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+

# Kuźnia Talentów: Sieci komputerowe

## Zarządzanie sieciami LAN

*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.

# Zarządzanie sieciami LAN

**Rodzaj zajęć:** Kuźnia Talentów
**Tytuł:** Zarządzanie sieciami LAN
**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.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.

# Zarządzanie sieciami LAN

**Dariusz Chaładyniak**
Warszawska Wyższa Szkoła Informatyki
dchalad@wwsi.edu.pl

**Józef Wacnik**
Warszawska Wyższa Szkoła Informatyki
j_wacnik@poczta.wwsi.edu.pl

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

**Streszczenie**

Do prowadzenia jakiejkolwiek działalności związanej w wymianą informacji niezbędne jest prawidłowe funkcjonowanie sieci **LAN** (ang. *Local Area Network*). Zrozumienie zasad budowy, projektowania i utrzymania architektury sieciowej są głównymi celami tego kursu. Wykład wyjaśnia budowę i działanie lokalnych sieci 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. Omawia najczęściej spotykane topologie sieciowe a także wyjaśnia pojęcia związane z segmentacją i domenami kolizyjnymi. Zawarto w nim również informacje o przewodowy mediach transmisyjnych oraz zasadach projektowania okablowania strukturalnego sieci (poziomego i pionowego). Przedstawione zostały ponadto podstawowe technologie spotykane w sieciach LAN (Ethernet, Token Ring, FDDI) a także zasady działania i konfigurowania wirtualnych sieci lokalnych (VLAN).

Warsztaty umożliwiają praktyczne przećwiczenie materiału z wykładu.

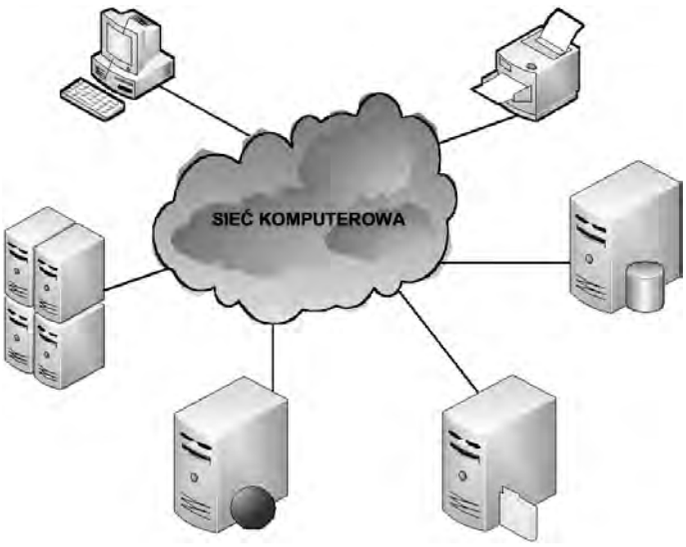
**Spis treści**



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

# 1 WPROWADZENIE DO BUDOWY I DZIAŁANIA SIECI KOMPUTEROWYCH

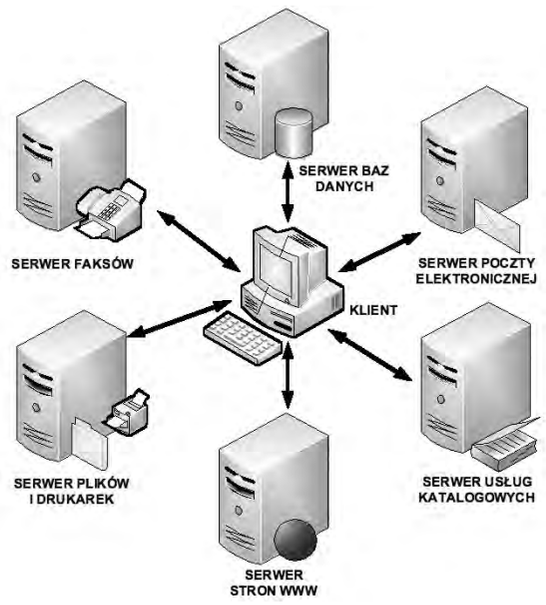
**Siecią komputerową** nazywamy zespół połączonych ze sobą komputerów, terminali, serwerów, drukarek za pomocą mediów transmisyjnych. Komunikacja w sieci jest możliwa dzięki odpowiednim protokołom.




*Rysunek 1.*
Przykład sieci komputerowej

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.

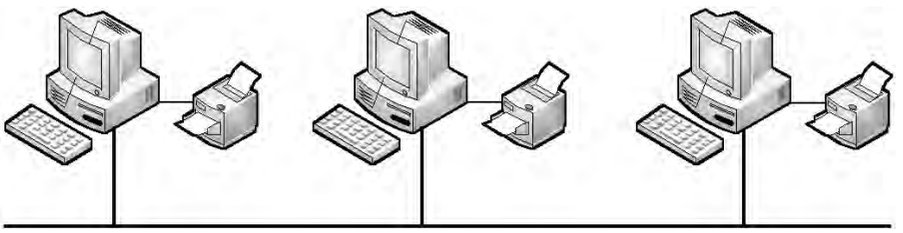



*Rysunek 2.*
Przykładowe role komputerów w sieci

Jak pokazano na rysunku 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.

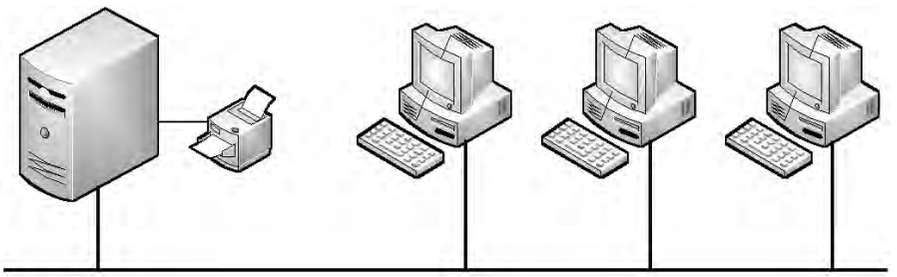
### 1.1 TYPY SIECI

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.



*Rysunek 3.*
Sieć równorzędna

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.



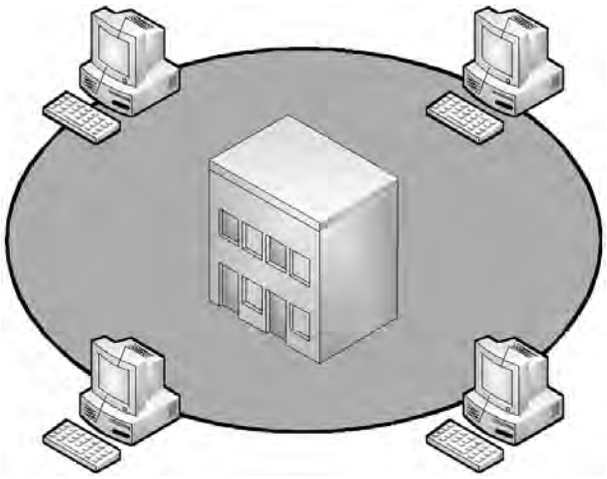
*Rysunek 4.*
Sieć typu klient-serwer

### 1.2 ZASIĘG SIECI KOMPUTEROWYCH

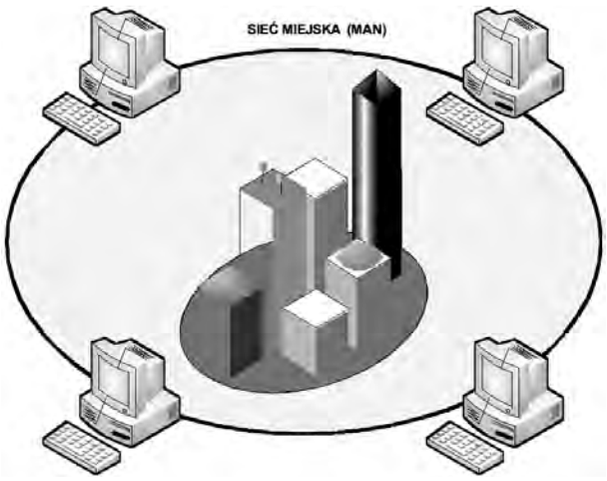
**Sieć lokalna LAN** (ang. *Local Area Network*) obejmuje stosunkowo niewielki obszar i zwykle łączy urządzenia sieciowe w ramach jednego domu, biura, budynku (rys. 5).

**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).

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



*Rysunek 5.*
Lokalna sieć komputerowa (LAN)




*Rysunek 6.*
Miejska sieć komputerowa (MAN)

**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)

## 1.3 MODELE SIECIOWE

### 1.3.1 Model odniesienia ISO/OSI

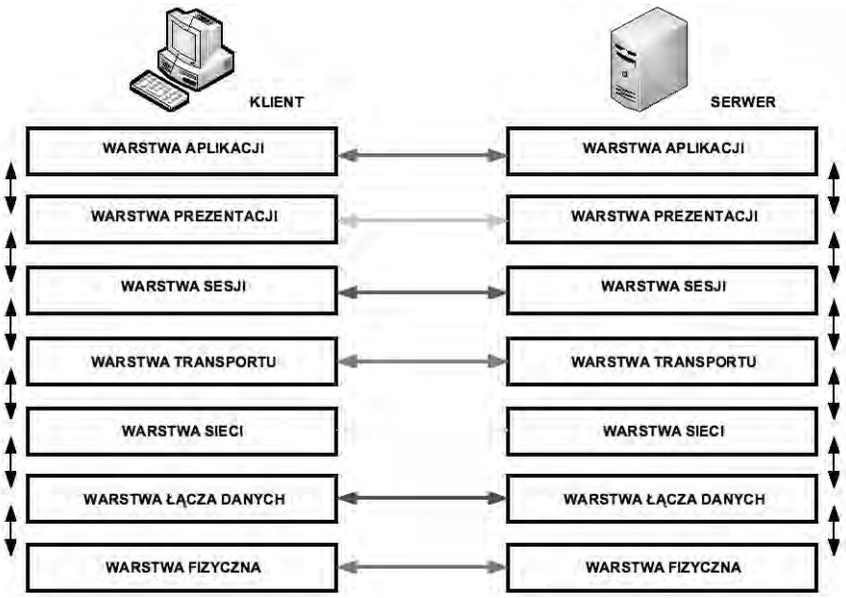

*Rysunek 8.*
Referencyjny model odniesienia ISO/OSI

**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.

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.).

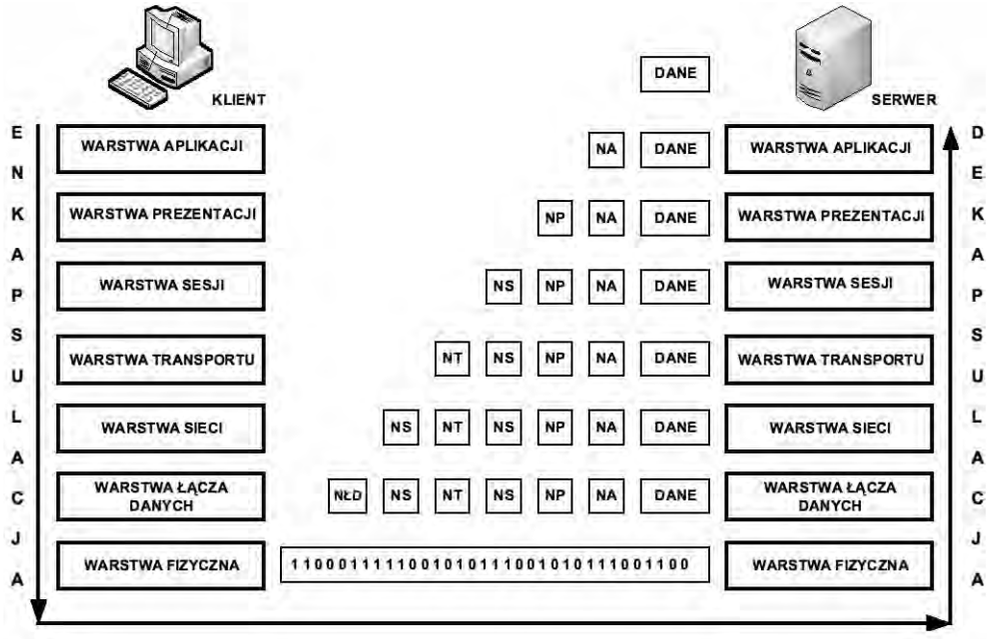
**Współpraca warstw w modelu ISO/OSI**

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**



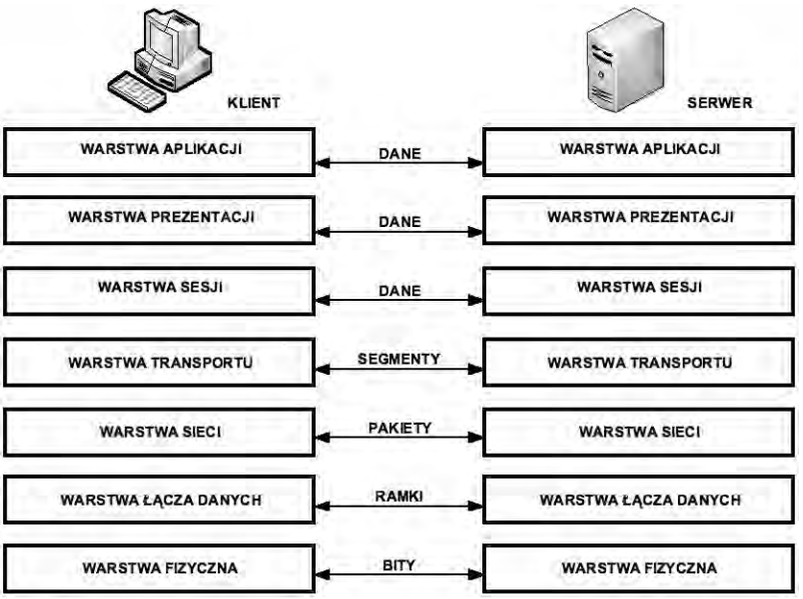

*Rysunek 10.*
Proces enkapsulacji i dekapsulacji danych

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**

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 **segmen-**

ty, 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.




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

### 1.3.2 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 od-

powiada 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.

