Sieci komputerowe – konwersatorium 1

Jarosław Szkoła

Sieć komputerowa

- Sieć komputerowa to medium umożliwiające połączenie dwóch lub więcej komputerów w celu wzajemnego komunikowania się.

Początki sieci komputerowych, komputery MainFrame, minikomputery

Komputer typu MainFrame z lat 60-tych

UNIX system

W tym samym roku firma Bell Laboratories opracowała system operacyjny UNIX, wielozadaniowy, wieloużytkownikowy system operacyjny, który stał się popularny w akademickich środowiskach obliczeniowych w latach 70. XX wieku. Typowym systemem UNIX w 1974 roku był minikomputer PDP-11 z dołączonymi prostymi terminalami. W konfiguracji z 768 KB pamięci z rdzeniem magnetycznym i kilkoma dyskami twardymi o pojemności 200 MB, koszt takiego systemu wynosił około 40 000 USD.

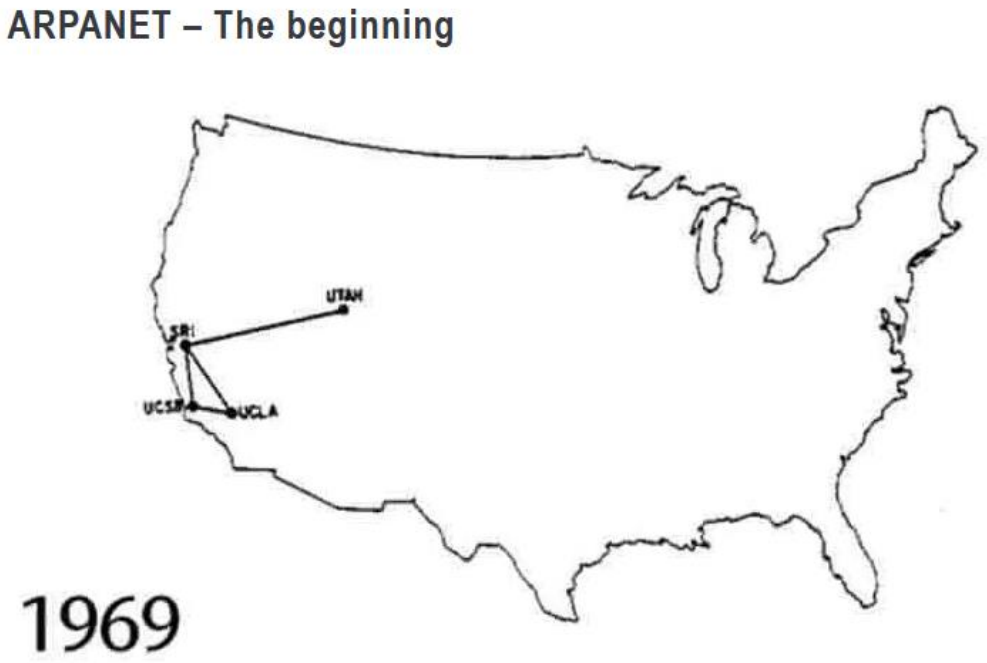
EBCDIC and ASCII

W latach sześćdziesiątych ewoluowały również standardy sieci komputerowych. W 1962 roku IBM wprowadził pierwszy 8-bitowy system kodowania znaków o nazwie Extended Binary-Coded Decimal Interchange Code (EBCDIC). Rok później wprowadzono konkurencyjny amerykański standardowy kod wymiany informacji (ASCII). ASCII ostatecznie wygrał z EBCDIC, mimo że EBCDIC był 8-bitowy, podczas gdy ASCII był tylko 7-bitowy. ASCII został formalnie ustandaryzowany przez American National Standards Institute (ANSI) w 1968 roku. ASCII został po raz pierwszy użyty w transmisji szeregowej między hostami mainframe i prostymi terminalami w środowiskach mainframe, ale ostatecznie został rozszerzony na wszystkie obszary technologii komputerowych i sieciowych.

IBM System/360

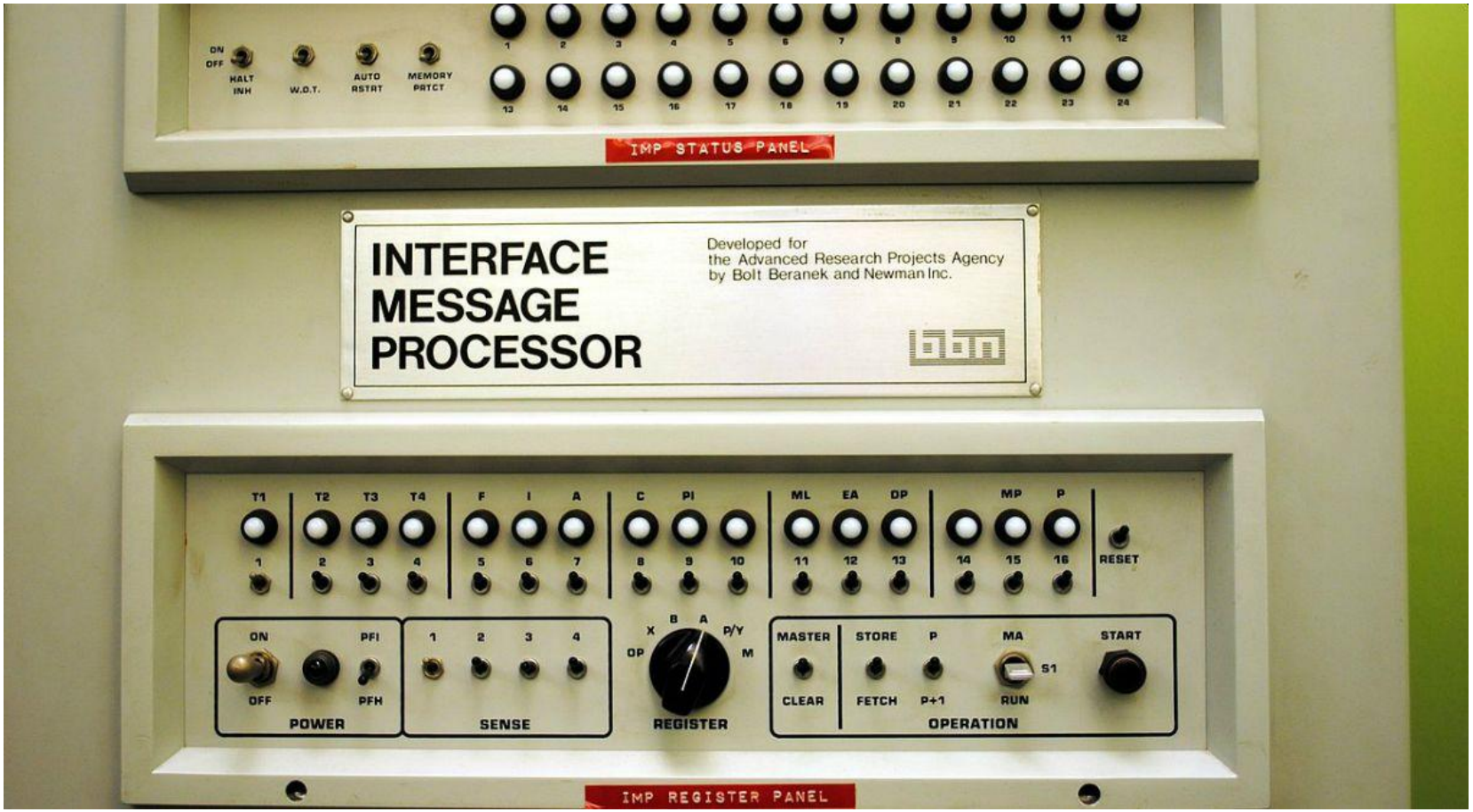
Inne osiągnięcia w latach 60. obejmowały wydanie w 1964 potężnego środowiska komputerowego IBM System/360 mainframe, które było szeroko wdrażane w rządowych, uniwersyteckich i korporacyjnych centrach obliczeniowych. W 1966 r. IBM wprowadził pierwszy dyskowy system pamięci masowej, który wykorzystywał 50 metalowych talerzy o szerokości 60 cm i miał pojemność 5 MB. IBM stworzył pierwszą dyskietkę w 1967. W 1969 Intel wypuścił układ RAM, który przechowywał 1 KB informacji, co w tamtych czasach było niesamowitym osiągnięciem inżynieryjnym.

Pierwsze sieci komputerowe - ARPANET



Oryginalny ARPANET połączył komputery w Stanford, University of California w Los Angeles (UCLA), University of California w Santa Barbara (UCSB) oraz University of Utah, z pierwszym węzłem zainstalowanym w Network Measurements Center UCLA.

Pierwsze sieci komputerowe - ARPANET



Panel sterowania urządzenia Interface Message Processor (IMP), które zostało użyte do przesłania pierwszej wiadomości internetowej źródło: Andrew Adams, Wikimedia Commons/CC BY-SA 3.0

Pierwsze sieci komputerowe – ARPANET

- Trudna droga pierwszej wiadomości internetowej

- ARPANET był tajnym projektem rządu Stanów Zjednoczonych, w którym w 1969 roku brały udział cztery uniwersytety. Pierwsza wiadomość w sieci została przesłana pomiędzy komputerami Uniwersytetu Kalifornijskiego w Los Angeles a Uniwersytetem Stanforda (także w Kalifornii).

- Nie wszystko poszło po myśli nadawców. Naukowcy z Los Angeles wysłali swoim kolegom w Stanford tajemniczy tekst, który składał się jedynie z dwóch liter: "LO". Był to efekt awarii komputera. Wiadomość miała się składać ze słowa "LOGIN" i dopiero po godzinie udało się przesłać jej pełną treść.

Sieć ALOHA

- Jednym z pierwszych projektów sieci komputerowych, rozpoczęto we wrześniu 1968 r. na Uniwersytecie Hawajskim pod kierownictwem Normana Abramsona i Franklina Kuo, a także Thomasa Gaardera, Shu Lina, Wesleya Petersona i Edwarda („Neda”) Weldona.

- Celem było wykorzystanie niedrogiego komercyjnego sprzętu radiowego do połączenia użytkowników na Oahu i innych hawajskich wyspach z centralnym komputerem współdzielącym czas na głównym kampusie Oahu.

