

informatyka+

Wszechnica Poranna: Sieci komputerowe

Podstawy budowy i działania
sieci komputerowych

Dariusz Chaładyniak, Józef Wacnik

Człowiek – najlepsza inwestycja



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI



WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Rodzaj zajęć: Wszelchnica Poranna

Tytuł: Podstawy budowy i działania sieci komputerowych

Autor: dr inż. Dariusz Chaładyniak, mgr inż. Józef Wacnik

Redaktor merytoryczny: prof. dr hab. Maciej M Sysło

Zeszyt dydaktyczny opracowany w ramach projektu edukacyjnego **Informatyka+**
– ponadregionalny program rozwijania kompetencji uczniów szkół ponadgimnazjalnych w
zakresie technologii informacyjno-komunikacyjnych (ICT).

www.informatykaplus.edu.pl

kontakt@informatykaplus.edu.pl

Wydawca: Warszawska Wyższa Szkoła Informatyki

ul. Lewartowskiego 17, 00-169 Warszawa

www.wysi.edu.pl

rektorat@wysi.edu.pl

Projekt graficzny: FRYCZ I WICHA

Warszawa 2009

Copyright © Warszawska Wyższa Szkoła Informatyki 2009

Publikacja nie jest przeznaczona do sprzedaży.



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI



WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Podstawy budowy i działania sieci komputerowych

Dariusz Chaładyniak

Warszawska Wyższa Szkoła Informatyki
dchalad@wwsi.edu.pl

Józef Wacnik

Warszawska Wyższa Szkoła Informatyki
j_wacnik@poczta.wwsi.edu.pl



Streszczenie

Wykład dostarcza podstawowych informacji, niezbędnych do zrozumienia architektury i działania sieci komputerowych. Przedstawia typowe role klientów (użytkowników komputerów) oraz serwerów w sieciach komputerowych. Prezentuje zasięgi sieci komputerowych (LAN, MAN, WAN). Wyjaśnia budowę podstawowych modeli sieciowych (ISO/OSI, TCP/IP) i przeznaczenie ich poszczególnych warstw. Przedstawia podstawowe aktywne urządzenia sieciowe i ich zastosowanie przy budowie sieci komputerowych (karty sieciowe, koncentratory, przełączniki, mosty, routery). Omawia ponadto najczęściej spotykane topologie sieciowe (magistrala, gwiazda, pierścień, siatka).

Warsztaty obejmują następujące zagadnienia: poznanie elementów sieci komputerowej (urządzeń, mediów, usług), łączenie elementów infrastruktury teleinformatycznej w sieć komputerową, korzystanie z usług sieciowych, rozwiązywanie podstawowych problemów sieciowych

Spis treści

Wykład

1. Role komputerów w sieci	3
2. Typ i zasięg sieci	4
3. Modele sieciowe	5
4. Urządzenia sieciowe	8
5. Topologie sieciowe	11

Literatura	13
------------	----

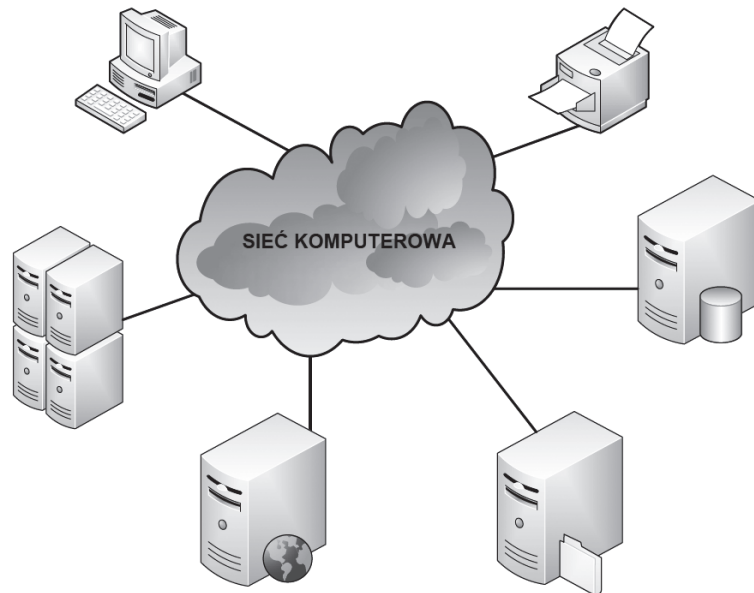
Warsztaty

1. Elementy sieci komputerowej	13
2. Usługi	14
3. Łączenie elementów infrastruktury teleinformatycznej w sieć komputerową	15
4. Korzystanie z usług sieciowych	15
5. Analiza działania sieci komputerowej	15



1 ROLA KOMPUTERÓW W SIECI

Co to jest sieć komputerowa



Rysunek 1.
Przykład sieci komputerowej

Siecią komputerową nazywamy zespół połączonych ze sobą komputerów, terminali, serwerów, drukarek za pomocą mediów transmisyjnych. Komunikacja w sieci jest możliwa dzięki odpowiednim protokołom.

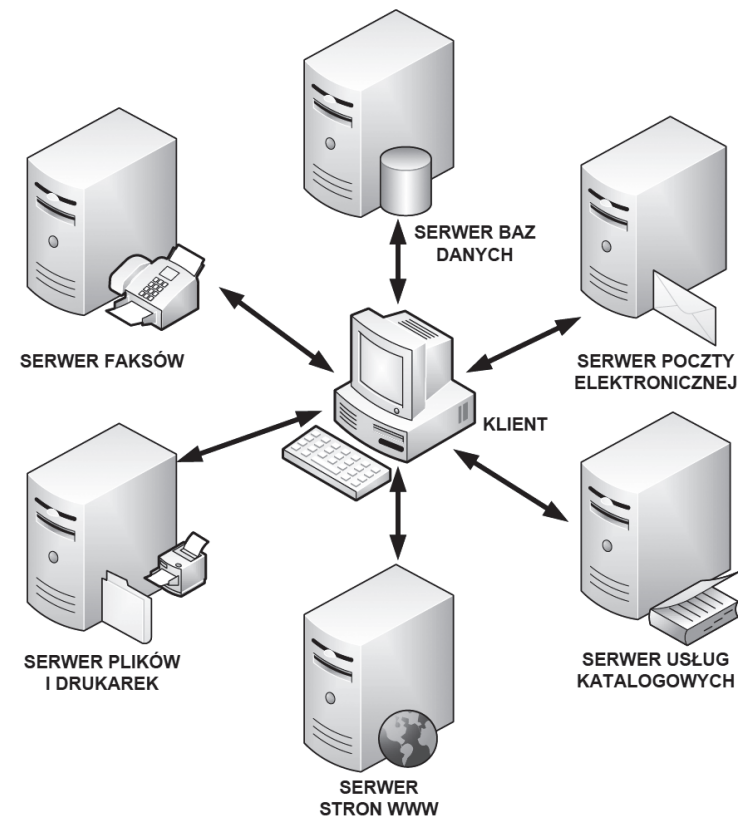
Co umożliwia praca w sieci komputerowej

Praca w sieci komputerowej umożliwia:

- scentralizowanie administracji – z jednego (dowolnego) komputera w sieci można zarządzać i administrować wszystkimi urządzeniami połączonymi w sieć;
- udostępnianie danych – na serwerach bazodanowych, znajdujących się w sieci można udostępniać informacje każdemu uprawnionemu użytkownikowi sieci;

- udostępnianie sprzętu i oprogramowania – użytkownikom sieci można udostępniać sprzęt komputerowy (drukarki, faksy, skanery, plotery, modemy itp.) przyłączony do sieci oraz oprogramowanie (edytory tekstu, arkusze kalkulacyjne, bazy danych, specjalizowane aplikacje itp.) znajdujące się w komputerach w sieci.

Jaką rolę pełnią komputery w sieci



Rysunek 2.
Przykładowe role komputerów w sieci

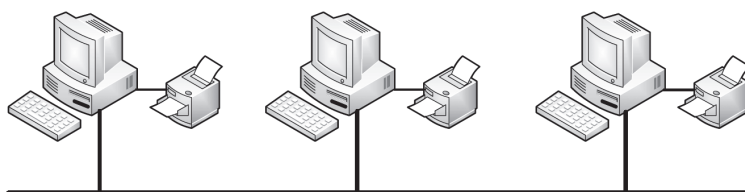


Jak pokazano na rys. 2, komputery połączone w sieć mogą pełnić następujące role:

- serwer baz danych – do udostępniania dowolnych danych;
- serwer poczty elektronicznej – do przechowywania i zarządzania pocztą elektroniczną przychodzącą i wychodzącą z serwera;
- serwer usług katalogowych – do optymalnego zarządzania zasobami firmy;
- serwer stron WWW – do obsługi zasobów „globalnej pajęczyny”, przeglądarek, wyszukiwarek;
- serwer plików i drukarek – do udostępniania dowolnych plików (na określonych zasadach) i drukarek;
- serwer faksów – do zarządzania i obsługi faksami;
- klient – użytkownik komputera w sieci.

