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.

informatyka+

Wszechnica Informatyczna: Sieci komputerowe

Budowa i działanie 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.

Budowa i działanie sieci komputerowych

Rodzaj zajęć: Wszechnica Informatyczna
Tytuł: Budowa i działanie sieci komputerowych
Autorzy: 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.wwsi.edu.pl
rektorat@wwsi.edu.pl

Projekt graficzny: FRYCZ I WICHA

Warszawa 2010

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.

Budowa i działanie 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. Prezentuje najważniejsze fakty z historii sieci komputerowych i Internetu mające istotny wpływ na obecny ich kształt i możliwości. 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 najczęściej spotykane topologie sieciowe (magistrala, gwiazda, pierścień, siatka), a także wyjaśnia pojęcia związane z segmentacją i domenami kolizyjnymi. Zawarto w nim również informacje o przewodowych i bezprzewodowych mediach transmisyjnych wykorzystywanych przy budowie sieci komputerowych oraz zasadach projektowania okablowania strukturalnego sieci (poziomego i pionowego).

Warsztaty umożliwiają praktyczne przećwiczenie materiału z wykładu.

Spis treści

1 HISTORIA SIECI KOMPUTEROWYCH I INTERNETU

Rys historyczny

1957 4 października Związek Radziecki wystrzelił na orbitę okołoziemską Sputnik – pierwszy sztuczny satelita Ziemi. W odpowiedzi – w USA powołano agencję **ARPA** (ang. *Advanced Research Projects Agency*).

1964 Raport Paula Barana *On Distributed Communications* dla RAND Corporation (amerykańska korporacja badawcza).

1967 Agencja ARPA zleca firmie BBN (Bolt, Beranek, Newman) zbudowanie sieci ARPANET (ang. ARPA Network), opartej na wymianie pakietów zaproponowanej przez Barana.

1968 Pierwsza funkcjonująca sieć pakietowa w National Physical Laboratories w Wielkiej Brytanii;

1969 Uruchomienie pierwszych czterech węzłów sieci ARPANET o przepustowość 50 kbps, ulokowanych w:
- Sieciowym Centrum Pomiarowe Uniwersytetu Kalifornijskiego w Los Angeles,
- Sieciowym Centrum Informacyjne Instytutu Badawczego Stanforda,
- Instytucie Interaktywnej Matematyki Cullera-Frieda Uniwersystetu Kalifornijskiego w Santa Barbara,
- Instytucie Grafiki Uniwersytetu Utah.

Pierwszy dokument z serii RFC (Steve Crocker „Host Software").

1970 Wprowadzenie w węzłach sieci ARPANet protokołu NCP (*Network Control Protocol*) – zapewniał transmisję danych w pojedynczej sieci komputerowej i obsługiwał maksymalnie 255 maszyn.

1972 Pierwsza publiczna prezentacja funkcjonowania sieci ARPANet.
Opracowanie Telnetu oraz programu do wymiany poczty elektronicznej (Ray Tomlinson).

1973 FTP (*File Transfer Protocol*).

1974 Specyfikacja protokołu TCPŁ Vinton Cerf i Bob Kahn, *A Protocol for Packet Network Intercommunication*.

1977 Pierwsza demonstracja funkcjonowania zestawu protokołów TCP/IP.

1982 Początki właściwego Internetu (sieci sieci) w związku z przejściem sieci ARPANet na protokół TCP/IP.

1983 Wyodrębnienie z sieci ARPANet części militarnej – sieci MILNET (*Military Network*).
DNS (*Domain Name System*), Paul Mockapetris.

1988 Narodowa Fundacja Nauki (**NSF** – *National Science Foundation*) rozpoczyna zakładanie linii T1 o przepustowości 1,544 Mbps – powstaje sieć szkieletowa NSFNET.
Opracowanie IRC (*Internet Relay Chat*) – Jarkko Oikarinen;

1989 Opracowanie WWW (*World Wide Web*) w Instytucie Fizyki Jądrowej CERN w Genewie przez Tima Bernersa-Le, absolwenta uniwersytetu w Oxfordzie w Wielkiej Brytanii.

1991 Wprowadzenie łączy T3 (45 Mbps) w sieci szkieletowej NSFNET.
Opracowanie rozproszonego systemu wyszukiwania tekstów na zdalnych komputerach, typu klient-serwer WAIS (*Wide Area Information Servers*) w siedzibie firmy Thinking Machines Corporation przez Brewstera Kahle'a.
Opracowanie Gopher w Uniwersytecie w Minnesocie przez Paula Lindnera i MarkaMcCahilla.

1993 Mosaic – pierwsza graficzna przeglądarka WWW.

1995 Zastąpienie sieci szkieletowej NSFNET kilkoma sieciami komercyjnymi.

1996 Konstrukcja sieci ATM (*Asynchronous Transfer Mode*) o przepustowości 155 Mbps.

1999 Początek programu SETI@home – wspólnego poszukiwania cywilizacji pozaziemskich przez internautów.

Dokumenty RFC

Aby usprawnić technologię wykorzystywaną przez sieć ARPANet, został zaprojektowany specjalny system obsługujący i ułatwiający wymianę korespondencji pomiędzy inżynierami pracującymi nad nową siecią.

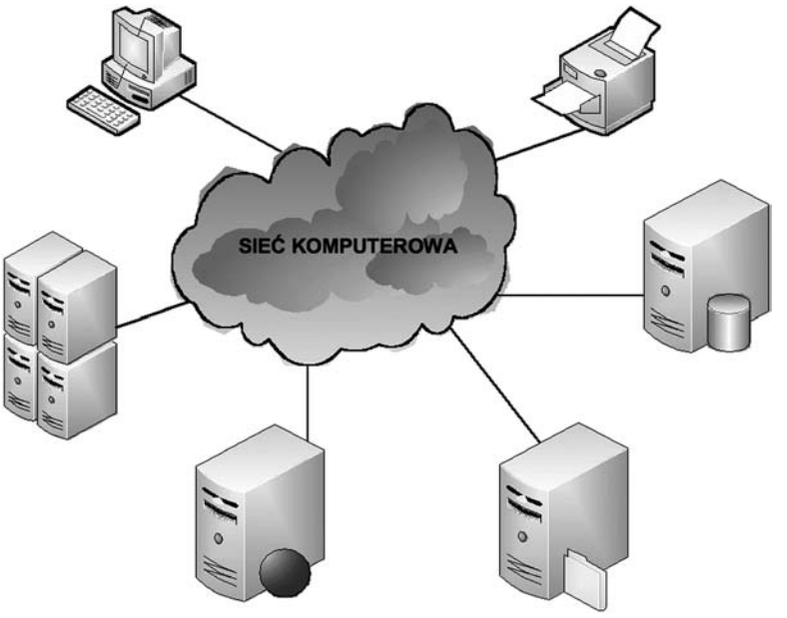
RFC (ang. *Request for Comments*) to dokumenty tworzone przez inżynierów, zespoły inżynierów lub kogoś kto miał po prostu lepszy pomysł na nową technologię albo jej usprawnienie. Proces powstawania RFC zastał zaprojektowany jako biuletyn dla zgłaszania koncepcji technologicznych. Po napisaniu i rozesłaniu RFC, może on być modyfikowany, krytykowany oraz wykorzystany przez innych inżynierów i wynalazców. Jeśli ktoś z nich chciał rozwinąć teorię, RFC zapewniał do tego celu otwarte forum.

RFC jest przedkładany do IETF (ang. *Internet Engineering Task Force*), gdzie zostaje mu przypisany numer, który jest automatycznie nazwą dokumentu RFC. RFC 1 został przekazany w 1969 roku przez wynalazcę Stevea Crockera (obecnie jest ich ponad 5700 – stan na październik 2009). Dokumenty RFC możemy przeczytać na oficjalnej stronie IETF (ang. *Internet Engineering Task Force*) – www.ietf.org.

2 ROLA, ZADANIA I PODZIAŁ SIECI KOMPUTEROWYCH

Co to jest sieć komputerowa

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



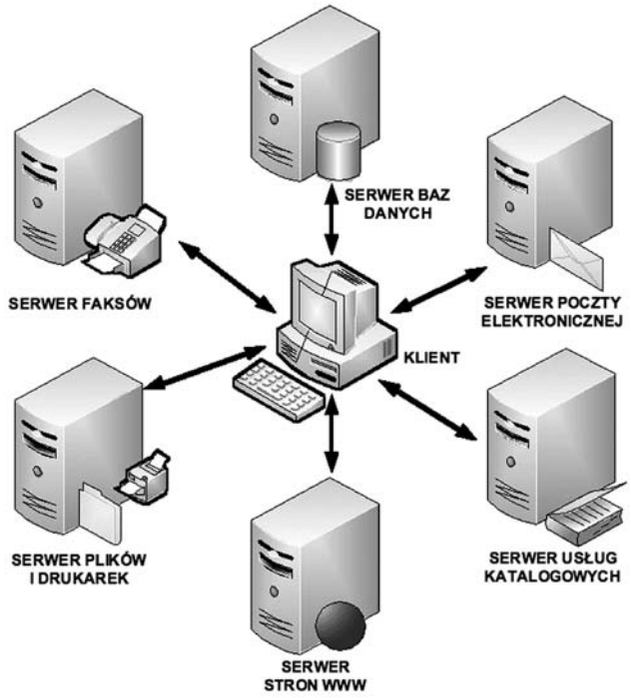
Rysunek 1.
Przykład sieci komputerowej

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

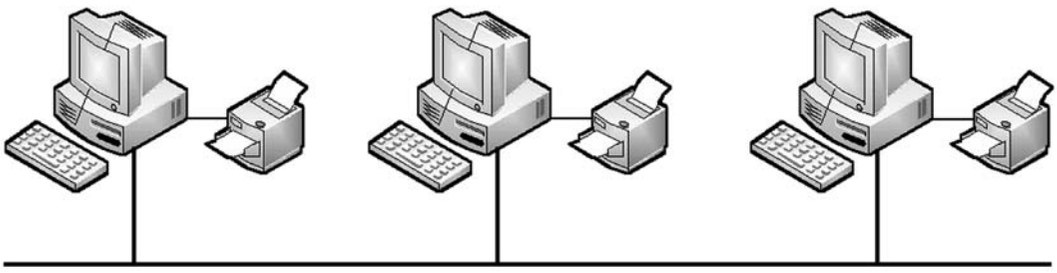


Rysunek 2.
Przykładowe role komputerów w sieci

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.

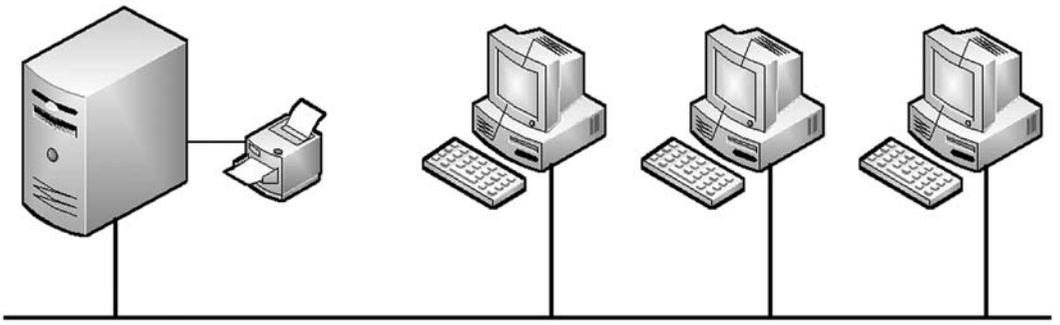
Sieć typu peer-to-peer (równorzędna)



Rysunek 3.
Sieć równorzędna

Na rysunku 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



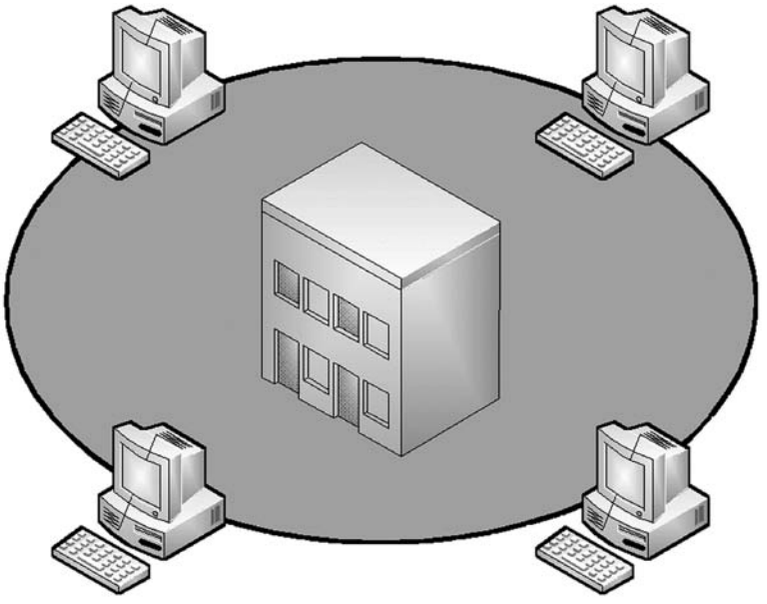
Rysunek 4.
Sieć typu klient-serwer

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: wymóg specjalistycznego oprogramowanie do monitorowania, administrowania i zarządzania, wyższy koszt urządzeń sieciowych, obecność wyszkolonego personelu administracyjnego.

Zasięgi sieci komputerowych

Sieć LAN

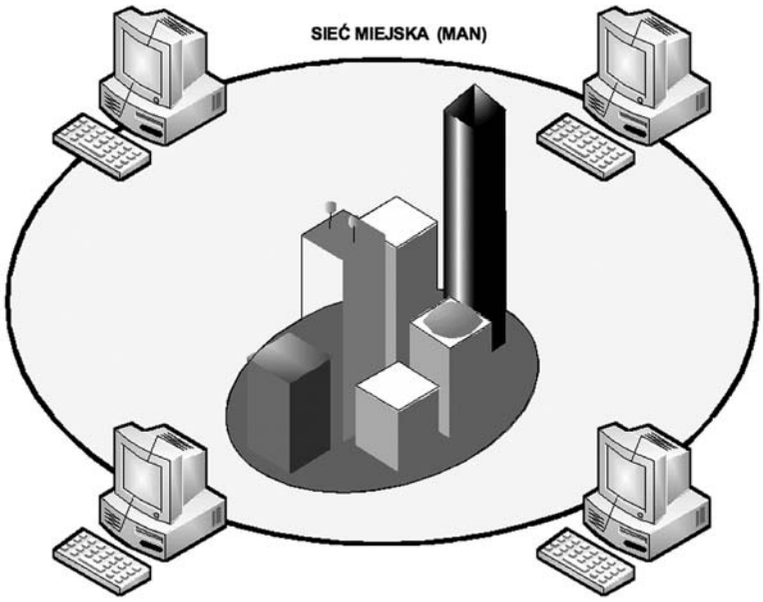
Sieć lokalna LAN (ang. *Local Area Network*) obejmuje stosunkowo niewielki obszar i zwykle łączy urządzenia sieciowe w ramach jednego domu, biura, budynku (rys. 5).



Rysunek 5.
Lokalna sieć komputerowa (LAN)

Sieć MAN

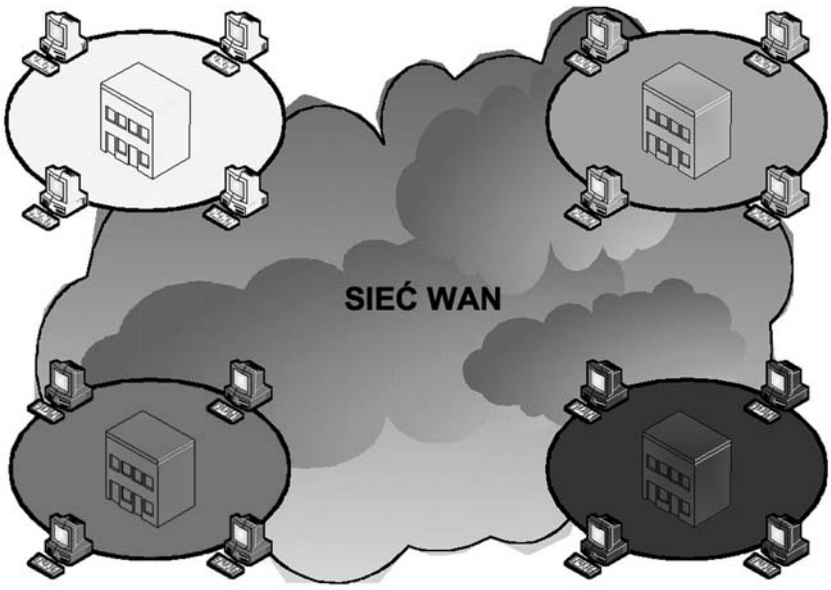
Sieć miejska MAN (ang. *Metropolitan Area Network*) jest siecią, która łączy sieci LAN i urządzenia komputerowe w obrębie danego miasta. Zasięg tej sieci zawiera się zwykle w przedziale od kilku do kilkudziesięciu kilometrów (rys. 6).