- Pierwsza jednostka transmisji pakietowej została uruchomiona w czerwcu 1971 r. Terminale były podłączone do specjalnego przeznaczenia jednostki połączenia terminala za pomocą RS-232 z szybkością 9600 bitów/s

Sieć ALOHA

Sieć ALOHA

- Pure ALOHA
- Slotted ALOHA

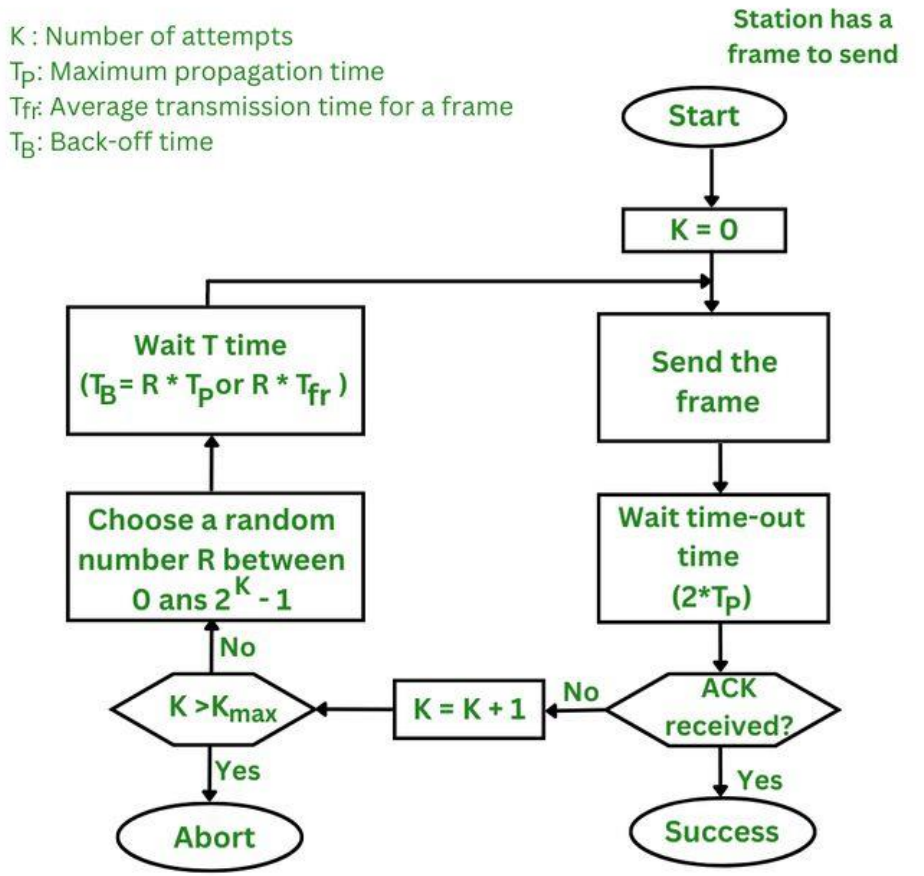
Pure ALOHA

- Pure ALOHA odnosi się do oryginalnego protokołu ALOHA. Idea polega na tym, że każda stacja wysyła ramkę, gdy tylko jest dostępna.
- Ponieważ istnieje tylko jeden kanał do udostępnienia, istnieje ryzyko, że ramki z różnych stacji będą się ze sobą kolidować.
- Pure ALOHA wykorzystuje potwierdzenia od odbiornika, aby zapewnić pomyślną transmisję.
- Gdy użytkownik wysyła ramkę, oczekuje potwierdzenia od odbiornika. Jeśli w wyznaczonym czasie nie zostanie odebrane żadne potwierdzenie, nadawca zakłada, że ramka nie została odebrana i ponownie ją przesyła.
- Gdy dwie ramki próbują zająć kanał jednocześnie, dochodzi do kolizji i obie ramki zostają zniekształcone.

Pure ALOHA

- Jeśli pierwszy bit nowej ramki nakłada się na ostatni bit ramki, która jest prawie ukończona, obie ramki zostaną całkowicie zniszczone i będą musiały zostać ponownie przesłane.
- Jeśli wszyscy użytkownicy ponownie prześlą swoje ramki w tym samym czasie po upływie limitu czasu, ramki ponownie się zderzą.
- Aby temu zapobiec, protokół ALOHA nakazuje, aby każdy użytkownik czekał losowo określoną ilość czasu, znaną jako back-off time, przed ponownym przesłaniem ramki.
- Ta losowość pomaga uniknąć dalszych kolizji.

Pure ALOHA


K : Number of attempts
T_P: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Station has a frame to send
Start
K = 0
Send the frame
Wait time-out time ($2*T_P$)
ACK received?
No
K = K + 1
$K > K_{max}$
No
Yes
Abort
Success
Yes
Choose a random number R between 0 ans $2^K - 1$
Wait T time ($T_B = R * T_P$ or $R * T_{fr}$)

Slotted ALOHA

- Slotted Aloha to po prostu zaawansowana wersja czystej Aloha, która pomaga w ulepszaniu sieci komunikacyjnej.
- Stacja musi czekać na początek następnego slotu, aby transmitować.
- Okres podatności jest skrócony o połowę w przeciwieństwie do Pure Aloha.
- Slotted Aloha pomaga w zmniejszaniu liczby kolizji poprzez prawidłowe wykorzystanie kanału, co zasadniczo skutkuje opóźnieniem użytkowników.
- W Slotted Aloha czas kanału jest podzielony na określone sloty czasowe.

Sieć ALOHA porównanie

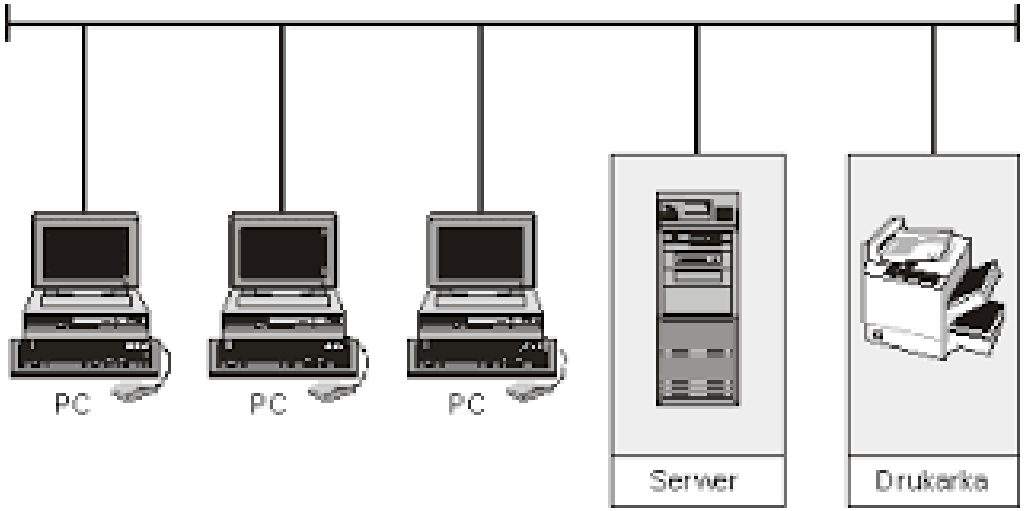
Pure Aloha	Slotted Aloha
Każda stacja może przesyłać dane w dowolnym momencie.	Dowolna stacja może transmitować dane na początku dowolnego przedziału czasowego.
Czas jest ciągły i nie jest globalnie zsynchronizowany.	Czas jest dyskretny i globalnie zsynchronizowany.
Czas podatności wynosi = 2 x Tt (czas transmisji)	Czas podatności wynosi= Tt (czas transmisji)
Prawdopodobieństwo pomyślnej transmisji pakietu danych wynosi $G \times e^{-2G}$	Prawdopodobieństwo pomyślnej transmisji pakietu danych wynosi $G \times e^{-G}$
Maksymalna wydajność 18.4%	Maksymalna wydajność 36.8%
Nie zmniejsza liczby kolizji o połowę	Zmniejsza liczbę kolizji o połowę i podwaja wydajność

* G - współczynnik prób (oczekiwana liczba pakietów przesłanych w slocie) w stanie n

Sieć ALOHA

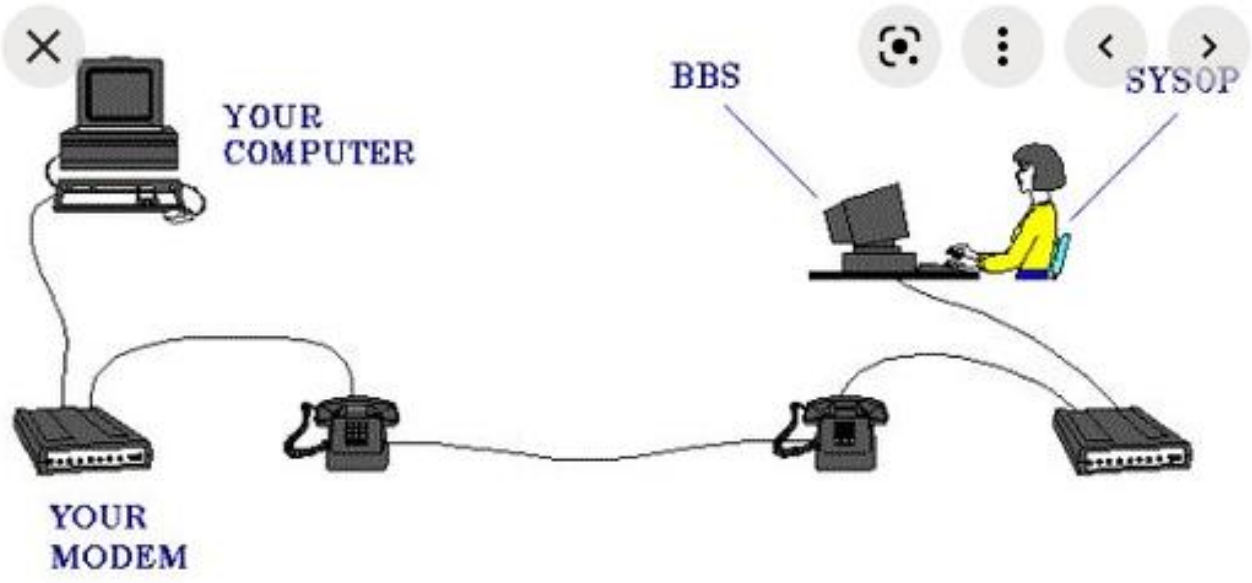
- Pomimo swojej prostoty i małej wydajności, szczelinowy protokół ALOHA znalazł zastosowanie nie tylko w kilku wczesnych eksperymentach.
- Jest używany, w wersji slotted ALOHA, m.in. w systemach GSM oraz UMTS.
- Wykorzystuje się go również w systemach dostępu do Internetu przez sieci telewizji kablowych.
- ALOHA jest protoplastą protokołu Ethernet.