## 1.4 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.

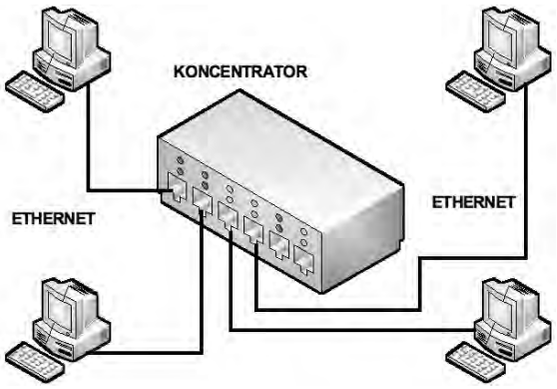
### Wzmacniak


*Rysunek 14.*
Przykład zastosowania wzmacniaka

**Wzmacniak** (ang. *repeter*) 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.

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

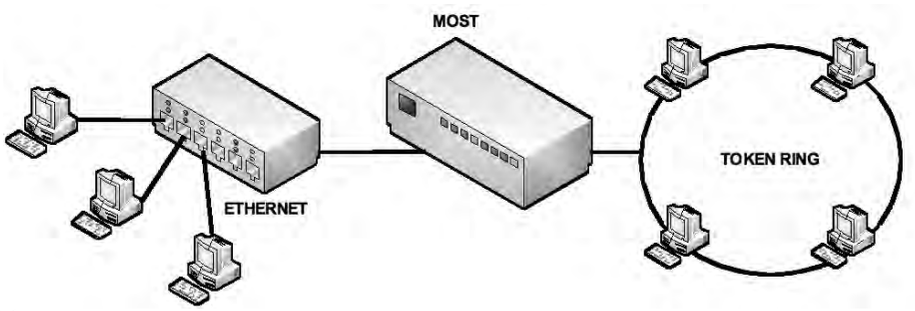
**Koncentrator**




*Rysunek 15.*
Przykład zastosowania koncentratora

**Koncentrator** (ang. *hub*) 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.

**Most**




*Rysunek 16.*
Przykład zastosowania mostu

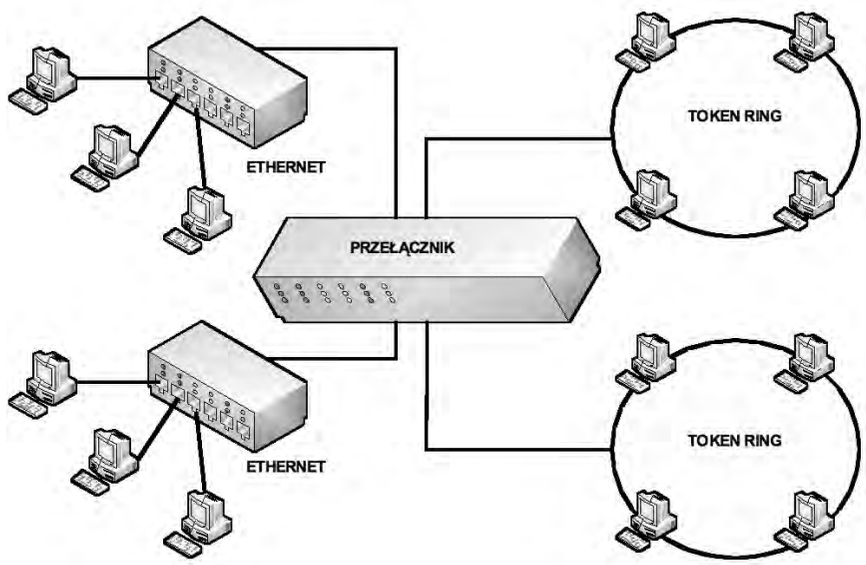
**Most** (ang. *bridge*) jest urządzeniem służącym do wzajemnego łączenia sieci lokalnych. Mosty, podobnie jak wzmacniaki, pośredniczą pomiędzy dwoma sieciami, mają przy tym większe możliwości. Największą ich zaletą jest to, że filtrują ramki, przesyłając je z segmentu do segmentu wtedy, gdy zachodzi 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**

Zadaniem **przełącznika** (ang. *switch*) 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

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




*Rysunek 17.*
Przykład zastosowania przełącznika

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.

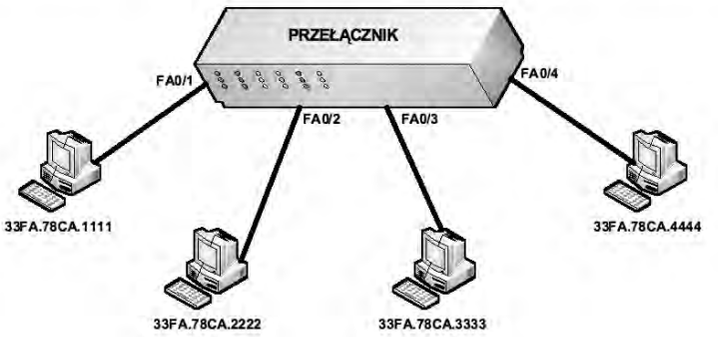
W trybie **fragment free** przełącznik odczytuje pierwsze 64 bajty ramki i podejmuje decyzję co do jej losu. Po odczytaniu 64 bajtów ma już informację, czy wystąpiła kolizja, i może odrzucić takie ramki, nie wczytując ich dalszego ciągu.

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

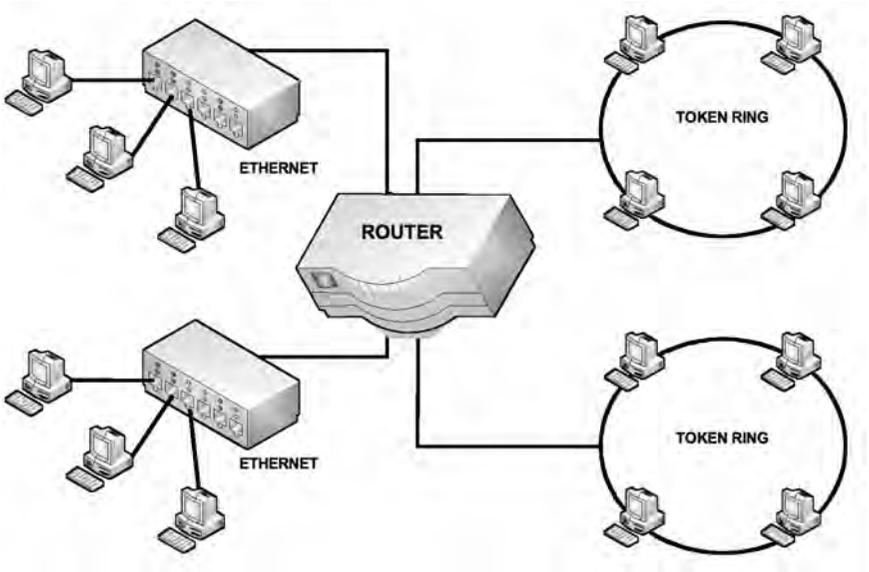
Tablica adresów MAC przechowywana jest w pamięci skojarzeniowej (asocjacyjnej). Dla każdego portu przełącznika kojarzony jest adres MAC podłączonego urządzenia sieciowego (patrz rys. 19).

| 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

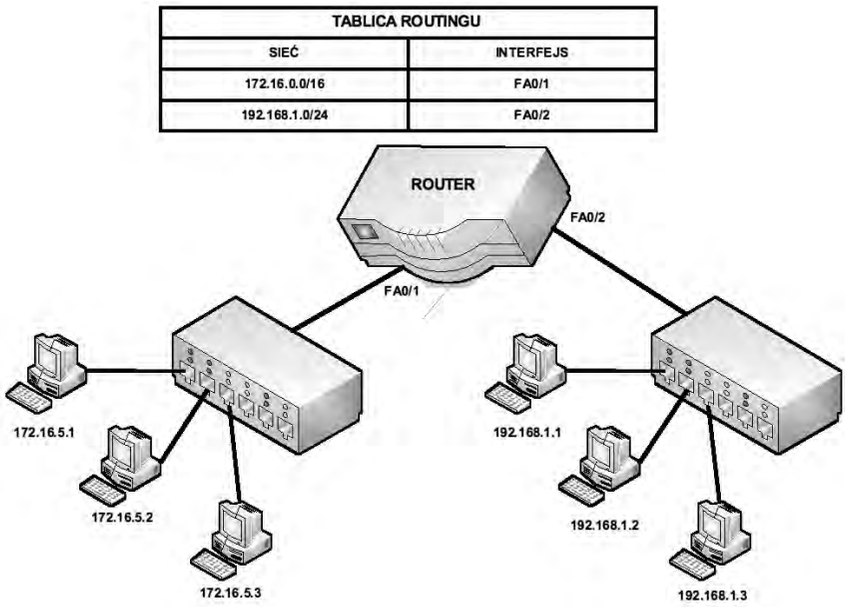
**Router**




*Rysunek 20.*
Przykład zastosowania routera

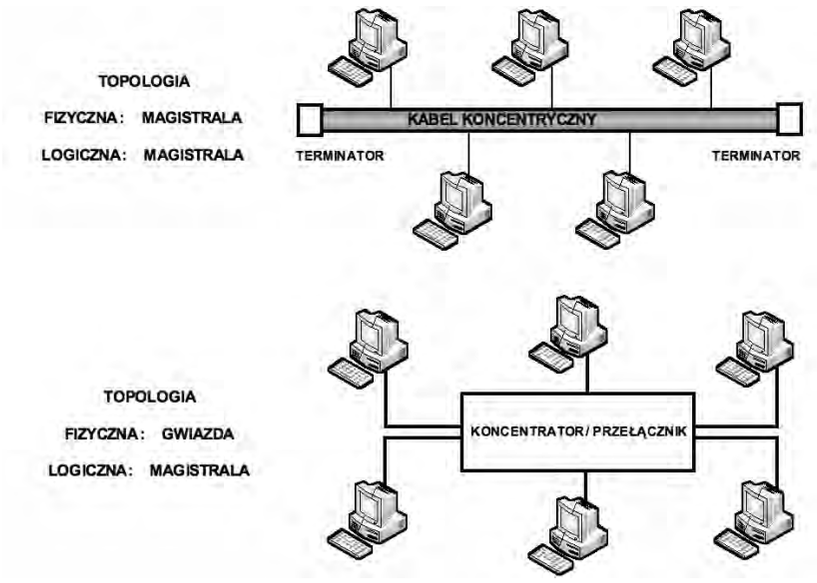
**Router** (ang *router*) służy do zwiększania fizycznych rozmiarów sieci poprzez łączenie jej segmentów. Urządzenie to wykorzystuje logiczne adresy hostów w sieci. Ponieważ komunikacja w sieci jest oparta na logicznych adresach odbiorcy i nadawcy, przesyłanie danych i informacji jest niezależne od fizycznych 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 użytkowników do wybranych segmentów czy komputerów sieciowych. Router jest konfigurowalny, umożliwia sterowanie przepustowością sieci oraz zapewnia pełną izolację pomiędzy segmentami.

**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

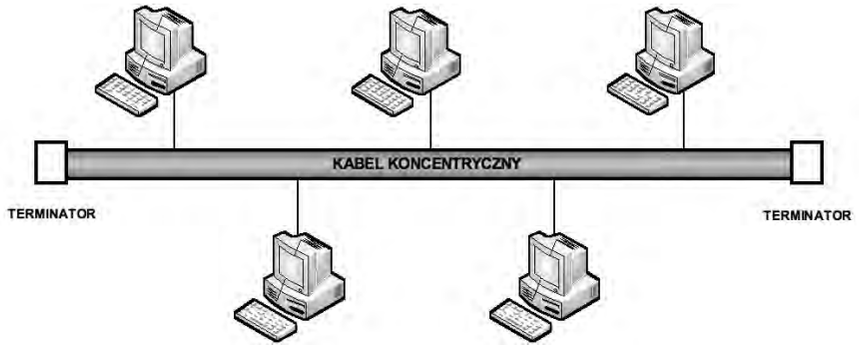
## 1.5 TOPOLOGIE FIZYCZNE I LOGICZNE




*Rysunek 22.*
Porównanie topologii fizycznej i logicznej

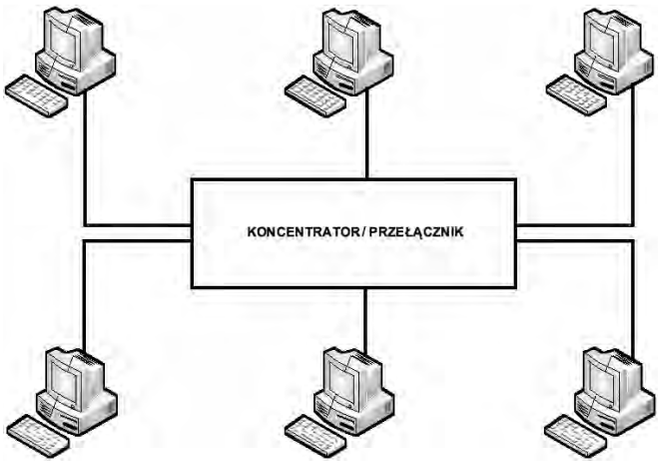
**Topologia fizyczna** (ang. *physical topology*) jest związana z fizycznym (elektrycznym, optycznym, radiowym) łączeniem ze sobą urządzeń sieciowych. **Topologia logiczna** (ang. *logical topology*) określa standardy komunikacji, wykorzystywane w porozumiewaniu się urządzeń sieciowych.

**Topologia magistrali** (**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 topo-



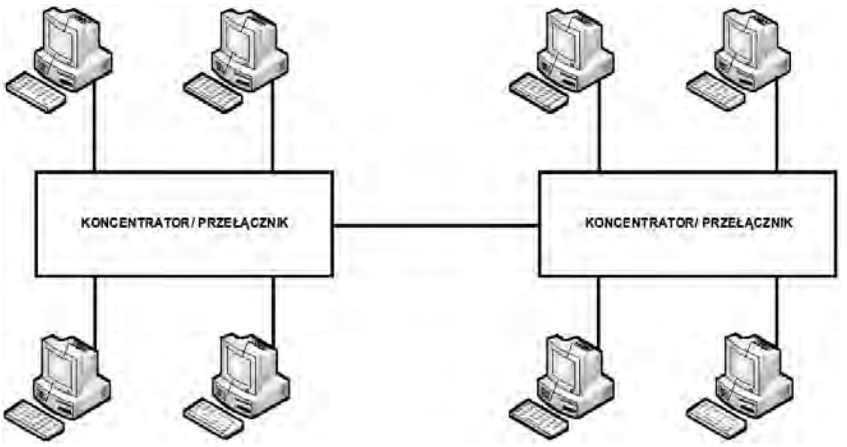

*Rysunek 23.*
Topologia magistrali

logii 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.



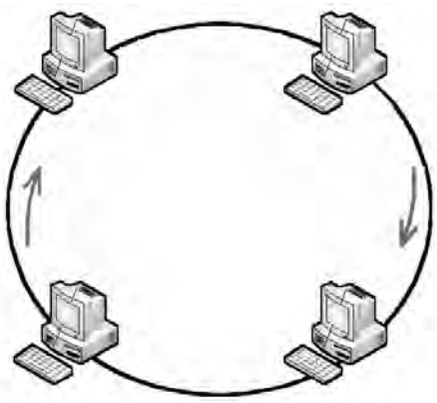

*Rysunek 24.*
Topologia gwiazdy

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.



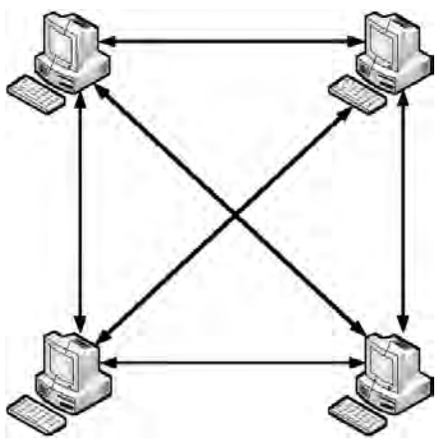

*Rysunek 25.*
Topologia rozszerzonej gwiazdy

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



*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.



*Rysunek 27.*
Topologia siatki

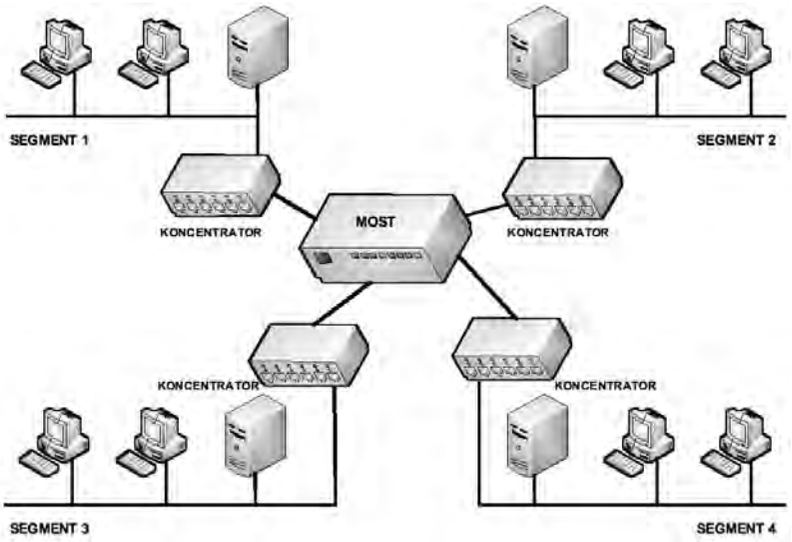
**Topologia siatki** (ang. *mesh topology*) jest stosowana w rozwiązaniach nadmiarowych (redundantnych), aby zapewnić bardzo wysoki poziom niezawodności. W topologii tej urządzenia sieciowe są połączone ze sobą każdy z każdym.

