Sieci komputerowe

dr inż. Sławomir Samolej
email: ssamolej@prz-rzeszow.pl
WWW: ssamolej.prz-rzeszow.pl

Slajdy zostały przygotowane
na podstawie materiałów opublikowanych na
(http://wazniak.mimuw.edu.pl/

Literatura

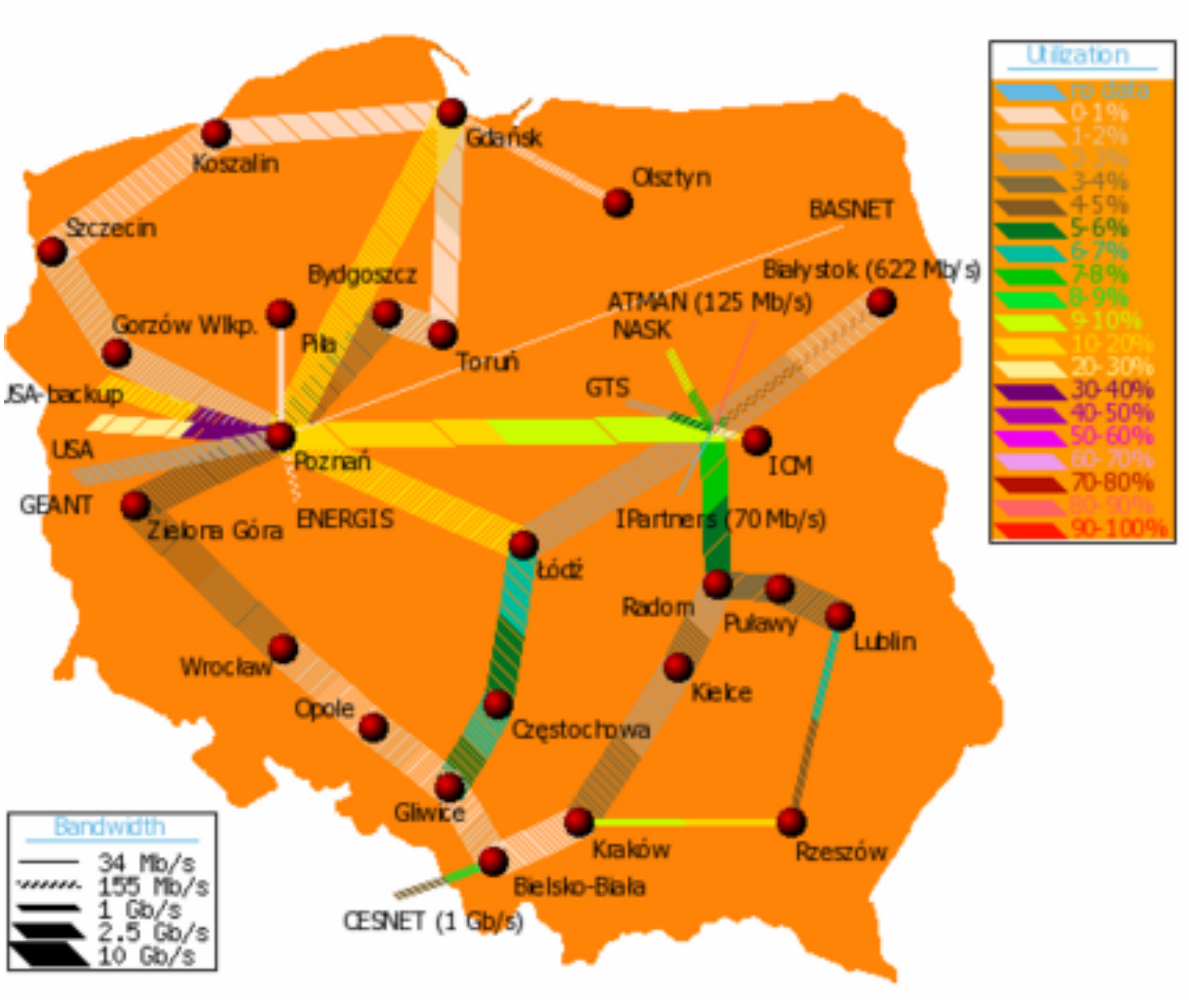
- K. Krysiak, *Sieci komputerowe - kompedium.* Helion, Gliwice 2003

Wprowadzenie

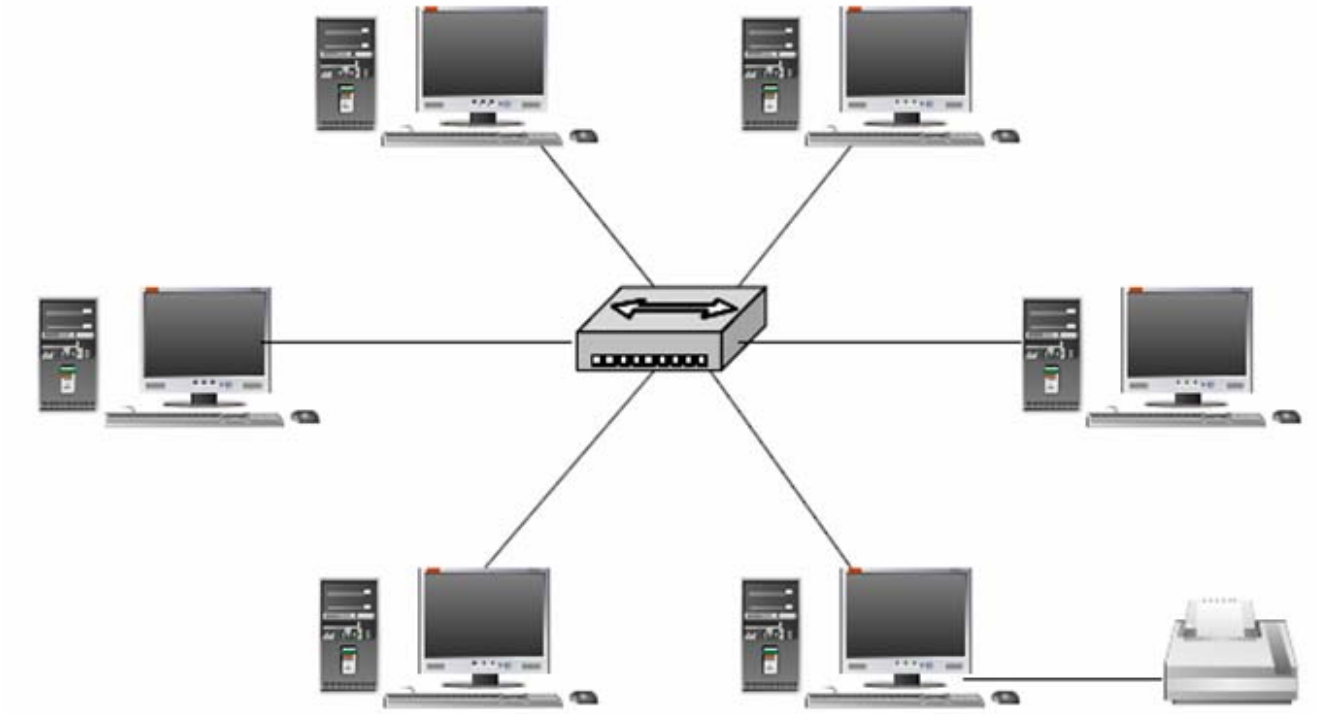
Definicja i typy sieci kompuerowych

- Sieć komputerowa to medium umożliwiające połączenie dwóch lub więcej komputerów w celu wzajemnego komunikowania się.
- Typy sieci:
  - WAN (Wide Area Network)
  - LAN (Local Area Network)
  - Sieci kampusowe
  - MAN (Metropolitan Area Network)
  - PAN (Private Area Network)

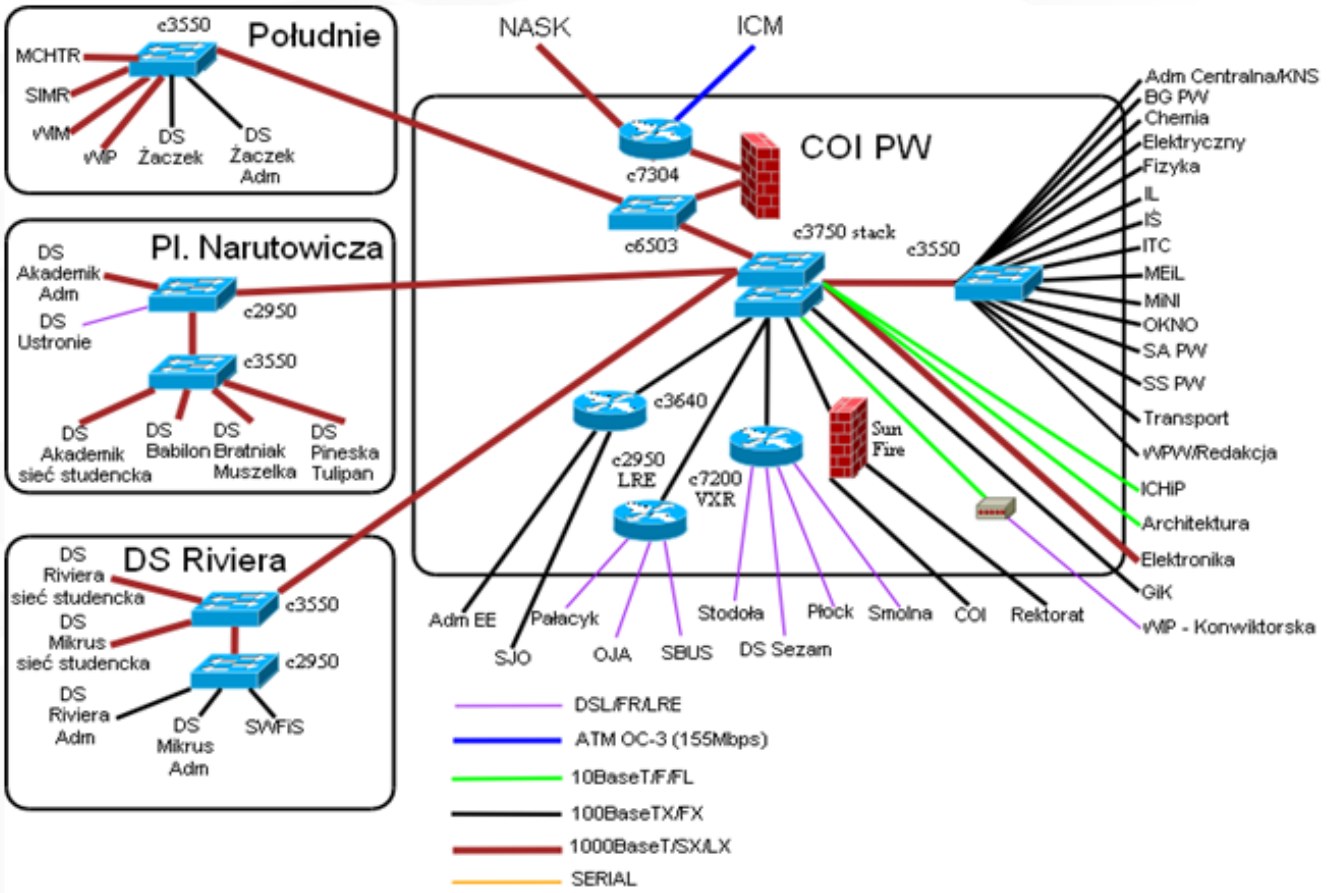
WAN


Utilization
no data
0-1%
1-2%
2-3%
3-4%
4-5%
5-6%
6-7%
7-8%
8-9%
9-10%
10-20%
20-30%
30-40%
40-50%
50-60%
60-70%
70-80%
80-90%
90-100%
Koszalin
Gdańsk
Olsztyn
BASNET
Szczecin
Bydgoszcz
Białystok (622 Mb/s)
ATMAN (125 Mb/s)
NASK
Gorzów Wlkp.
Piła
Toruń
GTS
USA-backup
USA
Poznań
ICM
GEANT
Zielona Góra
ENERGIS
IPartners (70 Mb/s)
Łódź
Radom
Puławy
Lublin
Wrocław
Kielce
Opole
Częstochowa
Gliwice
Kraków
Rzeszów
Bielsko-Biała
CESNET (1 Gb/s)
Bandwidth
34 Mb/s
155 Mb/s
1 Gb/s
2.5 Gb/s
10 Gb/s

LAN

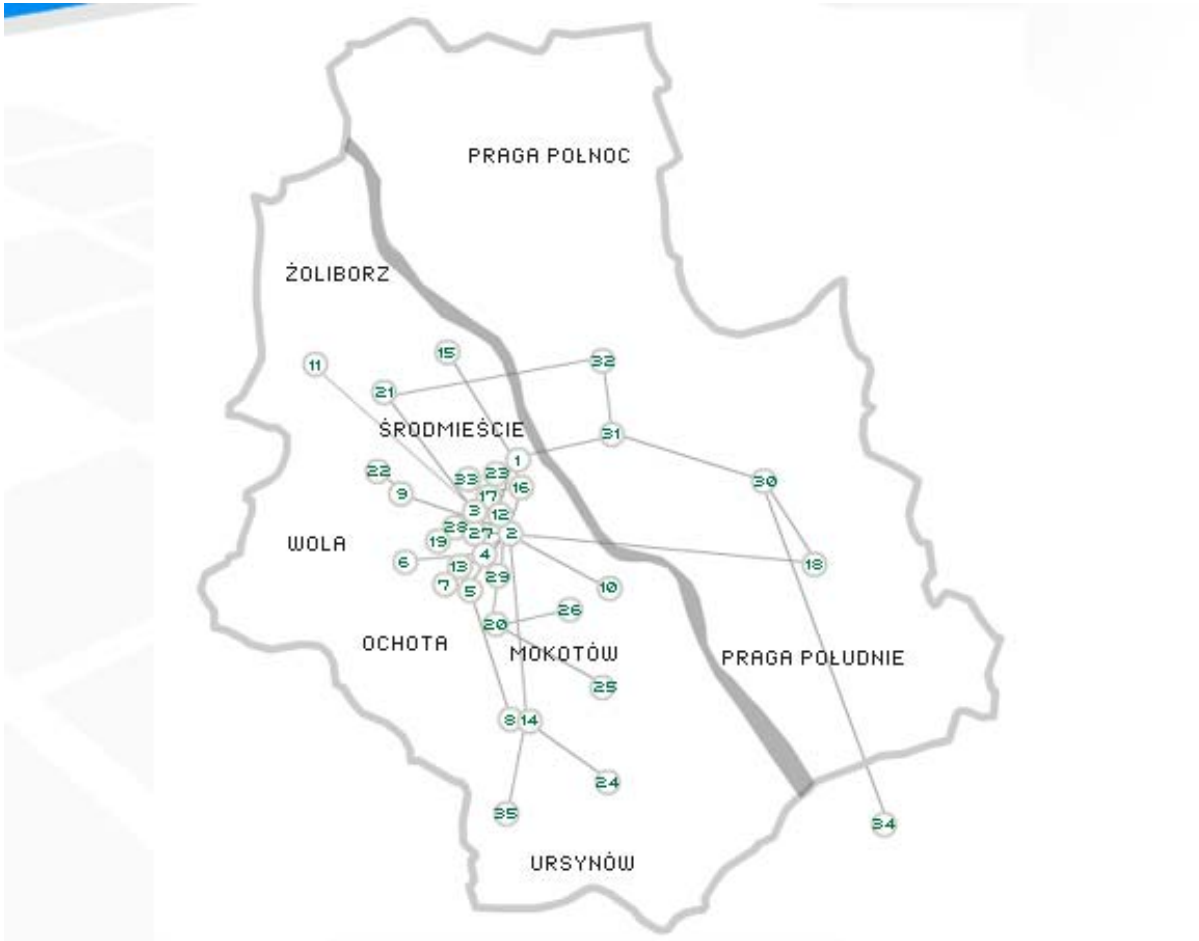


Przykład sieci kampusowej



Fizyczno – logiczny układ połączeń sieci Politechniki Warszawskiej

MAN

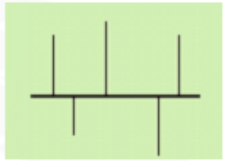
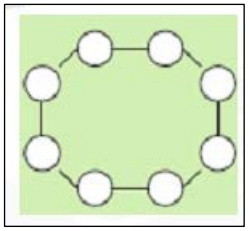
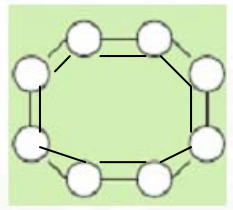
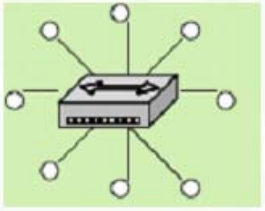
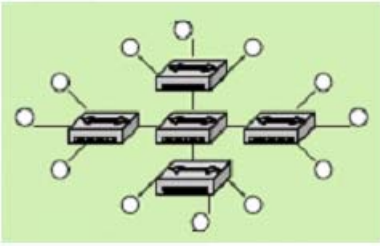
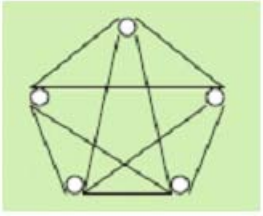
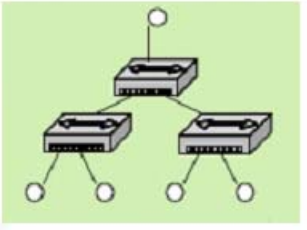


Sieć miejska Warszawy „Warman” (ze strony Nask)

PAN

Fizyczne topologie sieci

- magistrali,
- pierścienia,
- podwójnego pierścienia,
- gwiazdy,
- rozszerzonej gwiazdy,
- hierarchiczna,
- siatki.