2 TYP I ZASIĘG SIECI

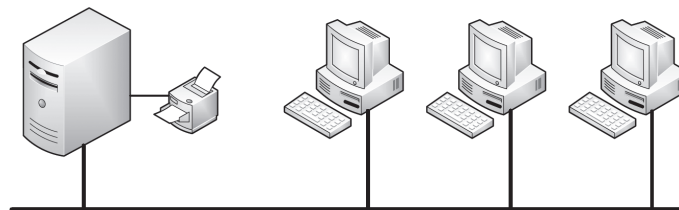
Sieć typu peer-to-peer (równorzędna)



Rysunek 3.
Sieć równorzędna

Na rys. 3 jest przedstawiona sieć typu **peer-to-peer** (p2p – równorzędna, partnerska). Jest to przykład rozwiązania bez wydzielonego urządzenia zarządzającego (serwera). Wszystkie podłączone do sieci urządzenia są traktowane jednakowo. Do zalet tego typu sieci należą: niski koszt wdrożenia, nie jest wymagane oprogramowanie do monitorowania i zarządzania, nie jest wymagane stanowisko administratora sieciowego. Natomiast wadami tego rozwiązania są: mniejsza skalowalność rozwiązania, niższy poziom bezpieczeństwa, i to, że każdy z użytkowników pełni rolę administratora.

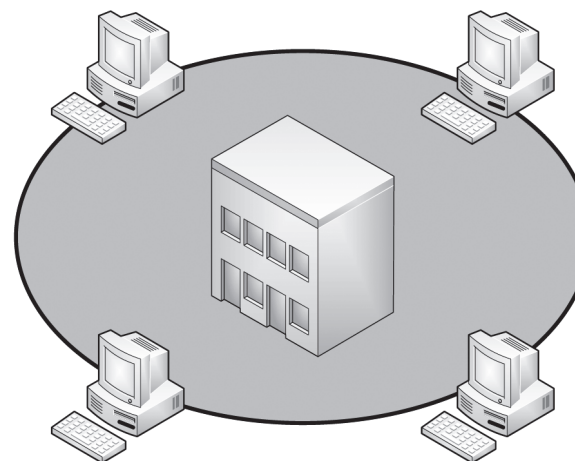
Sieć typu klient-serwer



Rysunek 4.
Sieć typu klient-serwer

Sieć typu **klient-serwer** jest rozwiązaniem z wydzielonym serwerem zarządzającym. Komputery użytkowników są administrowane, monitorowane i zarządzane centralnie. Do zalet tego typu sieci należą: zdecydowanie wyższy poziom bezpieczeństwa, łatwiejsze zarządzanie i utrzymanie, prostsze i wygodniejsze tworzenie kopii zapasowych. Natomiast wadami tego rozwiązania są: wymów specjalistycznego oprogramowanie do monitorowania, administrowania i zarządzania, wyższy koszt urządzeń sieciowych, obecność wyszkolonego personelu administracyjnego.

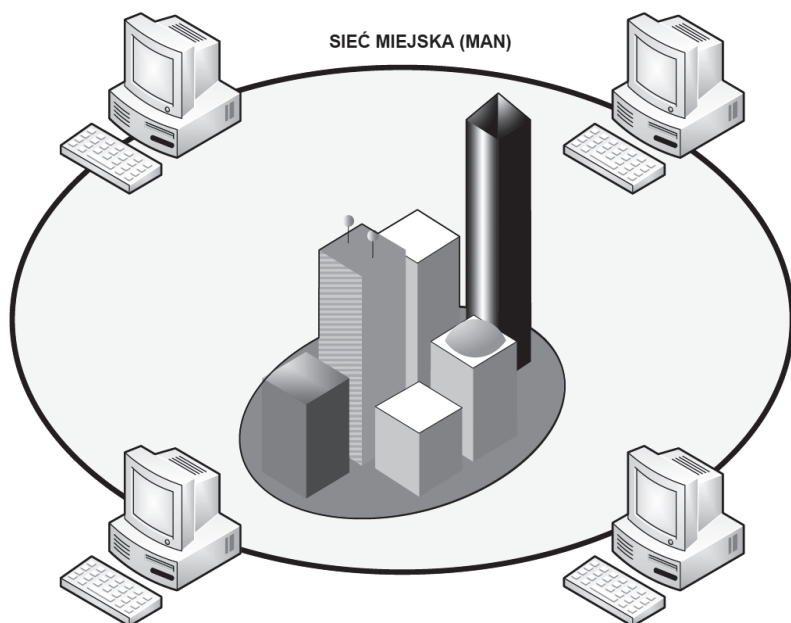
Zasięg sieci komputerowych Sieć LAN



Rysunek 5.
Lokalna sieć komputerowa (LAN)

Sieć lokalna LAN (ang. *Local Area Network*) obejmuje stosunkowo niewielki obszar i zwykle łączy urządzenia sieciowe w ramach jednego domu, biura, budynku.

Sieć MAN

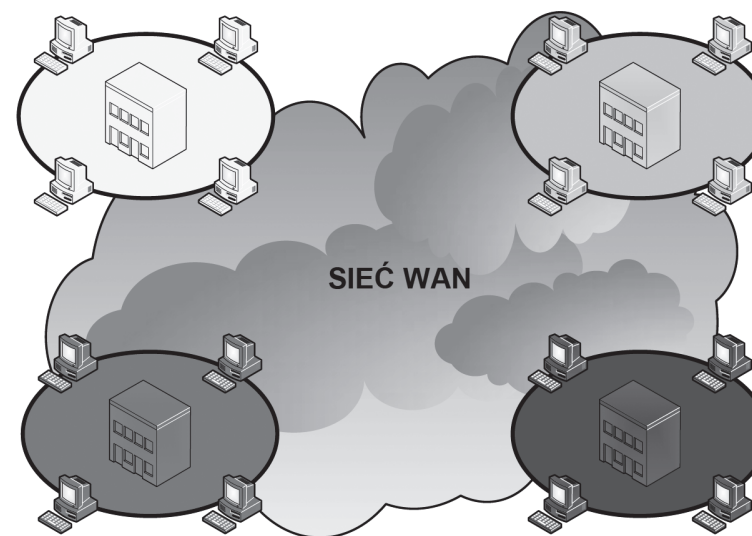


Rysunek 6.
Miejska sieć komputerowa (MAN)

Sieć miejska MAN (ang. *Metropolitan Area Network*) jest siecią, która łączy sieci LAN i urządzenia komputerowe w obrębie danego miasta. Zasięg tej sieci zawiera się zwykle w przedziale od kilku do kilkudziesięciu kilometrów.

Sieć WAN

Sieć rozległa WAN (ang. *Wide Area Network*) jest siecią o zasięgu globalnym. Łączy ona sieci w obrębie dużych obszarów, obejmujących miasta, kraje a nawet kontynenty.



Rysunek 7.
Rozległa sieć komputerowa (WAN)

3 MODELE SIECIOWE

Model odniesienia ISO/OSI

Model odniesienia ISO/OSI (ang. *The International Organization for Standardization/Open Systems Interconnection*) został opracowany, aby określić wymianę informacji pomiędzy połączonymi w sieć komputerami różnych typów. Składa się on z siedmiu warstw.

1. **Warstwa fizyczna** (ang. *physical layer*) – definiuje elektryczne, mechaniczne, proceduralne i funkcjonalne mechanizmy aktywowania, utrzymywania i dezaktywacji fizycznego połączenia pomiędzy urządzeniami sieciowymi. Warstwa ta jest odpowiedzialna za przenoszenie elementarnych danych (bitów) za pomocą sygnałów elektrycznych, optycznych lub radiowych.
2. **Warstwa łączy danych** (ang. *data link layer*) – zapewnia niezawodne przesyłanie danych po fizycznym medium transmisyjnym. Warstwa to jest





Rysunek 8. Referencyjny model odniesienia ISO/OSI

odpowiedzialna za adresowanie fizyczne (sprzętowe), dostęp do łącza, informowanie o błędach i kontrolę przepływu danych.

3. **Warstwa sieci** (ang. *network layer*) – zapewnia łączność i wybór optymalnych ścieżek między dwoma dowolnymi hostami, znajdującymi się w różnych sieciach. Do podstawowych funkcji tej warstwy należy: adresowanie logiczne oraz wybór najlepszych tras dla pakietów.

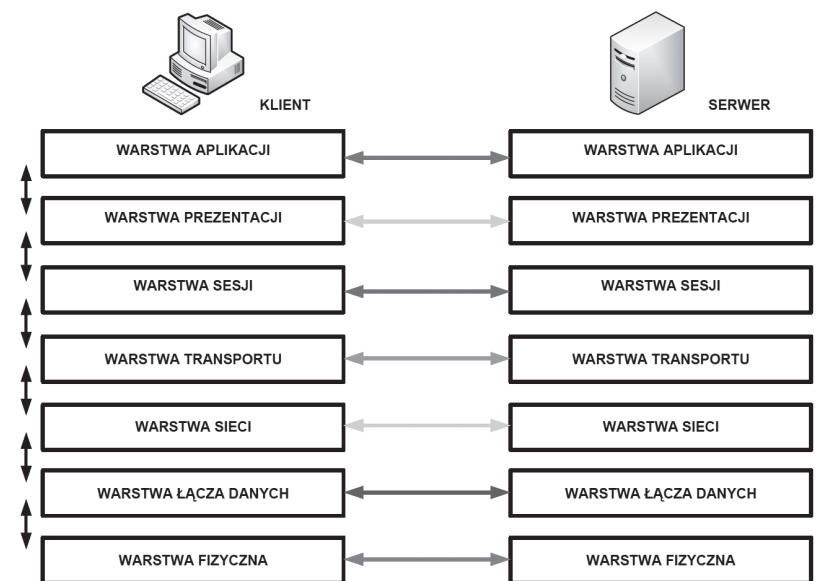
4. **Warstwa transportu** (ang. *transport layer*) – odpowiedzialna jest za ustanowienie niezawodnego połączenia i przesyłania danych pomiędzy dwoma hostami. Dla zapewnienia niezawodności świadczonych usług, w tej warstwie sa wykrywane i usuwane błędy a także jest kontrolowany przepływ informacji.