## 1.6 SEGMENTACJA I DOMENY KOLIZYJNE

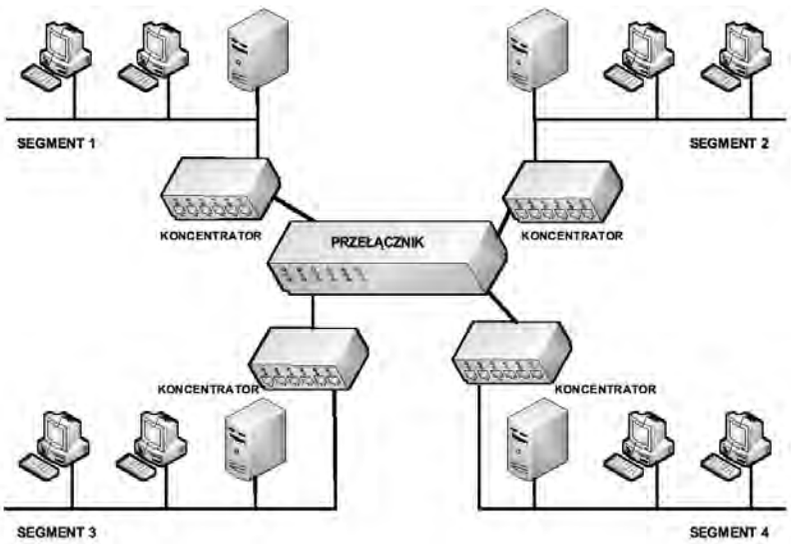
### Segmentacja sieci komputerowych

**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 przeszkadzają sobie wzajemnie w pracy. Dzięki urządzeniom potrafiącym inteligentnie zatrzymać zbędny ruch sieć zostaje zrównoważona i znacznie odciążona. Na rysunkach 28-30 przedstawiono przykładowe segmentacje sieci komputerowych.

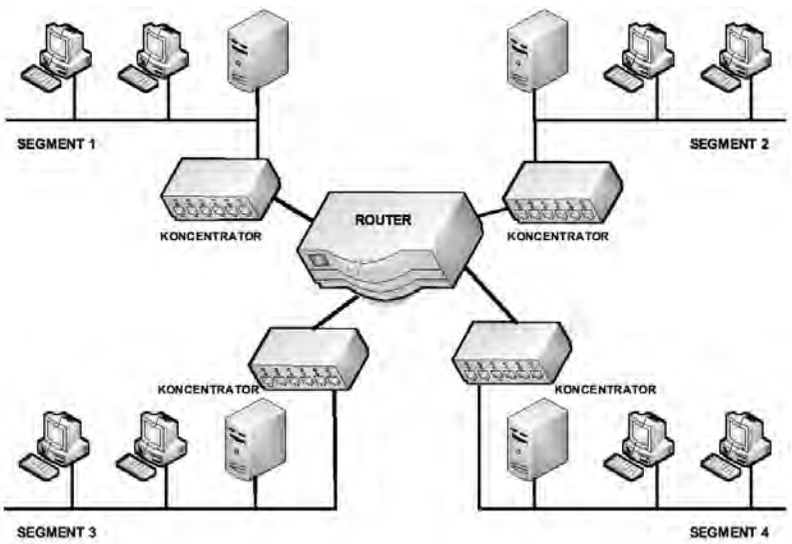
KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
Warszawska Wyższa Szkoła Informatyki
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego




*Rysunek 28.*
Przykład segmentacji za pomocą mostu sieciowego




*Rysunek 29.*
Przykład segmentacji za pomocą przełącznika

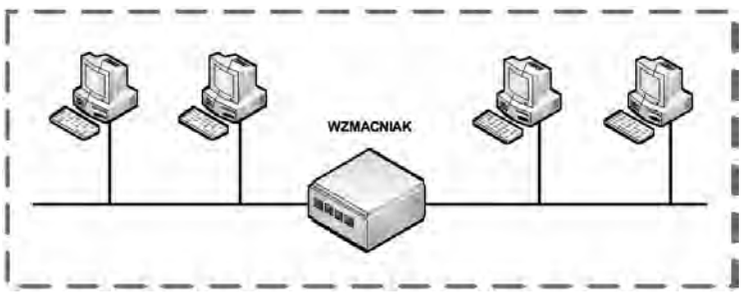



*Rysunek 30.*
Przykład segmentacji za pomocą routera

**Domeny kolizyjne**

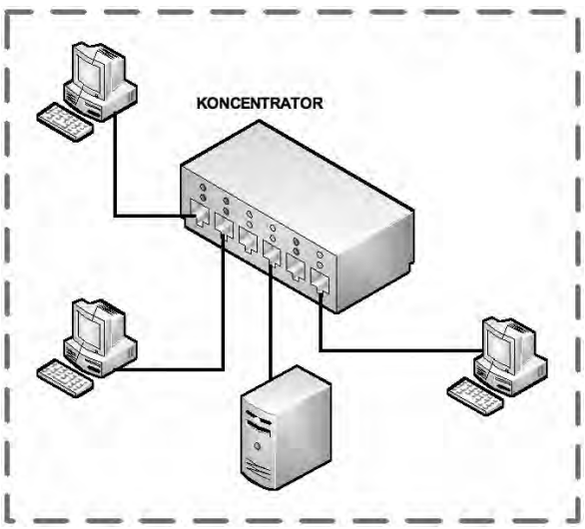
W sieciach z technologią Ethernet stacje robocze wysyłają dane w **trybie rozgłoszeniowym** (ang. *broadcast*). Każda stacja transmituje sygnał do wszystkich innych, stacje wsłuchują się w rozsyłane dane i odbierają tylko pakiety przeznaczone dla siebie. Dużym zagrożeniem są sztormy broadcastowe, powstające,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

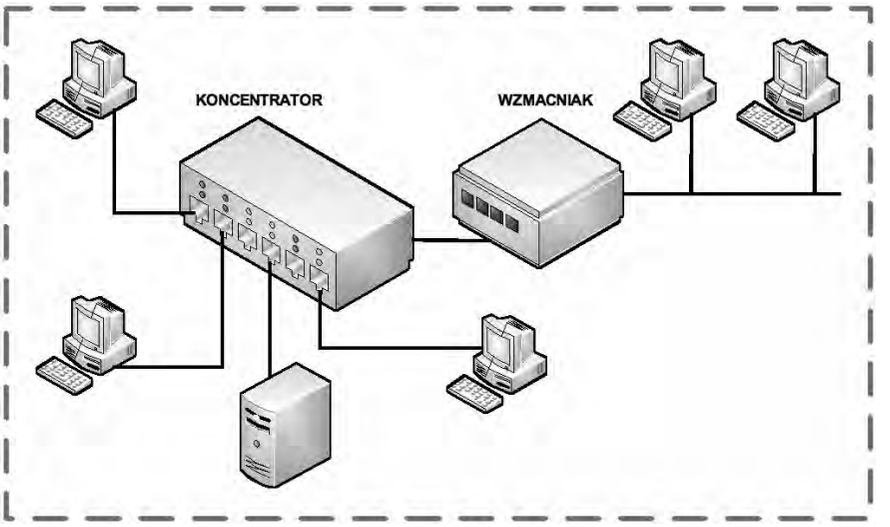
Wszystkie podłączone do koncentratora urządzenia sieciowe stanowią jedną domenę kolizyjną, gdyż koncentrator pracuje w pierwszej warstwie modelu odniesienia ISO/OSI (warstwie fizycznej) i nie potrafi filtrować ramek po adresach MAC.



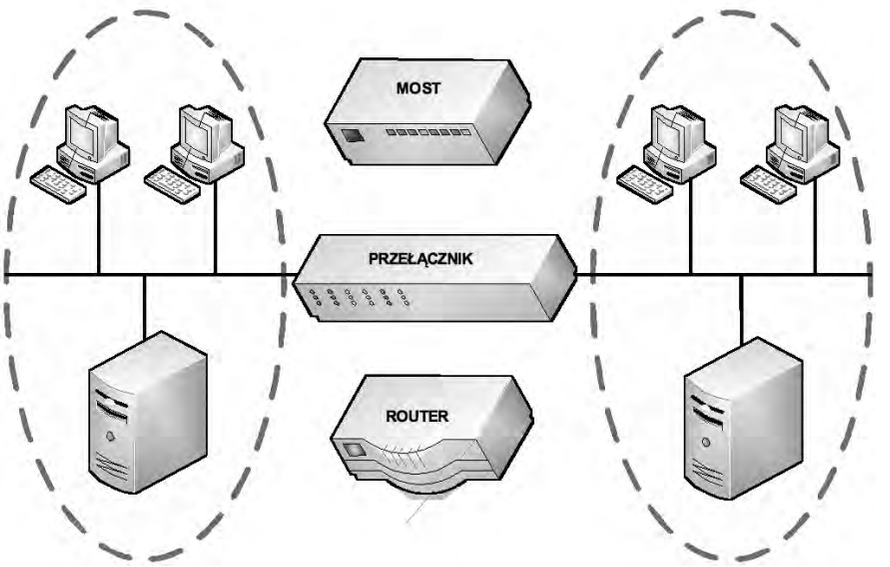

*Rysunek 32.*
Powiększenie domeny kolizyjnej przy zastosowaniu koncentratora

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

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.



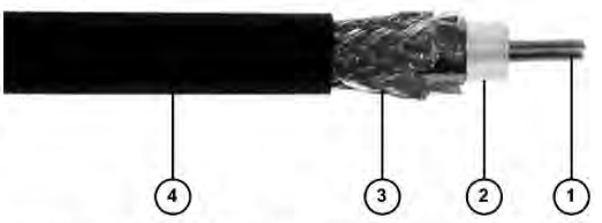

*Rysunek 33.*
Powiększenie domeny kolizyjnej przy wspólnym zastosowaniu koncentratora i wzmacniaka




*Rysunek 34.*
Przykłady użycia urządzeń sieciowych nie powiększających domen kolizyjnych

## 1.7 PRZEWODOWE MEDIA TRANSMISYJNE

### 1.7.1 Cienki kabel koncentryczny




1 – główny przewód przenoszący dane
2 – warstwa izolacyjna
3 – miedziany ekran
4 – powłoka zewnętrzna

*Rysunek 35.*
Cienki kabel koncentryczny

Największy wpływ na standardy mediów transmisyjnych mają **TIA** (ang. *Telecommunications Industry Association*) oraz **EIA** (ang. *Electronic Industries Alliance*).

**Kabel koncentryczny** (**współosiowy**) (ang. *coaxial cable*) – nazwa tego kabla pochodzi od dwóch przewodów o wspólnej centralnej osi. W kablu takim zastosowano pleciony miedziany ekran, który ma osłaniać wewnętrzny przewód od zewnętrznych pól elektromagnetycznych. Każda z końcówek kabla tworzącego segment musi posiadać terminator (*opornik 50* Ω), który absorbuje wszystkie sygnały docierające na koniec kabla. Maksymalna długość połączeń dla **cienkiego koncentryka** (ang. *thinnet, cheapernet*) wynosi 185 m, a dla **grubego koncentryka** (ang. *thicknet*) 500 m. Można podłączyć maksymalnie 30 węzłów. Minimalna odległość między węzłami – 0.5 m.

**Złącza dla cienkiego kabla koncentrycznego**

Złącza dla cienkich kabli koncentrycznych wykonuje się w oparciu o standard 10Base2, a dla grubych kabli koncentrycznych – w oparciu o standard 10Base5. Trójnik BNC wykorzystuje się do podłączenia do karty sieciowej. Męskie złącze BNC wpina się do trójnika BNC.

Aby zaterminować kabel koncentryczny musimy posiadać właściwe elementy złącza BNC a także odpowiednią zaciskarkę.

Opornik BNC (może być z uziemieniem lub bez) zapina się na końcach kabla koncentrycznego. Jego impedancja falowa wynosi 50 omów.


*Rysunek 36.*
Typowe złącza przeznaczone dla cienkich kabli koncentrycznych

### 1.7.2 Kable skrętkowe

**System AWG**

*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 |

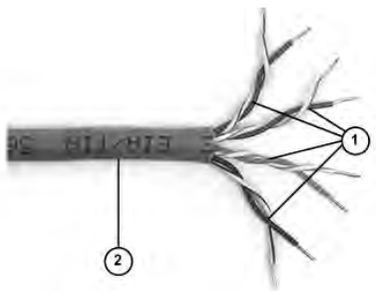
Średnica kabli jest zazwyczaj mierzona przy użyciu systemu **AWG** (ang. *American Wire Gauge*), znanego również jako Brown & Sharpe Wire Gauge. AWG jest standardem używanym do pomiarów średnicy kabli miedzianych i aluminiowych w USA. Typowe kable sieciowe mają średnicę z przedziału od 12 do 26 AWG. 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.

**Powłoki kabli miedzianych**

Rodzaje powłok kabli miedzianych:

1. Kable w powłoką **PVC** (ang. *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** (ang. *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** (ang. *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**

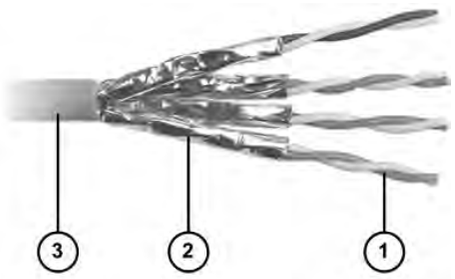



1 - cztery pary skrętek
2 - powłoka zewnętrzna

*Rysunek 37.*
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**

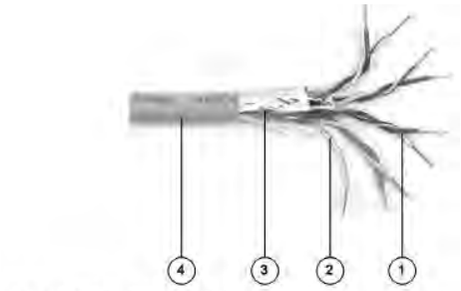



1 – cztery pary skrętek
2 – ekran z folii aluminiowej
3 – powłoka zewnętrzna

*Rysunek 38.*
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**

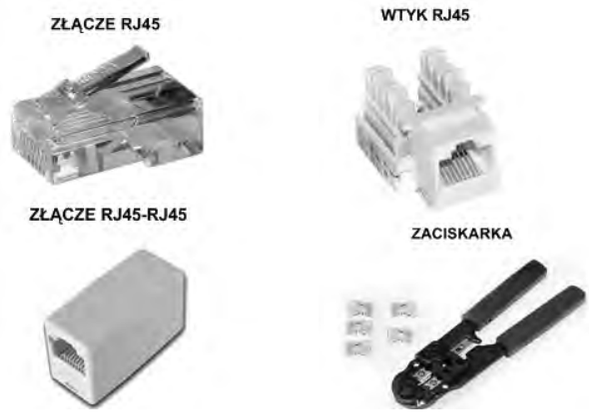



1 – cztery pary skrętek
2 – przewód uziemiający
3 – folia ekranująca
4 – powłoka zewnętrzna

*Rysunek 39.*
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**

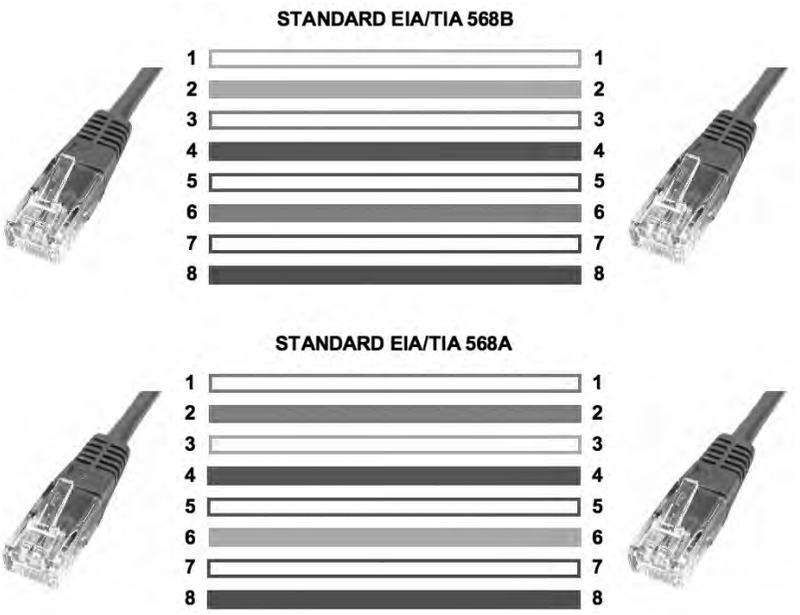



*Rysunek 40.*
Złącza dla kabli skrętkowych

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**

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.



