

Podstawy lokalnych Sieci i Topologii Komputerowych.

1. Podstawowe zagadnienia dotyczące Sieci Komputerowych.

Sieć Komputerowa – jest systemem komunikacyjnym służącym do przesyłania i wymiany danych między przynajmniej dwoma hostami, lub innymi urządzeniami sieciowymi i peryferiami.

Podział sieci na ich typy:

PAN – Sieci Osobiste, sieci o zasięgu dosłownie kilku metrów, lub mniejszym głównie wykorzystywane przez mniejsze urządzenia sieciowe np. telefony w celu wymiany danych, lub peryferia np. Mysz bezprzewodową.

LAN – Sieci Lokalne, Sieci łączące użytkowników na niewielkim obszarze, zwykle dom, biuro, serwerownia, budynek. Prędkość przesyłania danych w sieciach LAN jest o wiele większa, posiada także o wiele większą przepustowość.

MAN – Sieci Miejskie, Sieci głównie o zasięgu Miejskim, najczęściej charakteryzują się oparciem o nowsze media transmisyjne np. światłowody, zdecydowanie większa przepustowość łącza, zwykle zrzeszają np. uczelnie, urzędy, ośrodki naukowe znajdujące się w aglomeracji miejskiej.

WAN – Sieci Rozległe, Sieci, których zasięg przekracza granice miast, państw lub kontynentów. Składają się z węzłów i łączących je łączy transmisyjnych realizowanych za pomocą publicznej sieci komunikacyjnej. Sieć taka zwana jest także Globalną lub Światową. Przykładem tak ogromnej sieci jest sam „Internet”. Zrzesza wszystkie możliwe zasoby teleinformatyczne.

Elementy Sieci Komputerowych (Sprzętowe):

- **Urządzenia transmisji** – Nośniki używane do transportu sygnałów biegnących przez sieć do miejsca docelowego. Najczęściej stosowane nośniki to: światłowody, kable miedziane. Nośniki również mogą być niematerialne np. fale radiowe lub świetlne.
- **Urządzenia dostępu** – Są odpowiedzialne za formatowanie danych i przekazywanie ich do nośników, a także odbieraniem ich. W sieci lokalnej urządzeniami takimi są karty sieciowe. Natomiast w sieciach rozległych są to modemy.
- **Urządzenia wzmacniania przesyłanych sygnałów** – Urządzenia które odbierają przesyłane sygnały, wzmacniają je a następnie wprowadza ponownie do sieci. W sieciach lokalnych funkcję taką pełni Koncentrator.

Elementy Sieci Komputerowych (Programowe):

- **Protokoły** – określają sposoby komunikowania się urządzeń, przykładem protokołu może być protokół IP.
- **Sterowniki urządzeń** – Programy umożliwiające działanie urządzeniom takim jak karty sieciowe.
- **Oprogramowanie komunikacyjne** – Korzysta ono z protokołów i sterowników w celu wymiany danych, są to programy np. do wymiany poczty, przeglądarki itp.

2. Jednostki miar w Sieciach Komputerowych:

W sieciach komputerowych, podobnie jak w procesach logicznych zachodzących np. w procesorach, koprocessorach interpretujemy konkretne dwie wartości:

- **0 i 1.**

Taki sposób interpretowania wartości 0 i 1 został przyjęty powszechnie w świecie IT i jest także stosowany do określania parametrów transmisji danych w sieciach komputerowych.

Bit – Podstawowa jednostka operacyjna oznaczana symbolem małego „b”

BPS – Podstawowa jednostka prędkości oznaczająca „bit per second” w sieciach komputerowych, zapisywana jako „bps” lub „b/s”

kb/s (kbps) – Kilobity na sekundę.

Mb/s (Mbps) – Megabity na sekundę.

Gb/s (Gbps) – Gigabity na sekundę.

***Decybele (dB)** – Zwykle podawane w nich są wyniki testowania sieci, najczęściej światłowodowych lub bezprzewodowych. Używamy je do porównania wielkości zmieniających się w bardzo szerokim zakresie, np. dzięki decybelom możemy sprawdzić moc przekazaną przez nadajnik i odebraną przez odbiornik.

Wartość wyrażona w decybelach wyraża wzrost mocy (Wartość dodatnia), lub jej spadek (Wartość ujemna). Liczba decybeli pozwala stwierdzić, ile energii pozostało w fali, np. radiowej po pokonaniu określonej odległości. Przykładowo, jeżeli nadajnik damy na to światłowód wyemitował sygnał o mocy 100[W], tłumienie w kanale komunikacyjnym (czyli w przewodzie) wynosi np. 10 dB, to odbiornik odbierze sygnał o mocy 10[W].

***SNR** – (Signal – Noise Ratio) Stosunek sygnału do szumu. Szum to niepożądany sygnał pochodzący najczęściej ze źródeł naturalnych, np. wyładowanie elektryczne podczas burzy, przewody energetyczne, lub urządzeń elektrycznych które mogą zakłócać pracę.

3. Rodzaje oraz charakterystyka medium transmisyjnego:

Aby wymieniać informacje w sieci, musimy je przez coś przestać, w coś je wdrożyć, urządzenia sieciowe muszą być jakoś ze sobą połączone.