Rozwój sieci komputerowych - minikomputery



Ponieważ komputery, a dokładnie minikomputery znalazły zastosowanie w firmach komercyjnych, także i tutaj pojawiła się potrzeba wzajemnego komunikowania się, np. między oddziałami tej samej firmy w celu wymiany i synchronizacji danych. W tym obszarze stosowano głównie rozwiązania autorskie pochodzące od firm, które były producentami sprzętu komputerowego (Xerox, Intel, DEC, IBM). W zdecydowanej większości protokoły te zostały całkowicie wyparte w sieciach lokalnych przez protokół Ethernet, natomiast ich elementy można znaleźć wśród protokołów stosowanych w centralach telefonicznych.

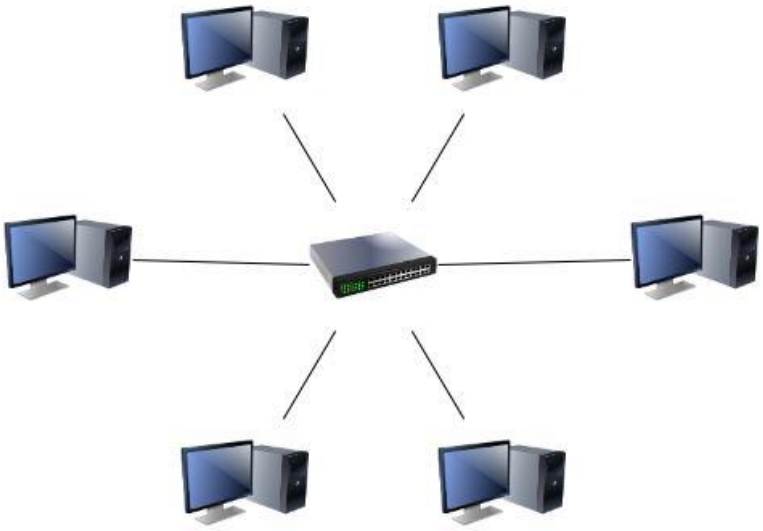
Bulletin Boards (BBS)



HOW YOU CONNECT TO A BULLETIN BOARD

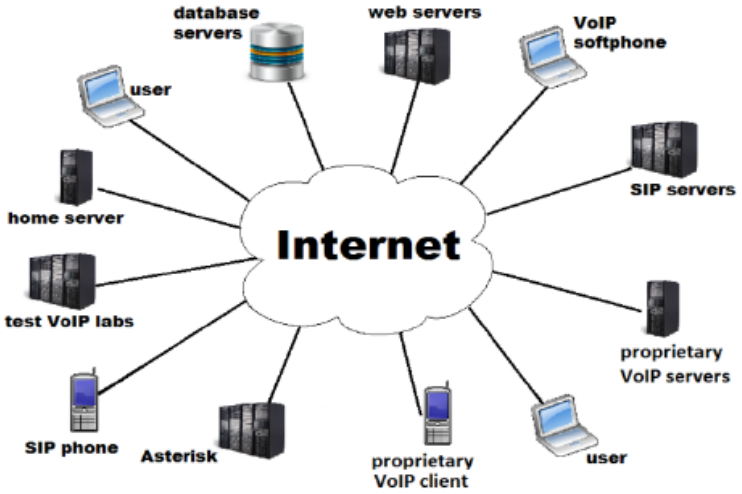
W latach 80tych XXw. opracowano sposób komunikacji typu punkt-punkt oparty na łączności modemowej wykorzystującej standardowe, komutowane łącza klasycznej sieci telefonicznej. Wykorzystując tę metodę stworzono specjalne centra zwane BBS'ami (ang. Bulletin Boards), pełniące rolę punktów kontaktowych, za pomocą których można było wymieniać wiadomości i pliki. Zaletą BBS'ów były: porównywalnie niższy koszt instalacji i utrzymania w stosunku do innych rozwiązań oraz tania metoda dostępu.

Sieci lokalne



Różnorodność sprzętu sieciowego, a przede wszystkim jego cena powstrzymywały firmy przed podejmowaniem decyzji o inwestowaniu w nowe technologie. Lęk przed chybionymi decyzjami wynikał też z niestabilnej sytuacji w obszarze komputerów osobistych. Szybki rozwój technologii oznaczał z jednej strony wzrost efektywności, z drugiej strony wymuszał zbyt częstą wymianę sprzętu. Sytuacja zmieniła się wraz z opracowaniem standardów dotyczących sieci lokalnych, co dawało gwarancje kompatybilności sprzętowej i chroniło inwestycje

Internet



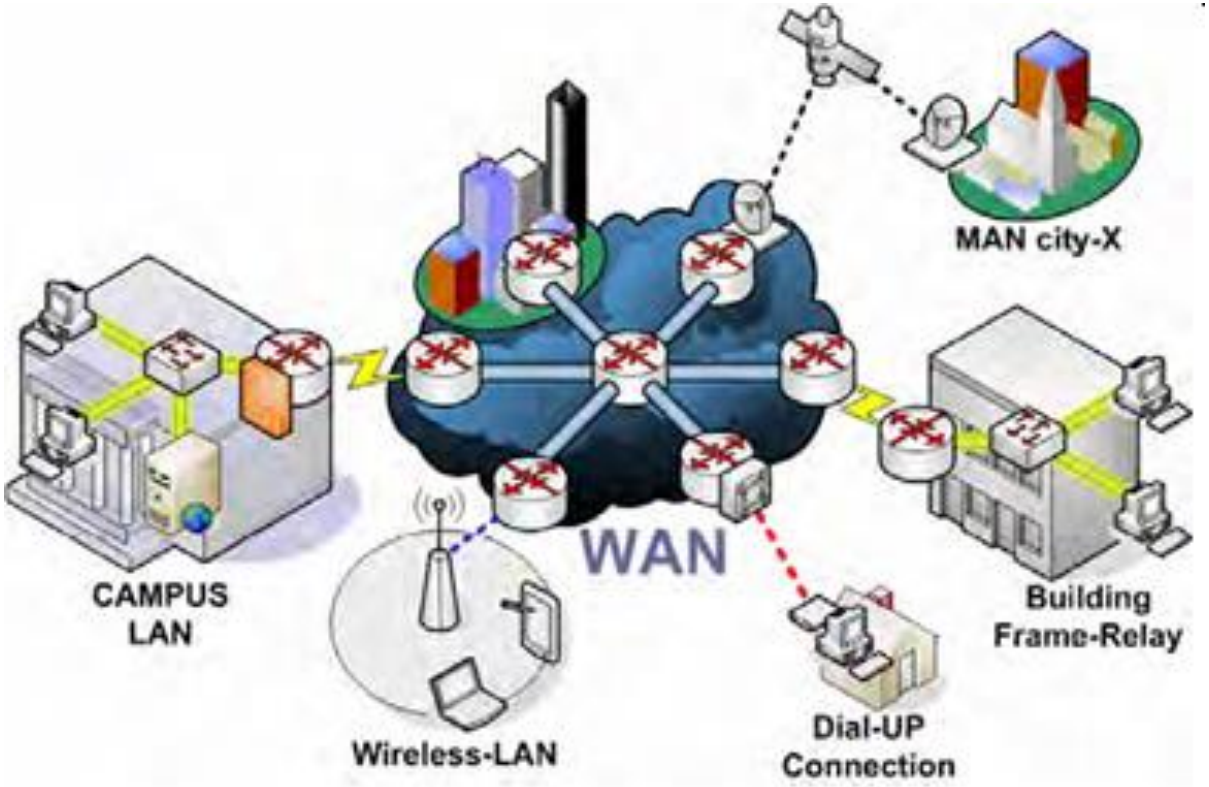
Funkcjonująca obecnie konstrukcja Internetu, zarówno na poziomie globalnym jak i pojedynczej sieci lokalnej oparta jest na tych samych zasadach jakie opracowano i opublikowano na przełomie lat 80tych i 90tych XX w. Zasadnicze zagadnienia, które związane są z budową Internetu dotyczą takich spraw jak:

- łączenie komputerów w lokalną sieć komputerową,
- podłączanie do sieci pojedynczych komputerów w sytuacji dużych odległości,
- rozbudowa lokalnych sieci komputerowych,
- komunikacja między sieciami lokalnymi,
- usługi sieciowe,
- bezpieczeństwo sieci,
- zarządzanie i monitoring sieci.

Typy sieci

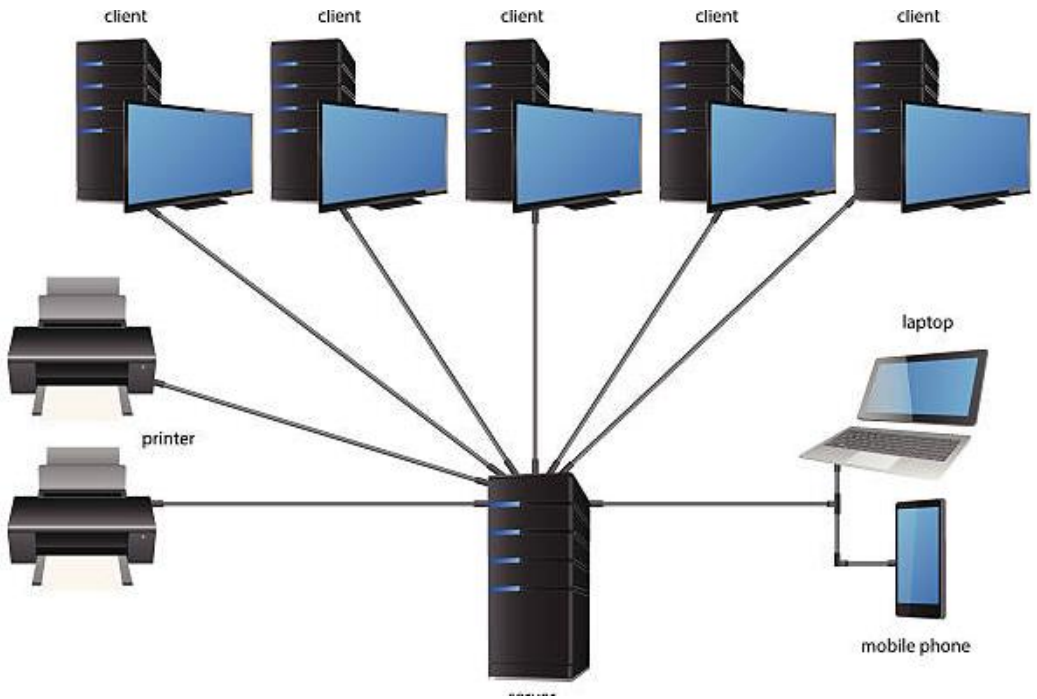
- WAN (Wide Area Network)
- MAN (Metropolitan Area Network)
- Kampusowe (uczelnianie, akademickie)
- LAN (Local Area Network)
- PAN (Private Area Network)

WAN



Sieci rozległe charakteryzują przede wszystkim długie połączenia zlokalizowane na stosunkowo dużym obszarze takim jak województwo, kraj, kontynent czy cały glob.