Rysunek 6.
Miejska sieć komputerowa (MAN)

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 (rys. 7).



Rysunek 7.
Rozległa sieć komputerowa (WAN)

3 MODELE SIECIOWE

Model odniesienia ISO/OSI

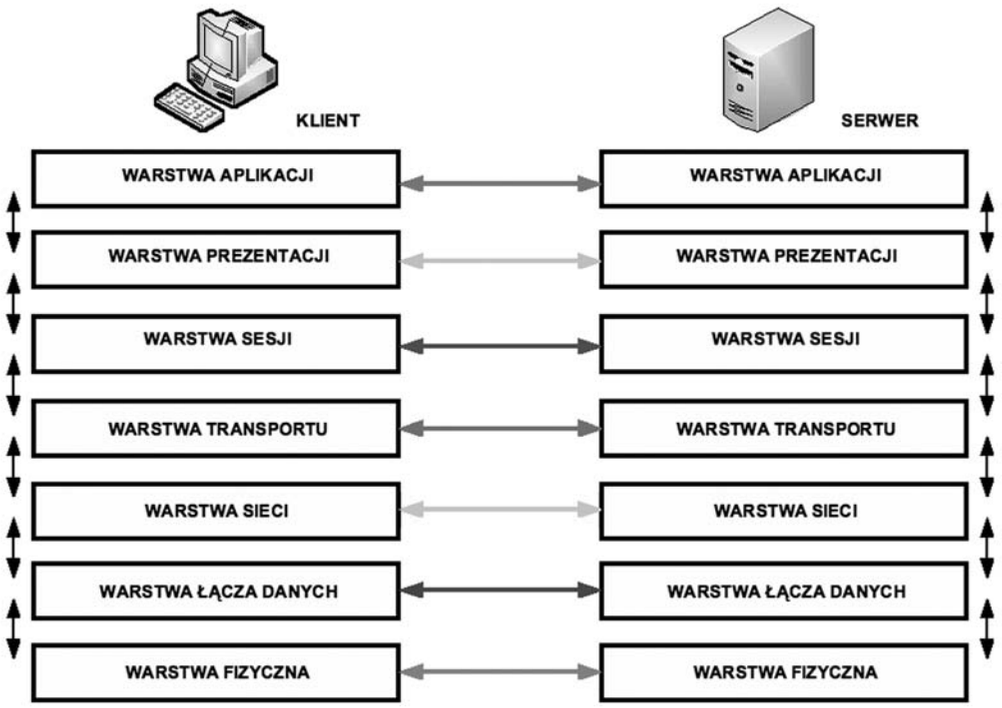
Model odniesienia ISO/OSI (ang. *The International Organization for Standardization/Open Systems Interconnection*) – patrz rys. 8 – został opracowany, aby określić wymianę informacji pomiędzy połączonymi w sieć komputerami różnych typów. Składa się on z siedmiu warstw.

Rysunek 8.
Referencyjny model odniesienia ISO/OSI

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 łącza danych** (ang. *data link layer*) – zapewnia niezawodne przesyłanie danych po fizycznym medium transmisyjnym. Warstwa to jest 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.).

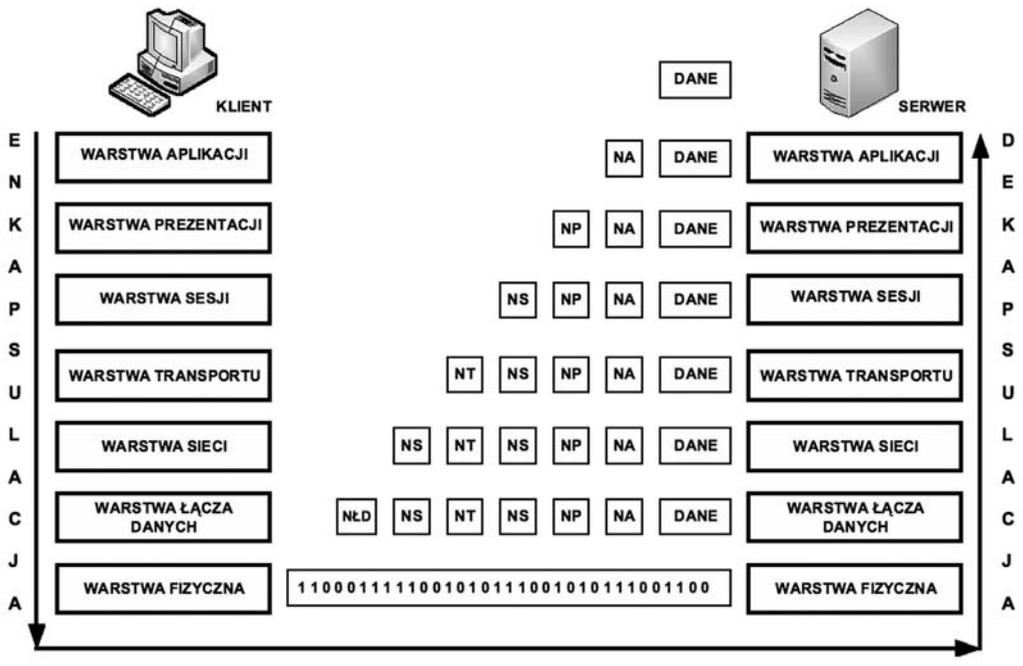
Współpraca warstw w modelu ISO/OSI

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.



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

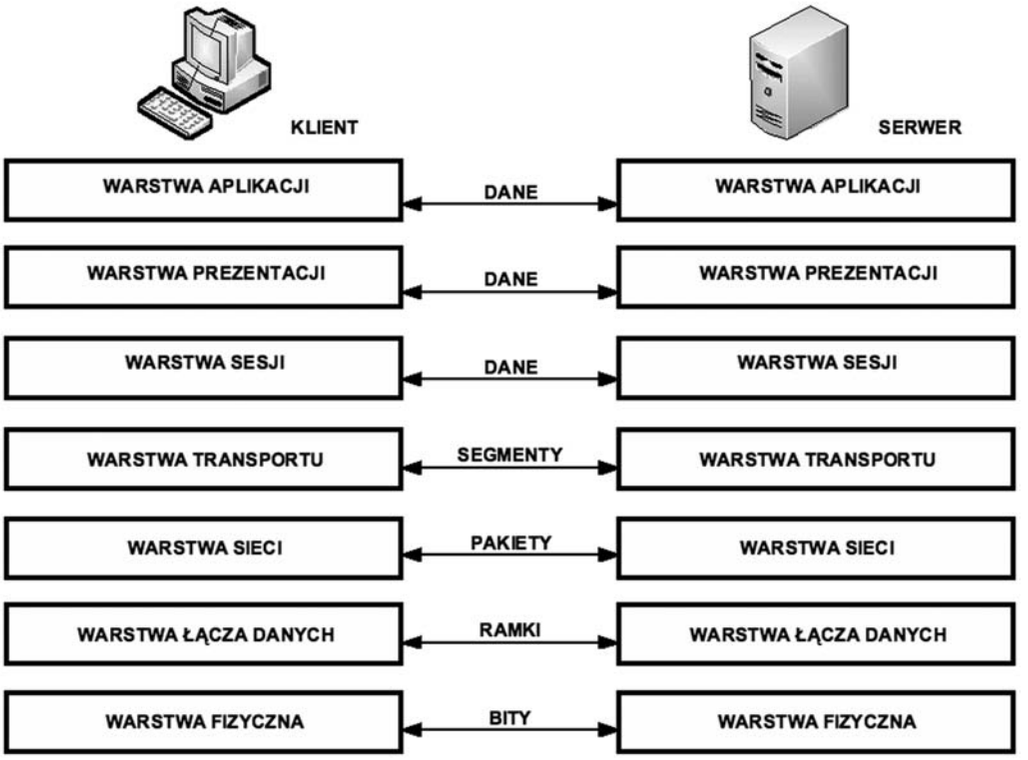
Enkapsulacja (dekapsulacja) danych



Rysunek 10.
Proces enkapsulacji i dekapsulacji danych

Enkapsulacja (dekapsulacja) danych jest procesem zachodzącym w kolejnych warstwach modelu ISO/OSI. **Proces enkapsulacji** oznacza dokładanie dodatkowej informacji (**nagłówka**) 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



Rysunek 11.
Jednostki informacji w poszczególnych warstwach w modelu odniesienia ISO/OSI

W poszczególnych warstwach w modelu odniesienia ISO/OSI przechodzące dane noszą nazwę **jednostek danych protokołu PDU** (ang. *Protocol Data Unit*). 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 jedynki). Jednostki te w poszczególnych warstwach różnią się częścią nagłówkową.

Model TCP/IP

Rysunek 12.
Model sieciowy 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. *Defence Advanced Research Projects Agency*). Model TCP/IP składa się z czterech warstw.

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 transportowe 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 AKTYWNE I PASYWNE URZĄDZENIA SIECIOWE

Karta sieciowa

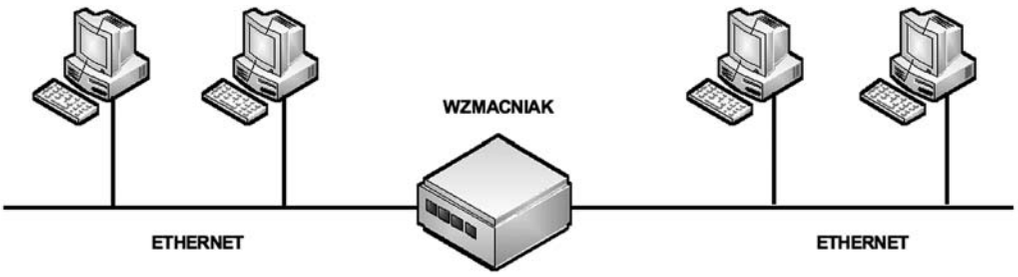
Rysunek 13.
Karty sieciowe

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.

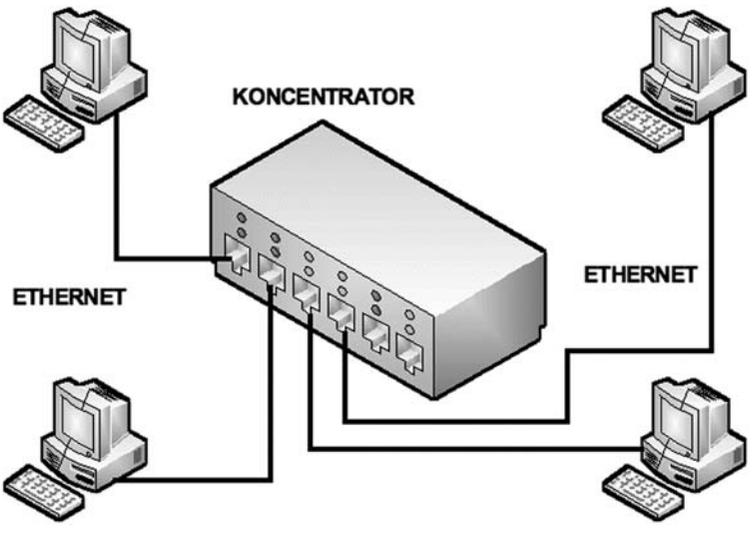
Wzmacniak



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 jednakowej 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

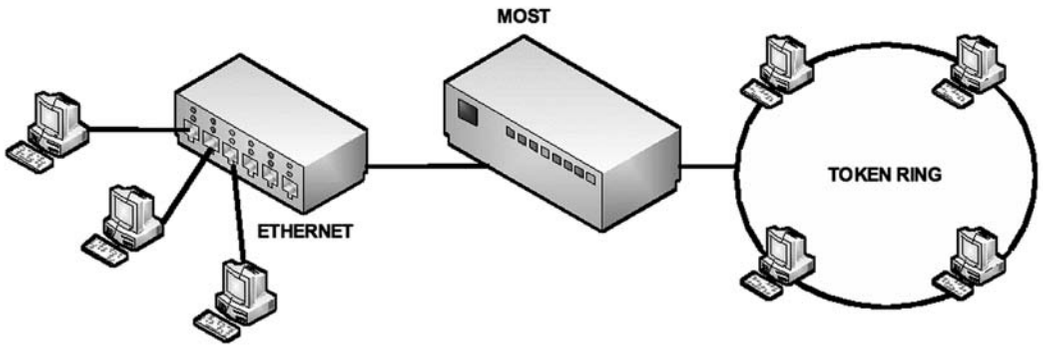


Rysunek 15.
Przykład zastosowania koncentratora

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 nale-

ży 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.

Most

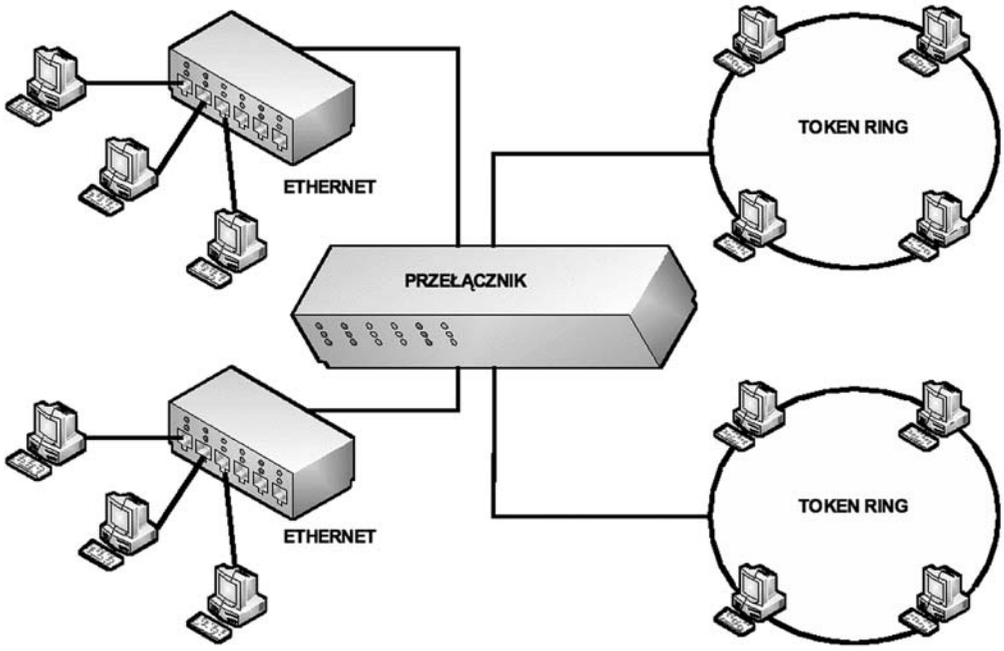


Rysunek 16.
Przykład zastosowania mostu

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 segmentu 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

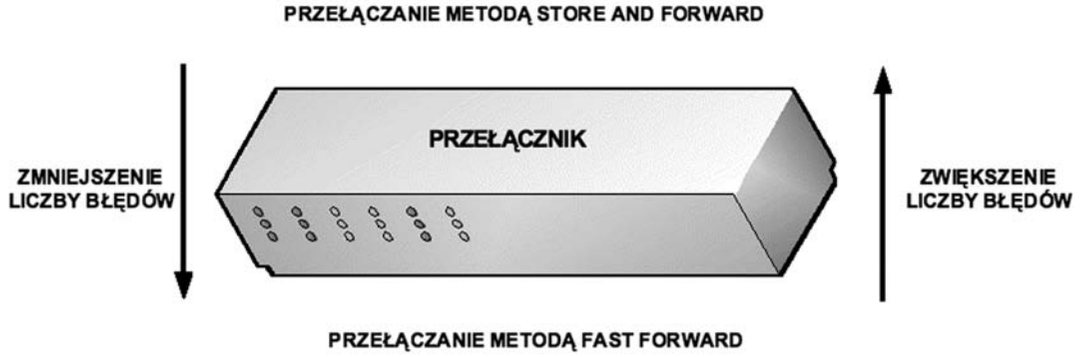
Nowoczesne inteligentne przełączniki mogą pracować w trzech trybach przełączania: fast forward (cut through), store and forward i fragment free (patrz rys. 18).

Tryb **cut through** oznacza, że odebrane ramki są wysyłane natychmiast po odczytaniu adresu docelowego na odpowiedni port, niezależnie od tego, czy w trakcie transmisji ramki pojawi się błąd lub kolizja.

W trybie **store and forward** każda ramka jest sprawdzana pod względem poprawności – eliminowane są wszystkie błędne ramki danych czy też biorące udział w kolizjach. Wadą tego trybu są duże opóźnienia w transmisji, a zaletą – duża niezawodność pracy.

W trybie **fragment free** przełącznik odczytuje pierwsze 64 bajty ramki i podejmuje decyzję co do jej losu. Po odczytaniu 64 bajtów ma już informację, czy wystąpiła kolizja, i może odrzucić takie ramki, nie wczytując ich dalszego ciągu.

Inteligentne przełączanie polega na tym, że standardowo urządzenie pracuje w trybie fast forward, a gdy liczba błędów przekracza kilkanaście na sekundę, zaczyna automatycznie stosować metodę store and forward. Tryb fragment free jest kompromisem pomiędzy wspomnianymi wyżej metodami, zapewnia szybsze przełączanie niż w metodzie store and forward i mniejszą liczbę błędów niż w fast forward.



