Sieci komputerowe

Tomasz Lewicki

WWSIS, Wrocław

czerwiec 2007

Definicja sieci komputerowej

Sieć komputerową możemy najogólniej zdefiniować jako zbiór urządzeń elektronicznych połączonych ze sobą w sposób umożliwiający im wymianę informacji o różnym przeznaczeniu i formacie oraz pozwalający na dzielenie się rozmaitymi zasobami.

Aktywne elementy sieci

Aktywnymi elementami sieci są urządzenia, które potrafią tworzyć pakiety i zmieniać ich zawartość lub wzmacniać sygnał:

- karta sieciowa (przewodowa i bezprzewodowa)
- *repeater*
- *router*, brama, most
- *access point*
- koncentrator, przełącznik

Pasywne elementy sieci

Pasywnymi elementami sieci są media transmisyjne, którymi przekazywane są pakiety bez ich modyfikacji:

- przewód miedziany koncentryczny cienki (*thin coaxial cable*) lub gruby (*thick coaxial cable*)
- „skrętka” (4 pary przewodów miedzianych) ekranowana (*Shielded Twisted Pair*, *STP*; *Foiled Twisted Pair*, *FTP*) lub nieekranowana (*Unshielded Twisted Pair*, *UTP*)
- światłowód (*fiber optic cable*) jedno- i wielomodowy
- fale radiowe i podczerwień

Urządzenia sieciowe

Przykłady urządzeń sieciowych:

- komputer osobisty, laptop
- serwer
- drukarka
- *router*, most (*bridge*), brama (*gateway*)
- przełącznik (*switch*) i koncentrator (*hub*)

Zasoby współdzielone w sieci

Zasoby współdzielone przez urządzenia sieciowe i ich użytkowników można rozumieć wielopłaszczyznowo, między innymi jako:

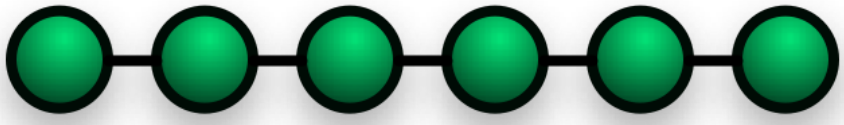
- sprzęt, np. drukarki i skanery
- pojedyńcze pliki lub ich zbiory
- programy
- bazy danych plików i użytkowników
- moc obliczeniową
- przestrzeń dyskową

Topologia sieci w ujęciu ogólnym

Topologia sieci komputerowej w znaczeniu fizycznym to sposób połączenia różnych elementów tej sieci, np. komputerów i przełączników. Wyróżniamy następujące podstawowe topologie:

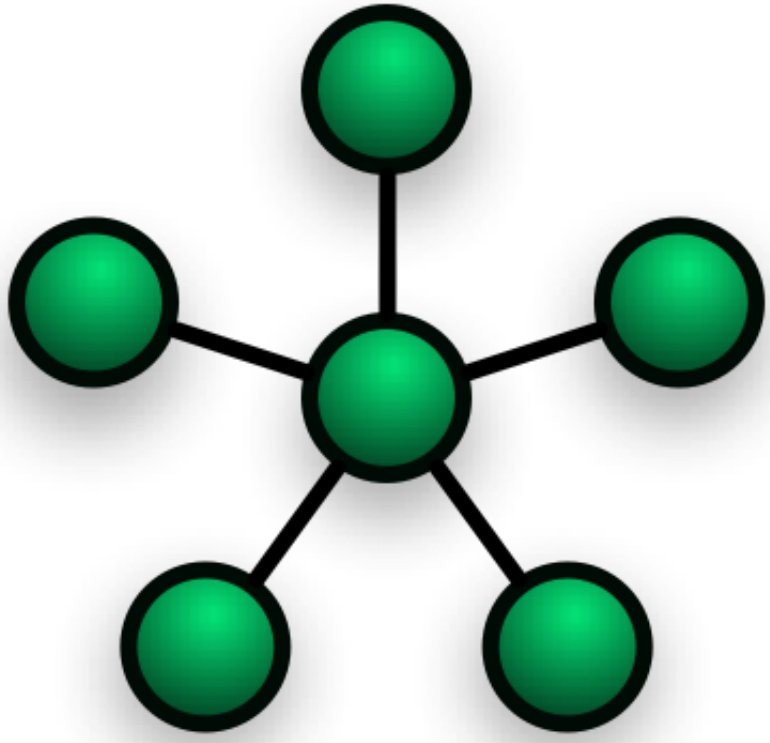
- linia (*line*)
- gwiazda (*star*), rozszerzona gwiazda
- magistrala, inaczej szyna (*bus*)
- pierścień (*ring*) pojedynczy i podwójny
- drzewo (kombinacja topologii gwiazdy i magistrali)
- siatka (*grid* oraz *mesh*)

