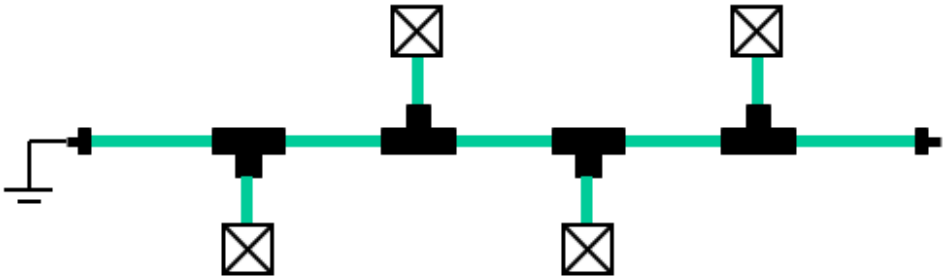
Służą do łączenia wielu kabli (prawie wyłącznie skrętki) schodzących sie w jednym miejscu. Zwykle
pełnią jednocześnie rolę wzmacniaków. Często mają jedno dodatkowe wyjście koncentryczne.
Zazwyczaj koncentratory mogą być łączone w większe zespoły, albo poprzez bezpośrednie osadzanie
jednego na drugim (koncentratory stosowe), albo poprzez specjalne porty (uplink) łączone skrętką ze
zwykłymi wejściami kolejnych koncentratorów.
Koncentratory zarządzane (droższe od zwykłych) umożliwiają (poprzez specjalny protokół) administratorowi sieci zdalne monitorowanie transmisji (bez potrzeby bezpośredniego sprawdzania
kontrolek na miejscu).

Najczęsciej spotykane topologie fizyczne i ich realizacje

Rozpatrujemy elementarne fragmenty sieci, w których poza stacjami końcowymi występują tylko
elementy bierne.

1) Magistrala

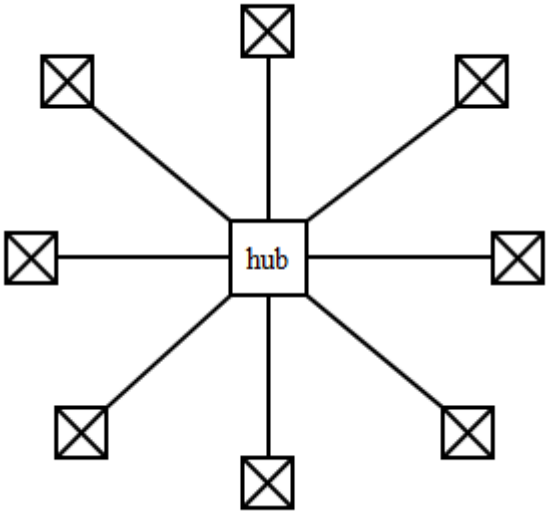
Jest typową konfiguracją dla kabla współosiowego.



Magistrala zazwyczaj jest dwukierunkowa, ale może też być jednokierunkowa. W przypadku topologii magistrali mogą występować kolizje sygnałów.

2) Gwiazda

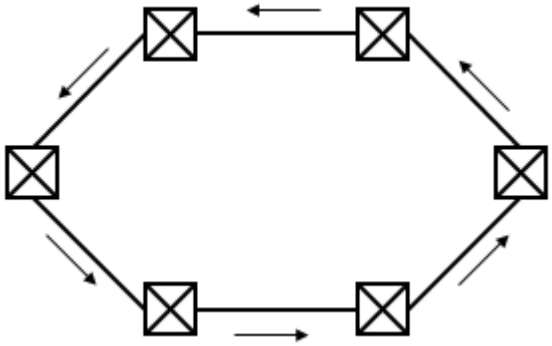
Jest typową konfiguracją dla skrętki.



Topologia gwiazdy wymaga dużej ilości kabla (ale taniego). Jeżeli stacje końcowe występują w kilku
rozrzuconych skupiskach, korzystne może być zmontowanie kilku gwiazd i połączenie ich centrów
(utworzenie tak zwanej gwiazdy uogólnionej). W przypadku topologii gwiazdy mogą występować
kolizje sygnałów.

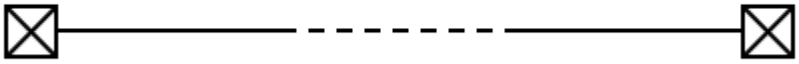
3) Pierścień

Jest typową konfiguracją dla światłowodu



Łącza pomiędzy stacjami są jednokierunkowe. Jeśli wymagana jest duża niezawodność, stosowany jest
podwójny pierścień, z drugim (rezerwowym) systemem łącz biegnących w przeciwnym kierunku.
Topologia pierścienia jest zwykle stosowana nie w sieciach lokalnych, lecz w sieciach spinających na
większym obszarze (np. sieciach miejskich). W przypadku topologii pierścienia nie występują kolizje
sygnałów.

W przypadku przesyłania sygnałów na bardzo duże odległości (w intersieciach spinających sieci
lokalne oraz miejskie) stosowane są praktycznie wyłącznie łącza dwupunktowe.



Łącza dwupunktowe można traktować jako szczególny przypadek zarówno magistrali, jak i gwiazdy.

5. WARSTWA ŁĄCZA

Zadaniem warstwy łącza jest zapewnienie transmisji informacji pomiędzy stacjami końcowymi oraz
węzłami podłączonymi do wspólnego medium transmisyjnego (tj. oddzielonymi co najwyżej elementami biernymi).
Informacja przekazywana jest w porcjach nazywanych **ramkami** (frame). Rozmiar ramki zależy od
implementacji konkretnego protokołu i zazwyczaj jest zmienny (np. dla protokołów Ethernet wynosi

od 64 bajtów do 1518 bajtów, nie wliczając preambuły i pola startu, obsługiwanych przez warstwę
fizyczną).
Obecnie praktycznie zawsze liczba bitów w ramce jest wielokrotnością 8. Tradycyjnie ósemka bitów
nazywana była **oktetem** (wywodzi się to z czasów, kiedy znaki alfanumeryczne były kodowane przy
użyciu ciągów krótszych, niż 8 bitów). Obecnie 1 oktet jest równy 1 bajtowi.

Protokoły warstwy łącza operują na **adresach fizycznych**, które w obrębie fragmentu sieci obsługiwanego przez dany protokół muszą być unikalne i mieć stałą długość. W najczęściej spotykanych realizacjach sieci lokalnych adresy fizyczne są kodowane na 2 lub 6 bajtach, przy czym
adresy 6-bajtowe zyskały w ostatnich latach znaczną przewagę (zapewniają one unikalność adresu
w skali całego świata).
Adresowanie fizyczne unikalne w skali całego świata jest administrowane przez IEEE, która przydziela numery kodowe poszczególnym producentom sprzętu sieciowego. Producenci przydzielają
unikalne numery seryjne swoim produktom. Każdy produkt (np. karta sieciowa) ma zapisany swój
kod producenta i numer seryjny w swojej pamięci stałej.

Struktura adresu fizycznego:

Szczególnymi przypadkami adresu są:
- adres mający wszystkie bity wyjedynkowane (szesnastkowo FF FF FF FF FF FF) - jest to tak zwany
adres rozgłoszeniowy (broadcast address) informujący, że ramka jest przeznaczona dla wszystkich
odbiorników w danym fragmencie sieci;
- adres mający wszystkie bity wyzerowane (szesnastkowo 00 00 00 00 00 00) - informujący, że ramka
nie zawiera danych, tylko jest **ramką organizacyjną** protokołu warstwy łącza.
Adresy fizyczne są też nazywane **adresami MAC** (Medium Access Control).
Ze względu na dużą liczbę różnorakich funkcji wykonywanych przez warstwę łącza, jest ona podzielona
na dwie podwarstwy:
- podwarstwę dostępu do nośnika (Medium Access Control sublayer) - MAC ;
- podwarstwę dostępu do łącza logicznego (Logical Link Control sublayer) - LLC .

Usługi świadczone przez podwarstwę LLC na rzecz protokołów wyższych warstw są poklasyfikowane
następująco:
Typ 1 - usługi bezpołączeniowe bez potwierdzeń
Typ 2 - usługi bezpołączeniowe z potwierdzeniami
Typ 3 - usługi połączeniowe
Poszczególnym usługom LLC odpowiadają obiekty logiczne nazywane **punktami udostępniania**
usług (**Service Access Point**). Determinują one adresy udostępniania usług po stronie nadawcy
(Source SAP) i po stronie odbiorcy (**Destination SAP).** Adresy te są zazwyczaj jedno- lub dwubajtowe,
a dwa pierwsze bity oraz adresy całe wyzerowane / wyjedynkowane są interpretowane analogicznie,
jak w przypadku adresów fizycznych.
Protokół wyższego poziomu przekazuje zatem podwarstwie LLC:
- blok danych do przesłania ;
- pełny adres źródłowy (fizyczny adres nadawcy + S-SAP) ;
- pełny adres docelowy (fizyczny adres odbiorcy + D-SAP) ;
- rodzaj żądanej usługi.

Podwarstwa LLC tworzy **ramkę LLC** (ramkę logiczną) o następującej strukturze:

D-SAP	S-SAP	Pole sterujące	Dane do przesłania
1 lub 2 bajty	1 lub 2 bajty	1 bajt	

Podwarstwa MAC dodaje do niej na początku **nagłówek** (zawierający między innymi adresy fizyczne -
źródłowy i docelowy), a na końcu **pole kontrolne**, pozwalające z dużym prawdopodobieństwem
stwierdzić, czy warstwa fizyczna przesłała utworzoną w ten sposób **ramkę MAC** (ramkę fizyczną)
bezbłędnie.

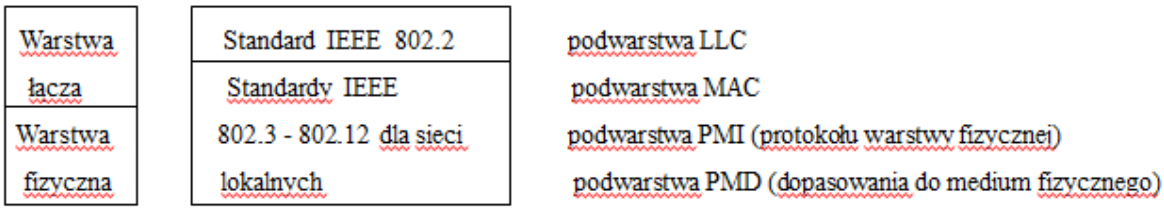
Zadaniami podwarstwy LLC są:

- organizowanie łączności na poziomie logicznym (np. przez tworzenie ramek organizacyjnych) ;
- reagowanie na błędy popełnione w warstwie fizycznej (które są wykrywane i zgłaszane, ale nie
  obsługiwane w podwarstwie MAC) ;
- ewentualne buforowanie ramek (po stronie nadawcy i odbiorcy), aby dostosować prędkość
  transmisji do możliwości łącza fizycznego.

Podwarstwa LLC zazwyczaj posiada oddzielną specyfikację, mogącą współpracować z różnymi
specyfikacjami podwarstw MAC. Specyfikacja MAC jest zależna od warstwy fizycznej, z którą współpracuje, dlatego też w praktyce standardy techniczne sieci są opracowywane łącznie dla warstwy
fizycznej i współpracującej z nią podwarstwy MAC.

Normy (standardy) IEEE dla sieci lokalnych:

ISO



Poniżej zostaną omówione typowe przykłady (najczęściej realizowane standardy IEEE) specyfikacji
warstwy fizycznej w połączeniu z podwarstwą MAC.

Przykład
Standard IEEE 802.3 (typowa realizacja - Ethernet 10 Mb/s)
Medium fizyczne - kabel koncentryczny lub skrętka.
Topologia fizyczna - odpowiednio magistrala lub gwiazda.
Maksymalna odległość pomiędzy urządzeniami przyłączonymi do jednego segmentu sieci (czyli
maksymalna długość odcinka kabla) - 500 m dla koncentryka, 100 m dla skrętki.
Maksymalna liczba regeneratorów dla kabla koncentrycznego - 4 (czyli maksymalna liczba segmentów -
5, a maksymalna odległość pomiędzy urządzeniami w sieci (tzw. średnica sieci) - 2500 m).
Maksymalna liczba koncentratorów - 4 (czyli dla skrętki średnica sieci nie przekracza 500 m).
Maksymalna liczba stacji przyłączonych do jednego segmentu sieci - 1024 (dla skrętki).
Typowe parametry transmisji - 10 Mb/s, w paśmie podstawowym.
Kodowanie bitów - Manchester.
Dostęp do łącza - rywalizacyjny (dopuszcza kolizje sygnałów).
Algorytm rozwiązywania kolizji - CSMA/CD **(Carrier Sense Multiple Access with Collision Detection).**

Opis algorytmu CSMA/CD.

Założenie: każda stacja prowadzi ciągły nasłuch stanu łącza i ma możliwość porównywania sygnału
w łączu z sygnałem emitowanym przez siebie. W związku z tym każda stacja ma możliwość stwierdzenia, czy sama bierze udział w kolizji. Aby powiadomić inne stacje, że sygnał w łączu jest
wynikiem kolizji, stacja taka generuje specjalny **sygnał zakłócający,** po odebraniu którego wszystkie
stacje mają obowiązek uciszyć się na pewien określony czas.
Należy brać pod uwagę, że w łączu obowiązuje zasada **względności czasu,** gdyż prędkość rozchodzenia
się sygnału jest skończona, a czas transmisji jednego bitu jest dużo krótszy, niż maksymalny czas
przepływu sygnału pomiędzy (najbardziej oddalonymi od siebie) stacjami. Z tego powodu projekt
techniczny sieci musi jednocześnie uwzględniać takie czynniki, jak dopuszczalne długości (i rodzaje)
kabla, dopuszczalne pasmo transmisji, dopuszczalne wielkości ramek i zaprogramowane czasy
oczekiwania pomiędzy transmisjami.

