# **Topologie**

**Topologia sieci komputerowej** – model układu połączeń różnych obiektów (linki, węzły itd.) sieci komputerowej. Określenie topologia sieci może odnosić się do konstrukcji fizycznej albo logistycznej sieci

**Topologia fizyczna** – opisuje fizyczną realizacje sieci komputerowej, jej układu przewodów, mediów transmisyjnych. Poza połączeniem fizycznym hostów i ustaleniem standardu komunikacji, topologia fizyczna zapewnia bezbłędną transmisje danych. Topologia fizyczna jest ściśle powiązana z topologią logiczną np. koncentratory, hosty.

**Topologia logiczna** – metoda dostępu urządzeń sieciowych do medium transmisyjnego. Można je podzielić na:

* Topologia rozgłoszenia
* Topologia przekazywania żetonu (tokenu)

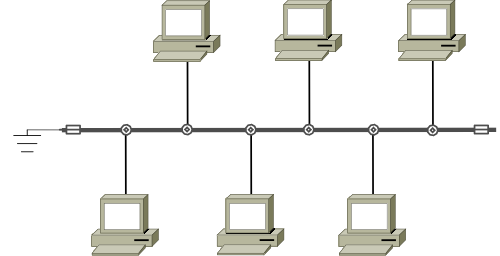
**Topologia rozgłoszenia** – polega na tym, że host wysyła dane do wszystkich hostów podłączonych do medium. Kolejność korzystania z medium według reguły kto pierwszy wyśle ten pierwszy zostanie obsłużony (ang. First came, first service). Przykładam są tutaj sieci Ethernet:

* IEEE 802.3 – 10 Mb Ethernet
* IEEE 802.3u – 100 Mb Ethernet
* IEEE 802.3x – Full Duplex Ethernet
* IEEE 802.3z – 1 Gb Ethernet

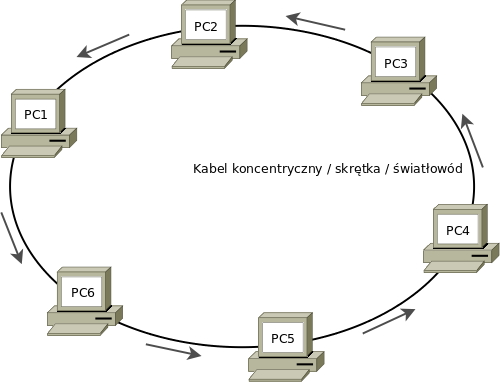
**Topologia przekazywania tokenu (żetonu)** – polega na kontrolowaniu dostępu do sieci poprzez przekazywanie elektronicznego tokenu. Host, który w danym momencie posiada token może korzystać z medium. W przypadku, gdy nie ma zadań przekazuje token kolejnemu hostowi i cykl się powtarza

* **IEEE 802.5** – token ring
* **IEEE 802.6** – sieci metropolitarne (MAN)
* **FDDI** (ang. Fiber Distributed Data Interface) – to standard transmisji danych, jest oparty na technologii światłowodowej. Transfer w tych sieciach wynosi 100 Mb/s. Sieć ta zbudowana jest z dwóch pierścieni (pierwotny, wtórny/zapasowy)