Topologia linii



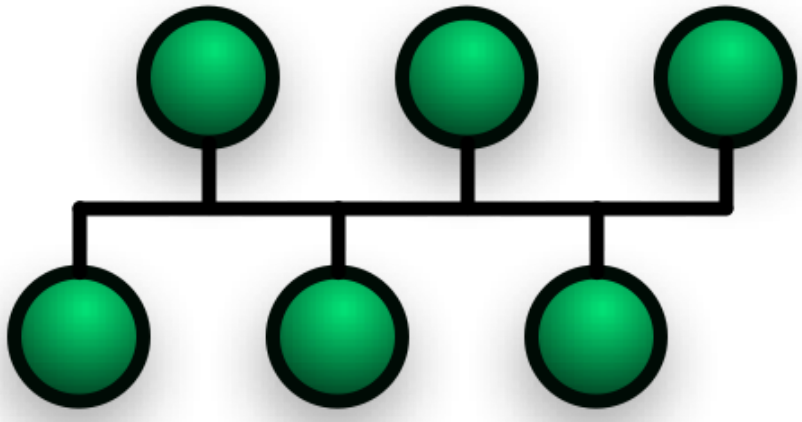
Źródło: Wikipedia

Topologia gwiazdy



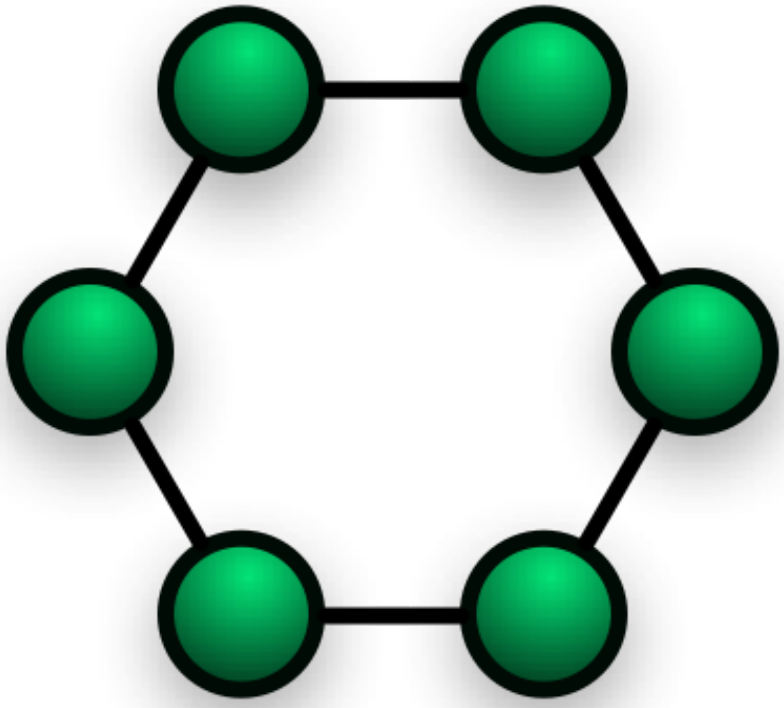
Źródło: Wikipedia

Topologia magistrali



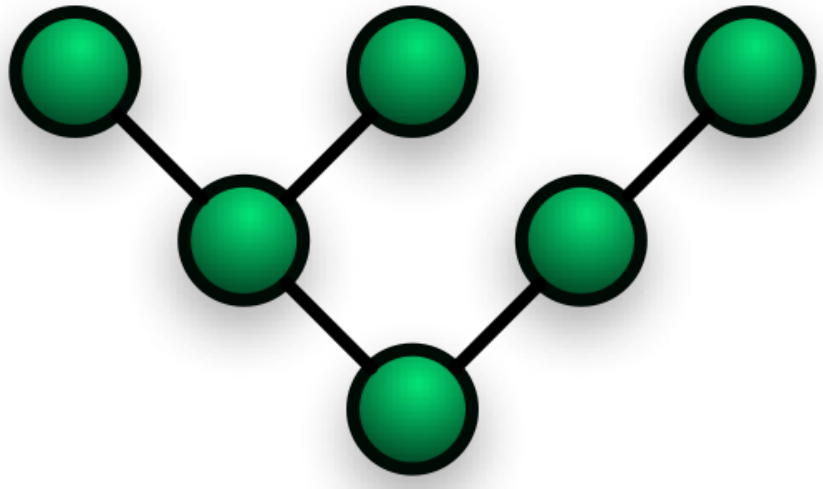
Źródło: Wikipedia

Topologia pierścienia



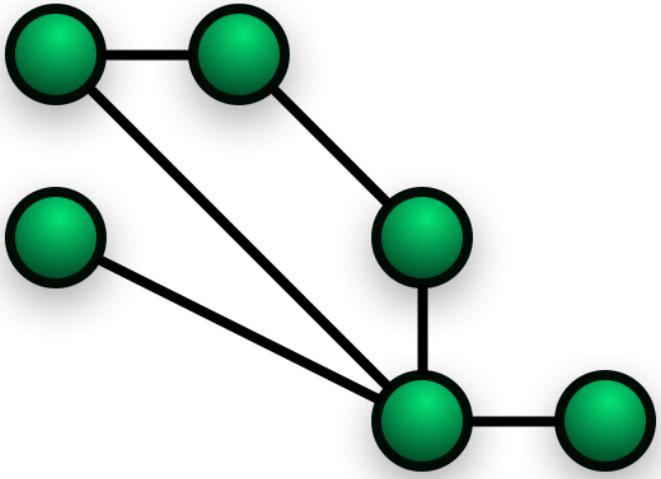
Źródło: Wikipedia

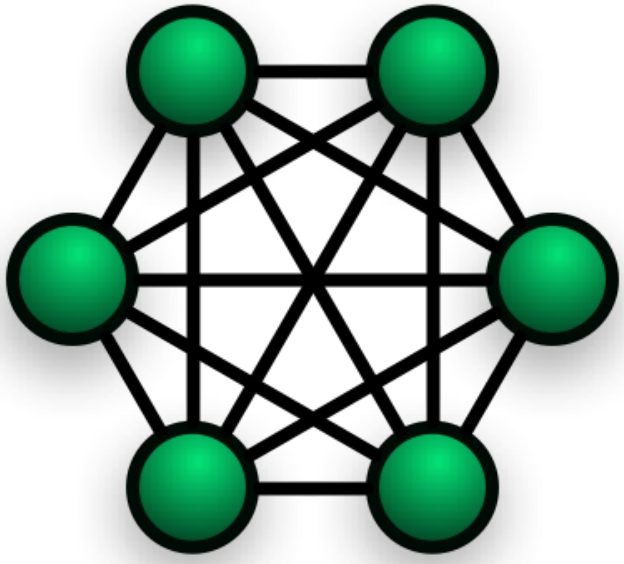
Topologia drzewa



Źródło: Wikipedia

Topologia siatki





Źródło: Wikipedia

Topologie sieci bezprzewodowych

W przypadku lokalnych sieci bezprzewodowych (*Wireless Local Area Network*, *WLAN*) nomenklatura jest inna. Mówimy raczej o:

- **połączeniach bezpośrednich** (*ad-hoc*), gdy komputery komunikują się bezpośrednio ze sobą bez pomocy innych urządzeń. Taka topologia ma zastosowanie w bardzo małych sieciach WLAN, tworzonych tymczasowo
- **sieci strukturalnej** (*infrastructure*), w której istnieje tzw. punkt dostępowy (*access point*), za pośrednictwem którego odbywa się wymiana danych między urządzeniami

Zasięg sieci

Innym kryterium podziału sieci komputerowych jest ich **zasięg**, czyli obszar objęty siecią:

- PAN (*Personal Area Network*) — sieć o zasięgu osobistym; obszar kilku metrów w „przestrzeni osobistej”
- LAN (*Local Area Network*) — sieć lokalna w pomieszczeniu, na kondygnacji, w budynku, ewentualnie w kilku budynkach
- CAN (*Campus Area Network*) — sieć kampusowa (akademicka), łączy sieci lokalne, ale ma mniejszy zasięg niż sieć miejska
- MAN (*Metropolitan Area Network*) — sieć miejska; zasięg kilkunastu-kilkudziesięciu kilometrów
