Bezpieczeństwo
Sieci Komputerowych

Część 2.
Charakterystyka infrastruktury sieciowej oraz informatycznych technologii komunikacyjnych.

Praktyczny Pedagog

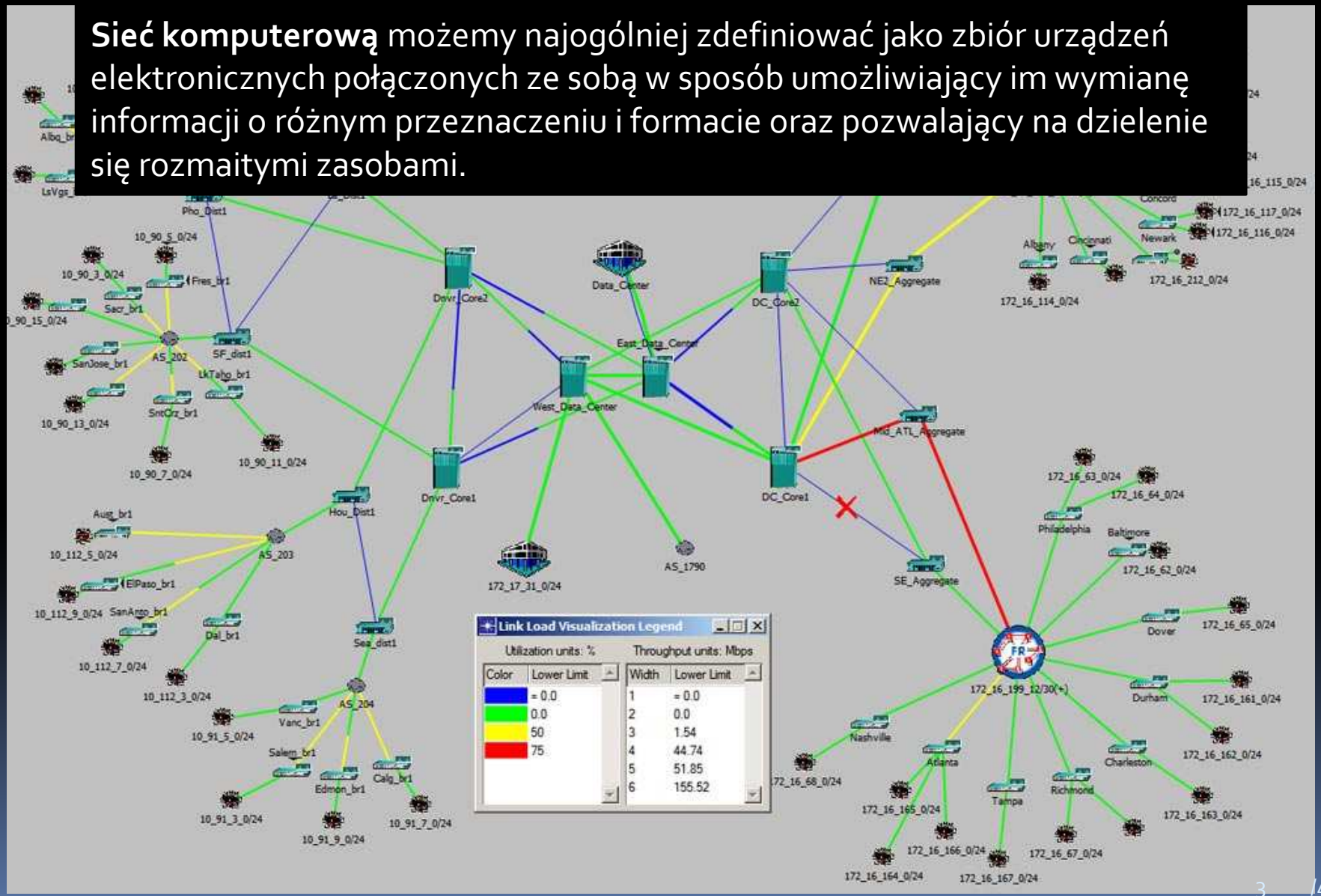
Bezpieczeństwo Sieci Komputerowych

PROGRAM ZAJĘĆ cz. 2

Definicja sieci komputerowej.
Pojęcia: serwer, klient, host, hosting.
Zasady budowy profesjonalnej serwerowni. Materiały filmowe – data center Onet oraz Google.
Podział sieci ze względu na zasięg.
Metodologia projektowania sieci LAN.
Model OSI oraz model internetowy.
Urządzenia sieciowe i ich producenci.
Aktywne elementy sieci: switch, router, punkt dostępowy.
Pasywne elementy sieci: media transmisyjne, gniazdko, końcówka, szafa, krosownica.
Topologia sieci.
Technologie budowy sieci.
Szczegóły sieci Ethernet.
Prawidłowe wykonanie łącza opartego na skrętce oraz złączu RJ45 w standardzie 100BASE-T568A

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.