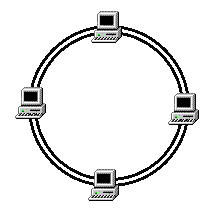
**Topologia liniowa (magistrali):**



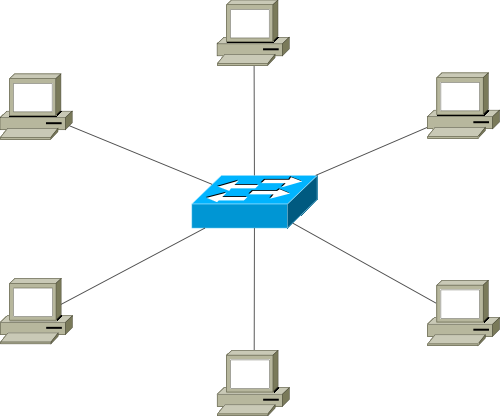
**Topologia pierścienia**



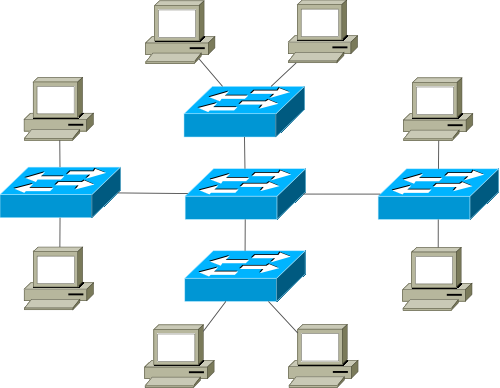
**Topologia podwójnego pierścienia:**



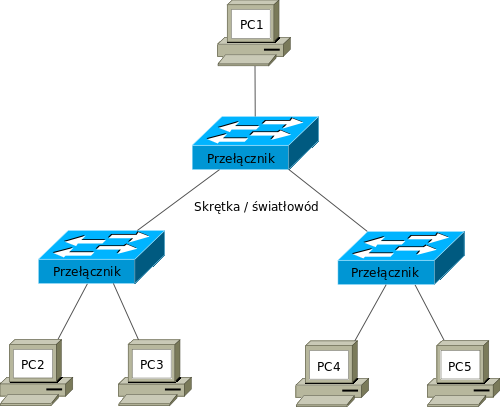
**Topologia gwiazdy:**



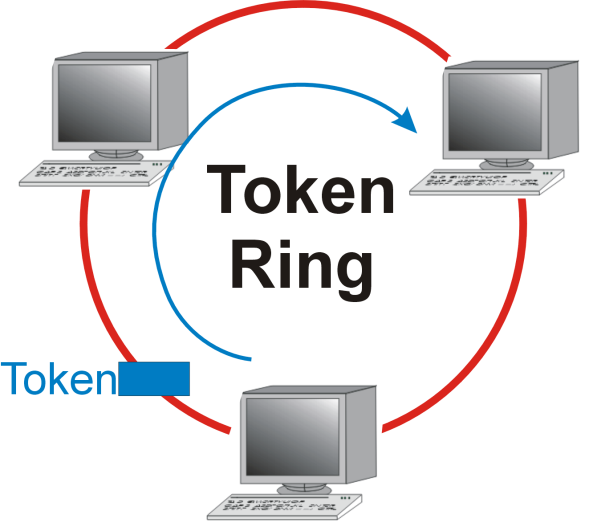
**Gwiazdy rozszerzonej:**



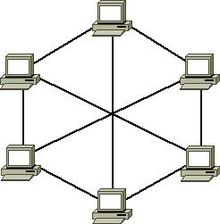
**Topologia hierarchiczna:**



**Topologia tokenu:**



**Topologia siatki (częściowa):**

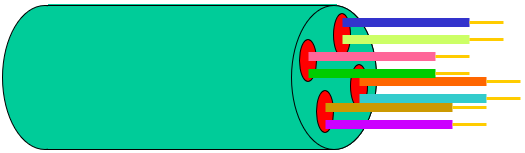


**Rodzaje okablowania:**

# **Okablowanie**

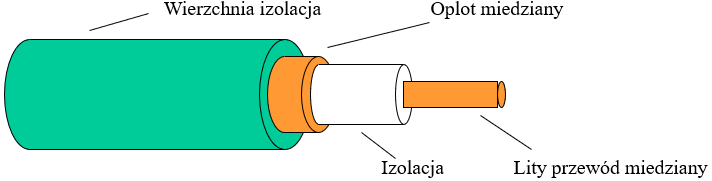
**Skrętka**

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

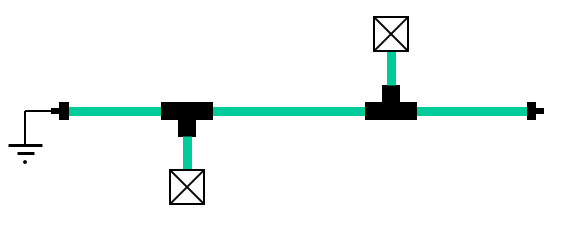


**Kabel koncentryczny**

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

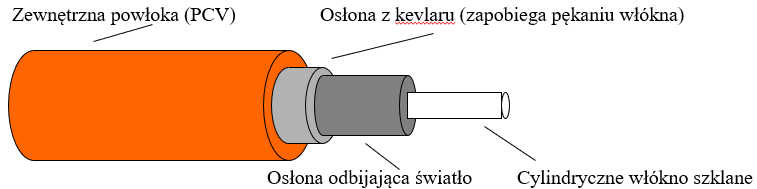


Do podłączenia koncentraka służą złączki BNC. Do jednego kabla może być podłączonych wiele stacji końcowych (za pomocą trójników i kabli dystansowych). Na końcach głównego kabla zakładane są terminatory, z których jeden powinien być uziemiony.



**Kabel światłowodowy**

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



# **Skrętka**

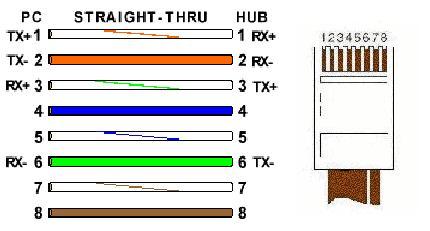
Kategoria skrętki według europejskiej normy EN 50171:

* **Kategoria 1** (Klasa A) – skrętka przeznaczona do przesyłania głosu. Obejmuje pasmo o częstotliwości do 100 kHz.
* **Kategoria 2** (Klasa B) – skrętka przeznaczona do nieco bardziej wymagających usług: aplikacji głosowych, usług terminalowych. Obejmuje pasmo o częstotliwości do 1 MHz.
* **Kategoria 3** (Klasa C) – pierwsza kategoria, która może być stosowana w sieciach komputerowych. Umożliwia transmisję danych o szybkości 10 Mb/s. Dawniej wykorzystywana w sieciach 10Base-T. Zbudowana ze skręconych ze sobą czterech par przewodów. Obejmuje pasmo o częstotliwości do 16 MHz.
* **Kategoria 5** (Klasa D) – pozwala na transmisję danych z szybkością do 1 Gb/s przy zachowaniu odległości do 100 m pomiędzy urządzeniami i częstotliwości 100 MHz.
* **Kategoria 5e** – ulepszona wersja kategorii 5.
* **Kategoria 6** (Klasa E) – umożliwia transmisję z częstotliwością do 200 MHz.
* **Kategoria 7** (Klasa F) – umożliwia transmisję danych w zakresie do 600 MHz. Osiągnięcie tego wymaga stosowania specjalnych złączy oraz izolowania każdej pary osobno.