- WAN (*Wide Area Network*) — sieć rozległa; zasięg rzędu setek lub tysięcy kilometrów (kraje, kontynenty)

Technologie budowy sieci i transmisji danych

Sieci komputerowe działają w różnych technologiach i protokołach, np.

- ATM (*Asynchronous Transfer Mode*) — zbudowana na różnych mediach transmisyjnych, ma zastosowanie w sieciach LAN i WAN
- FDDI (*Fiber Distributed Data Interface*) — złożona z dwóch pierścieni (pierwotnego i wtórnego), stosowana w sieciach szkieletowych i CAN
- Frame Relay — łączy odległe od siebie sieci LAN lub pojedyńcze hosty dzięki dzierżawionym kanałom PVC (*Permanent Virtual Circuit*)
- Ethernet — jedna z najbardziej rozpowszechnionych technologii budowy sieci LAN, występuje w rozmaitych odmianach i prędkościach transmisji

W dalszej części wykładu mowa będzie wyłącznie o odmianach technologii Ethernet.

Ethernet

Ethernet jest standardem budowy sieci komputerowych opisanym w specyfikacji 802.3 organizacji IEEE (*Institute of Electrical and Electronics Engineers*). Opis obejmuje specyfikację mediów transmisyjnych, format pakietów (ramek) oraz sposób uzyskiwania dostępu do medium transmisyjnego.

Koncepcja Ethernetu sięga pierwszej połowy lat 70. XX wieku, a za ojca tej technologii uważa się dr Roberta Metcalfe'a, wówczas pracownika ośrodka badawczego firmy Xerox w Palo Alto, później założyciela firmy 3Com. Patent na Ethernet został zarejestrowany w 1975 r. Pierwsza wersja tej sieci działała z prędkością ok. 3 Mb/s i miała nieco odmienny sposób adresowania pakietów niż stosowany w obecnym Ethernecie.