LAN

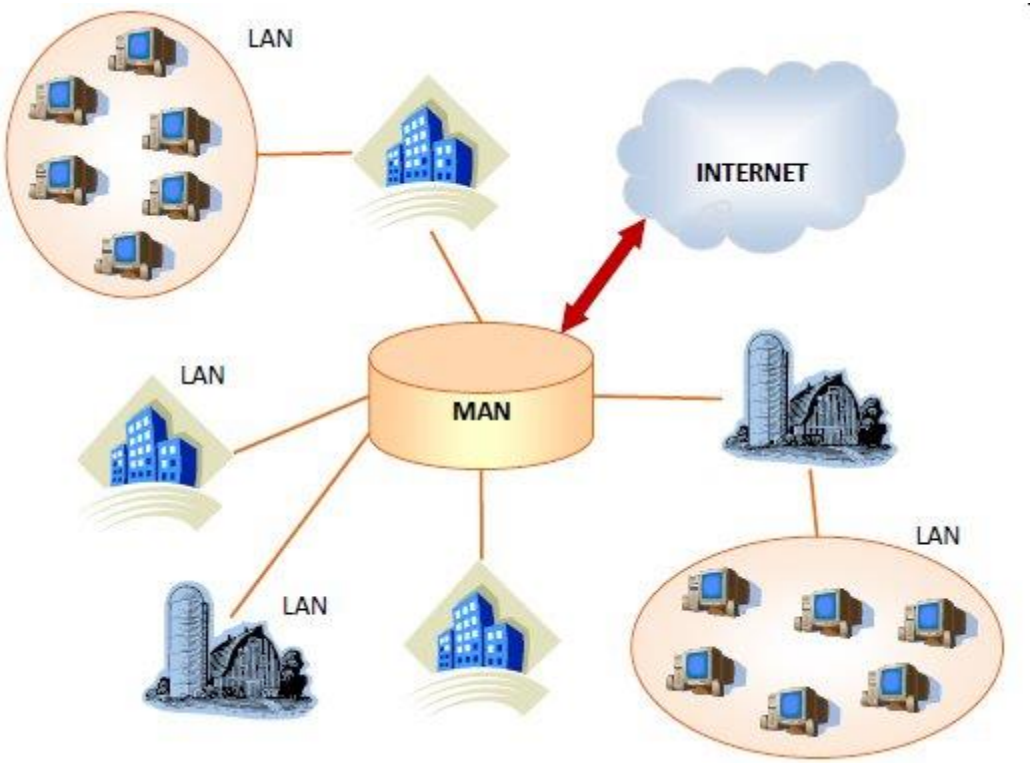


- Sieci lokalne dotyczą instalacji zlokalizowanych na stosunkowo niewielkim obszarze. Teoretyczna średnica sieci lokalnej może wynosić nawet kilkaset metrów, jednak po uwzględnieniu geometrii pomieszczeń obszar instalacji ogranicza się do jednego budynku lub jego części, np. piętra. W sieciach lokalnych stosuje się krótkie łącza (do ok.. 100m) o wysokiej przepustowości lub rozwiązania oparte na technice radiowej. Sieci lokalne charakteryzuje też wysoka niezawodność działania

Sieci kampusowe

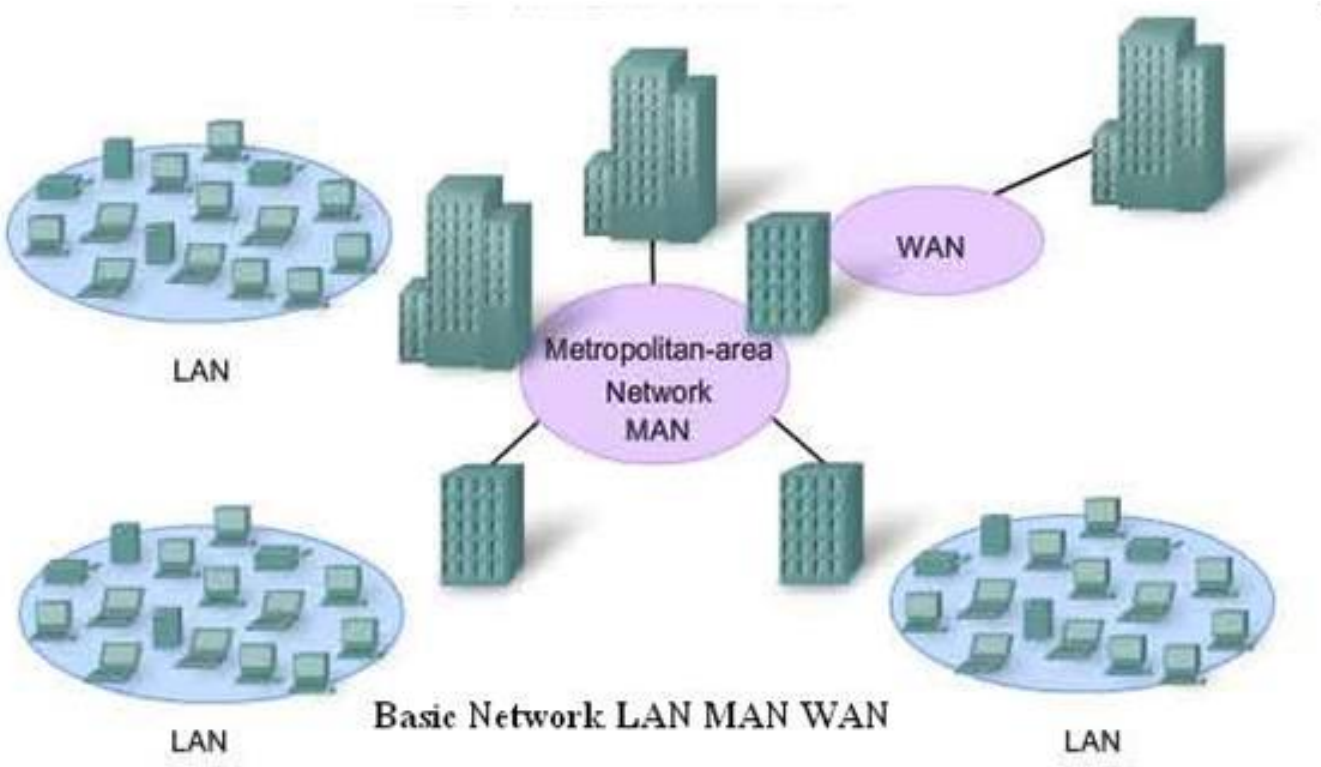
W przypadku uniwersytetów na ogół stosuje się rozwiązanie polegające na łączeniu poszczególnych, wewnętrznych sieci lokalnych łączami charakterystycznymi dla technik stosowanych w budowie lokalnych, a nie rozległych sieci komputerowych.

MAN

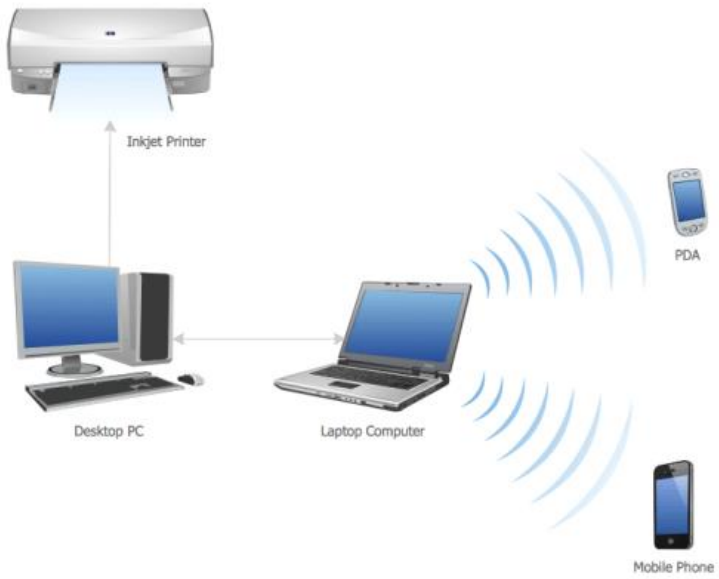


- Sieci metropolitalne przypominają swoją budową zarówno sieci kampusowe jak i sieci rozległe. Ich zadaniem jest łączenie wielu sieci lokalnych znajdujących się w obrębie aglomeracji miejskiej, co nadal stanowi stosunkowo niewielki obszar. Jednak w tym przypadku względy formalne oraz względy bezpieczeństwa sprawiają, że połączenia te mają na ogół charakter typowy dla sieci rozległych. Dodatkowo, do zadań sieci metropolitalnych należy łączenie indywidualnych komputerów, głównie osób prywatnych do Internetu.