W naszym przykładzie:
- częstotliwość 10 Mb/s (więc czas nadawania jednego bitu wynosi 0.1 ms);
- najmniejsza długość ramki 64 bajty = 512 bitów, zatem szerokość **szczeliny czasowej** wynosi
$512 \cdot 0.1\ ms = 51.2\ ms$;
- czas trwania sygnału zakłócającego $tz = 3.2\ ms$;
- aby można było reagować na sytuację powstania kolizji, musi być spełniona następująca zależność

$$szczelina > 2 \cdot tmax + tz$$

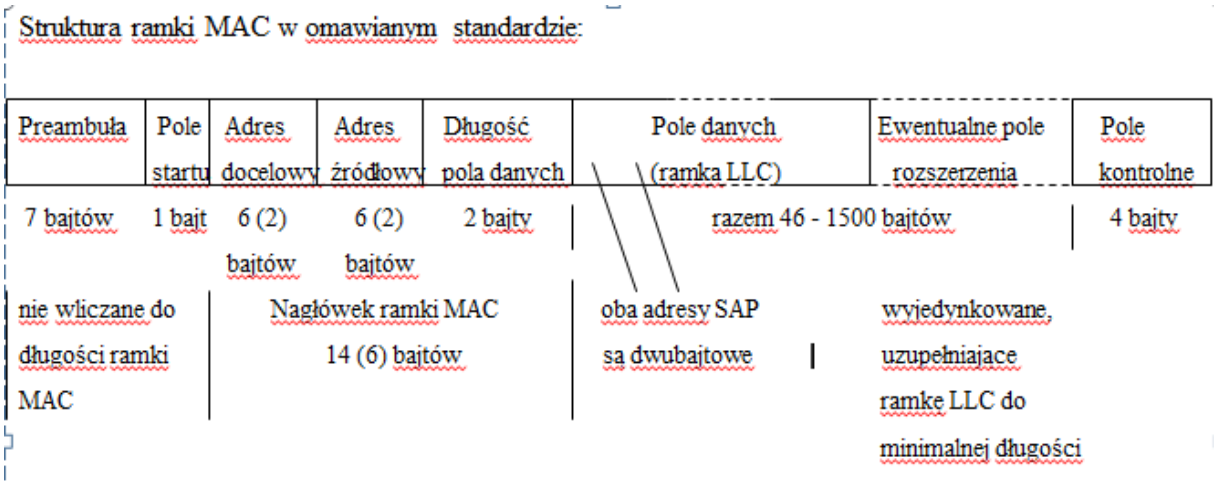
co limituje geometryczny rozmiar (średnicę) sieci dla ustalonego nośnika fizycznego.
Uwaga: maksymalny czas propagacji przez sieć tmax jest równy ilorazowi średnicy sieci przez
prędkość rozchodzenia się sygnału w nośniku fizycznym, z którego wykonana jest sieć,
powiększonemu o opóźnienia wprowadzane przez elementy bierne sieci.

Zasady postępowania dla indywidualnych stacji:

a) Jeśli uprzednio stacja nie brała udziału w kolizji, może rozpocząć nadawanie ramki po okresie ciszy
w łączu trwającym co najmniej 9.6 ms.
b) Jeśli została wykryta kolizja, następna próba retransmisji ramki przez każdą ze stacji biorących
udział w kolizji następuje (po stwierdzeniu, że łącze jest wolne) w wylosowanej spośród dwóch
kolejnych szczelin czasowych (prawdopodobieństwo wylosowania każdej ze szczelin wynosi 0.5,
każda ze stacji ma inny „zarodek” generatora losowego, aby uniknąć powtarzania się kolizji).
c) W przypadku ponownej kolizji następuje (po odczekaniu) losowanie jednej spośród czterech

kolejnych szczelin czasowych, jeśli to nie da rezultatu, jednej spośród ośmiu, szesnastu itd., aż do
osiągnięcia szerokości przedziału czasowego 1024 szczeliny. Jeśli dalej występują kolizje, losowanie
jest powtarzane jeszcze sześciokrotnie dla takiej samej szerokości przedziału czasowego. Jeśli
szesnasta próba transmisji nie powiedzie się, warstwa łącza zaprzestaje dalszych prób i przesyła
do wyższej warstwy stosu protokołów **sygnał niesprawności łącza**.
Uwaga: ze wzrostem wykorzystania przepustowości sieci średnia liczba kolizji w jednostce czasu rośnie.
Badania statystyczne wykazują, że pożądane jest utrzymywanie średniego wykorzystania sieci
w granicach około 50% (jeśli to niemożliwe, należy podzielić sieć na segmenty lub zmienić standard).

Struktura ramki MAC w omawianym standardzie:



Uwaga: ponieważ istnieje ograniczenie od dołu długości ramki (związane z wyżej omówionym
algorytmem rozwiązywania kolizji), w przypadku, gdy ramka LLC jest za krótka, jest automatycznie
uzupełniana do pełnej długości przez opcjonalne pole rozszerzające.
Pole kontrolne zabezpiecza przed pojedynczymi (i niektórymi wielokrotnymi) przekłamaniami bitów
w ramce MAC (nie wliczając do niej preambuły i pola startu) stosując **cykliczną kontrolę nadmiarową CRC (Cyclic Redundancy Check).**

Ogólna idea kodowania nadmiarowego.

Na *m* bitach można zapisać 2 różnych ciągów zero-jedynkowych. Jeśli dodatkowo przydzielimy
r bitów nadmiarowych, to moglibyśmy zapisać 2 różnych ciągów. Ponieważ chcemy zakodować

tylko 2 różnych ciągów, możemy w zależności od pierwszych *m* bitów tak dobrać wartości pozostałych
r bitów, aby otrzymane kodowanie miało jakieś szczególne własności.
Przykładowo, jeśli *r* = 1, nadmiarowy bit może być tzw. bitem parzystości (bitem o tak dobranej
wartości, aby liczba jedynek w ciągu kodowym zawsze była parzysta), umożliwiającym wykrywanie
pojedynczych błędów.
W naszym przypadku *r* = 32 (4 bajty), więc można stosować bardziej złożoną kontrolę, umożliwiającą
wykrywanie również niektórych rodzajów błędów wielokrotnych (a w szczególności błędów seryjnych,
będących najczęściej występującym w praktyce rodzajem błędów wielokrotnych).

Sposób kodowania i dekodowania.
Ciąg kodowany (zawartość ramki) jest traktowany jako ciąg współczynników pewnego wielomianu
binarnego (stopnia *m* - 1). Wielomian ten jest dzielony binarnie przez pewien **wielomian generacyjny**
stopnia *r*. Współczynniki reszty z tego dzielenia (ciąg *r*-elementowy) są traktowane jako **ciąg kontrolny**
w tym sensie, że podzielenie łącznego ciągu (ciągu kodowanego i dołączonego do niego ciągu
kontrolnego, razem *m* + *r* elementów) przez ten sam wielomian generacyjny powinno dać resztę 0.
W zależności od doboru współczynników wielomianu generacyjnego uzyskujemy różne możliwości
wykrywania błędów. W omawianym standardzie stosowany jest następujący wielomian generacyjny:

$$G^{32}(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$ (tzw. CRC-32)

Zastosowanie powyższego wielomianu pozwala na wykrywanie:
- wszystkich błędów pojedynczych i podwójnych;
- wszystkich błędów polegających na przekłamaniu nieparzystej liczby bitów;
- wszystkich błędów seryjnych o długości serii nie przekraczającej 32.

Ponadto prawdopodobieństwo niewykrycia dłuższych serii przekłamań jest bardzo małe.

Uwagi:
1) W praktyce test poprawności polegający na sprawdzeniu, czy reszta z dzielenia jest równa zero, nie
jest zbyt dobry, bo prawdopodobieństwo błędnego uzyskania ciągu wyzerowanego jest większe, niż
jakiegokolwiek innego ciągu (wynika to ze specyfiki konstrukcji układów elektronicznych).
W związku z tym ciąg kontrolny jest dodatkowo modyfikowany tak, aby w przypadku braku błędów
reszta z dzielenia nie była równa zeru, lecz pewnej ustalonej liczbie niezerowej (w omawianym
standardzie jest to 11000111 00000100 11011101 01111011).
2) Wszystkie wyżej opisane obliczenia (związane z kodowaniem i dekodowaniem ciągów bitów) są

wykonywane jako równoległe operacje na bitach przez wyspecjalizowane układy scalone umieszczo-
ne na kartach sieciowych, więc wykonywane są szybko i nie absorbują czasu procesora centralnego.

Uwaga:
W sieci Ethernet (i każdej innej dopuszczającej kolizje) każda wysyłana ramka dociera do wszystkich
stacji w danym segmencie sieci - każda stacja dopiero po przeczytaniu części adresowej ramki
decyduje, czy ramkę zignorować, czy też czytać dalej. W związku z tym w obrębie danego segmentu
sieci każda stacja ma możliwość podsłuchiwania każdej transmisji, niezależnie od tego, czy ramki są
adresowane do niej, czy też do innej stacji.
**Chcąc uniknąć podsłuchu w obrębie sieci lokalnej, należy stosować szyfrowanie w wyższych
warstwach stosu protokołów !**

Protokoły warstwy łącza oparte na przekazywaniu uprawnień

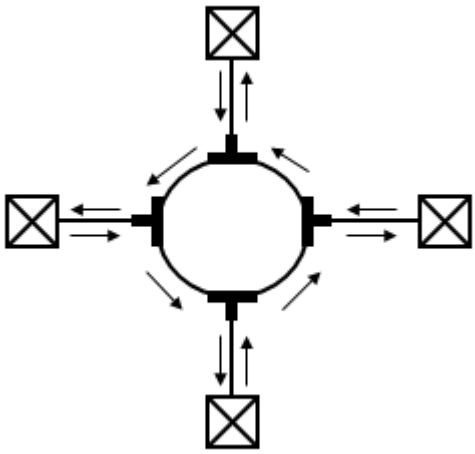
Protokoły oparte ***na przekazywaniu uprawnień*** (żetonu, przepustki) (token passing) nie dopuszczają
do kolizji ramek poprzez ustalenie kolejności, w jakiej poszczególne stacje mają prawo nadawać
ramki. W ogólności kolejność nie musi być zależna od fizycznej konfiguracji sieci. Nie wszystkie
stacje muszą też być traktowane jednakowo - algorytm może uwzględniać system priorytetów, tj.
niektóre stacje mogą uzyskiwać prawo głosu częściej, a inne rzadziej.
Teoretycznie byłoby możliwe rozwiązanie, w którym poszczególne stacje dowiadywałyby się, kiedy
przychodzi ich kolej nadawania, poprzez zliczanie ramek nadawanych przez inne stacje. Takie
rozwiązanie byłoby jednak niedogodne, gdyż:
- nie wszystkie stacje muszą mieć co nadawać, kiedy przychodzi ich kolej (musiałyby nadawać ramki
bez treści informacyjnej);
- nie wszystkie stacje muszą być jednocześnie włączone;
- co jakiś czas liczba stacji w sieci może się zmieniać.

Za lepsze rozwiązanie uznane zostało stworzenie ramki organizacyjnej zwanej **żetonem** (tokenem),
której część adresowa jest zmieniana przez każdą kolejną otrzymującą ją stację, która wpisuje do niej
adres swojego następnika. Stacja, która otrzymała żeton, uzyskuje prawo nadawania informacji.
Przykład
Standard IEEE 802.4 (protokół z przekazywaniem uprawnień dla fizycznej topologii magistrali).

Pomijamy parametry fizyczne medium oraz transmisji (są podane w [Nowicki, Woźniak]).
Format ramki informacyjnej oraz pole CRC - podobne, jak w przypadku standardu IEEE 802.3,
ale pole danych może mieć rozmiar 0 - 8182 bajty.
Zasady transmisji - zdecentralizowany algorytm z przekazywaniem uprawnień (tj. bez wyróżnionej
stacji nadrzędnej, sprawującej kontrolę nad całością transmisji).
Rodzaje ramek organizacyjnych:
- żeton;
- żądanie żetonu;
- ustalenie następcy;
- rozwiązanie rywalizacji;
- ubieganie się o dołączenie;
- kto następny.

W trakcie normalnej pracy jedyną wykorzystywaną ramką organizacyjną jest żeton (pozostałe są
stosowane w sytuacjach nietypowych lub awaryjnych: dołączenie / odłączenie stacji, zgubienie żetonu,
awaria łącza itd.). W sytuacjach nietypowych (nieustabilizowanych) może wystąpić kolizja, która
rozstrzygana jest na podobnej zasadzie, jak w CSMA/CD.
W sytuacji normalnej pracy wszystkie stacje prowadzą ciągły nasłuch. Stacja, która otrzymała żeton,
może wyemitować dowolną liczbę ramek do dowolnych innych stacji (a na końcu żeton do swojego
następnika), ale w granicach określonego limitu czasu i o dozwolonym priorytecie.
Ramki mogą mieć nadane priorytety: 0 (najniższy), 2, 4 lub 6 (najwyższy). Stacje są zobowiązane
mierzyć czas pomiędzy kolejnymi pojawieniami się żetonu u nich. Czas ostatniego zmierzonego
obiegu determinuje minimalny priorytet ramek, jakie wolno wysyłać (przy większym czasie obiegu,
czyli zagęszczonym ruchu w sieci, wolno wysyłać tylko ramki o większym priorytecie).
Uwaga
Ramki organizacyjne są pozapriorytetowe (ich emisja podlega innym algorytmom).

Przykład
Standard IEEE 802.5 (protokół z przekazywaniem uprawnień dla fizycznej topologii pierścieniowej).
Struktura fizyczna - ciąg łącz jednokierunkowych (dowolnego rodzaju) typu punkt - punkt, połączonych sprzęgami magistralowymi w pierścień. Do każdego sprzęgu stacja jest dołączona
dwukierunkowym kablem dystansowym. Sprzęgi mają zwory, pozwalające na natychmiastowe
zwieranie łącza w przypadku awarii stacji.



Długości kabli dystansowych mogą znacznie przewyższać rozmiary geometryczne pierścienia,
który ze względów diagnostycznych dogodnie jest
przechowywać w jednym pomieszczeniu.
Jeżeli chcemy mieć duży pierścień (na przykład

w sieci miejskiej), możemy stosować regeneratory

wstawiane w miejsce sprzęgów magistralowych.
Maksymalna liczba łącz w pierścieniu - 250.

Format żetonu:

pole początku	pole sterowania dostępem	pole końca
1 bajt	1 bajt	1 bajt

Jeden z bitów w polu sterowania dostępem jest **bitem stanu** - w żetonie jest wyzerowany (co oznacza
„żeton wolny"). Jeżeli stacja chce nadawać, to po otrzymaniu żetonu (po przeczytaniu pierwszych
dwóch bajtów już wie, że jest to wolny żeton) ustawia w nim bit stanu na 1 i „na bieżąco" tworzy
z niego ramkę informacyjną o strukturze:

pole początku	pole sterowania dostępem	pole typu	adres docelowy	adres źródłowy	dane (LLC)	CRC	pole końca	pole statusu
1 bajt	1 bajt	1 bajt	6 (2) bajtów	6 (2) bajtów	dowolne (limitowane czasem nadawania)	4 bajty	1 bajt	1 bajt

Zasady transmisji - zcentralizowany algorytm z przekazywaniem uprawnień.