Odmiany standardu Ethernet — cz. 1

Starsze technologie

Ethernet występuje w różnych odmianach. Najbardziej znane to:

- 10Base-5 (Thicknet) — sieć o prędkości 10 Mb/s, zbudowana na „grubym" kablu koncentrycznym o długości segmentu sieci do 500 m
- 10Base-2 (Thinnet) — sieć o prędkości 10 Mb/s, zbudowana na „cienkim" kablu koncentrycznym o długości segmentu sieci do 185 m (300 m w niektórych firmowych rozwiązaniach)
- 10Base-T — sieć o prędkości 10 Mb/s, zbudowana na skrętce kat. 3 lub 5 o długości segmentu sieci do 100 m (150 m przy kablu wysokiej jakości)

Powyższe trzy rozwiązania są już przestarzałe, choć czasami jeszcze można spotkać działające instalacje lub co najmniej ich pozostałości.

Odmiany standardu Ethernet — cz. 2

Nowsze technologie

Nowsze odmiany Ethernetu to m.in.:

- 100Base-TX (Fast Ethernet) — sieć o prędkości 100 Mb/s, zbudowana na skrętce kat. 5 o długości segmentu sieci do 100 m. **Jest to w tej chwili najbardziej rozpowszechniona odmiana**
- 100Base-FX — sieć o prędkości 100 Mb/s, zbudowana na włóknach światłowodowych
- 1000Base-T (Gigabit Ethernet) — sieć o prędkości 1 Gb/s, zbudowana na skrętce kat. 5 lub wyższej. Używane są wszystkie przewody — inaczej niż we wcześniejszych wersjach Ethernetu budowanego na skrętce, które korzystają z dwóch par przewodów
- 10GBase-T — sieć o prędkości 10 Gb/s, zbudowana na skrętce kat. 6, 6a lub 7 o długości segmentu od 55 do 100 m
- Ethernet bezprzewodowy — sieć o prędkości od 1 do 54 Mb/s (lub więcej w rozwiązaniach firmowych)

Media transmisyjne

Medium transmisyjne (nośnik) ma decydujące znaczenie dla określenia różnych właściwości sieci Ethernet. Jego fizyczne cechy determinują szerokość pasma transmisyjnego i częstotliwość sygnału, a przez to efektywną prędkość transmisji.

Z maksymalnej prędkości transmisji, opóźnień w rozchodzeniu się sygnału, maksymalnej dozwolonej (akceptowalnej) tłumienności będącej miarą spadku mocy sygnału w kablu oraz możliwości występowania kolizji wynika górne ograniczenie na długość segmentu sieci bez wzmacniania i powielania sygnału.

Koncentrator (hub)

- urządzenie sieciowe pierwszej warstwy modelu OSI (fizycznej)
- *hub* tworzy sieć o topologii gwiazdy
- zadaniem *huba* jest wzmacnianie i kopiowanie (powielanie) sygnałów w sieci lokalnej oraz przekazywanie ich do wszystkich urządzeń sieciowych podłączonych do *huba*
- *hub* zwiększa domenę rozgłoszeniową i kolizyjną w sieci LAN
- opóźnienia w przekazywaniu pakietów wprowadzane przez *hub* są mniejsze niż w przypadku *routera* i *switcha*

Przełącznik (switch)

- urządzenie sieciowe drugiej warstwy modelu OSI (łącza danych)
- zadaniem *switcha* jest przekazywanie pakietów pomiędzy „wirtualnymi segmentami" w sieci lokalnej, tworzącymi domeny bezkolizyjne (ograniczone do pojedynczego portu)
- *switch* jest wieloportowym mostem, przekazującym pakiety w oparciu o zawarty w nagłówku pakietu adres MAC urządzenia sieciowego
- jeśli *switch* nie potrafi określić portu docelowego, wysyła pakiet do wszystkich portów z wyjątkiem źródłowego
- *switch* jest „inteligentnym *hubem*" — przekazuje pakiety tylko do docelowego portu, a nie do wszystkich jak *hub*
- opóźnienia w przekazywaniu pakietów wprowadzane przez *switch* są mniejsze niż w przypadku *routera*, ale większe niż w przypadku *huba*

Most (bridge)

- urządzenie sieciowe drugiej warstwy modelu OSI (łącza danych)
- most łączy dwie lub więcej (pod)sieci LAN
- zadaniem mostu jest przekazywanie pakietów w oparciu o tablicę *forwardingu*, zawierającej numery portów oraz adresy MAC urządzeń działających w segmencie sieci
- most działa w tzw. trybie nasłuchu (*promiscuous mode*), tzn. odbiera wszystkie pakiety przepływające przez nośnik
- most jest przezroczysty dla innych urządzeń sieciowych, ponieważ nie zmienia zawartości pakietów
- most poprawia wydajność sieci dzięki blokowaniu pakietów, które nie powinny wydostać się z segmentu sieci, w którym działa most
- most wprowadza opóźnienia w przekazywaniu pakietów