LAN MAN WAN - porównanie



PAN



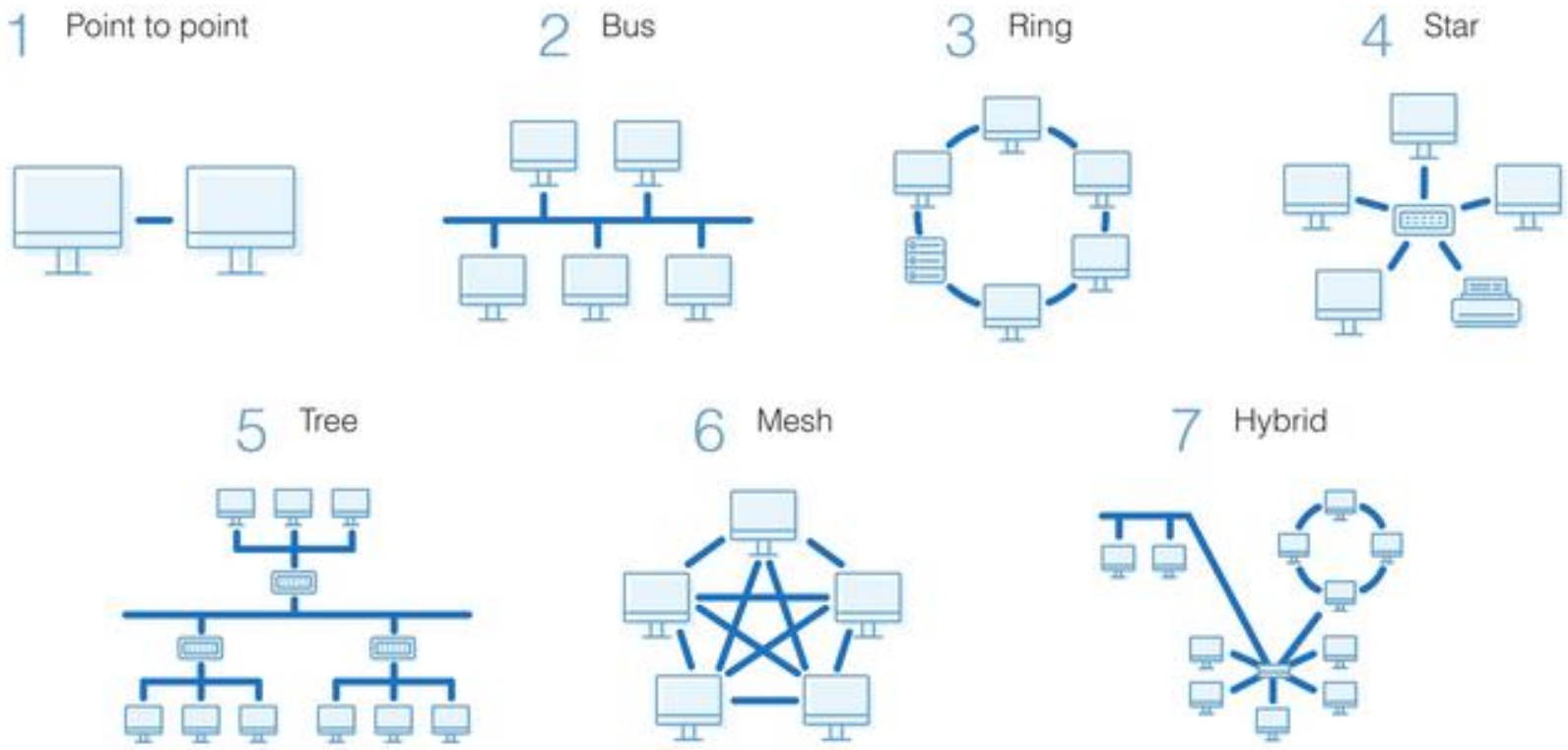
- Sieci prywatne (PAN), to konstrukcje stosowane głównie w domach i niewielkich biurach. Charakteryzuje je niewielki zasięg geograficzny (do ok. 10m) i dość duża różnorodność mediów, jak:
  - skrętka
  - sieć bezprzewodowa
  - bluetooth
  - podczerwień
  - inne

Topologie sieci

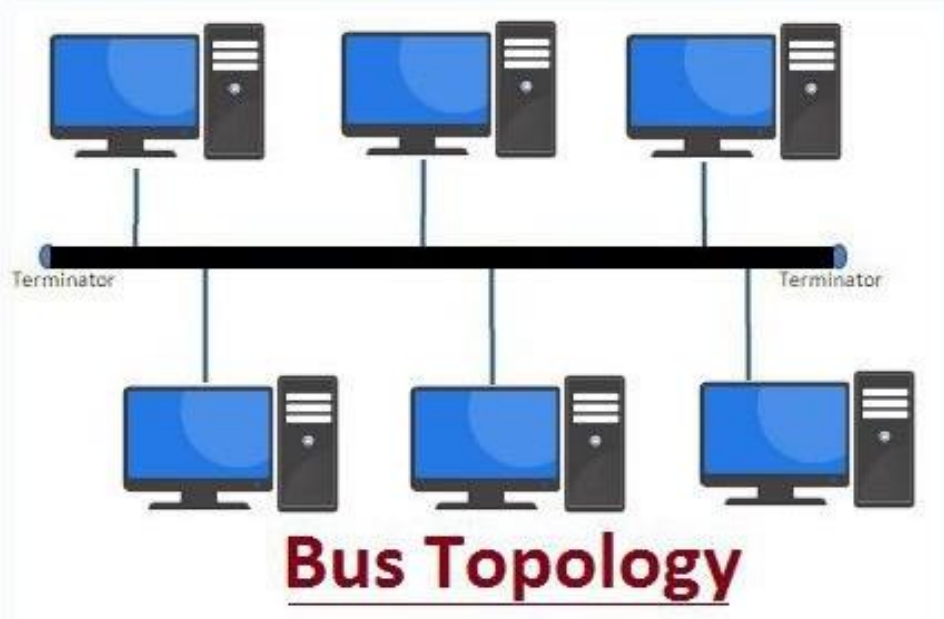
Topologia określająca sposób łączenia poszczególnych urządzeń sieciowych.

- Fizyczne topologie sieci to:
  - magistrali,
  - pierścienia,
  - podwójnego pierścienia,
  - gwiazdy,
  - rozszerzonej gwiazdy,
  - hierarchiczna,
  - siatki.

Topologie sieci

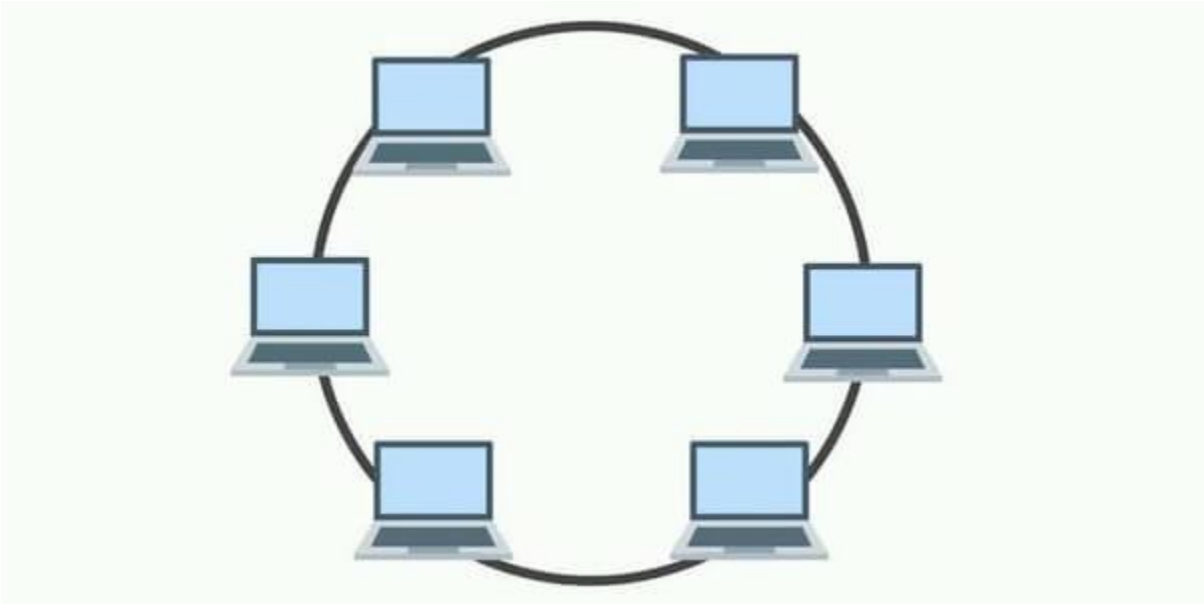


Topologia magistrali



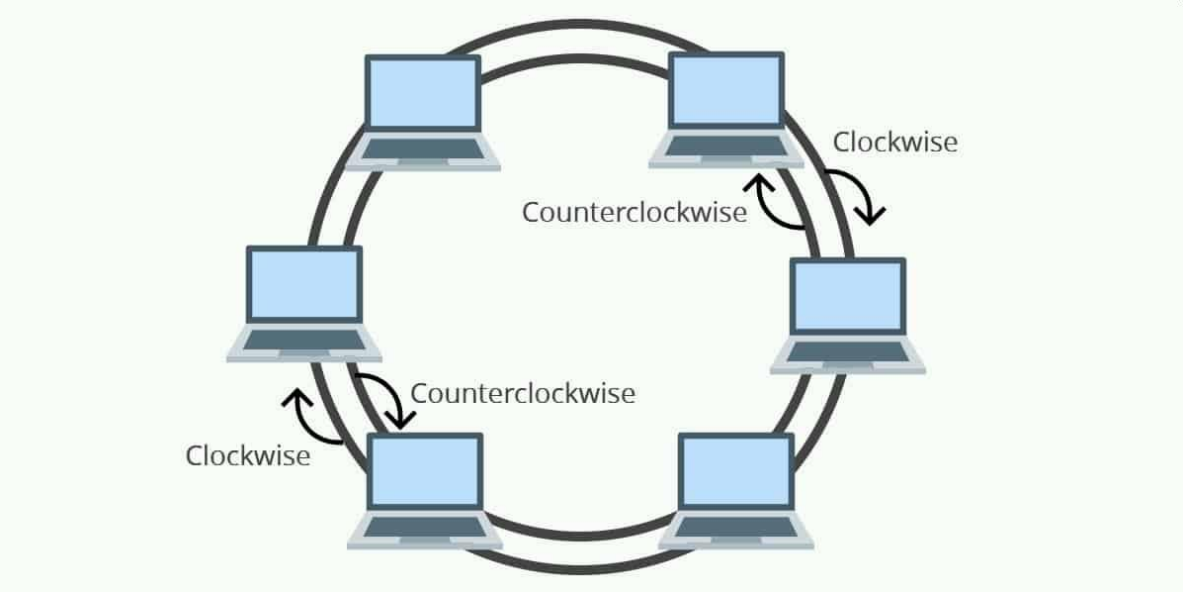
- Topologia magistrali charakteryzuje się tym, że wszystkie urządzenia podłączone są do jednego, współdzielonego medium fizycznego, którym zazwyczaj jest kabel koncentryczny zakończony z obu stron terminatorami (oporniki o parametrach dostosowanych do typu kabla).Topologię magistrali stosuje się do budowy lokalnych sieci komputerowych. Zaletą tej topologii jest niska cena wynikająca z małego zużycia kabli i braku urządzeń pośredniczących w dostępie do medium. Do zalet należy zaliczyć także łatwość instalacji. Wadą są ograniczenia związane z rozbudową sieci i wrażliwość na awarię. Przerwanie magistrali w jednym miejscu oznacza awarię całej sieci.