Rysunek 18.
Metody przełączania ramek

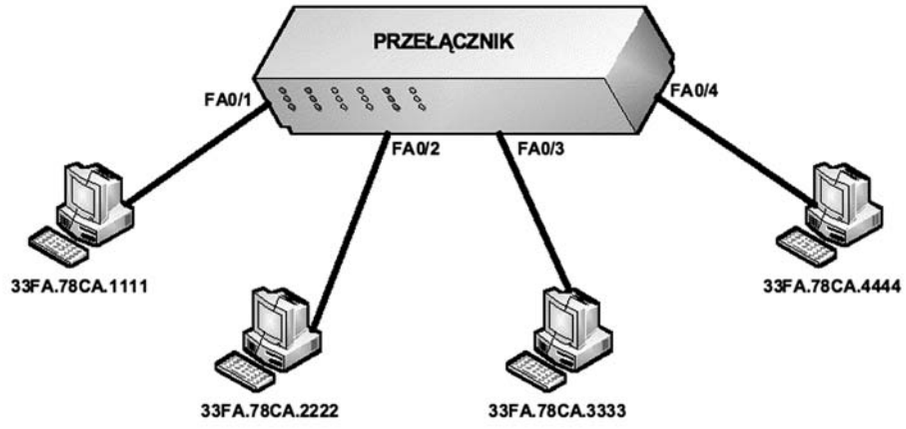
Tablica adresów MAC przechowywana jest w pamięci skojarzeniowej (asocjacyjnej). Dla każdego portu przełącznika kojarzony jest adres MAC podłączonego urządzenia sieciowego (patrz rys. 19).

Router

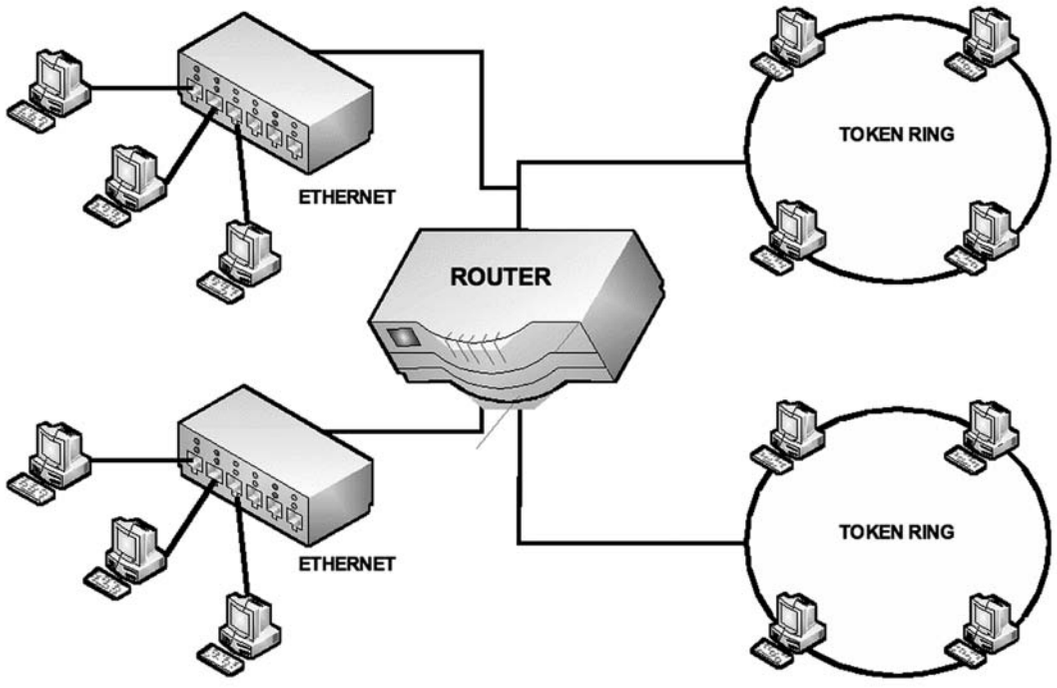
Router służy do zwiększania fizycznych rozmiarów sieci poprzez łączenie jej segmentów. Urządzenie to wykorzystuje logiczne adresy hostów w sieci. Ponieważ komunikacja w sieci jest oparta na logicznych adresach odbiorcy i nadawcy, przesyłanie danych i informacji jest niezależne od fizycznych adresów urządzeń. Oprócz filtracji pakietów pomiędzy segmentami, router określa optymalną drogę przesyłania danych po sieci między nadawcą i odbiorcą. Dodatkowo eliminuje on pakiety bez adresata i ogranicza dostęp określonych użytkow-

ników do wybranych segmentów czy komputerów sieciowych. Router jest konfigurowalny, umożliwia sterowanie przepustowością sieci oraz zapewnia pełną izolację pomiędzy segmentami.

TABLICA ADRESÓW MAC			
FA0/1	FA0/2	FA0/3	FA0/4
33FA.78CA.1111	33FA.78CA.2222	33FA.78CA.3333	33FA.78CA.4444

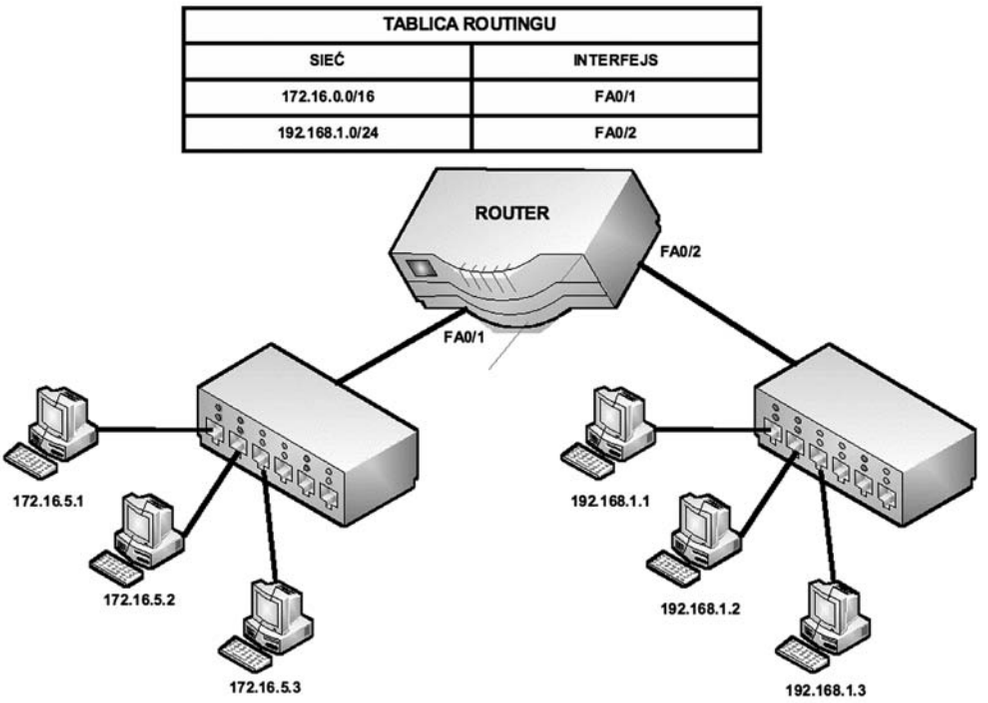


Rysunek 19.
Przykład tablicy adresów MAC



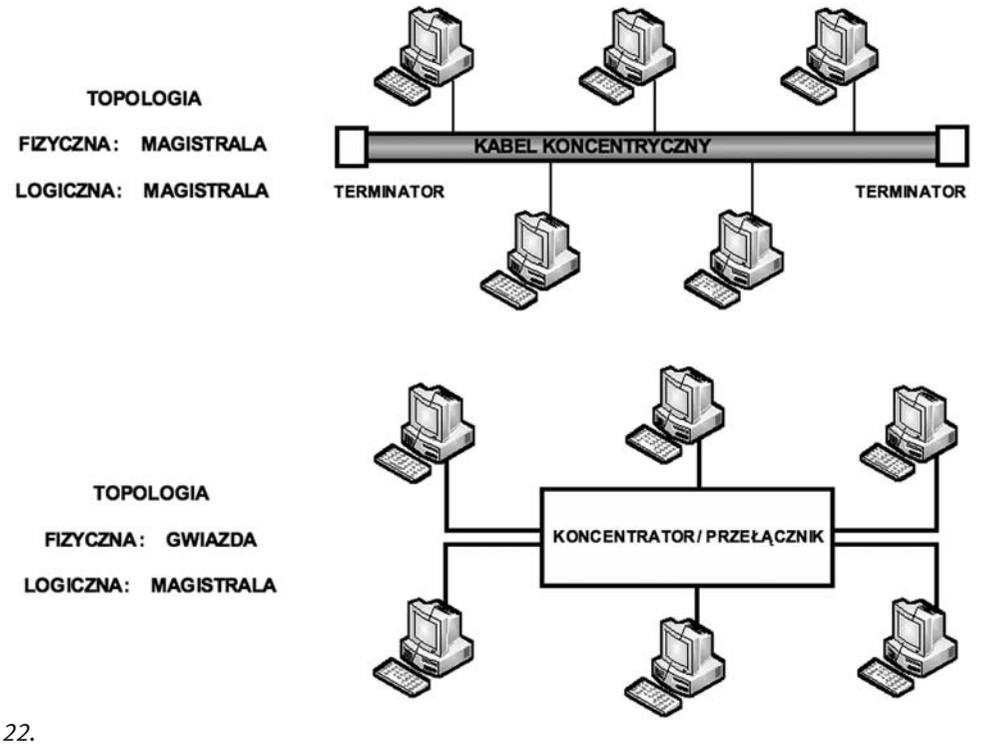
Rysunek 20.
Przykład zastosowania routera

Tablica routingu (ang. *routing table*) jest miejscem, w którym przechowywane są informacje o adresach logicznych sieci lub podsieci, maskach oraz interfejsach wyjściowych (ethernetowych lub szeregowych).



Rysunek 21.
Przykład tablicy routingu

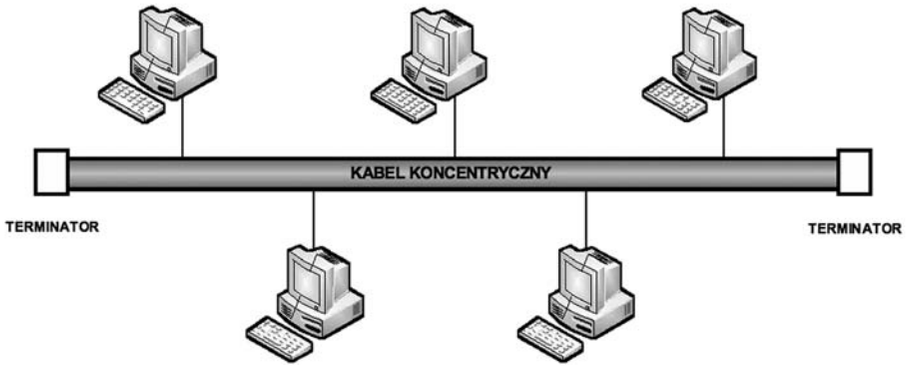
5 TOPOLOGIE FIZYCZNE I LOGICZNE



Rysunek 22.
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.

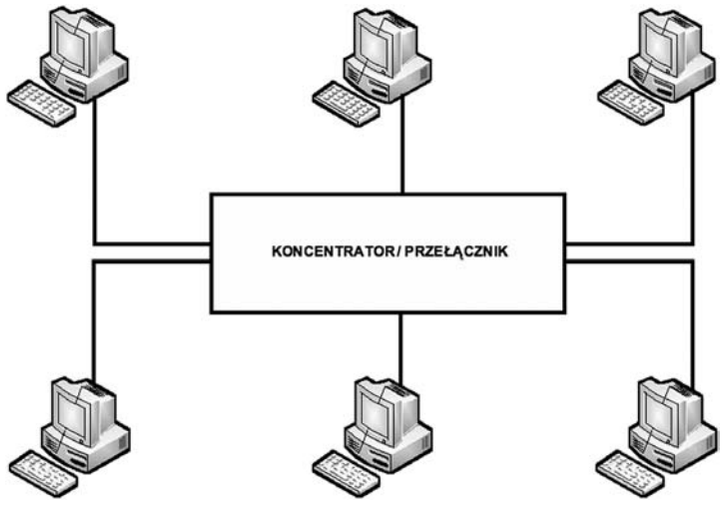
Topologia magistrali



Rysunek 23.
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.

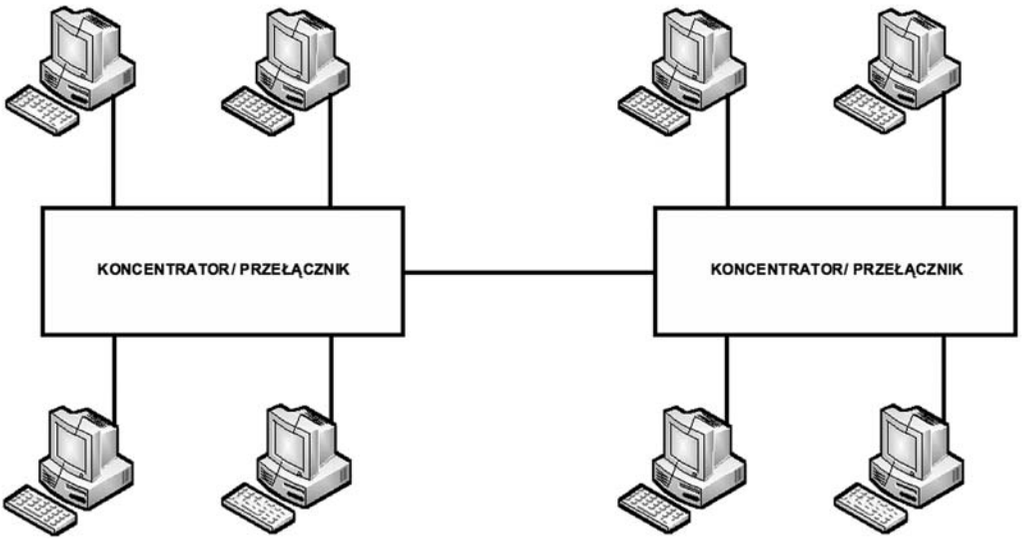
Topologia gwiazdy



Rysunek 24.
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 całkowitą długość okablowania, czyli koszty założenia sieci. Poważniejszy problem wynika z centralnego koncentratora lub przełącznika - ich awaria powoduje awarię całej sieci.

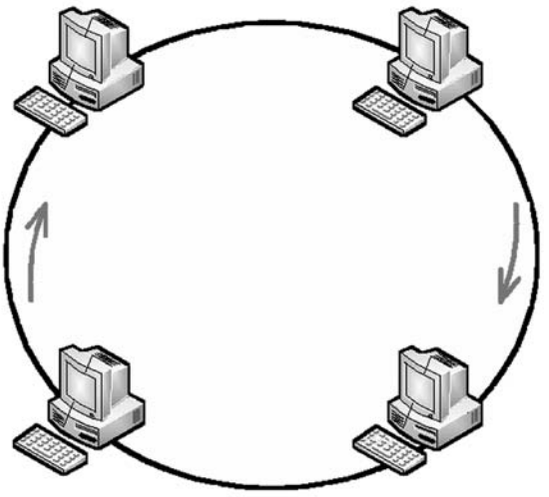
Topologia rozszerzonej gwiazdy



Rysunek 25.
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.

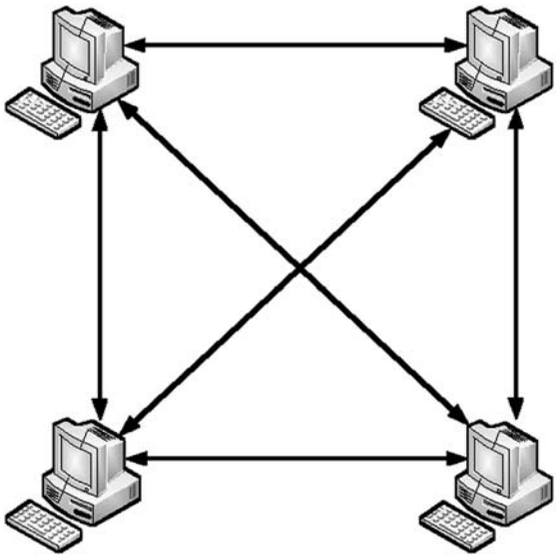
Topologia pierścienia



Rysunek 26.
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 (dołączenie, odłączenie urządzenia sieciowego) wymaga wyłączenia całej sieci.

