1. Podstawowe informacje o sieciach komputerowych.

Sieć komputerowa jest to zespół oddalonych od siebie komputerów i urządzeń peryferyjnych, połączonych ze sobą liniami transmisji danych; w przypadku sieci specjalizowanych – również urządzeń o specjalnych funkcjach (np. uliczne automaty wydające gotówkę w sieci bankowej, punkty ogniowe w sieciach militarnych i inne). Zależnie od wielkości, rodzaju i stopnia złożoności sieci komputerowej, liniami transmisyjnymi danych mogą być zwykłe kable lub linie telekomunikacyjne. Sieć komputerowa może ograniczać się do jednego lub kilku budynków, do miasta, ale może też pokrywać wielkie obszary – kraje, a nawet kontynenty.

1.1 Po co tworzymy sieć?

Do najważniejszych przesłanek przemawiających za instalacją sieci należą:

- dzielenie programów i informacji;
- dzielenie zasobów (a zatem umożliwienie użytkownikom wspólnego ich wykorzystania, np. drukarek);
- zwiększenie niezawodności działań, dzięki możliwości użycia kilku komputerów do wykonania tego samego programu;
- bardziej równomierne wykorzystanie mocy obliczeniowej sprzętu informatycznego (gdy dany komputer jest przeciążony zadaniami, można wykorzystać inny, w danej chwili nieobciążony);
- usprawnienie zbierania, przetwarzania, rozprowadzania i wykorzystania na rozległych obszarach informacji o specjalnym znaczeniu, np. militarnym, gospodarczym, medycznym, itp.;
- przesyłanie tekstów pocztą elektroniczną (tzw. e-mail);
- upowszechnianie dostępu do informacji z różnych dziedzin, np. nauki;
- usprawnienie pracy biur podróży, rezerwacji lotniczych, operacji bankowych, handlu, bibliotekarstwa, systemu ubezpieczeń i innych, itp.

1.2 Podział sieci komputerowych.

Sieci komputerowe można podzielić ze względu na:

a) ich zasięg:

- **lokalne** (***LAN*** - *Local Area Network*) - sieci o najmniejszym zasięgu, obejmujące zwykle budynek lub grupę sąsiednich budynków, zwane również okablowaniem strukturalnym;
- **sieci kampusowe** - sieci obejmujące wiele grup budynków np. budynki wydziałów, domy studenckie i laboratoria jednej uczelni;
- **metropolitalne** inaczej: miejskie (***MAN*** - *Metropolitan Area Network*) - sieci obejmujące swym zasięgiem miasto (np. w Białymstoku działa sieć BIAMAN);
- **zdalne** (***WAN*** - *Wide Area Network*) - sieci o dużym zasięgu, przekraczającym obszar jednego miasta - np. sieć globalna czy sieć łącząca rozsiane po kraju lub świecie oddziały przedsiębiorstwa.

b) medium transmisyjne:

Sieci przewodowe	**Sieci bezprzewodowe**
• kabel koncentryczny	• radiowe (w tym też satelitarne)
• skrętka	• mikrofalowe
• światłowód	• podczerwone

1.3 Organizacje tworzące standardy i powiązania między nimi.

ANSI – Amerykański Narodowy Instytut Normalizacji (ang. The American National Stan-dards Institute) jest prywatną organizacją niekomercyjną. Jej misją jest ułatwianie rozwoju, koordynacja oraz publikowanie nieobligatoryjnych standardów. „Nieobligatoryjność" standardów ANSI polega na tym, że organizacja ta nie wdraża aktywnie ani nie narzuca nikomu swoich standardów. Uczestniczy natomiast w pracach organizacji ustanawiających standardy globalne, takich jak IOS, IEC itp., w związku z czym niezgodność z jej standardami powoduje niezgodność ze standardami globalnymi.

IEEE – Instytut Elektryków i Elektroników (ang. The Institute of Electrical and Electronic Engineers) jest odpowiedzialny za definiowanie i publikowanie standardów telekomunikacyjnych oraz przesyłania danych. Jego największym jak dotąd osiągnięciem jest zdefiniowanie standardów sieci LAN oraz MAN. Standardy te tworzą wielki i skomplikowany zbiór norm technicznych, ogólnie określanych jako „Project 802" lub jako seria standar-dów 802.