5. **Warstwa sesji** (ang. *session layer*) – ustanawia, zarządza i zamyka sesje pomiędzy dwoma porozumiewającymi się ze sobą hostami. Ponadto warstwa ta synchronizuje komunikację pomiędzy połączonymi hostami i zarządza wymianą danych między nimi.

6. **Warstwa prezentacji** (ang. *presentation layer*) – odpowiedzialna jest za właściwą reprezentację i interpretację danych. Warstwa ta zapewnia, że informacje przesłane przez warstwę aplikacji jednego systemu będą czytelne dla warstwy aplikacji drugiego systemu.

7. **Warstwa aplikacji** (ang. *application layer*) – świadczy usługi sieciowe dla programów użytkowych (przeglądarek internetowych, wyszukiwarek, programów pocztowych itp.).

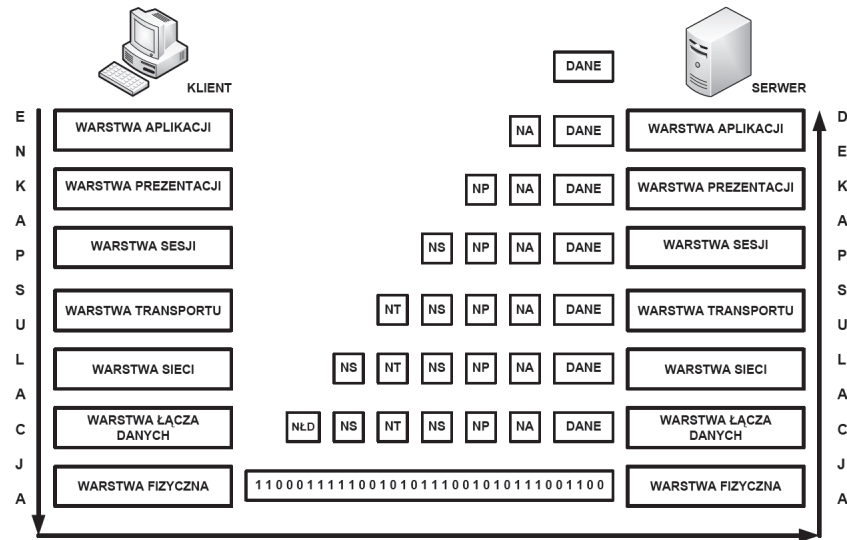
Współpraca warstw w modelu ISO/OSI



Rysunek 9. Przykład współpracy kolejnych warstw w modelu ISO/OSI

Warstwy w modelu odniesienia ISO/OSI współpracują ze sobą zarówno w pionie jak i w poziomie. Na przykład warstwa transportu klienta współpracuje z warstwami sesji i sieci klienta a także warstwą transportu serwera.

Enkapsulacja (dekapsulacja) danych



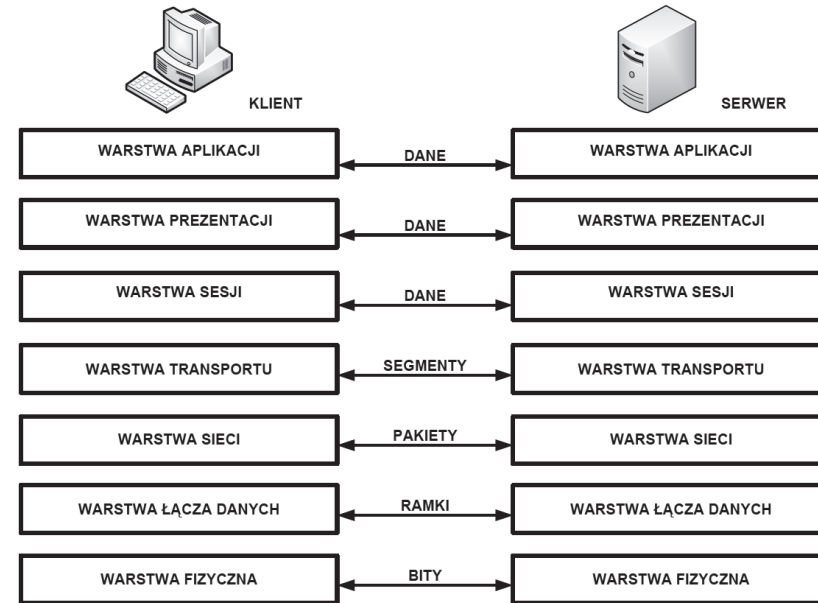
Rysunek 10.

Proces enkapsulacji i dekapulacji danych

Enkapsulacja (dekapsulacja) danych jest procesem zachodzącym w kolejnych warstwach modelu ISO/OSI. Proces enkapsulacji oznacza dokładanie dodatkowej informacji (**nagłówek**) związanej z działającym protokołem danej warstwy i przekazywaniu tej informacji warstwie niższej do kolejnego procesu enkapsulacji. Proces **dekapsulacji** polega na zdejmowaniu dodatkowej informacji w kolejnych warstwach modelu ISO/OSI.

Dane, segmenty, pakiety, ramki, bity

W poszczególnych warstwach w modelu odniesienia ISO/OSI przechodzące dane noszą nazwę jednostek danych protokołu PDU (ang. *Protocol Data Unit*).



Rysunek 11.

Jednostki informacji w poszczególnych warstwach w modelu odniesienia ISO/OSI

Jednostki te mają różne nazwy w zależności od protokołu. I tak w trzech górnych warstwach mamy do czynienia ze **strumieniem danych**, w warstwie transportu są **segmenty**, w warstwie sieci są **pakiety**, w warstwie łącza danych – **ramki**, a w warstwie fizycznej – **bity** (zera i jedyneki). Jednostki te w poszczególnych warstwach różnią się częścią nagłówkową.

Model TCP/IP

Historycznie starszym modelem sieciowym jest **model TCP/IP** (ang. *Transmission Control Protocol/Internet Protocol*). Działanie sieci Internet opiera się właśnie na tym modelu sieciowym (patrz rys. 12). Opracowano go w połowie lat siedemdziesiątych XX wieku w amerykańskiej agencji DARPA (ang. *Defense Advanced Research Projects Agency*). Model TCP/IP składa się z czterech warstw.





Rysunek 12. Model sieciowy TCP/IP

1. **Warstwa dostępu do sieci** (ang. *network access layer*) – określa właściwe procedury transmisji danych w sieci, w tym dostęp do medium transmisyjnego (Ethernet, Token Ring, FDDI).
2. **Warstwa internetu** (ang. *internet layer*) – odpowiada za adresowanie logiczne i transmisję danych, a także za fragmentację i składanie pakietów w całość.
3. **Warstwa transportu** (ang. *transport layer*) – odpowiada za dostarczanie danych, inicjowanie sesji, kontrolę błędów i sprawdzanie kolejności segmentów.
4. **Warstwa aplikacji** (ang. *application layer*) – obejmuje trzy górne warstwy modelu odniesienia ISO/OSI realizując ich zadania.

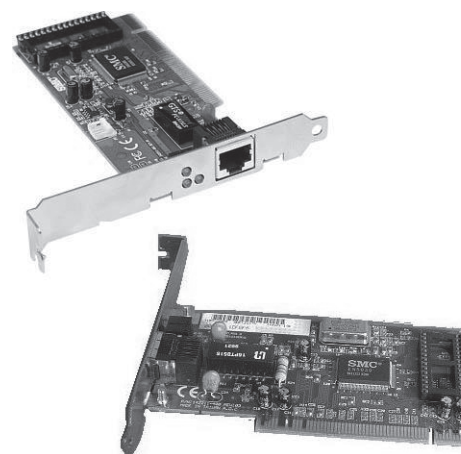
Porównanie modelu ISO/OSI i TCP/IP

Model ISO/OSI i model TCP/IP pomimo, że mają różną liczbę warstw i zostały opracowane w różnych czasach i przez inne organizacje wykazują wiele podobieństw w funkcjonowaniu. Dwie dolne warstwy w modelu ISO/OSI pokrywają się z najniższą warstwą w modelu TCP/IP. Warstwa sieci w modelu ISO/OSI funkcjonalnie odpowiada warstwie Internetu w modelu TCP/IP. Warstwy trans-

portowe występują w obu modelach i spełniają podobne zadania. Z kolei trzy górne warstwy w modelu odniesienia ISO/OSI pokrywają się z najwyższą warstwą w modelu TCP/IP.