Topologia siatki



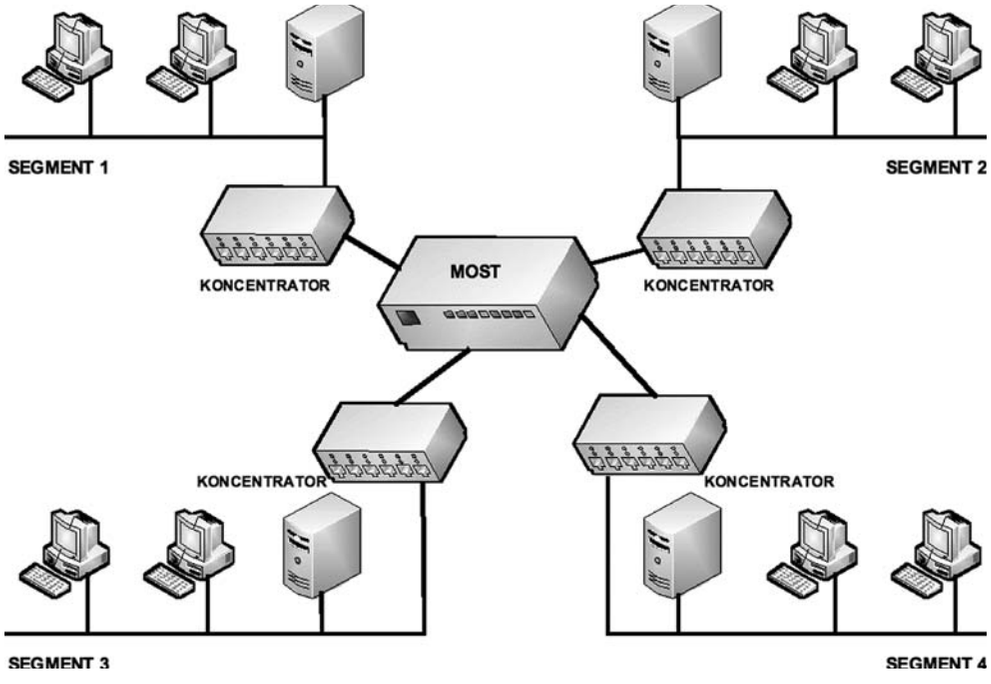
Rysunek 27.
Topologia siatki

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.

6 SEGMENTACJA I DOMENY KOLIZYJNE

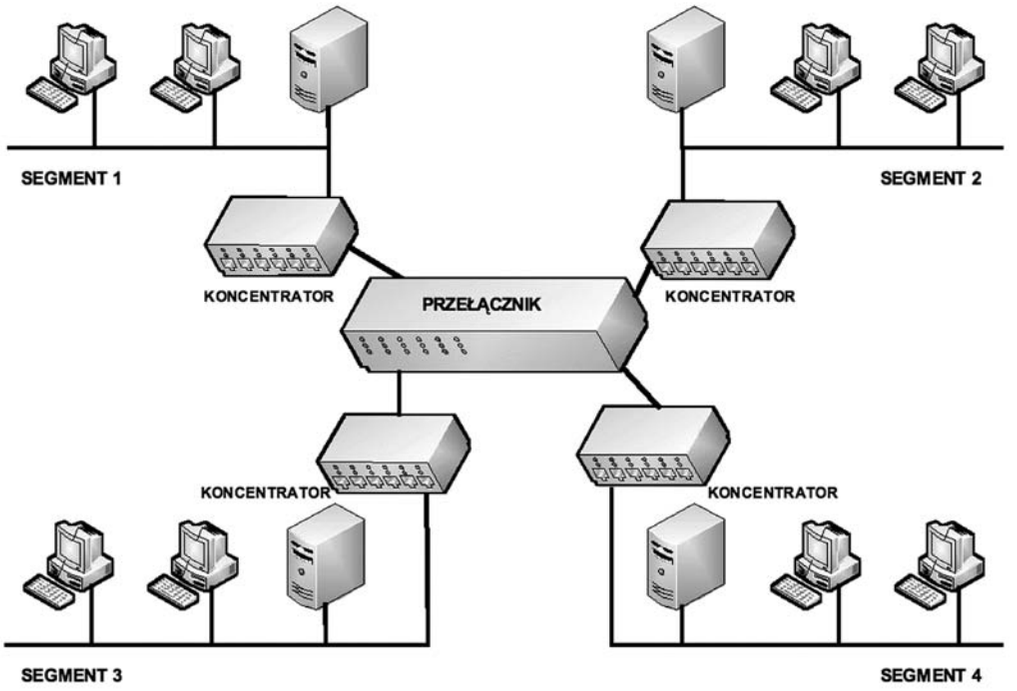
Segmentacja sieci komputerowych

Segmentacja polega na podziale sieci na kilka mniejszych części. Przy zastosowaniu segmentów oddzielonych od siebie mostami, przełącznikami czy routerami najintensywniej komunikujące się stacje robocze nie

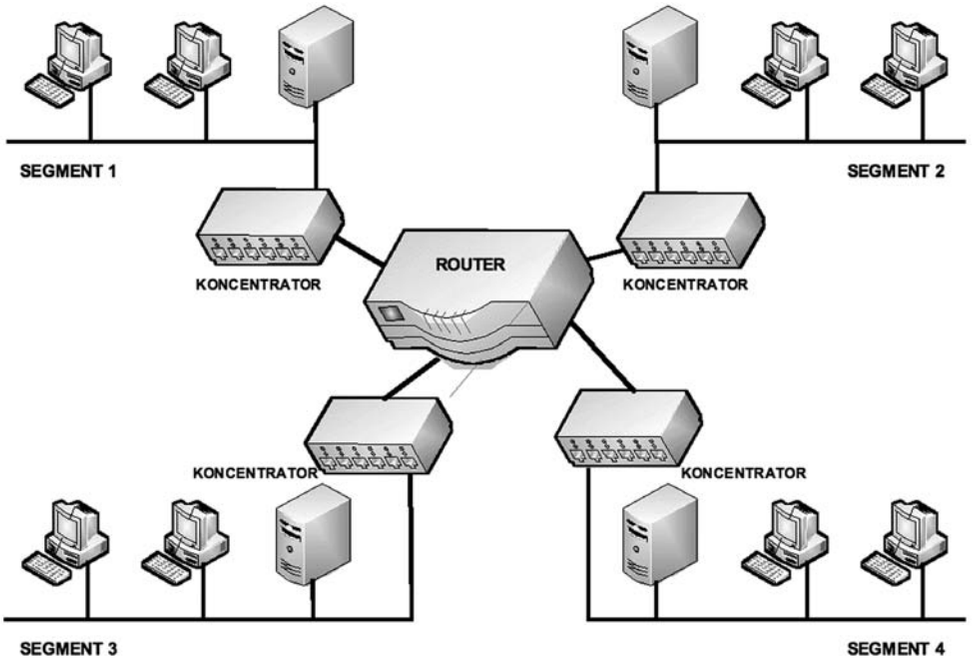


Rysunek 28.
Przykład segmentacji za pomocą mostu sieciowego

przeszkadzają sobie wzajemnie w pracy. Dzięki urządzeniom potrafiącym inteligentnie zatrzymać zbędny ruch sieć zostaje zrównoważona i znacznie odciążona. Na poniższych rysunkach przedstawiono przykładowe segmentacje sieci komputerowych.



Rysunek 29.
Przykład segmentacji za pomocą przełącznika



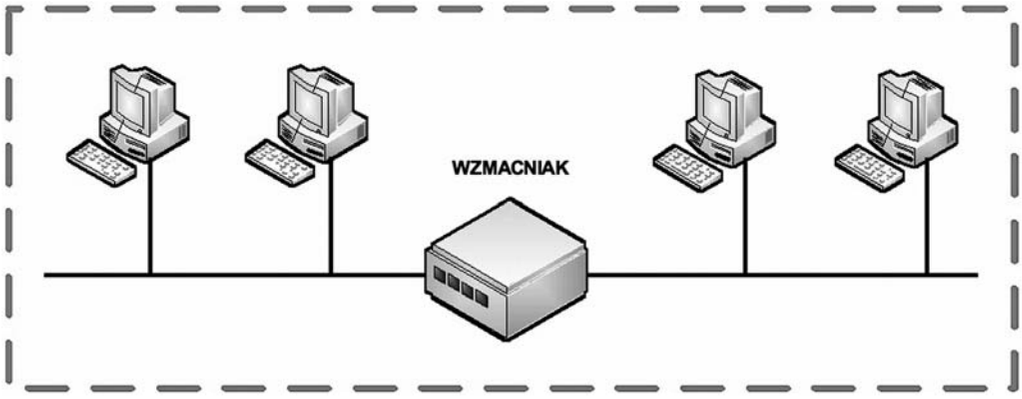
Rysunek 30.
Przykład segmentacji za pomocą routera

Domeny kolizyjne

W sieciach z technologią Ethernet stacje robocze wysyłają dane w **trybie rozgłoszeniowym** (*broadcast*). Każda stacja transmituje sygnał do wszystkich innych, stacje wsłuchują się w rozsyłane dane i odbierają tylko pakiety przeznaczone dla siebie. Dużym zagrożeniem są sztormy broadcastowe, powstające, gdy komputer cy-

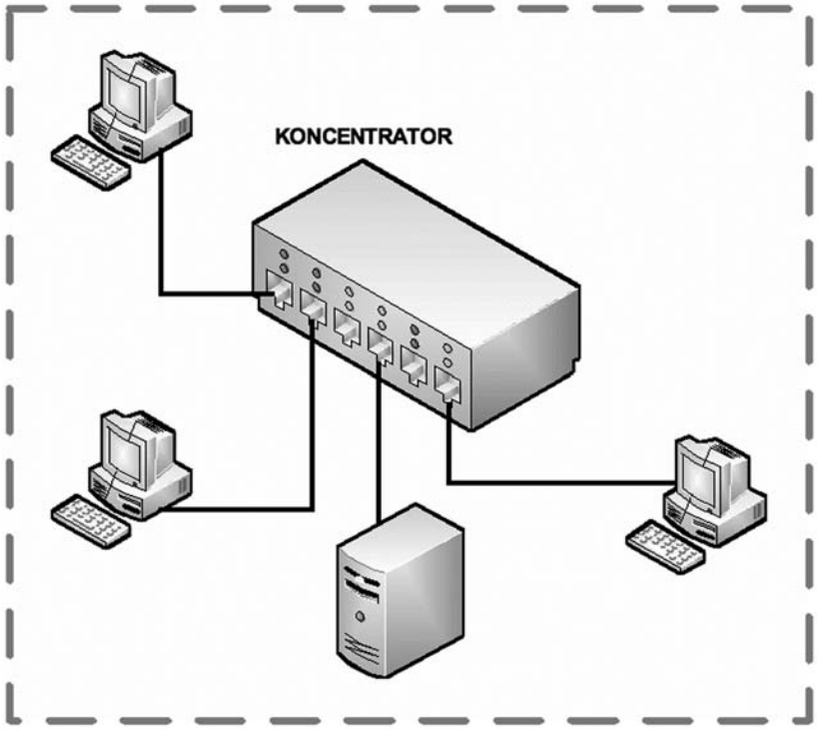
klicznie wysyła odpowiedzi na pytanie krążące w sieci w nieskończoność. Następuje wtedy nagromadzenie wysyłanych pakietów, co prowadzi do zatorów w sieci.

Problemem też jest zjawisko **kolizji**, zachodzące wówczas, gdy dwie lub więcej stacji roboczych jednocześnie zgłoszą chęć nadawania informacji. Zadaniem administratora sieci jest zadbanie, aby kolizji i zatorów było jak najmniej, a komunikujący się użytkownicy nie obciążali całej sieci. Na poniższych rysunkach zaprezentowano przykłady domen kolizyjnych.



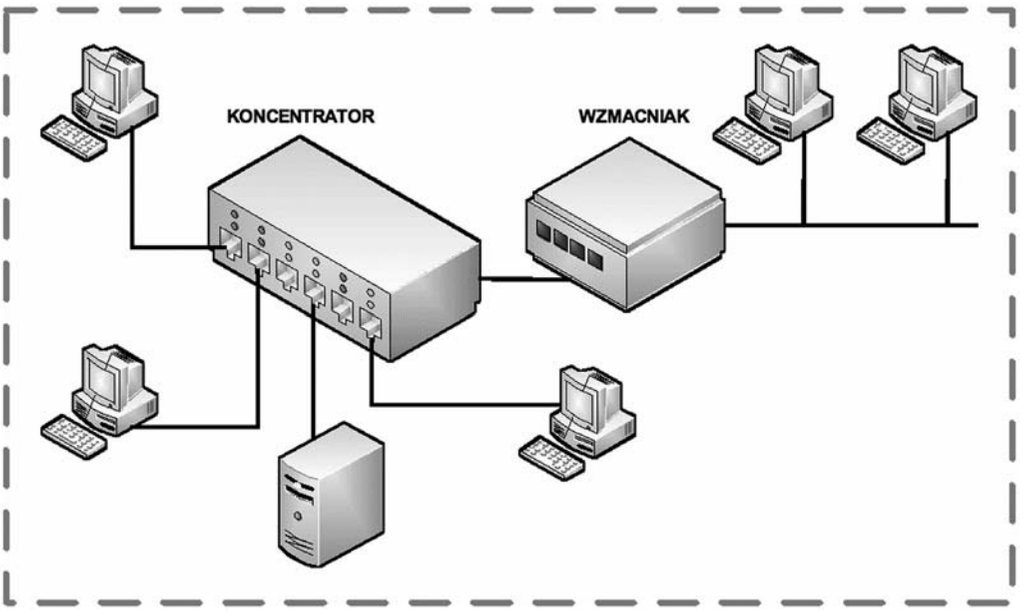
Rysunek 31.
Powiększenie domeny kolizyjnej przy zastosowaniu wzmacniaka

Wszystkie podłączone do koncentratora urządzenia sieciowe stanowią jedną domenę kolizyjną, gdyż koncentrator pracuje w pierwszej warstwie modelu odniesienia ISO/OSI (warstwie fizycznej) i nie potrafi filtrować ramek po adresach MAC.



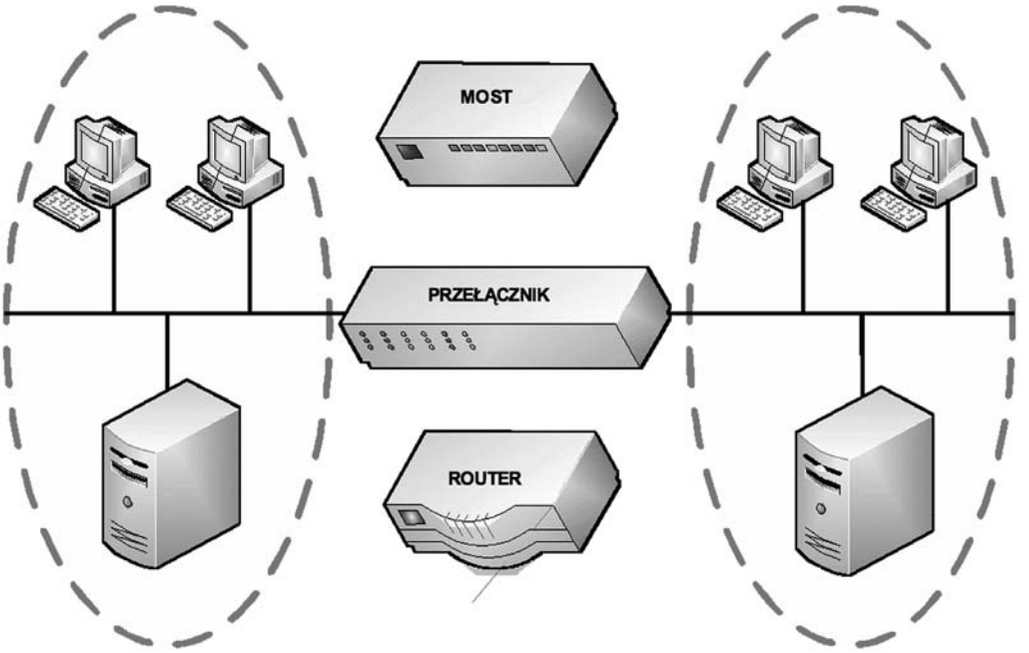
Rysunek 32.
Powiększenie domeny kolizyjnej przy zastosowaniu koncentratora

Zarówno urządzenia sieciowe podłączone do koncentratora jak i wzmacniaka stanowią jedną wielką domenę kolizyjną.



Rysunek 33.
Powiększenie domeny kolizyjnej przy wspólnym zastosowaniu koncentratora i wzmacniaka

Przy zastosowaniu urządzeń sieciowych warstwy łącza danych (mosty, przełączniki) lub warstwy sieciowej (routery) łączone ze sobą sieci stanowią osobne domeny kolizyjne. Jest to bardzo pożądane rozwiązanie.



Rysunek 34.
Przykłady użycia urządzeń sieciowych nie powiększających domen kolizyjnych

7 PRZEWODOWE MEDIA TRANSMISYJNE

System AWG

Średnica kabli jest zazwyczaj mierzona przy użyciu systemu American Wire Gauge (znanego również jako Brown & Sharpe Wire Gauge). AWG jest standardem używanym do pomiarów średnicy kabli miedzianych i alu-

miniowych w USA. Typowe kable sieciowe mają średnicę z przedziału od 12 do 26 AWG. Im niższy numer wskaźnika, tym grubszy przewód. Grubszy przewód charakteryzuje się mniejszą opornością i może przenieść więcej prądu, co daje lepszy sygnał na dłuższych odległościach.