Router

- urządzenie sieciowe trzeciej warstwy modelu OSI (sieci)
- *router* łączy dwie lub więcej (pod)sieci LAN, CAN, MAN lub WAN
- zadaniem *routera* jest trasowanie (*routing*) pakietów, tzn. kierowanie ich do kolejnego punktu w sieci w oparciu o zawarty w nagłówku pakietu adres IP docelowego urządzenia sieciowego oraz tablicę *routingu* (statyczną lub dynamiczną)
- w sieci Ethernet *router* może dzielić sieć lokalną na wiele tzw. wirtualnych LAN (*Virtual LAN*, VLAN) — podsieci wydzielonych logicznie na jednym fizycznym interfejsie sieciowym
- *router* dzieli sieć LAN na domeny rozgłoszeniowe i kolizyjne
- *router* wprowadza opóźnienia w przekazywaniu pakietów

Transmisja danych w sieci Ethernet

W sieci Ethernet stacje nadawczo-odbiorcze są podłączone do wspólnego medium transmisyjnego, za pośrednictwem którego wymieniają się pakietami (ramkami). Takie rozwiązanie nosi nazwę **wielodostępu z wykrywaniem (fali) nośnej i wykrywaniem kolizji** (*Carrier Sense Multiple Access with Collision Detection*, *CSMD/CD*). Schemat jego działania jest następujący:

1. ramka jest gotowa do wysłania
2. sprawdź stan nośnika: jeśli jest wolny, wyślij ramkę; jeśli jest zajęty, odczekaj pewien okres (wyrażony w tzw. *czasie bitowym*) zależny od rodzaju sieci
3. rozpocznij transmisję
4. jeśli wystąpiła kolizja, poinformuj o tym fakcie węzły w segmencie sieci (sygnał zagłuszania, *jam signal*); jeśli kolizji nie było, idź do punktu 8
5. odczekaj losowy odstęp czasu i wróć do punktu 1
6. jeśli kolizje się powtarzają i została przekroczona ich maksymalna ilość, zaprzestań transmisji ramki
7. wróć do punktu 1
8. w przypadku udanej transmisji zakończ nadawanie

Ramka sieci Ethernet

Ramka sieci Ethernet składa się z kilku pól, zawierających informacje potrzebne do dostarczenia pakietu do celu:

Preambuła	7+1 bajtów
Adres celu	6 bajtów
Adres źródła	6 bajtów
Rodzaj ramki	2 bajty
Właściwe dane	46-1500 bajtów
Suma kontrolna	4 bajty

Preambuła służy do nawiązania łączności. Jeśli danych jest mniej niż 46 bajtów, są uzupełniane zerami do tej długości. Rodzaj ramki to np. IPv4, IPv6, IPX, ARP, ...

Model OSI

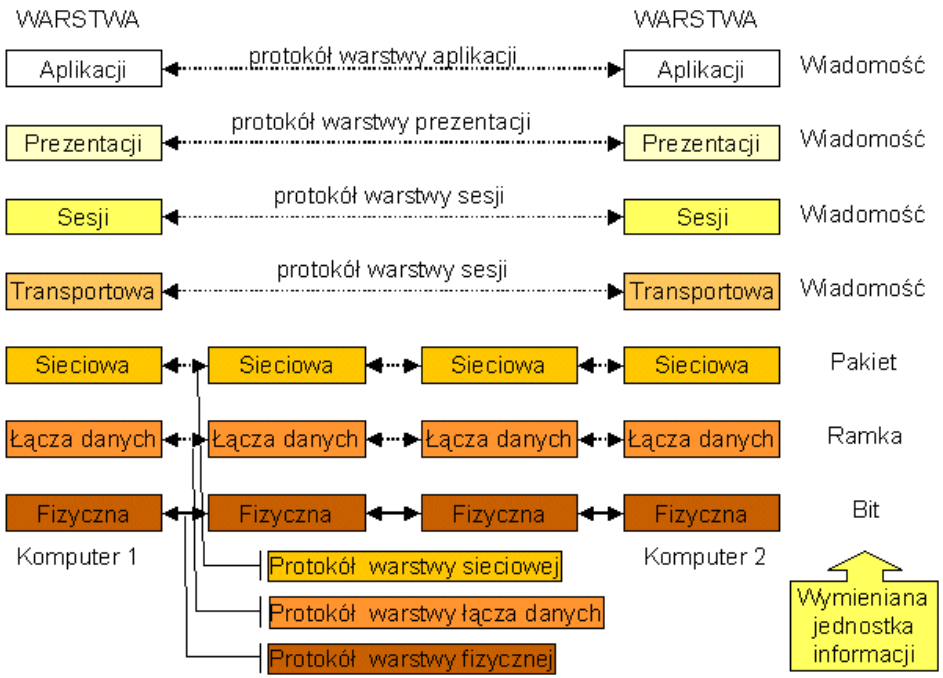
Model OSI (*Open System Interconnection*) to standard opisujący komunikację w sieci. Został zdefiniowany przez ISO (*International Standard Organization*) oraz ITU (*International Telecommunication Union*). Dzieli on komunikację sieciową na **siedem niezależnych warstw**:

- aplikacji
- prezentacji
- sesji
- transportu
- sieci
- łącza danych
- fizyczna

Model OSI jest **modelem odniesienia** dla innych modeli sieciowych.