Nośniki te w Sieciach Komputerowych nazywamy: „**Mediami Transmisyjnymi**”

Media Transmisyjne – Mogą być one różne np. przewodowe (kable miedziane, światłowody), lub także bezprzewodowe (fale radiowe, fale świetlne)

Najpopularniejsze Media Transmisyjne:

- Jednym z nich jest „skrętka” składa się ona z czterech par przewodów przeplecionych ze sobą dlatego aby zmniejszyć wpływ zakłóceń z innych par na inne pary skrętki.
Rozróżniamy dwie najpopularniejsze kategorie skrętki, a raczej jej opłotu czyli:
 - a) UTP – Skrętka nieekranowana (Unshielded Twisted Pair) stosowana w większości sieci.
 - b) STP – Skrętka ekranowana (Shielded Twisted Pair) wyposażona w specjalną warstwę chroniącą przed wpływem zakłóceń elektromagnetycznych na przewody.

Skrętka jest stosowana w telekomunikacji do przesyłania danych zarówno analogowych i cyfrowych.

Kategorie skrętki usprawniają podział odpowiednich do naszej dyspozycji i idealnych do projektu sieci.

- **Kategoria 3 (CAT 3)** – Stosowana w przestarzałych sieciach max. 10Mb/s
- **Kategoria 5 (CAT 5)** – Stosowana w sieciach o przepustowości do max. 100Mb/s
- **Kategoria 5e (CAT 5e)** - Skrętka (CAT 5) z poprawionymi parametrami zakłóceń i transmisji max. 100Mb/s lub 1Gb/s.
- **Kategoria 6 (CAT 6)** – Stosowana do przenoszenia danych z prędkością do 10Gb/s.
- **Kategoria 7 (CAT 7)** – Ekranowana skrętka stosowana do przenoszenia danych w sieciach o przepustowości powyżej 1Gb/s.

Większość nowoczesnych Sieci oparta jest o rozwiązania **CAT 5e** lub wyższych.

Warto zapamiętać że Maksymalna długość połączeń wykonywanych za pomocą skrętki przy standardowych parametrach użytkowania wynosi **100 Metrów!**

Rodzaje skrętek:

U/UTP – skrętka nieekranowana

F/UTP – skrętka foliowana

U/FTP – skrętka z każdą parą w osobnym ekranie z folii.

F/FTP – skrętka z każdą parą w osobnym ekranie z folii dodatkowo w ekranie z folii

SF/UTP – skrętka ekranowana folią i siatką

S/FTP – skrętka z każdą parą foliowaną dodatkowo w ekranie z siatki

SF/FTP – skrętka z każdą parą foliowaną dodatkowo w ekranie z folii i siatki

Przesłuchy:

a) Przesłuch zbliżny (NEXT Near-End Crosstalk)

Przesłuch zbliżny, czyli zakłócenie jakie może zostać wygenerowane na danej parze skrętki, w skutek transmisji danych w sąsiedniej parze.

b) Przesłuch zdalny (FEXT)

FEXT, przesłuch zdalny, mierzony na przeciwnym końcu przewodu niż sygnał wywołujący zakłócenie. Zależy od długości przewodu.

c) Tłumienie

Określa o ile zmniejszy się jakość przesyłanego sygnału po przejściu całego toru kabla.

d) Propagacja (Propagation)

Określa różnicę opóźnienia transmisji między najszybszą, a najwolniejszą parą w skrętce.

Przy dużych prędkościach transmisji może powstawać problem z poprawnie zakodowanym odbiorem. Max wartość 45-50 ns.

4. Standardy Sieci bezprzewodowych (WLAN)

802.11 – Transmisja danych obejmuje dwie prędkości **1 i 2 Mb/s**. Przesył danych miał się odbywać za pomocą podczerwieni oraz fal częstotliwości **2.4 GHz**.

802.11a – Dane są tutaj przesyłane falami o częstotliwości **5 GHz** z prędkością **54 Mb/s**, ale w praktyce wynosi ona ok. **20 Mb/s**. **802.11a** obejmuje **8 kanałów dla pracy w budynkach i 4 kanały point to point**. Standard ten nie jest bardzo popularny, gdyż ma mały zasięg i pobiera więcej prądu niż inne.

802.11b – Pracuje w częstotliwości **2.4 GHz**. Umożliwia przesyłanie danych z prędkością **11 Mb/s**. Zasięg na powierzchni zagospodarowanej do 50 metrów od nadajnika oraz do 120 metrów na otwartej przestrzeni. W domach betonowe ściany znacznie zmniejszają zasięg. Standard ten wykorzystuje algorytmy do usuwania zakłóceń oraz unikania kolizji podczas komunikacji kilku bezprzewodowych kart sieciowych.

802.11g – Jest ulepszeniem standardu „b”. Zmiany to przyspieszenie prędkości przesyłu danych do **54 Mb/s**.

Jest zgodny ze standardem „b” i często można się spotkać z napisem **WLAN b/g** co oznacza zastosowanie karty sieciowej „g” zgodnej wstecznie z „b”. W wielu urządzeniach można spotkać się z określeniem „Super G”. Umożliwia ono transfer na poziomie **108 Mb/s**.

802.11n Maksymalna przepustowość wynosi **600 Mb/s** 802.11n może wykorzystywać wiele kanałów transmisyjnych do jednego połączenia, co zwiększa prędkość transmisji. Zasięg w otwartej przestrzeni wynosi ok. 120 metrów. Wspomniane wcześniej **600 Mb/s** można osiągnąć poprzez nadmiar kodowania i wykorzystanie kilku anten.