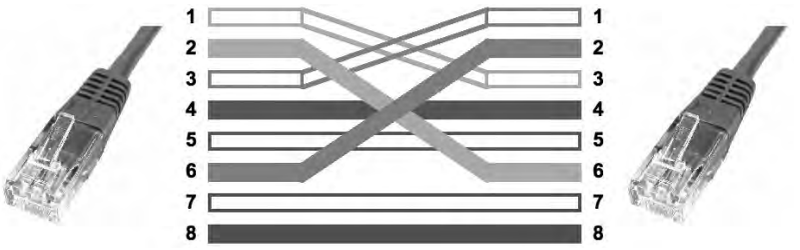

*Rysunek 41.*
Standardy terminowania kabli skrętkowych

**Kabel prosty**


*Rysunek 42.*
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.

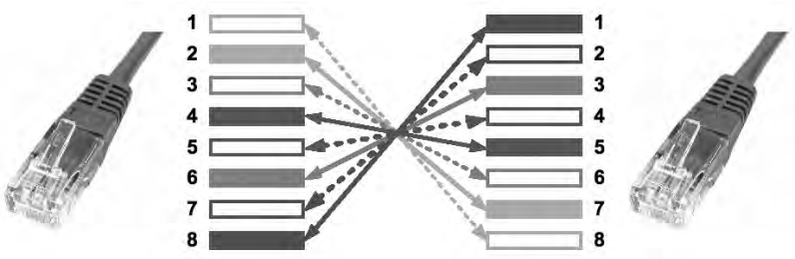
**Kabel krosowy**




*Rysunek 43.*
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 44.*
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).

### 1.7.3 Kable światłowodowe

**Budowa włókna światłowodowego**

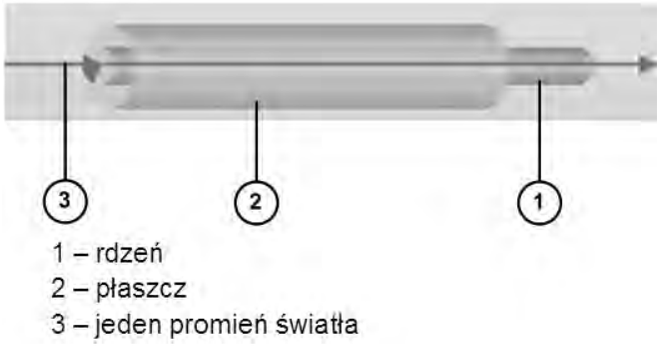
**Światłowód** to włókno szklane z centralnie umieszczonym rdzeniem przewodzącym światło, otoczonym cylindrycznym płaszczem odbijającym promienie świetlne i zewnętrzną powłoką lakierniczą, nadającą włóknu odpowiednią odporność i wytrzymałość mechaniczną.

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).

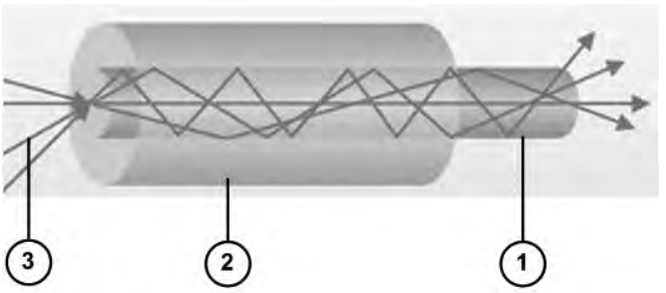
**Światłowód jednodomowy**




*Rysunek 45.*
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. 45).

**Światłowód wielodomowy**




1 – rdzeń
2 – płaszcz
3 – wiele promieni światła

*Rysunek 46.*
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. 46).

**Wymiary włókien światłowodowych**

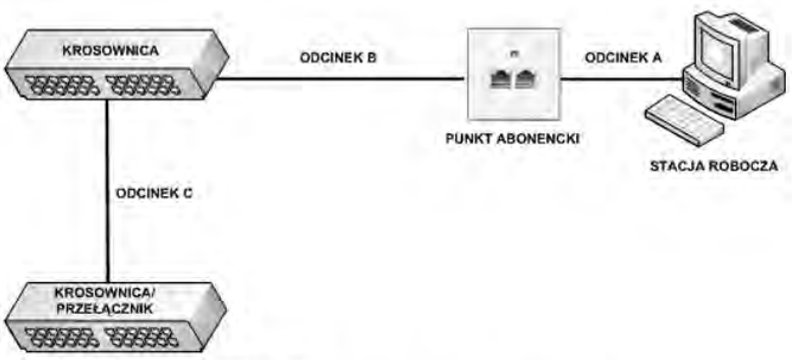
Średnicę światłowodu określa się w mikronach, podając zarówno średnicę rdzenia, jak też powłoki zewnętrznej. We współcześnie produkowanych światłowodach jednomodowych średnica rdzenia wynosi 9 µm, przy średnicy powłoki zewnętrznej do 125 µm.

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.

## 1.8 OKABLOWANIE STRUKTURALNE POZIOME I PIONOWE

**Okablowanie poziome**




Odcinek A – kabel stacyjny
Odcinek B – kabel łączący punkt abonencki z krosownicą
Odcinek C – kabel krosowy

*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):

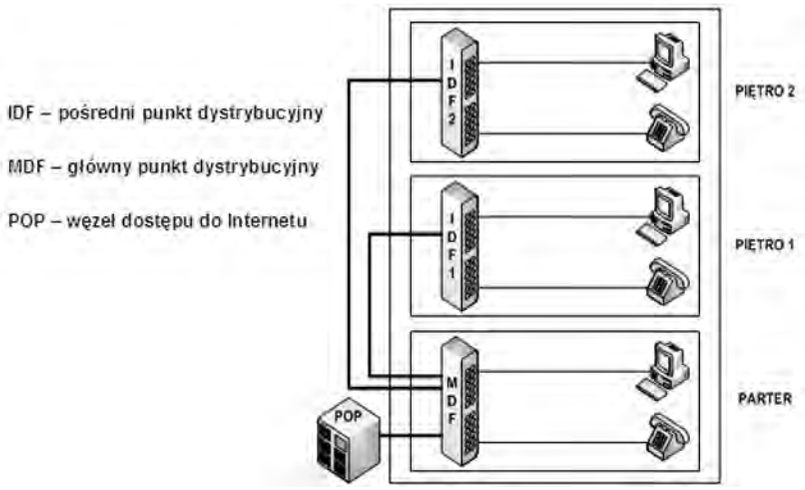
- gniazda naścienne w punktach abonenckich,
- kable połączeniowe,
- kable transmisyjne,
- panele krosowe (krosownice).

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).

## 1.9 OZNAKOWANIE PUNKTÓW ABONENCKICH

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.

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


*Rysunek 49.*
Przykład oznakowania punktu abonenckiego

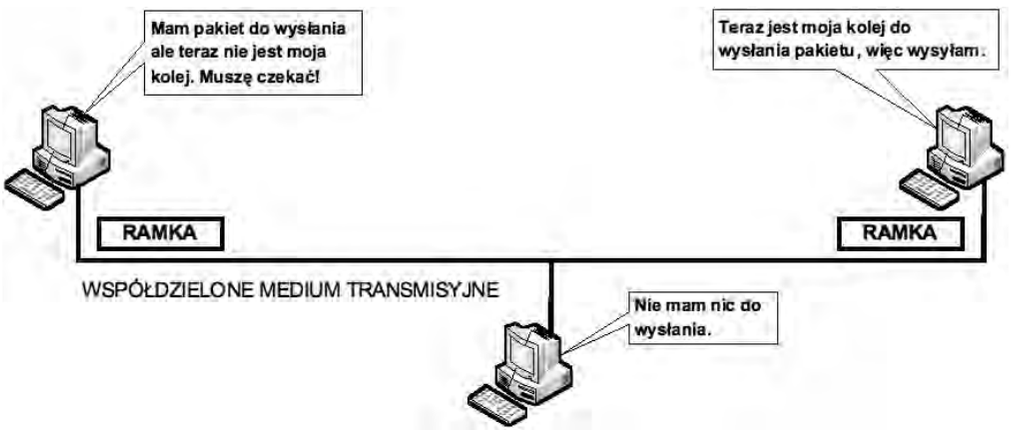
## 2 TECHNOLOGIA ETHERNET

**Kontrolowany dostęp do medium**

W lokalnych sieciach komputerowych są wykorzystywane dwie metody dostępu do medium transmisyjnego. Dostęp do medium może być kontrolowany lub rywalizacyjny. Istnieją implementacje wykorzystujące zarówno pierwszą, jak i drugą metodę.

W kontrolowanym dostępie do medium transmisyjnego stacja chcąca nadawać musi czekać na swoją kolej tzn. przed transmisją danych musi przejąć specjalną ramką zwaną **żetonem** (ang. *token*). Z uwagi na to, że tylko stacja posiadająca żeton może transmitować dane w rozwiązaniu tym nie występują kolizje. Do popularnych implementacji wykorzystujących kontrolowany dostęp do medium należą: Token Ring, FDDI i CDDI.

Na rysunku 50 pokazano mechanizm kontrolowanego dostępu do współdzielonego medium transmisyjnego.



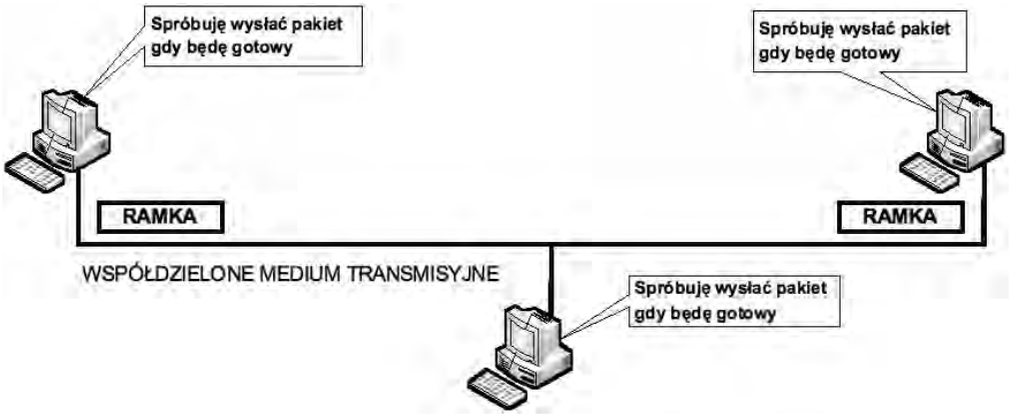

*Rysunek 50.*
Przykład kontrolowanego dostępu do medium transmisyjnego

**Rywalizacyjny dostęp do medium**

W rywalizacyjnym dostępie do medium transmisyjnego teoretycznie wiele stacji może próbować nadawać dane w tym samym czasie (patrz rys. 51). Niestety, gdy taka sytuacja wystąpi mamy do czynienia z kolizją wysyłanych ramek i transmisja musi zostać przerwana. Twórcy technologii sieciowych opracowali specjalne mechanizmy, które **wykrywają kolizje CSMA/CD** (ang. *Carrier Sense Multiple Acccess with Collision Detection*) lub nawet ich **unikają CSMA/CA** (ang. *Carrier Sense Multiple Acccess with Collision Avoidance*).

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

Do popularnych implementacji wykorzystujących rywalizacyjny dostęp do medium należą: Ethernet 802.3 z mechanizmem wykrywania kolizji CSMA/CD oraz sieci bezprzewodowe 802.11 z mechanizmem unikania kolizji CSMA/CA.




*Rysunek 51.*
Przykład rywalizacyjnego dostępu do medium transmisyjnego

**Rys historyczny technologii Ethernet**

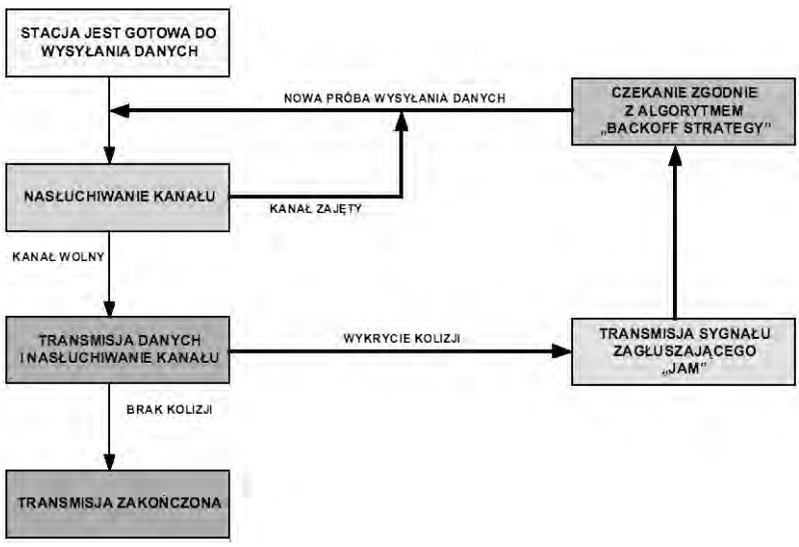
Początek technologii Ethernet dał **program Alohanet** w roku 1970. Była to cyfrowa sieć radiowa zaprojektowana do transmisji informacji przez współdzielony kanał częstotliwości radiowych między wyspami archipelagu hawajskiego. Twórcą tego powyższego projektu był Norman Abramson z Uniwersytetu Hawajskiego.

Pierwsza sieć LAN była pierwotną wersją sieci Ethernet. Opracował ją Robert Metcalfe wraz ze swoimi współpracownikami z firmy Xerox ponad 30 lat temu. Pierwszy standard sieci Ethernet został opublikowany w roku 1980 przez konsorcjum DIX utworzone przez firmy DEC (Digital Equipment Corporation), Intel i Xerox. Dwa lata później pojawiła się druga wersja standardu Ethernet – DIX Ethernet II.

W roku 1985 komitet standaryzacyjny IEEE ds. sieci lokalnych i miejskich opublikował standardy odnoszące się do sieci LAN. Standardy te rozpoczyna numer 802. Dla sieci Ethernet standardem jest 802.3.

Pierwotny projekt Ethernetu zakładał występowanie wielu wzajemnie połączonych komputerów w sieci o topologii współdzielonej magistrali. W pierwszych wersjach sieci Ethernet do połączenia komputerów w sieć o topologii magistrali był używany gruby kabel koncentryczny (10Base5). Później jego miejsce zastąpił cienki kabel koncentryczny (10Base2) a aktualnie dominują standardy oparte na kablach skrętkowych (10BaseT, 100BaseTX, 1000BaseTX, 10GBaseT) i światłowodowych (100BaseFX, 1000BaseSX, 1000BaseLX, 10GBaseLX4).

**Metoda dostępu do medium CSMA/CD**




*Rysunek 52.*
Metoda dostępu do medium CSMA/CD

Podstawowe założenia, na jakich oparto specyfikowanie standardu IEEE 802.3 wynikały z koncepcji budowy pierwszych sieci Ethernet:

1. Założono, że szybkość pracy sieci będzie równa 10 Mb/s,
2. Dostęp do medium będzie realizowany zgodnie z algorytmem CSMA/CD (patrz rys. 52),
3. Zasięg sieci powinien być rzędu 2.5 km.

Najlepszym rodzajem medium, którym wówczas dysponowano był gruby kabel koncentryczny:

- jego parametry tłumieniowe pozwalały na zapewnienie poprawnej transmisji danych na odcinku nie dłuższym niż 500 metrów, zatem należało wprowadzić cztery regeneratory sygnału,
- kable i regeneratory wprowadzały określone opóźnienia (rzędu 25 μs).

Stosowanie metody CSMA/CD wymaga, aby w przypadku kolizji wszystkie węzły były w stanie ją wykryć, zatem czas trwania ramki nie może być mniejszy niż podwojony czas opóźnienia transferu bitu przez sieć (maksymalnie rzędu 50 μs). Przy założeniu 10 Mb/s szybkości transmisji długość ramki powinna być nie mniejsza niż 500 bitów (10000000 b/s * 50 μs). Stąd przyjęto 512 bitów (64 bajty). W protokole CSMA/CD wprowadzenie sygnału do kanału jest poprzedzane nasłuchem stanu kanału:

- czas ten nie może być krótszy niż czas trwania transmisji 96 bitów,
- w przypadku, gdy kanał jest wolny, strumień bitów wprowadzanych do medium transmisyjnego jest kodowany w układzie sygnalizacji **PLS** (ang. *Physical Layer Signalling*) kodem Manchester,
- w przypadku, gdy nie występuje kolizja ramki przesłanej przez daną stację z innymi ramkami, podwarstwa MAC przekazuje stosowną informację podwarstwie LLC i oczekuje na żądanie przesłania kolejnej ramki.