Rodzaje usług sieciowych

Tradycyjnie wyróżnia się pięć rodzajów usług sieciowych:

- Współdzielenie drukarek
- Współdzielenie plików
- Pocztę elektroniczną
- Sieciowe bazy danych
- Aplikacji sieciowe

Host

Komputer podłączony do sieci komputerowej używającej protokołu komunikacyjnego TCP/IP, posiadający adres IP. Jeżeli użytkownik komputera łączy się z siecią komputerową, to karta sieciowa lub modem jego komputera otrzymuje adres IP i wtedy staje się hostem. W tym znaczeniu host jest dowolną maszyną, uczestniczącą w wymianie danych poprzez sieć komputerową, np. poprzez Internet. Host może być klientem i/lub serwerem.

Klient

Program komputerowy występujący w roli klienta wobec usług dostarczanych przez serwer.
W znaczeniu potocznym, mianem klienta określa się również komputer lub hosta, na którym działa program w roli klienta.

Serwer

Serwer - program świadczący usługi na rzecz innych programów, zazwyczaj korzystających z innych komputerów połączonych w sieć.
Serwerem nazywa się często komputer świadczący takie usługi, sprowadzające się zazwyczaj do udostępniania pewnych zasobów innym komputerom lub pośredniczący w przekazywaniu danych między komputerami.
Serwerem nazywa się też systemy oprogramowania biorące udział w udostępnianiu zasobów. Przykładami udostępnianych zasobów są pliki, bazy danych, łącza internetowe, a także urządzeń peryferyjnych jak drukarki i skanery.

Serwerem może być zwykły komputer, jednak w celu pełnego wykorzystania możliwości, jakie daje oprogramowanie serwerowe, powinna to być maszyna przeznaczona do tej roli. Maszyny takie są przystosowane do pracy ciągłej, wyposaża się je w duże i szybkie dyski twarde, głównie SCSI, dużą ilość pamięci RAM najczęściej z ECC oraz wydajne procesory serwerowe. Często serwerowe płyty główne mogą obsłużyć 2, 4 lub więcej procesorów.

Serwer

Serwer musi być maszyną niezawodną, w tym celu często posiada 2 lub więcej wbudowanych zasilaczy typu hot-plug i awaryjne zasilanie, a pomieszczenie, w którym stoi powinno posiadać odpowiednią wentylację lub klimatyzację. Dodatkowo niezawodność podnosi zastosowanie układu kontroli poprawnej pracy, tzw. watchdog, którego zadaniem jest przeprowadzenie restartu serwera w razie "zapętlenia się" programu.

Serwer jest zazwyczaj podłączony do Internetu szybkim łączem, które dzięki oprogramowaniu maskarady (NAT) potrafi dzielić pomiędzy aktualnie chcących korzystać z zasobów internetu użytkowników, których nazywa się klientami. Serwer niepodłączony do internetu, na przykład w sieci lokalnej może zarządzać współdzieleniem zasobów na poszczególnych komputerach (na przykład zainstalowanymi programami, danymi czy też urządzeniami peryferyjnymi).

Serwer

Serwery najczęściej pracują pod kontrolą systemów operacyjnych takich jak: FreeBSD, GNU/Linux, Solaris, Novell NetWare, Microsoft Windows Server 2003 lub 2008, Mac OS X Server. Oprogramowanie zainstalowane na komputerze, który pełni rolę serwera, zależne jest od jego funkcji.

Wśród wielu usług realizowanych przez serwery w internecie są między innymi: obsługa stron WWW, poczty elektronicznej, przesyłanie plików (np. FTP), komunikacja online czy strumieniowa transmisja audio i wideo oraz wiele innych. Przykładowo jeśli ma to być serwer WWW, wykorzystuje się najczęściej oprogramowanie Apache.

Klient-serwer

((ang.) client/server, client-server model) – architektura systemu komputerowego, w szczególności oprogramowania, umożliwiająca podział zadań (ról). Polega to na ustaleniu, że serwer zapewnia usługi dla klientów, zgłaszających do serwera żądania obsługi ((ang.) service request).

Podstawowe, najczęściej spotykane serwery działające w oparciu o architekturę klienet-serwer to: serwer poczty elektronicznej, serwer WWW, serwer plików, serwer aplikacji. Z usług jednego serwera może zazwyczaj korzystać wielu klientów. Jeden klient, w ogólności, może korzystać jednocześnie z usług wielu serwerów. Według schematu klient-serwer działa też większość, obecnie spotykanych, systemów zarządzania bazą danych.

P2P jest odmianą architektury klient-serwer, w której każdy host może pełnić jednocześnie rolę klienta i rolę serwera.