W normalnych (stabilnych) warunkach centralizacja algorytmu w niczym się nie przejawia - żeton
krąży wzdłuż pierścienia retransmitowany przez kolejne sprzęgi stacji (dysponujące co najmniej
1-bitowym buforem) w takiej kolejności, w jakiej fizycznie są włączone do pierścienia. Jeżeli stacja
chce nadawać, przechwytuje żeton i „na bieżąco" robi z niego ramkę (lub cały ciąg ramek, mogący
zawierać zarówno ramki informacyjne, jak i organizacyjne). Ramka obiega cały pierścień i wraca do

nadawcy - na nim ciąży obowiązek usunięcia jej z obiegu. Adresat ramki jedynie zaznacza ją jako
„odczytaną” w polu statusu - nadawca w ten sposób dowiaduje się, że nie ma potrzeby retransmisji tej
ramki.
Stacja, przez której sprzęg przechodzi ramka z wyjedynkowanym bitem stanu, czyta jej adres
docelowy i porównuje z własnym - jeśli ramka jest adresowana do innej stacji, przepuszczają ją dalej,
jeśli do niej, kopiuje ją do swojego bufora, jednocześnie zaznaczając jako „odczytaną”. Gdy ramka
wróci do nadawcy (lub cały ciąg ramek, z których ostatnia jest zaznaczona), nadawca nie przepuszcza
jej dalej, tylko wpuszcza do pierścienia wolny żeton.

Możliwa jest sytuacja, w której „ramka jest dłuższa, niż pierścień”, czyli pierwsze bity ramki wracają
do nadawcy jeszcze przed nadaniem ostatnich bitów. Aby nadawca mógł wypuścić wolny żeton,
zazwyczaj musi zachodzić koniunkcja dwóch warunków:
1) czoło ramki dotarło już z powrotem do nadawcy;
2) nadawanie ramki (ciągu ramek) już się zakończyło.
Możliwe też są inne rozwiązania:
1) żeton jest wypuszczany dopiero po powrocie do nadawcy całej ramki (wtedy mamy gwarancję, że
w każdej chwili w pierścieniu jest dokładnie jedna ramka);
2) żeton jest wypuszczany zaraz po zakończeniu nadawania ramki (ciągu ramek) (early token release) -
wtedy w pierścieniu mogą przebywać ramki informacyjne i żeton jednocześnie.
Druga metoda powoduje większą komplikację algorytmów, ale w przypadku dużych pierścieni
i dość krótkich ramek poprawia wydajność działania sieci.

Norma IEEE 802.5 dopuszcza wprowadzenie pojęcia priorytetu ramki - implementacja polega na
zaznaczaniu przez stacje odpowiednich bitów w nagłówku przekazywanej ramki, co odpowiada
podnoszeniu priorytetu. Do wolnego żetonu o podwyższonym priorytecie można dowiązywać tylko
wiadomości o nie mniejszym priorytecie. Obowiązek obniżenia priorytetu ma ta stacja, która go
uprzednio podwyższyła, zatem wszystkie stacje muszą przechowywać na stosach informacje o swoich
podwyższeniach priorytetu żetonu.
Zcentralizowanie algorytmu transmisji przejawia się w tym, że w każdej chwili jedna ze stacji w pierścieniu (dowolna z nich) pełni rolę nadzorcy. Do obowiązków nadzorcy należy:
- kontrola obecności żetonu w pierścieniu (po upływie limitu czasu generuje nowy);
- wykrywanie i usuwanie uszkodzonych i „bezpańskich” ramek (nie usuniętych przez nadawcę np.
wskutek jego awarii);
- wydłużanie czasu obiegu żetonu (jeżeli żeton jest „dłuższy niż pierścień”).
Jeśli aktualny nadzorca przestaje pełnić swoją funkcję (wskutek wyłączenia lub awarii), jego następca

jest natychmiast wyłaniany w drodze rywalizacji pomiędzy pozostałymi czynnymi stacjami.

Tryby przekazywania ramek przez urządzenia aktywne w sieci

Ramki przekazywane przez dowolne urządzenie aktywne w sieci mogą być przekazywane „na bieżąco”,
czyli zaraz po przeczytaniu adresu docelowego - jest to **tryb skróconej analizy adresu** (Cut - Through),
lub też mogą być buforowane w całości i dopiero wtedy przekazywane dalej - jest to **tryb komutacji**
ramek (Store-and-Forward). Oba tryby mają swoje zalety i wady.
Zaletą trybu skróconej analizy adresu jest duża szybkość działania, gdy przypadki uszkodzenia ramek
lub kolizji są rzadkie. Zaletą trybu komutacji ramek jest nietransmitowanie ramek, które są uszkodzone
lub brały udział w kolizji (dowiadujemy się o tym dopiero czytając końcowe pola ramek).

Sprzęt sieciowy działający na poziomie warstwy łącza

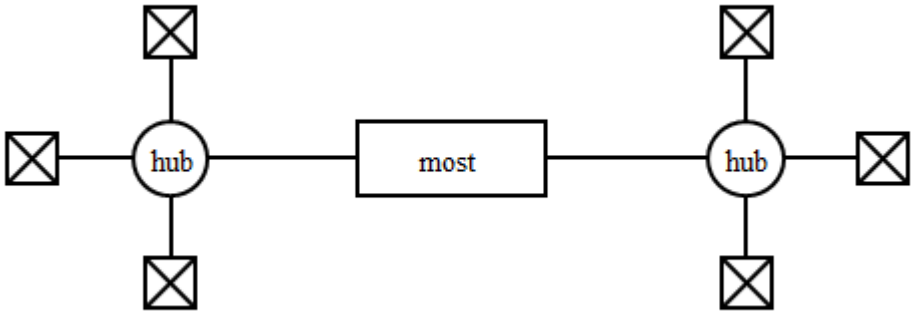
Elementy aktywne sieci działające na poziomie warstwy łącza zajmują się selekcją i kierowaniem całych
ramek do odpowiednich podsieci na podstawie analizy ich adresów docelowych. Mogą zatem służyć do
oddzielania od siebie poszczególnych **domen kolizyjnych** w obrębie jednej **domeny rozgłoszeniowej**
(domena rozgłoszeniowa dysponuje jednym protokołem warstwy łącza i wspólnym systemem
adresowania MAC, zatem wszystkie ramki z adresem rozgłoszeniowym są rozsyłane w obrębie całej
domeny rozgłoszeniowej).
Spotyka się też **elementy tłumaczące** w warstwie łącza, których zadaniem jest przesyłanie ramek LLC
pomiędzy fragmentami sieci dysponującymi różnymi (ale współpracującymi z tym samym protokołem
LLC) protokołami podwarstwy MAC - takie elementy mogą zmieniać pola ramki dodawane przez
podwarstwę MAC i obliczać nowe wartości pól CRC.

1) Mosty (bridge).

Mosty są dwuportowymi, dwukierunkowymi urządzeniami, które mogą odebrać ramkę na jednym
z portów i, jeżeli zechcą, transmitować ją na drugim (przy okazji pełnią też rolę regeneratorów
i poprawiają kształt sygnału). Mosty retransmitują wszystkie ramki typu broadcast (tj. z adresem
rozgłoszeniowym) i wszystkie ramki, co do których nie są pewne, że ich adresat znajduje się po tej

samej stronie mostu, z której przyszedł sygnał. Mosty są urządzeniami uczącymi się, które w swojej
wewnętrznej pamięci przechowują tablice adresów MAC, których położenie już poznały (z adresów
źródłowych ramek przychodzących).

Przykład



Domena rozgłoszeniowa składa się z dwóch oddzielnych domen kolizyjnych.

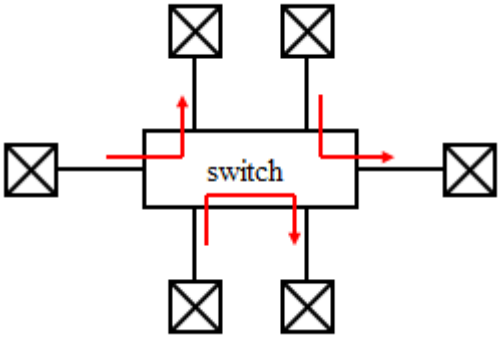
Zadaniem mostu jest zmniejszenie ruchu w sieci poprzez jego rozdzielenie na ruch lokalny w obrębie
każdej z domen kolizyjnych i ruch pomiędzy domenami kolizyjnymi. Rozdział stacji / węzłów na dwie lub
więcej domeny kolizyjne powinien nastąpić na podstawie oszacowań, kto z kim w sieci będzie najczęściej
współpracował (przykładowo mogą istnieć dwie oddzielne grupy użytkowników korzystające z oddzielnych serwerów, a między sobą komunikujące się tylko przy użyciu poczty elektronicznej).
Uzyskujemy w ten sposób znaczne zmniejszenie ogólnej liczby kolizji ramek, przy niewielkim tylko
opóźnieniu ramek przechodzących przez most. Z badań statystycznych wynika, że korzystną jest sytuacja,
kiedy około 80% ramek rozsyłanych jest w ruchu lokalnym, a tylko około 20% przechodzi przez most.

Uwaga

W sieci lokalnej może być zainstalowany cały system mostów, który niekoniecznie organizuje sieć
w postaci grafu acyklicznego. W szczególności, jeżeli jakieś połączenie jest uznane za ważne, most
może być zdublowany na wypadek awarii. W takiej sytuacji mosty muszą „mieć świadomość” struktury
całej sieci lokalnej, aby nie dochodziło do zjawiska zapętlania ramek (nieskończonego retransmitowania
ich przez mosty wzdłuż jakiegoś cyklu). Do rozpoznawania struktury sieci mosty stosują grafowy
algorytm **drzewa rozpinającego** (**spanning tree**) - okresowo rozsyłają do siebie ramki organizacyjne
BPDU (Bridge Protocol Data Unit), przy użyciu których najpierw ustalają (rywalizacyjnie) korzeń
drzewa, a następnie sukcesywnie dołączają pozostałe mosty jako węzły drzewa.

2) Przełączniki (switch).

Przełącznik może być traktowany jako wieloportowe uogólnienie mostu, tj. urządzenie mogące
separować od siebie pewną liczbę domen kolizyjnych, a jednocześnie w razie potrzeby mogące
przepuszczać ramki z każdej do każdej. Ramki typu broadcast są przepuszczane przez przełącznik we
wszystkich kierunkach. Jednym z możliwych zastosowań jest użycie przełącznika jako koncentratora
przełączającego:



W takiej sytuacji komutowane są całe ramki, dzięki czemu pomimo gwiaździstej konfiguracji nie

występują kolizje (odbywa się to jednak kosztem pewnego spowolnienia przesyłu pojedynczych ramek).
W przypadku chwilowych zagęszczeń ruchu ramki muszą być buforowane w poszczególnych portach,
przełącznik musi więc dysponować pojemną pamięcią (również do przechowywania tablic adresów).
W miarę obniżania cen przełączników powyższe rozwiązanie staje się coraz bardziej popularne.

Przegląd innych standardów sieci fizycznych i protokołów warstwy łącza

Ogólna klasyfikacja:
LAN (Local Area Network) - **sieć lokalna** (mieszcząca się w obrębie jednego budynku lub instytucji,
długości kabli co najwyżej rzędu pojedynczych kilometrów)
MAN (Metropolitan Area Network) - **sieć miejska** (szkieletowa, spinająca wiele sieci lokalnych,
długości kabli co najwyżej rzędu dziesiątek kilometrów)
WAN (Wide Area Network) - **sieć rozległa** (połączenia dwupunktowe, międzymiastowe lub międzynarodowe, długości łącz nieograniczone)

1) Ethernet 100 Mb/s (Fast Ethernet)

Standard dla sieci lokalnych podobny do Ethernetu 10 Mb/s, przewiduje użycie skrętki Cat. 5 i przełączników, stosowane kodowanie bitów MLT-3 zamiast Manchester.
Obecnie produkowane karty sieciowe Ethernet zazwyczaj są w stanie automatycznie rozpoznawać
i obsługiwać zarówno standard 10 Mb/s, jak i 100 Mb/s, a nawet 1000Mb/s.

2) Ethernet 1 Gb/s (Gigabit Ethernet)

Dalsze rozwinięcie technologii Ethernet, przewidziane głównie dla łącz światłowodowych (dopuszcza
też krótkie odcinki skrętki Cat.5). Stosowany jest najczęściej do komunikacji pomiędzy wyspecjalizo-
wanym przełącznikiem spinającym kable od stacji roboczych pracujących w standardzie Ethernet 100
Mb/s, a szybkim serwerem (lub zespołem serwerów) umieszczonym w innej części budynku. Jest
(jak na razie) częściej stosowany w sieciach MAN, niż LAN. Kodowanie bitów – PAM-5.

3) Ethernet 10 Gb/s (10-Gigabit Ethernet)

Najszybsza istniejąca technologia Ethernet, stosowana w sieciach MAN i WAN.

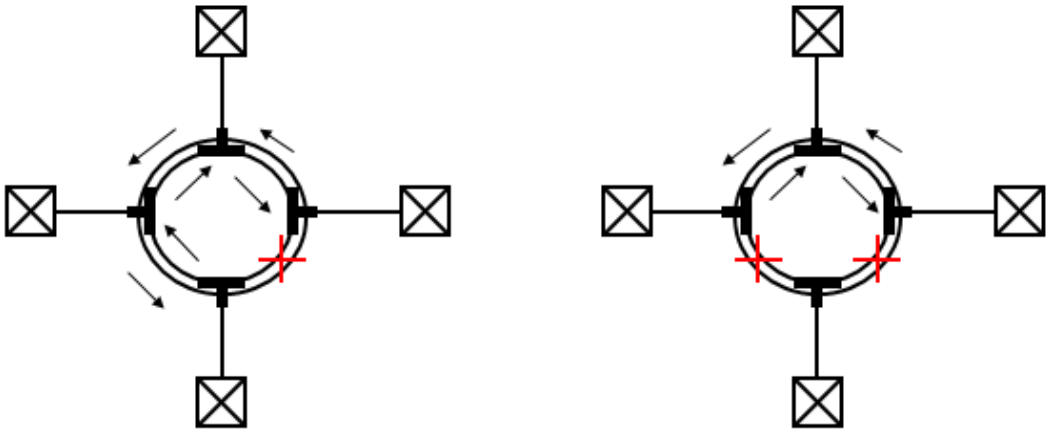
4) 100 VG-AnyLAN

Sieć o prędkości transmisji 100Mb/s, wykorzystująca czterokanałowe łącze (skrętkę 4× 2, multiplekso-
waną skrętkę ekranowaną 2× 2 lub światłowód) w trybie naprzemiennym (half-duplex) - każdy kanał
przenosi 25 Mb/s. Kolizje unikane są wskutek zastosowania specjalnych koncentratorów, które cyklicznie
przeglądają wszystkie swoje porty (zatem topologia logiczna jest pierścieniowa) i obsługują je według
algorytmu uwzględniającego priorytety ramek. Ramki fizyczne (MAC) mogą być tworzone na bazie
ramek logicznych (LLC) wyspecyfikowanych w innych systemach (np. Ethernet 100 Mb/s).
Koncentratory 100VG-AnyLAN mogą być połączone w hierarchiczną strukturę drzewiastą
z wyróżnionym koncentratorem głównym (root hub).