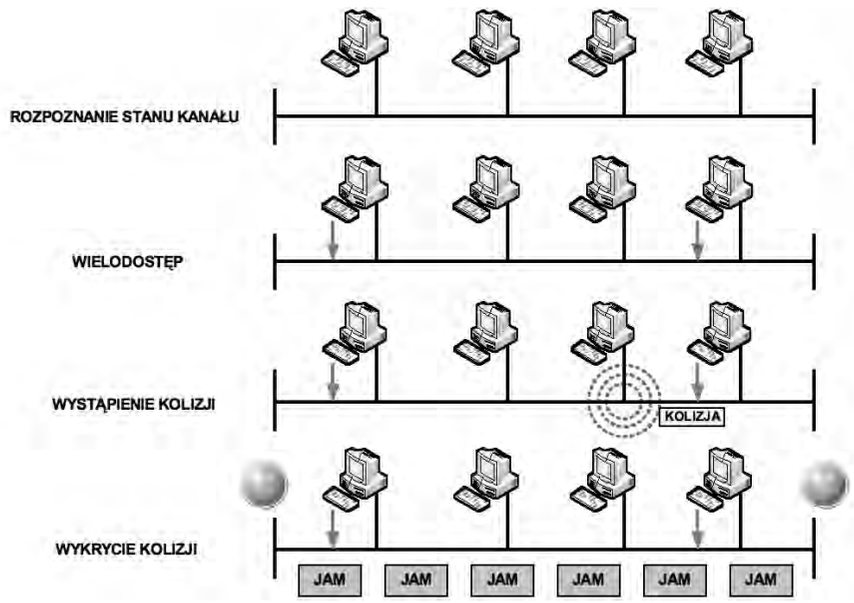
Gdy dwie lub więcej stacji inicjuje transmisje prawie jednocześnie, po stwierdzeniu, że kanał jest wolny, mają miejsce kolizje przesyłanych ramek (objawia się to wzrostem amplitudy sygnału). Kolizje mogą przy tym wystąpić jedynie na początku transmisji ramek w tzw. **oknie wykrywania kolizji** (ang. *collision window*):

- w systemie z 10 MHz pasmem podstawowym czas trwania okna odpowiada czasowi trwania pojedynczej szczeliny i wyrażony w bitach wynosi 512 (odpowiada to minimalnej długości ramki – 64 bajty).

Kolizja ramek jest przez elementy podwarstwy MAC:

- wykryciu kolizji towarzyszy przerwanie transmisji ramki i generacja sygnału zakłócającego (jam), zmuszającego wszystkie stacje do zaprzestania transmisji,
- kolejna transmisja ramki realizowana jest zgodnie z procedurą nazywaną algorytmem z binarnym-wykładniczym rozszerzeniem czasu rywalizacji (binary-exponential back-off).

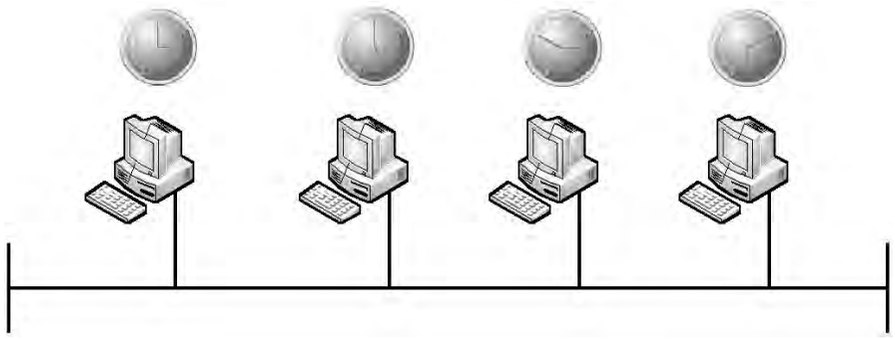
**Sygnał jam**




*Rysunek 53.*
Mechanizm wystąpienia kolizji ramek

W przypadku, gdy dwa urządzenia transmitują równocześnie, procedura CSMA/CD podejmuje działanie mające na celu rozwiązanie tego problemu. Gdy tylko kolizja zostaje wykryta, stacje wysyłające nadają 32-bitowy sygnał zakłócający (jam), który wymusza kolizję. Takie działanie zapewnia, że kolizja zostanie wykryta przez wszystkie urządzenia w sieci (patrz rys. 53). Ważne jest, żeby sygnał zakłócający nie został potraktowany jako poprawna ramka, bo w przeciwnym przypadku kolizja mogłaby nie być zidentyfikowana. Najczęściej występującym wzorcem dla sygnału zakłócającego jest po prostu powtarzający się ciąg jedynek i zer, taki sam jak dla preambuły. Uszkodzona, częściowo nadana wiadomość, jest zwykle nazywana fragmentami kolizyjnymi lub **ramkami karłowatymi** (ang. *runts*). Zwykłe kolizje mają mniej niż 64 oktety długości i dlatego są wykrywane zarówno z powodu zbyt małej długości, jak i przez test sumy kontrolnej **FCS** (ang. *Frame Check Sequence*).

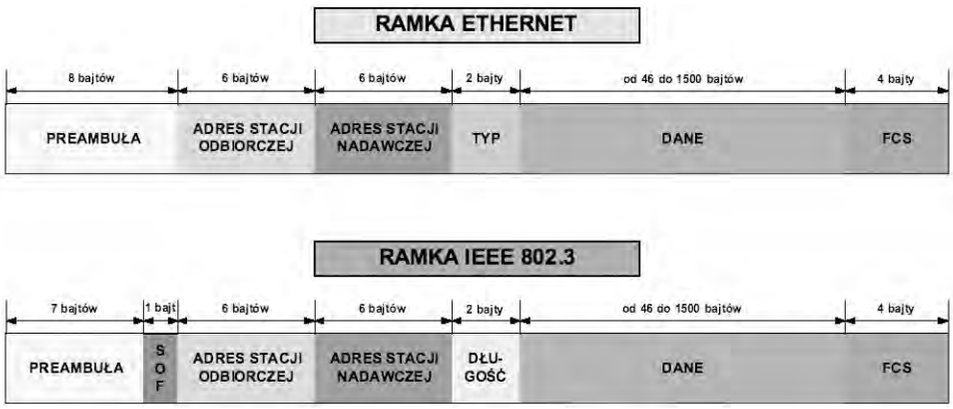
**Metoda backoff**



*Rysunek 54.*
Mechanizm realizacji metody **backoff**

Po wystąpieniu kolizji, stacje biorące udział w kolizji muszą odczekać dodatkowy czas (który może rosnąć wykładniczo) przed przystąpieniem do próby ponownego nadania ramki, przy nadawaniu której wystąpiła kolizja (patrz rys. 54). Okres oczekiwania jest celowo zaprojektowany jako losowy, po to, by dwie stacje nie generowały takiego samego opóźnienia przed ponowieniem transmisji, gdyż powodowałoby to wystąpienie kolejnych kolizji. Częściowo zostało to osiągnięte przez zwiększanie najkrótszego interwału, na podstawie którego jest określany losowy czas ponowienia transmisji przy każdej następnej próbie. Okres oczekiwania jest mierzony w przyrostach jednostki, którą jest szczelina czasowa. Jeśli przeciążenie medium sprawia, że warstwa MAC nie może wysłać ramki, to po 16 próbach rezygnuje ona z tego procesu, a następnie zwraca błąd do warstwy sieci. Takie zdarzenie jest dosyć rzadkie w poprawnie działającej sieci i zachodzi jedynie przy niezmiernie dużych obciążeniach sieci, lub gdy w sieci istnieje jakiś problem natury fizycznej.

**Ramka Ethernet i IEEE 802.3**




*Rysunek 55.*
Różnice w polach ramek standardu Ethernet oraz IEEE 802.3

W IEEE 802.3 ramka rozpoczyna się 7 bajtami preambuły, z których każdy jest ciągiem 10101010. Preambuła umożliwia układowi sygnalizacji **PLS** (ang. *Physical Layer Signalling*) osiągnięcie stabilnej synchronizacji bitowej przy odbiorze ramki. Kolejne pole początkujące ramkę właściwą **SOF** (ang. *Start of Frame*) jest ciągiem o postaci 10101011. Kolejne dwa pola to odpowiednio: 48-bitowy adres MAC stacji odbiorczej oraz adres MAC stacji nadawczej.

W ramce Ethernetowej pojawia się pole typ, które określa protokół warstwy sieciowej natomiast w ramce IEEE 802.3 występuje pole długość , które określa liczbę bajtów danych, jaka następuje po tym polu. Kolejnym polem zarówno w jednej jak i drugiej ramce jest pole danych, mające rozmiar od 46 do 1500 bajtów. Jeżeli długość pola danych jest mniejsza niż 46 bajtów, wówczas pole to ulega wydłużeniu przez dodanie w polu rozszerzenia (*padding*) wymaganej liczby bajtów. Ostatnim polem jest **FCS** (ang. *Frame Check Sequence*), które jest wykorzystywane do wykrywania błędów w ramce. W celu określenia jego wartości, stosowana jest metoda cyklicznego kodu nadmiarowego **CRC** (ang. *Cyclic Redundancy Check*), służąca do obliczenia sumy kontrolnej danych. Urządzenie wysyłające umieszcza wynik sumy kontrolnej w polu FCS ramki. Stacja odbierająca odbiera ramkę i oblicza sumę kontrolną CRC w celu sprawdzenia, czy ramka nie ma błędów. Jeśli wartości są zgodne, to przyjmuje się, że błędy nie wystąpiły. Jeśli wartości CRC nie są zgodne wskazuje to, że dane zostały zmienione i dlatego ramka jest odrzucana.

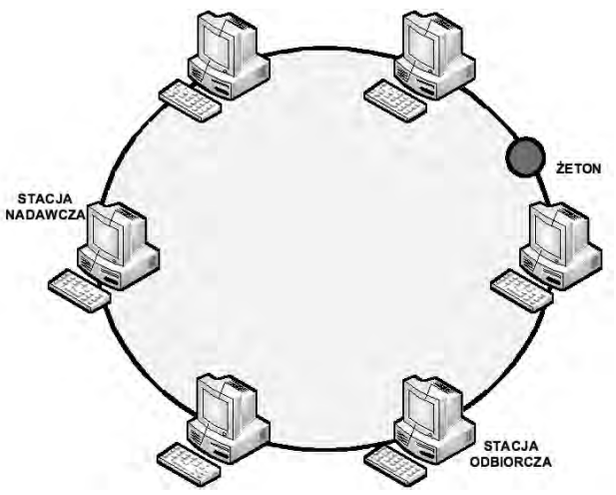
## 3 TECHNOLOGIA TOKEN RING

### Geneza technologii Token Ring

**Token Ring**, jak na dzisiejsze standardy informatyczne, jawi się jako technologia wręcz starożytna. Został stworzony przez firmę IBM jako technologia centrum danych dla pracujących w sieci komputerów *mainframe*. Po raz pierwszy przedstawiono go instytutowi IEEE do standaryzacji w roku 1969. Gdy pojawiły się komputery osobiste, zauważono, że Token Ring może posłużyć do łączenia ich ze sobą. Przyspieszyło to włączenie Token Ringu do projektu IEEE 802. Standaryzacja w ramach projektu 802 wymusiła dokonanie pewnych zmian w warstwie łącza danych, tak aby mogło obsługiwać adresowanie sprzętowe i połączenia mostowe z innymi architekturami LAN 802.

IEEE nazwało Token Ring specyfikacją 802.5 – jest ona niemal identyczna ze specyfikacją Token Ringu firmy IBM. Oprócz wspomnianych wcześniej zmian sprzętowych, IEEE znormalizowała format wiadomości oraz protokoły warstwy 2. Nawiasem mówiąc, IBM był głównym orędownikiem wysiłków standaryzacyjnych IEEE.

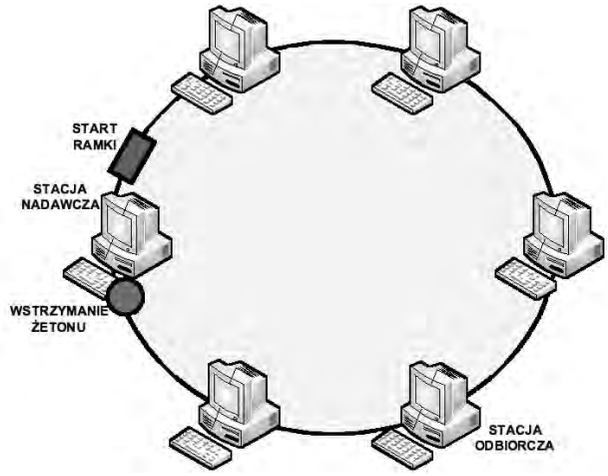
### Jak działa Token Ring



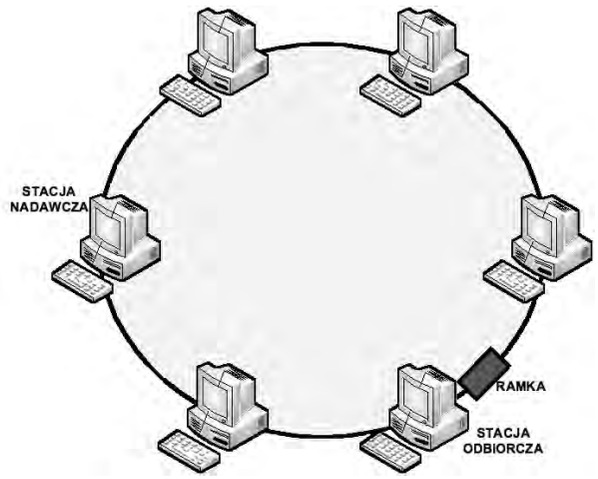

*Rysunek 56.*
Żeton krąży w pierścieniu przechodząc od stacji do stacji

Token Ring i IEEE 802.5 stosują metodę dostępu nazywaną *Token-Passing*. Metoda ta jest również stosowana w technologii FDDI. W pierścieniu sieci Token Ring krąży mała ramka zwana żetonem (ang. *token*). Stacja sieciowa uzyskuje prawo do transmisji informacji tylko wtedy, gdy posiada żeton. Jeśli więc dowolna stacja sieciowa przejmuje żeton, ale w tym momencie nie zamierza transmitować, to przesyła żeton do następnej w kolejności stacji sieciowej.

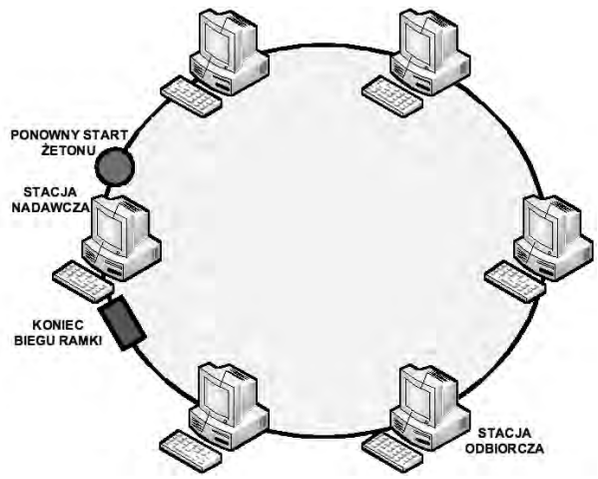
KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
Warszawska Wyższa Szkoła Informatyki
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego




*Rysunek 57.*
Stacja, która przejęła żeton i pragnie nadawać generuje ramkę




*Rysunek 58.*
Ramka krąży w pierścieniu przechodząc od stacji źródłowej do stacji docelowej




*Rysunek 59.*
Po odebraniu ramki stacja generuje następny żeton

Każda stacja może przetrzymywać żeton tylko przez określony czas. Aby zapewnić, że żadna stacja nie zmonopolizuje łącza, stosuje się mechanizm znany jako zegar przetrzymywania żetonu, śledzący i regulujący maksymalną ilość czasu, przez który dowolna stacja może mieć prawo do nadawania. Ten mechanizm czaso-

wy jest przydatny także podczas przywracania normalnego działania sieci w wypadku, gdy stacja posiadająca żeton przestanie działać.