ISO – Międzynarodowa Organizacja Standaryzacyjna (ang. International Organization of Standarization) została utworzona w 1946 roku w Szwajcarii, w Genewie – tam też znajduje się dziś jej główna siedziba. Niektóre źródła organizację tę identyfikują za pomocą akronimu IOS. Mimo, iż to właśnie ten skrót jest formalnie poprawny, organizacja woli określać się za pomocą bardziej mnemonicznego (łatwiejszego do zapamiętania) skrótu: ISO. Skrót ten pochodzi od greckiego słowa isos, który jest odpowiednikiem polskiego „równy" lub „standardowy". Dlatego właśnie ten skrót jest uznawany za skrót Międzynarodowej Organizacji Standaryzacyjnej, która przy okazji jest niezależnym podmiotem wy-najętym przez ONZ do określania standardów międzynarodowych. Zakres jej działania obejmuje praktycznie wszystkie dziedziny wiedzy ludzkiej, poza elektryką i elektroniką. Aktualnie ISO składa się z ponad 90 różnych organizacji standardodawczych z siedzibami na całym świecie. Najważniejszym standardem ustanowionym przez ISO jest Model Referencyjny Połączonych Systemów Otwartych, czyli model OSI (ang. Open Systems Interconnection Reference Model).

IEC – Międzynarodowa Komisja Elektrotechniczna (ang. Internarional Electrotechnical Commision), z siedzibą w Genewie, została założona w roku 1909. Komisja IEC ustanawia międzynarodowe standardy dotyczące wszelkich zagadnień elektrycznych i elektronicz-nych. Aktualnie w jej skład wchodzą komitety z ponad 40 państw. W USA Instytut ANSI reprezentuje zarówno IEC jak i ISO.

IEC oraz ISO dostrzegły, że technologie informatyczne stanowią potencjalny obszar zazębiania się ich kompetencji. W celu określenia standardów dla technologii informatycznych utworzyły więc Połączony Komitet Techniczny (ang. **JTC** – Joint Technical Committee).

IAB – Komisja Architektury Internetu (ang. The Internet Architecture Board), uprzednio znany jako komisja działań Internetu (Internet Activities Board), zarządza techniczną stroną rozwoju sieci Internet. Składa się z dwóch komisji roboczych: Grupy Roboczej ds. Technicznych Internetu oraz Grupy Roboczej ds. Naukowych Internetu. Każda z tych grup, na co wskazują ich nazwy, pracuje indywidualnie.

Pojęcie LAN (Local Area Network) zostało dokładniej opisane przez dwa gremia. Organizacja ISO już w czerwcu 1981 r. zdefiniowała to określenie w następu-jący sposób:
„ ... jest lokalną siecią komputerową, służącą wymianie informacji za pomocą szeregowej transmisji bitowej pomiędzy urządzeniami, które są z sobą połączone, ale funkcjonują niezależnie od siebie. Sieć LAN podlega użytkownikowi i ogranicza się do jego terenu."

IEEE określa LAN jako sieć komputerową, która:
„ ... odróżnia się od innych sieci tym, że komunikacja ogranicza się tu najczęściej do mniejszego obszaru geograficznego, np. budynku, biura, czy terenów uniwersyteckich. Wymiana informacji odbywa się poprzez fizyczny kanał o średniej lub dużej prędkości bądź o odpowiednio niskim wskaźniku błędu..."

Obie organizacje określiły w swoich definicjach przede wszystkim stronę prawną sieci, wprowadzając w ten sposób rozgraniczenie w stosunku do sieci publicznej. W praktyce oznacza to, że w każdym wypadku trzeba korzystać z usług służb użyteczności publicznej (w Polsce jest to Telekomunikacja Polska S.A.) lub innych firm komercyjnych, jeśli między dwoma osieciowanymi budynkami przebiega np. ulica. Z tego można wywnioskować, że system LAN nie podlega przepisom o publicznej transmisji informacji.

1.4 Podstawowa topologia sieci.

Topologia jest to sposób połączenia stacji roboczych w sieci lokalnej. Topologia fizyczna definiuje geometryczną organizację sieci, czyli sposób fizycznego połączenia ze sobą komputerów oraz urządzeń sieciowych.

Trzema podstawowymi topologiami sieci LAN są magistrala, gwiazda i pierścień. Jednak w referacie zostały przedstawione również inne topologie.

1.4.1 Topologia magistrali

Rys.: Sieć o topologii magistrali

Topologię magistrali wyróżnia to, że wszystkie węzły sieci połączone są ze sobą za pomocą pojedynczego, otwartego kabla (czyli umożliwiającego przyłączanie kolejnych urządzeń). Kabel taki obsługuje tylko jeden kanał i nosi nazwę magistrali. Niektóre technologie oparte na magistrali korzystają z więcej niż jednego kabla, dzięki czemu obsługiwać mogą więcej niż jeden kanał, mimo że każdy z kabli obsługuje niezmiennie tylko jeden kanał transmisyjny.

Oba końce magistrali muszą być zakończone opornikami ograniczającymi, zwanymi również często terminatorami. Oporniki te chronią przed odbiciami sygnału. Zawsze, gdy komputer wysyła sygnał, rozchodzi się on w przewodzie automatycznie w obu kierunkach. Jeśli sygnał nie napotka na swojej drodze terminatora, to dochodzi do końca magistrali, gdzie zmienia kierunek biegu. W takiej sytuacji pojedyncza transmisja może całkowicie zapełnić wszystkie dostępne szerokości pasma i uniemożliwić wysyłanie sygnałów wszystkim pozostałym komputerom przyłączonym do sieci.