5) FDDI

Sieć oparta na podwójnym pierścieniu światłowodowym. W przypadku zastosowania światłowodów
jednomodalnych długość pierścienia może sięgać 200 km (typowa dla współczesnych sieci MAN).
Prędkość transmisji wynosi 100 Mb/s. W trakcie normalnej pracy wykorzystywany jest tylko **pierścień**
podstawowy (primary ring). Drugi - **pierścień dodatkowy** (secondary ring) - włączany jest automatycznie (być może tylko odcinkami) w przypadku awarii pierścienia podstawowego.

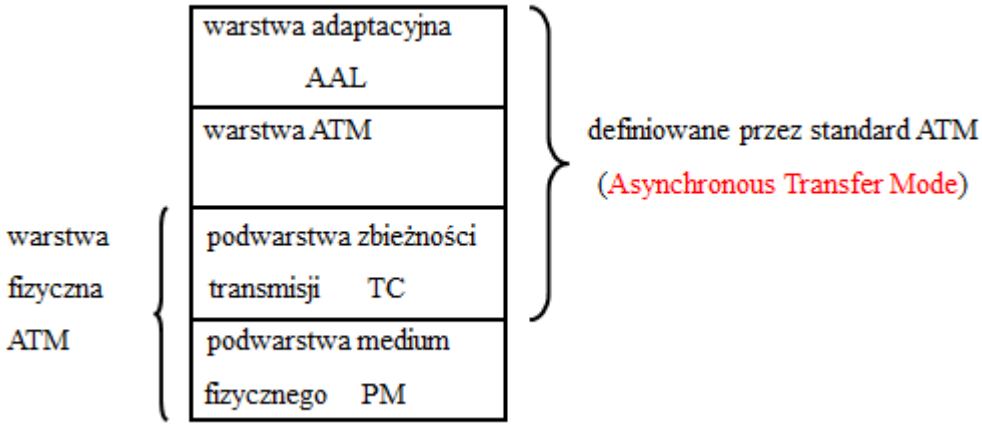
Oprogramowanie FDDI jest tak skonstruowane, aby sieć mogła (nawet tylko we fragmentach)
działać w sytuacji wielokrotnej awarii.
Przykład



Uwaga
Sieć FDDI wykorzystuje podwarstwę LLC według standardu IEEE 802.2, zaś podwarstwę MAC
według standardu nieco podobnego do IEEE 802.5 .

6) X.25
Jedno z najstarszych rozwiązań dla sieci WAN, definiuje protokoły warstwy fizycznej, łącza i sieciowej. Umożliwia prędkości transmisji rzędu dziesiątek Kb/s. Standard ten jest starannie opracowany i dobrze udokumentowany, przez wiele lat był najbardziej rozpowszechniony w cyfrowych sieciach telekomunikacyjnych.
7) Frame Relay
Nowsze i dużo wydajniejsze rozwiązanie dla sieci WAN. Może być widziane jako etap pośredni
w ewolucji od X.25 do ATM
8) ATM
Jest nowoczesnym standardem, teoretycznie mogącym w jednolity sposób obsługiwać ruch zarówno
w sieciach LAN, MAN jak i WAN.

Standard ATM obejmuje warstwy protokołów (niezbyt zgodne z modelem OSI):



Suma warstw ATM i AAL w przybliżeniu odpowiada warstwie łącza i części warstwy sieciowej w modelu OSI.

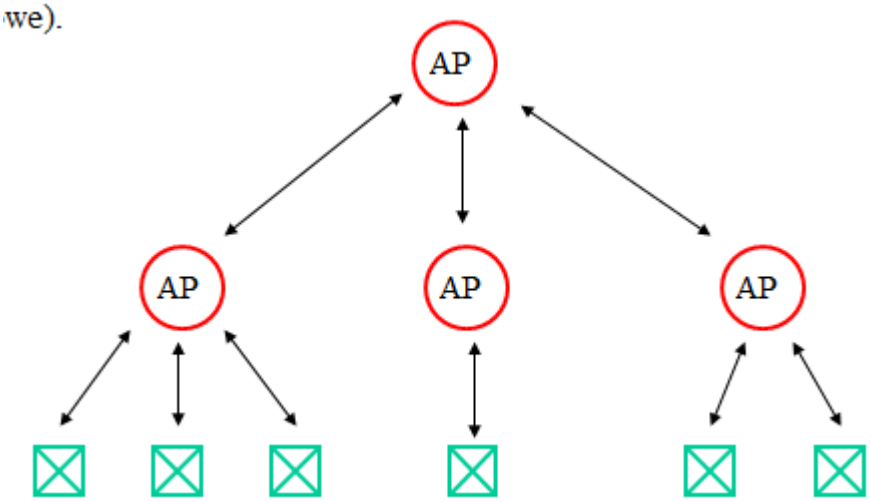
Podwarstwa medium fizycznego nie jest definiowana przez standard ATM. Zazwyczaj jest to jedna
z **sieci synchronicznych** - **SONET (Synchronous Optical Network)** w USA lub SDH **(Synchronous
Digital Hierarchy)** w Europie. Sieci synchroniczne transmitują bity w sposób ciągły (niezależnie od
aktualnej potrzeby przesyłania informacji), porcjując je w nieduże ramki o ustalonej wielkości.

Warstwa ATM operuje na obiektach logicznych zwanych **komórkami ATM** mających ustaloną
wielkość 53 bajty (5-bajtowy nagłówek i 48 bajtów danych). Ponieważ zarówno ramki podwarstwy
medium fizycznego, jak i pakiety obsługiwane przez protokoły wyższych warstw mają znacznie
większą długość, niż kilkadziesiąt bajtów, na styku warstw muszą być wykonywane operacje **rozdrabniania** oraz **scalania** porcji danych (zjawisko takie jest też charakterystyczne dla stosów
protokołów bardziej zgodnych z modelem OSI, występuje np. na styku protokołów IP oraz Ethernet).
Dla światłowodu jednomodalnego typowa prędkość transmisji w sieci ATM wynosi 622 Mb/s, ale
standard ATM przewiduje też wyższe i niższe prędkości transmisji.
Węzłami sieci ATM są wyspecjalizowane **przełączniki ATM**, mogące ustalać **ścieżki wirtualne** dla
przesyłania komórek ATM.
9) Sieci bezprzewodowe (rodzina standardów IEEE 802.11)
W ostatnich latach sieci bezprzewodowe znacznie rozpowszechniły się. Przyczyny:
a) rozpowszechnienie się komputerów przenośnych (notebooki itp.) i zapotrzebowanie na łatwy
dostęp do Internetu ich użytkowników.
b) umożliwienie dostępu do sieci w miejscach, gdzie instalacja sieci kablowej byłaby technicznie
niemożliwa lub ekonomicznie nieopłacalna;

c) rozwój technologii elektronicznej umożliwiającej łączność radiową w zakresie częstotliwości
powyżej 1 GHz.
W Polsce istotną rolę odegrało również udostępnienie pasm częstotliwości, które dawniej były
zastrzeżone do celów militarnych.
Najprostsza sieć bezprzewodowa umożliwia bezpośrednią łączność pomiędzy komputerami na
zasadzie „każdy z każdym” (tak zwane sieci *ad hoc*). Przypomina to działanie sieci Ethernet z rywalizacyjnym dostępem do medium, ale zamiast algorytmu CSMA/CD jest tu stosowany algorytm CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Pozwala on na unikanie kolizji ramek informacyjnych przez wcześniejsze uzgodnienie czasowego zajęcia kanału
przy użyciu ramek organizacyjnych.
Bardziej typowa organizacja sieci bezprzewodowych oparta jest o zastosowanie **stacji bazowych**
nazywanych zwykle **punktami dostępowymi** (Access Point). Punkty dostępowe pozwalają unikać
kolizji w dostępie do wspólnego medium, ale działają na innej zasadzie, niż przełączniki w sieciach
Ethernet - cyklicznie odpytują przyłączone komputery, czy mają jakieś ramki do wysłania, a jeśli tak,
to przydzielają im na to pewien odcinek czasu. Na ogół wszystkie przyłączone komputery mają takie
same prawa, a zatem dostępna przepustowość sieci bezprzewodowej jest dzielona na tyle równych
części, ilu aktualnie jest przyłączonych użytkowników.

Punkty dostępowe zwykle są połączone ze sobą siecią kablową, ale mogą też być elementami
spinającej sieci bezprzewodowej o szerszym zasięgu (na przykład wykorzystującej anteny kierunkowe).

we).

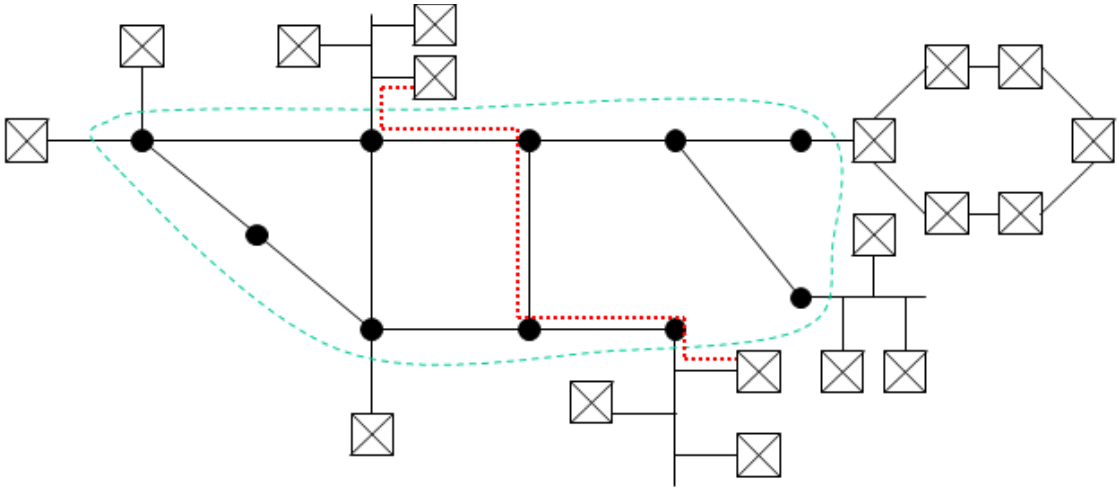


Wiele zjawisk występujących w sieciach bezprzewodowych jest swoistych dla nich i nie występuje

w sieciach przewodowych (na przykład użytkownik może w czasie pracy przemieścić się z zasięgu
jednego AP do zasięgu innego AP bez przerywania połączenia z Internetem, jeśli te dwa zasięgi
częściowo pokrywają się).

6. WARSTWA SIECIOWA

Protokoły warstwy sieciowej służą do organizowania łączności na większą odległość, niż pomiędzy
sąsiadującymi ze sobą stacjami lub węzłami. W związku z tym wymagają one rozwiązania dwóch
problemów:
1) Jak ustalić system adresowania, żeby w możliwie dużym stopniu odzwierciedlał on hierarchiczną
strukturę sieci ?
2) Jak wytyczać trasę przesyłu informacji przez węzły tranzytowe, aby zoptymalizować ruch w sieci ?



ad.1. Adresy fizyczne (MAC) używane w warstwie łącza nie nadają się do tego, bo sprzęt sieciowy
(pochodzący od różnych producentów) jest rozmieszczony na świecie w sposób dość przypadkowy
i rozmieszczenie to nie odzwierciedla struktury sieci. Potrzebny jest więc inny, niezależny od
sprzętu a zależny od logicznej struktury sieci, zbiór adresów, który zostanie **odwzorowany** na
zbiór adresów fizycznych.

Uwaga

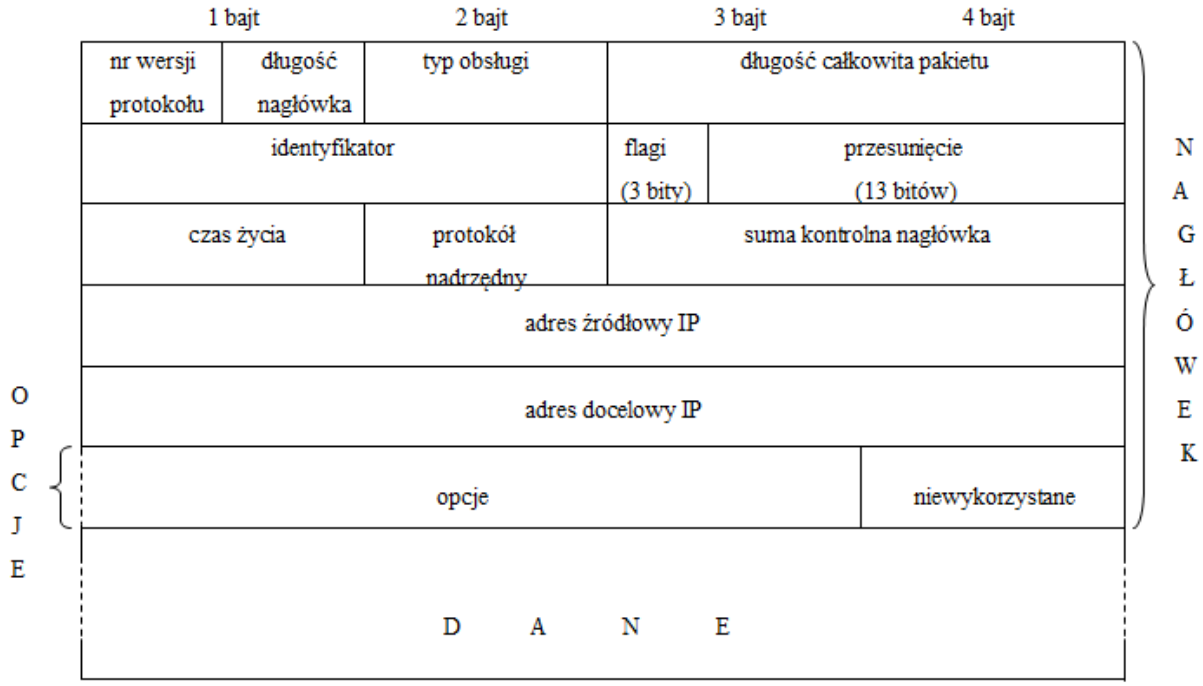
Adresowanie sieciowe jest związane z konkretnym używanym protokołem warstwy sieciowej, w związku z tym stacje używające różnych protokołów warstwy sieciowej (np. IP i IPX) nie mają
możliwości porozumiewania się ze sobą (chyba, że dysponują odpowiednimi emulatorami innych
systemów adresowania).

ad.2. W małych sieciach jest możliwe przechowywanie **informacji globalnej** o strukturze połączeń
wszystkich węzłów sieci i ustalanie na jej podstawie trasy połączenia pomiędzy dwiema stacjami,
a dopiero potem transmitowanie informacji (w całości po ustalonej z góry trasie). W sieci
o zasięgu światowym takie rozwiązanie byłoby praktycznie niemożliwe ze względu na ilość tej
informacji, jak również ze względu na szybko zmieniające się warunki w różnych fragmentach
takiej sieci - awarie i rekonfiguracje, nagłe wzrosty i spadki natężenia ruchu itd. W związku z tym
typowym rozwiązaniem jest przechowywanie **informacji lokalnej** (rozproszonej po różnych
węzłach sieci) i **dynamiczne podejmowanie decyzji** co do wyboru trasy przesyłu na kolejnym
odcinku (przykładowo w sytuacji nagłego wzrostu natężenia ruchu oprogramowanie węzła może
podjąć decyzję o skierowaniu części przesyłanej informacji „trasą okrężną”, na której natężenie
ruchu jest mniejsze).