Żetony są rozpoznawane i obsługiwane przez wszystkie stacje pracujące w sieci. Żeton może być tylko jeden i tylko jego posiadacz może nadawać. Żeton jest przekazywany od stacji do stacji w tylko w jednym kierunku. Ponieważ pierścień nie ma jasno zdefiniowanego początku i końca, żeton po prostu ciągle po nim krąży. Mechanizm ten znany jest jako wywoływanie **metodą okrężną** lub inaczej **metodą *round-robin***.

Każda stacja, która otrzyma żeton i chce nadawać, może przekształcić jego strukturę bitową w sekwencję początku ramki **SOF** (ang. *Start of Frame*). Żeton służy więc do utworzenia ramki danych. Nadająca stacja zmienia sekwencję SOF, dodaje potrzebne dane, adresuje je i umieszcza z powrotem w sieci. Jeśli stacja nie chce nadawać, może po prostu z powrotem umieścić żeton w sieci - wtedy otrzyma go kolejna stacja. Gdy ramka dotrze do miejsca przeznaczenia, urządzenie odbierające nie wyciąga ramki z sieci, lecz po prostu kopiuje jej zawartość do bufora w celu dalszego wewnętrznego przetwarzania.

**Ramka Token Ring**


*Rysunek 60.*
Pola ramki **Token Ring**

Minimalna długość ramki w sieci Token Ring wynosi 21 bajtów. Maksymalny rozmiar ramki zależy od prędkości sygnału w pierścieniu. Czas potrzebny na przesłanie ramki musi być mniejszy niż ustalony czas przetrzymywania żetonu – czas ten jest domyślnie ustawiany na 10 milisekund. Pole danych w sieci opartej na żetonie ma zmienną długość, zależną od prędkości sygnału w pierścieniu.

W Token Ringu pracującym z szybkością 4 Mbps daje to maksymalną długość ramki równą 4500 bajtów. Przy szybkości 16 Mbps ramki mogą mieć długość do 18000 bajtów. Ramka Token Ring składa się z następujących pól:

- Start Delimiter – alarmuje każdą stację sieciową o nadejściu żetonu;
- Sterowanie dostępem – składa się z następujących elementów: pola Priorytet, pola Rezerwacja, bitu Token, bitu Monitor;
- Sterowanie ramką – określa, czy ramka ma charakter danych czy informacji sterującej;
- Adres stacji odbiorczej – 48-bitowy adres MAC stacji odbierającej dane;
- Adres stacji nadawczej – 48-bitowy adres MAC stacji wysyłającej dane;
- Dane – długość tego pola jest ograniczona czasem przetrzymywania żetonu przez stację sieciową;
- **FCS** (ang. *Frame Check Sequence*) – sekwencja sprawdzania poprawności dostarczenia ramki;
- Koniec Delimiter – sygnalizuje koniec biegu żetonu. Zawiera także bity wskazujące ramkę błędnie przesłaną oraz identyfikuje ramkę w logicznej sekwencji;
- Stan ramki – pole kończące ramkę.

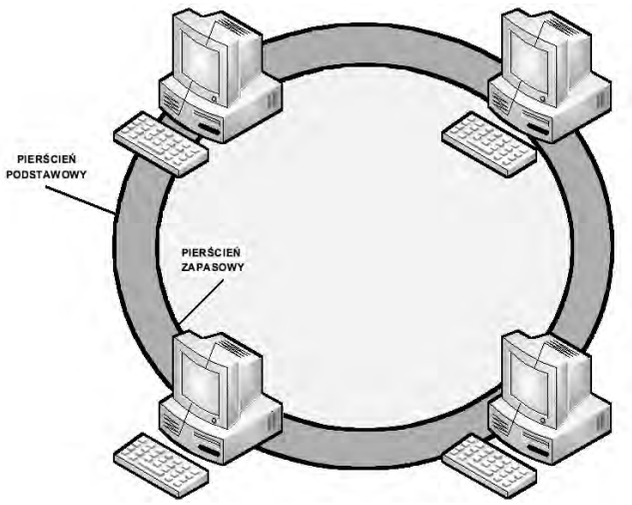
## 4 TECHNOLOGIA FDDI

**Wprowadzenie do FDDI**

Technologia **FDDI** (ang. *Fiber Distributed Data Interface*) została opracowana przez Komitet X3T9.5 amerykańskiego Instytutu **ANSI** (ang. *American National Standards Institute*) w połowie lat 80 ubiegłego wieku. FDDI jest standardem sieci lokalnej LAN o następujących parametrach:

1. Przepływność: 100 Mb/s,
2. Metoda dostępu: Token-Passing,
3. Maksymalna długość pierścieni: 200 km,
4. Medium transmisyjne: kabel światłowodowy,
5. Topologia: podwójny pierścień (*Dual-Ring*).

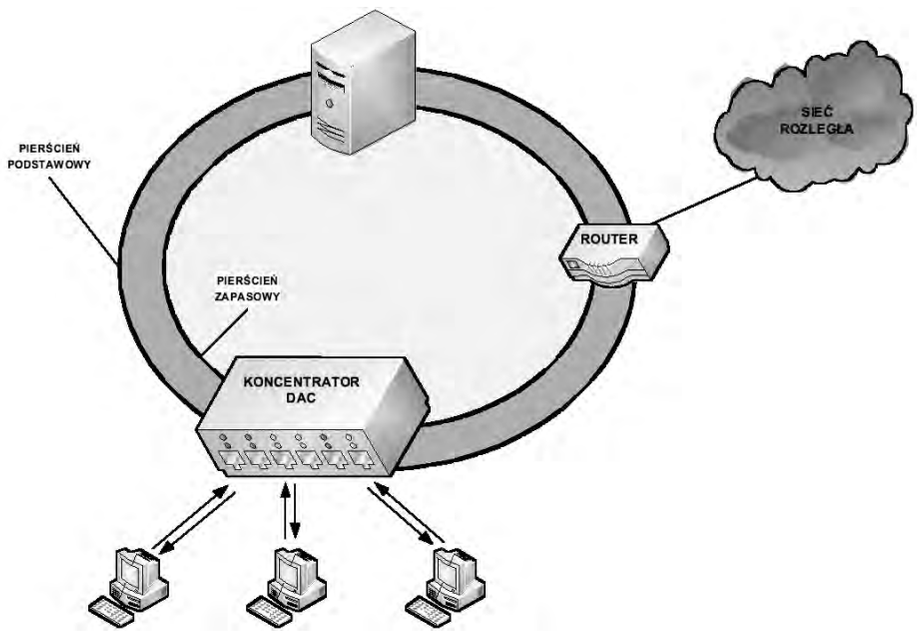
KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
Warszawska Wyższa Szkoła Informatyki
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego




*Rysunek 56.*
Pierścienie (podstawowy i zapasowy) przenoszące dane w sieciach FDDI

Technologia FDDI jest często używana do budowy sieci szkieletowych ze względu na jej istotne zalety: dużą przepływność i niezawodność oraz możliwość stosowania na długich dystansach. Niedawno wprowadzono odmianę FDDI, tzw. technologię **CDDI** (ang. *Copper Distributed Data Interface*), której istotą jest stosowanie protokołów FDDI, ale na infrastrukturze kablowej zbudowanej z miedzianego kabla, również zapewniającej przepływność 100 Mb/s. W technologii FDDI stosuje się topologię podwójnego pierścienia, czyli struktury składającej się z dwóch różnych fizycznie pierścieni światłowodowych. Ruch ramek w każdym z nich odbywa się w przeciwnym kierunku (patrz rys. 56).

**Działanie FDDI**

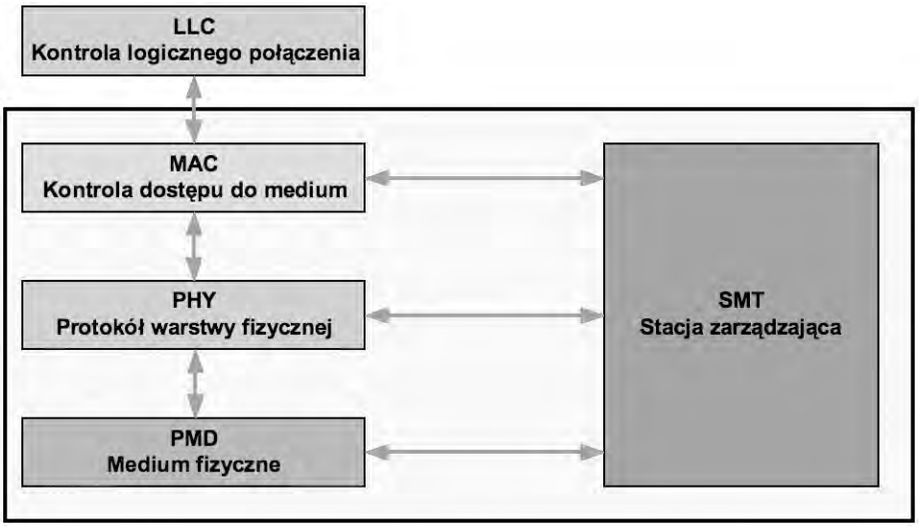



*Rysunek 57.*
Mechanizm działania technologii FDDI

Pierwszy z pierścieni zwany **podstawowym** (ang. *primary ring*), a drugi zwany **dodatkowym** (ang. *secondary ring*). Ruch w pierścieniach odbywa się w przeciwnych kierunkach. W czasie normalnej pracy, pierścień podstawowy służy do transmisji danych, a pierścień dodatkowy jest nieczynny. Zasadniczym celem podwójnego pierścienia jest zapewnienie wysokiego poziomu niezawodności (patrz rys. 57).

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

**Specyfikacje FDDI**




*Rysunek 58.*
Specyfikacje technologii FDDI

Technologia FDDI sprecyzowana jest w czterech oddzielnych specyfikacjach, z których każda opisuje określoną funkcję (patrz rys. 58). Łącznie zapewniają one możliwość szybkiego połączenia między protokołami wyższych warstw, np. TCP/IP, a medium takim jak kabel światłowodowy. Specyfikacje FDDI są następujące:

1. **MAC** (ang. *Media Access Control*);
2. **PHY** (ang. *Physical-Layer Protocol*);
3. **PMD** (ang. *Physical-Medium Depedent*);
4. **SMT** (ang. *Station Management*).

Specyfikacja **MAC** definiuje metodę dostępu do medium, w tym format ramki, sterowanie elementem token, adresowanie, algorytmy dla obliczania wartości **CRC** i mechanizm usuwania błędów.

Specyfikacja **PHY** definiuje procedurę kodowania/dekodowania, wymagania na zegar, tworzenie ramek i inne funkcje.

**PMD** specyfikuje charakterystyki medium transmisyjnego, poziomy mocy, częstotliwość występowania błędów, komponenty optyczne i złącza.

Specyfikacja **SMT** określa konfiguracje stacji FDDI, konfiguracje pierścienia i sposoby sterowania pierścieniem, podłączanie i usuwanie stacji, izolowanie i usuwanie błędów.

Jedną z charakterystycznych cech technologii FDDI jest możliwość wielorakiego podłączania stacji sieciowych do pierścienia. Specyfikacja FDDI definiuje trzy sposoby podłączania:

- stacja podłączana do pojedynczego pierścienia **SAS** (ang. *Single-Attachment Station*),
- stacja podłączana do podwójnego pierścienia **DAS** (ang. *Dual-Attachment Station*),
- koncentrator podłączany do podwójnego pierścienia **DAC** (ang. *Dual-Attachment Concentrator*).

**Ramka FDDI**


*Rysunek 59.*
Pola ramki FDDI

Ramka FDDI składa się z następujących pól:

- Preambuła – unikalna sekwencja przygotowująca każdą stację do przyjęcia nadchodzącej ramki;

- Start Delimiter – wskazuje początek ramki przez zadziałanie wzoru sygnalizacyjnego, który odróżnia go od reszty ramki;
- Sterowanie ramką – wskazuje rozmiar pól adresowych, rodzaj danych i inne informacje sterujące;
- Adres stacji odbiorczej – 48-bitowy adres MAC stacji odbierającej dane;
- Adres stacji nadawczej – 48-bitowy adres MAC stacji wysyłającej dane;
- Dane – zawiera dane przeznaczone dla protokołu wyższego poziomu lub informację sterującą;
- **FCS** (ang. *Frame Check Sequence*) – sekwencja sprawdzania poprawności dostarczenia ramki;
- Koniec Delimiter – zawiera unikalne symbole wskazujące koniec ramki;
- Status ramki – zezwala stacji nadawczej określić, czy wystąpił błąd oraz czy ramka została rozpoznana i skopiowana przez stację odbiorczą.

## 5 WIRTUALNE SIECI LAN

### Wprowadzenie do sieci VLAN

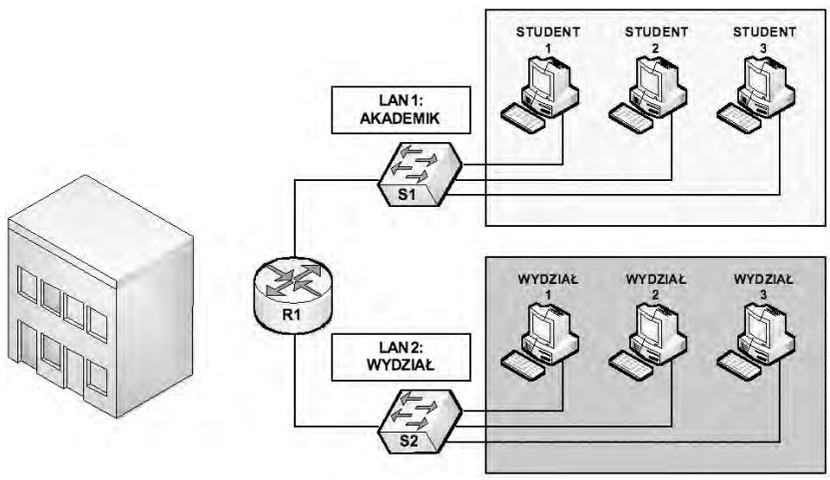
Istotną cechą przełączania w sieciach Ethernet jest możliwość tworzenia wirtualnych sieci LAN (VLAN). Sieć VLAN jest logiczną grupą stacji i urządzeń sieciowych. Sieci VLAN można tworzyć na podstawie stanowisk lub departamentów w firmie, niezależnie od miejsca, w którym fizycznie znajdują się użytkownicy. Ruch między sieciami VLAN jest ograniczony. Przełączniki i mosty przekazują ruch transmisji pojedynczej (unicast), rozsyłania grupowego oraz rozgłaszania tylko w tych segmentach LAN, które obsługują sieć VLAN, do której ruch ten należy. Innymi słowy, urządzenia w sieci VLAN komunikują się tylko z urządzeniami znajdującymi się w tej samej sieci VLAN. Połączenie między sieciami VLAN zapewniają routery.

Sieci VLAN zwiększają ogólną wydajność sieci poprzez logiczne grupowanie użytkowników i zasobów. Firmy często używają sieci VLAN w celu logicznego grupowania określonych użytkowników niezależnie od ich fizycznego rozmieszczenia. Za pomocą sieci VLAN można pogrupować użytkowników pracujących w jednym departamencie. Na przykład pracownicy Dziekanatu są umieszczani w sieci VLAN Dziekanat, a pracownicy Rektoratu – w sieci VLAN Rektorat.

Sieci VLAN mogą zwiększyć skalowalność i bezpieczeństwo sieci oraz usprawnić zarządzanie nią. Routery w sieciach VLAN filtrują ruch rozgłoszeniowy, zapewniają bezpieczeństwo i służą do zarządzania przepływem.

Właściwie zaprojektowane i skonfigurowane sieci VLAN stanowią bogate w możliwości narzędzie dla administratorów sieci. Sieci VLAN upraszczają dodawanie, przenoszenie i modyfikacje w sieciach. Zwiększają także bezpieczeństwo sieci i pomagają sterować rozgłaszaniem w warstwie 3. Jednakże niepoprawnie skonfigurowana sieć VLAN może zaburzyć funkcjonowanie sieci lub całkowicie je uniemożliwić. Prawidłowa konfiguracja i implementacja sieci VLAN jest kluczowym elementem procesu projektowania sieci.