4 URZĄDZENIA SIECIOWE

Karta sieciowa



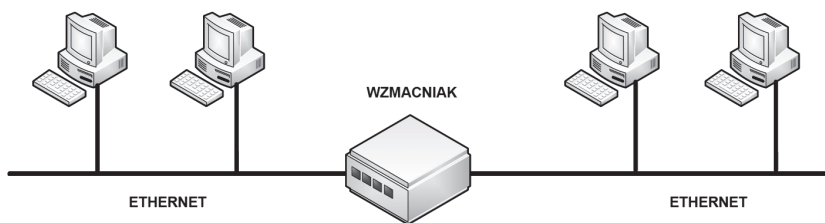
Rysunek 13. Karty sieciowe

Karta sieciowa (ang. *network interface card*), chociaż formalnie jest przypisana do warstwy łącza danych w modelu odniesienia ISO/OSI, funkcjonuje również w warstwie fizycznej. Jej podstawowa rola polega na translacji równoległego sygnału generowanego przez komputer do formatu szeregowego wysyłanego medium transmisyjnym.

Każda karta sieciowa ma unikatowy w skali całego świata **adres fizyczny (sprzętowy) MAC** (ang. *Media Access Control*), składający się z 48 bitów i przedstawiany przeważnie w postaci 12 cyfr w zapisie szesnastkowym. Pierwszych 6 szesnastkowych cyfr adresu MAC identyfikuje producenta OUI (ang. *Organizational Unique Identifier*), a ostatnie 6 szesnastkowych cyfr reprezentuje numer seryjny karty danego producenta.

Każde urządzenie sieciowe musi zawierać kartę sieciową i tym samym ma adres MAC.

Wzmacniak

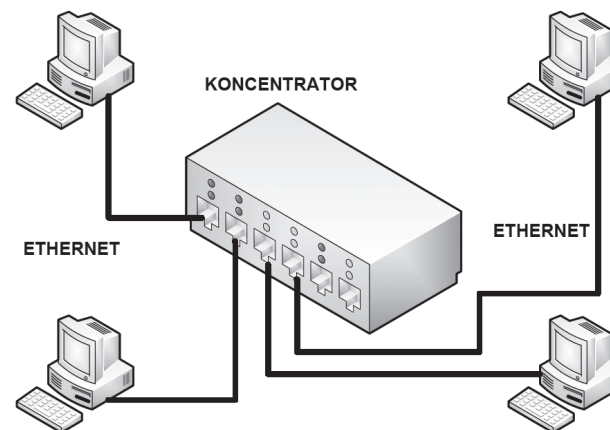


Rysunek 14.
Przykład zastosowania wzmacniaka

Wzmacniak jest najprostszym elementem sieciowym stosowanym do łączenia różnych sieci LAN. Głównym zadaniem wzmacniaka jest regeneracja (wzmocnienie) nadchodzących doń sygnałów i przesyłanie ich pomiędzy segmentami sieci. Wzmacniak może łączyć różne sieci ale o jednokowej architekturze, używając tych samych protokołów, metod uzyskiwania dostępu oraz technik transmisyjnych. Wzmacniak jest urządzeniem nieinteligentnym, nie zapewnia izolacji między segmentami, nie izoluje też uszkodzeń i nie filtruje ramek, w związku z czym informacja, często o charakterze lokalnym, przenika do pozostałych segmentów, obciążając je bez potrzeby.

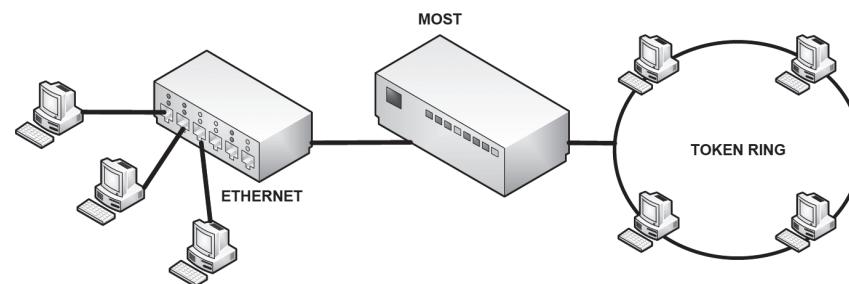
Koncentrator

Koncentrator jest podstawowym urządzeniem sieciowym w topologii gwiazdy. Każde stanowisko sieciowe jest podłączone do koncentratora, który jest centralnym elementem sieci. Koncentratory zawierają określoną liczbę portów, z reguły od 4 do 48. Jeżeli jest więcej stanowisk niż portów koncentratora, to wtedy należy użyć dodatkowego koncentratora i połączyć je ze sobą. W przypadku dużych sieci jest możliwe kaskadowe łączenie koncentratorów. Niestety, większe sieci, oparte wyłącznie na koncentratorach, są nieefektywne, gdyż wszystkie stacje w sieci współdzielą to samo pasmo. Jeżeli jedna stacja wyemituje jakąś ramkę, to pojawia się ona zaraz we wszystkich portach koncentratorów. Przy większym ruchu powoduje to kompletną niedrożność sieci.



Rysunek 15.
Przykład zastosowania koncentratora

Most



Rysunek 16.
Przykład zastosowania mostu

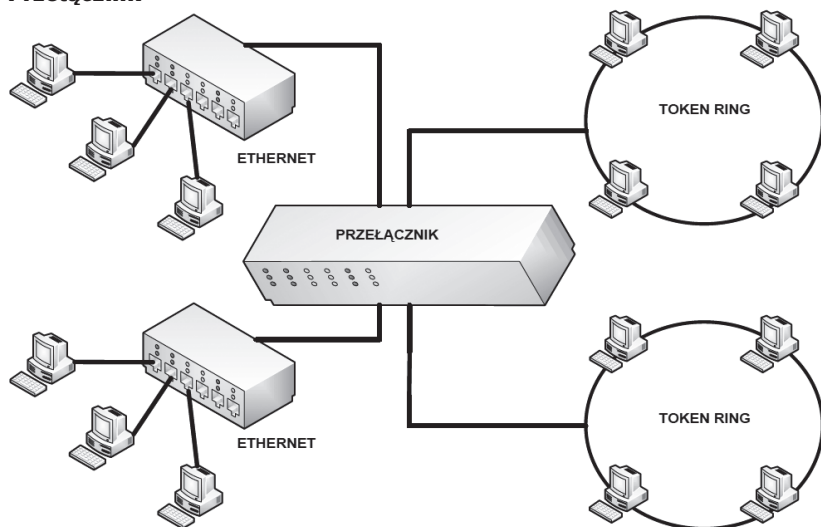
Most jest urządzeniem służącym do wzajemnego łączenia sieci lokalnych. Mosty, podobnie jak wzmacniaki, pośredniczą pomiędzy dwoma sieciami, mają przy tym większe możliwości. Największą ich zaletą jest to, że filtrują ramki, przesyłając je z segmentu do segmentu wtedy, gdy zachodzi taka potrzeba. Na przykład, jeżeli komunikują się dwie stacje należące do jednego segmen-



tu most nie przesyła ich ramek do drugiego segmentu. Wzmacniak w tym przypadku wysyłałby wszystko do drugiego segmentu, powiększając obciążenie zbędnym ruchem.

Mosty „wykazują zdolność” uczenia się. Zaraz po dołączeniu do sieci wysyłają sygnał do wszystkich węzłów z żądaniem odpowiedzi. Na tej podstawie oraz w wyniku analizy przepływu ramek, tworzą tablicę adresów fizycznych komputerów w sieci. Przy przesyłaniu danych most odczytuje z tablicy położenie komputera odbiorcy i zapobiega rozsyłaniu ramek po wszystkich segmentach sieci.

Przełącznik

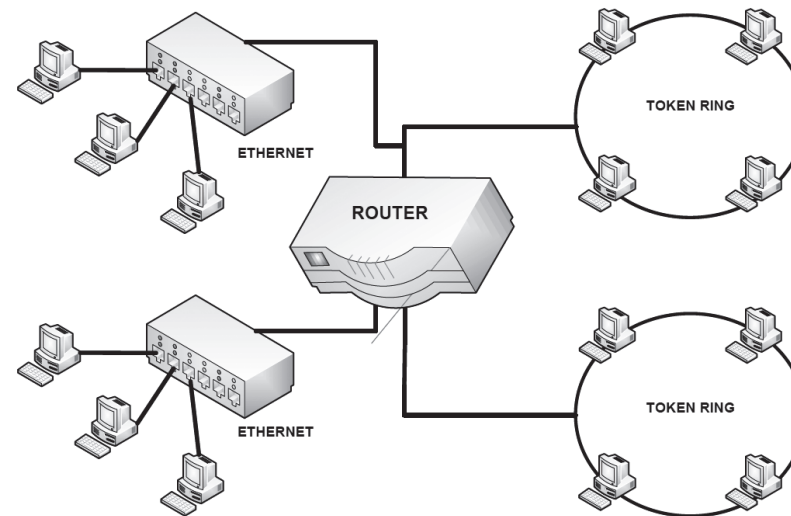


Rysunek 17. Przykład zastosowania przełącznika

Zadaniem **przełącznika** jest podział sieci na segmenty. Polega to na tym, że jeżeli w jakimś segmencie występuje transmisja danych angażująca jedynie stacje znajdujące się w tym segmencie, to ruch ten nie jest widoczny poza tym segmentem. Wydatnie poprawia to działanie sieci poprzez zmniejszenie natężenia ruchu i wystąpienia kolizji. Każdy przełącznik zawiera tablicę fizycznych adresów sieciowych MAC i na tej podstawie określa, czy dany adres docelowy znajduje się po stronie

portu z którego nadszedł, czy też jest przypisany innemu portowi. W ten sposób po inicjacji połączenia dane nie są rozsyłane w całej sieci, lecz są kierowane tylko do komunikujących się urządzeń. Użytkownikowi jest przydzielana wówczas cała szerokość pasma i na jego port są przesyłane wyłącznie dane skierowane do niego. W efekcie pracy przełącznika zawierającego np. 16 portów powstaje 16 niezależnych segmentów sieci, dysponujących całą szerokością pasma. Potencjalna przepustowość przełącznika jest określana przez sumaryczną przepustowość każdego portu. Szesnastoportowy przełącznik Fast Ethernet ma zatem zagregowaną przepustowość 1.6 Gb/s, podczas gdy wyposażony w szesnaście portów koncentrator Fast Ethernet – zaledwie 100 Mb/s.