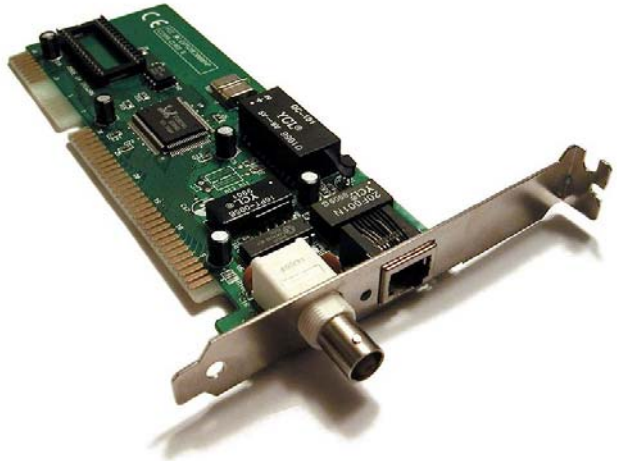








Urządzenia sieciowe

- Karty sieciowe
- Modemy
- Koncentratory (hub)
- Przełączniki (switch)
- Punkty dostępowe (acces point)
- Routery
- Urządzenia końcowe:
  - Serwery
  - Drukarki z interfejsem sieciowym
  - Komputery Desktop/Laptop/Palmtop
  - Telefony IP
  - Inne urządzenia z wbudowanym łączem sieciowym (urz. Pomiarowe, sterujące, lodówki itd.)

Karta sieciowa

- **Karta sieciowa** (ang. NIC - *Network Interface Card*) - karta rozszerzeń, która służy do przekształcania pakietów danych w sygnały, które są przesyłane w sieci komputerowej.
- Każda karta NIC posiada własny, unikatowy w skali światowej adres fizyczny, znany jako adres MAC, przyporządkowany w momencie jej produkcji przez producenta, zazwyczaj umieszczony na stałe w jej pamięci ROM. W niektórych współczesnych kartach adres ten można jednak zmieniać.
- Karta sieciowa pracuje tylko w jednym standardzie np. Ethernet. Nie może pracować w dwóch standardach jednocześnie np. Ethernet i FDDI. Karty sieciowe, podobnie jak switche są elementami aktywnymi sieci Ethernet.



Modem

- **Modem** (od ang. ***MO****dulator-****DEM****odulator*) - urządzenie elektroniczne, którego zadaniem jest zamiana danych cyfrowych na analogowe sygnały elektryczne (modulacja) i na odwrót (demodulacja) tak, aby mogły być przesyłane i odbierane poprzez linię telefoniczną (a także łącze telewizji kablowej lub fale radiowe). Jest częścią DCE (Data Communications Equipment), które w całości wykonuje opisane wyżej czynności. Nieodzowne do współpracy jest DTE (Data Terminal Equipment) i to dopiero stanowi całość łącza przesyłania danych. Dzięki modemowi można łączyć ze sobą komputery i urządzenia, które dzieli znaczna odległość.

Koncentrator

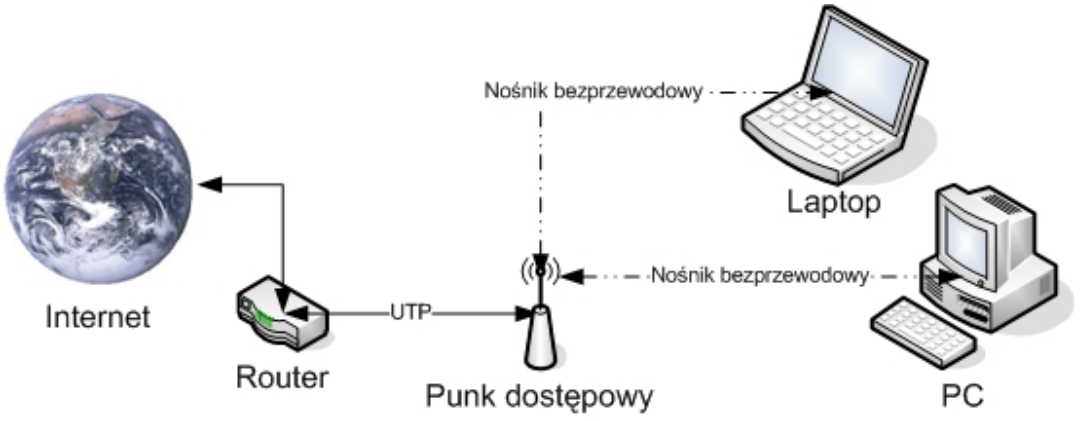
- **Koncentrator** (także z ang. ***hub***) - urządzenie łączące wiele urządzeń sieciowych w sieci komputerowej o topologii gwiazdy.
- Koncentrator pracuje w warstwie pierwszej modelu ISO/OSI (warstwie fizycznej), przesyłając sygnał z jednego portu na wszystkie pozostałe. Nie analizuje ramki pod kątem adresu MAC oraz IP. Ponieważ koncentrator powtarza każdy sygnał elektroniczny, tworzy jedną domenę kolizyjną.
- Koncentrator najczęściej podłączany jest do routera jako rozgałęziacz, do niego zaś dopiero podłączane są pozostałe urządzenia sieciowe: komputery pełniące rolę stacji roboczych, serwerów, drukarki sieciowe i inne.

Przełącznik

- **Przełącznik** (**przełącznica, komutator**, także z ang. ***switch***) – urządzenie łączące segmenty sieci komputerowej pracujące w drugiej warstwie modelu ISO/OSI (łącza danych), jego zadaniem jest przekazywanie ramek między segmentami.
- Przełącznik określa się też jako wieloportowy most lub inteligentny koncentrator, gdyż:
  - przekazuje ramki wyłącznie do docelowego segmentu sieci (podobnie do mostu, w przeciwieństwie do koncentratora),
  - umożliwia połączenie wielu segmentów sieci w gwiazdę (podobnie do huba, w przeciwieństwie do mostu ograniczonego do dwóch segmentów),
  - działa w trybie dupleks (w przeciwieństwie do koncentratora).

Punkt dostępowy

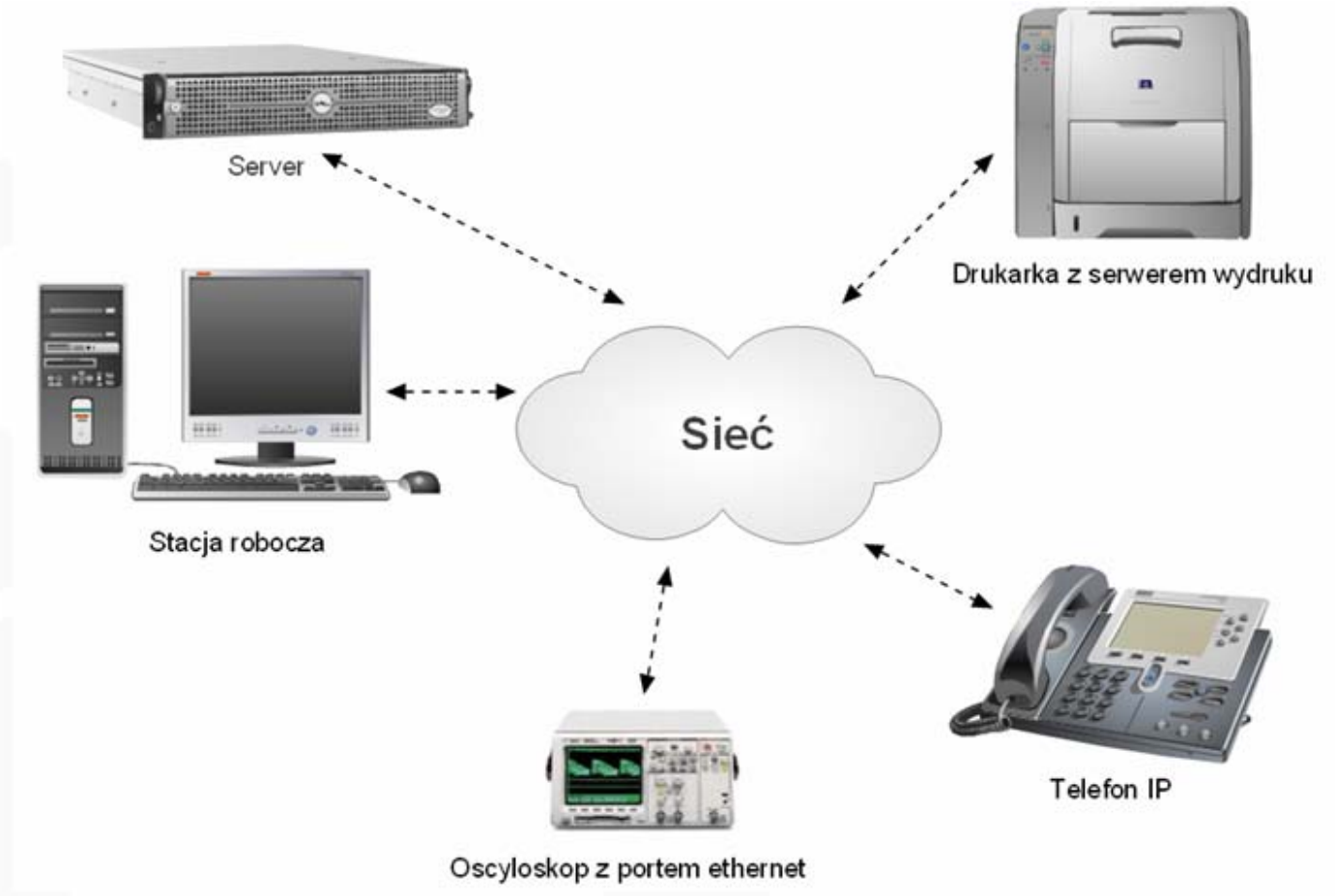
- **Access Point** (ang. punkt dostępu) - urządzenie zapewniające stacjom bezprzewodowym dostęp do zasobów sieci za pomocą bezprzewodowego medium transmisyjnego (częstotliwości radiowe).
- Access point jest także mostem łączącym sieć bezprzewodową z siecią przewodową (najczęściej Ethernet). W związku z tym każdy access point ma minimum dwa interfejsy: interfejs bezprzewodowy komunikujący się z sieciami standardu 802.11 oraz drugi służący połączeniu AP z siecią przewodową.



Router

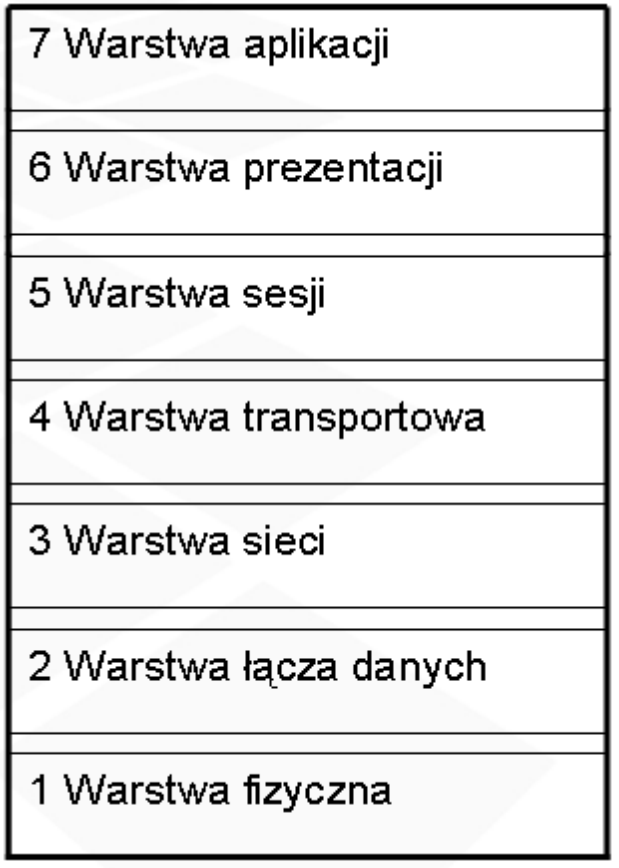
- **Router** (po polsku – **ruter**, **trasownik**) – urządzenie sieciowe pracujące w trzeciej warstwie modelu OSI, pełniące rolę węzła komunikacyjnego, służącego do rozdzielenia sygnału i rozgałęzienia połączeń internetowych. Proces kierowania ruchem nosi nazwę **trasowania, routingu lub rutowania**.
- Trasowanie musi zachodzić między co najmniej dwiema podsieciami, które można wydzielić w ramach jednej sieci komputerowej. Urządzenie tworzy i utrzymuje tablicę trasowania, która przechowuje ścieżki do konkretnych obszarów sieci oraz metryki z nimi związane (odległości od siebie licząc kolejne routery).
- Skuteczne działanie routera wymaga wiedzy na temat otaczających go urządzeń, przede wszystkim innych routerów oraz przełączników. Może być ona dostarczona w sposób statyczny przez administratora, wówczas nosi ona nazwę **tablicy statycznej** lub może być pozyskana przez sam router od sąsiadujących urządzeń pracujących w trzeciej warstwie, tablice tak konstruowane nazywane są **dynamicznymi**.
- Podczas wyznaczania tras dynamicznych router korzysta z różnego rodzaju protokołów trasowania i polega przede wszystkim na odpytywaniu sąsiednich urządzeń o ich tablice trasowania, a następnie kolejnych w zależności od zapotrzebowań ruchu, który urządzenie obsługuje.

Urządzenia końcowe



Model odniesienia ISO/OSI

Model ISO-OSI



Każda warstwa odpowiada konkretnemu fragmentowi procesu komunikacji, który sam w sobie stanowi zamkniętą całość. Dla każdej warstwy zdefiniowano interfejsy do warstw sąsiednich. Przy użyciu tego modelu można wyjaśnić, w jaki sposób pakiet przechodzi przez różne warstwy do innego urządzenia w sieci, nawet jeśli nadawca i odbiorca dysponują różnymi typami medium sieciowego. Dzięki takiemu podejściu uporządkowano reguły konstrukcji i jednocześnie uproszczono proces projektowania sieci, który w pewnym sensie także uległ rozbiciu na „warstwy”.