Model OSI — c.d.

Warstwy są **niezależne od siebie**. Dla każdej z nich zdefiniowane są protokoły komunikacji z innymi warstwami. Działanie warstw wyższych jest zależne od warstw leżących niżej. Model OSI definiuje swego rodzaju **protokół określający sposób porozumiewania się protokołów sieciowych**.



Źródło: `http://www.staff.amu.edu.pl/~psi`

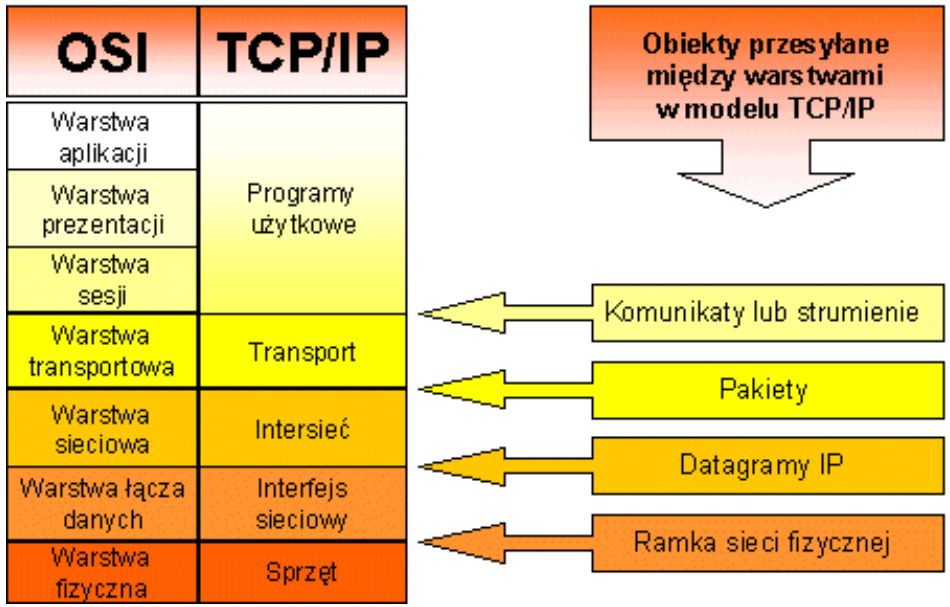
Model internetowy

Model internetowy, znany również jako model TCP/IP lub DoD (*Departament of Defense*), to uproszczona wersja modelu OSI, posiadająca cztery warstwy:

- aplikacji
- transportu
- sieci
- dostępu do sieci

Model ten dobrze oddaje **strukturę Internetu**.

Porównanie modeli OSI i internetowego



Źródło: `http://www.staff.amu.edu.pl/~psi`

Adresy MAC

Adres MAC (*Media Access Control*) to unikalny sprzętowy numer urządzenia sieciowego, nadawany w procesie produkcji na stałe (chociaż metodami programowymi można go zmieniać). Adres MAC ma długość 48 bitów i zapisuje się go w postaci szesnastkowej w sześciu grupach po dwa znaki z zakresu 0...9, A...F. Pierwsze 24 bity to oznaczenie producenta urządzenia sieciowego, pozostałe 24 bity to niepowtarzalny numer urządzenia. Adres MAC bywa nazywany **adresem fizycznym**. Adres MAC jest używany do identyfikacji urządzeń w sieci lokalnej.

Listę kodów przypisanych do producentów (pierwsze 24 bity adresu MAC) można znaleźć pod adresem
`http://standards.ieee.org/regauth/oui/oui.txt`

Adresy IP

wersja 4 (IPv4)

Adres IP (*Internet Protocol*) to numer przypisywany urządzeniom sieciowym, zarówno w sieciach lokalnych, jak i Internecie. Jest zbudowany z **czterech oktetów**, czyli ma długość **32 bitów** (4 grupy po 8 bitów). Wynika z tego, że każda z czterech grup tworzących adres IP może przyjmować wartości z zakresu $0 \ldots 255$ (2^8). Najczęściej IP zapisuje się w postaci dziesiętnej, łatwiejszej do zapamiętania.

Przykładowy adres IP w zapisie dziesiętnym: **156.17.1.38**.
Ten sam adres w postaci oktetów wygląda następująco:
10011100.00010001.00000001.00100110.

Adresy IPv4

Klasy adresowe

Adres IP składa się z **części sieciowej** oraz **części hosta**. W różnych adresach IP występują one w różnych „proporcjach”, a do ich oddzielenia stworzono pojęcie **maski podsieci** (*subnet mask*). Cała 32-bitowa przestrzeń adresowa jest podzielona na pięć tzw. **klas adresowych**: A, B, C, D i E.

	Klasa A — duże sieci (mało sieci, dużo hostów)
IP	0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
Adresy	0.0.0.0 — 127.255.255.255
Liczba sieci	128 (2^7)
Liczba hostów	$\approx 17 \cdot 10^6$ ($16777214 = 2^{24} - 2$)

Adresy IPv4

Klasy adresowe — c.d.