Topologia pierścienia



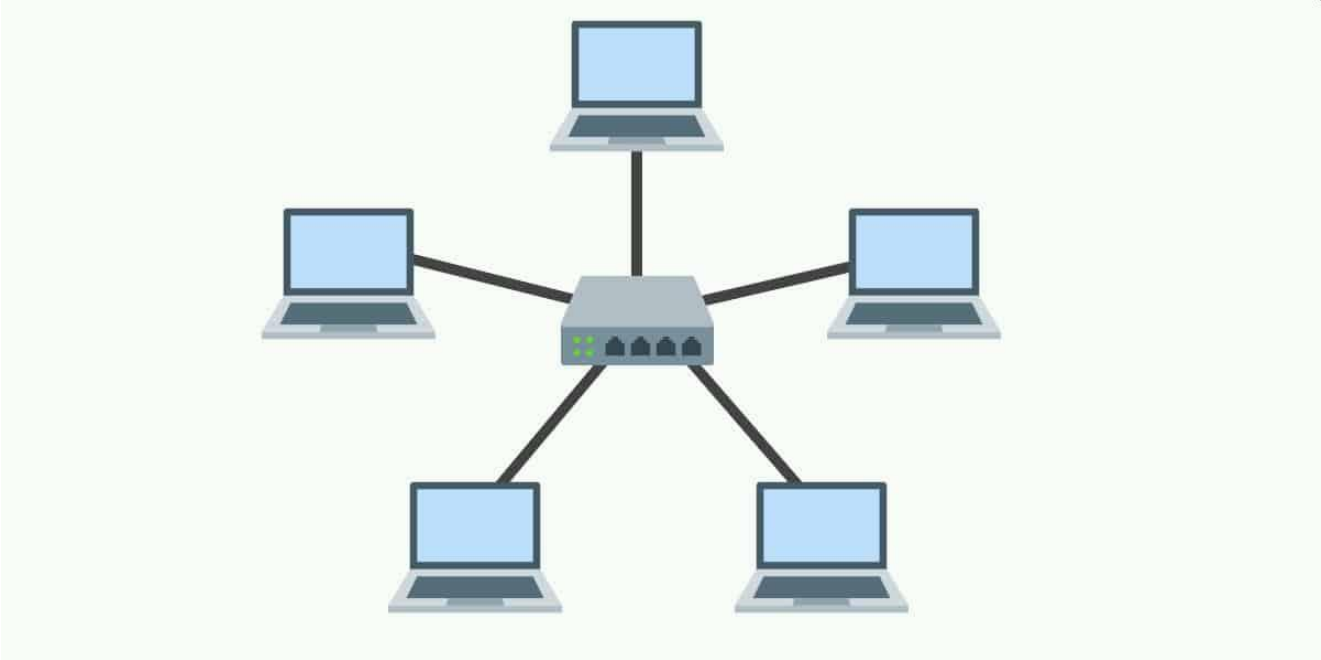
Konstrukcja topologii pierścienia polega na bezpośrednim łączeniu urządzeń (każde urządzenie połączone jest z dwoma sąsiednimi), tak że całość tworzy krąg. Topologia ta stosowana jest głównie do budowy lokalnych sieci komputerowych. Transmisja w sieci zbudowanej w oparciu o tę topologię polega na przekazywaniu żetonu dostępu. Oprócz tego, każde urządzenie pełni rolę regeneratora sygnału. Podobnie jak w przypadku topologii magistrali zaletą topologii pierścienia jest niska cena wynikająca z małego zużycia kabli i braku aktywnych urządzeń pośredniczących w komunikacji między komputerami. Dodatkowo do budowy sieci w tej topologii można użyć różnych mediów transmisyjnych (kabel koncentryczny, skrętkę, kable światłowodowe). Wadą tej topologii są ograniczenia i utrudnienia związane z rozbudową i konserwacją sieci. Uszkodzenie jednego z urządzeń lub łączy oznacza przerwę w pracy całej sieci.

Topologia podwójnego pierścienia



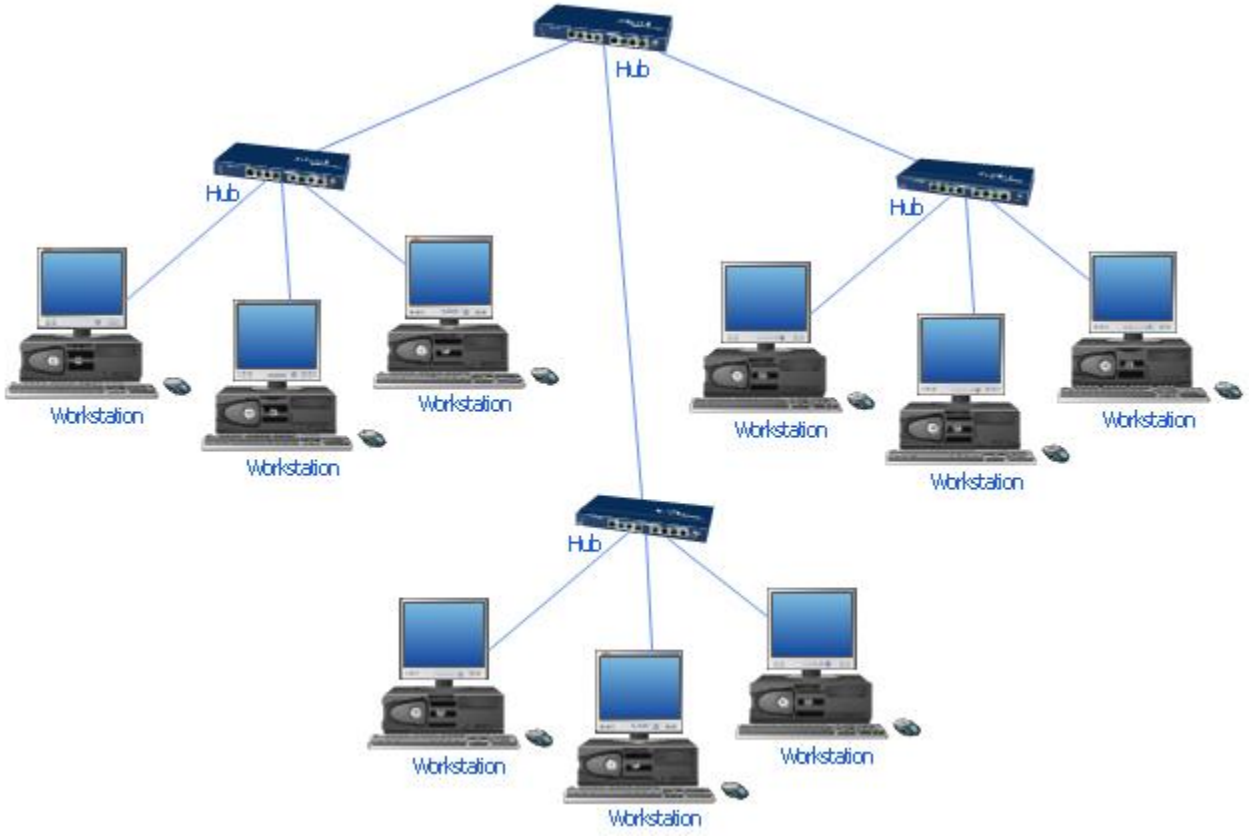
Topologia podwójnego pierścienia polega na tych samych zasadach, co topologia pierścienia, z tą różnicą, że urządzenia połączone są podwójnymi łączami, co pozwala na zachowanie transmisji w obszarach ograniczonych punktami awarii. W przypadku jednego punktu uszkodzenia sieć zachowuje możliwość działania w pełnym zakresie.Tego typu topologie stosowane są w budowie sieci szkieletowych lub w sieciach kampusowych i metropolitalnych.

Topologia gwiazdy



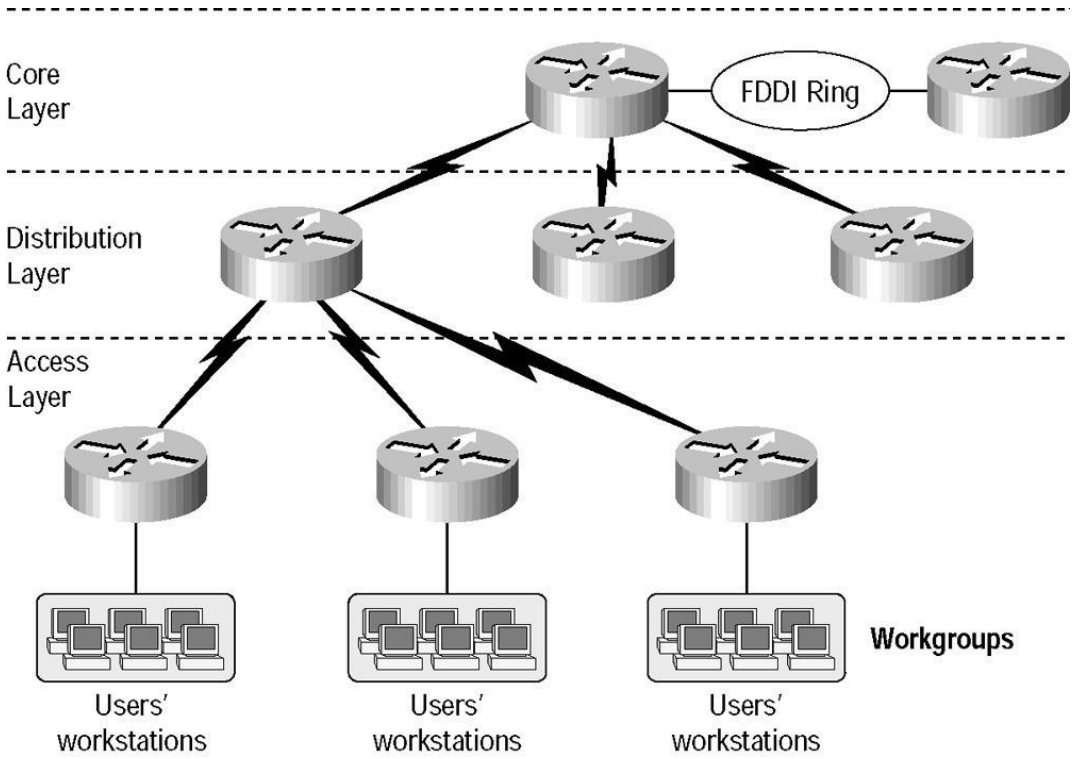
- W topologii gwiazdy wszystkie urządzenia połączone są w jednym wspólnym punkcie, w którym znajduje się aktywne urządzenie pośredniczące (koncentrator) pełniące rolę regeneratora sygnału.Łączenie urządzeń może odbywać się przy pomocy różnych mediów transmisyjnych. Istotną zaletą tej topologii jest niewątpliwie przejrzystość konstrukcji i odporność całej sieci na awarię zarówno urządzeń jak i łączy. Wadą tej topologii jest wysoki koszt okablowania oraz dodatkowy koszt związany z obecnością koncentratora.