Warstwa fizyczna – transmisja binarna

Zadaniem warstwy fizycznej jest transmitowanie sygnałów cyfrowych pomiędzy urządzeniami sieciowymi. Jednostką informacji na poziomie tej warstwy jest pojedynczy **bit**. Parametry charakteryzujące tę warstwę to właściwości fizyczne łącza takie jak częstotliwości, napięcia, opóźnienie, długość, zniekształcenia, poziom zakłóceń, itp.

Warstwa łącza danych – bezpośrednie sterowanie łączem, dostęp do medium

Warstwa łącza danych odpowiada za komunikację pomiędzy hostami, podłączonymi do tego samego medium. Jej głównym zadaniem jest sterowanie dostępem do medium. Jednostką informacji w tej warstwie jest **ramka** składająca się z bitów o ściśle określonej strukturze zawierająca adresy nadawcy i adresata. Adresy urządzeń mogą mieć dowolną postać, określoną w specyfikacji zastosowanego standardu komunikacji. **Warstwa wyposażona jest w mechanizm kontroli poprawności transmisji**, w celu zapewnienia niezawodnego przesyłania danych przez medium.

Warstwa sieci – adresacja sieciowa i wybór najlepszej ścieżki

Głównym zadaniem warstwy sieci jest umożliwienie komunikacji pomiędzy hostami znajdującymi się w różnych sieciach lokalnych. Realizacja tego zadania możliwa jest dzięki dwóm mechanizmom: jednolitej adresacji urządzeń w całej sieci oraz routingu. Podstawową jednostką informacji w tej warstwie jest **pakiet** o ściśle określonej strukturze zawierający oprócz danych, adresy: nadawcy i odbiorcy pakietu. **Warstwa ta nie gwarantuje niezawodności transmisji**, natomiast wyposażona jest w mechanizmy monitorowania transmisji, co pozwala m.in. na identyfikację przyczyn uniemożliwiających komunikację.

Warstwa transportowa - połączenie typu end-to-end

Warstwa transportowa **odpowiedzialna jest za niezawodne przesyłanie danych między urządzeniami**. Warstwa ta posiada mechanizmy umożliwiające inicjację, utrzymanie i zamykanie połączenia między urządzeniami, sterowanie przepływem danych oraz wykrywanie błędów transmisji.

Warstwa sesji – komunikacja między hostami

- Zadaniem warstwy sesji jest zarządzanie komunikacją między aplikacjami działającymi na danym hoście, a aplikacjami działającymi na innych hostach w sieci.
- Ze względu na funkcjonalność systemów operacyjnych zawsze występuje sytuacja, gdy liczba aplikacji korzystających z sieci jest większa od liczby fizycznych interfejsów sieciowych.
- Rola tej warstwy sieci polega na stworzeniu mechanizmu umożliwiającego dostarczanie danych jakie przyszły z sieci oraz wysyłanie danych do sieci do aplikacji, dla której te dane są przeznaczone.

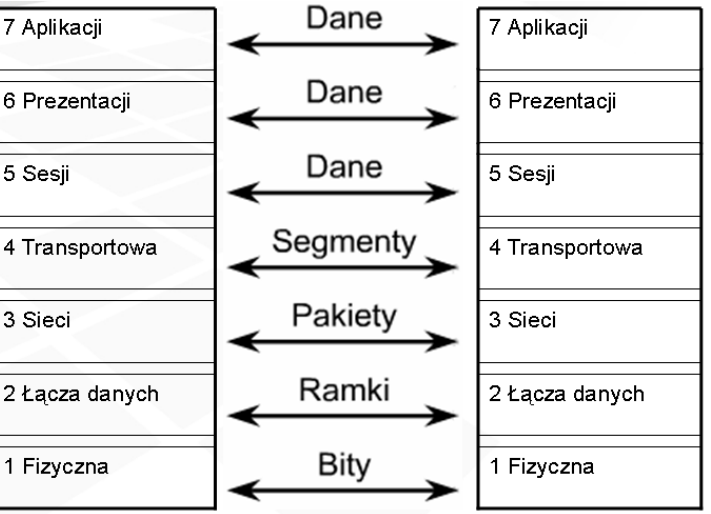
Warstwa prezentacji – reprezentacja danych

- Zadaniem warstwy prezentacji jest konwersja danych pod względem formatu oraz struktury aby interpretacja tych danych była jednakowa na obu urządzeniach: wysyłającym i odbierającym.
- Najczęściej konieczność dostosowania danych wynika z różnic między platformami sprzętowymi, na których działają komunikujące się aplikacje.

Warstwa aplikacji – połączenie procesów sieciowych z aplikacjami

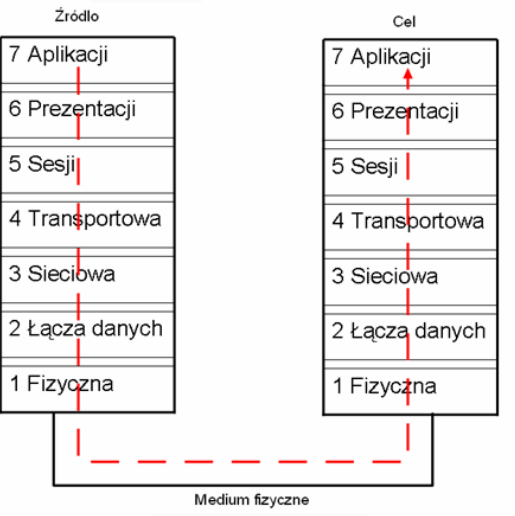
- Zadaniem warstwy aplikacji jest zapewnienie dostępu do usług sieciowych procesom aplikacyjnym, działającym na danym urządzeniu.

Model komunikacji 1



- Model komunikacji w sieci komputerowej oparty jest na komunikacji równorzędnej (ang. peer-to-peer).
- W procesie przesyłania danych między dwoma hostami, każda warstwa sieciowa jednego hosta komunikuje się z odpowiadającą jej warstwą drugiego hosta. Komunikacja równorzędnych warstw odbywa się poprzez wymianę ściśle określonych dla danej warstwy jednostek informacji oznaczanych skrótowo PDU (ang. Protocol Data Unit).

Model komunikacji 2

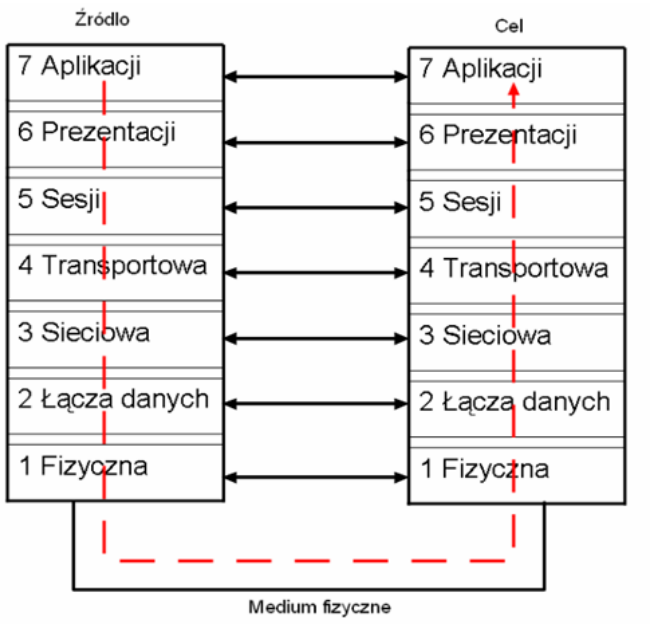


Aby taka forma komunikacji mogła zostać zrealizowana warstwy wyższe hosta wysyłającego muszą skorzystać z usług świadczonych przez warstwy niższe, natomiast w przypadku hosta odbierającego odwrotnie. Polega to na tym, że warstwa wyższa przekazuje dane do wysłania warstwie niższej, która przekształca dane do odpowiedniej postaci i przekazuje następnej, niższej warstwie. Gdy dane dojdą do warstwy fizycznej zostają przekształcone do postaci ciągu bitów i przekazane za pomocą medium transmisyjnego do warstwy fizycznej hosta odbierającego, na którym zachodzi proces odwrotny.

Enkapsulacja

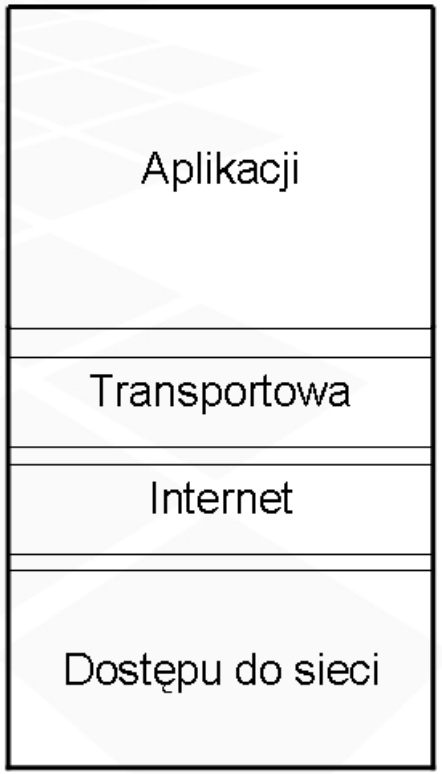
- Wędrówce danych między warstwami modelu odniesienia towarzyszy proces enkapsulacji (opakowania) jeżeli dane przekazywane są w dół stosu oraz proces dekapsulacji (rozpakowania), gdy dane przekazywane są w kierunku przeciwnym.
- Warstwa niższa przekształcając dane do odpowiedniej postaci dodaje niezbędne informacje (enkapsulacja), aby dane te mogły zostać poprawnie przesłane do równorzędnej warstwy hosta odbierającego i poprawnie przez nią zinterpretowane. Następnie, równorzędna warstwa hosta odbierającego dokonuje procesu dekapsulacji i przekazuje dane warstwie wyższej.

Protokół



- Wszystkie procesy związane z dwustronną komunikacją zarówno między warstwami równorzędnymi komunikujących się urządzeń, jak i warstwami sąsiednimi danego urządzenia opisane są w postaci zestawu reguł zwanych protokołami.
- Protokoły określają wszystkie aspekty komunikacji w sieci: budowa sieci fizycznej, sposoby łączenia komputerów z siecią, sposoby formatowania danych do transmisji, sposoby wysyłania danych, sposoby obsługi błędów. Dzięki temu dane wysłane z jednego urządzenia mogą być poprawnie transmitowane przez szereg pośredniczących urządzeń sieciowych do urządzenia docelowego, a następnie poprawnie odebrane i zinterpretowane. Nad procesem tworzenia protokołów czuwają specjalnie do tego celu powołane organizacje międzynarodowe: Institute of Electrical and Electronic Engineers (IEEE), American National Standards Institute (ANSI), Telecommunications Industry Association (TIA), Electronic Industries Alliance (EIA), International Telecommunications Union (ITU, dawny Comité Consultatif International Téléphonique et Télégraphique (CCITT)).

Model TCP/IP



Zadaniem modelu odniesienia ISO/OSI było uporządkowanie i ujednolicenie procesów związanych z komunikacją w sieci: budowa sieci, działanie sieci, zarządzanie siecią. Ze względów praktycznych (stan rozwoju technologii, konkurencja między producentami, preferencje użytkowników, sytuacja polityczna) zaproponowane wraz z modelem ISO/OSI rozwiązania nie przyjęły się, poza samym modelem odniesienia. Weryfikacji rozwiązań dokonał „rynek”. Można zaryzykować stwierdzenie, że momentem decydującym było opracowanie rodziny protokołów TCP/IP, zaimplementowanie ich w sieci ARPANET oraz w systemach UNIX’owych. Z czasem, w celu zachowania jednolitego modelu komunikacji w całym Internecie rodzina protokołów TCP/IP stała się także podstawowym standardem wykorzystywanym w sieciach lokalnych.

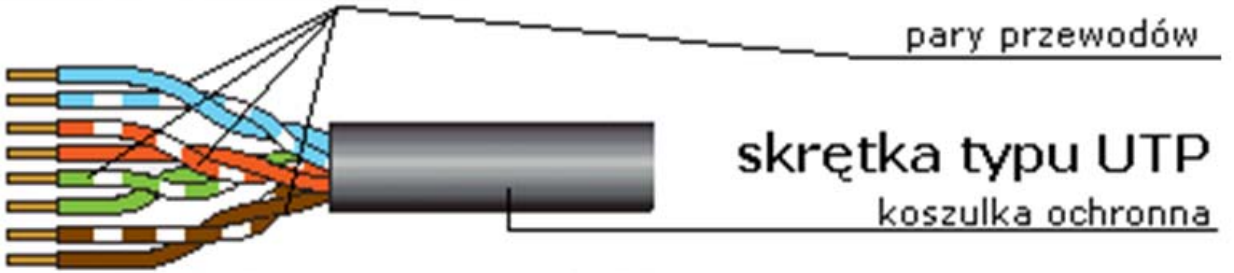
TCP/IP vs. ISO/OSI 1

TCP/IP vs. ISO/OSI

- Model TCP/IP składa się z czterech warstw:
  - warstwy dostępu do sieci,
  - warstwy internetu,
  - warstwy transportowej,
  - warstwy aplikacji.
- Ze względu na dużą różnorodność rozwiązań w zakresie fizycznej konstrukcji sieci, jaka istniała w chwili opracowywania, model TCP/IP zapewnia interfejs do warstwy dostępu do sieci traktując ją jako monolit. Warstwa ta odpowiada dwóm najniższym warstwom, fizycznej oraz łącza danych modelu ISO/OSI.
- Warstwa internetu odpowiada warstwie sieci w pełnym zakresie funkcjonalności. Warstwa transportowa modelu TCP/IP realizuje te same zadania, co warstwa transportowa modelu ISO/OSI oraz dodatkowo zajmuje się podstawowymi aspektami związanymi z zarządzaniem sesjami aplikacyjnymi.
- Pozostałe zadania warstwy sesji modelu ISO/OSI oraz zadania warstwy prezentacji i aplikacji zostały umieszczone w modelu TCP/IP w warstwie aplikacji. Obecnie rodzina protokołów TCP/IP jest podstawowym modelem komunikacji w Internecie i zdecydowanej większości lokalnych sieci komputerowych nie podpiętych do Internetu.

Media

Media – skrętka nieekranowana



- UTP (ang. Unshielded Twisted Pair) – skrętka nieekranowana – skrętka wykonana z dwóch przewodów, ze zmiennym splotem (zwykle 1 zwój na 6-10 cm), co chroni transmisję przed oddziaływaniem otoczenia. Skrętka nieekranowana UTP jest powszechnie stosowana w sieciach telefonicznych (jedna, dwie lub cztery pary) i w kablach komputerowych (cztery skrętki w kablu). Zwykle poszczególne skrętki w kablu mają odmienny skręt w celu minimalizacji przesłuchów zbliżnych NEXT i zdalnych FEXT. Ich przydatność do transmisji cyfrowych określają kategorie, a przydatność do aplikacji - klasy kabli miedzianych. Przy przesyłaniu sygnałów cyfrowych za pomocą skrętek UTP (cztery pary) uzyskuje się standardowa przepływności do 100 Mb/s (kat. 5), oraz 1 Gb/s w technologii Gigabit Ethernet. Dla przesyłania sygnałów w sieciach komputerowych konieczne są skrętki kategorii 3 (10 Mb/s) i kategorii 5 (100 Mb/s), przy czym powszechnie stosuje się tylko tą ostatnią.