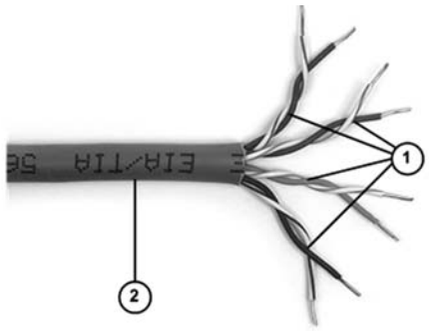
Tabela 1.
Numery AWG i odpowiadające im średnice kabli skrętkowych

nr AWG	przekrój [mm²]	nr AWG	przekrój [mm²]
1	42.40	16	1.31
2	33.60	17	1.04
3	26.60	18	0.823
4	21.20	19	0.6530
5	16.80	20	0.5190
6	13.30	21	0.4120
7	10.60	22	0.3250
8	8.35	23	0.2590
9	6.62	24	0.2050
10	5.27	25	0.1630
11	4.15	26	0.1280
12	3.31	27	0.1020
13	2.63	28	0.0804
14	2.08	29	0.0646
15	1.65	30	0.0503

Powłoki kabli miedzianych
Rodzaje powłok kabli miedzianych:

1. Kable w powłoką **PVC** (*polyvinyl chloride* – polichlorek winylu) w przypadku pożaru ograniczają widoczność do 10%, co znacznie utrudnia poruszanie się w ciągach komunikacyjnych. Dodatkowo substancje wydzielane w trakcie spalania są szkodliwe dla organizmu. Powinny być stosowane tylko na zewnątrz budynków.
2. Kable z powłoką **LS0H** (*Low Smoke Zero Halogen*) nie wydzielają dymu (uzyskujemy przez to około 90% widoczności w trakcie pożaru) ani trujących halogenków. Mogą być stosowane wewnątrz budynków.
3. Kable z powłoką **LSFR0H** (*Low Smoke Fire-Resistant Zero Halogen*) dodatkowo mają właściwości samogasnące – po zniknięciu źródła ognia przewód przestaje się palić. Mogą być stosowane wewnątrz budynków.

Skrętka UTP

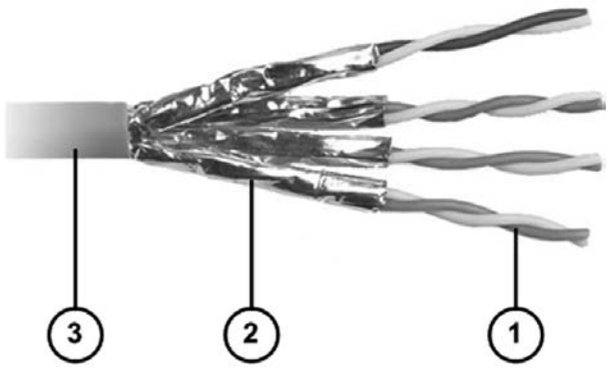


1 - cztery pary skrętek
2 - powłoka zewnętrzna

Rysunek 35.
Skrętka nieekranowana

Skrętka nieekranowana UTP (ang. *Unshielded Twisted Pair*) to przeważnie cztery pary przewodów w jednej osłonie. Każda para jest skręcona ze zmiennym splotem (1 zwój na 6-10 cm) chroniącym transmisję przed oddziaływaniem otoczenia, jak: silniki, przekaźniki czy transformatory. Przepustowość skrętki jest zależna od tzw. kategorii. Skrętka kategorii 1 to kabel telefoniczny, kategorii 2 – jest przeznaczona do transmisji danych z szybkością 4 Mb/s, kategorii 3 – do transmisji o przepustowości do 10 Mb/s, kategorii 4 – do 16 Mb/s, a kategorii 5 – do ponad 100 Mb/s. Maksymalna długość połączeń dla UTP wynosi 100 m (długość ta jest limitowana przez minimalną długość ramki i szybkość propagacji sygnałów w medium oraz opóźnienia wnoszone przez urządzenia sieciowe).

Skrętka STP

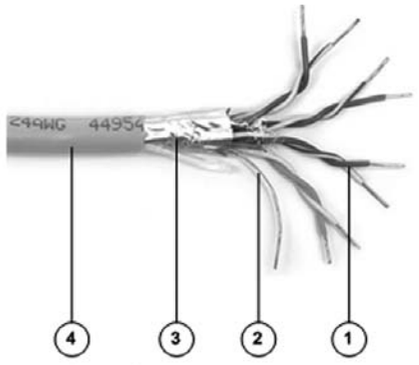


1 – cztery pary skrętek
2 – ekran z folii aluminiowej
3 – powłoka zewnętrzna

Rysunek 36.
Skrętka ekranowana

Skrętka ekranowana STP (ang. *Shielded Twisted Pair*) ma miedziany oplot, osłonę z folii pomiędzy parami przewodów i dookoła każdego z nich. Przewody są skręcone. To wszystko zapewnia wysoki stopień odporności na zewnętrzne pola elektromagnetyczne. Maksymalna długość połączeń dla STP wynosi 250 m.

Skrętka FTP

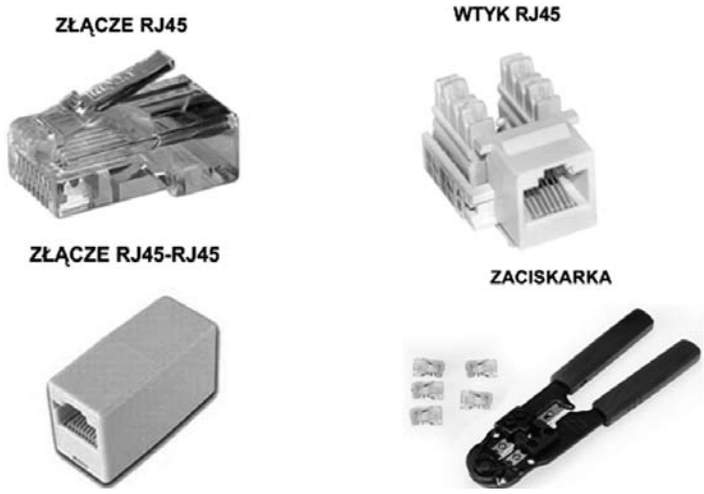


1 – cztery pary skrętek
2 – przewód uziemiający
3 – folia ekranująca
4 – powłoka zewnętrzna

Rysunek 35.
Skrętka foliowana

Skrętka foliowana FTP (ang. *Foiled Twisted Pair*) jest odmianą kabla będącego skrzyżowaniem UTP z STP. Kabel FTP to skrętka UTP otoczona aluminiową folią ekranującą z przewodem lub bez przewodu uziemiającego.

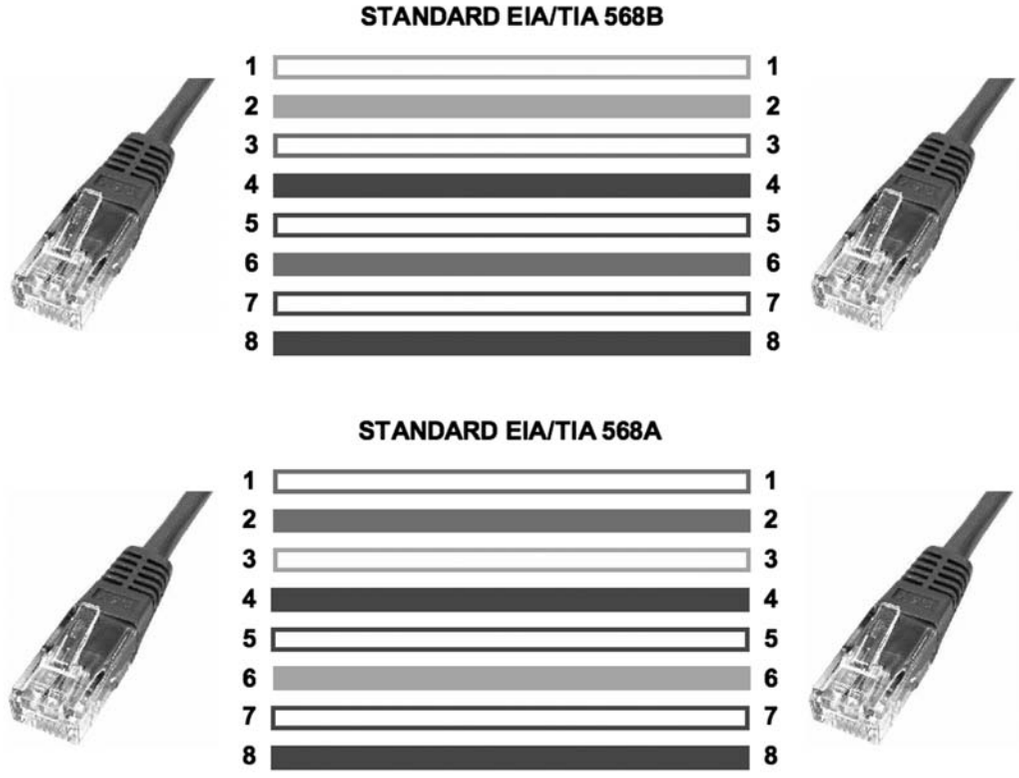
Złącza dla kabli skrętkowych



Rysunek 36.
Złącza dla kabli skrętkowych

Złącza dla kabli skrętkowych wykonuje się w oparciu o następujące przykładowe standardy: 10BaseT, 100BaseTX, 1000BaseT. Złącze RJ45 jest terminowane na końcach kabla skrętkowego. Wtyk RJ45 jest instalowany w ścianie i krosownicy. Przejściówka RJ45-RJ45 jest stosowana w przypadku przedłużenia kabla skrętkowego. Aby zaterminować złącze RJ45 należy użyć odpowiedniej zaciskarki.

Normy kabli skrętkowych



Rysunek 37.
Standardy terminowania kabli skrętkowych

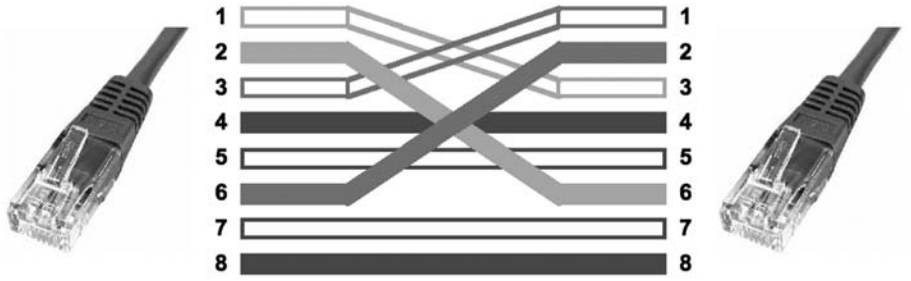
Istnieją dwa standardy kabli skrętkowych: EIA/TIA 568B oraz EIA/TIA 568A. Różnią się one kolejnością zaterminowanych żył. W standardzie EIA/TIA 568B kolejność ta jest następująca: 1 – żyła biało-pomarańczowa, 2 – żyła pomarańczowa, 3 – żyła biało-zielona, 4 – żyła niebieska, 5 – żyła biało-niebieska, 6 – żyła zielona, 7 – żyła biało-brązowa, 8 – żyła brązowa. Natomiast zgodnie ze standardem EIA/TIA 568A kolejność żył powinna być następująca: 1 – żyła biało-zielona, 2 – żyła zielona, 3 – żyła biało-pomarańczowa, 4 – żyła niebieska, 5 – żyła biało-niebieska, 6 – żyła pomarańczowa, 7 – żyła biało-brązowa, 8 – żyła brązowa.

Kabel prosty

Rysunek 38.
Przykład zaterminowania kabla prostego według normy EIA/TIA 568B

Kabel prosty (ang. *straight-through cable*) charakteryzuje się tym, że oba jego złącza RJ45 są tak samo zaterminowane. Wykorzystywany jest przy połączeniach typu: przełącznik – router, koncentrator – router, przełącznik – komputer PC, koncentrator – komputer PC.

Kabel krosowy



Rysunek 39.
Przykład zaterminowania kabla krosowego według normy EIA/TIA 568B

Kabel krosowy (ang. *crossover cable*) charakteryzuje się tym, że dwie jego pary są zamienione miejscami – pin nr 1 w miejsce pinu nr 3 a pin nr 2 w miejsce pinu nr 6. Wykorzystywany jest przy połączeniach typu: przełącznik – przełącznik, przełącznik – koncentrator, koncentrator – koncentrator, router – router, komputer PC – komputer PC, komputer PC – router (interfejs ethernetowy).

Kabel konsolowy

Rysunek 40.
Przykład zaterminowania kabla konsolowego według normy EIA/TIA 568B

Kabel konsolowy (ang. *rollover cable*) charakteryzuje się tym, że wszystkie jego pary są zamienione miejscami – pin nr 1 w miejsce pinu nr 8, pin nr 2 w miejsce pinu nr 7 itd. Wykorzystywany jest przy połączeniach typu: komputer PC (terminal) – router (port konsoli), komputer PC (terminal) – przełącznik (port konsoli).

Budowa włókna światłowodowego

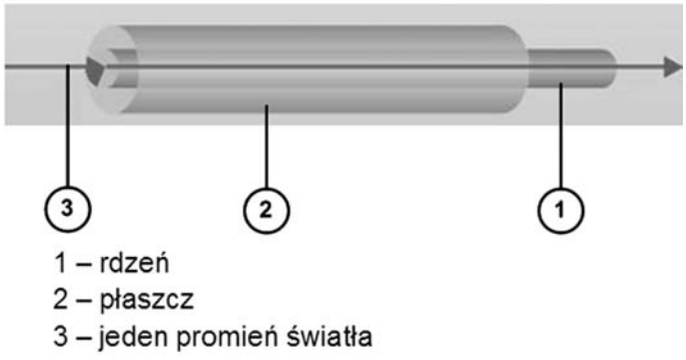
Światłowód to włókno szklane z centralnie umieszczonym rdzeniem przewodzącym światło, otoczonym cylindrycznym płaszczem odbijającym promienie świetlne i zewnętrzną powłoką lakierniczą, nadającą włóknu odpowiednią odporność i wytrzymałość mechaniczną.

Medium transmisyjnym światłowodu jest rdzeń o kołowym przekroju, wykonany ze szkła krzemionkowego SiO2, czyli tzw. szkła kwarcowego. Płaszcz otaczający rdzeń jest wykonany z czystego szkła kwarcowego, natomiast sam rdzeń włókna ma domieszkę germanu i innych pierwiastków rzadkich, co zwiększa współczynnik załamania światła w rdzeniu o wielkość zależną od koncentracji domieszki - w praktyce o ok. 1 proc.

Dla częstotliwości promieni świetlnych w zakresie bliskim podczerwieni współczynnik załamania światła w płaszczu jest mniejszy niż w rdzeniu, co powoduje całkowite wewnętrzne odbicie promienia i poprowadzenie go wzdłuż osi włókna. Istotny wpływ na tłumienie światłowodu ma zanieczyszczenie jego rdzenia jonami metali, takich jak: Fe, Cu, Co, Cr, Ni, Mn, oraz jonami wodorotlenowymi OH-.

Włókna światłowodowe klasyfikuje się według ich średnicy, tłumienności, dyspersji, zakresu zmian współczynnika załamania oraz liczby prowadzonych modów (promieni wiązki świetlnej).

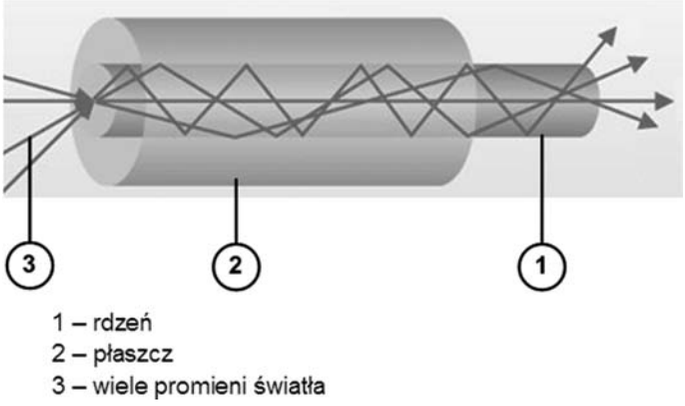
Światłowód jednodomowy



Rysunek 41.
Rozchodzenie się promienia świetlnego w światłowodzie jednomodowym

Dla **światłowodów jednomodowych SMF** (ang. *Single Mode Fiber*) do jego rdzenia jest wprowadzany tylko jeden promień światła (patrz rys. 41).

Światłowód wielodomowy



Rysunek 42.
Rozchodzenie się promieni świetlnych w światłowodzie wielodomowym

W przypadku **światłowodów wielomodowych MMF** (ang. *Multi Mode Fiber*) do jego rdzenia jest wprowadzanych wiele promieni świetlnych (patrz rys. 42).