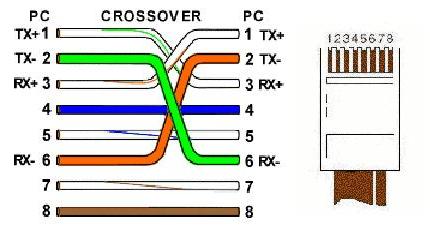
Skrętki komputerowe, czyli 4-parowe najczęściej zakańczamy wtyką RJ45. Takie kable nazywamy "patchcordami". Istnieją dwa schematy połączeń.

**Schematy budowy patchcordów komputerowych:**

* **Skrętka z połączeniem prostym (straight-through)** – Taki kabel głównie stosujemy do połączenia Ethernet karty sieciowej w komputerze z koncentratorem (np. routerem).



* **Skrętka z połączeniem krzyżowym (cros-over)** – Takie połączenie stosujemy do połączenia dwóch komputerów bez koncentratora, czasem przy połączeniu dwóch koncentratorów.



**Ethernet (IEEE 802.3)** jest najszerzej wykorzystywaną technologią w sieciach lokalnych (LAN). Na przestrzeni wielu lat od powstania technologii Ethernet rozwijały i nadal rozwijają się różne jego wersje różniące się szybkością transmisji (czasem również kilkoma różnicami w realizacji tej transmisji). Te wersje to Ethernet, Fast Ethernet, Gigabit Ethernet i 10 Gigabit Ethernet.

**Wersje Ethernet**

Najbardziej popularną na dzień dzisiejszy wersją Ethernet jest Ethernet 100 Mb/s, który nazywany jest jako Fast Ethernet. Oryginalny Ethernet działał z przepływnością 10 Mb/s. Kolejnymi wersjami są Gigabit Ethernet pracujący z szybkością 1Gb/s (1000 Mb/s) i 10 Gigabit Ethernet z szybkością 10 Gb/s.

**Standardy definiujące poszczególne wersje Ethernet to:**

* **10 Mb/s (Ethernet)**
  + IEEE 802.3, 10Base5 Ethernet, topologia szyny, do 500m segment
  + IEEE 802.3a, 10Base2 Ethernet, topologia szyny, do 185m segment
  + IEEE 802.3i, 10Base-T Ethernet, topologia gwiazdy, do 100m segment
  + IEEE 802.3j, 10Base-FL Ethernet, topologia gwiazdy, do 2000m segment
* **100 Mb/s (Fast Ethernet)**
  + IEEE 802.3u, 100Base-TX Fast Ethernet, topologia gwiazdy, do 100m segment
  + IEEE 802.3u, 100Base-FX Fast Ethernet, topologia gwiazdy, do 100m segment
* **1 Gb/s (Gigabit Ethernet)**
  + IEEE 802.3z, 1000Base-LX Gigabit Ethernet, topologia gwiazdy, do 310m segment
  + IEEE 802.3z, 1000Base-SX Gigabit Ethernet, topologia gwiazdy, do 310m segment
  + IEEE 802.3z, 1000Base-CX Gigabit Ethernet, topologia gwiazdy, do 310m segment
  + IEEE 802.3z, 1000Base-T Gigabit Ethernet, topologia gwiazdy, do 25m segment
* **10 Gb/s (10 Gigabit Ethernet)**
  + IEEE 802.3ae - 10 Gigabit Ethernet

# **Światłowód**

**Światłowód** (fiber optic cable) to:

* Nośnik umożliwiający przenoszenie sygnałów o wyższych częstotliwościach spektrum elektromagnetycznego, czyli światła;
* Kabel optotelekomunikacyjny stosowany do budowy lokalnych bądź rozległych połączeń światłowodowych, zbudowany z wielu (nawet kilkuset) włókien optycznych

**Światłowód** – w światłowodach do transmisji informacji wykorzystywana jest wiązka światła, która jest odpowiednikiem prądu w innych kablach. Wiązka ta jest modulowana zgodnie z treścią przekazywanych informacji. To rozwiązanie otworzyło nowe możliwości w dziedzinie tworzenia szybkich i niezawodnych sieci komputerowych. Właściwie dobrany kabel może przebiegać w każdym środowisku. Szybkość transmisji może wynosić nawet 3 Tb/s.

Światłowód jest wykonany ze szkła kwarcowego, składa się z rdzenia (złożonego z jednego lub wielu włókien), okrywającego go płaszcza oraz warstwy ochronnej. Dielektryczny kanał informatyczny eliminuje konieczność ekranowania. Transmisja światłowodowa polega na przepuszczeniu przez szklane włókno wiązki światła

Światłowody wykonuje się zasadniczo jako jednomodowe i wielomodowe. Światłowody wielomodowe, można podzielić na dwa typy: o współczynniku skokowym i gradientowym najczęściej spotykane są światłowody o płynnej zmianie współczynnika załamania pomiędzy rdzeniem a płaszczem.