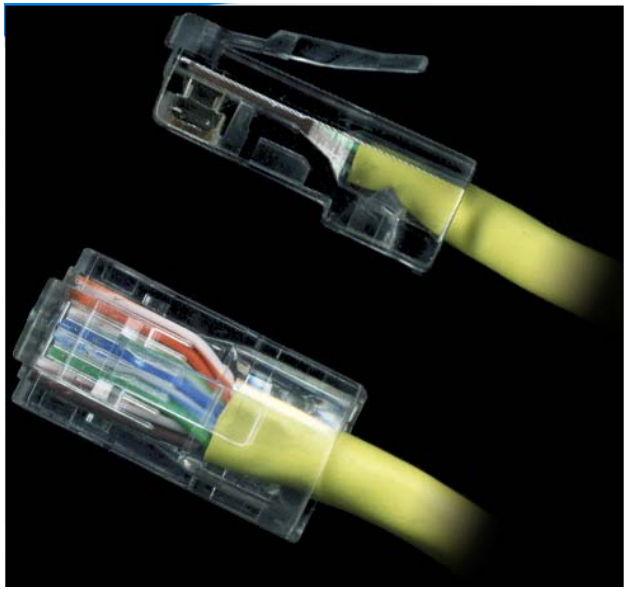
Kategorie kabli

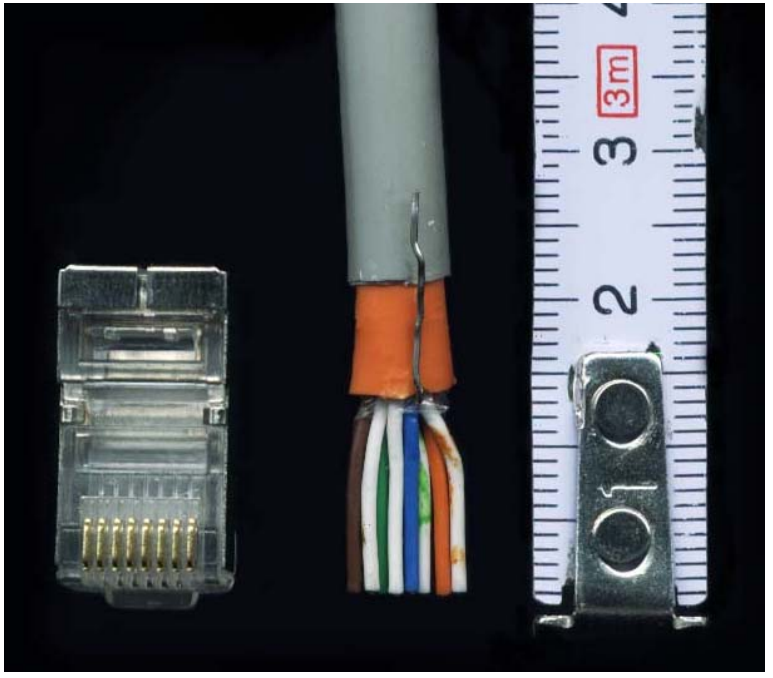
- Kategorie kabli miedzianych zostały ujęte w specyfikacji EIA/TIA w kilka grup, w których przydatność do transmisji określa się w MHz:
  - kategoria 1 – tradycyjna nieekranowana skrętka telefoniczna przeznaczona do przesyłania głosu, nie przystosowana do transmisji danych
  - kategoria 2 – nieekranowana skrętka, szybkość transmisji do 4 MHz. Kabel ma 2 pary skręconych przewodów
  - **kategoria 3** – skrętka o szybkości transmisji do 10 MHz, stos. w sieciach Token Ring (4 Mb/s) oraz Ethernet 10Base-T (10 Mb/s). Kabel zawiera 4 pary skręconych przewodów
  - kategoria 4 – skrętka działająca z szybkością do 16 MHz. Kabel zbudowany jest z czterech par przewodów
  - **kategoria 5** – skrętka z dopasowaniem rezystancyjnym pozwalająca na transmisję danych z szybkością 100 MHz pod warunkiem poprawnej instalacji kabla (zgodnie z wymaganiami okablowania strukturalnego) na odległość do 100 m
  - **kategoria 5e** – (enchanced) – ulepszona wersja kabla kategorii 5. Jest zalecana do stosowana w przypadku nowych instalacji
  - kategoria 6 – skrętka umożliwiająca transmisję z częstotliwością do 200 MHz.
  - kategoria 7 – kabel o przepływności do 600 MHz. Będzie wymagać już stosowania nowego typu złączy w miejsce RJ-45 oraz kabli każdą parą ekranowaną oddzielnie.

Sieci oparte na kablu UTP

- Zalety sieci UTP
  - Posiada bardzo korzystny stosunek możliwości do ceny. Jest prosta w montażu. Charakteryzuje się dużą przepustowością - do 1000Mb/s.
  - Łatwa diagnoza usterki. Daje duże możliwości rozbudowy (modularna budowa). Awaria kabla w jednym miejscu nie unieruchamia całej sieci.
- Wady sieci UTP
  - Jest nieco droższa niż sieć BNC.
  - Konieczność zakupu HUB-a.
  - Mała odporność na zakłócenia środowiska (w wersji nie ekranowanej, nie dotyczy FTP i STP).
  - Niska odporność na uszkodzenia mechaniczne.
  - Maksymalna odległość od koncentratora wynosi jedyne 100m.
- Dwa najczęściej stosowane standardy sieci UTP:
  - 10 Base-T - Najpopularniejszy obecnie standard. Opiera się on na topologii gwiazdy, do łączenia komputerów używa się nie ekranowanego kabla skręcanego (podobny do kabla telefonicznego) kategorii CAT-3 firmy IBM (lub kompatybilnego DIV firmy AT&T). Maksymalna długość kabla w jakichkolwiek połączeniach wynosi 100m. Jako złącznika używa się ośmiopozycyjne wtyczki RJ-45, nie mylić z telefoniczną RJ-11. Maksymalna osiągalna przepustowość sieci mieści się w granicach 10Mb/s.
  - 100Base-TX Jest to szybsza modyfikacja wyżej wymienionego standardu. Łatwo wywnioskować iż różni się maksymalną przepustowością sieci, w tym przypadku jest to 100Mb/s. Aby sieć mogła pracować z taką szybkością należy zastosować lepsze kable CAT-5 oraz HUB-y i karty sieciowe umożliwiające pracę z opisywanym standardem.

Wtyk RJ-45





Typy połączeń przewodów

- W sieciach 10Base-T i 100Base-TX stosuje się dwa typy podłączeń końcówek RJ-45:
  - Zgodne (proste) - wszystkie żyły wewnątrz przewodu podłączamy do wtyków w następujący sposób: styk pierwszy we wtyczce pierwszej do styku pierwszego we wtyczce drugiej, 2 do 2, 3 do 3, itd.
  - Krzyżowe - w tym połączeniu dwie pary wewnętrznych przewodów są zamienione ze sobą (1-3, 2-6). Tak powstały kabel nazywa się cross-over.
- Kable proste (ang. straight-through) stosowane są do łączenia:
  - Przełącznik z routerem Ethernet
  - Komputer z przełącznikiem
  - Komputer z koncentratorem

- Natomiast skrzyżowane (ang.crossover) do łączenia :
  - Przełącznika z przełącznikiem
  - Przełącznik z koncentratorem
  - Koncentrator z koncentratorem
  - Router z routerem (Ethernet port connection)
  - Komputer z komputerem
  - Komputer z routerem (Ethernet port).

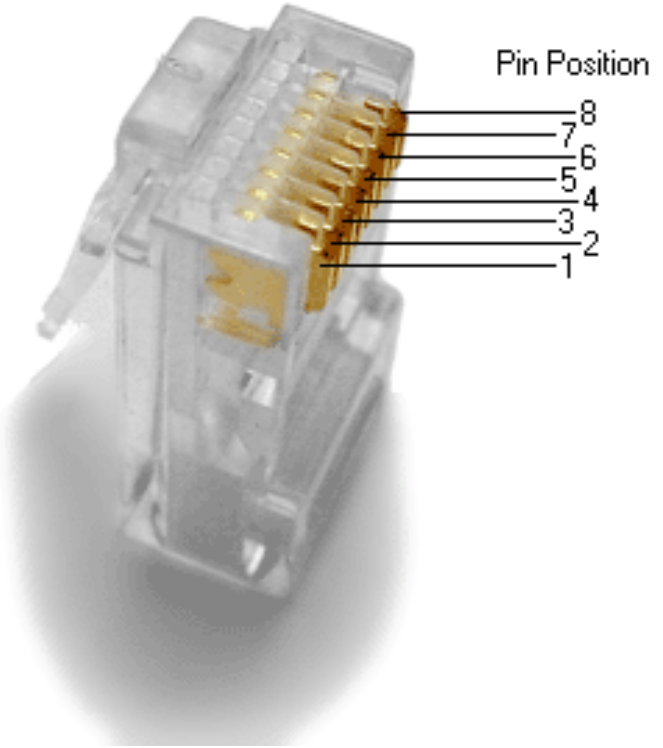
Układ prosty

Wtyczka 1	Nr	Kolor przewodu	Nr	Wtyczka 2
Odbiór +	1	Biało - Pomarańczowy	1	Transmisja +
Odbiór -	2	Pomarańczowy	2	Transmisja -
Transmisja +	3	Biało - Zielony	3	Odbiór +
(nie używane)	4	Niebieski	4	(nie używane)
(nie używane)	5	Biało - Niebieski	5	(nie używane)
Transmisja -	6	Zielony	6	Odbiór -
(nie używane)	7	Biało - Brązowy	7	(nie używane)
(nie używane)	8	Brązowy	8	(nie używane)

Układ krzyżowy

Wtyczka 1	Nr	Kolor przewodu	Nr	Wtyczka 2
Odbiór +	1	Biało - Pomarańczowy	3	Transmisja +
Odbiór -	2	Pomarańczowy	6	Transmisja -
Transmisja +	3	Biało - Zielony	1	Odbiór +
(nie używane)	4	Niebieski	7	(nie używane)
(nie używane)	5	Biało - Niebieski	8	(nie używane)
Transmisja -	6	Zielony	2	Odbiór -
(nie używane)	7	Biało - Brązowy	4	(nie używane)
(nie używane)	8	Brązowy	5	(nie używane)

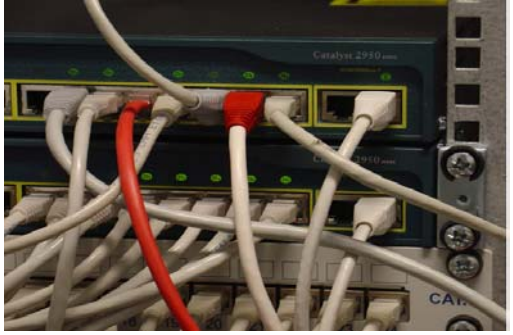
Ułożenie pinów we wtyczce:



Elementy montażowe – panel krosowniczy

Panel krosowniczy - (ang. patch panel) to pasywny element sieci komputerowych i telekomunikacyjnych. Montowany jest w szafach krosowniczych. Z jednej strony przyłączane są przewody prowadzące do gniazdek RJ-45. Przy pomocy tzw. patch cordów gniazda te (a i przez to urządzenia będące na drugim końcu kabla) przyłączane są do urządzeń sieciowych. Jest to ważny element sieci strukturalnej. Dzięki zastosowaniu paneli krosowniczych można bardzo łatwo zarządzać architekturą sieci. Obecnie często wykorzystywane także do podłączeń telefonicznych.

Elementy montażowe – Patchcord



Patchcord – krótki przewód służący do przesyłania sygnałów elektrycznych lub (rzadziej) optycznych. Najczęściej jest on kojarzony z sieciami komputerowymi – skrętką. Wtedy jest to przewód połączony według schematu 1:1. Są także patchordy służące do łączenia osprzętu optycznego (patchcord optyczny – światłowód) oraz do łączenia osprzętu wideo.

Patchcord jest to przewód o znormalizowanej długości, który można kupić w sklepie w przeciwieństwie do kabli sieciowych, które trzeba zrobić samemu. Jest to umowny podział, ponieważ mogą one być używane zamiennie. Patchcord najczęściej używany jest w szafach krosowniczych do łączenia elementów aktywnych (przełącznik, koncentrator, router) i pasywnych (panele krosownicze) sieci komputerowej.

Media – światłowód 1

- **Światłowód** to falowód służący do przesyłania promieniowania świetlnego. Jest w formie włókien dielektrycznych - najczęściej szklanych, z otuliną z tworzywa sztucznego, charakteryzującego się mniejszym współczynnikiem załamania światła niż wartość tego współczynnika dla szkła. Promień światła rozchodzi się w światłowodzie po drodze będącej łamaną tzn. ulegając kolejnym odbiciom (w przypadku światłowodu z włókien są, to odbicia całkowite wewnętrzne). Transmisja światłowodowa polega na przesyłaniu sygnału optycznego wewnątrz włókna szklanego. Podstawowym składnikiem do budowy światłowodu jest dwutlenek krzemu, ale nie w formie czynnej - Si02
- **Transmisja światłowodowa** polega na prowadzeniu przez włókno szklane promieni optycznych generowanych przez laserowe źródło światła. Ze względu na znikome zjawisko tłumienia, a także odporność na zewnętrzne pola elektromagnetyczne, przy braku emisji energii poza tor światłowodowy, światłowód stanowi obecnie najlepsze medium transmisyjne.
- **Kabel światłowodowy** składa się z jednego do kilkudziesięciu włókien światłowodowych. Medium transmisyjne światłowodu stanowi szklane włókno wykonane najczęściej z domieszkowanego dwutlenku krzemu (o przekroju kołowym) otoczone płaszczem wykonanym z czystego szkła (SiO2), który pokryty jest osłoną (buforem). Dla promieni świetlnych o częstotliwości w zakresie bliskim podczerwieni współczynnik załamania światła w płaszczu jest mniejszy niż w rdzeniu, co powoduje całkowite wewnętrzne odbicie promienia i prowadzenie go wzdłuż osi włókna. Zewnętrzną warstwę światłowodu stanowi tzw. bufor wykonany zazwyczaj z akrylonu poprawiający elastyczność światłowodu i zabezpieczający go przed uszkodzeniami. Jest on tylko osłoną i nie ma wpływu na właściwości transmisyjne światłowodu.

Media – światłowód 2

- Wyróżnia się światłowody **jednomodowe** (100km bez wzmacniacza) oraz **wielomodowe** (5 km bez wzmacniacza).
- Światłowód wielomodowy charakteryzuje się tym, że promień światła może zostać do niego wprowadzony pod wieloma kątami.
- Światłowody **jednomodowe** oferują większe pasmo przenoszenia oraz transmisję na większe odległości niż światłowody wielomodowe. Niestety koszt światłowodu jednomodowego jest wyższy. Zazwyczaj przy transmisji typu full-duplex stosuje się dwa włókna światłowodowe do oddzielnej transmisji w każdą stroną, choć spotykane są rozwiązania umożliwiające taką transmisję przy wykorzystaniu tylko jednego włókna.
  Zalety:
  - większa przepustowość w porównaniu z kablem miedzianym, a więc możliwość sprostania przyszłym wymaganiom co do wydajności transmisji,
  - małe straty, a więc zdolność przesyłania informacji na znaczne odległości,
  - niewrażliwość na zakłócenia i przesłuchy elektromagnetyczne, wyeliminowanie przesłuchów międzykablowych,
  - mała masa i wymiary,
  - duża niezawodność poprawnie zainstalowanego łącza
  - względnie niski koszt, który ciągle spada

Przykłady światłowodów

Światłowód
wielomodowy

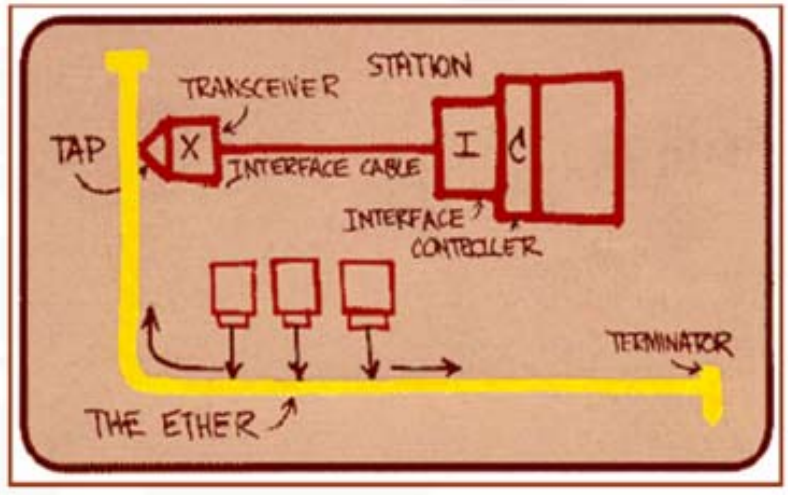
Światłowód
jednomodowy

Zasady konstruowania sieci

- Typowa topologia fizyczna: gwiazda
- Centra sieciowe znajdujące się w większej odległości łączy się światłowodem
- Lokalnie sieć tworzy się w oparciu o „skrętkę” lub łączność bezprzewodową.
- W przypadku stosowania łączności bezprzewodowej należy zwrócić uwagę na konfigurację urządzeń w taki sposób, aby przesyłane dane były bezpieczne (np. zastosowanie szyfrowania).