5. Rodzaje, budowa i funkcje urządzeń sieciowych:

Podstawowymi urządzeniami sieciowymi, czyli pracującymi w sieciach komputerowych są:

- **Koncentrator ang. (Hub)** – To urządzenie wyposażone podobnie jak przełącznik w porty do podłączania hostów. Koncentratory mogą być pasywne lub aktywne, Pasywny pełni tylko funkcję skrzynki łączeniowej, przekazując sygnał z jednego portu na wszystkie prócz z tego którego dostał informację. Natomiast Hub aktywny cechuje się wzmacnianiem sygnału.
- **Most ang. (Bridge)** – To urządzenie konkretnie z dwoma portami, służącymi do łączenia segmentów sieci. W swojej pamięci przechowuje adresy MAC urządzeń przyłączonych do poszczególnych portów. Po otrzymaniu ramki danych sprawdza adres miejsca docelowego i określa, do jakiego segmentu należy przestać daną ramkę. Gdy komputer z jednego segmentu sieci wysyła wiadomość most analizuje zawarte w niej adresy MAC i na tej podstawie podejmuje decyzję, czy sygnał przestać do drugiego segmentu czy go zablokować. W sieci nie są przesyłane dodatkowe zbędne ramki co skutkuje większą wydajnością sieci.
- **Przełącznik ang. (Switch)** – Oferuje te same funkcje co koncentrator czyli hub, też ma możliwość podziału sieci na segmenty, ale ma jedną przewagę nad Hub'em czyli nie wysyła zbędnych ramek do wszystkich hostów tylko sam decyduje do jakiego hosta nadana ramka ma dotrzeć, co powoduje jeszcze lepszą wydajność sieci a z tym mniejsze opóźnienia i mniej ruchu, ponieważ to już nie host decyduje czy do niego należy ramka, za to odpowiada już switch.





- **Punkt dostępowy ang. (Access point)** – Zapewnia dostęp do sieci przewodowej poprzez rozsył fal radiowych dla hostów korzystających z tej technologii. Access point może być połączony z routerem w jedną całość.
- **Router** – To urządzenie stosowane do łączenia sieci, np. do przyłączania sieci LAN do Internetu lub 2 osobnych sieci LAN o innych adresacjach. Jest urządzeniem konfigurowalnym co pozwala na dostosowanie go do potrzeb sieci.
- **Brama sieciowa ang. (Gateway)** – To urządzenie za którego pośrednictwem komputery z sieci LAN komunikują się z komputerami w innych sieciach. Najczęściej funkcję bramy sieciowej spełniają routery, a konkretnie ich adresy służą hostom jako brama domyślna.
- **Bramka VoIP and. (Voice over Internet Protocol)** – Umożliwia wykonywanie połączeń tradycyjnymi aparatami telefonowymi, zamienia sygnały analogowe na sygnały VoIP możliwe do przesłania w sieci.
- **Zapora sieciowa ang. (Firewall)** – Specjalne oprogramowanie lub sprzęt zabezpieczająco-listujący przed niepożądanym dostępem do sieci i z sieci.

6. Symbole graficzne urządzeń sieciowych:

Tabela 1. Symbole graficzne wybranych urządzeń używane w schematach

Symbol	Znaczenie	Symbol	Znaczenie
	modem		punkt dostępowy
	koncentrator		router
	most		stacja robocza
	przełącznik		zapora sieciowa

Połączenia pomiędzy urządzeniami mogą być wykonane za pomocą różnych typów łącz. Wybrane symbole łącz używane w schematach zebrano w tabeli 2.

Symbol	Znaczenie	Symbol	Znaczenie
 PC-PT PCD 2950-24 Switch2	kabel Ethernetowy prosty	 1841 Router0 1841 Router1	kabel szeregowy
 2950-24 Switch1 2950-24 Switch0	kabel Ethernetowy krosowany	 Router-PT Router2 Router-PT Router4	kabel światłowodowy

7. Topologie sieciowe Logiczna i Fizyczna:

Topologia – Określa sposób jej wykonania, czyli połączenia urządzeń komputerowych za pomocą mediów transmisyjnych. Topologie sieci LAN mogą być opisane zarówno na płaszczyźnie fizycznej, jak i logicznej.

Topologia fizyczna – Określa geometryczną organizację sieci lokalnej, graficznie przedstawiając jej kształt i strukturę.

Topologia logiczna – Opisuje reguły komunikacji, z których korzystają urządzenia komunikujące się w sieci. Za jej pomocą można opisać, które urządzenia mogą się ze sobą komunikować lub mają wzajemne, bezpośrednie połączenie fizyczne.

W sieciach LAN stosuje się topologie logiczne:

- **Topologia rozgłaszania** – Polega na tym, że host wysyła dane do wszystkich hostów podłączonych do medium. Kolejność korzystania z medium określa reguła: „Kto pierwszy wysłał, ten pierwszy zostanie obsłużony.” Przykładem takiej topologii jest sieć Ethernet.
- **Topologia przekazywania tokenu (żetonu)** – Polega na kontrolowaniu dostępu do sieci przez przekazywanie elektronicznego tokenu (specjalnej ramki kontrolnej danych). Host, który w danym momencie ma token, może skorzystać z medium. W przypadku gdy host nie potrzebuje dostępu do medium przekazuje żeton dalej i tak w kółko. Z tej topologii korzystają sieci FDDI i Token Ring.