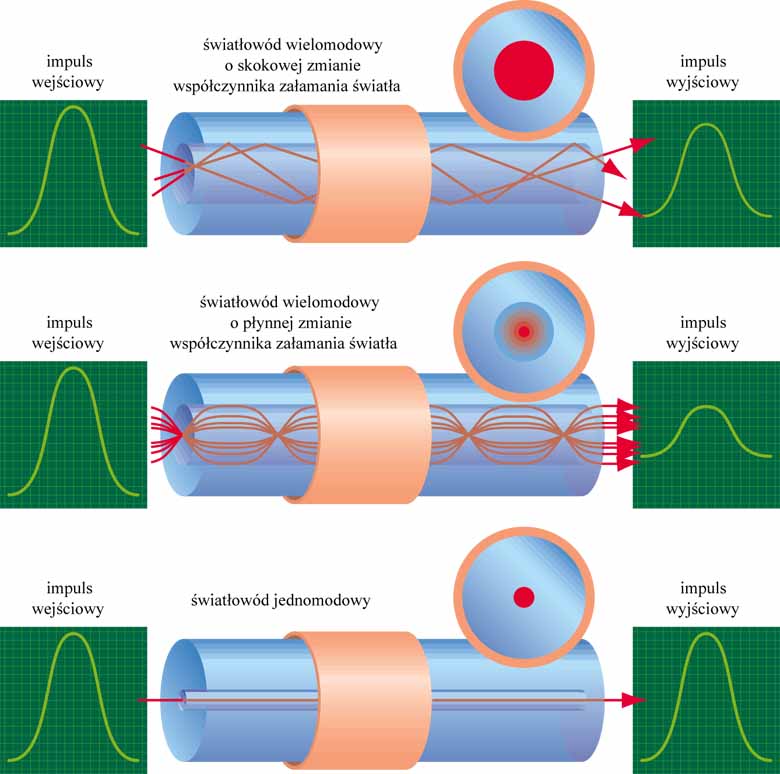
**Światłowody dzielą się na:**

* Jednomodowe
* Wielomodowe
  + Gradientowe
  + Skokowe
* Wewnętrzne i zewnętrzne

**W światłowodzie jednomodowym**, przenosi się tylko jeden mod. Oznacza to, że wszystkie promienie odbijane są pod tym samym kątem do powierzchni płaszcza. Wszystkie promienie mają wiec jednakową drogę do przebycia i zajmuje to taki sam czas. Oznacza to, że nie powstaje dyspersja. Światłowody jednomodowe są lepsze. Umożliwiają transmisję danych bez ich wzmacniania na odległość do 150 km.

**W wielomodowym światłowodzie**, jest możliwość występowania różnych kątów odbicia i w związku z tym następuje rozmycie krawędzi przesyłanego sygnału, czyli dyspersja.

**Dyspersja** – rozmycie krawędzi przesyłanego sygnału

  
**Zalety światłowodu**

* Wysoka jakość
* Duża szybkość
* Brak zakłóceń przez pole elektromagnetyczne
* Szerokie pasmo transmisji
* Możliwość połączenia na dużą odległość
* Niezawodność
* Bezpieczeństwo
* Mała waga i wymiary, trwałość

**Światłowód składa się z 3 części:**

* **Rdzeń** – jego grubość wynosi w zależności od rodzaju światłowodu od 5 do 50 mikronów. Zbudowany jest najczęściej ze szkła kwarcowego lub plastiku, rzadziej z innych rodzajów szkieł lub materiałów krystalicznych, jak np. szafir.
* **Płaszcz** – jego średnica to ok. 125 µm. Jest wykonany z materiału o mniejszym współczynniku załamania światła niż rdzeń. Najczęściej są to plastiki, lecz niekiedy także stosuje się szkła z odpowiednimi domieszkami.
* **Pokrycie** – jego zadaniem jest chronienie płaszcza i rdzenia przed mikropęknięciami. Wykonane jest z elastycznych materiałów, jak np. akryl. W procesie technologicznym najczęściej składa się z dwóch lub więcej warstw; łączna średnica to ok. 250 µm.

# **Sieć bezprzewodowa**

**Sieć bezprzewodowa** używa fal elektromagnetycznych (radiowych lub podczerwonych) do przesyłania informacji z jednego punktu do drugiego bez użycia medium fizycznego. Fale radiowe często są traktowane jako radiowy nośnik, ponieważ po prostu pełnią funkcję dostarczania energii do zdalnego odbiornika. Transmitowane dane są nakładane na nośnik radiowy tak, aby mogły być dokładnie wydobyte w punkcie odbioru. Zwykle określa się to modulacją nośnika przez informację przesyłaną. Gdy dane są nakładane (modulowane) do nośnika radiowego, sygnał radiowy zajmuje więcej niż pojedynczą częstotliwość, ponieważ częstotliwość lub (bit rate) modulowanej informacji dodaje się do nośnika. Wiele radiowych nośników może współistnieć w tym samym miejscu o tym samym czasie bez wzajemnej interferencji, jeśli fale radiowe są transmitowane na różnych częstotliwościach.