Hosting

Hosting to udostępnianie przez dostawcę usług internetowych zasobów serwerowni.
Innymi słowy, polega to na "zarezerwowaniu" (oddaniu do dyspozycji):

- określonej objętości dysku twardego (zazwyczaj na macierzy RAID),
- maksymalnej ilości danych do przesłania przez łącza internetowe serwerowni,
- usług obsługiwanych przez serwerownię (w zakresie zależnym od specyfiki usługi, np. udostępnienie bazy danych z określeniem maksymalnej jej objętości),
- maksymalnego stopnia obciążenia serwerowni przez usługi.

Własny serwer czy wynajęcie serwera dedykowanego?

Malejące ceny hostingu coraz częściej skłaniają do skorzystania z tej usługi, jeśli tylko istnieje taka możliwość (serwer nie musi znajdować się w siedzibie firmy). Dostawca hostingu z reguły zapewnia najwyższy poziom bezpieczeństwa i takie parametry, które ciężko osiągnąć w zwykłej serwerowni.
Z punktu widzenia dostawcy takich usług polega to głównie na dbaniu o stałe, poprawne działanie dysków i połączenie serwera z Internetem. Dobry dostawca powinien się zatem troszczyć o:

- dobry stan techniczny zarówno dysków jak i innych podzespołów koniecznych do prawidłowego funkcjonowania serwera,
- dobry stan techniczny połączenia z Internetem,
- ochronę danych dotyczących klientów i ich kont - zarówno przed przeciekami typu kserowanie dokumentów z biurka jak i kradzieżami elektronicznymi,
- ochronę serwerów oraz znajdujących się na nich kont przed różnego typu atakami poprzez Internet,
- maksymalnie pełną, szybką i stałą dostępność do przechowywanych zasobów przez Internet.

Serwerownia

Serwerownia to wydzielone pomieszczenie będące środowiskiem pracy komputerów pełniących rolę serwerów, a także aktywnych i pasywnych elementów sieci komputerowych. Urządzenia te są umieszczane najczęściej w szafach stelażowych (rackowych) wewnątrz serwerowni.

Serwerownia

Serwerownia posiada specyficzny mikroklimat. W pomieszczeniu dla poprawnej pracy urządzeń powinna być zachowana odpowiednia wilgotność (45%) i temperatura powietrza (20 °C). Profesjonalne serwerownie posiadają czujniki ww. parametrów i automatycznie regulują zmiany mikroklimatu.

W celu utrzymania ciągłości pracy urządzeń stosuje się dwa (lub więcej) źródła zasilania serwerowni oraz systemy zasilania awaryjnego UPS.

W przypadku serwerów internetowych, stosuje się także kilka łączy do różnych dostawców internetu, w celu zapewnienia widoczności serwerów nawet podczas awarii jednego z łącz.

7 zasad budowy własnej serwerowni*

1. Zasilanie
- Wydajny UPS (koszt od 1500 zł)
- Generator prądu (jeśli występują częste przerwy)
- Wytrzymały zasilacz (koszt od 300 zł)

* Test Fornalskiego dla serwerowni za stroną http://fornalski.blox.pl

7 zasad budowy własnej serwerowni

2. Archiwizacja
- Sprzętowy kontroler RAID1 + kieszenie hot-swap na dyski
- Wytrzymałe i wydajne dyski dedykowane do serwerów

7 zasad budowy własnej serwerowni

3. Ochrona
- Alarm
- Całodobowa ochrona
- Kopie zapasowe w innej lokalizacji

7 zasad budowy własnej serwerowni

4. Łącza
- Wydajne łącze szerokopasmowe
- Internet od dwóch dostawców
- Router przełączający na łącze zapasowe w razie awarii

7 zasad budowy własnej serwerowni

5. System przeciwpożarowy
- Gaśnice
- System gaśniczy oparty na gazach niepalnych
- Hermetyczne pomieszczenie
- Automatyczne wykrywanie pożaru

7 zasad budowy własnej serwerowni

6. Wentylacja
- Dobry przepływ powietrza i wentylatory
- Nienasłonecznione pomieszczenie
- Klimatyzacja odpowiedniej wydajności (dodatkowo eliminacja kurzu)

7 zasad budowy własnej serwerowni

7. Urządzenia zdalnego dostępu
- KVM i RR (Keyboard Video Mouse, Remote Reset) - urządzenia umożliwiające zdalny dostęp do konsoli, pozwalające na zarządzanie zdalne komputerem (koszt od 2000 zł).