Podstawowymi topologiami fizycznymi stosowanymi w budowie lokalnych sieci są:

- **Magistrala ang. (Bus)** – W topologii magistrali wszystkie węzły sieci (np. komputery, drukarki sieciowe itp.) połączone są połączone ze sobą za pomocą pojedynczego kabla koncentrycznego, który obsługuje tylko jeden kanał i nosi nazwę „magistrali”. Węzły są dołączane do wspólnej magistrali za pomocą „trójkątów” zwanych również „Trójkątami BNC”. Oba końce magistrali muszą być zakończone tzw. „Terminatorami BNC” aby zapobiec odbiciu sygnału z powrotem do magistrali.

Zalety Magistrali: Krótkie odcinki kabla użyte do budowy sieci, brak konieczności stosowania dodatkowych urządzeń sieciowych (switchy i hub'ów), łatwość przyłączenia nowego urządzenia do sieci.

Wady Magistrali: Trudna lokalizacja uszkodzenia kabla. Możliwa jest tylko jedna transmisja w danym momencie, a awaria kabla może spowodować niechciany podział na segmenty sieci, lub całkowite jej przerwanie.

- **Pierścień** ang. (**Ring**) – Każda przyłączona do sieci nowa stacja robocza ma dwa połączenia – po jednym do każdego najbliższego sąsiada. Połączenie takie tworzy fizyczną pętlę, czyli pierścień. Dane są przesyłane wokół pierścienia w jednym kierunku. Każda stacja robocza działa podobnie jak wzmacniak, pobierając pakiety do niej zaadresowane i odpowiadając na nie, a także przesyłając pozostałe pakiety do następnej stacji i tak w kółko.

Zalety Pierścienia: Można określać czas przepływu czyli ruchu co nie jest możliwe w innych topologiach fizycznych.

Wady Pierścienia: Wadą jest to, że awaria pojedynczego przewodu unieruchamia całą sieć, natomiast zawsze można użyć topologii podwójnego pierścienia co zmniejsza ryzyko kompletnego odcięcia sieci.

Jest o wiele wolniejsza niż inne pozostałe topologie.

- **Siatka** ang. (**Mesh**) – Jest używana wtedy, gdy każdy węzeł ma własne połączenia z wszystkimi pozostałymi tzw. (Każdy z Każdym)

Zalety Siatki: Niezawodność.

Wady Siatki: Wysoki koszt i skomplikowana budowa w sieciach LAN i w sieciach WAN.

- **Gwiazda** ang. (**Star**) – Połączenia sieci rozchodzą się z centralnego punktu, którym może być Switch lub Hub. Każde urządzenie przyłączone do sieci może uzyskiwać dostęp do współdzielonego nośnika. Topologia ta dominuje w dzisiejszych sieciach LAN, jest bardzo elastyczna i skalowalna.

Zalety Gwiazdy: Zaletą gwiazdy jest to że posiada bardzo dużą przepustowość i łatwą lokalizacją uszkodzeń. W przypadku awarii łącza lub komputera pozostała część sieci pracuje bez zakłóceń.

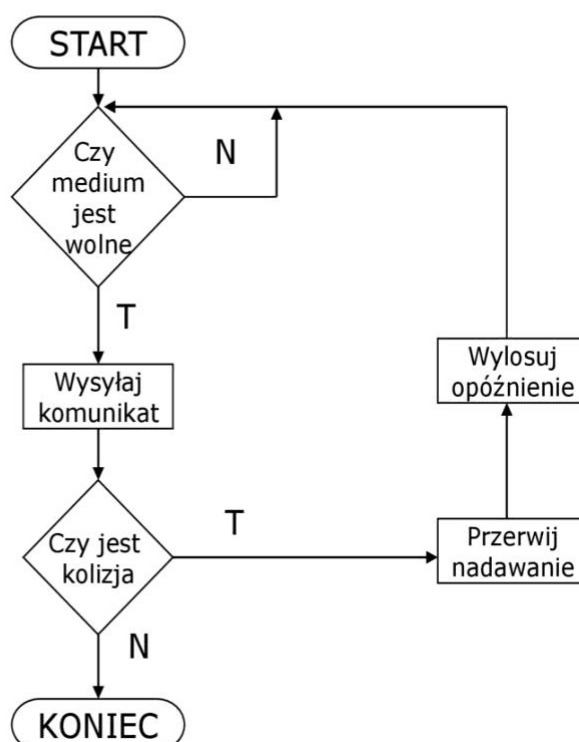
Wady Gwiazdy: Wadami są większe zapotrzebowanie na kable oraz konieczność stosowania switchy (głównie w dzisiejszych czasach) których awaria unieruchamia całą sieć.

- **Rozszerzona Gwiazda** ang. (**Extended Star**) – Jest oparta na topologii gwiazdy z tym wypadkiem że punkt centralny może mieć wiele pobocznych punktów spinających więcej sieci ze sobą.