Topologia gwiazdy rozszerzonej



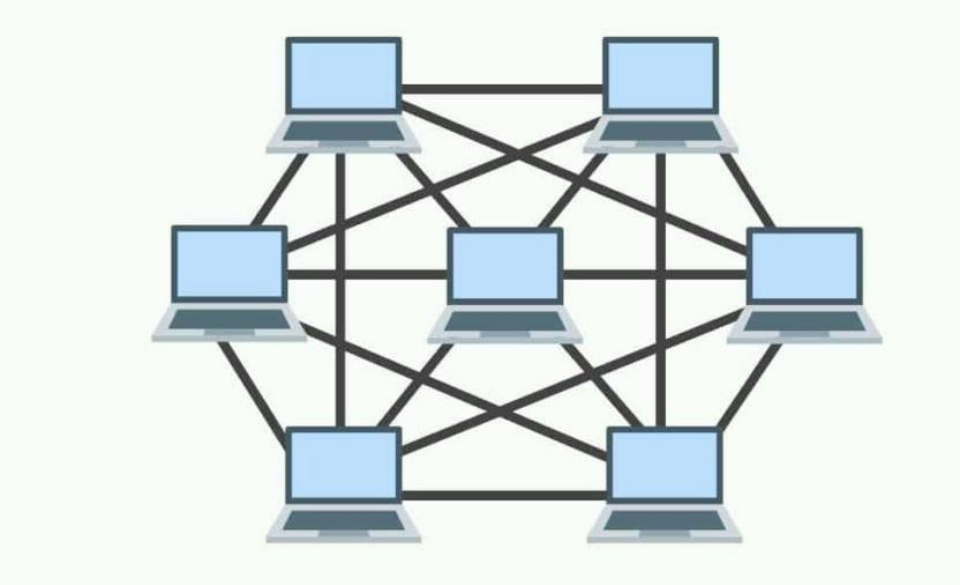
Podstawą konstrukcji topologii rozszerzonej gwiazdy jest topologia gwiazdy ze wszystkimi zaletami i wadami. Topologia ta stosowana jest głównie w przypadku rozbudowanych sieci lokalnych oraz sieci kampusowych.

Topologia hierarchiczna



Topologia hierarchiczna jest łudząco podobna do topologii rozszerzonej gwiazdy jednak różni się co do sposobu działania. W topologii hierarchicznej urządzenia aktywne oprócz regeneracji sygnału pełnią rolę urządzeń sterujących dostępem do sieci.

Topologia siatki

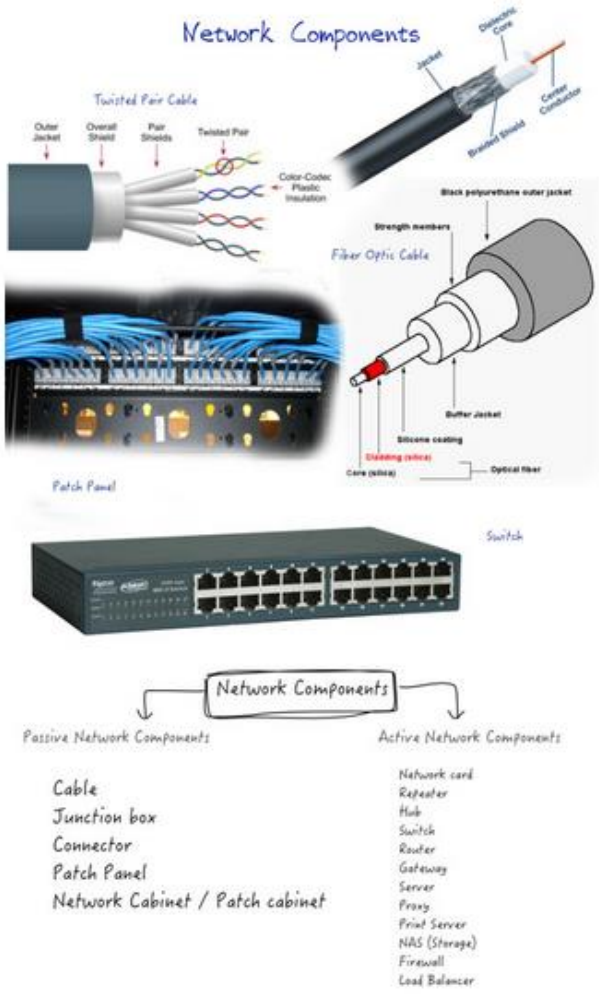


- Topologia siatki jest typowa dla sieci metropolitalnych i sieci rozległych. Konstrukcja tej topologii oparta jest na takim łączeniu urządzeń, że każde z nich połączone jest z więcej niż jednym urządzeniem.Tego typu rozwiązania stosowane są w celu zapewnienia redundantnych połączeń między wszystkimi urządzeniami.

Urządzenia sieciowe

Urządzenia sieciowe stanowią trzeci element fizycznej budowy sieci. Zaliczamy do nich zarówno urządzenia bierne: kable koncentratory bierne jak i elementy aktywne: huby mosty przełączniki routery konwertery modemy punkty dostępowe sieci bezprzewodowych oraz urządzenia końcowe: stacje robocze serwery drukarki terminale inne sieciowe urządzenia peryferyjne

Urządzenia sieciowe pasywne i aktywne



Urządzenia sieciowe pasywne i aktywne

- Urządzenia sieciowe pasywne (bierne) to wszelkiego rodzaju peryferia sieciowe nie wymagające dodatkowego zasilania, oraz takie, które nie powodują zmian w przesyłanych sygnałach (wzmocnienie, filtracja, regeneracja)
- Zwykle do tej grupy zaliczamy nośniki sygnału tj. kable sieciowe, światłowody, złącza i inne

Urządzenia sieciowe pasywne i aktywne

- Urządzenia aktywne to wszelkiego rodzaju peryferia, które mają możliwość przetwarzania sygnałów, tj. wzmacniania, filtracji, rozdzielnia, łączenie transmisji na styku różnych mediów itp.,
- Urządzenia aktywne wymagają zasilania, są to m.in. Routery, switch`e, regeneneratory sygnałów, bramy, mosty, modemy, punkty dostępowe i inne

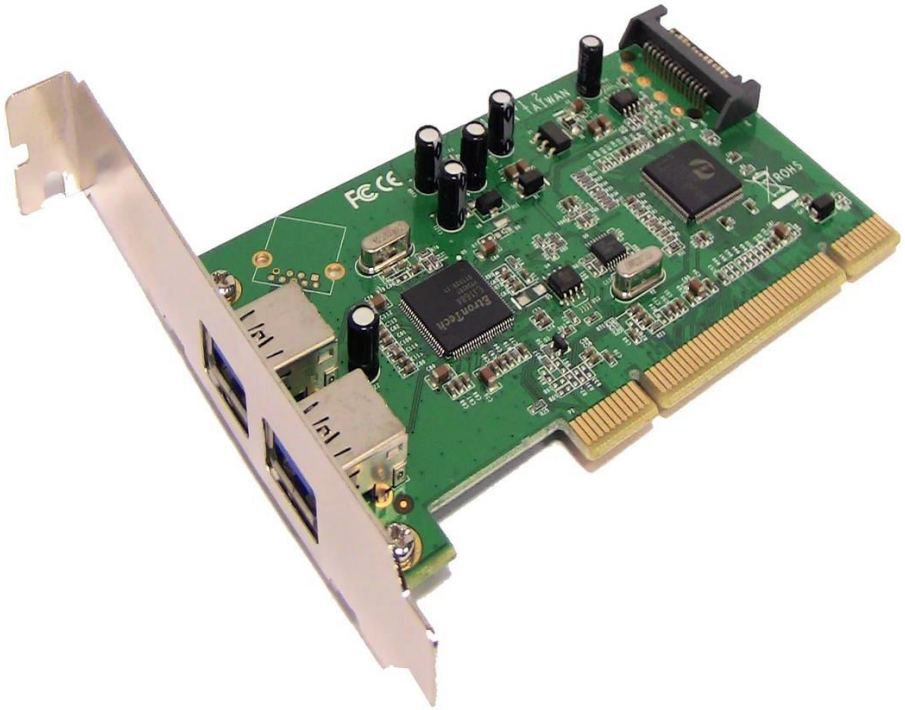
Przykłady urządzeń sieciowych

- Modemy
- Karty sieciowe przewodowe i bezprzewodowe
- Konwertery
- Koncentratory (huby)
- Punkty dostępowe WLAN
- Routery

Modemy

Zewnętrzny modem wykorzystujący połączenia komutowane realizowane w ramach telefonii tradycyjnej. Obecnie stosowany jest głównie do celów administracyjnych, gdy wymagany jest zapasowy dostęp do urządzeń sieciowych w przypadku awarii sieci komputerowej.

Modemy



Przykład wewnętrznego modemu do połączeń komutowanych. Wadą tego typu modemów jest brak pełnej kontroli przez użytkownika, co jest szczególnie dotkliwe (finansowo) w przypadku „zarażenia” systemu operacyjnego wirusem, którego działanie polega na wykonywaniu połączeń komutowanych bez wiedzy użytkownika.

Połączenie modemowe

Konwertery

Mediakonwerter umożliwiający łączenie dwóch urządzeń, wyposażonych w interfejsy sieciowe dostosowane do różnego rodzaju mediów:skrętka/światłowód, kabel koncentryczny/skrętka, kabel koncentryczny/światłowód, złącze AUI/(skrętka albo kabel koncentryczny, albo światłowód). Mediakonwertery stosowane są najczęściej do łączenia dwóch odległych urządzeń za pomocą linii światłowodowych.

Koncentrator (hub)

- Przykład typowego koncentratora (huba) do zastosowań w niewielkich biurach, grupach roboczych, czy w domach.

Punkt dostępowy WLAN

Przykład standardowego punktu dostępowego dla sieci bezprzewodowych. Zastosowanie odpowiedniej anteny w sposób zasadniczy poprawia jakość połączeń z urządzeniami końcowymi.