Data Center – fabryka danych

Google Data Center (ang. napisy)
http://www.youtube.com/watch?v=zRwPSFpLX8I&cc=1

Onet Data Center
http://www.youtube.com/watch?v=bWEfO6KbH84

Zasięg sieci

Jednym z kryteriów 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)

Metodologia projektowania sieci LAN*

Aby sieci LAN były wydajne i spełniały potrzeby użytkowników, powinny być projektowane i implementowane w oparciu o zaplanowane sekwencje czynności:

- zebranie wymagań i oczekiwań;
- analiza wymagań i danych;
- zaprojektowanie struktury lub topologii sieci LAN w warstwach 1, 2 i 3;
- dokumentacja logicznej i fizycznej implementacji sieci LAN.

Proces zbierania informacji pomaga wyjaśnić i rozpoznać problemy aktualnie występujące w sieci. Informacje te obejmują historię organizacji, jej aktualny stan, przewidywany wzrost, reguły działania i procedury zarządzania, procedury i systemy stosowane w pracy biurowej oraz opinie ludzi, którzy mają korzystać z tej sieci LAN.

*http://www.rogaski.org/cisco/sem3/switches.html

Metodologia projektowania sieci LAN

Podczas zbierania informacji należy sobie zadać następujące pytania:

Kim są ludzie, którzy będą korzystali z sieci?
Jaki jest poziom umiejętności tych osób?
Jaki jest ich stosunek do komputerów i aplikacji komputerowych?
Jak zaawansowane są udokumentowane regulaminy organizacji?
Czy niektóre dane zostały określone jako newralgiczne dla działania firmy?
Czy niektóre operacje zostały określone jako newralgiczne dla działania firmy?
Jakie protokoły są dozwolone w sieci?
Czy tylko niektóre typy komputerów stacjonarnych są obsługiwane?
Kto jest odpowiedzialny za adresy LAN, nazewnictwo, projektowanie topologii i konfigurację?
Jakimi zasobami ludzkimi, sprzętowymi i programowymi dysponuje organizacja?
W jaki sposób teraz są te zasoby połączone i współdzielone?
Jakimi zasobami finansowymi dysponuje organizacja?

Metodologia projektowania sieci LAN

Dokumentacja wymagań umożliwia oszacowanie kosztów i ustalenie harmonogramu wdrożenia projektowanej sieci LAN w oparciu o fakty. Ważne jest zrozumienie zagadnień dotyczących wydajności wszystkich sieci.
Projekty sieci powinny zapewniać jak największą dostępność przy jak najniższych kosztach.

Metodologia projektowania sieci LAN

Projekt sieci LAN zależy od wymagań danej organizacji, ale zwykle koncentruje się na zapewnieniu funkcjonalności, skalowalności, możliwości zarządzania i możliwości adaptacji. Aby sieć LAN mogła być wydajna, jej projektowanie i implementacja powinny przebiegać w oparciu o zaplanowane sekwencje czynności. Czynności te obejmują zbieranie i analizowanie danych, implementowanie warstw 1, 2 i 3 oraz sporządzenie pełnej dokumentacji. Najważniejsze elementy dokumentacji projektu sieci LAN to:

- mapa topologii warstw OSI,
- mapa logiczna sieci LAN,
- mapa fizyczna sieci LAN,
- logiczny plan okablowania,
- logiczna mapa sieci VLAN,
- logiczna mapa warstwy 3,
- mapy adresów

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 warstw.** Działanie warstw wyższych jest zależne od warstw leżących niżej:

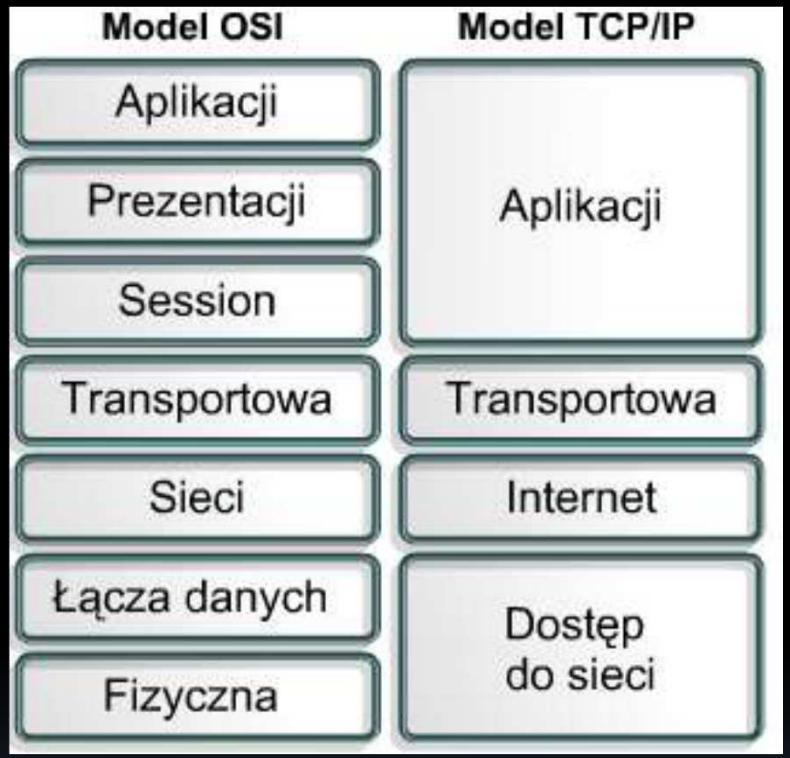
Model OSI jest **modelem odniesienia** dla innych modeli sieciowych. Dla każdej z warstw zdefiniowane są protokoły komunikacji z innymi warstwami. Model OSI definiuje swego rodzaju **protokół określający sposób porozumiewania się protokołów sieciowych**.