Router



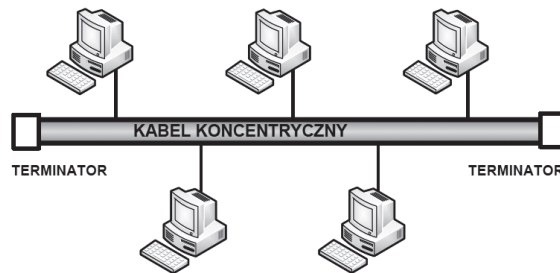
Rysunek 18. Przykład zastosowania routera

Router służy do zwiększania fizycznych rozmiarów sieci poprzez łączenie jej segmentów. Urządzenie to wykorzystuje logiczne adresy hostów w sieci. Ponieważ komunikacja w sieci jest oparta na logicznych adresach odbiorcy i nadawcy, przesyłanie danych i informacji jest niezależne od fizycznych adresów urządzeń. Oprócz filtracji pakietów pomiędzy segmentami, router określa optymal-

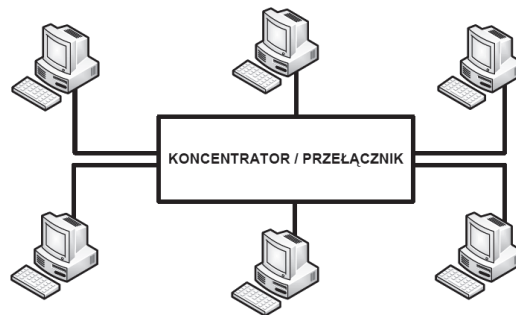
ną drogę przesyłania danych po sieci między nadawcą i odbiorcą. Dodatkowo eliminuje on pakiety bez adresata i ogranicza dostęp określonych użytkowników do wybranych segmentów czy komputerów sieciowych. Router jest konfigurowalny, umożliwia sterowanie przepustowością sieci oraz zapewnia pełną izolację pomiędzy segmentami.

5 TOPOLOGIE SIECIOWE

TOPOLOGIA
FIZYCZNA: MAGISTRALA
LOGICZNA: MAGISTRALA



TOPOLOGIA
FIZYCZNA: GWIAZDA
LOGICZNA: MAGISTRALA

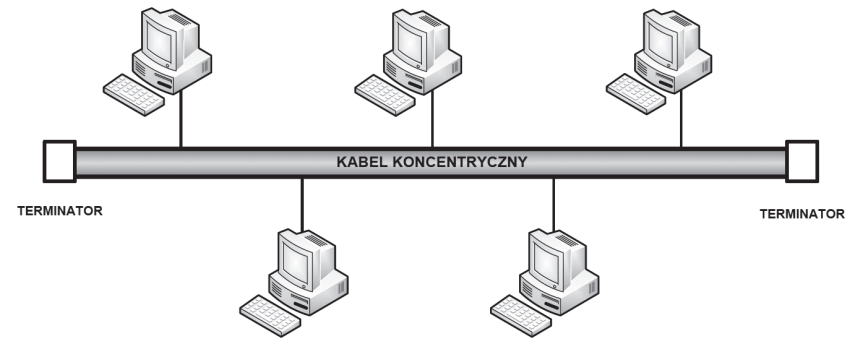


Rysunek 19.

Porównanie topologii fizycznej i logicznej

Topologia fizyczna (ang. *physical topology*) jest związana z fizycznym (elektrycznym, optycznym, radiowym) łączeniem ze sobą urządzeń sieciowych. **Topologia logiczna** (ang. *logical topology*) określa standardy komunikacji, wykorzystywane w porozumiewaniu się urządzeń sieciowych.

Topologia magistrali



Rysunek 20.

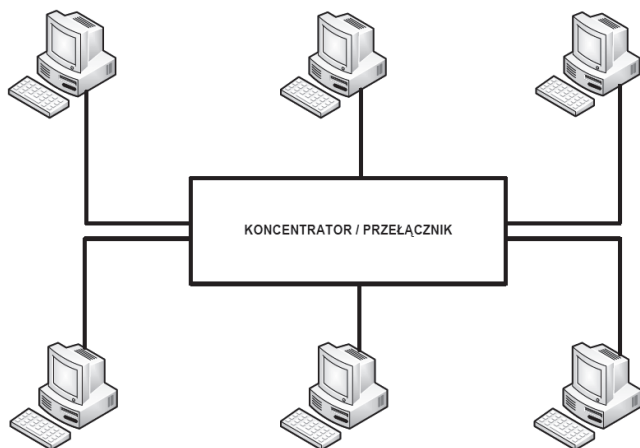
Topologia magistrali

Topologia magistrali (szyny) (ang. *bus topology*) do niedawna była jedną z najpopularniejszych topologii sieciowych. Składa się z wielu komputerów przyłączonych do wspólnego kabla koncentrycznego (grubego lub cienkiego) zakończonego z obu stron terminatorem (opornikiem). Gdy dane zostają przekazane do sieci, w rzeczywistości trafiają do wszystkich przyłączonych komputerów. Wówczas każdy komputer sprawdza, czy adres docelowy danych pokrywa się z jego adresem MAC. Jeżeli zgadza się, to komputer odczytuje (kopiuje) przekazywane informacje (ramki), a w przeciwnym przypadku przesyłka zostaje odrzucona. Do zalet topologii magistrali należą: niewielka długość kabla oraz prostota układu przewodów. Pojedyncze uszkodzenie (awaria komputera) nie prowadzi do unieruchomienia całej sieci. Wadą jest to, że wszystkie komputery muszą dzielić się wspólnym kablem.

Topologia gwiazdy

Sieć w **topologii gwiazdy** (ang. *star topology*) zawiera centralny koncentrator połączony ze wszystkimi komputerami użytkowników za pomocą kabli skrętkowych. Cały ruch w sieci odbywa się przez koncentrator lub przełącznik. W stosunku do pozostałych topologii, struktura gwiazdy ma parę zalet. Jedną z nich jest łatwość konserwacji i łatwiejsza diagnostyka. Na przykład łatwo odszukać uszkodzony odcinek kabla, gdyż każdemu węzłowi odpowiada tylko jeden kabel dołączony do koncentratora. Wadą tej topologii jest zwiększona całość

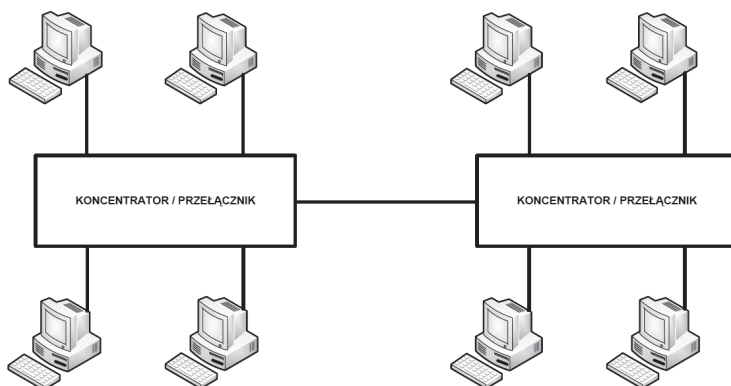




Rysunek 21.
Topologia gwiazdy

kowitą długość okablowania, czyli koszty założenia sieci. Poważniejszy problem wynika z centralnego koncentratora lub przełącznika - ich awaria powoduje awarię całej sieci.

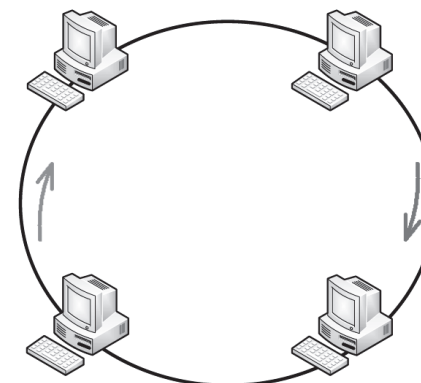
Topologia rozszerzonej gwiazdy



Rysunek 22.
Topologia rozszerzonej gwiazdy

Topologia rozszerzonej gwiazdy (ang. *extended star topology*) to obecnie najczęściej stosowana topologia sieciowa. Umożliwia dużą skalowalność, zwłaszcza gdy są stosowane przełączniki jako węzły centralne.