Karty sieciowe

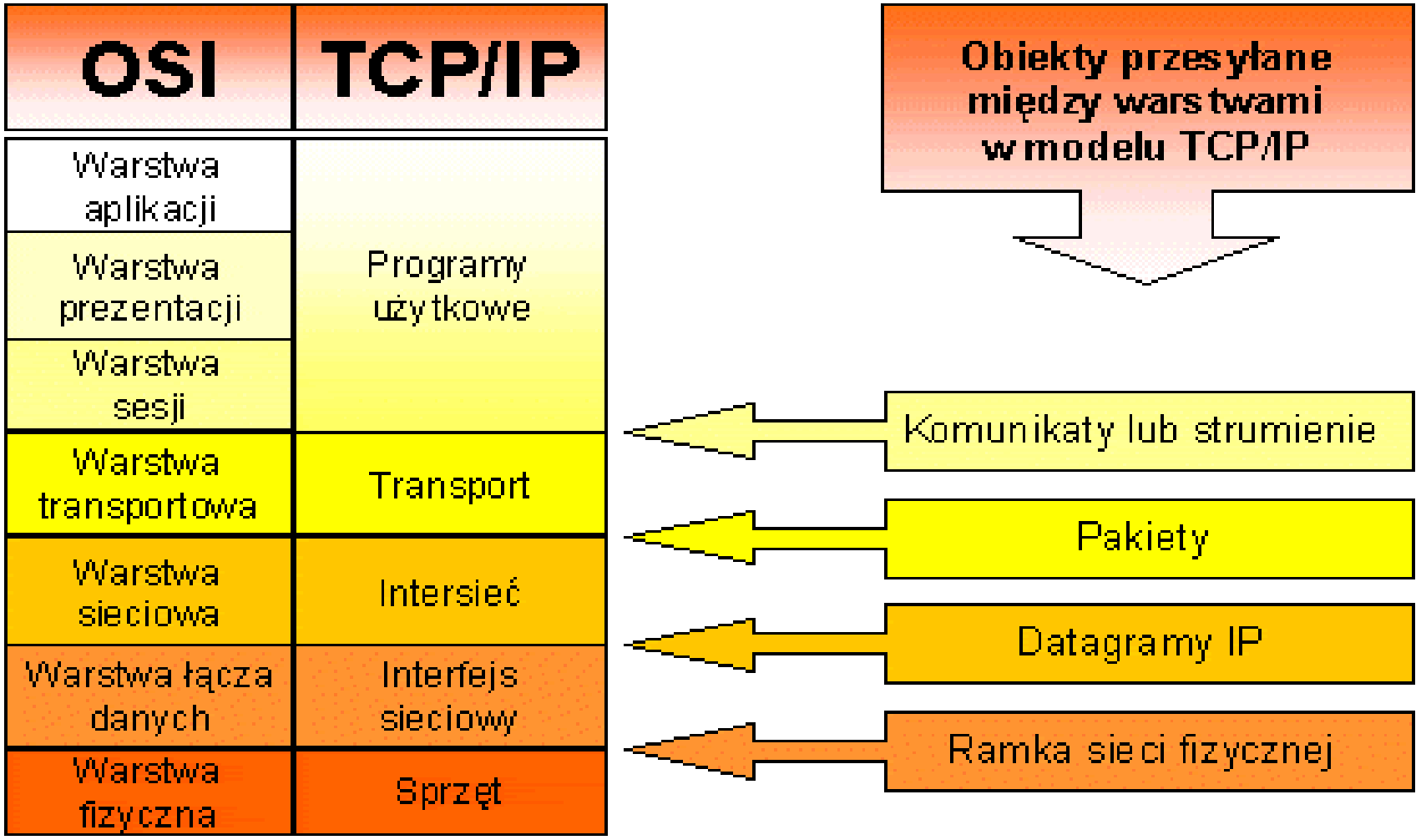
Routery

Pozwalają na łączenie ze sobą różnych sieci, mogą łączyć dane z różnych mediów np. sieci bezprzewodowych i sieci kablowych, czy światłowodowych

Model TCP/IP - ISO/OSI

- Model TCP/IP jest określany jest jako model protokołów.
- Każda z jego warstw wykonuje konkretne zadania, do realizacji który wykorzystywane są konkretne protokoły,
- Model ISO/OSI natomiast zwany modelem odniesienia, stosowany jest raczej do analizy, która pozwala lepiej zrozumieć procesy komunikacyjne zachodzące w sieci.
- W przypadku modelu TCP/IP wyróżnić możemy 4 warstwy:
- aplikacji,
- transportu,
- Internetowa,
- dostępu do sieci.

Model TCP/IP - ISO/OSI



Adresacja IP

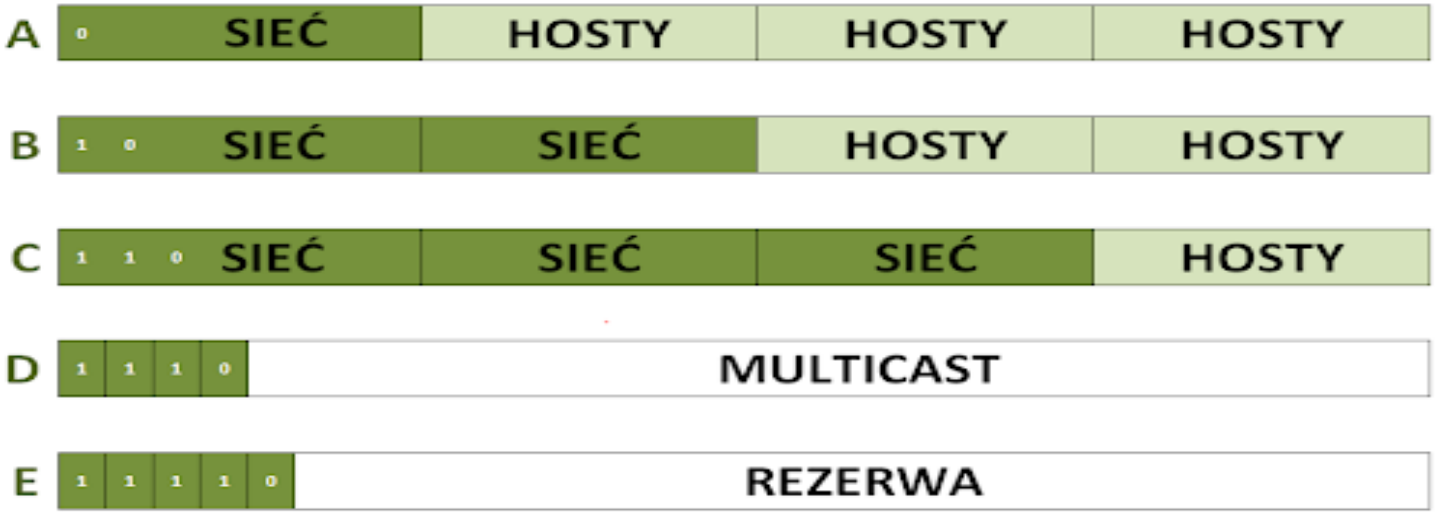
- 32 bity, 4 oktety po 8 bitów,

- Numeracja binarna – dla maszyn
- 10010101.01110010.10011111.00000011

- Numeracja dziesiętna – dla ludzi
- 149.114.159.3

- Zamiana postaci liczb binarnych na dziesiętne

Klasy adresów IP v4



Klasy adresów IP v4

Klasa adresu	Zakres pierwszego oktetu	Bity pierwszego oktetu	Części adresu: sieci (S) i hosta (H)	Domyślna maska	Możliwa liczba sieci	Możliwa liczba hostów
A	1 – 127	00000000 – 01111111	S.H.H.H	255.0.0.0	128 (2^7)	16 777 214 ($2^{24} - 2$)
B	128 – 191	100000000 – 10111111	S.S.H.H	255.255.0.0	16 384 (2^{14})	65 384 ($2^{14} - 2$)
C	192 – 223	11000000 – 11101111	S.S.S.H	255.255.255.0	2 097 150 (2^{21})	254 ($2^8 - 2$)

Adresy specjalne (nierutowalne) i zastrzeżone

- Dla klasy A:
- 10.0.0.0 – 10.255.255.255

- Dla klasy B:
- 172.16.0.0 – 172.31.255.255

- Dla klasy C:
- 192.168.0.0 – 192.168.255.255

- 127.0.0.0 - *loopback*
- 0.0.0.0 - *broadcast*

Maski sieciowe

- Celem stosowania maski jest wyznaczenie
- jaka część adresu identyfikuje sieć lub
- podsieć (NID), a jaka identyfikuje
- urządzenie w ramach tej podsieci (HID),

- Adres podsieci wyznacza się przez logiczna
- koniunkcje adresu IP i maski,

- Maska ma taka sama długość, jak adres IP
- (czyli 32-bity dla IPv4, 128-bitów dla IPv6)

Maski sieciowe

- Zasady zamiany notacji dziesiętnej, binarnej i szesnastkowej
- Stosowane do wydzielenia podsieci z dużej sieci,
- Pozwalają na adresacje większej liczby hostów w skali globalnej - likwidują potencjalne „dziury” puli adresów
- Możliwość stosowania dowolnej liczby (nie 8,16 czy 24) bitów na określenie adresu sieci
- Praca w układzie {nr sieci}{nr podsieci}{nr hosta}

Maski sieciowe

- Reprezentacja maski MUSI* składać się z kolejno po sobie następujących bitów „1”

- Poprawne
- 11111111.11111111.11111111.11000000

- Niepoprawne
- 11111111.11111111.11111110.11000011

Maski sieciowe - notacje

- Zapis pełny – cala maska binarnie lub dziesiętnie
- 11111111.11111111.11111111.00000000
- 255.255.255.0

- Zapis skrócony – tylko ostatni oktet
- .128

- Zapis skrócony – liczba bitów „1” w masce
- adres IP/24 149.156.114.3/24

- Zapis „trójkowy” – oznacza adres klasy B sieci
- 149.156.x.x, same 1 w polu adresu i same 0 w polu id hosta {149.156,-1,0}

NAT, Maskarada adresów IPv4

Technika polegająca na zmianie adresu źródłowego pakietu IP na inny.

Maskarada dla wybranych klasy adresów IPv4:

- dla klasy A - adresy z zakresu
- 10.0.0.0 - 10.255.255.255
- dla klasy B - adresy z zakresu
- 172.16.0.0 - 172.31.255.255
- dla klasy C - adresy z zakresu
- 192.168.0.0 - 192.168.255.255

NAT, Maskarada - zastosowania

- ukrycie (zamaskowanie) adresów IP komputerów w sieci przez router podłączony do internetu
- dostęp do internetu komputerom nie posiadającym publicznego adresu IP
- ochrona komputerów nawet jeżeli mają publiczne adresy IP - maskarada jest jedną z odmian firewalla.
- NAT zamienia prywatne adresy IP, jakimi posługują się komputery w sieci LAN na publiczny adres bramy internetowej, którą może być inny komputer lub ruter. Dzięki NAT każdy komputer w LAN może uzyskać dostęp do internetu, gdyż ruter na bieżąco przetwarza prywatne adresy IP użytkowników LAN na publiczny adres IP wymagany do komunikacji w internecie
- Maskarada (IP Masquerading) polega na translacji adresów (NAT-Network Adress Translation), dzięki czemu możliwe jest udostępnienie połączenia z internetem wszystkim komputerom

Dziękuję za uwagę