Klasa B — średnie sieci (średnia ilość sieci i hostów)

IP	01nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh
Adresy	128.0.0.0 — 191.255.255.255
Liczba sieci	16384 (2^{14})
Liczba hostów	65534 ($2^{16} - 2$)

Klasa C — małe sieci (dużo sieci, mało hostów)

IP	110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh
Adresy	192.0.0.0 — 223.255.255.255
Liczba sieci	$\approx 2 \cdot 10^6$ ($2097150 = 2^{21}$)
Liczba hostów	254 ($2^8 - 2$)

Klasa D to tzw. **adresy grupowe**, służące do *multicastingu* (stosowanego m.in. w telekonferencjach). Klasa E jest klasą badawczą i eksperymentalną.

Adresy IPv4

Adresy publiczne, zarezerwowane i prywatne

Z puli dostępnych adresów IP wydzielono kilka zakresów o specjalnym przeznaczeniu:

Zarezerwowane

0.0.0.0 — wszystkie komputery w Internecie
127.0.0.0-127.0.0.255 (127.0.0.1/8) — interfejs lokalny (*localhost*)

Prywatne

10.0.0.0-10.255.255.255 (10.0.0.0/8) — sieć klasy A (1 sieć)
172.16.0.0-172.31.255.255 (172.16.0.0/12) — sieć klasy B (16 sieci)
192.168.0.0-192.168.255.255 (192.168.0.0/16) — sieć klasy C (256 sieci)

Adresy IPv4

Adresy publiczne, zarezerwowane i prywatne — c.d.

Poza wymienionymi wcześniej zakresami istnieje jeszcze kilkanaście innych, nieużywanych „na co dzień". Pozostałe zakresy znajdują się w gestii organizacji IANA (*Internet Assigned Numbers Authority*), która rozdziela klasy adresowe lokalnym organizacjom (*Internet Service Providers*, ISPs); te z kolei dzielą zakresy na „własnym podwórku".

Adresy prywatne mają szczególne znaczenie, umożliwiają bowiem budowanie prywatnych sieci lokalnych, w których adresy urządzeniom sieciowym przypisuje administrator odpowiedniej sieci LAN. Najczęstszym powodem stosowania adresów z puli prywatnej jest niewielka pojemność klas publicznych przydzielonych danej organizacji. Dobrym przykładem wykorzystania adresów prywatnych jest NAT (*Network Address Translation*), w którym do jednego adresu publicznego można przypisać wiele adresów prywatnych.

Adresy ARP

ARP (*Address Resolution Protocol*) to protokół wykorzystywany do zamieniania adresów **logicznych** (IP) na adresy **fizyczne** (MAC) urządzeń sieciowych. **ARP ma zastosowanie tylko w sieciach LAN**. Operuje w warstwie łącza danych (druga warstwa modelu OSI).

Tablica ARP zawiera pary IP-MAC dla konkretnych urządzeń. Każde „inteligentne" urządzenie sieciowe posiada taką tablicę, dzięki czemu może lokalizować inne urządzenia w sieci na podstawie ich adresów sprzętowych. Jeśli informacja ma być wysłana poza sieć lokalną (ewentualnie podsieć), to adres MAC jest zastępowany adresem IP.

Tablice ARP zazwyczaj są **dynamiczne**, ale można również utworzyć tablicę statyczną.

Adresy IPv4

Routing (wyznaczanie tras)

Wyznaczaniem drogi dla pakietów przeznaczonych dla odległych systemów zajmują się *routery*. Określenie, czy pakiet jest przeznaczony dla urządzenia w sieci lokalnej czy poza nią opiera się na masce sieci urządzenia, które jest źródłem pakietu. Jeśli maska sieci celu jest identyczna z maską sieci źródła pakietu, to rozpoznanie urządzenia docelowego odbywa się za pomocą protokołu ARP. Jeśli maski urządzenia źródłowego i docelowego są różne — pakiet jest kierowany do urządzenia trasującego. Przechodząc przez kolejne *routery* pakiet dociera do urządzenia docelowego.

Trasę pakietu do zdalnego systemu można sprawdzić za pomocą polecenia `traceroute` (Linux) lub `tracert` (Windows). Różne ciekawe informacje o odległych hostach można również uzyskać komendą `ping`, która posługuje się protokołem ICMP (*Internet Control Message Protocol*).

IPv4 vs. IPv6

Aby zapobiec niebezpieczeństwu wyczerpania się adresów IP z puli adresów 32-bitowych, IANA zaproponowała wprowadzenie adresacji 128-bitowej, tzw. **IP w wersji 6** (IPv6). Nowa adresacja eliminuje niedoskonałości starszej wersji, m.in. ułatwia autokonfigurację urządzeń sieciowych na podstawie adresu MAC, wprowadza mechanizmy zabezpieczeń na poziomie pakietu, umożliwia „znakowanie" pakietów, np. dla celów QoS.