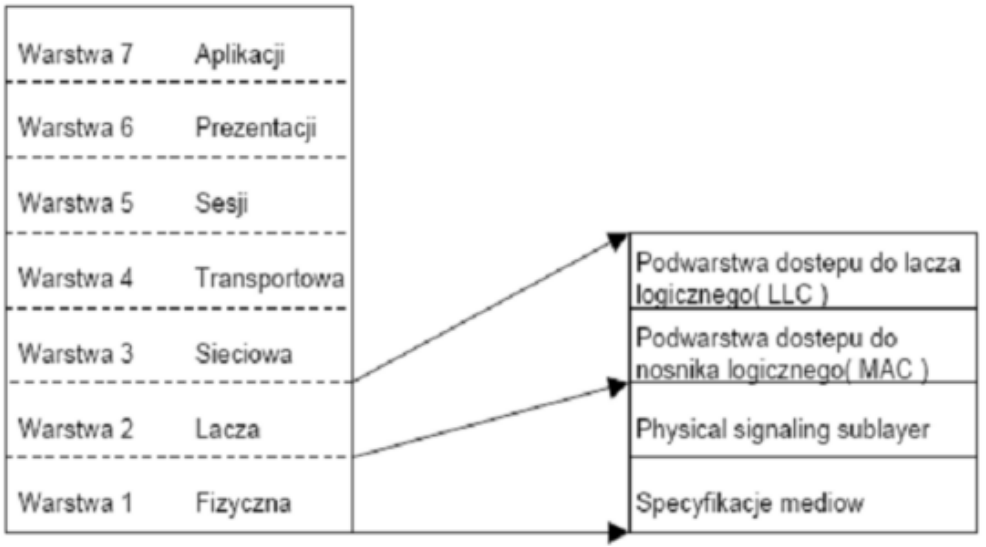
Ethernet

Ethernet



- **Ethernet** to technologia, w której zawarte są standardy wykorzystywane w budowie głównie lokalnych sieci komputerowych. Obejmuje ona specyfikację kabli oraz przesyłanych nimi sygnałów.
- Ethernet opisuje również format ramek i protokoły z dwóch najniższych warstw Modelu OSI.
- Jego specyfikacja została podana w standardzie 802.3 IEEE.
- Ethernet jest najpopularniejszym standardem w sieciach lokalnych. Inne wykorzystywane specyfikacje to Token Ring, FDDI czy Arcnet.
- Ethernet został opracowany przez Roberta Metcalfa w Xerox PARC czyli ośrodku badawczym firmy Xerox i opublikowany w roku 1976.
- Ethernet bazuje na idei węzłów podłączonych do wspólnego medium i wysyłających i odbierających za jego pomocą specjalne komunikaty (ramki). Ta metoda komunikacji nosi nazwę CSMA/CD (ang. *Carrier Sense Multiple Access with Collision Detection*). Wszystkie węzły posiadają unikalny adres MAC.

Ethernet a model OSI



Standard Ethernet opisuje funkcje toru komunikacyjnego, umieszczonego w modelu ISO/OSI w warstwach 2 i 1.

- Na poziomie warstwy łącza zdefiniowano dwie podwarstwy:
  - LLC (Logical Link Control) oraz
  - MAC (Medium Accesss Control).
- Warstwa LLC jest warstwą niezależną od zastosowanego systemu sieci lokalnej (LAN). Jej zadaniem jest identyfikowanie danych przesyłanych w ramce Ethernet.
- Warstwa MAC opisuje protokół określający sposób dostępu do medium w systemie Ethernet.
- Podwarstwy zdefiniowane w warstwie 1 modelu ISO/OSI są zmienne i określają rodzaj sieci Ethernet jaki został zastosowany, np. 10Mb, 100Mb, czy 1Gb.

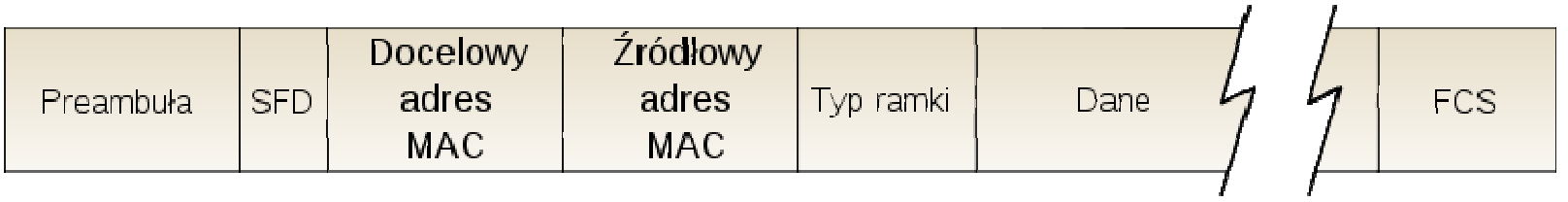
Cechy standardu Ethernet

- Klasyczne sieci Ethernet mają cztery cechy wspólne. Są to:
  - parametry czasowe,
  - format ramki,
  - proces transmisji oraz
  - podstawowe reguły obowiązujące przy ich projektowaniu.
- Standardem jest izolacja o wytrzymałości minimum 250V~ między kablem a komputerem (niektóre firmy, np. 3Com, stosowały lepszą, co skutkowało dużo większą trwałością ich kart sieciowych).

Ramki Ethernet

- Istnieją 3 standardy ramek:
  - Ethernet wersja 1 - już nie używana,
  - Ethernet wersja 2 (Ethernet II) - zwana też ramką DIX od firm DEC, Intel i Xerox, które opracowały wspólnie ten typ ramki i opublikowały w 1978. Jest ona w tej chwili najczęściej stosowana,
  - IEEE 802.x LLC,
- Ramki różnią się pomiędzy sobą długościami nagłówków, maksymalną długością ramki (MTU) i innymi szczegółami. Różne typy ramek mogą jednocześnie korzystać z tej samej sieci.

Budowa ramki Ethernet wersja 2



- Preambuła - składająca się z 7 bajtów złożonych z naprzemiennych jedynek i zer: 10101010101010101010101010101010101010101010101010101010
- SFD - (ang. *start frame delimiter*), czyli znacznik początkowy ramki w postaci sekwencji 8 bitów (1 bajt): 10101011
- adres MAC odbiorcy (6 bajtów)
- adres MAC nadawcy (6 bajtów)
- typ (2 bajty) - jeżeli wartość mniejsza niż 1500, to oznacza długość ramki, jeżeli większa to typ pakietu
- dane (46 - 1500 bajtów) - jeżeli dane mniejsze niż 46 bajtów, to uzupełniane są zerami
- suma kontrolna (4 bajty) CRC

Szybkości transmisji ethernet

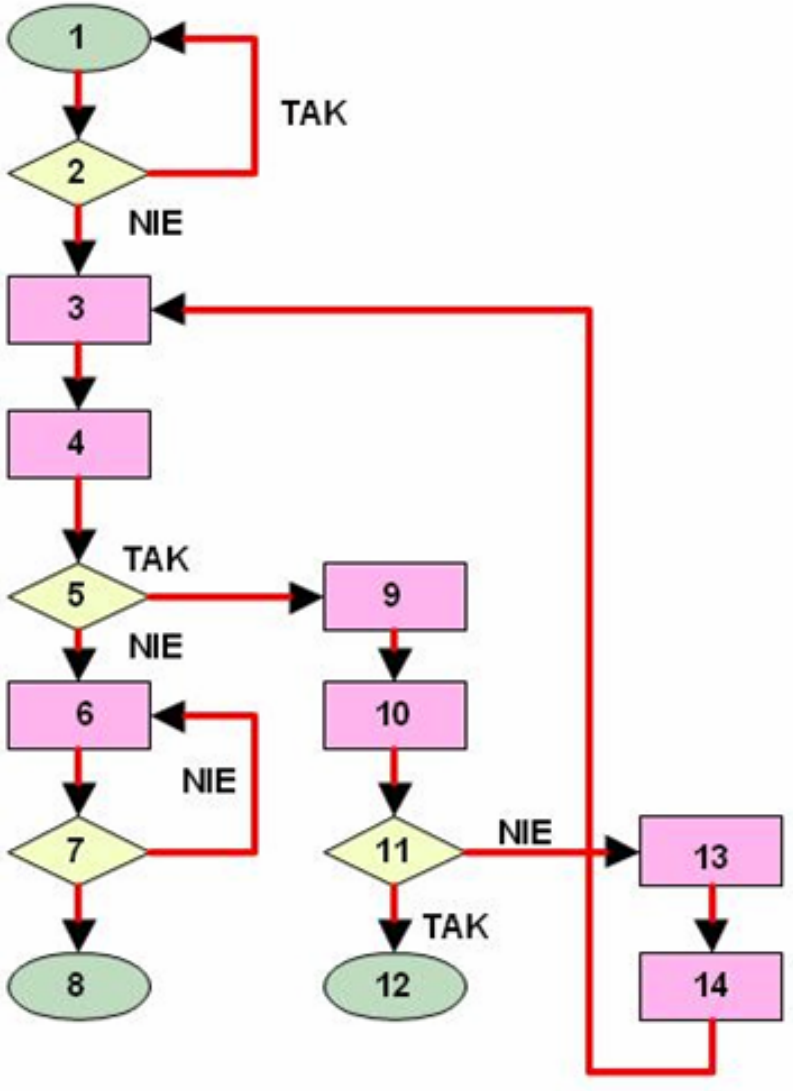
- 10 Mbit/s, np.;
  - 10Base-T - pracuje na 4 żyłach (2 pary 'skrętki') kategorii 3 lub 5. Każda karta sieciowa musi być podłączona do huba lub switcha.
- Fast Ethernet, np.:
  - 100Base-TX - podobny do 10BASE-T, ale z szybkością 100Mb/s. Wymaga 2 par skrętki kategorii 5. Obecnie jeden z najpopularniejszych standardów sieci opartych na 'skrętce'.
  - 100Base-FX - Ethernet 100Mb/s za pomocą włókien światłowodowych wielomodowych. Zasięg rozwiązania wynosi do 2km.
  - 100Base-LX - Ethernet 100Mb/s za pomocą włókien światłowodowych.
- Gigabit Ethernet np.:
  - 1000BASE-T - 1 Gb/s na kablu miedzianym -popularnej skrętce kat. 5 lub wyższej. Ponieważ kabel kategorii 6 może bez strat przenosić do 125 Mb/s, osiągniecie 1000 Mb/s wymaga użycia czterech par przewodów oraz modyfikacji układów transmisyjnych dającej możliwość transmisji ok. 250Mb/s na jedną parę przewodów w skrętce.
  - 1000BASE-LX - 1 Gb/s na światłowodzie. Zoptymalizowany dla połączeń na dłuższe dystanse (do 10 km) za pomocą światłowodów jednomodowych.
- 10 Gigabit Ethernet np.:
  - **10GBASE-LX4 - stosując modulację typu 'WDM' umożliwia zasięg 240 lub 300 m za pomocą światłowodów wielomodowych (przy 1310nm) lub 10 km za pomocą jednomodowych.**
  - 10GBASE-T – najnowszy standard w tej kategorii. Umożliwia transmisję o prędkości 10 Gb/s na odległość 100 m kablem nieekranowanym UTP kategorii 6a/7. Możliwe jest również wykorzystanie kabla kategorii 6 – wtedy maksymalna długość kabla nie powinna przekraczać 55m.

Protokół MAC (CSMA/CD)

- Protokół CSMA/CD odpowiedzialny jest za cały proces transmisji danych: wysyłanie i odbieranie ramek z danymi, dekodowanie ramek i sprawdzanie poprawności zawartych w nich adresów przed przekazaniem ich do wyższych warstw modelu OSI, wykrywanie błędów wewnątrz ramek lub w sieci.
- Pracując w oparciu o protokół CSMA/CD urządzenie przechodzi w stan nasłuchiwania przed rozpoczęciem nadawania. Nasłuchiwanie ma na celu sprawdzenie zajętości kanału transmisji.
  - Jeżeli w kanale transmisji zostanie wykryta nośna (obecność jakiegokolwiek sygnału w sieci) oznacza to, że inne urządzenie wysyła dane, czyli kanał jest zajęty.
  - Jeżeli w kanale nastąpi cisza i będzie utrzymywała się przez z góry ustalony okres czasu (przerwa międzyramkowa), to urządzenie stwierdza, że kanał jest wolny i rozpoczyna nadawanie.
- Podczas nadawania pierwszej, ściśle określonej liczby bitów (minimalna długość ramki) urządzenie sprawdza, czy nie wystąpiła kolizja.
  - Jeżeli transmisja dobiegła końca i nie stwierdzono kolizji, urządzenie zakłada, że operacja zakończyła się powodzeniem.
  - Jeżeli jednak wykryto kolizję (nadmierny wzrost amplitudy sygnału świadczący o nałożeniu się sygnałów) następuje wysłanie do sieci specjalnego sygnału.
- Wszystkie urządzenia, które brały udział w kolizji zaprzestają nadawania oraz obliczają losowy odcinek czasu, po którym ponowią próbę transmisji. Jeżeli ponownie wystąpi kolizja, obliczony wcześniej losowy odcinek czasu jest podwajany i po tak obliczonym czasie wykonywana jest kolejna próba transmisji. Podwajanie losowo obliczonego odcinka czasu może występować najwyżej 16 razy, jeżeli każda kolejna próba transmisji zakończyła się kolizją. Po przekroczeniu dopuszczalnej liczby kolejnych kolizji urządzenie odczekuje pewien czas i uruchamia proces nadawania od początku.