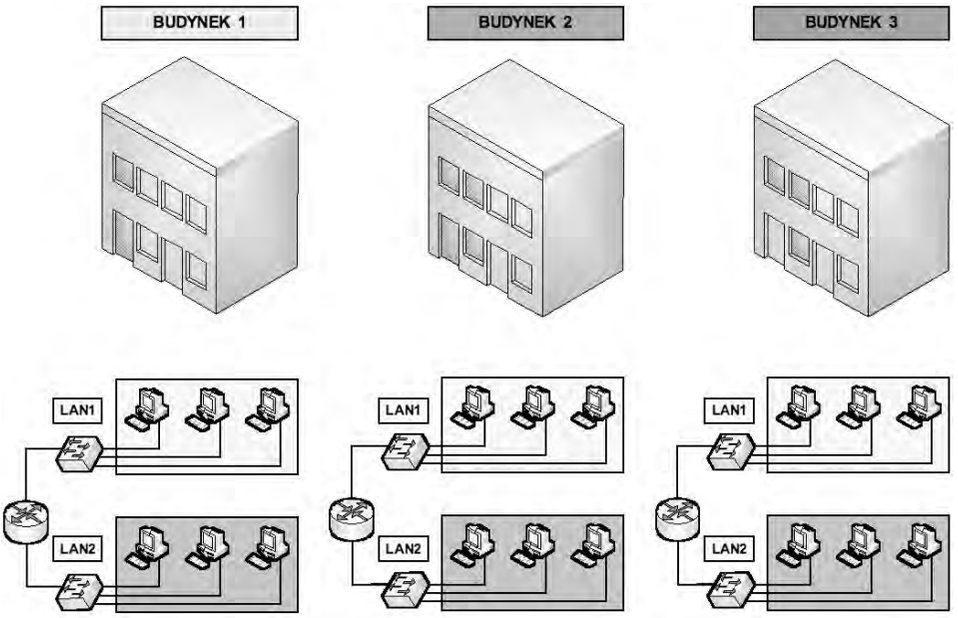
### Bez sieci VLAN – jeden budynek




*Rysunek 60.*
Przykład połączeń sieciowych w jednym budynku

Aby uświadomić sobie, dlaczego sieci VLAN są dzisiaj powszechnie używane, rozważmy uczelnię wyższą z akademikiem i biurami wydziałów mieszczącymi się w jednym budynku. Na rysunku 60 pokazano komputery studenckie w jednej sieci LAN (AKADEMIK) i komputery wydziałowe w drugiej sieci LAN (WYDZIAŁ). Rozwiązanie to dobrze się sprawdza, ponieważ poszczególne wydziały są fizycznie skupione, a zatem łatwo jest zapewnić im niezbędne zasoby sieciowe.

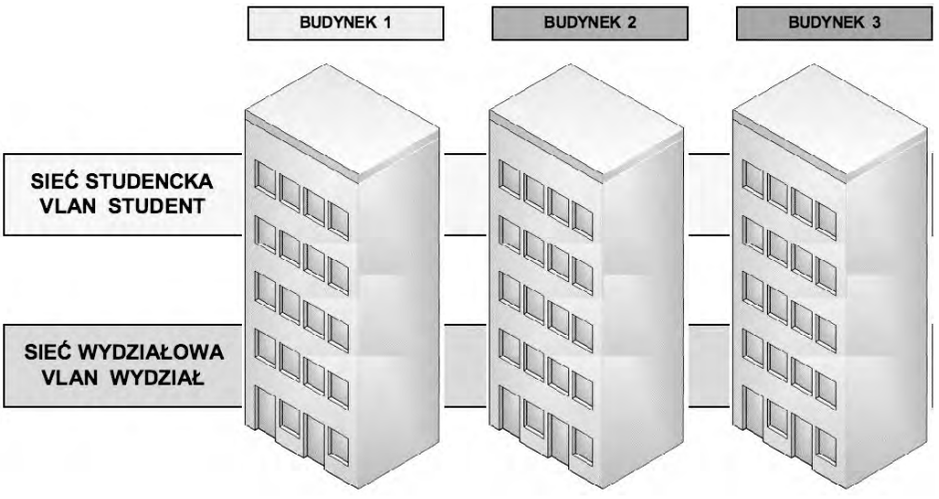
**Bez sieci VLAN – trzy budynki**




*Rysunek 61.*
Przykład połączeń sieciowych w trzech budynkach – bez VLAN

Po jakimś czasie uczelnia wyższa rozrosła się i aktualnie ma już trzy budynki. Na rysunku 61 widzimy, że pierwotna sieć nie uległa zmianie, lecz komputery studenckie i wydziałowe są rozproszone między trzy budynki. Zakład Systemów Teleinformatycznych chce jednak, aby wszystkie komputery studenckie korzystały z tych samych mechanizmów zabezpieczających i kontrolujących wykorzystanie szerokości pasma. Wygodne byłoby zgrupowanie ludzi wraz z wykorzystywanymi przez nich zasobami bez względu na ich lokalizację, co ułatwiłoby zarządzanie ich specyficznymi wymaganiami w kwestii bezpieczeństwa i szerokości pasma.

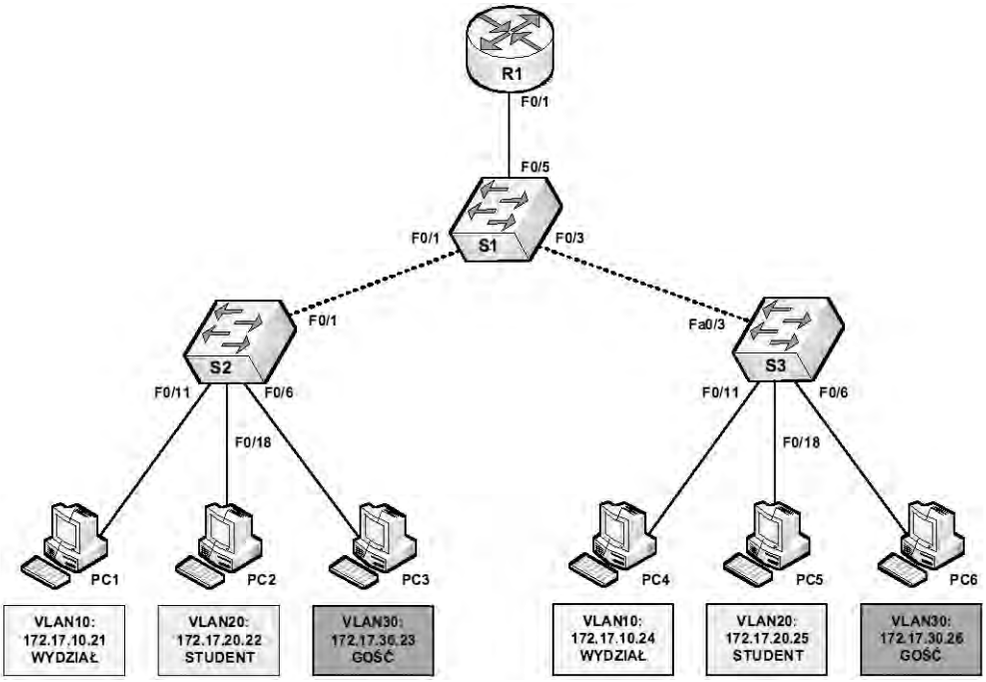
**Sieci VLAN – trzy budynki**




*Rysunek 62.*
Przykład połączeń sieciowych w trzech budynkach – z zastosowaniem VLAN

Optymalnym rozwiązaniem uprzednio zdefiniowanego problemu dla uczelni wyższej jest skorzystanie z technologii lokalnej sieci wirtualnej (VLAN). Technologia VLAN umożliwia administratorowi sieci tworzenie grupy urządzeń połączonych logicznie, które działają tak, jakby znajdowały się w swojej niezależnej sieci, nawet jeśli współdzielą infrastrukturę z innymi sieciami VLAN. Na rysunku 62 przedstawiono jedną sieć VLAN utworzoną dla studentów i drugą sieć VLAN utworzoną dla wydziału. Sieci te umożliwiają administratorowi zaimplementowanie zasad kontroli dostępu i bezpieczeństwa obowiązujących dla konkretnych grup użytkowników.

**Działanie sieci VLAN**




*Rysunek 63.*
Przykładowy scenariusz połączeń pomiędzy sieciami VLAN

Sieć VLAN jest oparta na sieci przełączanej, która została logicznie posegmentowana. Do sieci VLAN można przypisać każdy z portów przełącznika. Porty przypisane do sieci VLAN odbierają i przekazują te same pakiety rozgłoszeniowe. Porty, które nie należą do tej sieci, nie przekazują tych pakietów. Zwiększa to wydajność sieci, ponieważ zmniejsza się ilość zbędnych pakietów rozgłoszeniowych. W momencie, gdy urządzenie jest dołączane do sieci, automatycznie przyjmuje ono członkostwo w sieci VLAN tego portu, do którego zostało podłączone.

Użytkownicy przyłączeni do tego samego współużytkowanego segmentu wspólnie korzystają z przepustowości tego segmentu. Każdy dodatkowy użytkownik przyłączony do wspólnego nośnika oznacza mniejszą przepustowość i spadek wydajności sieci. Sieci VLAN zapewniają użytkownikom większą przepustowość niż współużytkowane sieci Ethernet oparte na koncentratorach. Domyślną siecią VLAN dla każdego portu przełącznika jest sieć VLAN zarządzania. Siecią VLAN zarządzania jest zawsze sieć VLAN 1. Sieci tej nie można usunąć. Aby móc zarządzać przełącznikiem, do sieci VLAN 1 musi być przypisany co najmniej jeden port. Wszystkie inne porty przełącznika mogą być przypisane do innych sieci VLAN.

Sieci VLAN z członkostwem dynamicznym są tworzone przez oprogramowanie zarządzające siecią. Dynamiczne sieci VLAN przyjmują członkostwo na podstawie adresu MAC urządzenia podłączonego do portu przełącznika. W momencie, gdy urządzenie jest podłączane do sieci, przełącznik, do którego jest ono podłączone, odpytuje bazę danych serwera konfiguracyjnego VLAN o członkostwo w sieci.

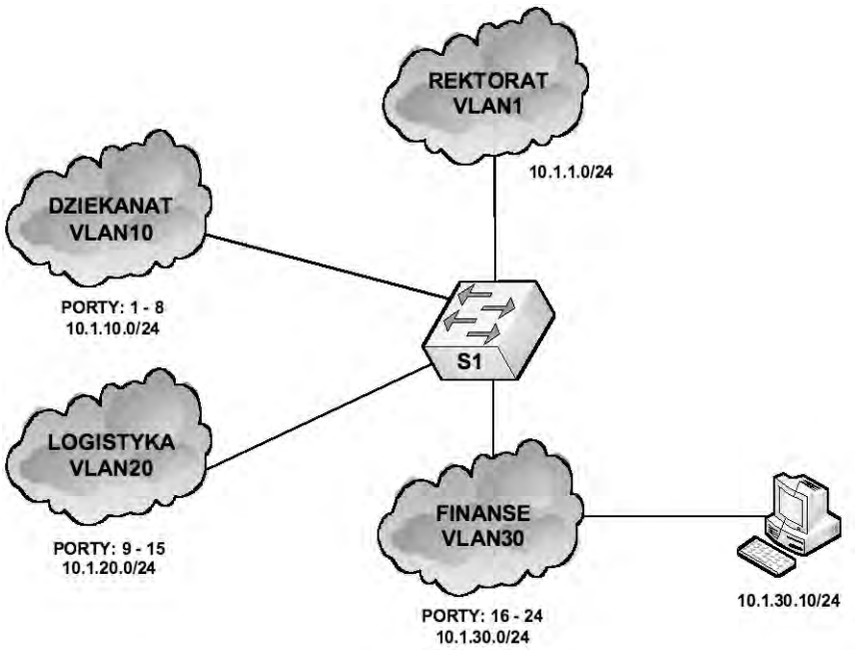
W członkostwie opartym na portach port jest przypisywany do konkretnej sieci VLAN niezależnie od użytkownika lub systemu podłączonego do portu. Gdy używana jest ta metoda członkostwa, wszyscy użytkownicy danego portu muszą być w tej samej sieci VLAN. Do portu może być podłączona dowolna liczba użytkowników, którzy nie zdają sobie sprawy, że sieć VLAN istnieje. Ułatwia to zarządzanie, ponieważ do segmentacji sieci VLAN nie są potrzebne złożone tablice wyszukiwania.

**Zalety sieci VLAN**

Sieci VLAN umożliwiają administratorom sieci logiczne, zamiast fizycznego, organizowanie struktury sieci LAN. Jest to kluczowa zaleta tych sieci. Dzięki temu administratorzy mogą wykonywać następujące zadania:

1. Łatwo przenosić stacje robocze w sieci LAN;
2. Łatwo dodawać stacje robocze do sieci LAN;
3. Łatwo zmieniać konfigurację sieci LAN;
4. Łatwo nadzorować ruch w sieci;
5. Zwiększyć bezpieczeństwo.

**Konfiguracja sieci VLAN**




*Rysunek 64.*
Przykładowa topologia sieciowa z zastosowaniem VLAN

Dla topologii przedstawionej na rysunku 64 skonfigurujemy sieci VLAN za pomocą następujących poleceń:

| | |
|---|---|
| **Switch›enable** | – wejście w tryb uprzywilejowany |
| **Switch#configure terminal** | – wejście w tryb konfiguracji globalnej |
| **Switch(config)#hostname S1** | – ustawienie nazwy przełącznika |
| **S1(config)#vlan 10** | – utworzenie sieci VLAN 10 i wejście w tryb konfiguracji VLAN |
| **S1(config-vlan)#name DZIEKANAT** | – przypisanie nazwy sieci VLAN |
| **vlan)#exit-vlan)#exit** | – powrót do trybu konfiguracji globalnej |
| **S1(config)#vlan 20** | – utworzenie sieci VLAN 20 i wejście w tryb konfiguracji VLAN |
| **S1(config-vlan)#name LOGISTYKA** | – przypisanie nazwy sieci VLAN |
| **S1(config-vlan)#exit** | – powrót do trybu konfiguracji globalnej |
| **S1(config)#vlan 30** | – utworzenie sieci VLAN 30 i wejście w tryb konfiguracji VLAN |
| **S1(config-vlan)#name FINANSE** | – przypisanie nazwy sieci VLAN |
| **S1(config-vlan)#exit** | – powrót do trybu konfiguracji globalnej |
| **S1(config)#interface range fastethernet 0/1 – 8** | – umożliwienie jednoczesnego ustawienia takich samych parametrów konfiguracji na wielu portach |
| **S1(config-if-range)#switchport mode access** | – ustawienie portów 1–8 jako porty dostępowe |
| **S1(config-if-range)#switchport access vlan 10** | – przypisanie portów 1–8 do VLAN 10 |
| **S1(config-if-range)#exit** | – powrót do trybu konfiguracji globalnej |
| **S1(config)#interface range fastethernet 0/9 – 15** | – umożliwienie jednoczesnego ustawienia takich samych parametrów konfiguracji na wielu portach |

| | | |
|---|---|---|
| **S1(config-if-range)#switchport mode access** | – | ustawienie portów 9–15 jako porty dostępowe |
| **S1(config-if-range)#switchport access vlan 20** | – | przypisanie portów 9–15 do VLAN 20 |
| **S1(config-if- range)#exit** | – | powrót do trybu konfiguracji globalnej |
| **S1(config)#interface range fastethernet 0/16 – 24** | – | umożliwienie jednoczesnego ustawienia takich samych parametrów konfiguracji na wielu portach |
| **S1(config-if-range)#switchport mode access** | – | ustawienie portów 16–24 jako porty dostępowe |
| **S1(config-if-range)#switchport access vlan 30** | – | przypisanie portów 16–24 do VLAN 30 |
| **S1(config-if-range)#exit** | – | powrót do trybu konfiguracji globalnej |
| **S1(config)#exit** | – | powrót do trybu uprzywilejowanego |
| **S1#copy running-config startup-config** | – | zapisanie konfiguracji w pamięci NVRAM |