**Standardy sieci bezprzewodowych**

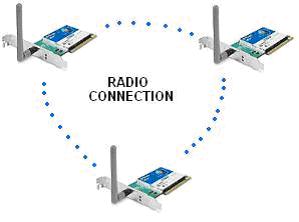
* **802.11a** wykorzystuje częstotliwość 5 GHz. Jego podstawowa prędkość to 54 Mb/s, ale w praktyce działa najlepiej w granicach 20 Mb/s. Mniejsze dopuszczalne prędkości to 48, 36, 34, 18, 12, 9 oraz 6 Mb/s. 802.11a obejmuje 12 niezachodzących kanałów, 8 przeznaczonych do pracy w budynkach oraz 4 przeznaczone do pracy między dwoma punktami (point to point). Istniały pewne próby uregulowania tego zakresu częstotliwości przez niektóre kraje, ale dziś większość państw pozwala na niekoncesjonowane wykorzystanie pasma dla 802.11a.
* **802.11b** ma zasięg 46 m w pomieszczeniu i 96 m na otwartej przestrzeni, aczkolwiek dane te mogą ulec zmianie przy zastosowaniu innych anten. Standardowe anteny wykorzystywane w urządzeniach 802.11b pozwalają zwykle na przekaz z przepływnością 11 Mb/s. Sprawność protokołu obniża tę przepływność do 5,5 Mb/s. Jednak materiały takie jak metal, woda lub beton znacznie pochłaniają fale i obniżają jakość sygnału. Standard 802.11b przewiduje wykorzystanie algorytmów do wykrywania sygnałów zagłuszających oraz unikania kolizji podczas komunikacji wielu radiowych kart sieciowych.
* **802.11g**. Pracuje on podobnie jak 802.11b na częstotliwości 2,4 GHz, ale pozwala na transfer z prędkością 54 Mb/s. Standard 802.11g jest całkowicie zgodny w dół ze standardem 802.11b
* **802.11n.** Umożliwia urządzeniom pracę na częstotliwościach 2,4 GHz lub 5 GHz i osiągnięcie maksymalnej przepustowości 600 Mbit/s na jeden kanał o szerokości 40 MHz. Producenci zapowiadają już udostępnienie urządzeń Wi-Fi oferujących przepustowość nawet na poziomie 1 Gbit/s. W standardzie 802.11n zrezygnowano z technik podziału czasu i częstotliwości. W sieciach 802.11n dane są transmitowane na tej samej częstotliwości i w tym samym czasie. Aby sygnały nie zakłócały się, wykorzystano zalety koncepcji dywersyfikacji przestrzennej (ang. spatial diversity), która zakłada oddzielenie transmisji poszczególnych użytkowników poprzez wykorzystanie wielu anten.
* **802.11 ac.** Standard 802.11ac znany również jako „Gigabit Wi-Fi” to kolejna, piąta już generacja sieci bezprzewodowych, której głównym celem jest zapewnienie prędkości połączenia przekraczającej 1 Gbps. Specyfikacja standardu zakłada prace wyłącznie w paśmie 5 GHz, a więc kompatybilność wsteczna będzie zapewniona tylko dla urządzeń działających w tym paśmie (802.11a/n).  
  Standard 802.11ac w stosunku do swojego poprzednika stanowi bardziej ewolucje niż rewolucje. Wiele technik zapoczątkowanych i stosowanych przez 802.11n zostało rozszerzonych oraz wykorzystanych w standardzie 802.11ac. Z tego względu warto zapoznać się z naszymi wcześniejszym raportami opisującymi standard 802.11n: Nowe możliwości sieci bezprzewodowych - Standard 802.11n oraz Technologia MIMO w sieciach 802.11abgn.

**Główne udoskonalenia wprowadzone przez standard 802.11ac obejmują:**

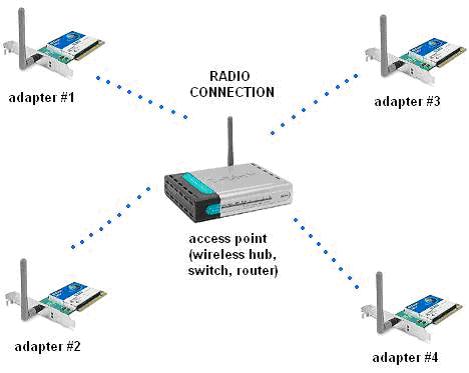
* Większe szerokości kanałów
* Poprawiona modulacja
* Zwiększona ilość strumienie przestrzennych
* Multi-user MIMO (MU-MIMO)
* Ujednolicony beamforming
* Zaktualizowany mechanizm RTS/CTS
* Zwiększony maksymalny rozmiar zagregowanej marki A-MPDU

**Standard IEEE 802.11**, określa zasady pracy urządzeń do transmisji bezprzewodowej w sieciach lokalnych. Został zdefiniowany w roku 1997 przez IEEE, a później zaakceptowany przez ETSI pod symbolem ETS 300 328. W standardzie tym przewiduje się dwie konfiguracje sprzętowe:

* **Sieć tymczasowa (ad-hoc)**, która nie posiada elementów stałych (brak punktu dostępowego) Sieci tymczasowe tworzy się zazwyczaj na czas spotkań, konferencji, itp. Sieci te nie posiadają dostępu do sieci przewodowej. Służą jedynie do wymiany informacji między klientami mobilnymi.



* **Sieć stacjonarna** (infrastructure), która zawiera elementy stałe oraz połączenie z siecią przewodową. Sieci stacjonarne mają zdecydowanie bardziej złożoną strukturę. Klienci nie łączą się już między sobą, ale podłączają się do punktu dostępowego (ang. access point), który ma dostęp do sieci przewodowej i pośredniczy w łączności między obiema sieciami.