Model internetowy

Model internetowy, znany również jako model TCP/IP, to uproszczona wersja modelu OSI.
Posiada cztery warstwy:

- aplikacji
- transportu
- sieci
- dostępu do sieci

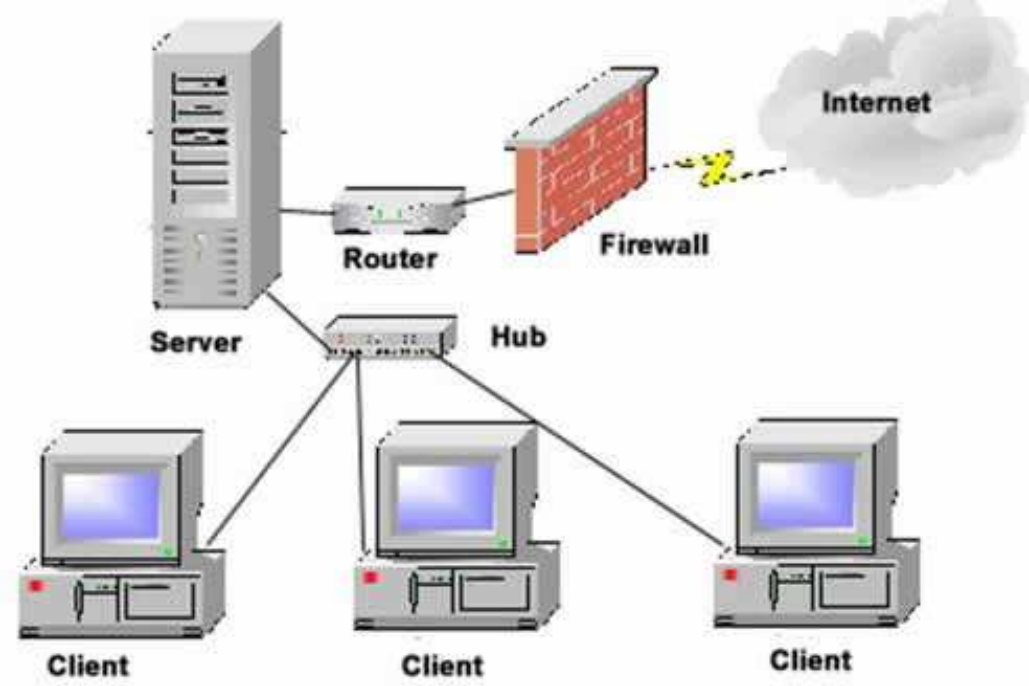
Protokół TCP/IP jest standardem, wokół którego powstał Internet.



Urządzenia sieciowe

Przykłady urządzeń sieciowych:

- komputer osobisty, laptop, smartfon
- serwer
- drukarka, skaner
- aktywne i pasywne elementy sieci



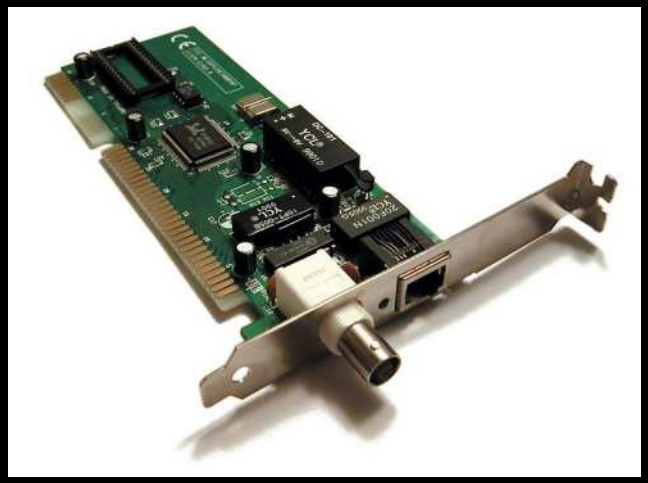
Aktywne elementy sieci

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

Aktywne elementy sieci

Karta sieciowa



(ang. NIC – Network Interface Card) – karta rozszerzenia, która służy do przekształcania pakietów danych w sygnały, które są przesyłane w sieci komputerowej. Karty NIC pracują w określonym standardzie, np. Ethernet, Token Ring, FDDI, ArcNet, 100VGAnylan.