8. Metody dostępu do nośnika (medium transmisyjnego):

- **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) – W tej metodzie urządzenia rywalizują ze sobą o dostęp do medium.
Stacja zamierzająca transmitować dane może uzyskać dostęp do niego w dowolnej chwili.
Przed wysłaniem danych stacja nasłuchuje czy w sieci odbywa się ruch, Jeżeli go wykryje to czeka do momentu, kiedy nośnik będzie wolny. Jeżeli dwie stacje nadają w tym samym momencie, następuje **kolizja** i obie transmisje muszą zostać powtórzone.
- **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance) – Transmisja z unikaniem kolizji może być zrealizowana przez zgłoszenia żądania transmisji. Stacja, która chce wysłać dane, sprawdza czy w sieci nadaje już inna stacja. Jeśli tak, czeka na zakończenie transmisji. Jeśli nie wykryła, sprawdza czy od ostatniego żądania transmisji minął określony czas np. „T”
Jeżeli czas „T” nie upłynął, ponownie sprawdza.
Jeżeli jednak upłynął czas „T”, stacja zgłasza żądanie transmisji i czeka przez ustalony czas.
(Jednakowy dla wszystkich)
Jeżeli stwierdzi żądanie innej stacji czeka losowy czas i zaczyna procedurę od początku.
Trochę skomplikowane nie?
Przedstawmy graficznie metodę **CSMA/CA**:

Metoda wykrywania nośnej z detekcją kolizji -CSMA/CD Algorytm



9. Rodzaje środowiska sieciowych, (klient – serwer & P2P)

- a) Jednym z podstawowych celów sieci komputerowych jest współdzielenie i współużytkowanie zasobów, takich jak pliki, drukarki, czy urządzenia sieciowe.
Każdy z tych zasobów musi być **udostępniony**, to znaczy że właściciel zasobu musi wyrazić zgodę na korzystanie z niego przez innych użytkowników.
- **Komputer** – lub inne urządzenie korzystające z zasobów udostępnianych przez serwer będzie nazywany **klientem**.
 - **Serwerem** – natomiast zostanie nazwany serwer czyli komputer który udostępnia swoje zasoby w sieci.

Takie środowisko nazywa się: **(Klient – Serwer)**

- b) W architekturze **równorzędnej** każdy użytkownik może być i klientem, i serwerem w danym momencie kiedy korzysta z zasobów innych, i wtedy kiedy sam udostępnia pewne zasoby.

Takie środowisko nazywa się: **(P2P – Peer to Peer)**

10. Komunikacja w Sieci:

Protokół Komunikacyjny ang. **Communication Protocol** – Zbiór zasad i norm, których muszą przestrzegać komunikujące się ze sobą urządzenia.

Tryb Połączeniowy – Polega na ustanowieniu logicznego połączenia między dwoma komunikującymi się ze sobą urządzeniami. Aby rozpocząć komunikację najpierw trzeba nawiązać stabilne połączenie. Z trybu połączeniowego korzysta się wtedy, gdy powstaje potrzeba przesyłania wielu komunikatów w obu kierunkach. Np. **TCP**

Tryb Bezpołączeniowy – Komunikaty są przekazywane niezależnie i nie sprawdzają stanu połączenia po prostu je wysyłają, np. podczas przekazywania wiadomości za pomocą poczty elektronicznej. W komunikacji biorą udział przynajmniej dwa urządzenia. Np. **UDP**

Tryb Unicast - Jeżeli jedno urządzenie wysyła dane do dokładnie jednego urządzenia, to taki tryb nazywamy trybem **unicast** czyli pojedynczym.

Tryb Broadcast – Urządzenie nadawcze może wysyłać informację do wszystkich dostępnych urządzeń. W takim przypadku adresem docelowym jest specjalny adres, nazywany **broadcast** czyli **rozgłoszeniowy**. Urządzenia traktują transmisję **broadcast** tak jakby były adresowane na ich adres wysyłkowy czyli do **wszystkich**.

Tryb Multicast – W rozgłaszaniu multicast dane natomiast są przeznaczone tylko dla pewnej grupy odbiorców, adres docelowy jest specjalnym adresem określającym daną grupę odbiorców.

11. Typy transmisji danych:

Transmisja jednokierunkowa ang. (**simplex**) – To transmisja, w której odbiornik nie może nadawać, tak samo jak w przypadku radia, radiostacja nadaje fale radiowe, natomiast słuchacze mogą je jedynie odbierać bez możliwości odpowiedzi.

Półdupleks ang. (**Half-Duplex**) – To **transmisja dwukierunkowa, naprzemienna**. W danym momencie jest ustalony tylko jeden kierunek transmisji, a urządzenie może albo nadawać, albo odbierać informacje. Do odwrócenia kierunku transmisji jest potrzebny system sygnalizacji, wskazujący, że urządzenie ukończyło nadawanie i może odbierać informacje. Przykładem takiej komunikacji jest rozmowa poprzez CB-radio.

Dupleks ang. (**Full-Duplex**) – To transmisja jednoczesna i dwukierunkowa. **Wymaga zazwyczaj dwóch par przewodów dla sieci cyfrowych.**

Dla połączeń analogowych dla jednej pary przewodów szerokość pasma jest dzielona na dwie części. Przykładem jest rozmowa telefoniczna, gdy naprzemiennie możemy rozmawiać z kimś w tym samym czasie.