Wymiary włókien światłowodowych

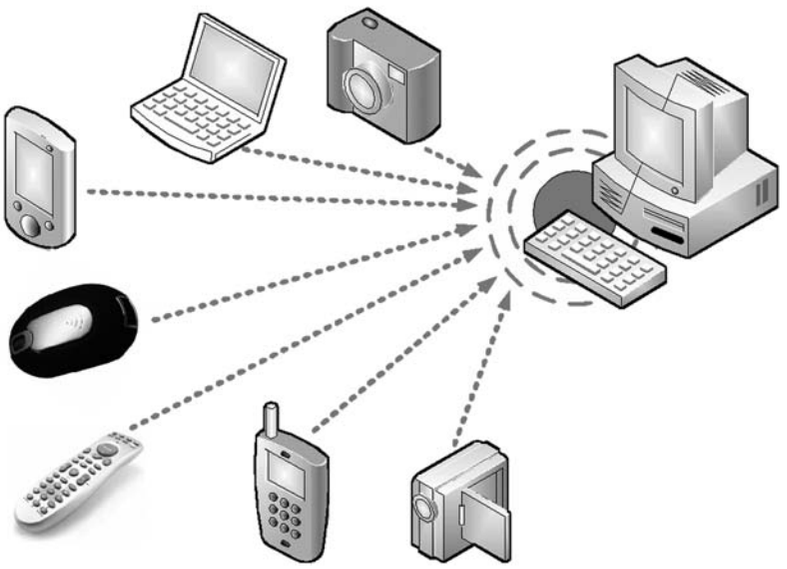
Średnicę światłowodu określa się w mikronach, podając zarówno średnicę rdzenia, jak też powłoki zewnętrznej. We współcześnie produkowanych światłowodach jednomodowych średnica rdzenia wynosi 9 μm, przy średnicy powłoki zewnętrznej do 125 μm.

W światłowodach wielomodowych o skokowym lub gradientowym współczynniku załamania światła średnica rdzenia mieści się w zakresie 50-100 μm, przyjmując typowo dwie wartości: 50 lub 62,5 μm. Dla takich światłowodów średnica zewnętrzna płaszcza zależy od struktury wewnętrznej i wynosi: 125-140 μm dla światłowodów ze współczynnikiem gradientowym oraz 125-1050 μm ze skokowym.

Najczęściej spotykana, znormalizowana średnica zewnętrzna płaszcza światłowodu wynosi 125 μm, średnica zaś płaszcza z pokryciem lakierowym 250 μm.

8 BEZPRZEWODOWE MEDIA TRANSMISYJNE

Podczerwień – IrDA



Rysunek 43.
Urządzenia wykorzystujące technologię IrDA

Technologia IrDA (ang. *Infrared Data Association*) wykorzystuje silnie skupioną wiązkę światła w paśmie podczerwieni (850 – 900 nm). Koniecznym warunkiem zastosowania tej technologii jest bezpośrednia widoczność nadajnika i odbiornika.

Właściwości technologii IrDA

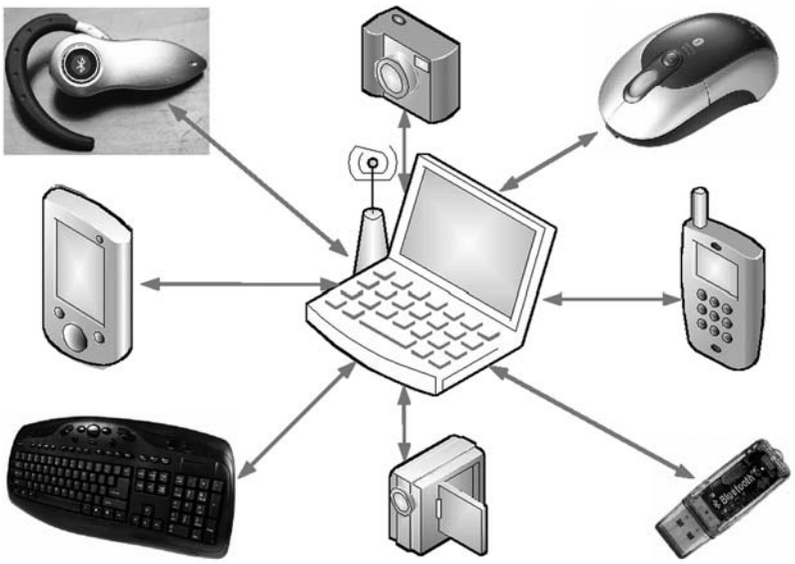
Tabela 2.
Wybrane parametry technologii IrDA

Tryb transmisji	Szybkość transmisji
Serial InfraRed SIR	2.4 - 115.2 kbps
Medium InfraRed MIR	0.576 - 1.15 Mbps
Fast InfraRed FIR	1.15 - 4 Mbps
Very Fast InfraRed VFIR	16 Mbps

Podstawowe właściwości technologii IrDA to:

- prosta i tania implementacja,
- mały pobór mocy,
- połączenie typu punkt-punkt,
- długość fali świetlnej: 850 – 900 nm,
- zasięg: do 10 metrów,
- kąt wiązki transmisji: 30.

Fale radiowe – Bluetooth



Rysunek 44.
Urządzenia wykorzystujące technologię Bluetooth

Technologia **Bluetooth** jest globalną inicjatywą bezprzewodowego dostępu radiowego grupy producentów: Ericsson, IBM, Intel, Nokia i Toshiba. Standard Bluetooth powstał w 1994 roku w Szwecji. Jego nazwa pochodzi od przydomka żyjącego w X wieku duńskiego króla Haralda I – „Blaatand" (czyli „Sinozęby").

Technologia Bluetooth jest standardem połączeń radiowych o ograniczonym zasięgu, między telefonami komórkowymi, komputerami przenośnymi, urządzeniami peryferyjnymi (klawiatury, myszy, monitory, drukarkami), a także audiowizualnymi (piloty, odbiorniki TV i radiowe). W Bluetooth stosuje się bezkierunkowe łącze radiowe o niewielkim zasięgu (do 10 m), o częstotliwościach pracy w paśmie 2,402-2,480 GHz. Możliwa jest komunikacja między różnymi urządzeniami przenośnymi (maks. 256) z przepływnością do 1 Mb/s.

Fale radiowe – Wi-Fi

Tabela 3.
Standardy sieci bezprzewodowych

Nazwa standardu	Częstotliwość radiowa	Zasięg sygnału	Maksymalna szybkość transmisji
802.11b	2.4 GHz	30 metrów	11 Mb/s
802.11a	5 GHz	30 metrów	54 Mb/s
802.11g	2.4 GHz	30 metrów	54 Mb/s
802.11n	2.4 GHz	50 metrów	540 Mb/s
802.15.1 Bluetooth	2.4 GHz	10 metrów	2 Mb/s

Sieci bezprzewodowe opierają się przede wszystkim na standardach z rodziny IEEE 802. IEEE. W tej rodzinie sieci bezprzewodowych dotyczy grupa standardów IEEE 802.11. Rodzina 802.11 obejmuje tak naprawdę trzy zupełnie niezależne protokoły skupiające się na kodowaniu (a, b, g). Pierwszym powszechnie zaakceptowanym standardem był 802.11b, potem weszły 802.11a oraz 802.11g. Standard 802.11n nie jest jeszcze oficjalnie zatwierdzony, ale coraz więcej sprzętu sieciowego jest kompatybilna z tą technologią.

Pierwszym standardem sieci radiowej był opublikowany w 1997 roku IEEE standard 802.11. Umożliwiał on transmisję z przepustowością 1 oraz 2 Mb/s przy użyciu podczerwieni bądź też pasma radiowego 2.4 GHz. Urządzenia tego typu są już praktycznie nie stosowane.

Standard 802.11b został zatwierdzony w 1999 roku. Pracuje w paśmie o częstotliwości 2.4 GHz. Umożliwia maksymalną teoretyczną szybkość transmisji danych do 11 Mb/s. Jego zasięg ograniczony jest do 30 metrów w pomieszczeniu i do 100 metrów w otwartej przestrzeni.

Standard 802.11a został zatwierdzony w 1999 roku. Pracuje w paśmie częstotliwości 5 GHz. Jego maksymalna teoretyczna przepływność sięga 54 Mb/s.

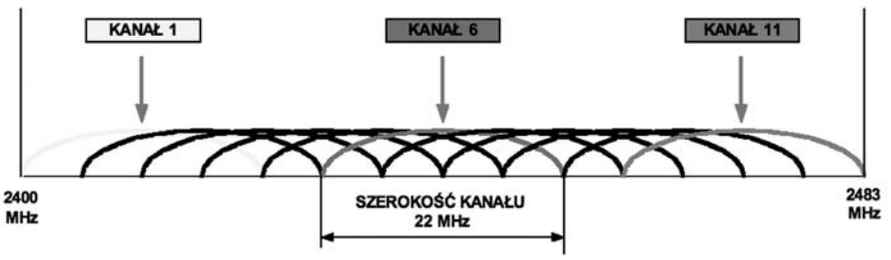
Standard 802.11g oficjalnie został zatwierdzony w 2003 roku. Pracuje podobnie jak standard 802.11g w paśmie o częstotliwości 2.4 GHz. Pozwala osiągnąć maksymalną teoretyczną szybkość transmisji danych do 54 Mb/s. Zasięg jego działania w budynku ograniczony jest do 30 metrów natomiast w przestrzeni otwartej dochodzi do 100 metrów.

Najnowszy standard 802.11n (oficjalnie zatwierdzony w 2009 roku) pracuje w paśmie radiowym o częstotliwości 2.4 GHz. Zapewnia szybkość przesyłu danych do 540 Mb/s. Został w nim również wydłużony zasięg działania do 50 metrów w pomieszczeniach.

Rysunek 45.
Przykłady urządzeń wykorzystujących technologię Wi-Fi

Technologia Wi-Fi polega na bezprzewodowej łączności w dwóch zakresach częstotliwości: 2.4 GHz oraz 5 GHz.

Kanały transmisyjne

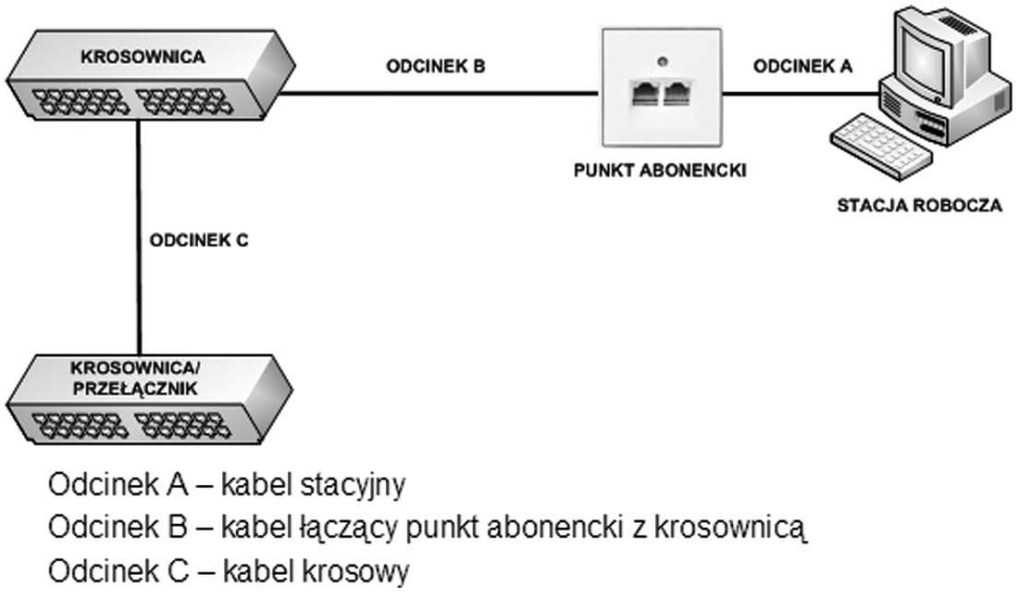


Rysunek 46.
Kanały transmisyjne

Dokładna częstotliwość stosowana w określonej sieci bezprzewodowej zależy od wykorzystywanego kanału transmisyjnego. Na przykład w USA używa się 11 kanałów, w Polsce 13, w Japonii 14 a we Francji tylko 4. Aby zachować światowy standard na całym świecie używa się tej samej numeracji kanałów, czyli kanał nr 6 w Warszawie odpowiada tej samej częstotliwości co w Tokio czy Los Angeles. W przypadku wyjazdu za granicę może wystąpić konieczność przestawienia karty sieciowej na inny kanał, aczkolwiek robią one to automatycznie. Jeśli nie mamy pewności z jakich kanałów można korzystać w danym kraju, wystarczy sprawdzić to w lokalnym urzędzie regulacyjnym. Niezależnie od tego można skorzystać z kanałów o numerach 10 i 11, które są dostępne na całym świecie (poza Izraelem).

9 OKABLOWANIE STRUKTURALNE POZIOME I PIONOWE

Okablowanie poziome



Rysunek 47.
Przykład okablowania strukturalnego poziomego

Okablowanie poziome łączy stację roboczą z lokalnym lub kondygnacyjnym punktem dystrybucyjnym. W skład okablowania strukturalnego poziomego wchodzą następujące elementy (patrz rys. 47):

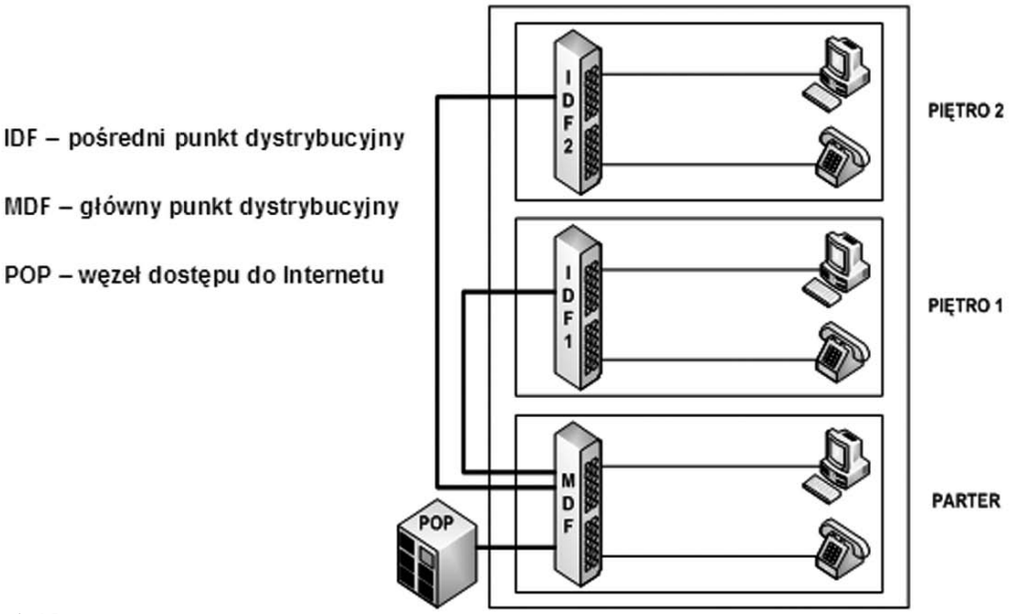
- gniazda naścienne w punktach abonenckich,
- kable połączeniowe,
- kable transmisyjne,
- panele krosowe (krosownice).

Przy projektowaniu okablowania poziomego musimy uwzględnić fakt, że odcinek pomiędzy stacją roboczą a punktem dystrybucyjnym (krosownicą, przełącznikiem) nie może przekroczyć 100 metrów (dla kabli skrętkowych). Odcinek ten składa się z następujących części:

- odcinek A – kabel stacyjny – jego maksymalna długość to 3 metry,
- odcinek B – kabel łączący punkt abonencki z krosownicą – jego maksymalna długość to 90 metrów,
- odcinek C – kabel krosowy – jego maksymalna długość to 5 metrów.

Po zsumowaniu długości wszystkich odcinków okablowania poziomego otrzymujemy wynik poniżej 100 metrów: 3 + 90 + 5 = 98.

Okablowanie pionowe



Rysunek 48.
Przykład okablowania strukturalnego pionowego

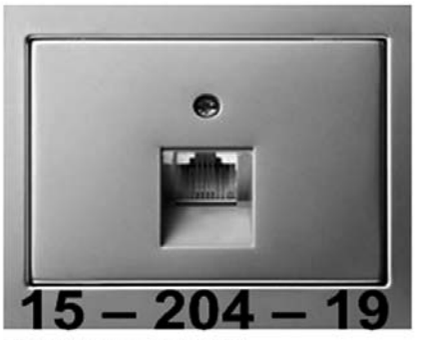
Okablowanie strukturalne pionowe łączy pośrednie punkty dystrybucyjne **IDF** (ang. *Intermediate Distribution Facility*) z głównym punktem rozdzielczym **MDF** (ang. *Main Distribution Facility*). W głównym punkcie rozdzielczym (dystrybucyjnym) znajduje się ponadto urządzenie dostępowe do sieci Internet (router, modem). Jest ono określane jako POP (ang. *Point of Presence*). Najczęściej spotykanym rozwiązaniem jest układanie tego typu okablowania w pionowych szybach pomiędzy poszczególnymi kondygnacjami budynków. Maksymalna długość okablowania strukturalnego pionowego zależy głównie od zastosowanego medium transmisyjnego. I tak:

- kabel telefoniczny (skrętka UTP kategorii 1) – 800 metrów,
- skrętka UTP/STP/FTP – 100 metrów,
- kabel światłowodowy – 2000 metrów.