# **Anteny**

**Antena** – urządzenie służące do zamiany fal elektromagnetycznych na sygnał elektryczny i odwrotnie. Jest elementem składowym każdego systemu radiokomunikacji. W XX w. najbardziej znanym typem anteny była antena odbiornika radiowego i antena telewizyjna; w XXI w. częściej kojarzona z elementem bezprzewodowych sieci komputerowych lub z odbiorem sygnałów z satelitów.

Ze względu na polaryzację możemy podzielić na:

* Liniową (pionowa, pozioma, +45°, -45°)
* Eliptyczną
  + Lewoskrętną
  + Prawoskrętną

Ze względu na sposób wykonania anteny dzielimy na:

* Dipolowe
* Kolinerane
* Mikropaskowe
* Szczelinowe
* Reflektorowe

**Antena dipolowa** – najstarsza, lecz najbardziej popularna antena. Słowo dipol pochodzi z greckiego i oznacza układ dwubiegunowy. Antena dipolowa składa się przeważnie z dwóch symetrycznych ramion zasilanych za pomocą symetrycznej linii transmisyjnej. Tego typu antena jest tzw. anteną symetryczną, ponieważ prądy płynące w obu ramionach są równe co do amplitudy i mają przeciwne zwroty

**Antena dookólna** – antena, której spadek mocy promieniowania wzdłuż wektora H jest nie większy niż 3 dB (połowa mocy). Najważniejszą cechą tej anteny jest charakterystyka promieniowania, która w tym przypadku jest dookólna. Oznacza to, że fala elektromagnetyczna wytworzona przez taką antenę rozchodzi się z jednakowym natężeniem we wszystkich kierunkach w płaszczyźnie poziomej.

**Antena kierunkowa** – jest to antena promieniująca prawie całą moc, w jednym wyróżnionym kierunku. Zysk wynosi nawet kilkadziesiąt dBi. Kształt charakterystyki promieniowania anteny jest przeważnie szpilkowy.

**Antena Yagi** – właściwie antena Yagi-Uda. Obecnie anteny te znalazły szerokie zastosowanie głównie do odbioru fal o długościach metrowych, decymetrowych, między innymi w odbiorze telewizji, sieciach radiowych typu WLAN, a także w telekomunikacji. Antena stosowana jest m.in do łączenia access pointa oraz anteny głównej w sieciach radiowych. Są także powszechnie stosowane przez krótkofalowców w pasmach 6m (50-52MHz), 2m (144-146MHz) i 70cm (430-440MHz).

**Antena satelitarna** – jest to antena paraboliczna zaprojektowana, aby odbierać i/lub nadawać sygnał z satelitów telekomunikacyjnych. W antenach satelitarnych sygnał odbija się od płaszcza anteny a następnie jest kierowany do konwertera.

**Antena panelowa** – potoczna nazwa anteny radiowej o płaskiej budowie. Najczęściej w hermetycznej obudowie umieszczony jest w tylnej części anteny płaski ekran pozwalający na maksymalne skupienie odbitej fali radiowej. W przedniej części obudowy umieszczony jest dipol lub zespół dipoli, które połączone są z urządzeniem radiowym za pomocą kabla koncentrycznego. Zysk energetyczny anteny panelowej. Osiąga od kilku do kilkunastu dBi.

# **Model OSI**

**Model OSI** (Open System Interconnection) powstał pod kontrolą Międzynarodowej Organizacji Normalizacyjnej (ISO – International Organization for Standarization). Został opracowany w celu ułatwienia realizacji otwartych (obsługiwane w środowiskach wielosystemowych) połączeń systemów komputerowych. Model ten umożliwiał współdziałanie urządzeń i oprogramowania od różnych producentów.

Model OSIzbiera w logicznie ułożone warstwy funkcje potrzebne do zdefiniowania, nawiązania i utrzymania komunikacji między dwoma (lub więcej) urządzeniami niezależnie od ich producenta i architektury. Procesy zachodzące podczas komunikacji dzielone są na 7 warstw funkcjonalnych, które zbudowane są w oparciu o naturalny ciąg zdarzeń zachodzących w czasie sesji komunikacyjnej.

**Warstwy te to:**

1. **Warstwa fizyczna** – najniższa warstwa odpowiedzialna za transmisję strumienia bitów,
2. **Warstwa łącza danych** – odpowiedzialna za poprawność przesyłanych danych,
3. **Warstwa sieciowa** – umożliwia współpracę pomiędzy sieciami, wybiera optymalną trasę transmisji danych,
4. **Warstwa transportu** – pełni funkcję zbliżoną do warstwy drugiej z tą różnicą, że odpowiada za końcową integralność transmisji także poza lokalną siecią,
5. **Warstwa sesyjna** – zarządza przebiegiem komunikacji podczas połączenia między dwoma komputerami (określa czy komunikacja może zachodzić w jednym czy dwóch kierunkach),
6. **Warstwa prezentacji** – odpowiedzialna za sposób kodowania danych,
7. **Warstwa aplikacji** – pełni rolę interfejsu pomiędzy aplikacjami użytkownika a usługami sieci.