Transmisja równoległa – Dane są przesyłane jednocześnie kilkoma przewodami, z których każdy przenosi jeden bit informacji, np. port LPT w komputerze. **Zasięg transmisji równoległej jest mniejszy niż transmisji szeregowej.**

Transmisja szeregową – Poszczególne bity informacji są przesyłane kolejno po sobie wraz z dodatkowymi danymi pozwalającymi na kontrolę tej transmisji, np. Port COM w komputerze.

Transmisja szeregową pozwala na wysyłanie danych na duże odległości. Transmisja szeregową umożliwia także przesyłanie danych w sposób:

- a) **Asynchroniczny** (Szeregowy – Asynchroniczny) – Dane są poprzedzone **bitem startu** (stan logiczny: **0**), który jest sygnałem rozpoczęcia transmisji. Po bicie startu są przesyłane **bity danych** (od **5** do **8**), od najmłodszego do najstarszego, bit parzystości (jeżeli jest używany) i **bit stopu** (stan logiczny: **1**)
- b) **Synchroniczny** (Szeregowy – Synchroniczny) – Dane są przesyłane w wyznaczonych odstępach czasu, ten odstęp czasu nazywa się tzw. „**Sygnałem Zegarowym CLK**”, wspólnym dla nadajnika i odbiornika. **Dane są przesyłane bez dodatkowych bitów startu i stopu**. Natomiast są poprzedzone informacją wstępną, pozwalającą wykryć ich początek – bajtami synchronizacji **SYN**, po których następuje znak rozpoczynający **ramkę SOH** (ang. *Start of Header*), i zakończone sekwencją oznaczającą koniec **ramki EXT** (ang. *End of Text*)

12. Modele warstwowe sieci, Model ISO/OSI & TCP/IP.

a) Model Sieci ISO/OSI:

Według modelu OSI ang. (Open Systems Interconnection) wyróżniamy konkretnie **siedem** takich warstw. Każda warstwa komunikuje się tylko z warstwą bezpośrednio wyższą, lub bezpośrednio niższą.

- **Warstwa Aplikacji:** Zajmuje się specyfikacją interfejsu, który wykorzystują do przesyłania danych do sieci. Warstwa ta świadczy usługi końcowe dla aplikacji. Na tym poziomie działają aplikacje sieciowe dostępne bezpośrednio dla użytkownika i jego oczu, takie jak: Klient poczty elektronicznej, czy przeglądarka WWW.
- **Warstwa Prezentacji:** Zajmuje się wstępnym przetworzeniem danych otrzymanych z warstwy aplikacji, dla niższych od siebie warstw. W odwrotnym procesie tłumaczy ona dane przychodzące na takie kompatybilne z warstwą aplikacji.
- **Warstwa Sesji:** Zadaniem warstwy sesji, jest kontrolowanie przebiegu połączenia tzw. „sesji” między urządzeniami podczas wymiany danych kontroluje odpowiednio przepływ danych tak aby trafiał do właściwych aplikacji i ich portów.
- **Zadania pozostałych 4 warstw:** Do ich zadań należy przede wszystkim transmisja danych. Zajmują się odnajdywaniem odpowiedniej drogi do miejsca przekazania konkretnej informacji. Dzielą dane na tzw. **PDU** ang. (**Protocol Data Unit**)

b) Stos Protokołów TCP/IP:

W modelu sieci TCP/IP wyróżniamy tylko 4 warstwy są to:

- **Warstwa aplikacji:** Obejmuje funkcje trzech najwyższych warstw modelu ISO/OSI. (Aplikacji, prezentacji i sesji) Użytkownicy uruchamiają programy, które uzyskują dostęp do usług a poziomie warstwy transportu i wysyłają lub odbierają dane w postaci pojedynczych komunikatów lub strumienia bajtów. Programy użytkowe przekazują do warstwy transportowej dane w wymaganym formacie, aby mogły one zostać dostarczone w odpowiednie miejsce. W warstwie tej działa wiele protokołów aplikacji, m.in.: HTTP, HTTPS, FTP, TELNET, SSH, SMTP, POP3.
- **Warstwa transportowa:** Zadaniem warstwy tej jest zapewnienie komunikacji między programami użytkownika. Warstwa ta może zarządzać przepływem informacji oraz zapewniać niezawodność przesyłania przez porządkowanie segmentów, a także za ponowną ich transmisję w przypadku ich zagubienia. W systemie operacyjnym może działać wiele aplikacji wymieniających dane w sieci przy wykorzystaniu **portów** określonych dla każdego połączenia. W ten sposób nie nastąpi wymieszanie podczas przekazywania informacji do każdej z powyższych aplikacji. Warstwa dzieli także strumień danych na **segmenty**, a w nagłówku umieszcza numer portu identyfikujący aplikację wysyłającą lub odbierającą dane. W tej warstwie działa także protokół połączeniowy **TCP** i protokół bezpołączeniowy **UDP**.
- **Warstwa internetowa:** Przyjmuje segmenty z warstwy wyższej czyli transportowej, razem z informacjami identyfikującymi osobę, zadaniem tej warstwy jest wysłanie pakietów i dostarczenie ich do właściwego odbiorcy. **Protokołem zarządzającym tą trasą jest protokół IP.** W warstwie internetowej działają także urządzenia zwane routerami i ich protokoły czyli **protokoły trasowania (routing)**.
- **Warstwa dostępu do sieci:** Odbiera pakiety IP i przesyła je przez daną sieć.