Topologia pierścienia

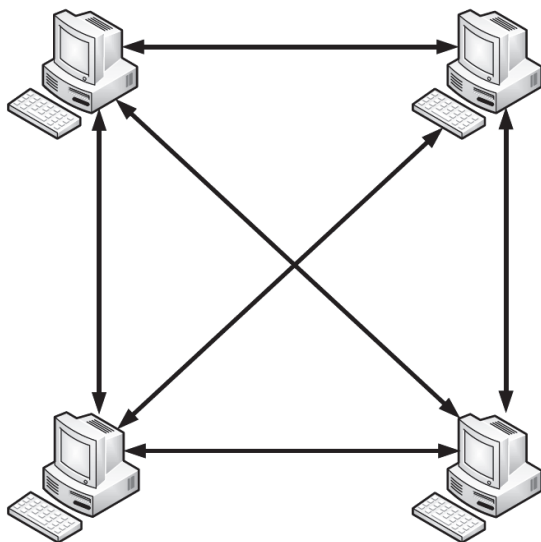


Rysunek 23.
Topologia pierścienia

W **topologii pierścienia** (ang. *ring topology*) wiele stacji roboczych łączy się za pomocą jednego nośnika informacji w zamknięty pierścień. Okablowanie nie ma żadnych zakończeń, bo tworzy pełny krąg. Każdy węzeł włączony do pierścienia działa jak wzmacniak, wyrównując poziom sygnału między stacjami. Dane poruszają się w pierścieniu w jednym kierunku, przechodząc przez każdy węzeł. Jedną z zalet topologii pierścienia jest niewielka potrzebna długość kabla, co obniża koszty instalacji. Nie ma tu również centralnego koncentratora, gdyż tę funkcję pełnią węzły sieci. Z drugiej strony, ponieważ dane przechodzą przez każdy węzeł, to awaria jednego węzła powoduje awarię całej sieci. Trudniejsza jest również diagnostyka, a modyfikacja (dotychczas, odłączenie urządzenia sieciowego) wymaga wyłączenia całej sieci.

Topologia siatki

Topologia siatki (ang. *mesh topology*) jest stosowana w rozwiązaniach nadmiarowych (redundantnych), aby zapewnić bardzo wysoki poziom niezawodności. W topologii tej urządzenia sieciowe są połączone ze sobą każdy z każdym.



Rysunek 24.
Topologia siatki

LITERATURA

1. Dye M.A., McDonald R., Ruff A.W., *Akademia sieci Cisco. CCNA Exploration. Semestr 1*, WN PWN, Warszawa 2002
2. Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2005
3. Mucha M., *Sieci komputerowe. Budowa i działanie*, Helion, Gliwice 2003
4. Odom W., Knot T., *CCNA semestr 1. Podstawy działania sieci*, WN PWN, Warszawa 2007
5. Pawlak R., *Okablowanie strukturalne sieci*. Wydanie II, Helion, Gliwice 2008

WARSZTATY

Celem warsztatów jest wprowadzenie do podstawowych koncepcji i technologii sieciowych, na których opiera się biznesowe budowa i funkcjonowanie sieci komputerowych. Prezentowany materiał zawiera podstawową wiedzę niezbędną do poznania usług, technologii i zagadnień, z którymi spotykają się użytkownicy infrastruktury sieciowej.

1 ELEMENTY SIECI KOMPUTEROWEJ

Urządzenia końcowe

Urządzenia końcowe to urządzenia, które pośredniczą (tworzą interfejs) pomiędzy człowiekiem a siecią komunikacyjną. Kilka przykładów takich urządzeń: komputery (stacje robocze, laptopy, serwery plików, serwery WWW), drukarki sieciowe, telefony VoIP, kamery w systemie do monitoringu, niewielkie urządzenia mobilne (bezprowadowe skanery kodów kreskowych, PDA). W terminologii sieci komputerowych, urządzenia końcowe nazywamy **hostami**. Host może być zarówno źródłem informacji, jak i urządzeniem docelowym dla wiadomości wysłanej w sieci. W sieciach są wykorzystywane również **urządzenia pośredniczące** dla zapewnienia łączności i poprawności przepływu informacji. Urządzenia te łączą poszczególne hosty z siecią oraz wiele niezależnych sieci, tworząc w ten sposób sieć globalną. Przykładem urządzeń pośredniczących są: urządzenia dostępowe (koncentratory, przełączniki, bezprzewodowe punkty dostępowe), urządzenia łączące sieci (routery), serwery komunikacyjne i modemy, urządzenia zapewniające bezpieczeństwo (firewalle). Inną rolą urządzeń pośredniczących jest zarządzanie przepływem danych.

Aktywne i pasywne elementy infrastruktury sieciowej

Karta sieciowa (ang. NIC - *Network Interface Card*) to karta rozszerzenia, która służy do przekształcania pakietów danych w sygnały, które są przesyłane w sieci komputerowej. Każda karta ma 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.

Router to urządzenie sieciowe pracujące w trzeciej warstwie modelu OSI. Służy do łączenia różnych sieci komputerowych (różnych w sensie informatycznym,



czyli np. o różnych klasach, maskach itd.), pełni więc rolę węzła komunikacyjnego. Na podstawie informacji zawartych w pakietach TCP/IP, router przekazuje pakiety z sieci źródłowej do sieci docelowej, rozróżniając ją spośród wielu sieci. Proces kierowania ruchem nosi nazwę **trasowania**, **routingu** lub **rutowania**.

Przełącznik (przełącznica, komutator, także z ang. *switch*) to urządzenie łączące segmenty sieci komputerowej, pracujące w drugiej warstwie modelu ISO/OSI (łącza danych). Jego zadaniem jest przekazywanie ramek między segmentami.

Nazwa **ramka** jest używana w odniesieniu do jednostek informacji przesyłanych w warstwie drugiej w modelu OSI. **Segment** to część sieci komputerowej, odseparowana od reszty przez urządzenie sieciowe, takie jak: przełącznik, router, most. Podział na segmenty wpływa na zmniejszenie obciążenia sieci lokalnej przez separację ruchu na ruch segmentowy i międzysegmentowy – jeśli dwa komputery znajdują się w jednym segmencie, to przesyłane między nimi pakiety nie wychodzą poza segment. Zwiększa liczbę domen kolizyjnych i wpływa na zmniejszenie kolizji pakietów w danej sieci.

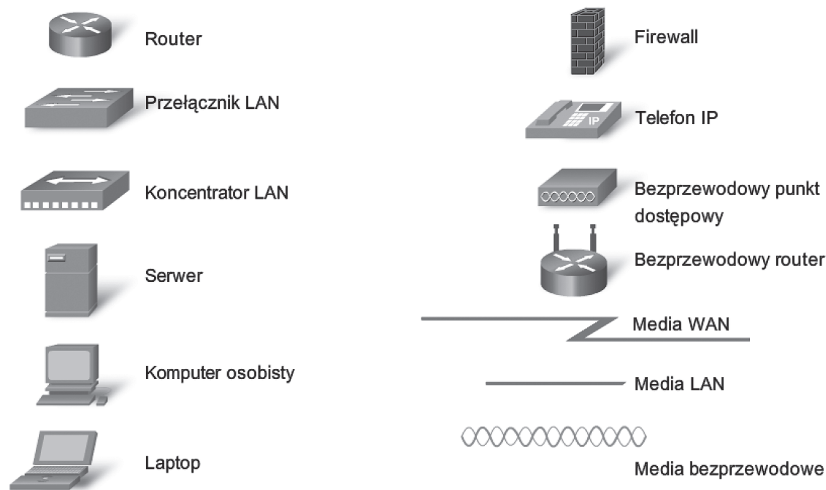
Koncentrator pracuje w warstwie pierwszej modelu ISO/OSI (warstwie fizycznej), przesyłając sygnał z jednego portu na wszystkie pozostałe. Nie analizuje ramki pod kątem adresu MAC oraz IP. Ponieważ koncentrator powtarza każdy sygnał elektroniczny, tworzy jedną domenę kolizyjną.

Punkt dostępowy (ang. *access point*, skóty PD lub AP) to urządzenie zapewniające komputerom dostęp do zasobów sieci za pomocą bezprzewodowego medium transmisyjnego. Punkt dostępowy jest także mostem łączącym sieć bezprzewodową z siecią przewodową (najczęściej Ethernet).

Modem (ang. *MOdulator-DEModulator*) to 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 (ang. *Data Communications Equipment*), które w całości wykonuje opisane wyżej czynności. Nieodzowne do współpracy jest DTE (ang. *Data Terminal Equipment*) i to dopiero stanowi całość łączą przesyłania danych. Dzięki modemowi można łączyć ze sobą komputery i urządzenia, które dzieli znaczna odległość.

Media

Komunikacja w sieci komputerowej odbywa się za pomocą **medium komunikacyjnego**. Medium zapewnia kanał, którym wiadomość jest przesyłana od źródła do celu. Sieci komputerowe wykorzystują głównie trzy typy mediów łączących urządzenia i zapewniających ścieżki transmisji danych. Te media to: metalowe przewody wewnątrz kabli (interfejs elektryczny), włókna szklane lub plastikowe – światłowód (interfejs optyczny), transmisja bezprzewodowa (interfejs radiowy).