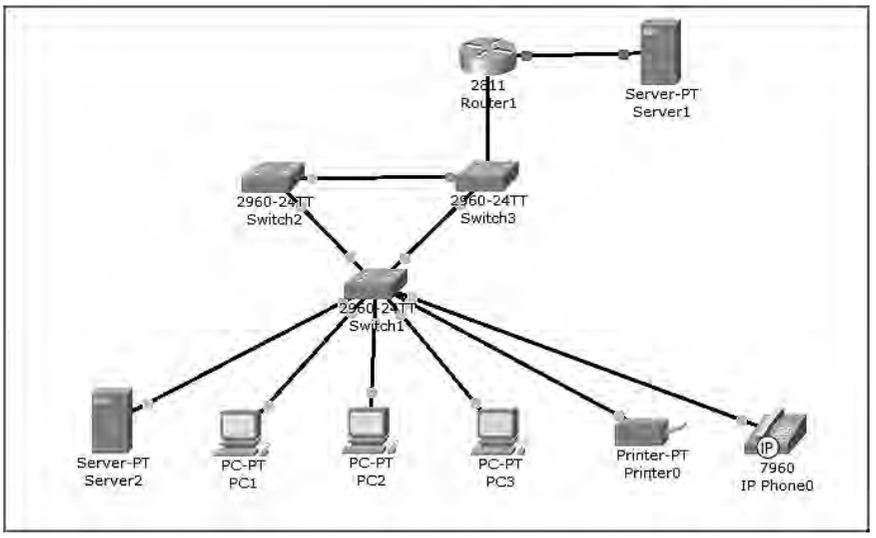
## LITERATURA


1. Empson S., *Akademia sieci Cisco. CCNA Pełny przegląd poleceń*, WN PWN, Warszawa 2008
2. Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2005
3. Lewis W., *Akademia sieci Cisco. CCNA Exploration. Przełączanie sieci LAN i sieci bezprzewodowe*, WN PWN, Warszawa 2009
4. Lewis W., *CCNA semestr 3. Podstawy przełączania oraz routing pośredni*, WN PWN, Warszawa 2007
5. Mucha M., *Sieci komputerowe. Budowa i działanie*, Helion, Gliwice 2003
6. *Vademecum teleinformatyka*, IDG Poland SA, Warszawa 1999


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

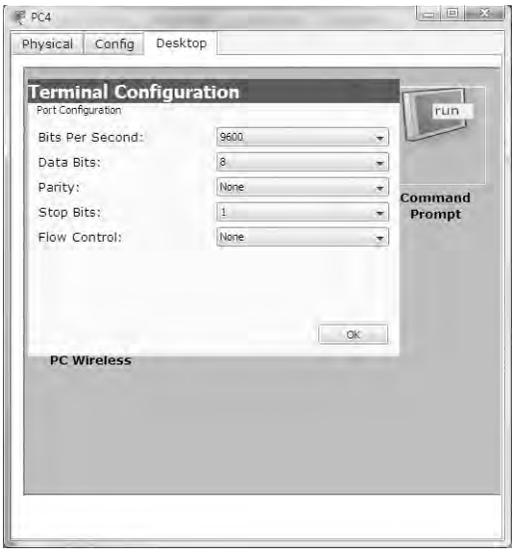
## WARSZTATY

**Ćwiczenie 1.** Stworzenie interaktywnego modelu sieciowego z wykorzystaniem oprogramowania Packet Tracer (firmy Cisco Systems).




*Rysunek 65.*
Model topologii sieci

**Ćwiczenie 2.** Podłączenie stacji zarządzającej.




*Rysunek 66.*
Konfiguracja terminala do połączenia z portem konsolowym

**Ćwiczenie 3.** Konfiguracja portu konsolowego.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#password test
Switch(config-line)#login
Switch(config-line)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

*Tabela 1.*
Tabela adresacji sieci

| Urządzenie | Interfejs | Adres | Maska | Brama domyślna |
|---|---|---|---|---|
| **Router1** | **Fa0/0** | 192.168.50.1 | 255.255.255.0 | N/A |
| | **Fa0/1.10** | 192.168.10.1 | 255.255.255.0 | N/A |
| | **Fa0/1.20** | 192.168.20.1 | 255.255.255.0 | N/A |
| | **Fa0/1.30** | 192.168.30.1 | 255.255.255.0 | N/A |
| | **Fa0/1.99** | 192.168.99.1 | 255.255.255.0 | N/A |
| **Switch1** | **VLAN 99** | 192.168.99.31 | 255.255.255.0 | 192.168.99.1 |
| **Switch2** | **VLAN 99** | 192.168.99.32 | 255.255.255.0 | 192.168.99.1 |
| **Switch3** | **VLAN 99** | 192.168.99.33 | 255.255.255.0 | 192.168.99.1 |
| **PC1** | **NIC** | 192.168.10.21 | 255.255.255.0 | 192.168.10.1 |
| **PC2** | **NIC** | 192.168.20.22 | 255.255.255.0 | 192.168.20.1 |
| **PC3** | **NIC** | 192.168.30.23 | 255.255.255.0 | 192.168.30.1 |
| **PC4** | **NIC** | 192.168.10.24 | 255.255.255.0 | 192.168.10.1 |
| **PC5** | **NIC** | 192.168.20.25 | 255.255.255.0 | 192.168.20.1 |
| **PC6** | **NIC** | 192.168.30.26 | 255.255.255.0 | 192.168.30.1 |

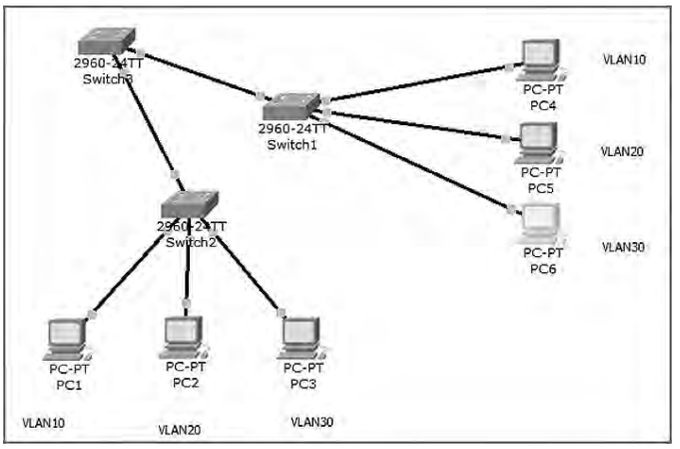
**Ćwiczenie 4.** Konfiguracja przełącznika.

Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 99
Switch(config-if)#ip address 192.168.99.33 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastethernet 0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport acces vlan 99

%LINK-5-CHANGED: Interface Vlan99, changed state to up% Access VLAN does not exist. Creating vlan 99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to upSwitch(config-if)
Switch(config)#ip default-gateway 192.168.99.1
Switch(config)#end
%SYS-5-CONFIG_I: Configured from console by console

witch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable secret class
Switch(config)#line vty 0 15
Switch(config-line)#password test
Switch(config-line)#^Z
%SYS-5-CONFIG_I: Configured from console by console

**Konfiguracja i weryfikacja działania sieci VLAN**




*Rysunek 67.*
Schemat topologii sieci VLAN

**Ćwiczenie 5.** Utworzenie VLAN-ów.

Switch(config)#vlan 10
Switch(config-vlan)#name Student
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Wykladowca
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name Administracja
Switch(config-vlan)#vlan 99
Switch(config-vlan)#name Zarzadzanie
– przydzielenie portów do VLAN-ów
Switch(config)#interface fastethernet 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface fastethernet 0/10
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#interface fastethernet 0/15
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#^Z

**Ćwiczenie 6.** Konfiguracja trunk (łącza multipleksowanego).

Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch(config-if)#switchport trunk nativ
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#interface fastethernet 0/3
Switch(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
Switch(config-if)#switchport trunk native vlan 99

**Ćwiczenie 7.** Weryfikacja działania sieci VLAN.

PC3›ipconfig
IP Address.....: 192.168.30.26
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.30.1

PC›ping 192.168.30.23 (do PC6)
Pinging 192.168.30.23 with 32 bytes of data:

Reply from 192.168.30.23: bytes=32 time=220ms TTL=128
Reply from 192.168.30.23: bytes=32 time=109ms TTL=128
Reply from 192.168.30.23: bytes=32 time=125ms TTL=128
Reply from 192.168.30.23: bytes=32 time=96ms TTL=128

Ping statistics for 192.168.30.23:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 96ms, Maximum = 220ms, Average = 137ms

**Konfiguracja i weryfikacja działania protokołu VTP**

**VTP** (ang. *VLAN Trunking Protocol*) – protokół komunikacyjny działający w warstwie drugiej modelu ISO/OSI, służący do zarządzania wieloma sieciami wirtualnymi na jednym, wspólnym łączu fizycznym. Pozwala on administratorowi na takie skonfigurowanie przełącznika, że może on rozsyłać konfigurację do innych przełączników w sieci. Protokół VTP działa w jednym z trzech trybów:

- tryb serwera – jest domyślnym trybem VTP. Jest możliwa edycja sieci VLAN, wersji VTP. Wszelkie zmiany są rozsyłane do innych urządzeń pracujących w sieci;
- tryb transparentny – istnieje możliwość edycji sieci wirtualnych, ale zmiany mają wpływ tylko na lokalny przełącznik. Przełącznik przekazuje ogłoszenia VTP, ale ich nie tworzy, ani nie przetwarza;
- tryb klienta – nie można edytować ustawień sieci VLAN. Informacje o sieciach VLAN są synchronizowane z innymi klientami i serwerami VTP.

**Ćwiczenie 8.** Konfiguracja serwera VTP.

Switch3(config)#vtp domain kurs1
Changing VTP domain name from NULL to kurs1
Switch3(config)#vtp version 1
VTP mode already in V1.
Konfiguracja klientów VTP:
Switch1(config)#vtp mode client
Setting device to VTP CLIENT mode

Switch2(config)#vtp mode client
Setting device to VTP CLIENT mode

**Konfiguracja i weryfikacja działania protokołu STP**

**Protokół drzewa rozpinającego** (ang. *Spanning-Tree Protocol* – STP) – jest to protokół wykorzystywany przez sieci komputerowe (np. LAN) w drugiej warstwie modelu sieciowego ISO/OSI. STP obsługiwany jest przez przełączniki i mostki sieciowe. Stworzony został dla zwiększenia niezawodności środowisk sieciowych, umożliwia on konfigurację tych urządzeń w sposób zapobiegający powstawaniu pętli. Protokół ten tworzy graf bez pętli (drzewo) i ustala zapasowe łącza. W trakcie normalnej pracy sieci blokuje je tak, by nie przekazywały one żadnych danych. Wykorzystywana jest tylko jedna ścieżka, po której może odbywać się komunikacja. Na szczycie grafu znajduje się główny przełącznik tzw. (ang.

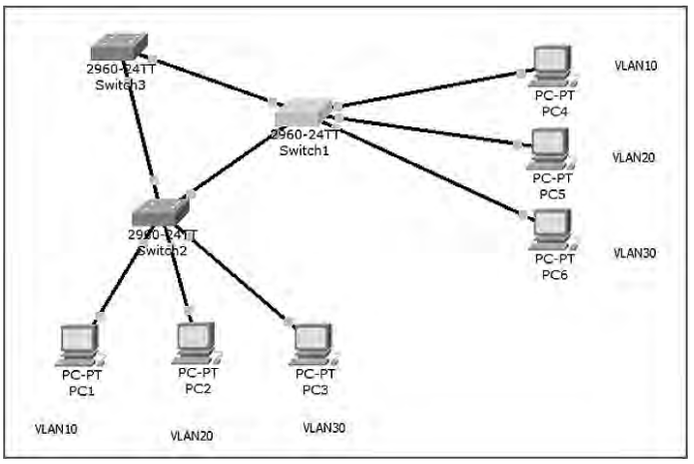
*root*), zarządzający siecią. Root'em zostaje przełącznik na podstawie identyfikatora. W momencie, gdy STP wykryje problem, np. zerwany link, to rekonfiguruje sieć uaktywniając łącze zapasowe (potrzebuje na to ok. 30 do 60 sekund).

Po ustabilizowaniu pracy sieci osiąga ona zbieżność i w każdej sieci istnieje jedno drzewo opinające. W wyniku tego we wszystkich sieciach przełączanych występują następujące elementy:

- jeden most główny w każdej sieci,
- jeden port główny w każdym moście oprócz mostu głównego,
- jeden port wyznaczony w każdym segmencie,
- porty nieużywane (takie, które nie zostały wyznaczone).

Porty przełącznika w topologii STP przyjmują pięć stanów od których zależy, w jaki sposób protokół MAC przetwarza i transmituje ramki:

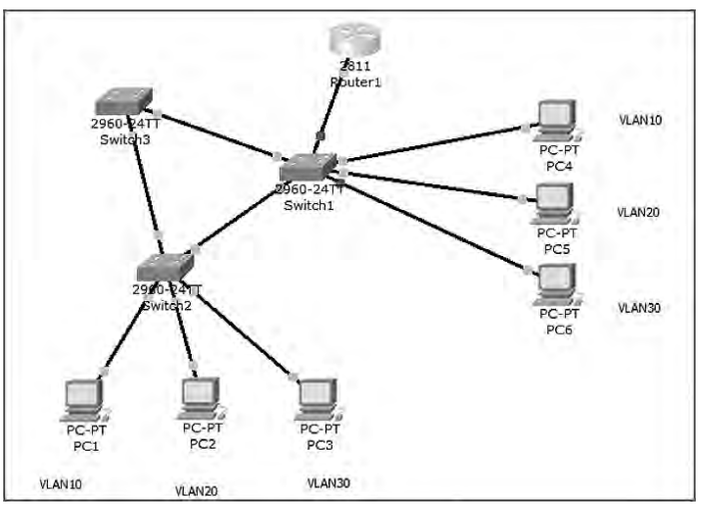
- port aktywny (ang. *listening*);
- uczenie się adresów MAC (ang. *learning*);
- przekazywanie ramek (ang. *forwarding*);
- port zablokowany (ang. *blocking*);
- odrzucanie ramek (ang. *discarding*).




*Rysunek 68.*
Schemat topologii sieci do badania działania protokołu STP

**Routing pomiędzy sieciami VLAN**

Routing pomiędzy sieciami VLAN jest procesem przekazywania ruchu sieciowego z jednej sieci VLAN do innej z wykorzystaniem routera lub przełącznika warstwy 3.




*Rysunek 69.*
Schemat topologii sieci do konfiguracji routingu pomiędzy sieciami VLAN

**Ćwiczenie 9.** Konfiguracja przełącznika.

```
Switch1(config)#int f0/24
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up
Konfiguracja routera:
Router1(config)#interface f0/0.10 (kreowanie subinterfejsów)
Router1(config-subif)#encapsulation dot1Q 10
Router1(config-subif)#ip address 192.168.10.1 255.255.255.0
Router1(config-subif)#interface f0/0.20
Router1(config-subif)#encapsulation dot1Q 20
Router1(config-subif)#ip address 192.168.20.1 255.255.255.0
Router1(config-subif)#interface f0/0.30
Router1(config-subif)#encapsulation dot1Q 30
Router1(config-subif)#ip address 192.168.30.1 255.255.255.0
Router1(config-subif)#int f0/0
Router1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up
```

**Ćwiczenie 10.** Weryfikacja działania routingu pomiędzy sieciami VLAN.

```
PC>ipconfig
IP Address.....: 192.168.10.21
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.10.1

PC>ping 192.168.20.22
Pinging 192.168.20.22 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.22: bytes=32 time=250ms TTL=127
Reply from 192.168.20.22: bytes=32 time=218ms TTL=127
Reply from 192.168.20.22: bytes=32 time=234ms TTL=127

Ping statistics for 192.168.20.22:
   Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
   Minimum = 218ms, Maximum = 250ms, Average = 234ms

PC>tracert 192.168.20.22
Tracing route to 192.168.20.22 over a maximum of 30 hops:
 1   93 ms    110 ms    109 ms    192.168.10.1
 2   250 ms    156 ms    187 ms    192.168.20.22
Trace complete.
```

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**

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