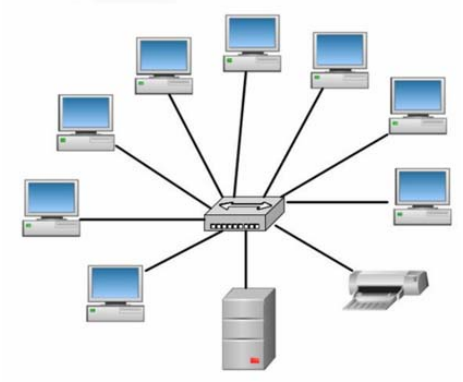
Protokół MAC (CSMA/CD)

1. Host zamierza nadawać
2. Czy wykryto nośną ?
3. Złożenie ramki
4. Początek transmisji
5. Czy wykryto kolizje ?
6. Kontynuacja transmisji
7. Czy transmisja dobiegla końca ?
8. Transmisja zakończona
9. Rozglaszanie sygnalu zakłócającego
10. Próby = Próby + 1
11. Próby > Zbyt Wiele ?
12. Zbyt wiele kolizji, przerwanie transmisji
13. Algorytm oblicza czas oczekiwania
14. Oczekiwanie przez t mikrosekund

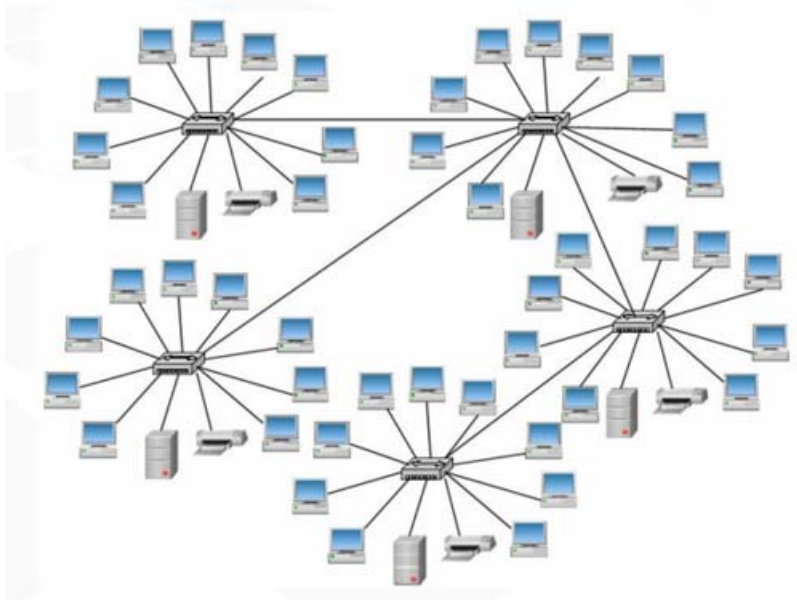


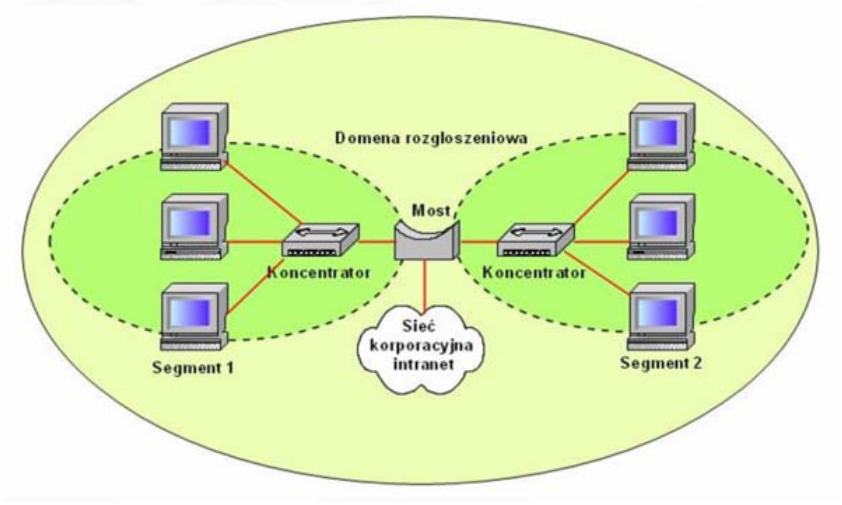
Zasady budowy sieci Ethernet

Koncentrator



Zestaw koncentratorów





Most/Switch

Protokół IP

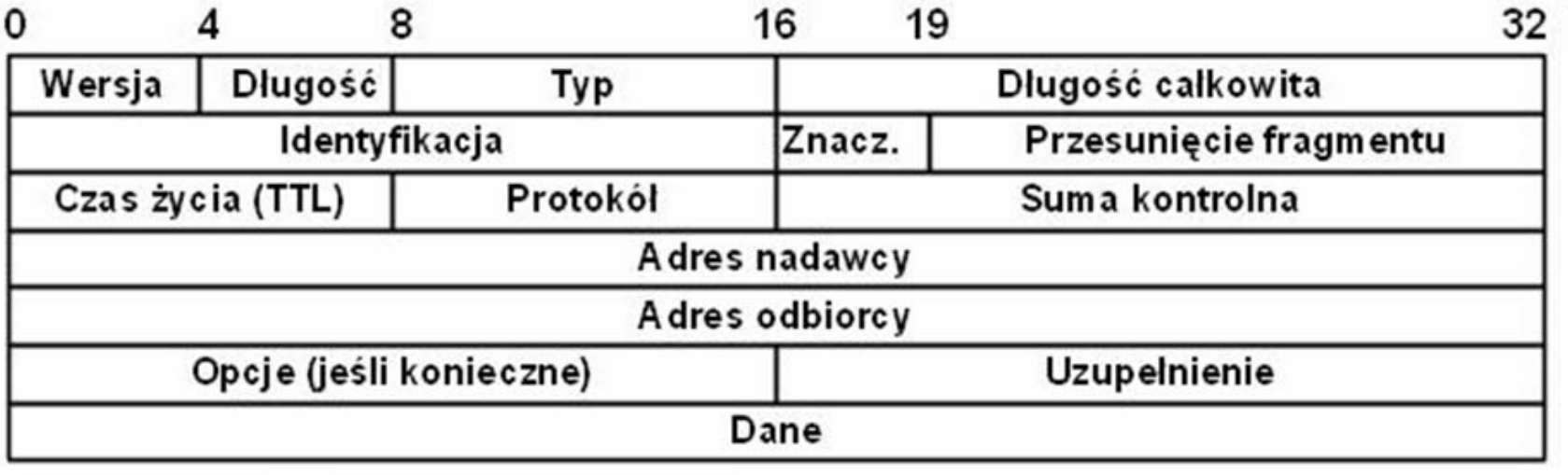
Protokół IP

- Urządzenia sieciowe połączone przy pomocy mediów transmisyjnych wymagają protokołów sieciowych, które umożliwiają komunikację. Może to zostać zrealizowane przy pomocy protokołów warstw wyższych modelu ISO/OSI. W szczególności za komunikację sieciową odpowiada protokół IP, który wraz z innymi protokołami zastosowanymi w stosie protokołów TCP/IP stanowi podstawę działania współczesnych sieci komputerowych.
- Protokół IP nie posiada mechanizmów sygnalizujących błędy oraz mechanizmów umożliwiających kontrolowanie przepływu pakietów.
- Z tego względu zgłaszaniem problemów z przesyłaniem datagramów oraz sterowaniem zajmuje się protokół ICMP
- Powszechnie stosowaną wersją protokołu IP jest wersja 4. Jednak ze względu na ograniczenia dotyczące adresowania logicznego spowodowane niedostateczną, w stosunku do potrzeb, liczbą bitów przeznaczonych na adres IP protokół ten będzie zastąpiony nowszą wersją IPv6.

IPv4

- Protokół IPv4 został szczegółowo opisany w dokumencie RFC 791. Sam protokół IP został opracowany do działania w sytuacjach ekstremalnych, np. w trakcie wojny. W normalnych warunkach jego funkcja sprowadza się do wyboru optymalnej trasy i przesyłania nią pakietów. W przypadku wystąpienia awarii, na którymś z połączeń protokół będzie próbował dostarczyć pakiety trasami alternatywnymi (nie zawsze optymalnymi).
- Protokół IP jest podstawowym protokołem przesyłania pakietów w Internecie. Protokół IP jest protokołem bezpołączeniowym. Oznacza to, że w celu przesłania pakietów nie jest nawiązywane połączenie z hostem docelowym. Pakiety mogą być przesyłane różnymi trasami do miejsca przeznaczenia, gdzie są następnie składane w całość. Podobna zasada działa przy przesyłaniu listów tradycyjnym systemem pocztowym. Tutaj również w momencie wysyłania listu adresat nie musi potwierdzać, że przesyłkę odbierze.
- Do przesyłania danych protokół IP używa specjalnego formatu pakietu. Pakiet ten składa się z nagłówka pakietu oraz danych do przesłania. Zgodnie z zasadą przesyłania strumieniowego dane protokołu IP są danymi pochodzącymi z wyższych warstw modelu ISO/OSI. Dane te są następnie enkapsulowane do postaci pakietu IP. Przy przejściu do warstwy łącza danych pakiet IP jest enkapsulowany do postaci ramki Ethernetowej.

Format pakietu IPv4 1



Format pakietu IPv4 2

- Poszczególne pola pakietu mają następujące znaczenie: -
  - wersja (VERS) - pole 4-bitowe określające typ protokołu IP. Jeśli jest tam wpisana wartość 4 oznacza to wersję czwartą protokołu. Jeśli jest tam wartość 6 oznacza to IPv6. Rozróżnianie pomiędzy pakietami wersji 4 i 6 jest przeprowadzane już przy analizowaniu ramki warstwy drugiej poprzez badanie pola typu protokołu.
  - długość nagłówka (HLEN) - pole 4 bitowe określające długość datagramu wyrażoną jako wielokrotność słów 32 bitowych.
  - typ usługi (TOS ang. Type-of-Service) - 8-bitowe pole określające poziom ważności jaki został nadany przez protokół wyższej warstwy. Znaczenie poszczególnych bitów tego pola jest następujące: pierwsze 3 bity: wartość 0 - stopień normalny, wartość 7 - sterowanie siecią czwarty bit - O - prośba o krótkie czasy oczekiwania piąty bit - S - prośba o przesyłanie danych szybkimi łączami szósty bit P - prośba o dużą pewność przesyłania danych bity 6, 7 nieużywane
  - całkowita długość - pole 16-bitowe. Długość całego pakietu wyrażona w bajtach. W celu uzyskania długości pola danych należy odjąć od długości całkowitej długość nagłówka. Wartość minimalna wynosi 576 oktetów zaś maksymalna 65535 oktetów, tzn. 64 kB
  - Identyfikacja - 16 bitowe pole używane do określania numeru sekwencyjnego bieżącego datagramu.
  - Znaczniki - 3 bitowe pole. Pierwszy najbardziej znaczący ma zawsze wartość 0. Kolejne znaczące bity sterują fragmentacją (0- oznacza, czy pakiet może zostać podzielony na fragmenty, 1 - nie może być podzielony). Trzeci bit oznacza: ostatni pakiet powstały w wyniku podzielenia (jeśli ma wartość 1) lub pakiet ze środka 0.

Format pakietu IPv4 3

- Przesunięcie fragmentu - 13-bitowe pole służące do składania fragmentów datagramu.
- Czas życia (TTL, ang. Time To Live) - 8-bitowe pole określające liczbę routerów (przeskoków), przez które może być przesłany pakiet. Wartość tego pola jest zmniejszana przy przejście przez każdy router na ścieżce. Gdy wartość tego pola wynosi 0, wtedy pakiet taki jest odrzucany. Zasada ta pozwala na stosowanie mechanizmów zapobiegających zapętlaniu się tras routingu.
- Protokół - 8-bitowe pole określające, który z protokołów warstwy wyższej odpowiada za przetworzenie pola Dane.
- Suma kontrolna nagłówka - 16-bitowe pole z sumą kontrolną nagłówka pozwalającą stwierdzić, czy nie nastąpiło, naruszenie integralności nagłówka. Ze względu na fakt, że każdy router dokonuje zmian w nagłówku musi ona być przeliczona na każdym z routerów.
- Adres IP nadawcy - 32-bitowe pole z adresem IP nadawcy pakietu
- Adres IP odbiorcy - 32-bitowe pole z adresem IP odbiorcy pakietu
- Opcje - pole to nie występuje we wszystkich pakietach.
- Uzupełnienie (Wypełnienie) - pole to jest wypełnione zerami i jest potrzebne, żeby długość nagłówka była wielokrotnością 32 bitów (patrz-> Długość nagłówka) Dane - pole od długości do 64kB zawierające dane pochodzące z wyższych warstw.

Wartość pola „protokół” nagłówka IPv4

- Wartości wpisane w pole „protokół” nagłówka IP mają następujące znaczenie:
  - 1 - ICMP (ang. Internet Control Message Protocol) - protokół komunikacyjny sterowania siecią Internet
  - 2 - IGMP (ang. Internet Group Message Protocol) - protokół zarządzania grupami Internetowymi
  - 6 – TCP - (ang. Transmission Control Protocol) - protokół sterujący transmisją
  - 8 - EGP - (ang. Exterior Gateway Protocol) - zewnętrzny protokół bramowy
  - 17 - UDP - (ang. User Datagram Protocol) - protokół datagramów użytkownika

Pole opcji nagłówka pakietu IPv4

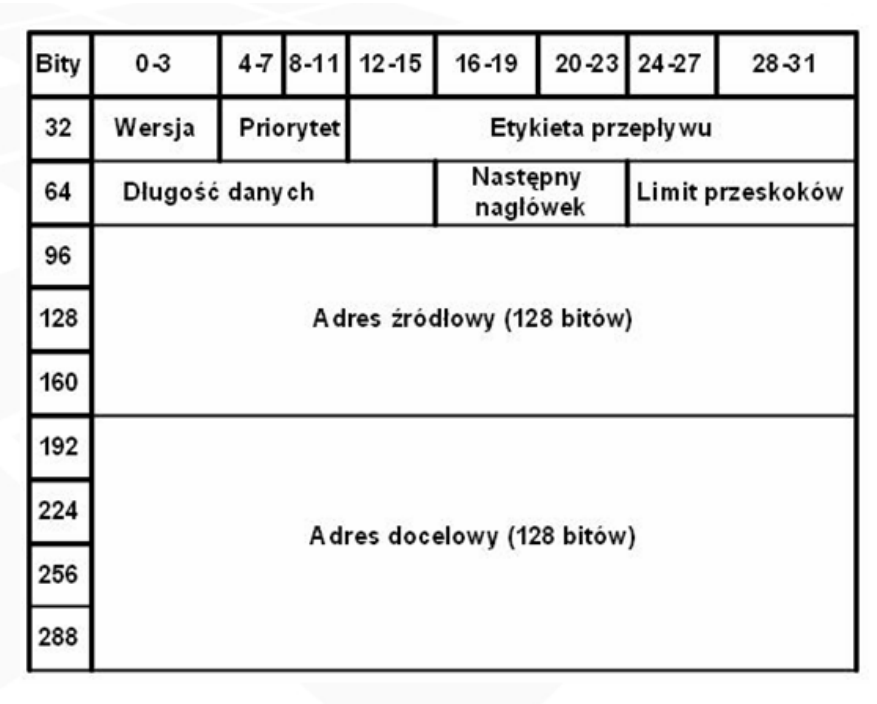
Bajt kodu w polu opcje

Klasa opcji	Numer opcji	Długość	Opis
0	0	-	Koniec listy opcji-używane,gdy opcje nie kończą się wraz z końcem nagłówka
0	1	-	Brak przypisanej funkcji, służy do wyrównania bajtów w liście opcji
0	2	11	Ograniczenia związane z bezpieczeństwem i obsługą
0	3	zmienna	Zapisuj trasę - do śledzenia trasy
0	7	zmienna	Identyfikator strumienia - przestarzałe
0	8	4	Rygorystyczne trasowanie według nadawcy
0	4	zmienna	Używana do zapisywania czasów wzdłuż trasy pakietów

Protokół IPv6

- Potrzeby wdrożenia:
  - Wyczerpywanie się dostępnej przestrzeni adresowej w IPv6
  - Wymagane ustalone parametry transmisji dla ruchu multimedialnego trudne do zagwarantowania przez IPv4
  - Brak możliwości uwierzytelnienia nadawcy.