Rysunek 25. Przykładowe symbole elementów sieci komputerowej

2 USŁUGI

Do **usług sieciowych** zalicza się różnego rodzaju świadczenia związane z komunikacją oraz realizacją różnych zadań w sieci, np.: serwisy internetowe WWW, usługi poczty elektronicznej, transakcje bankowe, zakupy internetowe i inne. Wiele współużytkujących Internet aplikacji używa różnych kombinacji interakcji pomiędzy stacjami klienckimi i serwerami. Usługa sieciowa może być: ■ zdefiniowana za pomocą języka opisu usług – standaryzowanym językiem, bazującym na XML (ang. *Extensible Markup Language*) jest WSDL (ang. *Web Services Description Language*);

- opublikowana i wyszukana w rejestrze usług za pomocą standardowego mechanizmu, np. rejestry UDDI (ang. *Universal Description, Discovery and Integration*);
- wywołana zdalnie przez zdefiniowany interfejs;
- częścią innych usług sieciowych lub być ich kompozycją.

Połączenie zestandaryzowanego języka komunikacji i prezentacji oraz mechanizmów interakcji pomiędzy stacjami klienckimi i serwerami, umożliwia projektowanie i budowanie zestawów usług sieciowych. Na bazie usług sieciowych można konstruować rozproszone systemy i aplikacje. Aplikacje komunikują się z usługami sieciowymi z wykorzystaniem internetowych protokołów i formatów danych.

3 ŁĄCZENIE ELEMENTÓW INFRASTRUKTURY TELEINFORMATYCZNEJ W SIĘĆ KOMPUTEROWĄ

Ćwiczenie 1. Zbudowanie modelu z wykorzystaniem oprogramowania Packet Tracer według załączonego schematu. Wykorzystując następujące elementy sieci komputerowych:

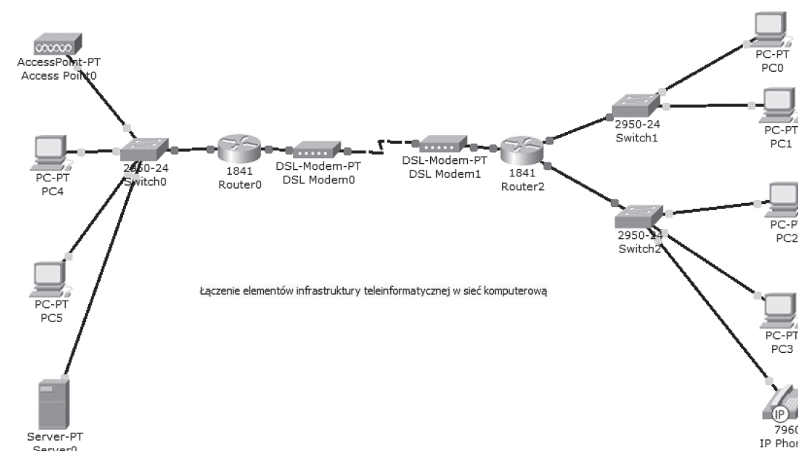
- urządzenia dostępne (koncentratory, przełączniki, bezprzewodowe punkty dostępne),
- urządzenia łączące sieci (routery),
- serwery komunikacyjne i modemy, oraz postępując się oprogramowaniem Packet Tracer zbudujemy model sieci przedstawionej schematycznie na rys. 26.

4 KORZYSTANIE Z USŁUG SIECIOWYCH

Wyróżnia się dwa podstawowe modele architektury sieci komputerowych – model klient-serwer oraz model peer-to-peer.

Ćwiczenie 2. Prezentacja pracy w modelu sieci typu klient-serwer:

- logowanie się do serwera FTP i pobieranie i wysyłanie plików;
- logowanie się do serwisów internetowych świadczących usługi udostępniania streamingu audio i video;
- logowanie się do portali społecznościowych.



Rysunek 26.

Schemat przykładowej sieci komputerowej

Ćwiczenie 3. Prezentacja pracy w modelu sieci typu peer-to-peer:

- wymiana plików w ramach jednej grupy roboczej;
- korzystanie z sieci eDonkey za pomocą oprogramowania klienckiego eMule.

Sytuacja prawna związana z wymianą plików w sieciach peer-to-peer jest dość złożona ze względu na ochronę praw autorskich. Systemy P2P same niczego nie rozpowszechniają, więc mogą być oskarżone co najwyżej o „współdziałanie” lub „czerpanie korzyści”. Systemy P2P próbują stosować system *opt-out* – blokując utwory z listy dostarczonych przez właścicieli praw autorskich. Samo ściąganie plików przez P2P zgodnie z polskim prawem autorskim nie jest jednak nielegalne. Świadczą o tym przepisy o dozwolonym użytku osobistym w art. 23 polskiej ustawy o prawie autorskim i prawach pokrewnych. Dopiero połączenie tego działania z rozpowszechnianiem utworów jest naruszeniem prawa RP.

5 ANALIZA DZIAŁANIA SIECI KOMPUTEROWEJ

Użycie komendy ping oraz tracert

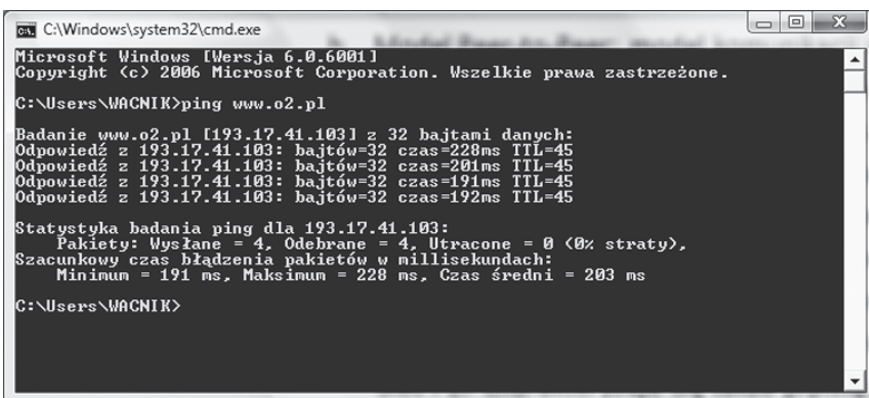
Komenda **ping** jest używana w sieciach komputerowych, wykorzystujących protokół TCP/IP (takich jak Internet), do diagnozowania połączeń sieciowych.



Umożliwia sprawdzenie, czy istnieje połączenie pomiędzy hostami testującym i testowanym i określenie jakości połączenia między nimi poprzez mierzenie liczby zgubionych pakietów oraz czasu potrzebnego na ich transmisję. Program ping korzysta z protokołu ICMP, wysyła pakiety ICMP Echo Request i odbiera ICMP Echo Reply. Większość publicznie dostępnych serwerów obsługuje te pakiety. W takiej sytuacji aplikacja ping umożliwia sprawdzenie poprawnego działania sieci komputerowej, chociaż większość użytkowników programu ping jest błędnie przekonana, że jeśli zdalny host nie odpowiada na wysłane przez ten program pakiety, to jest tak tylko wtedy, gdy host nie jest włączony lub jest problem z siecią pomiędzy obiema maszynami. Warto pamiętać, iż blokowanie wysyłania pakietów-odpowiedzi ICMP Echo Reply (stosuje się do tego celu zapory sieciowe lub filtry w routerach) jest jedną z powszechnie stosowanych metod ochrony przed atakami w sieci. Spowodowane jest to tym, że analiza pakietów ICMP Echo Reply nie tylko potwierdza istnienie hosta pod danym adresem IP, ale często również umożliwia dokładne określenie systemu operacyjnego, co ułatwia zaatakowanie komputera.

Ćwiczenie 4. Użycie komendy ping w systemie operacyjnym Windows:

- wywołania okna linii komend;
- wpisanie i parametryzacja komendy ping;
- analiza otrzymanych wyników.