Jeżeli chodzi o typy interfejsów kart sieciowych to dzielą się one na PCI , PCMCIA i USB. Te ostatnie są coraz powszechniej stosowane.

Aktywne elementy sieci

Przełącznik (switch)

Urządzenie sieciowe drugiej warstwy modelu OSI (łacza danych).

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).

Aktywne elementy sieci

Punkt dostępowy (access point)

Urządzenie zapewniające stacjom bezprzewodowym dostęp do zasobów sieci za pomocą bezprzewodowego medium transmisyjnego (częstotliwości radiowe).

Punkt dostępowy jest także mostem łączącym sieć bezprzewodową z siecią przewodową (najczęściej Ethernet). W związku z tym każdy punkt dostępowy ma minimum dwa interfejsy: interfejs bezprzewodowy komunikujący się z sieciami standardu 802.11 oraz drugi służący połączeniu PD z siecią przewodową. Stacjami łączonymi w sieć bezprzewodową za pomocą punktów dostępowych są komputery wyposażone w bezprzewodowe karty sieciowe.

Aktywne elementy sieci

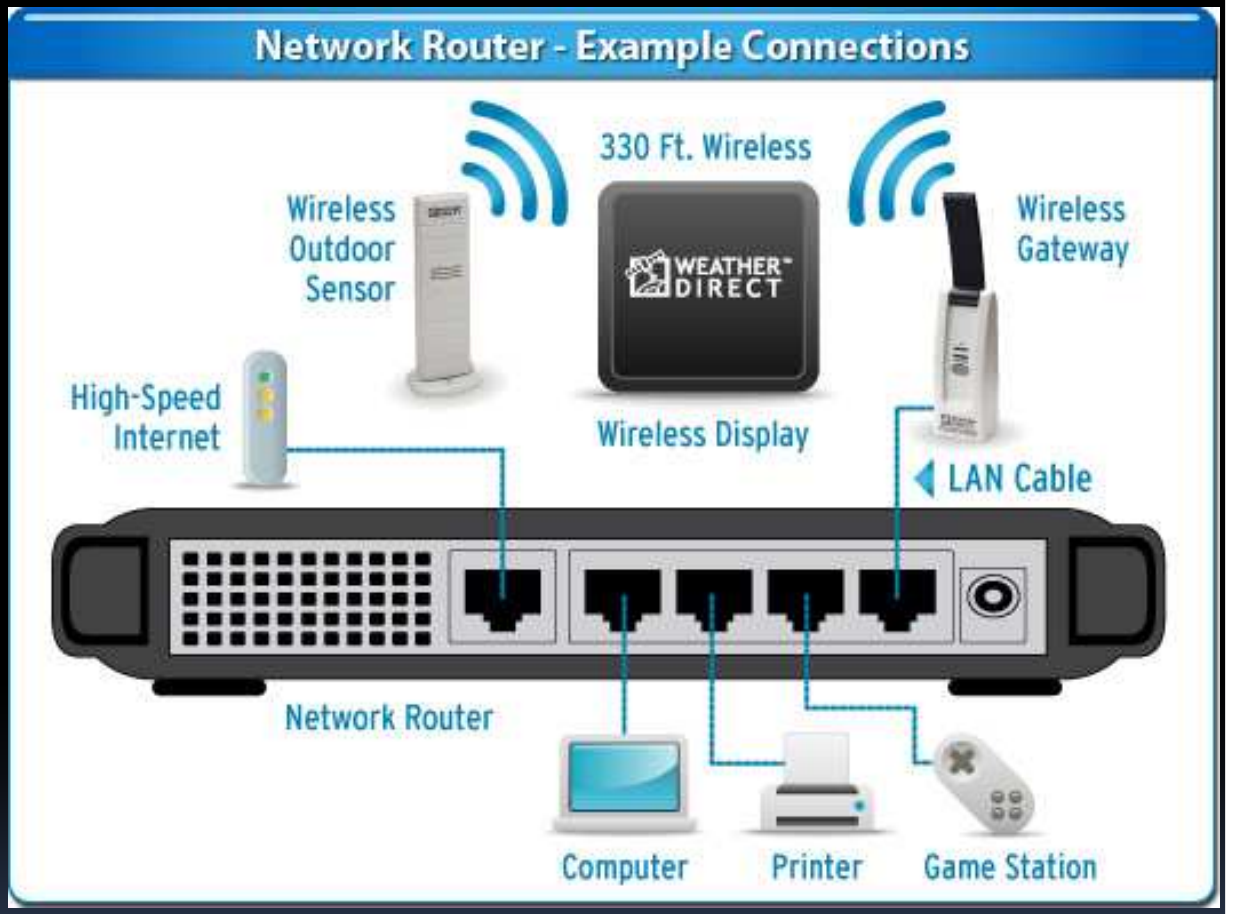
Punkt dostępowy (access point)

Dodatkowo większość produkowanych aktualnie punktów dostępowych wyposażonych jest również w wbudowany router, który umożliwia tworzenie sieci mieszanych (sieć wykorzystująca więcej niż jedną technologię sieciową np. sieć bezprzewodowa i Ethernet). Podstawową funkcją PD jest konwersja ramek sieci bezprzewodowej na inny rodzaj ramek (zazwyczaj ramki Ethernetu).