Budowa datagramu IPv6



- Pole priorytet pozwala na ustalenie ważności (priorytetu) pakietu – multimedia
- Etykieta przepływu – możliwość wskazania wrażliwości na zmiany czasów opóźnień
- Wydłużone pola adresów – $6.7*10^{17}$ adresu na mm^2 powierzchni Ziemi

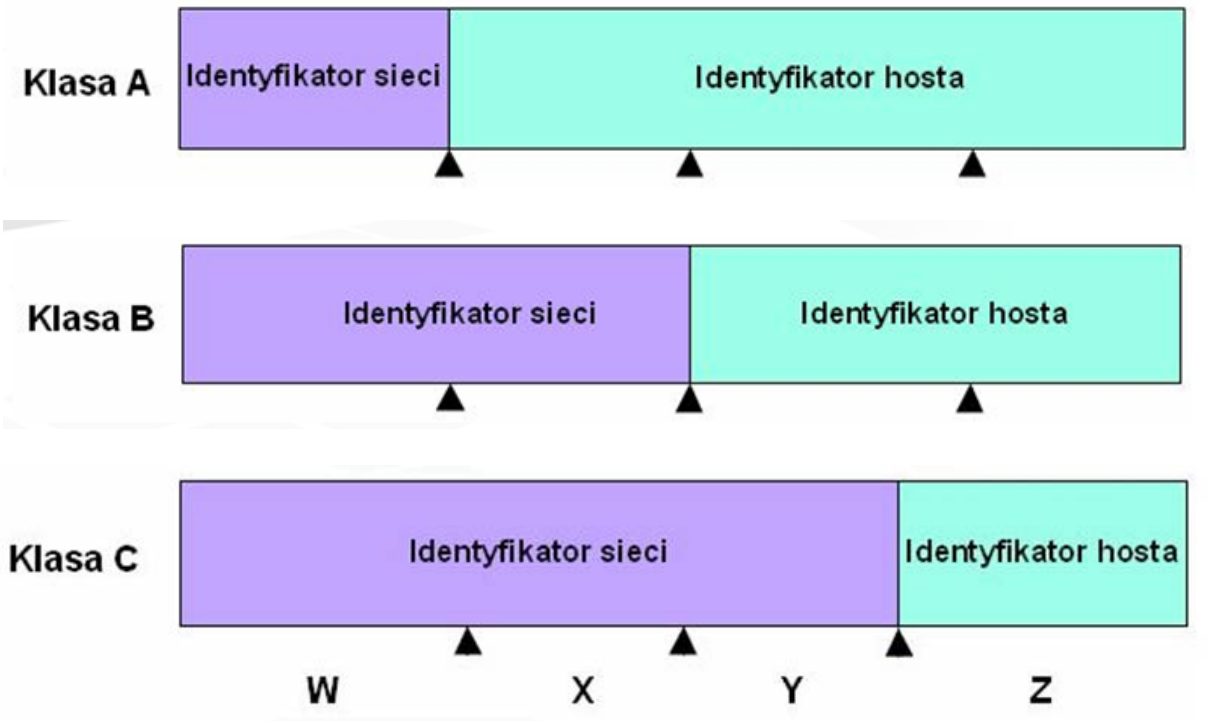
Adresacja w sieciach komputerowych 1

- Adres MAC – Adresacja fizyczna – warstwa łącza danych
  - Adres MAC jest adresem identyfikującym konkretne urządzenia i nadawanym przez producenta,
- Adres IP – Adresacja logiczna – warstwa sieci
  - Adres IP jest adresem logicznym i nadawany w zależności od tego do jakiej sieci zostało podłączone dane urządzenie sieciowe,

Przydział adresu IP

- Organizacja przydzielająca:
  - Internet Assigned Numbers Authority (IANA)
- Wersje adresacji:
  - IPv4 : 32 bity - dostępne adresy 2^32
  - IPv6: 128 bitów odstępne adresy 2^128
- Struktura adresu:
  - Identyfikator sieci
  - Identyfikator hosta
  - Maska sieciowa - netmaska

Adresacja klasowa



Klasa adresu IP	Zakres adresu IP (zapis dziesietny - zapis binarny)
Klasa A	1 - 126 (00000001 - 01111110)
Klasa B	128 - 191 (10000000 - 10111111)
Klasa C	192 - 223 (11000000 - 11011111)
Klasa D	224 - 239 (11100000 - 11101111)
Klasa E	240 - 255 (11110000 - 11111111)

Zasady adresowania

- pierwszą liczbą identyfikatora nie może być 127
- identyfikator hosta nie może składać się z samych liczb 255
- identyfikator hosta nie może składać się z samych zer
- identyfikator hosta nie może powtórzyć się w sieci

Ograniczenia adresacji z zastosowaniem klas

- niedopasowanie liczby dostępnych adresów do faktycznej liczby hostów w sieci:
  - nadmiarowość adresów w organizacjach z niewielką liczbą hostów (np. 25 hostów)
  - braki adresów dla organizacji z dużą liczbą hostów (np. 300)
- duże tablice routingu.

Próby rozwiązania problemów z niedoborem adresów IPv4

- Tworzenie podsieci (1985 r)
- Tworzenie podsieci o zróżnicowanej długości adresów (1987 r)
- Bezklasowy routing międzydomenowy - CIDR (1993)
- Wydzielenie prywatnych adresów IP
- Translacja adresów sieciowych (NAT)
- Automatyczne przydzielanie adresów

Adresy prywatne

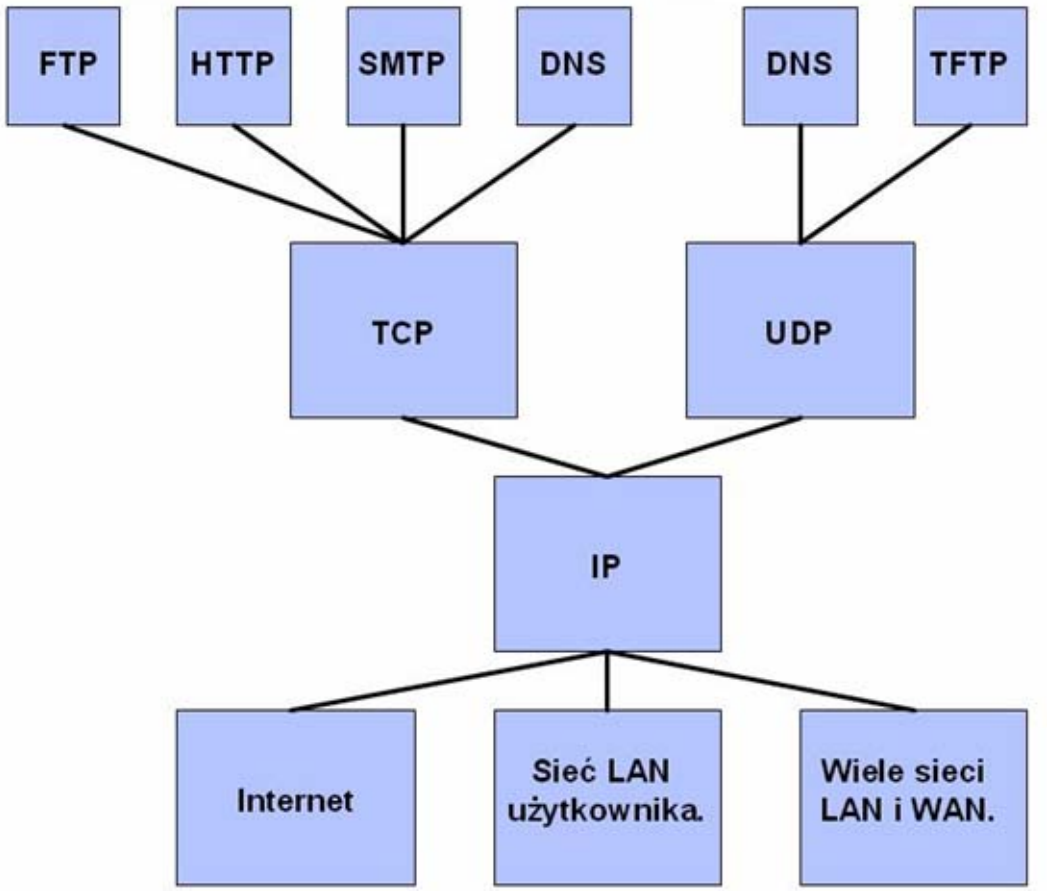
- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Adresy IPv6

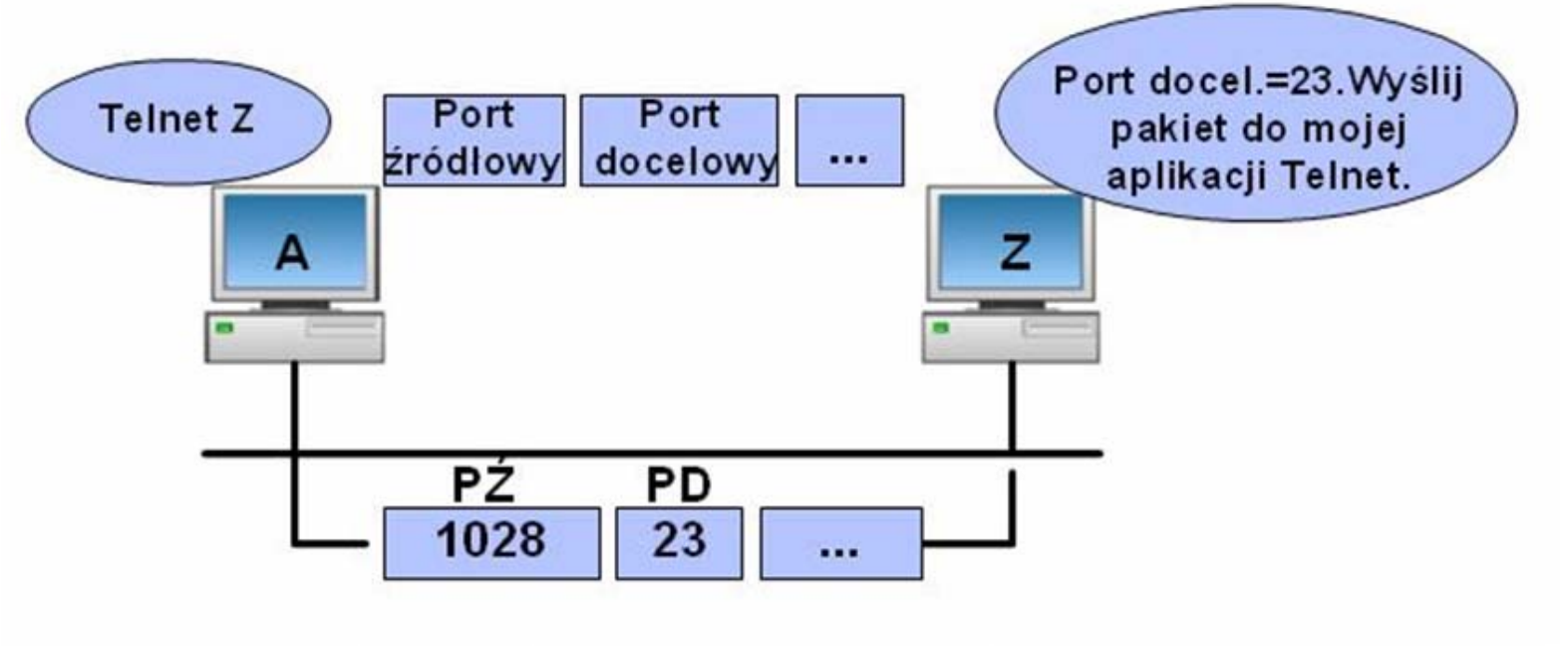
- Adres 128 bitowy
- Zapisywany w postaci heksadecymalnej co 16 bitów np.:
  - 0432:5678:abcd:00ef:0000:0000:1234:4321
  - 432:5678:abcd:ef::1234:4321
  - 0:0:0:0:0:FFFF:129.144.52.38
- Obecnie tunelowany w sieciach IPv6

Protokoły warstwy transportowej

- UDP
- TCP



Port



W warstwie transportowej istnieje mechanizm określania, do której aplikacji adresowane są przesyłane przy pomocy protokołu IP pakiety. Zarówno protokół TCP jak i UDP dysponują niezależnymi numerami, które określają numer portu. Standardowe numery portów zostały określone w dokumencie RFC 1700

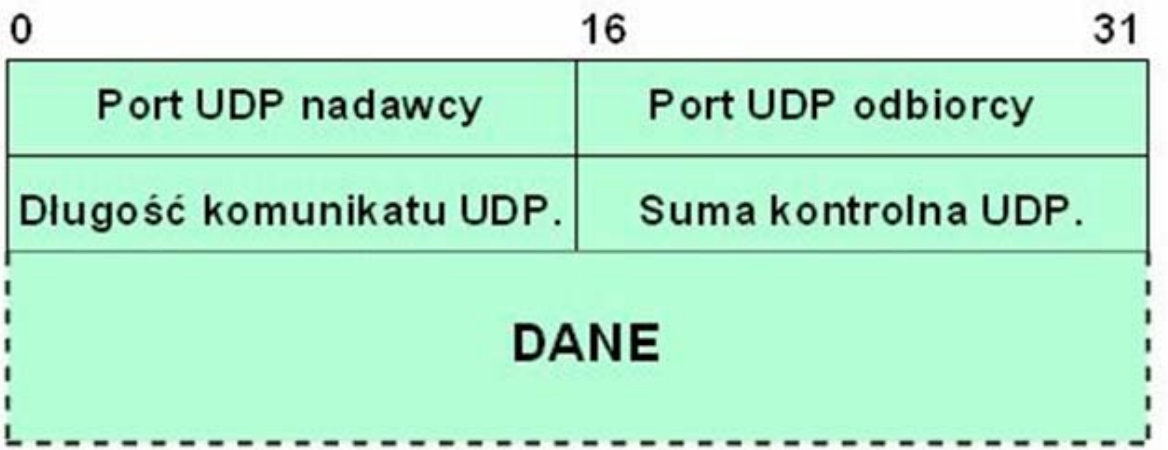
Definicja gniazda

- Numer IP
- Numer portu TCP lub UDP

UDP

- Cechy:
  - Bezpołączeniowy
  - Brak kontroli przepływu
  - Zawodny
- Zastosowania:
  - Wideokonferencje
  - Przesyłanie strumieni dźwięku
  - Gry sieciowe
  - Komunikatory sieciowe
  - Rozwiązywanie nazw symbolicznych (DNS)
  - Przesyłanie plików (TFTP)
  - NFS
  - VoiPRPC

Protokół UDP – format segmentu

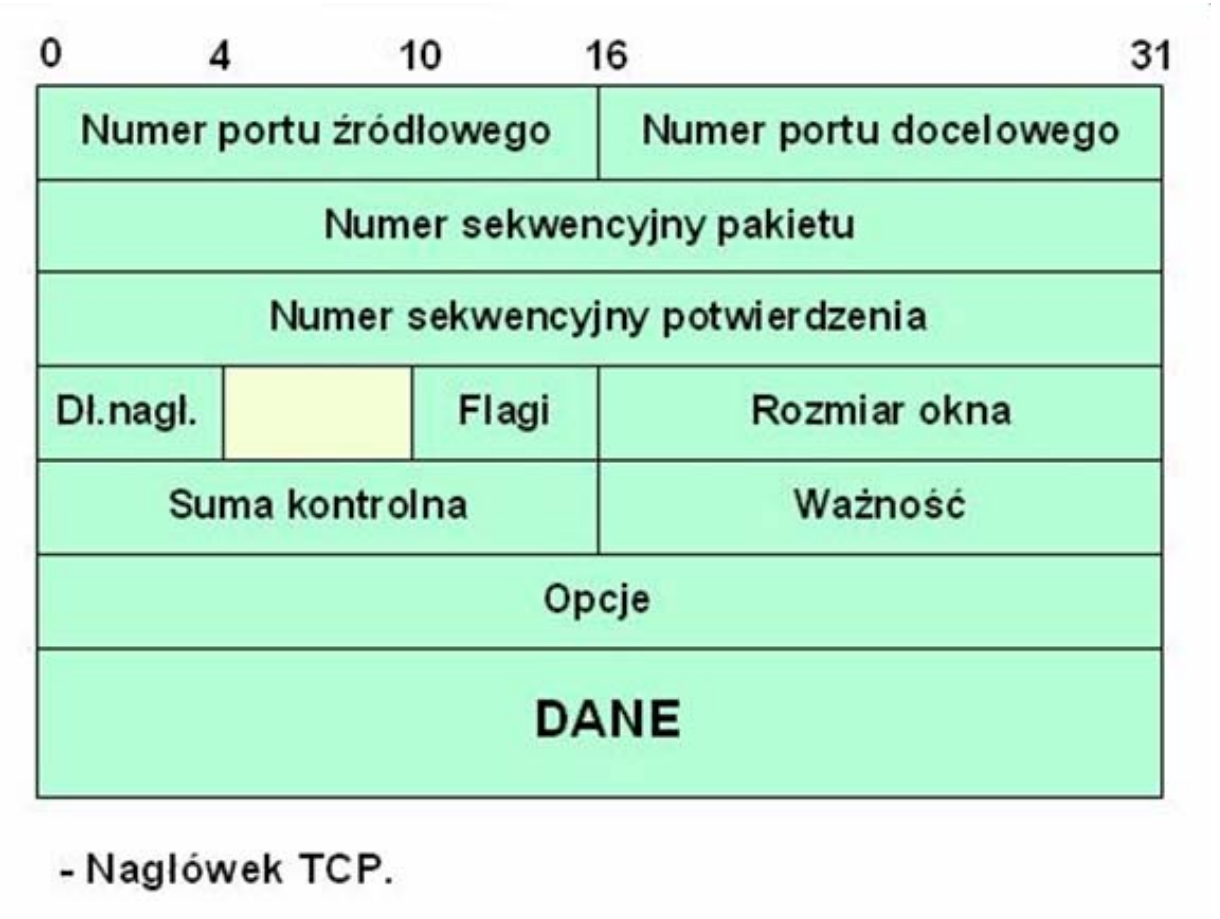


- Nagłówek UDP.