Protokół IP (Internet Protocol)

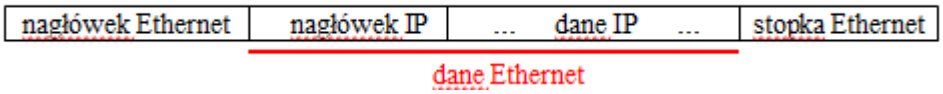
Poniżej omówimy najbardziej obecnie rozpowszechniony na świecie protokół IP w wersji nr 4 (IPv.4)
(wersja IPv.5 istnieje jako wersja eksperymentalna, zaś IPv.6 dopiero niedawno zaczął się rozpo-
wszechniać). Protokół IPv.6 dysponuje dużo większą przestrzenią adresową i lepiej jest dostosowany
do aplikacji czasu rzeczywistego (np. multimedialnych), niż IPv.4.
Protokół IP jest protokołem bezpołączeniowym, zawodnym (ewentualnym tworzeniem połączenia
i zapewnianiem niezawodności zajmują się protokoły warstwy transportowej, np. TCP). Logiczną
jednostką informacji jest **datagram IP**, który będąc przesyłanym przez warstwę łącza jest zazwyczaj
rozdrabniany na mniejsze fragmenty (mieszczące się w pojedynczych ramkach LLC) zwane **pakietami**.

Struktura pakietu IP:



Opisy pól:
- numer wersji jest numerem wersji protokołu IP (aktualnie 4);
- długość nagłówka podawana jest w słowach czterobajtowych - może wynosić od 5 do 15 (długość pola „opcje” może więc wynosić od 0 do 10);
- pole „typ obsługi” zawiera życzenia użytkownika (jego programu użytkowego) co do sposobu traktowania pakietu na trasie przesyłu - nadawania priorytetu, kierowania do łącza o największej przepustowości lub niezawodności itp. (węzły tranzytowe starają się je w miare możności uwzględniać, ale nie zawsze ich oprogramowanie to umożliwia);
- długość całkowita pakietu (tj. nagłówka i danych łącznie) jest zapisywana na 2 bajtach (16 bitach), zatem może wynosić co najwyżej 2 - 1 (64 KB - 1);
- pola „ identyfikator”, „flagi” i „przesunięcie” służą do tego, aby datagram można było rozdrobnić, zapakować w ramki, a następnie scalić, gdyby długość całkowita datagramu przekraczała maksymalną długość pola danych ramki w przebywanym łączu. Identyfikator musi być liczbą unikalną dla pary (adres źródłowy, adres docelowy). Flagi: 0 - na razie nie została zdefiniowana; 1 - zakaz rozdrabniania datagramu; 2 - nie jest to ostatni fragment rozdrobnionego datagramu.
Przesunięcie wskazuje, od którego bajtu w rekonstruowanym datagramie należy wstawić pole danych pakietu (dokładniej: zawartość pola „przesunięcie” należy pomnożyć przez 8);

Przykład opakowania danych:



(powyższy rysunek nie uwzględnia bitów dodawanych przez warstwę fizyczną)
- pole „czas życia" zapobiega dowolnie długiemu błąkaniu się po sieci „bezpańskich" pakietów (np.
z uszkodzoną częścią adresową) - na początku pole to jest jedynkowane przez nadawcę (czyli
ustawiane na 255), a każde przejście przez jakikolwiek węzeł tranzytowy zmniejsza jego wartość
o 1. Po wyzerowaniu się tego pola pakiet jest usuwany z sieci;
- pole „protokół nadrzędny" zawiera kod liczbowy protokołu warstwy nadrzędnej względem IP (np.
TCP ma numer 6), który zlecił protokołowi IP przesłanie danego pakietu;
- suma kontrolna nagłówka pozwala kontrolować poprawne przesłanie samego nagłówka pakietu (nie
obejmuje danych), podobnie jak pole CRC ramki Ethernet (teoretycznie węzły tranzytowe
powinny po drodze sprawdzać wartość tego pola, ale nie zawsze to robią);
- adres IP (źródłowy i docelowy) w IPv.4 jest 32-bitowy (w IPv.6 jest 128-bitowy);
- pole „opcje" może służyć do różnych celów (np. trasowanie źródłowe, rejestrowanie trasy i in.).

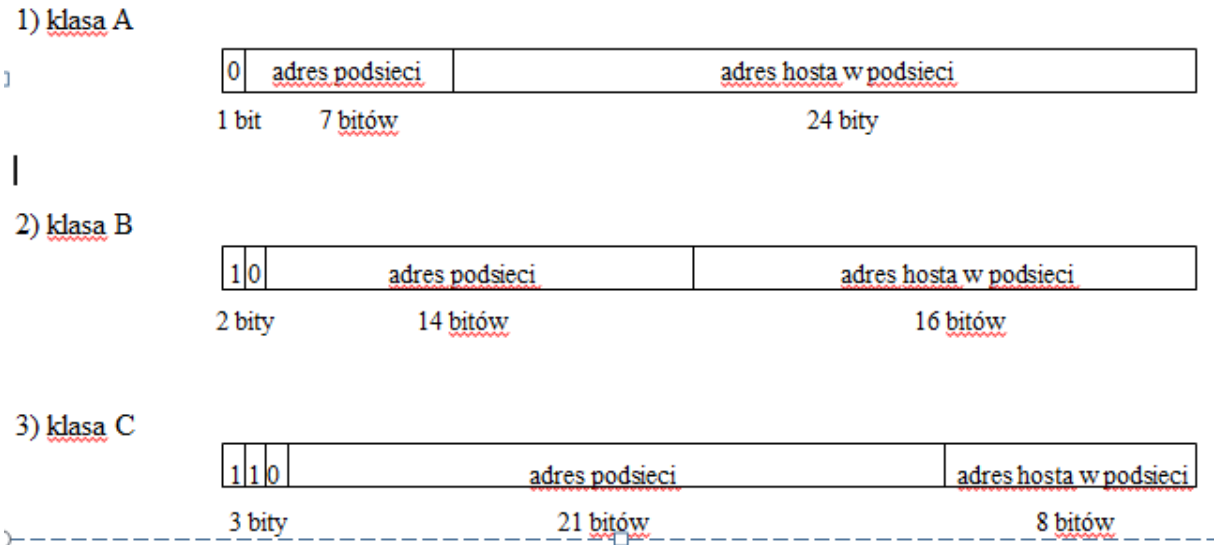
Adresowanie IP

Adres IP może być przydzielony każdemu interfejsowi sieciowemu (np. karcie sieciowej) urządzenia
przesyłającego przez ten interfejs pakiety IP. Urządzenia działające na poziomie warstwy sieciowej
i służące do przekazywania informacji pomiędzy różnymi domenami rozgłoszeniowymi (węzły
tranzytowe IP) nazywane są **ruterami** (router) (dosł. „traser"). Oprogramowanie rutera podejmuje
decyzję, jaki kolejny odcinek trasy powinien przebyć przekazywany pakiet (decyzja ta objawia się
w przekierowaniu pakietu do innego interfejsu sieciowego rutera). Rutery są zazwyczaj wyspecjalizo-
wanymi urządzeniami, ale ich rolę mogą też pełnić komputery „ogólnego użytku" posiadające
odpowiednie oprogramowanie i więcej, niż jedną kartę sieciową (jest to rozwiązanie powolniejsze,
ale na ogół tańsze - stosowane w sytuacji niezbyt dużego natężenia ruchu).
Rutery IP umieszczane na granicy sieci lokalnej i intersieci obyczajowo nazywane są **bramami**
(gateway). Nazywane są też tak rutery wieloprotokołowe (pracujące na styku sieci opartych na
różnych protokołach warstwy sieciowej).
Sieć ogólnoświatowa korzystająca z protokołu IP i systemu adresowania IP, którego jednoznaczność
nadzorowana jest przez organizacje międzynarodowe, nazywana jest **Internetem**.

Uwagi:

1) Istnieją sieci (np. lokalne) korzystające z protokołu IP i nie podłączone do Internetu - w takim
przypadku nie podlegają one kontroli międzynarodowej i jednoznaczność adresowania w ich
obrębie muszą zapewniać ich administratorzy.
2) W literaturze można napotkać termin **internet** oznaczający dowolnego rodzaju połączone sieci
lokalne korzystające ze wspólnego protokołu warstwy sieciowej.
3) Sieć Internet wyrosła z amerykańskiej sieci ARPANET (utworzonej z myślą o zastosowaniach
militarnych i naukowych). Przydzielaniem zakresów adresów internetowych do roku 1993
zajmowała się organizacja NIC **(Network Information Center**), w 1993 roku jej kompetencje zostały
rozdzielone pomiędzy kilka współpracujących organizacji międzynarodowych obsługujących różne
regiony geograficzne. Organizacje te nazywane są **Rejestrami Zasobów Internetowych** (Internet
Resources Registries, IRR). Przydzielają one duże zakresy adresów internetowych dużym
dostawcom usług internetowych, którzy zajmują się dalej ich redystrybucją mniejszym firmom
i organizacjom. Rejestrem Zasobów Internetowych dla Europy jest RIPE (Resaux IP Europeen).
Naczelną organizacją ogólnoświatową (niedochodową) jest ICANN (Internet Corporation for
Assigned Names and Numbers).

W IPv.4 adres IP jest 32-bitowy. Pewna jego część początkowa określa **adres podsieci**, w której
znajduje się dane urządzenie, a pozostała część określa **adres urządzenia** w obrębie tej podsieci
(adres hosta). Pojęcie podsieci jest pojęciem logicznym, związanym z hierarchicznością adresowania.
Tradycyjne adresowanie IP przyjmuje, że rozmiar adresu hosta musi być całkowitą krotnością
jednego bajtu. W związku z tym wyróżniane są następujące **klasy adresów IP**:



4) klasa D

Cztery pierwsze bity są ustawione odpowiednio na 1110. Adres taki jest traktowany jako **adres**
grupowy (multicast address) służący do zorganizowania grupy hostów położonych w różnych
podsieciach i intensywnie współpracujących ze sobą.

5) klasa E

Cztery pierwsze bity są ustawione na 1111. Tego typu adresy są zarezerwowane do celów
specjalnych (np. eksperymentalnych).
Tradycyjne adresy IP zazwyczaj przedstawia się w postaci czterech liczb dziesiętnych (odpowiadających kolejnym bajtom) oddzielonych od siebie kropkami, np.
204.13.139.7 .
Pierwsza z tych liczb umożliwia łatwe zidentyfikowanie klasy adresu:
- mniejsza niż 128 - adres klasy A
- od 128 do 191 - adres klasy B
- od 192 do 223 - adres klasy C
- od 224 do 239 - adres klasy D
- większy niż 239 - adres klasy E

Poza zarezerwowanymi adresami klasy E istnieją jeszcze następujące ograniczenia możliwości
adresowania:
- adres 0.0.0.0 oznacza tzw. **ścieżkę domyślną** (upraszcza zapis informacji o trasowaniu w ruterach);
- adres 127.0.0.0 oznacza tzw. **pętlę** - ścieżkę prowadzącą od hosta do niego samego (może służyć
do celów autodiagnostycznych, pozwala sprawdzić poprawność zainstalowanego oprogramowania IP
przed podłączeniem hosta do sieci);
- we wszystkich klasach adresów zarezerwowane są adresy hostów: wyzerowany i wyjedynkowany
(adres wyzerowany jest używany wewnętrznie przez protokół IP w tablicach rutowania, adres
wyjedynkowany jest adresem rozgłoszeniowym dla danej podsieci).
- w klasach A i B zarezerwowane są pule **adresów prywatnych** (wyłącznie do użytku wewnątrz
sieci lokalnych, pakiety z takimi adresami nie mogą pojawić się w sieci zewnętrznej):

od	10.0.0.0	do	10.255.255.255
od	172.16.0.0	do	172.31.255.255
od	192.168.0.0	do	192.168.255.255

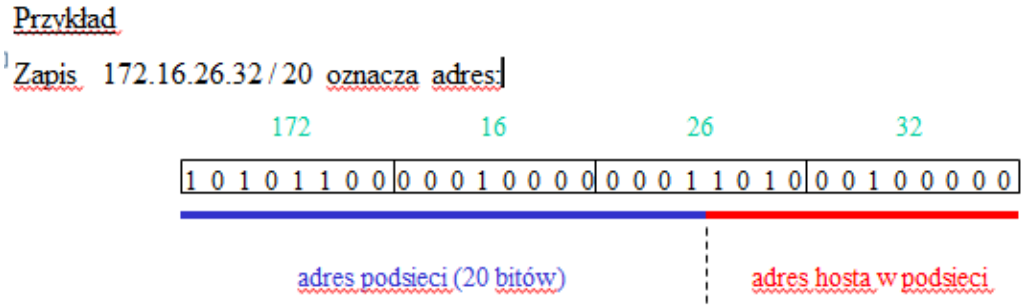
Istotnym problemem związanym z tradycyjnym systemem adresowania w IPv.4 jest możliwość
wyczerpania się adresów w klasie B. Sieć klasy A może zawierać prawie 2 (około 4 mln.) komputerów - firm i organizacji potrzebujących sieci klasy A jest niewiele na świecie. Sieć klasy C
może zawierać do 254 hostów (co wystarcza na potrzeby niedużej firmy) i takich sieci można utworzyć ponad 2 mln. (co prawdopodobnie wystarczy jeszcze na długo). Sieć klasy B może zawierać
prawie 2 hostów (około 65 tys.), co zaspokaja potrzeby średnich i dużych firm, i takich sieci może
powstać tylko niewiele ponad 4 tys. (może niedługo zabraknąć).
Możliwości rozwiązania problemu braku adresów w klasie B:
1) wprowadzenie do powszechnego użytku IPv.6 (wymaga dużych nakładów finansowych i czasu);
2) stosowanie **bezklasowego adresowania IP** (Classless Inter-Domain Routing, CIDR). Stosowanie adresowania bezklasowego wiąże się z możliwością przydzielania sieciom lokalnym
nawet pojedynczych adresów IP (lub kilku takich adresów), które następnie są wykorzystywane przez
większą liczbę komputerów wewnątrz takiej sieci przy użyciu mechanizmu **translacji adresów
sieciowych** (Network Address Translation, NAT).