Aktywne elementy sieci

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 tablice *routingu.*



W sieci Ethernet *router* może dzielić sieć lokalna na wiele tzw. wirtualnych LAN (*Virtual LAN*, VLAN) — podsieci wydzielonych logicznie na jednym fizycznym interfejsie sieciowym.

Koncentrator (hub)

Urządzenie sieciowe pierwszej warstwy modelu OSI (fizycznej).
Zadaniem *huba* jest wzmacnianie i kopiowanie (powielanie) sygnałów w sieci lokalnej oraz przekazywanie ich do wszystkich urządzeń sieciowych podłączonych do *huba.*
Opóźnienia w przekazywaniu pakietów wprowadzane przez *hub* są mniejsze niż w przypadku *routera* i *switcha.*

Pasywne elementy sieci

Pasywnymi elementami sieci są głównie 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*)
- swiatłowód (*fiber optic cable*)
- fale radiowe i podczerwień

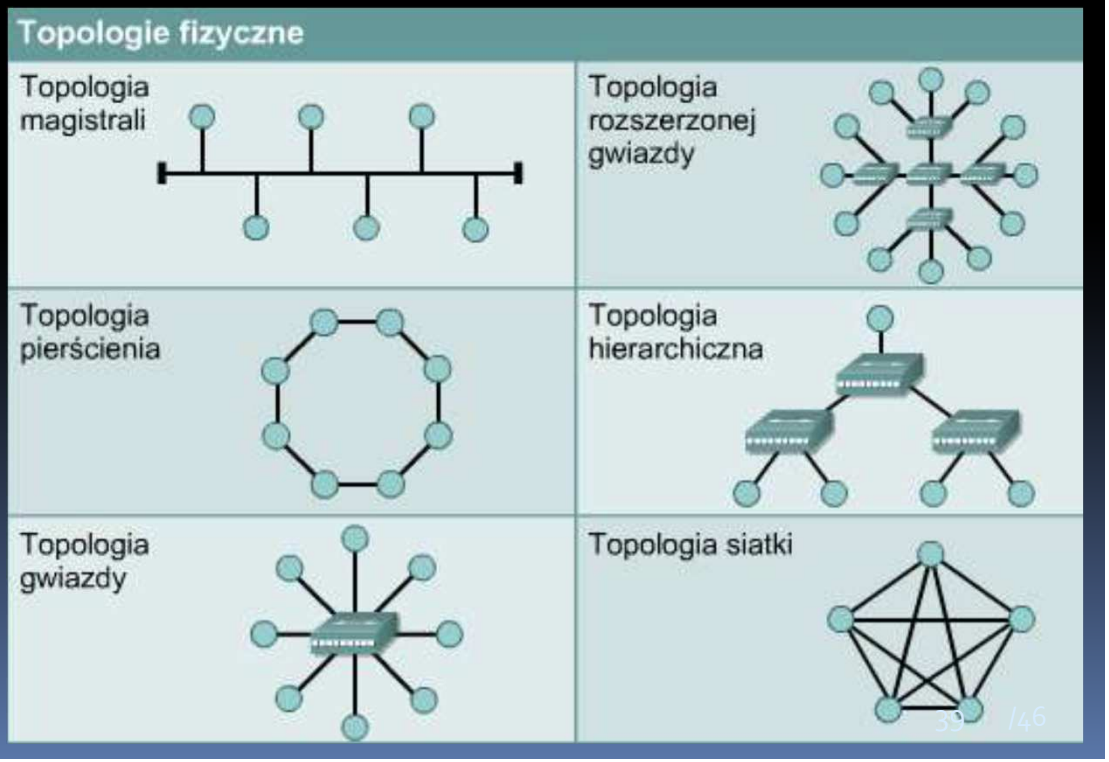
Oraz pozostałe urządzenia:

- przełącznice, krosownice
- gniazdka, szafy

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*)



Topologie sieci bezprzewodowych

W przypadku lokalnych sieci bezprzewodowych (*Wireless Local Area Network*, *WLAN*) nazewnictwo jest inne niż LAN. 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 miedzy urządzeniami.