Rysunek 27. Użycie komendy ping w oknie systemu Windows

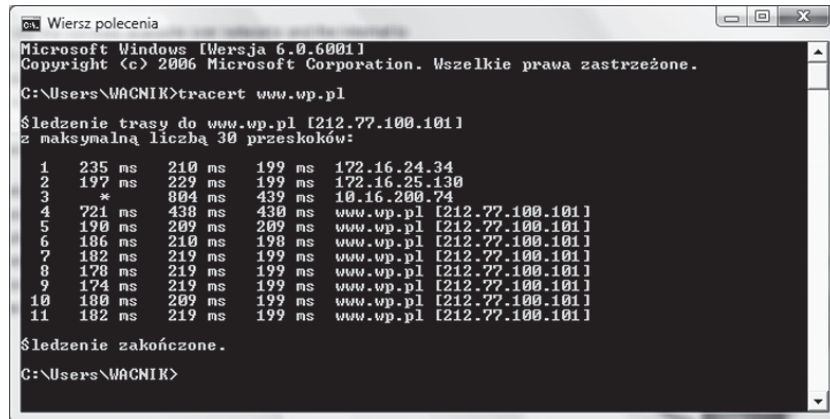
Polecenie **tracert** służy do badania trasy pakietów w sieci IP, i jest szeroko dostępne we wszystkich uniksowych systemach operacyjnych. Istnieje również program **tracert** o podobnej funkcjonalności, zawarty w systemach z rodziny Microsoft Windows. Działanie tego programu jest oparte na protokołach komunikacyjnych UDP oraz ICMP:

- Na początku jest wysyłany pakiet z polem TTL (*Time To Live*) ustawionym na 1. Wartość ta jest zmniejszana przy przechodzeniu przez kolejne routery na trasie. Jeżeli pole TTL osiągnie wartość 0 to pakiet jest odrzucany przez router, który wysyła wtedy informację zwrotną w postaci komunikatu ICMP typu Time Exceeded. W ten sposób komputer źródłowy uzyskuje adres IP pierwszego routera na trasie.
- W następnym wysylnym pakiecie z komputera źródłowego pole TTL ma wartość 2. Pierwszy router zmniejszy tę wartość do 1 i przekaże do drugiego routera na trasie. Drugi router zachowa się podobnie jak ten pierwszy poprzednio, czyli zmniejszy TTL do 0 i odrzuci pakiet wysyłając komunikat Time Exceeded do komputera źródłowego.
- Informacje o kolejnych routerach na trasie uzyskuje się analogicznie zwiększając wartość pola TTL stopniowo o 1 w wysyłanych pakietach.
- Jeżeli pakiet dotrze w końcu do hosta docelowego, to najprawdopodobniej zostanie odesłany komunikat ICMP Port Unreachable. Dzieje się tak dlatego, że uniksowe implementacje programu tracert świadomie wysyłają pakiety UDP z numerem portu powyżej 30000. Zazwyczaj w porcie o tak wysokim numerze nie działają żadne usługi, więc żaden proces w komputerze docelowym nie będzie chciał obsłużyć nadchodzącego pakietu. W tej sytuacji badanie trasy zostaje zakończone.

W systemach z rodziny Microsoft Windows program tracert jest zaimplementowany nieco inaczej. Główna zasada działania polegająca na stopniowym zwiększaniu pola TTL w wysyłanych pakietach pozostaje jednak taka sama. Różnica polega na tym, że wysyłane pakiety nie są datagramami UDP, lecz komunikatami ICMP typu Echo Request. Jeżeli taki komunikat osiągnie swoje przeznaczenie, to zawsze zostanie odesłana odpowiedź Echo Reply. Dzięki temu nie trzeba polegać na założeniu związanym z wysokimi numerami portów dla datagramów UDP.

Ćwiczenie 5. Użycie komendy *tracert* w systemie operacyjnym Windows:

- wywołania okna linii komend;
- wpisanie i parametryzacja komendy *tracert*;
- analiza otrzymanych wyników.



Rysunek 28.

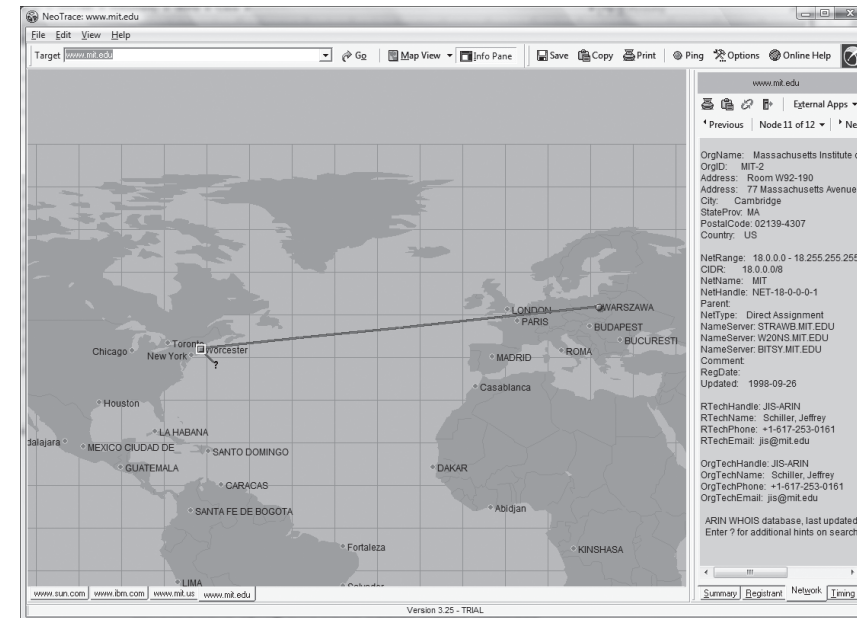
Użycie komendy tracert w oknie systemu Windows

Wykorzystanie oprogramowania NeoTrace do wizualizacji sieci

Oprogramowanie NeoTrace służy do wizualizacji działania sieci w wykorzystaniem programów ping oraz tracert. Prezentuje w formie graficznej internetową ścieżkę pomiędzy komputerem użytkownika a dowolną stroną (serwerem) WWW. Zawiera mapę świata, na której wyświetla lokalizację poszczególnych węzłów (np. routerów).

Ćwiczenie 7. Śledzenie trasy z wykorzystaniem NeoTrace:

- uruchom program NeoTrace;
- w menu View wybierz Options Wybierz zakładkę Map i w sekcji Home Location kliknij przycisk Set Home Location;
- zgodnie z instrukcjami wybierz swój kraj i lokalizację w kraju;
- alternatywnie możesz wybrać opcje zaawansowane przez kliknięcie przycisku Advanced , to umożliwi podanie współrzędnych geograficznych Twojej lokalizacji;
- wprowadź np. "www.mit.edu" w polu Target i kliknij Go;
- naciśnięcie opcji List View w menu View powoduje wyświetlenie listy routerów, podobnej do otrzymanej za pomocą programu tracert;
- naciśnięcie Node View z menu View graficznie powoduje wyświetlenie połączenia z symbolami;



Rysunek 29.

Okno aplikacji NeoTrace

- wybranie Map View z menu View powoduje wyświetlenie łącza i routerów umiejscowionych na mapie, adekwatnie do ich realnej geograficznej pozycji;
- wybierz każdy ze sposobów prezentowania danych i zauważ różnice i podobieństwa;
- przetestuj różne adresy URL i obejrzyj trasy do tych miejsc przeznaczenia.

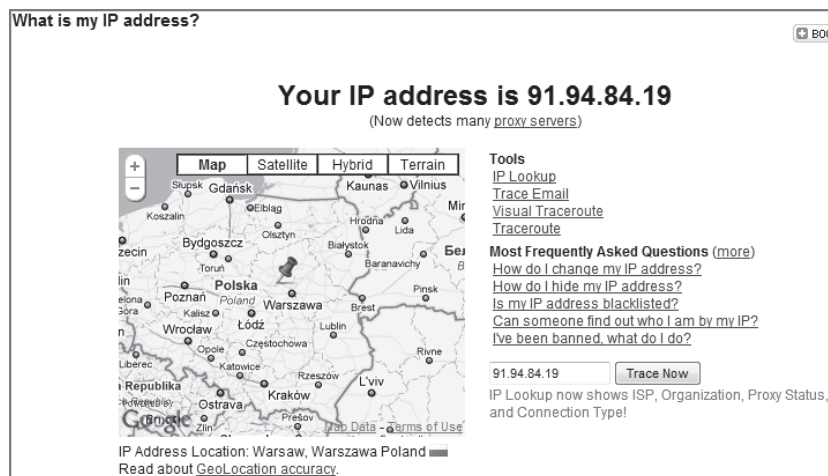
Narzędzia WWW

Do analizy działania sieci komputerowych możemy wykorzystać także aplikacje WWW. Jako przykład prezentujemy tutaj aplikację Whatismyipaddress (<http://whatismyipaddress.com>) służącą do analizy i wizualizacji naszej konfiguracji sieciowej wraz z elementami testowania i diagnostyki

Ćwiczenie 7. Testowanie sieci internetowej z wykorzystaniem aplikacji Whatismyipaddress:



- otwarcie strony <http://whatismyipaddress.com>;
- wykonanie testu IP Lookup;
- wykonanie testu Trace Email;
- wykonanie testu Visual Traceroute.



Rysunek 30.
Okno aplikacji NeoTrace

--	--



--	--



--	--	--

W projekcie **Informatyka +**, poza wykładami i warsztatami,
przewidziano następujące działania:

- 24-godzinne kursy dla uczniów w ramach modułów tematycznych
- 24-godzinne kursy metodyczne dla nauczycieli, przygotowujące do pracy z uczniem zdolnym
 - nagrania 60 wykładów informatycznych, prowadzonych przez wybitnych specjalistów i nauczycieli akademickich
 - konkursy dla uczniów, trzy w ciągu roku
 - udział uczniów w pracach kół naukowych
 - udział uczniów w konferencjach naukowych
 - obozy wypoczynkowo-naukowe.

Szczegółowe informacje znajdują się na stronie projektu **www.informatykaplus.edu.pl**

informatyka+

Algorytmika i programowanie

Bazy danych

Multimedia, grafika i technologie internetowe

Sieci komputerowe

Tendencje w rozwoju informatyki i jej zastosowań

Człowiek – najlepsza inwestycja



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI



WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.