Adresowanie bezklasowe (jednolite)

Podstawową ideą bezklasowego adresowania IP jest rezygnacja z założenia, że długość adresu hosta
musi być całkowitą wielokrotnością długości bajtu.
Maską adresu (maską bitową) nazywamy ciąg bitów, w którym jedynki odpowiadają pozycjom

użytym do zapisu adresu podsieci, zaś zera - pozycjom użytym do zapisu adresu hosta w tej podsieci.
Dla tradycyjnego adresowania IP mamy zatem:
255.0.0.0 - maska adresu klasy A
255.255.0.0 - maska adresu klasy B
255.255.255.0 - maska adresu klasy C
(stosujemy tę samą notację, co dla zapisu samych adresów IP).

Jeśli rezygnujemy z założenia, że adres hosta w podsieci może być jedno-, dwu- lub trzybajtowy, to
nie możemy korzystać z informacji zapisanej w początkowych 1 - 4 bitach mówiącej o klasie adresu.
W takim przypadku wraz z samym 32-bitowym adresem musi być podana jego maska (mówiąca,
jak dany adres prawidłowo zinterpretować). Symboliczny zapis ma postać adres / długość, gdzie
długość jest liczbą jedynek w masce (tj. liczbą bitów służących do zapisu adresu podsieci).
Przykład
Zapis 172.16.26.32 / 20 oznacza adres:



Taki zmodyfikowany system adresowania wymaga pewnych zmian oprogramowania ruterów IPv.4
(jest to jednak związane z mniejszymi kosztami, niż wprowadzenie IPv.6).

Podsieci (subnet)

W sposób analogiczny do jednolitego adresowania IP, administrator dużej sieci IP należącej do firmy
lub instytucji może podzielić ją na pewną liczbę podsieci stosując maski niestandardowe. Podział taki
może być dogodny, jeżeli firma (instytucja) składa się z kilku autonomicznych działów posiadających
różniące się sprzętem sieci fizyczne i rzadko komunikujących się ze sobą. Maski poszczególnych
podsieci muszą być pamiętane przez rutery oddzielające od siebie te podsieci oraz ruter łączący
tę sieć z Internetem (podział na podsieci nie jest widoczny z punktu widzenia zewnętrznych użytkowników Internetu).
Pewną wadą podziału na podsieci jest to, że zmniejsza on nieco sumaryczną przestrzeń adresową
danej sieci (w każdej z wydzielonych podsieci zarówno wyzerowany, jak i wyjedynkowany adres
hosta nie może być wykorzystany). Ogólnie, jeśli dana sieć podzielona jest na *k* podsieci, łączna
strata przestrzeni adresowej wynosi $2k - 2$.

Przykład

Sieć IP klasy C (256 - 2 = 254 adresy) po podzieleniu na cztery podsieci będzie dysponowała jedynie
4 * (64 - 2) = 248 adresami, zatem łączna strata przestrzeni adresowej wyniesie 254 - 248 = 6 adresów.

Nazwy i domeny IP

System adresów IP w postaci liczbowej jest niezbyt wygodny w użyciu dla ludzi, został więc wprowadzony alternatywny system nazw (nazwy są łatwiejsze do zapamiętywania). Nazwy są
wieloczęściowe i, podobnie jak system adresów, tworzą strukturę hierarchiczną.
Ogólnie biorąc, nie ma związku pomiędzy hierarchią nazw a hierarchią adresów IP.
Nazwa może być nadana każdemu urządzeniu posiadającemu adres IP, mogą być też nadawane nazwy
alternatywne (aliasy). Każda **domenowa nazwa hosta** (analogiczna do pełnej nazwy ścieżkowej pliku)
musi jednoznacznie określać pewnego hosta (posiadającego jeden lub więcej adresów IP). Podobnie, jak krótkie nazwy plików mogą się powtarzać w różnych katalogach jednego systemu plików,
ale ich pełne nazwy ścieżkowe muszą być unikalne w obrębie tego systemu, również krótkie nazwy
hostów IP mogą powtarzać się w różnych miejscach Internetu (administratorzy nie uzgadniają ich
z nikim), ale domenowa nazwa hosta musi jednoznacznie określać hosta w obrębie całego Internetu.
W zapisie ścieżek dostępu do plików stosowane są przednie ukośniki (Unix) lub tylne ukośniki (DOS),
w przypadku domen stosowane są kropki. Jest to o tyle mylące, że zwyczajowo kropkami rozdzielamy

też poszczególne liczby wchodzące w skład adresu IP, a pomiędzy strukturą adresu (np. 172.17.12.4)
a strukturą nazwy, której ten adres odpowiada (np. tiger.zoo.animals.ax) **w ogólności nie ma**
żadnego związku.
Uwaga:
1) Adres IP zawsze zawiera cztery liczby rozdzielone trzema kropkami, natomiast nazwy mają
zmienną liczbę elementów (np. poprawną nazwą jest sigma.inf.ug.edu.pl).
2) Czasem można jednak zaobserwować pewną zależność pomiędzy nazwami a adresami – na
przykład w przypadku niedużej firmy nie posiadającej filii w innych miejscach, jej sieć IP klasy C
może pokrywać się z jej domeną.
W zapisie ścieżek dostępu do plików nazwa katalogu stojącego najwyżej w hierarchii jest umieszczona
na początku, a sama nazwa pliku na końcu, w przypadku pełnych nazw hostów jest odwrotnie: sama
nazwa hosta umieszczona jest na początku, a nazwa domeny najwyższego poziomu – na końcu zapisu

Hierarchia domen:

- **korzeń** (domena główna) oznaczony jest przez kropkę (jest ona pomijana w zapisie pełnej nazwy);
- **domeny górnego poziomu** – mogą być organizacyjne lub geograficzne. Domeny organizacyjne

górnego poziomu są używane głównie w USA. Ich tradycyjny zestaw:
com - organizacje komercyjne;
edu - instytucje naukowe;
gov - agencje rządowe;
mil - organizacje wojskowe;
net - organizacje podtrzymujące działanie sieci;
int - organizacje międzynarodowe;
org - inne organizacje (niedochodowe).
Domenami górnego poziomu początkowo zarządzała organizacja InterNIC (wywodząca się z NIC).
Obecnie zarządza nimi ICANN. Tradycyjny podział na domeny zawsze wzbudzał kontrowersje.

W 2000 r. tradycyjny zestaw domen organizacyjnych górnego poziomu został rozszerzony przez
ICANN o następujące [Tanenbaum]:
biz – dla biznesu
info – dla celów informacyjnych
name – dla użytkowników indywidualnych
pro – dla popularnych zawodów
aero – dla przemysłu kosmicznego
coop – dla współpracy przedsiębiorstw
museum – dla muzealnictwa
Kontrowersje wokół podziału na domeny górnego poziomu trwają nadal (w szczególności wokół
podziału ich kompetencji) i należy oczekiwać tworzenia następnych.

Domeny geograficzne górnego poziomu są przydzielane wszystkim krajom na świecie i oznaczane są
dwuliterowymi skrótami (pl, de, fr, uk, ...). Geograficzna domena Stanów Zjednoczonych (us) również
istnieje i jest używana.
- poniżej domen górnego poziomu są **domeny niższych poziomów** (co najmniej drugiego, zwykle też
trzeciego, a często również czwartego i niższych).
Zazwyczaj domeny geograficzne górnego poziomu dzielą się na domeny drugiego poziomu w sposób
odzwierciedlający podział na górnym poziomie (np. istnieją domeny organizacyjne drugiego poziomu
com.pl oraz edu.pl , jak również domeny geograficzne drugiego poziomu, np. waw.pl czy gda.pl).
Uwaga
1) Nazwy domen niższych poziomów rejestrują właściciele nazw domen wyższych poziomów.
2) Komputer (jego interfejs sieciowy) może mieć pełne nazwy należące do różnych domen.
3) Domena pewnego poziomu może być „rozrzucona” po większym obszarze i nic nie mieć wspólnego
z logiczną topologią sieci - zazwyczaj odzwierciedla ona tylko logiczną strukturę pewnej firmy lub
organizacji (np. jej podział na filie).

Możliwość podziału Internetu na domeny (nazewnicze) wydaje się być w sprzeczności ze stwierdzeniem niemożliwości wykorzystywania adresów fizycznych (MAC) w skali globalnej.
Różnica między adresowaniem fizycznym a adresowaniem przy użyciu nazw polega na tym, że
w nazewnictwie domen jest utrzymywana hierarchia, a przydzielanie nazw domen jest rejestrowane.
O ile utrzymywanie **informacji scentralizowanej** o nazwach nie byłoby możliwe, o tyle jest możliwe
utrzymywanie w sieci **informacji rozproszonej**.
Zazwyczaj komputery przechowują dane o najważniejszych (dla nich) hostach (hostach w sieci
lokalnej oraz hostach odległych, z którymi komunikują się najczęściej) w swoich lokalnych **tablicach
hostów**. Szybki dostęp do takiej tablicy odciąża sieć lokalną i częściowo zabezpiecza przed skutkami
awarii serwerów przechowujących fragmenty informacji rozproszonej.
Podstawową metodą kojarzenia nazw z adresami IP hostów odległych jest korzystanie z rozproszonej
obsługi nazw domen (Domain Name Service - DNS). Idea działania DNS: domena główna (root
domain) zawiera serwery nazw dla domen górnego poziomu, tak zwane **serwery główne**. Serwery
główne z kolei zawierają dane o serwerach DNS drugiego poziomu itd. Zasadniczo każdą domenę
powinny obsługiwać co najmniej dwa niezależne serwery DNS (na wypadek awarii jednego z nich).

Jeśli indywidualny host chce skontaktować się z jakimś innym hostem, którego nazwę zna, a adresu IP

nie zna, wysyła **zapytanie** do swojego lokalnego serwera DNS (musi znać jego adres). Jeśli lokalny
serwer zna **odpowiedź** na to zapytanie, to jej udziela, a w przeciwnym razie przekazuje zapytanie do
swojego nadrzędnego serwera DNS.
Ogólnie, algorytm obsługi takiego zapytania może być **rekurencyjny** lub **nierekurencyjny**.
W przypadku rekurencyjnym zapytany serwer sam dalej zajmuje się wyszukaniem odpowiedzi w sieci
(a po znalezieniu przekazuje ją pytającemu). W przypadku nierekurencyjnym zapytany serwer jedynie
przekazuje adres innego („lepiej zorientowanego”) serwera, który należy dalej indagować.
Najważniejsze serwery DNS (w szczególności serwery główne) nigdy nie biorą udziału
w wyszukiwaniach rekurencyjnych.
Uwaga
Jeżeli z daną nazwą domenową związanych jest kilka adresów IP, są one podawane wszystkie, ale
w zmiennej kolejności – najbardziej typową polityką serwera DNS jest „cykliczne przewijanie” listy
adresów, co powoduje względnie równomierny rozkład obciążenia tych adresów.

Rozproszona baza danych usługi DNS przechowuje w poszczególnych serwerach zbiory **rekordów**
zasobów (resource records), które zawierają rozmaite informacje dotyczące różnych domen. Każdy
rekord składa się z 5 pól: nazwa domeny, czas życia, klasa, typ i wartość.
Z nazwą domeny może być związany jeden rekord lub więcej rekordów. Czas życia określa termin
ważności danego rekordu (w sekundach) – dla informacji uważanych za trwałe typowa wartość wynosi
86 400 sekund (jedna doba). Klasa w przypadku Internetu zawsze ma wartość IN. Pole typ określa
sposób interpretacji pola wartość [Tanenbaum]:

Typ	**Znaczenie**	**Wartość**
SOA	Początek strefy wpływów	Parametry strefy serwera nazw
A	Adres IP hosta	32-bitowa liczba całkowita
MX	Wymiana poczty	Nazwa i priorytet serwera pocztowego domeny
NS	Serwer nazw	Nazwa serwera DNS dla domeny
CNAME	Nazwa kanoniczna	Nazwa domeny
PTR	Wskaźnik	Alias adresu IP
HINFO	Opis hosta	Identyfikator procesora i systemu operacyjnego (tekst)
TXT	Tekst	Tekst (dowolna interpretacja)

Problemy przydziału adresów IP w sieciach lokalnych

W sieci lokalnej nie zawsze jest możliwe (i uzasadnione) przechowywanie w komputerach przydzielonych im na stałe adresów IP. Możliwe powody:
- komputery mogą nie mieć dysków twardych (a tym samym możliwości przechowywania informacji
  po ich wyłączeniu);
- mogą być używane komputery przenośne (laptopy) wyposażone w karty sieciowe umożliwiające

przyłączanie ich do różnych sieci lokalnych;
- w dużej i zamożnej firmie rotacja i modernizacja sprzętu komputerowego może być bardzo częstym
zjawiskiem.
Każdy komputer zna swój adres fizyczny (MAC), gdyż jest on zapisany w pamięci jego interfejsu
sieciowego. Swojego adresu IP natomiast nie musi pamiętać - wystarczy, że pamięta go jeden
z serwerów w sieci lokalnej (i udostępnia na żądanie). Serwer taki przechowuje tak zwaną **tablicę
translacji** pomiędzy aktualnymi adresami IP a adresami MAC.

Wyróżniane są trzy metody przydziału adresów IP w sieci lokalnej:
- **ręczna** (manual) - przydziału dokonuje bezpośrednio administrator sieci lokalnej, adres zostaje
zapisany na stałe na dysku komputera i / lub w tablicy translacji utrzymywanej przez pewien serwer;
- **automatyczna** (automatic) - w momencie pierwszego zgłoszenia się komputera w sieci serwer
automatycznie przydziela mu na stałe adres IP z posiadanej puli wolnych adresów i wpisuje go do
swojej tablicy translacji;
- **dynamiczna** (dynamic) - serwer dysponuje pulą wolnych adresów IP i z niej przydziela adresy
zgłaszającym się komputerom nie na stałe, lecz na pewien czas (tak zwany **okres dzierżawy**), który
jest automatycznie przedłużany, jeśli w międzyczasie komputer nie został odłączony.