Protokół TCP

- Niezawodne przesyłanie danych
  - Wykorzystywanych jest do tego kilka mechanizmów, takich jak: sumy kontrolne i numery sekwencyjne. Zagubione pakiety są ponownie retransmitowane.
- Kontrola przeciążeń
  - W przypadku, gdy następuje przeciążenie protokół TCP zmniejsza prędkość nadawania segmentów przez urządzenie nadawcze.
- Porządkowanie
  - Segmenty protokołu TCP są enkapsulowane w pakiety IP i przesyłane przy użyciu tego protokołu. Ze względu na właściwości IP polegające na przesyłaniu w sposób skuteczny pakietów wszelkimi możliwymi drogami, segmenty mogą dotrzeć do adresata w różnej kolejności. Mechanizm porządkowania segmentów umożliwia nadawanie im numerów sekwencyjnych, które następnie ułatwiają ponowne złożenie danych.
- Sterowanie przepływem
  - w sytuacji, gdy host docelowy lub łącze pozwala na szybszą transmisję następuje przesyłanie kilku segmentów w jednym pakiecie. W sytuacji odwrotnej, tzn. przy przeciążonym adresacie lub ograniczonej przepustowości łącza następuje zwolnienie transmisji poprzez przesyłanie mniejszej liczby segmentów lub pojedynczych segmentów.

Protokół TCP: format segmentu



- Naglówek TCP.

UDP vs. TCP

Cecha	UDP	TCP
połączeniowy	nie	tak
nagłówek zawiera długość segmentu	tak	nie
sumy kontrolne	opcjonalne	tak
potwierdzenie pozytywne	nie	tak
retransmisje i kontrola czasu	nie	tak
wykrywanie powtórzeń	nie	tak
numery sekwencyjne	nie	tak
kontrola przepływu	nie	tak

DNS

- Kluczowym elementem projektu DNS jest hierarchiczna struktura nazw. Wszystkie nazwy są wieloczłonowe i rozpoczynają się od wspólnego korzenia (ang. root), reprezentowanego znakiem „.” (kropki). Poszczególne człony nazwy także oddzielane są od siebie znakiem kropki, np.: www.prz.edu.pl.
- Nazwę zapisuje się począwszy od ostatniego członu, który najczęściej oznacza nazwę hosta w danej organizacji, w kierunku członów bardziej ogólnych tworzących nazwę domeny tej organizacji.

DNS – hierarchia domen

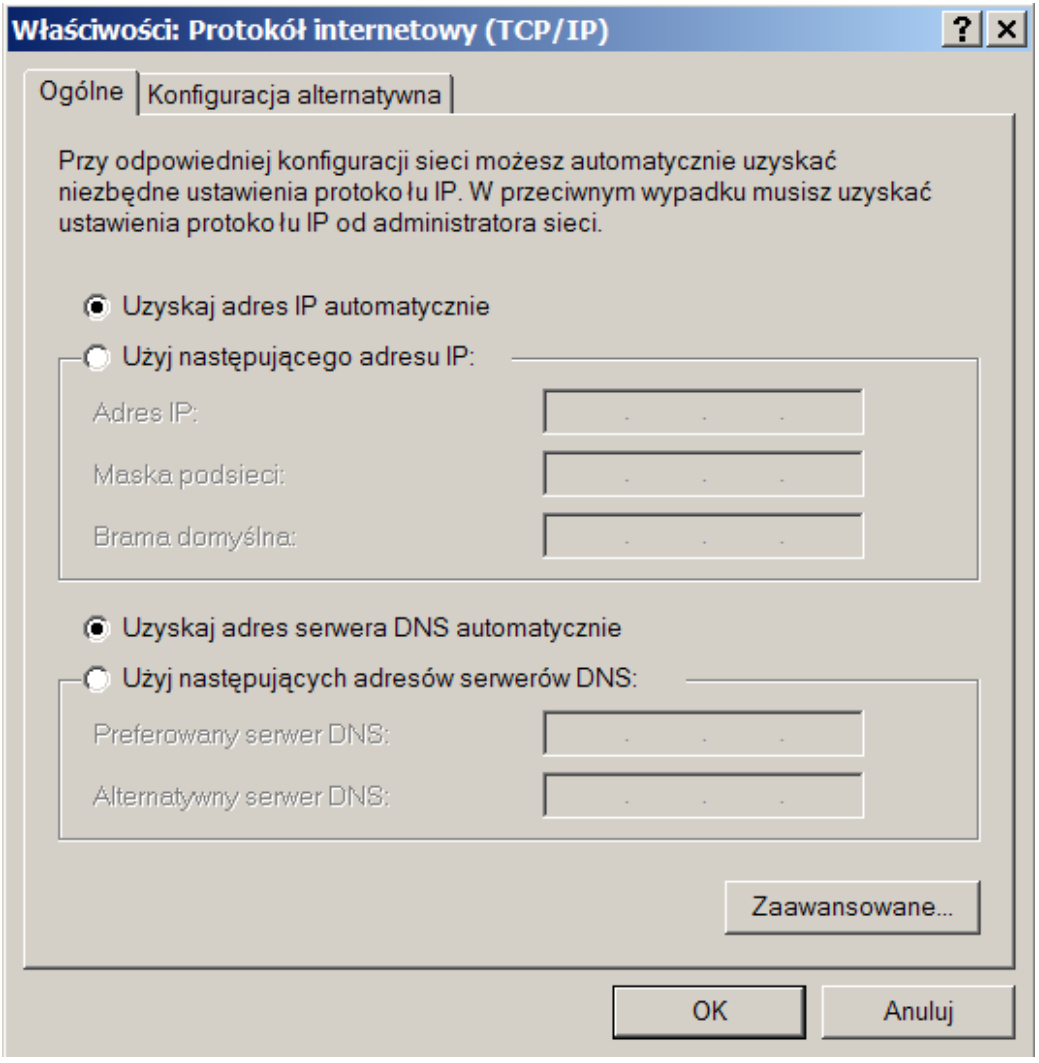
- Pierwszym członem w nazwie domenowej jest tzw. domena pierwszego poziomu TLD (and. Top-Level Domain). Poniżej domeny pierwszego poziomu może znajdować się dowolnie dużo poddomen drugiego poziomu, poniżej których może znajdować się dowolnie wiele poddomen trzeciego poziomu, itd.
- W pierwotnej specyfikacji znalazło się siedem domen pierwszego poziomu: .com, .edu, .mil, .gov, .net, .org, .int, oraz dwuliterowe domeny narodowe. Obsługa każdej z domen delegowana jest do odpowiedniej organizacji, odpowiedzialnej za daną domenę. Po kilkunastu latach od chwili ogłoszenia pierwszej specyfikacji zostały zgłoszone propozycje nowych domen pierwszego poziomu, z których zaakceptowano kolejnych siedem, z czego cztery .biz, .info, .name, .pro otrzymały status domen ogólnie dostępnych, natomiast pozostałe trzy .aero, .coop, .museum status domen sponsorowanych.
- Spośród domen znajdujących się w pierwotnej specyfikacji, w trzech: .com – firmy comercyjne, .net – firmy/organizacje zajmujące się ogólnie rozumianą technologią sieciową, .org – firmy/organizacje non-profit rejestracja nie podlega ograniczeniom, natomiast w pozostałych czterech rejestracja odbywa się według ściśle określonych kryteriów: .edu – jednostki oficjalnie uznane za edukacyjne w USA, .mil – Armia USA, .gov – instytucje rządowe USA, .int – organizacje oficjalnie zajmujące się obsługą Internetu na podstawie umów międzynarodowych.
- Nazwy domen pierwszego poziomu oraz związane z nimi zasady rejestracji zostały przeniesione i zaakceptowane w odniesieniu do domen drugiego poziomu domen narodowych. Ostatecznie zasady organizacji domen zostały dość mocno rozluźnione.

Serwery DNS

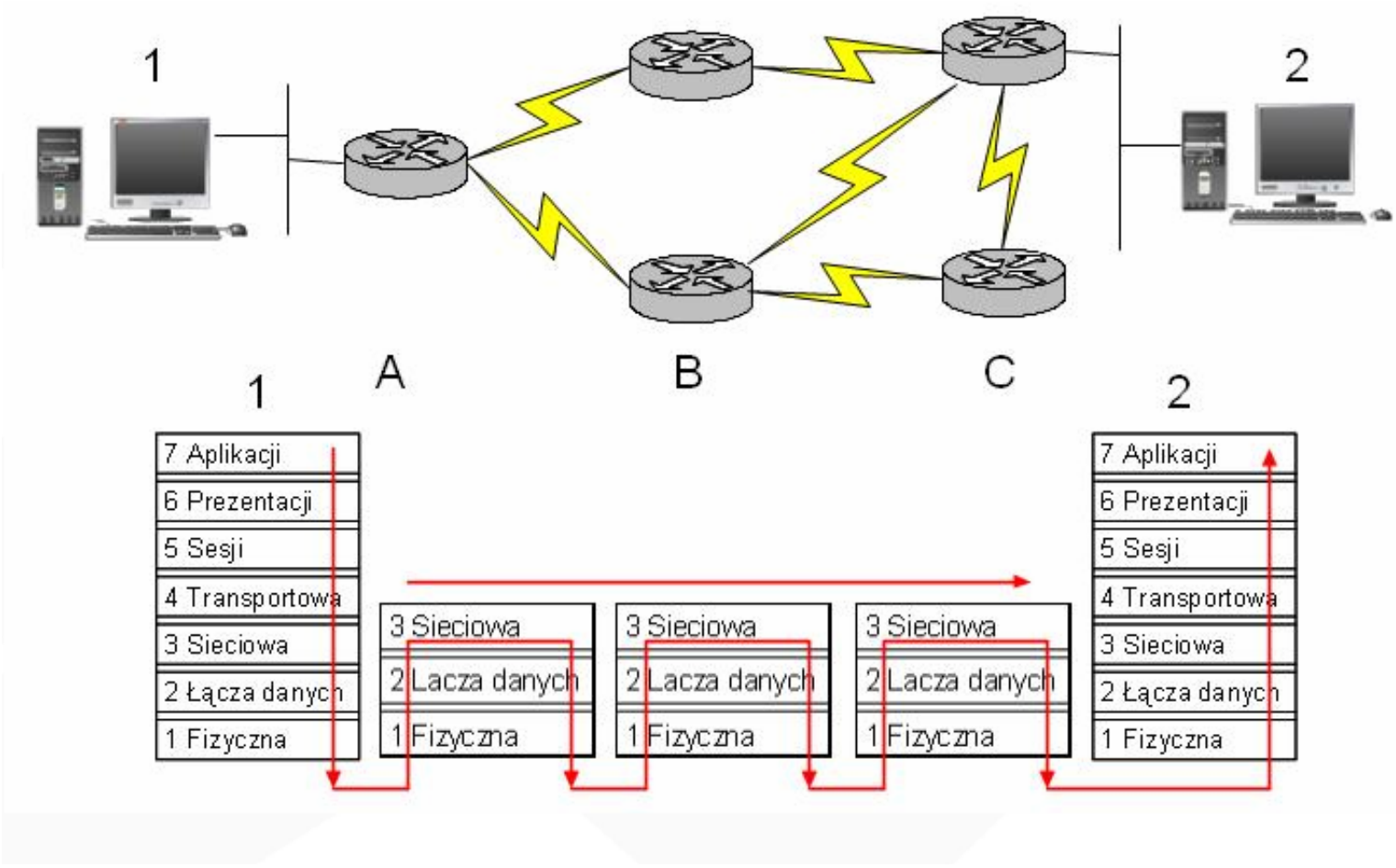
- Nie ma jednej centralnej bazy danych adresów IP i nazw. Najważniejszych jest 13 serwerów rozrzuconych na różnych kontynentach.
- Serwery DNS przechowują dane tylko wybranych domen.
- Każda domena ma co najmniej 2 serwery DNS obsługujące ją, jeśli więc nawet któryś z nich będzie nieczynny, to drugi może przejąć jego zadanie.
- Serwery DNS przechowują przez pewien czas odpowiedzi z innych serwerów (ang. *caching*), a więc proces zamiany nazw na adresy IP jest często krótszy niż w podanym przykładzie.
- Każdy komputer może mieć wiele różnych nazw. Na przykład komputer o adresie IP *207.142.131.245* ma nazwę *pl.wikipedia.org* oraz *de.wikipedia.org*
- Czasami pod jedną nazwą może kryć się więcej niż 1 komputer po to, aby jeśli jeden z nich zawiedzie, inny mógł spełnić jego rolę.
- Jeśli chcemy przenieść serwer WWW na inny szybszy komputer, z lepszym łączem ale z innym adresem IP, to nie musimy zmieniać adresu WWW strony, a jedynie w serwerze DNS obsługującym domenę poprawiamy odpowiedni wpis.
- Protokół DNS posługuje się do komunikacji tylko protokołem UDP.
- Serwery DNS działają na porcie numer *53*.

Konfiguracja DNS w Windows

- START -> Panel sterowania -> Połączenia sieciowe -> Połączenie lokalne -> Właściwości -> Protokół internetowy (TCP/IP) -> Właściwości.



Przepływ danych przez urządzenia sieciowe



Tablica routingu - przykład

Routing Table: IPv4

Destination	Gateway	Flags	Ref	Use	Interface
194.29.160.1	194.29.144.1	UGH	1	354	
194.29.150.0	194.29.144.1	UG	1	0	
194.29.149.0	194.29.144.1	UG	1	0	
194.29.148.0	194.29.144.1	UG	1	1	
194.29.147.0	194.29.144.1	UG	1	0	
194.29.146.0	194.29.144.1	UG	1	423	
194.29.145.0	194.29.145.18	U	1	3059	hme1
194.29.144.0	194.29.144.18	U	1	2958	hme0
192.168.30.0	192.168.30.2	U	1	12	le0
10.40.192.0	194.29.145.12	UG	1	3	
10.44.0.0	194.29.144.1	UG	1	713	
224.0.0.0	194.29.144.18	U	1	0	hme0
127.0.0.1	127.0.0.1	UH	3	38	lo0

Usługi sieciowe

- Poczta elektroniczna: MIME/POP3/IMAP
- Transmisja danych: FTP/NFS/SCP
- Usługi terminalowe: Telnet/SSH/Suługi terminalowe Windows
- Serwisy informacyjne: Protokół HTTP/WWW/HTML/NNTP
- Synchronizacja czasu

Ochrona danych w sieci

- Fizyczne bezpieczeństwo serwera
- Zasilanie
- Strategie tworzenia kopii zapasowych
- Procedury awaryjne
- Zasady dostępu
- Ochrona sieciowa
- Kryptografia