Porównanie TCP/IP & ISO/OSI:

Model OSI	Model TCP/IP	PROTOKÓŁ / urządzenie sieciowe
Warstwa aplikacji	Warstwa aplikacji	HTTP, TELNET SSH, FTP POP3, SMTP IMAP, DNS
Warstwa prezentacji		
Warstwa sesji		
Warstwa transportowa	Warstwa transportowa	TCP, UDP
Warstwa sieci	Internet	IP, RIP OSPF, EIGRP /Router, Switch
Warstwa łącza danych	Warstwa dostępu do sieci	ETHERNET / Switch, Most, Hub
Warstwa fizyczna		Media transmisyjne (skrętka, światłowód), kodowanie

13. Typy kabli wykorzystywane do łączenia urządzeń:

Prędkość wyrażona w Mb/s:

- Np. 10, 100, 1000.

Rodzaje transmisji:

- **Base** – Oznacza transmisję w paśmie podstawowym. ang. (**baseband**)
- **Broad** – Oznacza transmisję szerokopasmową. ang. (**broadband**)

Rodzaj stosowanego medium:

- 2 – Cienki kabel koncentryczny.
- 5 – Gruby kabel koncentryczny.
- T – Skrętka ang. (**Twisted Pair**)
- F – Światłowód ang. (**Fiber Optic**)

Najczęściej stosowane nośniki danych dla sieci Ethernet:

- 10Base2 – Cienki kabel koncentryczny o prędkości 10 Mb/s, z transmisją pasmem podstawowym.
- 1Base5 – Gruby kabel koncentryczny o maksymalnej długości 500m.
- 10BaseT – Długość kabla ograniczona do 100 m, litera T symbolizuje skrętkę.

Najczęściej stosowane nośniki danych dla sieci Fast Ethernet:

- 100BaseTX – Niekierowana skrętka kategorii 5.
- 100BaseFX – Światłowód obsługujący transmisję danych z szybkością 100 Mb/s na odległość 400m.

Najczęściej stosowane nośniki danych dla sieci Gigabit Ethernet:

- 1000BASE-T – Skrętka cat. 5 lub wyższej 4 pary przewodów.
- 1000BASE-SX – 1 Gb/s na światłowodzie wielomodowym do 550m.
- 1000BASE-LS – 1 Gb/s na światłowodzie jedno-modowym do 100km.

14. Protokoły Routingu:

Routing – System protokołów odpowiadających za trasowanie przebiegu pakietów w sieci.
„Protokoły Routingu” wykorzystywane są w systemach routerów czyli „trasowników”.

Protokoły Routingu dzielimy na:

- **Statyczne** – Statyczne Trasy dla pakietów ustalane są przez administratora sieci, natomiast wymaga to sporo czasu, konfiguracji i sporo przewidywania układów tras dla rekonfigurowania routerów w przypadku zmiany topologicznej sieci, lub awarii jednego z oddalonych routerów. Statyczne trasy są już bardzo rzadko wykorzystywane ponieważ zostały wyparte przez:
- **Dynamiczne** – Routery w celu konfiguracji tras dynamicznych korzystają z tzw: „Protokołów Routingu”, wymieniają one w ten sposób swoje bazy z tablicami routingu, wykrywają zmiany topologiczne sieci, dodatkowo same uczą się na podstawie swoich protokołów gdzie najlepiej pakiet „podać dalej” czyli sprawić żeby trafił do odbiorcy szybciej, i bardziej efektywnie nie powodując zamieszania w sieci.

Lista najpopularniejszych protokołów:

- **RIP** – Jest to protokół wykorzystujący tzw: „**Wektor odległości**”. Posiada bardzo małe wymagania sprzętowe dlatego jest bardzo popularny, **Router na którym uruchomiony jest protokół RIP, okresowo (standardowo co 30s) przesyła do swoich bezpośrednich kopię swojej tablicy routowania.** Natomiast kiedy otrzyma informację od sąsiada porówna go ze swoją tablicą i w razie potrzeby zaktualizuje swoją. W tablicy znajdują się wszystkie trasy do najlepszych sieci. **Liczba przeskoków niestety wynosi tylko 15.**
- **OSPF** – Jest to protokół „**Stanu łącza**” wykorzystującym algorytm Dijkstry. Algorytm najlepszego łącza bazujący na auto-aktualizacji tras na podstawie algorytmu Dijkstry. **Routery które pracują na tym protokole szukają najlepszej i najwydajniejszej trasy poprzez wymienianie się specjalnym pakietem LSA (Link State Advertisement).** Na tej podstawie dokonując skomplikowanych obliczeń

odszukują najlepsze i najszybsze trasy. Zmiany w danym obszarze sieci nie powoduje od razu uruchomienie protokołu Dijkstry. Obliczenia protokołu OSPF są o wiele bardziej skomplikowane niż protokołu RIP, dlatego też wymagają o wiele potężniejszych routerów.

- **IGRP & EIGRP** – Protokół IGRP oraz jego następca czyli EIGRP zostały opracowane przez firmę **CISCO**. IGRP podobnie jak RIP jest protokołem wektora odległości, natomiast EIGRP jest nowszą i ulepszoną wersją IGRP. EIGRP pracuje jako hybryda czyli połączenie cech algorytmu wektora odległości i stanu łącza.