Protokoły używane do przydzielania, translacji i odwrotnej translacji adresów

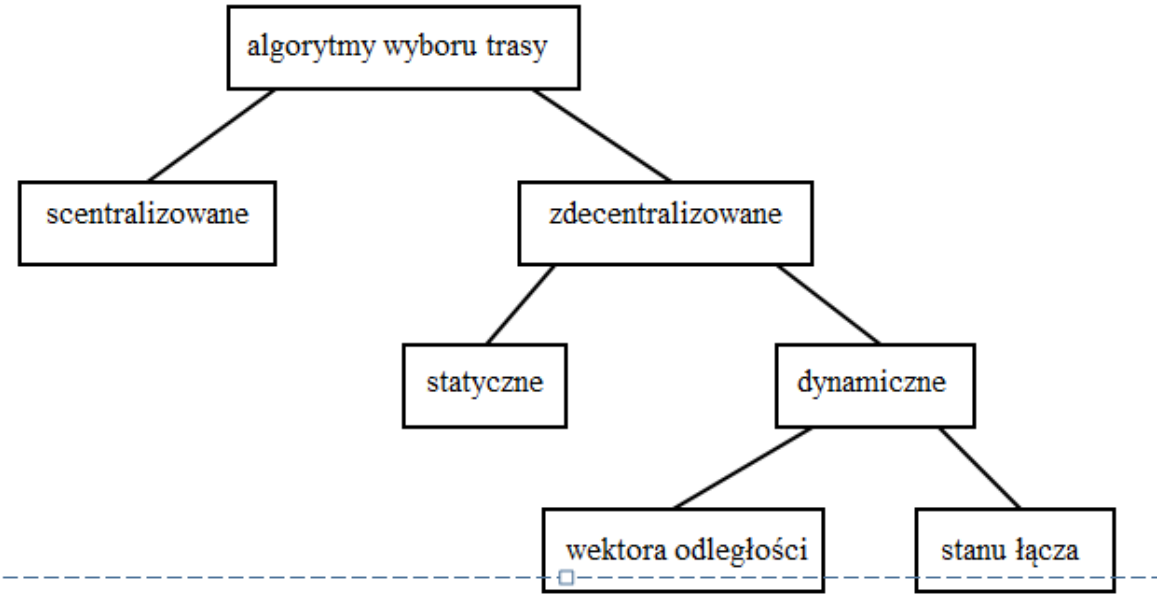
Protokół IP powinien być w stanie funkcjonować niezależnie od konkretnych rozwiązań zastosowanych w danej sieci lokalnej. W związku z tym współpracuje on z kilkoma protokołami
pomocniczymi, które dostarczają mu potrzebnych informacji niezależnie od konfiguracji systemu.
ARP (Address Resolution Protocol) jest protokołem na pograniczu warstwy łącza i warstwy sieciowej.
Przyjmuje zapytania zawierające adresy IP w sieci lokalnej i odsyła w odpowiedzi skojarzone z nimi
adresy MAC. Serwer ARP sprawdza najpierw, czy istnieje odpowiednia pozycja w tablicy translacji
(wtedy udziela odpowiedzi od razu), a jeśli nie, to wysyła ramkę rozgłoszeniową z zapytaniem do
wszystkich hostów w sieci lokalnej, czy któryś z nich ma przydzielony i zapisany we własnej pamięci
taki adres IP. W przypadku pomyślnym otrzymuje odpowiedź z adresem MAC, który przekazuje
hostowi pytającemu (a przy okazji uzupełnia własną tablicę translacji).

W przypadku odwrotnym (podajemy adres MAC, chcemy uzyskać odpowiadający mu adres IP), adres
IP mógł być przydzielony już wcześniej, bądź trzeba go przydzielić dopiero teraz. Do obsługi odwrotnej translacji adresów może służyć kilka protokołów, które są w jedną stronę zastępowalne
(kompatybilne).
RARP (Reverse Address Resolution Protocol) podobnie jak ARP jest protokołem działającym na
pograniczu warstwy łącza i warstwy sieciowej. Klient RARP wysyła ramkę rozgłoszeniową z własnym
adresem MAC, serwer RARP odsyła mu w odpowiedzi ramkę zawierającą odczytany z tablicy
translacji przydzielony mu adres IP. Tablica w tym przypadku musi być wypełniana ręcznie.
BOOTP (Bootstrap Protocol) wykonuje tę samą funkcję, co RARP, ale nie korzystając z mechanizmów
warstwy łącza. Klient BOOTP wysyła rozgłoszeniowy pakiet IP z zapytaniem (zawierający jego adres
MAC), serwer BOOTP wysyła w odpowiedzi również pakiet rozgłoszeniowy, umieszczając w nim
zarówno otrzymany adres MAC, jak i odczytany dla niego adres IP. Host porównując zawarty w
pakiecie adres MAC ze swoim własnym dowiaduje się, czy odpowiedź jest dla niego przeznaczona.
BOOTP umożliwia metodę automatyczną przydziału adresu.

DHCP (Dynamic Host Configuration Protocol) jest kompatybilnym rozszerzeniem BOOTP, umożliwia wszystkie trzy metody przydziału adresu. Zazwyczaj jest wykorzystywany do dynamicznego przydzielania adresów IP.

ZAGADNIENIA WYBORU TRASY W INTERNECIE

Ogólny podział algorytmów wyboru trasy (wg [Nowicki, Woźniak]):



Algorytmy wyboru trasy są realizowane przez rutery (ich oprogramowanie) w oparciu o posiadane
przez nie **tablice trasowania** (routing table). Zadaniem algorytmu jest optymalizacja decyzji o kierunku przekazania pakietu przy uwzględnieniu pewnego kryterium kosztu całego połączenia
(może to być na przykład liczba przejść pakietu przez kolejne rutery lub przewidywany „fizyczny”
czas połączenia). W związku z tym różna może być postać informacji przechowywanej w tablicach
trasowania - mogą to być np. trójki: (adres sieci docelowej, sąsiedni ruter, liczba przeskoków).
Tworzenie tablic trasowania odbywa się w oparciu o (mniej lub bardziej fragmentaryczną) wiedzę na
temat topologii sieci i własności poszczególnych łącz. Algorytm scentralizowany może być stosowany wtedy, gdy pewien ruter dysponuje pełną wiedzą na temat sieci (w pierwotnej sieci
ARPANET zakładano istnienie **rdzenia sieci** i **ruterów rdzeniowych**). Wskutek burzliwego i niekontrolowanego rozrostu Internetu obecnie prawie wyłącznie stosowane są algorytmy zdecentralizowane.

Uwaga
Protokół IP umożliwia tzw. **ruting źródłowy** (source routing) polegający na tym, że urzadzenie
wysyłające pakiet zapisuje w nim swoje żądanie wyboru konkretnej trasy w sieci (a węzły tranzytowe
tylko realizują to żądanie). Ruting źródłowy stosowany jest przez administratorów sieci do celów

testowo-diagnostycznych. Wyróżniamy **ruting źródłowy pełny**, w którym zdeterminowana jest cała
trasa, i **ruting źródłowy częściowy**, w którym określone są tylko niektóre węzły tranzytowe, a pomiędzy nimi istnieje swoboda wyboru trasy.
Ruting zdecentralizowany może być statyczny lub dynamiczny. W przypadku rutingu statycznego
tablice trasowania są wypełniane „ręcznie” przez administratorów i tylko oni mogą zmienić ich
zawartość - jest to metoda stosowana w niedużych sieciach o prostej strukturze. W dużych, skomplikowanych sieciach stosowany jest ruting dynamiczny, który bazuje na okresowym automatycznym komunikowaniu się ruterów pomiędzy sobą i wymianie informacji aktualizujących.
Rutery wymieniają pomiędzy sobą informację przy użyciu specjalnych **protokołów trasowania**
(routing protocol), które pełnią rolę pomocniczą względem protokołu IP.
Uwaga. Protokoły trasowania mogą być realizowane na bazie protokołów wyższego poziomu (np. TCP).

Tablice trasowania mogą zawierać zarówno informacje na temat ścieżek prowadzących do konkretnych
hostów, jak i ścieżek prowadzących do całych sieci - z oczywistych względów te pierwsze odnoszą się
tylko do wybranych najważniejszych hostów w bezpośrednim sąsiedztwie. Każda tablica zawiera też
ścieżkę domyślną, wytyczającą kierunek przesyłania pakietów do sieci docelowych nie wymienio-
nych w tablicy.
Obecnie nie istnieje żadna spójna polityka trasowania w skali globalnej. Wielcy dostawcy usług
internetowych prowadzą niezależne polityki w obrębie swoich obszarów działalności i wymieniają
jedynie pomiędzy sobą „informacje graniczne”. W związku z tym współczesny model trasowania
w Internecie zakłada istnienie **systemów autonomicznych** (Autonomous System, AS) zwanych też
domenami trasowania (routing domain).
Z definicji system autonomiczny jest zbiorem ruterów podlegających wspólnej administracji technicznej i stosującym wspólny algorytm trasowania w swoim obrębie, jak również wymieniającym
informacje o rutowaniu (tzw. **informacje o dostępności**) z sąsiednimi systemami.

Uwaga
Na ogół system autonomiczny jest dużo większym fragmentem Internetu, niż pojedyncza sieć lokalna
(nawet bardzo rozbudowana i posiadająca wiele ruterów mogących przesyłać pakiety do różnych
sąsiednich sieci). Duże systemy autonomiczne mogą logicznie dzielić się na **obszary**.
Protokoły rutujące, które zakładają istnienie systemów autonomicznych, dzielą się na **wewnętrzne**
protokoły rutujące (Interior Gateway Protocol, IGP), stosowane w obrębie systemów autonomicz-
nych, oraz **zewnętrzne protokoły rutujące** (Exterior Gateway Protocol, EGP), służące do wymiany

informacji o dostępności z sąsiednimi systemami.
Typowymi przykładami protokołów wewnętrznych są **RIP** (Routing Information Protocol), stosujący
algorytm wektora odległości, oraz **OSPF** (Open Shortest Path First), stosujący algorytm stanu łącza.
Najczęściej obecnie stosowanym protokołem zewnętrznym jest **BGP** (Border Gateway Protocol).

Dla protokołu RIP kryterium jakości połączenia stanowi liczba przeskoków pakietu przez rutery po
drodze (hop count). Ruter często widzi (ma zapisane w swojej tablicy) więcej, niż jedną ścieżkę
umożliwiającą osiągnięcie sieci docelowej - wybiera z nich tę, która zawiera najmniej przeskoków
(ale inne pamięta dalej na wypadek awarii lub rekonfiguracji sieci). Po pierwszym włączeniu do sieci
tablica trasowania rutera jest pusta, więc ruter rozsyła pakiet rozgłoszeniowy z **żądaniem aktualizacji**.
Sąsiednie rutery (z tej samej sieci) odsyłają mu **pakiety aktualizacyjne** zawierające informacje z ich tablic trasowania - na ich podstawie nowo włączony ruter wypełnia własną tablicę.
Pakiety aktualizacyjne rozsyłane są też okresowo bez żądania (zwykle co pół minuty). Jeśli pewien
ruter nie rozsyła pakietów przez dłuższy czas (zwykle 3 minuty), jest uznawany przez inne rutery za
uszkodzony / wyłączony i wiodące przez niego ścieżki są usuwane z tablic.
W działaniu protokołu RIP może wystąpić zjawisko **odliczania do nieskończoności** (counting to
infinity). Z tego powodu maksymalna liczba przeskoków w połączeniach obsługiwanych przez RIP
została ograniczona do 15.

ruter C ruter A ruter B

Czas rozprzestrzenienia informacji o awarii („czas zbieżności” sieci) jest dość długi, dlatego od 1996r.
pierwotna wersja protokołu RIP jest uznawana za przestarzałą (została zastąpioną wersją RIPv2).

Działanie protokołu OSPF bazuje na budowaniu przez rutery drzewa rozpinającego sieci o minimalnym
koszcie (przy zastosowaniu algorytmu Dijkstry). Rutery stosują następujące reguły:
- koszt osiągnięcia ich sieci lokalnych wynosi 0;
- koszt osiągnięcia sąsiednich sieci jest ustalany przez wysłanie pakietu Hello do sąsiednich ruterów;
- informacje o kosztach osiągnięcia sąsiadów są rozgłaszane (rozsyłane rozpływowo) pomiędzy
ruterami w celu zbudowania przez każdy ruter w swojej pamięci obrazu topologii sieci.
W przypadku, gdy duży system autonomiczny podzielony jest na obszary (z wyróżnionym obszarem
szkieletowym), drzewa rozpinające budowane są dla każdego obszaru oddzielnie. Trasy pomiędzy
ruterami umieszczonymi w różnych obszarach są trzyczęściowe: - w obrębie pierwszego obszaru;
- przez szkielet; - w obrębie drugiego obszaru.

Specyfikacja protokołu OSPF wyróżnia cztery klasy ruterów:
- rutery wewnętrzne (wszystkie ich połączenia leżą wewnątrz tego samego obszaru);
- rutery brzegowe (łączące dwa lub więcej obszary);
- rutery szkieletowe (rutery wewnętrzne szkieletu);
- rutery brzegowe AS (łączące się z ruterami brzegowymi w innych systemach autonomicznych).

Protokół BGP formalnie jest protokołem stosującym algorytm wektora odległości. Specyfikacja
protokołu BGP zawiera formę informacji wymienianej pomiędzy ruterami granicznymi. Wykorzystanie
tej informacji w poszczególnych systemach autonomicznych jest „zależne od polityki" (policy based)
i może uwzględniać nie tylko koszt przesyłu, ale i inne czynniki (np. arbitralnie określone „bezpieczeństwo trasy" itp.).

PROTOKOŁY WARSTWY TRANSPORTOWEJ

Na bazie protokołu internetowego (IP) zbudowane są dwa protokoły warstwy transportowej:

UDP

(User Datagram Protocol) - protokół bezpołączeniowy, zawodny;

TCP

(Transmission Control Protocol) - protokół połączeniowy, niezawodny.
Protokoły warstwy transportowej zapewniają łączność pomiędzy procesami wykonywanymi na dwóch
różnych komputerach (a w szczególnym przypadku też na jednym i tym samym komputerze), nie
ingerując w wybór trasy przesyłu informacji (to jest zadaniem podrzędnego względem nich protokołu
IP). Ponieważ na jednym komputerze może być wykonywanych wiele procesów jednocześnie, muszą
one korzystać z różnych „punktów kontaktowych", aby sobie wzajemnie nie przeszkadzały. Takie
logiczne obiekty służące jako „skrzynki nadawczo-odbiorcze" dla poszczególnych procesów nazywane są **portami**. Porty numerowane są liczbami dwubajtowymi dla każdego protokołu warstwy
transportowej oddzielnie.
Uwaga
Nie należy mylić powyższych portów z fizyczną przestrzenią portów danego komputera.