**Protokoły komunikacyjne poszczególnych warstw grupuje się w kategorie:**

* **Protokoły aplikacji -** obejmują warstwy: aplikacji, prezentacji i sesji. Zapewniają wzajemne oddziaływanie aplikacji i wymianę danych. Przykłady: FTP, Telnet, SMTP, SNMP, Net BIOS, ...
* **Protokoły transportowe -** realizują połączeniowe usługi przesyłania danych, zapewniają wymianę danych pomiędzy systemami końcowymi w sposób sekwencyjny Przykłady: TCP, SPX, NetBIOS, NetBEUI.
* **Protokoły sieciowe -** zapewniają usługi łączy dla systemów komunikacyjnych, obsługują adresowanie i informację routingu, weryfikację błędów oraz żądania retransmisji. Obejmują również procedury dostępu do sieci określone przez wykorzystywany rodzaj sieci. Przykłady: IP, IPX.

**Protokół** – zdefiniowany sposób komunikowanie się z innym systemem

**Pakiet** – rodzaj „paczki danych” przesyłanej między urządzeniami przy wykorzystaniu łącza komunikacyjnego

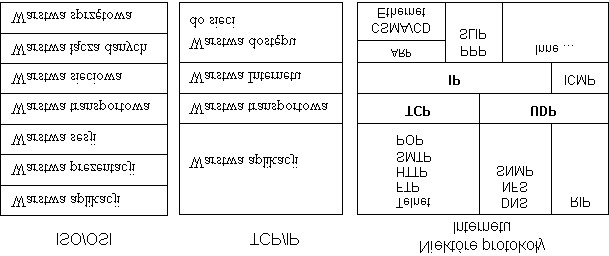
**Ramka** – strumień danych przesyłany przez połączenie fizyczne

# **TCP/IP**

W obrębie TCP/IP działa dużo innych protokołów, za pomocą których dane podróżują po sieci. Są one podzielone na warstwy.

**Podsumowując, protokół TCP/IP dzieli się na 4 warstwy od najważniejszej:**

* Warstwa fizyczna dostępu do sieci
* Warstwa Internet (sieciowa, międzysieciowa, warstwa IP)
* Warstwa transportowa
* Warstwa aplikacji (zastosowań)



**Warstwa dostępu do sieci** odpowiada za dostarczanie danych do innych urządzeń bezpośrednio dołączonych do sieci. Współpracuje ona bezpośrednio ze sprzętem i sterownikami odpowiedzialnymi za współpracę z siecią Ethernet. W przypadku innych sieci mogą to być protokoły PPP, SLIP lub inne. Warstwa ta współpracuje więc z interfejsem sieciowym (kartą sieciową), modemem lub innym urządzeniem pozwalającym na bezpośrednie połączenie dwóch lub więcej komputerów i separuje resztę warstw od zastosowanych rozwiązań fizycznych (niskopoziomowych). Świadczy ona usługę warstwie wyższej polegającą na wysyłaniu i odbieraniu porcji danych (zwanych ramkami) z komputerów w danej sieci fizycznej.

**Warstwa Internet** (IP) odpowiada za dostarczanie danych do urządzeń nie tylko w danej sieci fizycznej. Organizuje ona ruch tzw. pakietów IP między poszczególnymi sieciami fizycznymi połączonymi w intersieć. Korzysta z usług warstwy dostępu do sieci, sama zaś świadczy usługi dostarczania pakietu do dowolnego komputera w Internecie.

**Warstwa transportowa** odpowiedzialna jest za niezawodną wymianę danych z dowolnym komputerem w Internecie. Organizuje też i utrzymuje tzw. sesje, czyli wirtualne połączenia między komputerami. Korzysta z warstwy IP, sama zaś dostarcza usług niezawodnego transportu danych.

**Warstwa zastosowań** jest najwyżej położona. Tej warstwie odpowiadają wszelkie programy (aplikacje) internetowe korzystające z warstwy transportowej. Tu znajdują się wszelkie konkretne zastosowania Internetu - przesyłanie plików (FTP), poczty (SMTP) i inne.

**Składa się ona z dwóch protokołów:**

* **IP** - **I**nternet **P**rotocol - jest protokołem warstwy sieciowej, oddziela on wyższe warstwy od znajdującej się poniżej sieci i obsługuje adresowanie i dostarczanie danych.
* **TCP** - **T**ransmission **C**ontrol **P**rotocol - jest protokołem warstwy transportowej, gwarantuje, że odbiorca otrzyma dane dokładnie w tej samej postaci, w jakiej zostały wysłane.

**Dodatkowe pojęcia:**

* **DTE** (data terminal equipment) - urządzenie terminalowe danych lub inaczej stacja, jest unikalnym, zaadresowanym urządzeniem w sieci.
* **Urządzenie nadawczo-odbiorcze** (transceiver) – urządzenie, które umożliwia stacji transmisje „do” i „z” któregoś ze standardowych mediów normy IEEE 802.3. Dodatkowo transceiver Ethernetowy zapewnia izolację elektryczną pomiędzy stacjami oraz wykrywa i reaguje na kolizje.
* **MAU** (Medium Attachement Unit) moduł dołączania medium jest jednym z określeń IEEE na transceiver. Karta sieciowa najczęściej ma zintegrowany wewnątrz transceiver.
* **AUI** (Attachment Unit Interface) - połączenie pomiędzy kontrolerem i transceiverem. Aktualnie prawie nie występuje, był to rodzaj kabla i gniazdek, do komunikowania się karty sieciowej z dołączanymi do niej transceiverami. Dopiero transceiver mógł zostać podłączony do medium transmisyjnego (np.: koncentryk, skrętka)
* **Segment** – część okablowania sieci ograniczona przez mosty (bridge), przełączniki (switche), rutery, wzmacniaki lub terminatory. Najczęściej połączenie między dwoma komputerami lub koncentratorem i komputerem (dla skrętki i światłowodu), lub jeden odcinek kabla koncentrycznego łączącego wiele urządzeń.