15. Normy i zalecenia dot. montażu okablowania:

Głównym celem stosowania standardów okablowania, oraz standardów urządzeń sieciowych jest, możliwość współpracy softu & hardware'u innych firm, gdyby nie standardy firmy kupujące dla przykładu przełączniki firmy Cisco z serii Catalyst dla warstwy głównej (rdzenia) swojej sieci musiałyby współpracować z innymi przełącznikami od tej firmy. Natomiast nie jest tak łatwo zaprojektować sieć dokładnie tak jak byśmy czasami chcieli, czasami inne rozwiązania są nawet wymagane! Co gdyby standardy nie istniały, wyobraźmy sobie ten bajzel! Przełączniki firmy Cisco nie mogłyby komunikować się np. z przełącznikami niższych warstw np. firmy Hewlett-Packard. No masakra! Dlatego właśnie dzisiejsi producenci, monterzy i informatycy muszą trzymać się ściśle określonych norm i zasad standaryzacyjnych.

W Polsce i Europie możemy wyróżnić kilka standardów okablowania:

- **Norma Europejska EN 50173** – Dotycząca okablowania strukturalnego dla budynków.
- **Norma Europejska EN 50167** – Dotycząca okablowania poziomego.
- **Norma Europejska EN 50168** - Dotycząca okablowania pionowego.
- **Norma Europejska EN 50169** – Dotycząca okablowania krosowego i stacyjnego.
- **Norma Krajowa (PL) PN-EN 50174-1** – Specyfikacja i zapewnienie jakości.
- **Norma Krajowa (PL) PN-EN 50174-2** – Planowanie i wykonywanie instalacji wewnątrz budynków.
- **Norma Krajowa (PL) PN-EN 50174-3** - Planowanie i wykonywanie instalacji na zewnątrz budynków.

Najważniejsze zalecenia wychodzące z tych norm:

- Okablowanie poziome powinno tworzyć nieprzerwane połączenie między punktem dystrybucyjnym a punktem abonenckim.
- Jeden punkt abonencki (2 x RJ-45) na każde 10m² powierzchni biurowych.
- Na każdym piętrze powinien być punkt dystrybucyjny.
- Wszystkie kable muszą mieć zakończenia w punktach abonenckich i szafach dystrybucyjnych.
- W obrębie całej sieci powinno utrzymywać standard okablowania tj. kable miedziane o tej samej impedancji i średnicy, przewody światłowodowe w tej samej technologii włókien.
- Rozplot kabla UTP nie powinien być większy niż 13 mm.
- Każdy element systemu powinien być czytelnie oznaczony.
- Sieć musi posiadać pełną dokumentację.

16. Terminologia funkcji urządzeń sieciowych:

- **Zabezpieczenie Portów** – Umożliwia switchowi podejmowanie decyzji ile urządzeń może się z nim kontaktować, lub jakie konkretne urządzenia tylko mogą to robić. Decyzje najczęściej podejmowane są na podstawie adresu fizycznego MAC.
- **Obsługa sieci VLAN** – Umożliwia oddzielenie grup osób podłączonych do przełącznika. specjalne wirtualne sieci stworzone na przełączniku nie pozwalają na komunikację z odrębnymi sieciami. Jest używany w celu zapewnienia prywatności dla danych obszarów logicznych sieci.
- **Obsługa standardu Gigabit Ethernet** – Jest po prostu zaletą nowocześniejszych urządzeń sieciowych ponieważ kiedyś urządzenia obsługujące ten zakres szybkości były o wiele droższe niż te obsługujące Fast Ethernet ludziom zupełnie wystarczyło do codziennej pracy. Natomiast teraz różnice w cenach są niezauważalne.
- **Zasilanie przez Ethernet (PoE)** – Stosowane jedynie w przypadku zasilania kamer IP wykorzystujących tę technologię, aparatów telefonicznych IP (np. firmy Cisco) i bezprzewodowych punktów dostępowych gdzie montaż okablowania zasilającego jest bardzo trudny lub praktycznie niemożliwy. Do wykorzystania technologii PoE wymagane jest urządzenie obsługujące tę technologię oraz specjalny przełącznik umożliwiający zasilanie takich urządzeń.
- **Obsługa jakości usług (QoS)** – Umożliwia nadawanie priorytetu danym którym np. Administrator sieci chce takowy nadać, np. przesyłać szybciej niż inne dane.
- **Agregacja łączy** – Funkcja pozwala przełącznikom na użycie kilku portów czyli kilku fizycznych połączeń jako jedno logiczne połączenie tworzące jeden przewód o bardzo wysokiej przepustowości łączy szerokości pasma. (Najczęściej stosowana do łączenia ze sobą przełączników).
- **Funkcja routingu między sieciami VLAN** – Tutaj wymagana jest większa wydajność przetwarzania oraz funkcjonalności warstwy rdzenia.
- **Nadmiarowość** – Ważne aby urządzenia aktywne sieci współpracowały ze sobą nadmiarowo, tzn. Aby posiadały więcej połączeń czy to ze sobą czy to z dodatkowym zasilaniem. Ogranicza to awaryjność sieci w przypadku np. braku dostaw zasilania czy uszkodzenia jednego z aktywnych urządzeń sieciowych.