Obok nomenklatury angielskojęzycznej w naszym kraju stosuje się także nazewnictwo polskie. I tak:

- MDF – PCS (Punkt Centralny Sieci).
- IDF – KPD (Kondygnacyjny punkt Dystrybucyjny).

Oznakowanie punktów abonenckich



1 – numer kondygnacji
5 – numer punktu dystrybucyjnego
2 – numer stelażu w szafie dystrybucyjnej
04 – numer krosownicy
19 – numer gniazda w krosownicy

Rysunek 49.
Przykład oznakowania punktu abonenckiego

Stosowanie się do poprawnego systemu oznakowania punktów abonenckich znacząco ułatwia lokalizację ewentualnych usterek. Ponadto właściwe oznakowanie gniazd abonenckich umożliwia szybką identyfikację fizycznej lokalizacji danej stacji roboczej w lokalnej sieci komputerowej.

LITERATURA

1. Dye M.A., McDonald R., Rufi A.W., *Akademia sieci Cisco. CCNA Exploration. Semestr 1*, WN PWN, Warszawa 2008
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

1 KONWERSJA POMIĘDZY SYSTEMAMI BINARNYM I DZIESIĘTNYM

Adresy IPv4 komputerów, a ogólniej – urządzeń sieciowych są przedstawiane jako układ czterech liczb w systemie dziesiętnym lub w systemie binarnym (dwójkowym). Zaczniemy więc zajęcia od przypomnienia tych systemów oraz algorytmów zamiany liczb między tymi systemami.

Liczbowy system pozycyjny

Systemy dziesiętny i binarny są przykładami systemu pozycyjnego. **System pozycyjny** jest metodą zapisywania liczb w taki sposób, że w zależności od pozycji danej cyfry w ciągu, oznacza ona wielokrotność potęgi pewnej liczby p uznawanej za **podstawę** danego systemu. W takiej konwencji zapisu, każda pozycja ma ściśle określoną i niezmienną wagę liczbową. System pozycyjny umożliwia również zapisywanie ułamków, przy czym liczby wymierne składają się albo ze skończonej liczby znaków, albo są od pewnego miejsca okresowe.

Na co dzień stosujemy **system dziesiętny**, zwany także **systemem dziesiątkowym**, czyli o podstawie $p = 10$. W tym systemie, na przykład liczba 539 oznacza:

$$539 = 5*100 + 3*10 + 9*1 \qquad \text{czyli} \qquad 539 = 5*10^2 + 3*10^1 + 9*10^0.$$

W informatyce jest stosowany system **dwójkowy**, zwany także **binarnym**, a więc o podstawie 2. Cyframi w tym systemie są 1 i 0 i na przykład, liczba 100101 w systemie binarnym – będziemy ją też zapisywać jako $(100101)_2$ – oznacza:

$$1*2^5 + 0*2^4 + 0*2^3 + 1*2^2 + 0*2^1 + 1*2^0$$

Ten zapis umożliwia obliczenie dziesiętnej wartości tej liczby:

$$\begin{aligned}(100101)_2 &= 1*2^5 + 0*2^4 + 0*2^3 + 1*2^2 + 0*2^1 + 1*2^0 = \\ &= 1*32 + 0*16 + 0*8 + 1*4 + 0*2 + 1*1 = \\ &= 37 = (37)_{10}\end{aligned}$$

Ogólnie, przy ustalonej podstawie p, liczby w systemie o tej podstawie są zapisywane z wykorzystywaniem cyfr $\{0, 1, 2, \ldots, p-1\}$. Liczbę w tym systemie, która ma i cyfr, oznaczamy $(c_{i-1}c_{i-2}\ldots c_2c_1c_0)_p$, gdzie c_{i-1}, c_{i-2}, ..., c_2, c_1, c_0 są cyframi tej liczby ze zbioru możliwych cyfr $\{0, 1, 2, \ldots, p-1\}$. W tym zapisie c_{i-1} jest **najbardziej znaczącą** cyfrą tej liczby, a c_0 jest **najmniej znaczącą cyfrą**. Liczba $(c_{i-1}c_{i-2}\ldots c_2c_1c_0)_p$, ma wartość dziesiętną:

$$(c_{i-1}c_{i-2}\ldots c_2c_1c_0)_p = c_{i-1}*p^{i-1} + c_{i-2}*p^{i-2} + \ldots + c_2*p^2 + c_1*p^1 + c_0*p^0$$

System pozycyjny o podstawie p charakteryzuje się następującymi cechami, które są uogólnieniem cech systemu dziesiętnego:

- system określa liczba p, będąca podstawą systemu; .
- do zapisu liczb w tym systemie służy p cyfr: 0, 1, 2, ..., $p - 1$;
- cyfry są ustawiane od najbardziej znaczącej do najmniej znaczącej pozycji;
- pozycje cyfr są numerowane od 0 poczynając od prawej strony zapisu;
- każdej pozycji odpowiada waga, równa podstawie systemu podniesionej do potęgi o wartości numeru pozycji;
- cyfry określają, ile razy waga danej pozycji uczestniczy w wartości liczby;
- wartość liczby jest równa sumie iloczynów cyfr przez wagi ich pozycji.

Zaletą systemów pozycyjnych jest łatwość wykonywania nawet złożonych operacji arytmetycznych oraz możliwość zapisu dowolnie dużej liczby.

Ćwiczenie 1. Jaki system zapisu liczb, który znasz bardzo dobrze, nie jest systemem pozycyjnym i dlaczego? Przypomnijmy tylko, że stosowano go w starożytności.

W dalekiej przeszłości, obok systemy dziesiętnego był stosowany powszechnie system **sześć dziesiątkowy**, zwany również **kopowym**. Zapewne wtedy pojawił się pomysł podziału godziny na 60 minut, a minuty na 60 sekund. Podobnie można wnioskować odnośnie miary kata pełnego, która wynosi 360°, czyli 6 x 60.

System binarny, upowszechniony w erze komputerów, ma swoje korzenie w filozoficznym systemie dwóch wartości: dobro i zło, dzień i noc, Ziemia i Niebo, kobieta i mężczyzna itp., powszechnie stosowanym w starożytnych Chinach. Bazując na tej idei, matematyczną wersję systemu dwoistego, jako systemu binarnego, przedstawił Gottfried W. Leibniz w 1703 roku, jednocześnie proponując, jak mają być wykonywane działania w tym systemie.

W informatyce, poza systemem binarnym, są wykorzystywane jeszcze systemy pochodne: ósemkowy, czyli o podstawie 8, i szesnastkowy, czyli o podstawie 16.

Zamiana reprezentacji dziesiętnej na reprezentację w innym systemie

Potrafimy zamienić liczbę dziesiętna na liczbę binarną. Odpowiedni algorytm polega na dzieleniu przez 2.

Ćwiczenie 2. Znajdź reprezentację binarną liczb dziesiętnych: 0, 1, 2, 8, 10, 20, 101, 110, 256, 1024, 10000, 1000000, 1000001.

Łatwo jest uzasadnić poprawność powyższej metody, korzystając z postaci liczby w systemie binarnym. Podobnie, korzystając z zapisu liczby w systemie o podstawie p, łatwo jest uzasadnić poprawność następującego algorytmu, który służy do zamiany liczby dziesiętnej na postać w systemie o dowolnej podstawie p.

Algorytm: 10 → *p*.
Dane: liczba dziesiętna n i podstawa systemu p.
Wynik: reprezentacja liczby n w systemie przy podstawie p.
Dopóki $n \neq 0$, wykonaj następujące dwa kroki:
1. Za kolejną cyfrę od końca (od najmniej znaczącej cyfry) przyjmij resztę z dzielenia n przez p.
2. Za nową wartość n przyjmij całkowity wynik dzielenia n przez p.

Ćwiczenie 3. Wyznacz następujące reprezentacje liczb dziesiętnych:
1. 3, 15, 30, 81, 312 w systemie trójkowym
2. 7, 12, 16, 64, 100, 1600 w systemie szesnastkowym. W tym systemie, cyfry większe od 9 oznacza się następująco: 10 → A, 11 → B, 12 → C, 13 → D, 14 → E, 15 → F.

Zamiana reprezentacji binarnej na dziesiętną
Podaliśmy powyżej, w jaki sposób obliczać wartość dziesiętną liczby binarnej:

$$(100101)_2 = 1*2^5 + 0*2^4 + 0*2^3 + 1*2^2 + 0*2^1 + 1*2^0 = 1*32 + 0*16 + 0*8 + 1*4 + 0*2 + 1*1 = 37$$

Istnieje nieco prostszy sposób, bazujący na tzw. **schemacie Hornera**. Zobaczmy na przykładzie tej samej liczby, jak to działa:

$$\begin{aligned}(100101)_2 &= 1*2^5 + 0*2^4 + 0*2^3 + 1*2^2 + 0*2^1 + 1*2^0 = \\ &= (1*2^4 + 0*2^3 + 0*2^2 + 1*2^1 + 0)*2 + 1*1 = \\ &= ((1*2^3 + 0*2^2 + 0*2^1 + 1)*2 + 0)*2 + 1 = \\ &= (((1*2^2 + 0*2 + 0)*2 + 1)*2 + 0)*2 + 1 = \\ &= (((1*2 + 0)*2 + 0)*2 + 1)*2 + 0)*2 + 1 = 37 = (37)_{10}\end{aligned}$$

W ostatnim wzorze widać, że zamieniliśmy liczenie potęg na mnożenie. Z kolei nawiasy pokazują kolejność działań – zauważmy, że działania są wykonywane od najbardziej znaczącego bitu.

Ten przykład możemy uogólnić na następujący algorytm:

Algorytmu: 2 → 10.
Dane: kolejne, od najbardziej znaczącego, bity liczby binarnej $(c_{i-1}c_{i-2}...c_2c_1c_0)_2$.
Wynik: wartość dziesiętna tej liczby obliczamy w następujący sposób:
z ← c_{i-1}; {Ten bit, jako najbardziej znaczący, jest zawsze równy 1.}
Dla $k = i - 2, i - 3, ..., 2, 1, 0$ wykonaj:
$z \leftarrow z*2 + c_k$;
{Innymi słowy, aktualną wartość *z* pomnóż przez 2 i dodaj kolejny bit.
Kontynuuj aż do wyczerpania bitów.}.

Ćwiczenie 4. Oblicz wartości dziesiętne liczb binarnych otrzymanych w ćwiczeniu 2. Porównaj wyniki z liczbami dziesiętnymi, danymi na początku tamtego ćwiczenia.

Algorytm **2 → 10** może być uogólniony na algorytm ***p*** **10** przez prostą zamianę w ostatnim kroku mnożenia przez 2 mnożeniem przez *p*.

Ćwiczenie 5. Oblicz wartości dziesiętne liczb reprezentowanych w innych systemach, otrzymanych w ćwiczeniu 3. Porównaj wyniki z liczbami dziesiętnymi, danymi na początku tamtego ćwiczenia.

2 DZIAŁANIA NA PRZESTRZENI ADRESOWEJ IPV4

Dla zapewnienia poprawnej komunikacji pomiędzy urządzeniami w sieci komputerowej, każde z nich musi być jednoznacznie identyfikowane. Niezbędne jest również, aby każdy z pakietów tworzonych w warstwie sieciowej podczas komunikacji pomiędzy dwoma hostami zawierał zarówno adres urządzenia źródłowego, jak i docelowego. W przypadku użycia protokołu IPv4 oznacza to, iż oba te 32-bitowe adresy są zawarte w nagłówku warstwy sieciowej. Dla użytkowników sieci, łańcuch 32-bitowy jest trudny do interpretacji i jeszcze trudniejszy do zapamiętania, zatem zwykle adresy IPv4 są prezentowane z użyciem notacji dziesiętnej z kropkami.

Określanie adresów sieci, adresów rozgłoszeniowych oraz adresów hostów
Adres sieciowy
Adres sieciowy jest standardowym sposobem odwoływania się do sieci. Adres sieci jest pierwszym (najniższym) adresem w zakresie adresów związanych z daną siecią. Jest to sposób jednoznacznie określający sieć

oraz informujący, iż wszystkie hosty pracujące w sieci np. 10.0.0.0 będą miały takie same bity w polu sieciowym adresu. W zakresie adresów IPv4 związanych z daną siecią, pierwszy (najniższy) adres zarezerwowany jest dla adresu sieciowego. W adresie tym wszystkie bity w polu hosta mają wartość 0.

Ćwiczenie 6. Wyodrębnij z podanych poniżej przykładowych adresów, adresy sieci (uwzględniając klasowy schemat adresowania):

192.168.1.212
212.89.73.255
172. 16.0.0
10.10.10.10

Adres rozgłoszeniowy

Adres rozgłoszeniowy IPv4 jest specjalnym adresem występującym w każdej sieci, umożliwiającym jednoczesne komunikowanie się ze wszystkimi hostami w danej sieci. Oznacza to, iż aby wysłać dane do wszystkich urządzeń końcowych w danej sieci, host wysyła pojedynczy pakiet zaadresowany adresem rozgłoszeniowym. Adres rozgłoszeniowy jest ostatnim (najwyższym) adresem w zakresie adresów związanych z daną siecią. Jest to adres, w którym wszystkie bity znajdujące się w polu hosta mają wartość 1. W przypadku sieci 172.16.0.0, adres rozgłoszeniowy będzie miał postać 172.16.255.255. Adres ten jest określany również jako rozgłoszenie skierowane (ang. *directed broadcast*).

Ćwiczenie 7. Wyodrębnij z podanych poniżej przykładowych adresów, adresy rozgłoszeniowe (uwzględniając klasowy schemat adresowania).

198.12.13.254
172.100.0.0
10.255.255.255
1.1.1.255

Adresy hostów

Każde urządzenie końcowe (w rozumieniu sieci komputerowych) musi być jednoznacznie określone za pomocą unikatowego adresu, aby móc dostarczyć do niego wysyłany pakiet. W adresacji IPv4 urządzenia końcowe pracujące w danej sieci, mogą mieć przypisane adresy z zakresu ograniczonego adresem sieciowym oraz rozgłoszeniowym.

Ćwiczenie 8. Obliczyć z wykorzystaniem podanych przykładowych adresów użyteczne zakresy adresów dla hostów (uwzględniając klasowy schemat adresowania).

192.168.0.0
172.16.0.0
199.199.199.255
10.10.10.10

3 ZASADY PROJEKTOWANIA I BUDOWANIA SIECI KOMPUTEROWYCH

3.1 OKABLOWANIE STRUKTURALNE

Ćwiczenie 9. Zarabianie i testowanie okablowania strukturalnego.

Potrzebne akcesoria:

- kabel Ethernet kat5/6,

- wtyki RJ45,
- zaciskarka,
- tester okablowania.

Izolacja na kablach CAT5/6 jest w różnych kolorach. Są specyficzne kody kolorów związanych ze standardami zarabiania połączeń modularnych do Ethernet. Najbardziej popularnym jest standard T568B, drugim jest T568A (patrz rys. 50).

Kiedy chcesz zaterminować przewód, najpierw upewnij się, jaki standard używasz w Twojej sieci. Przewód w jednym kolorze wraz z kolorem przerywanym (kolor biały) tworzą tę samą parę i są skręcone razem wewnątrz koszulki. Bardzo ważne przy zarabianiu jest, aby ta para pozostała skręcona jak najdłużej i jak najbliżej konektora jak to możliwe (max 12mm). Przy zarabianiu należy zwrócić uwagę, że są różne typy kabli i powinno się użyć właściwego do danego typu narzędzia ściskającego (plecionka, drut).

Czynności do wykonania:

- Zdejmij zewnętrzną koszulkę (łatwiej jest ściągnąć więcej niż potrzeba a potem przyciąć odpowiednio przewody).
- Rozprostuj poszczególne żyły skręconych par.
- Wyprostuj kable i przytnij je na odpowiednia długość. Spróbuj zostawić skręcone odcinki tak blisko konektora, jak to tylko możliwe. Nie więcej niż 12mm skrętki może być rozkręcone dla kabla Cat5e, w przeciwnym razie ucierpi jakość przesyłu przy dużych długościach kabla (pojawianie się zjawisk falowych).
- Włóż każdą parę w odpowiedni punkt łączenia. Bądź ostrożny, ponieważ kolory pomarańczowy i brązowy wyglądają podobnie. Kiedy osadzisz odpowiednio wszystkie 8 przewodników, wciśnij do konektora również koszulkę tak, aby się naprężyła i umożliwiła trwałe zaciśnięcie konektora. Włóż konektor do narzędzia, naciśnij i piny konektora usuną (przebiją) izolację na każdej żyle tworząc pewne polaczenie.
- Włóż obydwa końce kabla zakończone konektorami do urządzenia testującego i zweryfikuj poprawność działania kabla.