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*) — oparta na technologii światłowodowej, złożona z dwóch pierścieni (pierwotnego i wtórnego)

Frame Relay — łączy odległe od siebie sieci LAN lub pojedyncze 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 zajęć 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 specyfikacje mediów transmisyjnych, format pakietów (ramek) oraz sposób uzyskiwania dostępu do medium transmisyjnego.

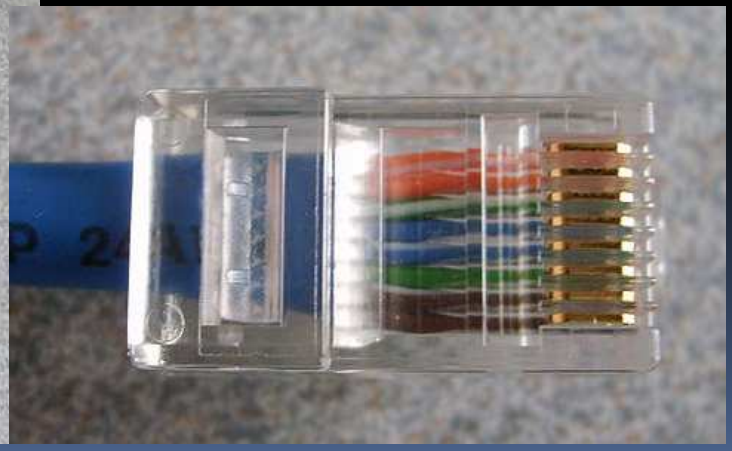
Najpopularniejszym standardem w sieciach LAN obecnie jest 100BASE-TX (100Base-TX) – jedna z technologii należących do standardu Ethernet, pozwalająca na komunikowanie się urządzeń w sieciach lokalnych z szybkością 100 Mb/s, zwana też Fast Ethernet.

Ethernet

Specyfikę technologii można wyczytać z jej nazwy, gdyż przedrostek 100 oznacza szybkość transmisji podana w Mb na sekundę, „Base" oznacza transmisję cyfrową czyli w paśmie podstawowym (w odróżnieniu od „Broad" – transmisji analogowej czyli szerokopasmowej), a oznaczenie TX oznacza skrętkę miedzianą kategorii 5e lub wyższej. Istnieją technologie wykorzystujące skrętkę o niższej kategorii, w takim przypadku oznaczane są T co oznacza po prostu skrętkę miedzianą.

Ethernet

Medium transmisyjnym jest na ogół miedziana skrętka nieekranowana UTP lub FTP kategorii 5 lub 6, zakończona obustronnie złączem RJ-45.

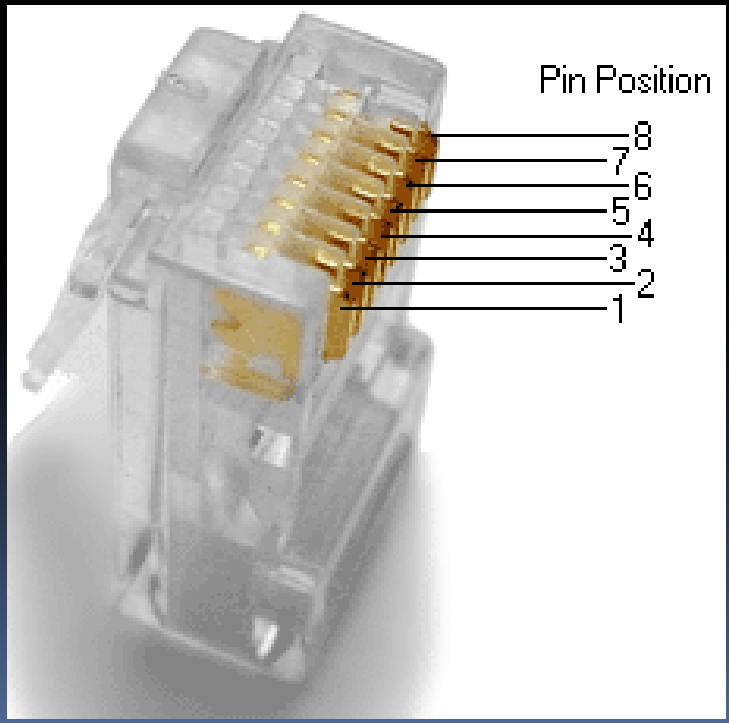


Ethernet

Zaciskarka do wtyków:

Specyfikacja kablowania końcówek RJ-45 (100BASE-T568A)

Pin	Para	Kabel	Kolor
1	3	1	biało-zielony
2	3	2	zielony
3	2	1	biało-pomarańczowy
4	1	2	niebieski
5	1	1	biało-niebieski
6	2	2	pomarańczowy
7	4	1	biało-brązowy
8	4	2	brązowy



Koniec cz. 2