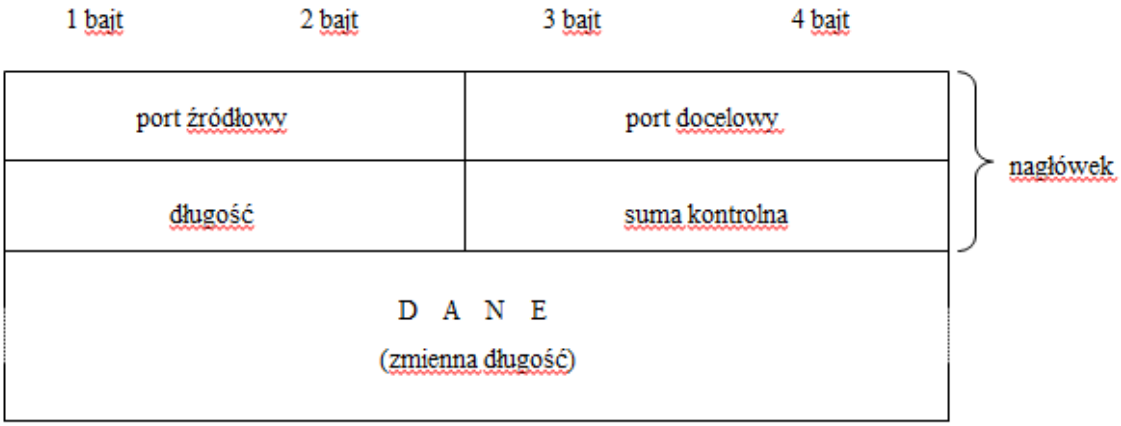
Aby dwa procesy mogły się skomunikować, należy określić elementy następującej piątki uporządkowanej:
(protokół, adres1, port1, adres2, port2).
Piątka taka nazywana jest **asocjacją** (skojarzeniem) (association).
Trójkę związaną z jednym tylko procesem:
(protokół, adres, port)
nazywamy **półasocjacją** (half-association), **adresem transportowym** (transport address) lub (co

pochodzi z terminologii związanej z Unixem BSD) **gniazdem** (socket). Konsekwentnie asocjacja
bywa też nazywana **parą gniazd** (socket pair), bo protokół jest wspólny dla obu półasocjacji.

Uwaga
Protokół IP pełni rolę „poczty zewnętrznej” dostarczając całość korespondencji od hosta do hosta
(multipleksując / demultipleksując przesyłki otrzymane od protokołów transportowych). Protokoły
transportowe obsługują „pocztę wewnętrzną” zbierając / rozdzielając przesyłki od / do poszczególnych
procesów („pracowników”) posiadających przyporządkowane porty („skrzynki na indywidualną
korespondencję”).
W praktyce z portów korzystają protokoły warstwy zastosowań (górne warstwy modelu OSI są na
ogół złączone w jeden moduł oprogramowania). Ponieważ praktycznie zawsze realizują one model
klient - serwer (pewna usługa jest udostępniana i czeka na zgłoszenia klientów), procesy klientów
muszą „wiedzieć”, do którego portu po stronie serwera należy się zgłosić, aby uzyskać określoną
usługę. W związku z tym istnieje zbiór **ogólnie znanych portów** (well-known port), które są przypo-
rządkowane standardowym, powszechnie używanym usługom - przykładowo serwer FTP (File
Transfer Protocol) przyjmuje zawsze zgłoszenia w porcie 21, serwer Telnet (usługi zdalnego terminala)
w porcie 23, a serwer HTTP (HyperText Transfer Protocol) - w porcie 80.

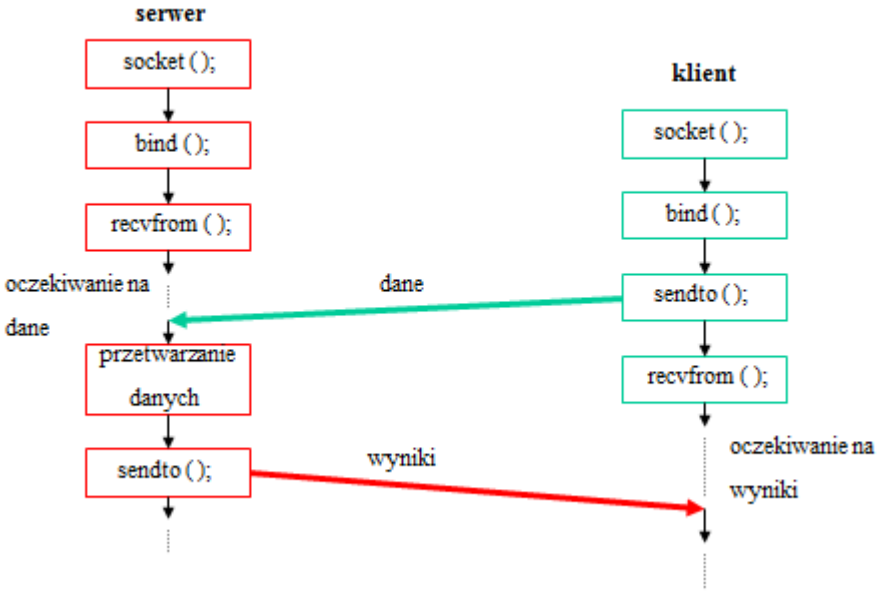
Numery portów są dwubajtowe, należą więc do przedziału 0 - 65535. Jako numery ogólnie znane
zostały zarezerwowane liczby 0 - 1023 (ich przyporządkowywaniem i administracją zajmuje się
organizacja IANA (Internet Assigned Numbers Authority)).
Numery 1024 - 49151 mogą być numerami **portów zarejestrowanych** (registered port) - IANA
nie sprawuje nad nimi nadzoru, ale na życzenie użytkowników rejestruje je i umieszcza w swoich
wykazach.
Numery powyżej 49151 mogą być dowolnie wykorzystywane - zwykle z tego zakresu wyznaczane są
porty do „doraźnego użytku” przez programy klienckie, jako tzw. **porty efemeryczne** (ephemeral
port). Klienci nie muszą mieć numerów portów przyporządkowanych na stałe i zazwyczaj po ich
doraźny przydział zgłaszają się do swojego systemu operacyjnego.
Uwaga
Niektóre usługi mogą być zrealizowane zarówno w oparciu o protokół TCP, jak i UDP - zwyczajowo
dla standardowych usług rezerwowane są te same numery portów zarówno TCP, jak i UDP, choćby
był wykorzystywany tylko jeden z nich.

Protokół UDP jest prostym protokołem bezpołączeniowym, operującym na jednostkach informacji
nazywanych **datagramami UDP** lub **komunikatami** (message). Struktura komunikatu:

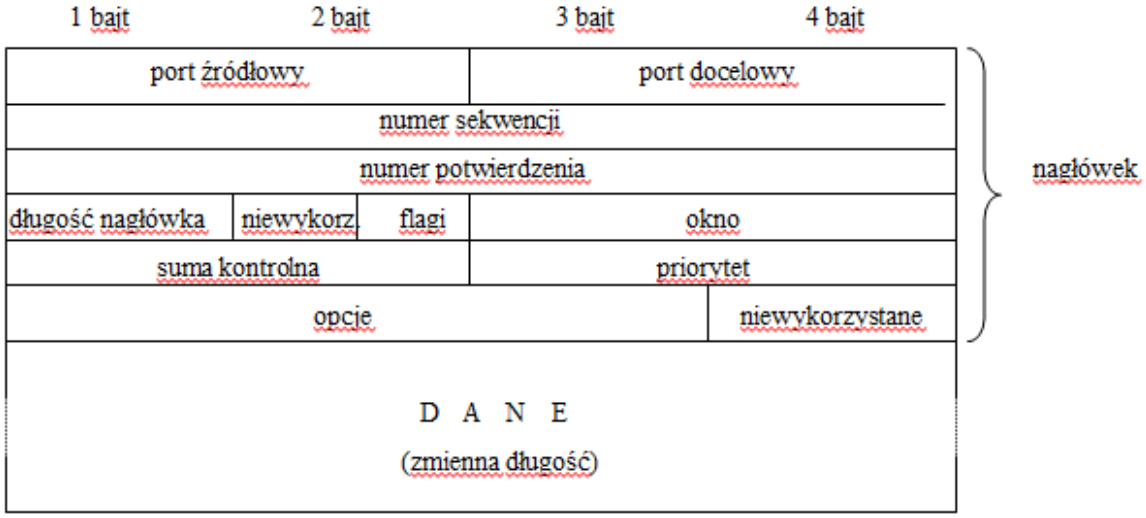


Numer portu źródłowego może być nieużywany (pole jest wtedy wyzerowane).
Długość jest łączną długością nagłówka i danych.
Suma kontrolna - w pewnym stopniu umożliwia sprawdzenie poprawności przesyłu komunikatu.

Obsługa komunikatu polega tylko na opakowaniu go przez protokół IP (dodaniu nagłówka IP) i przekazaniu go warstwie łącza. Zawodność protokołu UDP jest taka, jaka jest zawodność protokołu
IP na danej ścieżce w sieci.
Protokół UDP jest dość szybki ze względu na swoją prostotę. Jest stosowany głównie tam, gdzie
przesyłane porcje informacji są nieduże, gdzie występuje pojedyncza wymiana informacji („pytanie -
odpowiedź”), jak również w sieciach lokalnych (w których transmisja charakteryzuje się dużo większą niezawodnością, niż w skali całego Internetu). Przy niedużych ilościach przesyłanej informacji może bardziej się opłacać zapewniać niezawodność na poziomie programu użytkowego,
niż korzystać z wbudowanych mechanizmów protokołu TCP (uznawanego obecnie za dość powolny).
Schemat komunikacji bezpołączeniowej pomiędzy klientem a serwerem przy użyciu UDP



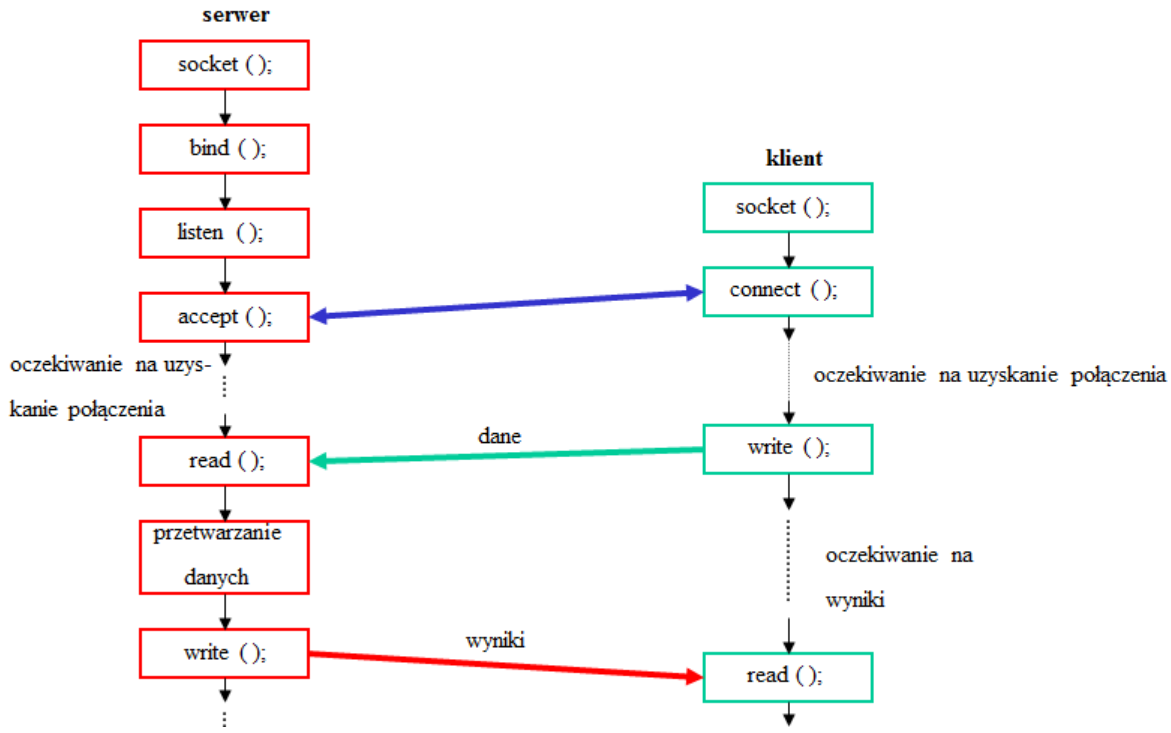
Protokół TCP jest protokołem połączeniowym (udostępniającym protokołom nadrzędnym łącze
logiczne przenoszące nieprzerwany ciąg bajtów o nieograniczonej długości), zapewniającym niezawodność transmisji poprzez stosowanie **numeracji** porcji informacji i **potwierdzeń** ich odebrania. Strumień bajtów otrzymany przez TCP od protokołu nadrzędnego jest dzielony na porcje
nazywane **segmentami**, których wielkość umożliwia opakowanie ich przez protokół IP i wysłanie
w postaci datagramów IP. Struktura segmentu:



Port źródłowy i docelowy - jak w protokole UDP (ale źródłowy musi być określony).
Numer sekwencji - liczba, od której protokół zaczyna odliczać wysyłane bajty.
Numer potwierdzenia - powiadamia drugą stronę, jaki numer sekwencji protokół spodziewa się

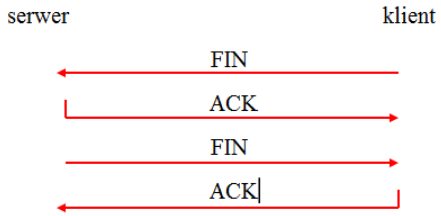
otrzymać w następnym segmencie (czyli stanowi potwierdzenie liczby
otrzymanych wcześniej bajtów).
Długość nagłówka - długość nagłówka TCP (w słowach 4-bajtowych)
Flagi - mogą informować, czy dany segment jest segmentem organizacyjnym (i jakiego rodzaju).
Okno - określa, ile bajtów protokół jest w stanie w danej chwili przyjąć do swojego bufora (żeby nie
powstało spiętrzenie).
Suma kontrolna - jak w protokole UDP.
Opcje - mogą na przykład określać maksymalny rozmiar segmentu, jaki protokół jest w stanie obsłużyć.

Schemat komunikacji połączeniowej pomiędzy klientem a serwerem przy użyciu TCP



Serwer jako pierwszy przygotowuje się do przyjęcia połączenia, wykonując funkcje *socket*, *bind*
i *listen* - jest to tzw. **otwarcie bierne** (passive open). Klient po pewnym czasie wywołuje funkcje
socket i *connect*, wykonując **otwarcie czynne** (active open). W odpowiedzi na to serwer wykonuje
funkcję *accept*. Naprzemienne wykonanie powyższych funkcji związane jest z utworzeniem stałego
połączenia poprzez **uzgadnianie trójfazowe** (three-way handshake). Segmenty organizacyjne, które
są w jego trakcie przesyłane, oznaczane są SYN (synchronization) i ACK (acknowledgement). Klient,
wykonując *connect*, wysyła SYN zawierający jego początkowy numer sekwencji (arbitralnie wybrany

przez protokół) i zawiesza swój proces, czekając na reakcję serwera. Serwer, wykonując *accept*,
wysyła (w jednym segmencie) swoje SYN (ze swoim początkowym numerem sekwencji) oraz ACK
(potwierdzające odbiór SYN klienta), a następnie zawiesza swój proces, czekając na reakcję klienta.
Klient następnie, wysyłając pierwszy segment z danymi, ustawia w nim flagę ACK i potwierdza
numer otrzymany od serwera.



Uwaga
W niektórych scenariuszach, aby zmniejszyć liczbę transmisji, ACK i FIN od serwera wysyłane są
w jednym segmencie. Ponadto FIN może być wysłany razem z ostatnią porcją danych.