# **TCP/UDP i usługi sieciowe**

Protokoły w. łącza danych (np. Ethernet) oraz w. sieciowej (IP) pozwalają tylko na zaadresowanie komputera (interfejsu sieciowego), a komunikacja zachodzi pomiędzy procesami (aplikacjami)

Do adresowania wybranej aplikacji stosuje się numer portu – adres warstwy transportowej (TCP)

Numer portu jest dwubajtowy (0-65535)

Według specyfikacji URL numer portu dodajemy po nazwie hosta i dwukropku

Pominięcie numeru portu oznacza, że zostanie użyty numer portu domyślny dla danej usługi

Łącze wymaga numerów portów po obu stronach

Najpopularniejsze usługi mają przydzielone specjalne porty, na których standardowo nasłuchują ich procesy serwerów

Usługi w. transportowej są ograniczane możliwościami w. sieci (przepustowość, opóźnienie), ale mogą (nie muszą) oferować jakościowo nową funkcjonalność

Niezawodność połączenia (izoluje proces komunikacji od zawodności w. sieci)

Oferowanie połączenia logicznego (mimo iż komunikacja w w. sieci jest pakietowa)

Oferowanie bezpieczeństwa komunikacji, np. poprzez szyfrowanie danych, mimo iż pakiety podróżują przez nieznane systemy

Kontrola przeciążenia łącza

Multipleksowanie/demultipleksowanie

**Protokół UDP (User Datagram Protocol):**

* Usługa: bezpołączeniowe dostarczenie datagramów
* Nie kontroluje poprawności i prędkości przesyłu
* Minimalizuje przesył dodatkowych danych

**Protokół TCP (Transfer Control Protocol):**

* Usługa: połączeniowe, niezawodne przesyłanie danych (strumień)
* Odpowiada za segmentowanie i powtórne scalanie danych, kontroluje prędkość przesyłu
* Wykorzystuje potwierdzenie z retransmisją (wysyła dane aż do otrzymania potwierdzenia)

**Połączenie pomiędzy aplikacjami odbywa się zwykle w architekturze klient-serwer (TCP/UDP)**

* Jedna aplikacja oczekuje na połączenie (serwer), druga je inicjuje (klient)
* Zakłada się, że transfer danych będzie w większości przebiegał od serwera do klienta, klienci nie komunikują się ze sobą

**Możliwa jest inna architektura: symetryczne połączenie pomiędzy równorzędnymi hostami (często UDP, ale możliwe też TCP)**

* Wykorzystanie: sieci P2P, telefonia internetowa
* Połączenie takie można traktować jako złożenie dwóch połączeń klient-serwer

**Protokoły TCP i UDP uzupełniają się, wybieramy jeden z nich w zależności od potrzeb**

**TCP**

* Gdy zależy nam na pewności połączenia i nie tolerujemy utraty danych
* Cena: mniejsza wydajność wykorzystania łącza
* Połączenie jest automatycznie ograniczane, gdy rośnie zajętość łącza
* Odpowiednie dla: poczta, zdalne logowanie, WWW, transfer plików

**UDP**

* Gdy zależy nam na maksymalnej wydajności i tolerujemy utratę danych (albo sami implementujemy niezawodność w warstwie wyższej!)
* Cena: bardziej skomplikowana implementacja
* Nie podlegamy automatycznemu ograniczaniu prędkości (dobrze dla nas, źle dla Internetu ...)
* Odpowiednie dla: strumieniowe multimedia, telefonia VOIP, routing, DNS, sieci P2P

**Firewall** to urządzenie działające w warstwie transportowej, kolejne w hierarchii urządzeń sieciowych

* Musi rozpoznawać nie tylko numery IP, ale także numery portów TCP/UDP
* Może sterować ruchem (przepuszczać/blokować lub sterować prędkością) na podstawie numerów portów (w domyśle – usług)
* Realizacja: filtrowanie pakietów

**Gateway** to urządzenie działające w warstwie aplikacji

* Do przepuszczenia połączenia wymagana jest autentykacja na urządzeniu
* Zwykle granulacja jest na poziomie usług (kolejna usługa wymaga nowego logowania)

**Serwer proxy** to kolejny sposób dostępu do Internetu z jednoczesną izolacją sieci lokalnej

* Dla każdej usługi na serwerze proxy uruchamiany jest oddzielny program, który przekazuje i jednocześnie buforuje komunikaty przekazywane pomiędzy sieciami
* Może być tradycyjny (wymaga logowania) lub przezroczysty („transparent proxy”)
* Najczęściej łączony z technologią NAT – adresy w sieci lokalnej są nieroutowalne
* Pakiety nigdy nie przechodzą pomiędzy sieciami, są zawsze buforowane i ponownie wysyłane przez serwer proxy