IPv4 ma pojemność $2^{32} \approx 4,3 \cdot 10^9$ adresów, natomiast IPv6 ma pojemność $2^{128} \approx 3,4 \cdot 10^{38}$ adresów.

W puli adresów IPv6 również wydzielono zakresy o specjalnym przeznaczeniu.

Protokoły sieciowe

W celu wymiany informacji różne urządzenia sieciowe i rozmaite systemy operacyjne posługują się **protokołami** — zbiorami reguł, jakich muszą przestrzegać pakiety krążące w sieci, by mogły być przyjęte, zrozumiane i przetworzone. Protokoły odpowiadają również za prawidłowe tworzenie pakietów.

W sieciach komputerowych istnieje wiele różnych zbiorów protokołów komunikacyjnych; jednym z nich jest TCP (*Transmission Control Protocol*). Inne znane protokoły to UDP (*User Datagram Protocol*), IPX i SPX (stosowany głównie w sieciach Novell Netware), NetBIOS oraz jego rozszerzenie NetBEUI (spotykane w sieciach Microsoft Windows).
W jednej sieci może działać wiele protokołów — o ile urządzenia sieciowe oparte o te protokoły potrafią „dogadać się" ze sobą, czyli wymienić dane.

Obecnie najbardziej rozpowszechnionym zbiorem protokołów jest **TCP/IP**, zaimplementowany w każdym liczącym się systemie operacyjnym.

Protokoły TCP i UDP

Cechą różniącą rodziny TCP i UDP jest **sposób dostarczania informacji** do celu. Protokół TCP posiada mechanizmy sprawdzania poprawności transmisji, obliczania sum kontrolnych pakietów oraz wykrywania i korekcji błędów. Stosuje się go w usługach, które muszą być **niezawodne**, np. w poczcie elektronicznej, protokole HTTP czy SSH.

Protokół UDP natomiast jest protokołem **bezpołączeniowym**, mającym bardzo ograniczoną kontrolę poprawności transmisji. Wymaga mniej „wysiłku" zarówno ze strony systemu źródłowego, jak i docelowego na stworzenie i przetworzenie pakietu. Ma zastosowanie w usługach, które mają mniejsze wymagania co do poprawności transmisji, np. przekaz dźwięku lub obrazu (usługi *Voice over IP*, strumienie wideo, połączenia telekonferencyjne) bądź nie mogą „pozwolić" sobie na zbędny narzut na kontrolę poprawności, np. DNS czy NFS (*Network File System*).

Porty protokołów

Porty są nierozłącznie związane z **protokołami**. Ich zadaniem jest identyfikacja procesów przypisanych do konkretnych usług działających na zdalnych systemach. Niektóre porty są uznawane za standardowe, inne można dowolnie zmieniać. Porty przyjmują wartości z zakresu 0...65535, a ich umowny podział jest następujący:

dobrze znane (systemowe, *well known*):	0-1023
zarezerwowane:	1024-49151
prywatne (dynamiczne):	49152-65535

Protokoły i porty TCP/IP

Przykłady

- FTP (*File Transfer Protocol*) — 20 i 21 (TCP)
- SSH (*Secure SHell*) — 22 (TCP)
- SMTP (*Simple Mail Transport Protocol*) — 22 (TCP)
- DNS (*Domain Name Service*) — 53 (UDP)
- TFTP (*Trivial File Transfer Protocol*) — 69 (UDP)
- HTTP (*Hyper Text Transfer Protocol*) — 80 i 8080 (TCP)
- POP3 (*Post Office Protocol*) — 110 (TCP)
- NNTP (*Network News Transfer Protocol*) — 119 (TCP)
- SNMP (*Simple Network Management Protocol*) — 161 (UDP)
- HTTPS (*HTTP over TLS/SSL*) — 443 (TCP)
- NFS (*Network File System*) — 2049 (UDP i TCP)

Nazwy domenowe vs. adresy IP

Urządzenia sieciowe komunikując się ze sobą posługują się adresami IP (ewentualnie adresami MAC). Dla człowieka łatwiejsze do zapamiętania są słowa, dlatego opracowano protokół tłumaczący tzw. **nazwy domenowe** na adresy IP. Protokół ten nosi nazwę **usługi nazw domenowych** (*Domain Name Service*, DNS).

DNS jest jednym z filarów Internetu. Jest to usługa rozproszona i hierarchiczna. Tzw. domeny najwyższego poziomu dzielą się na domeny niższych poziomów i tworzą strukturę drzewiastą. Przykłady „tradycyjnych" domen najwyższego poziomu: `com`, `edu`, `gov`, `net`, `org`. Szczególnym rodzajem domen najwyższego poziomu są **domeny narodowe**, np. `pl`, `ca`, `ru`, `br`.

Przyznawaniem nazw domenowych zajmuje się IANA i jej regionalne przedstawicielstwa, którzy z kolei udzielają odpowiednich uprawnień lokalnym dostawcom Internetu.

Przydatne adresy

- http://www.iana.org
- http://www.ieee.org
- http://www.nask.pl