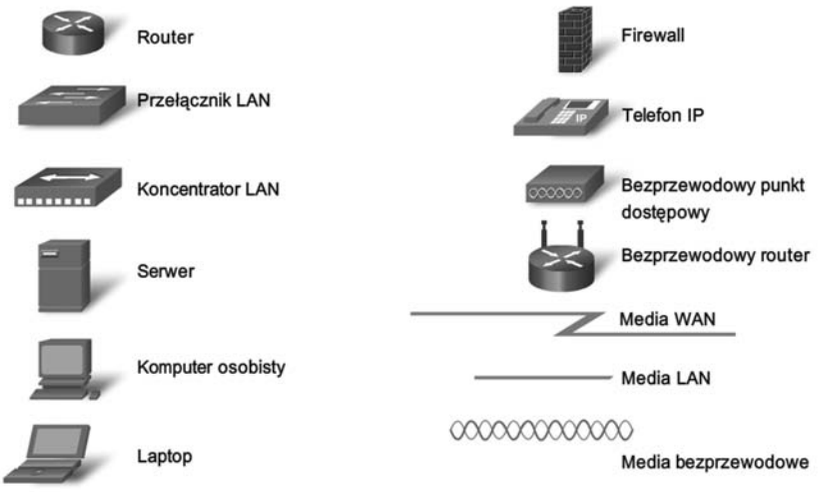
3.2 PROJEKTOWANIE INFRASTRUKTURY TELEINFORMATYCZNEJ

Ćwiczenie 10. Wykonanie projektu architektury technicznej.

a) Schemat okablowania. Na planie (podkładzie budowlanym lub innym dostępnym) należy zaznaczyć jak jest przeprowadzony kabel, rozmieszczenie gniazdek sieciowych i elektrycznych. Wskazanie punktu centralnego sieci, lokalnych punktów dystrybucyjnych (np. piętrowe punkty dystrybucyjne) i elementów infrastruktury teleinformatycznej z wykorzystaniem symboli pokazanych na rysunku 50 (wykorzystujemy oprogramowanie Packet Tracer lub np. MS Visio).

b) Mapa zasięgu radiowego (dla radiowego punktu dostępowego). Dla przewidywanych lokalizacji radiowych punktów dostępowych, należy wykreślić, na planie szkoły, kołowe wykresy zasięgu.

c) Sposób podpięcia do Internetu. Określić sposób i świadczenia usługi przez ISP, rodzaj urządzenia zastosowanego do zakończenia łącza, jego własności oraz możliwości integracji z projektowaną siecią.

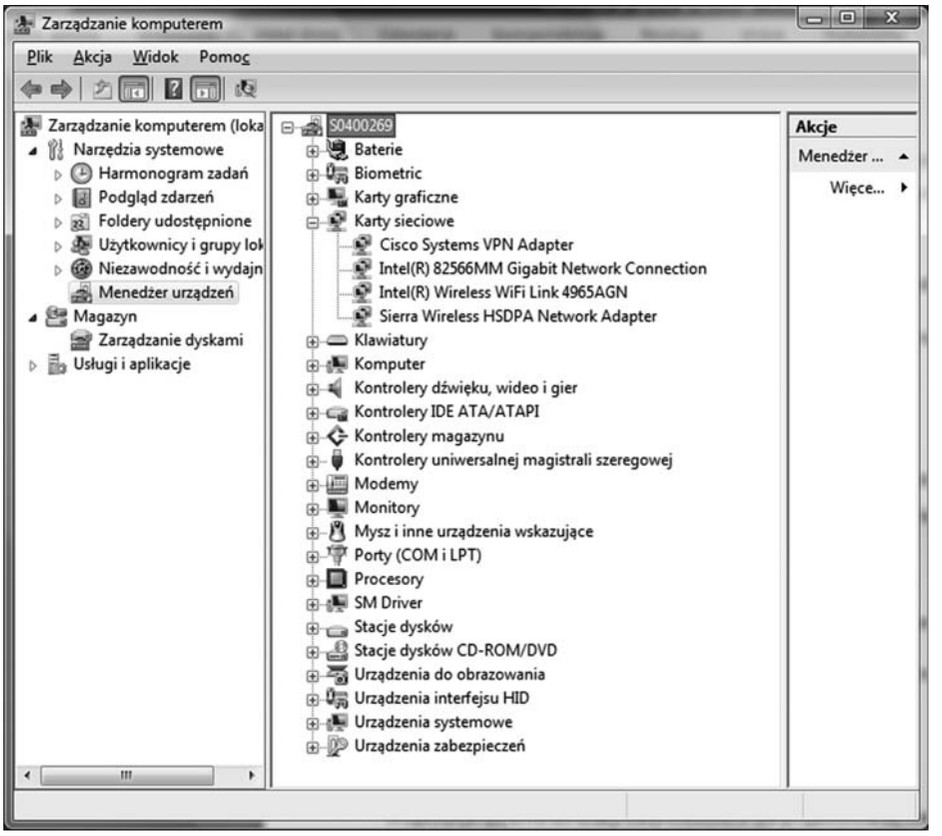


Rysunek 50.
Symbole urządzeń sieciowych

4 ROZWIĄZYWANIE PROBLEMÓW SIECIOWYCH

4.1 WERYFIKACJA KONFIGURACJI SPRZĘTOWEJ

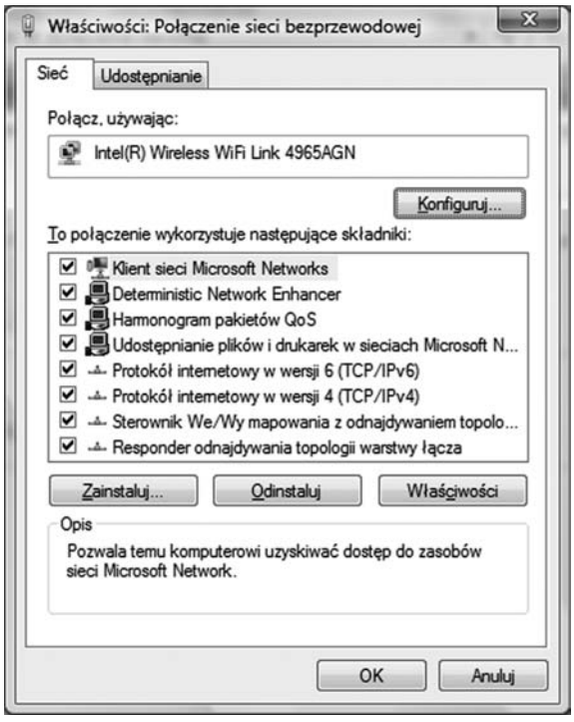
Ćwiczenie 11. Za pomocą dostępnych narzędzi systemowych (dostępnych z panelu sterowania) należy zweryfikować konfigurację sprzętową oraz zinterpretować możliwości zastosowanych technologii.



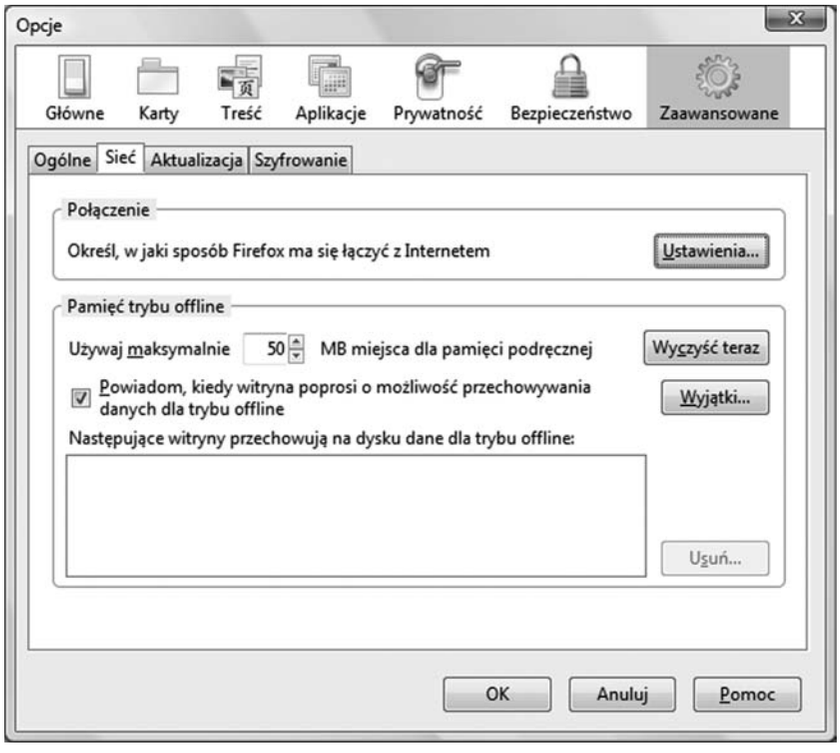
Rysunek 51.
Panel zarządzania komputerem MS Windows Vista

4.2 WERYFIKACJA KONFIGURACJI SYSTEMÓW SIECIOWYCH I APLIKACJI

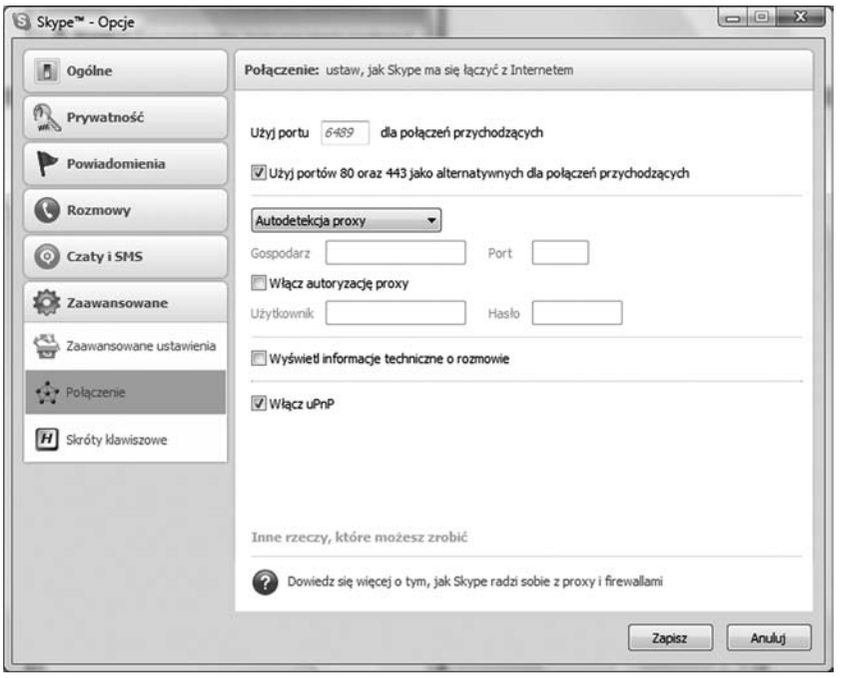
Ćwiczenie 12. Za pomocą dostępnych narzędzi systemowych (dostępnych z panelu sterowania) oraz paneli konfiguracyjnych aplikacji użytkowych należy zweryfikować konfigurację parametrów sieciowych oraz możliwości komunikacyjnych aplikacji



Rysunek 52.
Panel zarządzania połączeniami sieciowymi MS Windows Vista



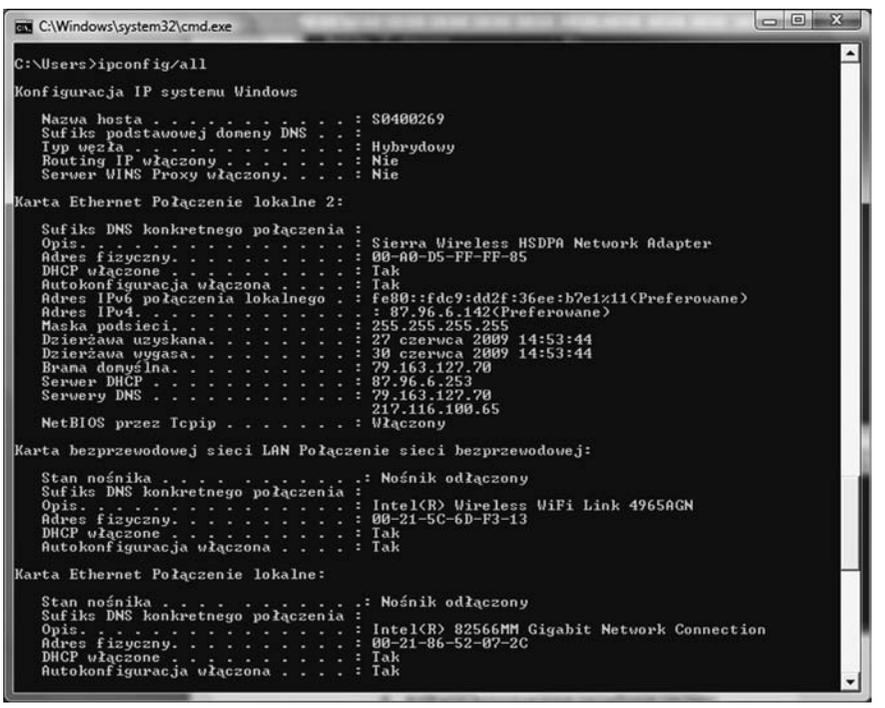
Rysunek 53.
Panel zarządzania konfiguracją połączeń sieciowych przeglądarki Firefox



Rysunek 54.
Panel zarządzania konfiguracji połączenia komunikatora internetowego Skype

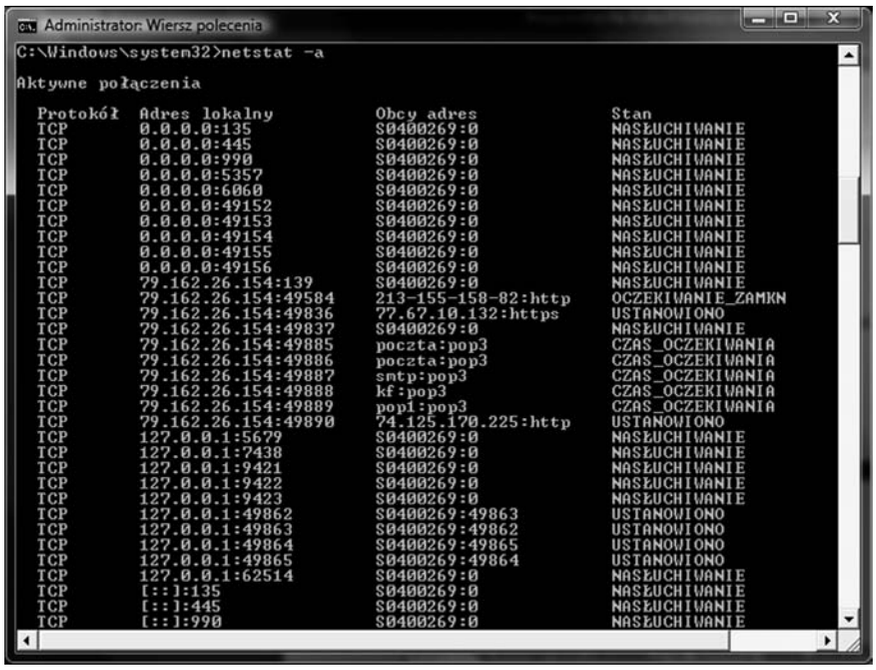
4.3 WERYFIKACJA DZIAŁANIA PROTOKOŁÓW SIECIOWYCH

Ćwiczenie 13. Za pomocą dostępnych narzędzi systemowych (dostępnych z panelu sterowania) oraz z linii komend należy zweryfikować konfigurację parametrów sieciowych oraz możliwości komunikacyjnych protokołów sieciowych.

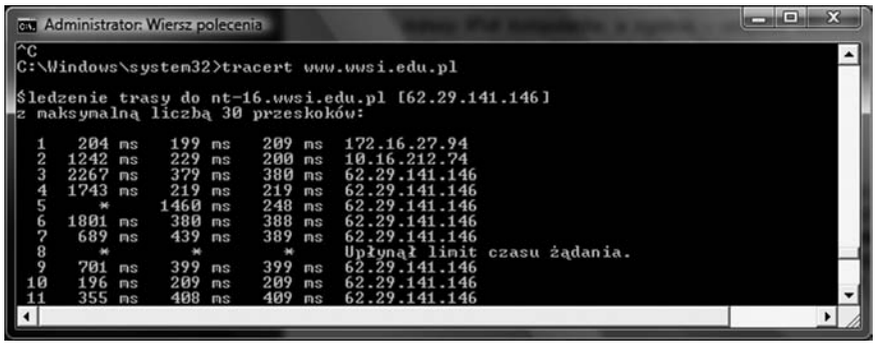


Rysunek 55.
Wykorzystanie komendy *ipconfig* do weryfikacji konfiguracji protokołu IP

Rysunek 56.
Wykorzystanie komendy *ping* do sprawdzenia połączenia sieciowego



Rysunek 57.
Wykorzystanie komendy *netstat* do wyświetlenia statystyki protokołu i bieżących połączeń sieciowych TCP/IP



Rysunek 58.
Wykorzystanie komendy *tracert* do sprawdzenia trasy do adresu docelowego

Rysunek 59.
Wykorzystanie komendy *netstat* do wyświetlenia tablicy routingu

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