Topologia ta jest dobrym rozwiązaniem do tworzenia sieci z niewielką liczbą stacji roboczych. Typowa magistrala składa się z pojedynczego kabla, łączącego wszystkie węzły w sposób charakterystyczny dla sieci równorzędnej. Długość sieci nie powinna przekroczyć odległości 185 m (licząc od jednego końca kabla do drugiego). Szyna nie jest obsługiwana przez żadne urządzenia zewnętrzne (niższe koszty utworzenia sieci), zatem każdy sprzęt przyłączony do sieci "słucha" transmisji przesyłanych magistralą i odbiera pakiety do niego zaadresowane. Topologie magistrali są przeznaczone przede wszystkim do użytku w domach i małych biurach.

Zalety

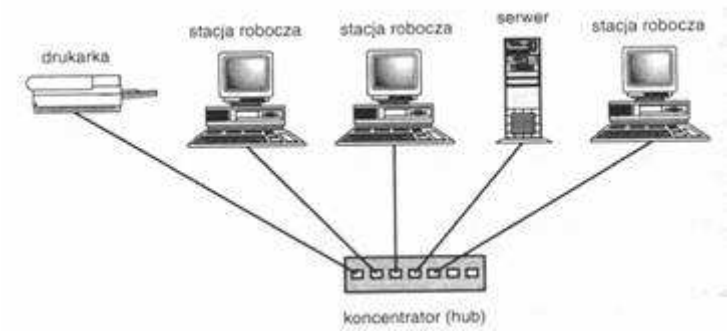
- Niski koszt okablowania sieci (kabel sieciowy musi być położony jedynie od jednej stacji sieciowej do następnej)
- Prosty układ okablowania
- Duża niezawodność (uszkodzenie jednej ze stacji roboczych nie powoduje awarii działania całej sieci)

Wady

- Podczas intensywnej transmisji danych może dochodzić do konfliktów, skutkujących spowolnieniem działania sieci

- Niski poziom bezpieczeństwa - wszystkie dane transmitowane są jednym łączem, więc prawdopodobieństwo ich przechwycenia przez nieuprawnionego użytkownika jest duże
- Przerwanie medium transmisyjnego (magistrali) powoduje awarię całej sieci
- Trudna diagnostyka i lokalizacja błędów

1.4.2 Topologia gwiazdy



Połączenia sieci LAN o topologii gwiazdy z przyłączonymi do niej urządzeniami rozchodzą się z jednego, wspólnego punktu, którym jest koncentrator. Każde urządzenie przyłączone do sieci w tej topologii może uzyskiwać bezpośredni i niezależny od innych urządzeń dostęp do nośnika, dlatego uszkodzenie jednego z kabli powoduje zerwanie połączenia tylko z jednym komputerem i nie wywołuje awarii całej sieci.

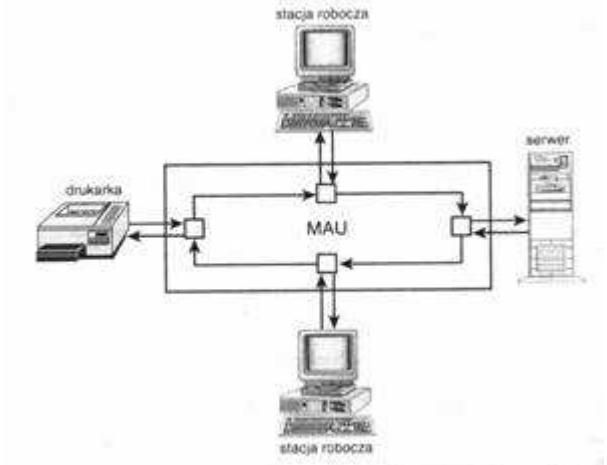
Zalety

- Duża przejrzystość struktury sieci
- Elastyczność i skalowalność - łatwość rozbudowy lub modyfikacji układu kabli
- Odporność na uszkodzenia poszczególnych stacji roboczych lub ich połączeń
- Duża wydajność
- Łatwa kontrola i likwidacja problemów

Wady

- Nadaje się jedynie do tworzenia niewielkich sieci
- Ograniczenie konfiguracji poprzez maksymalne odległości komputera od huba
- Kosztowna (duża długość kabli)

1.4.3 Topologia pierścienia



W sieci o topologii pierścienia (ring) wszystkie komputery są połączone logicznie w okrąg. Dane wędrują po tym okręgu i przechodzą przez każdą z maszyn. W układzie fizycznym sieć pierścieniowa wygląda podobnie jak sieć o topologii gwiazdy. Kluczową różnicą jest urządzenie połączeniowe, nazywane wielostanowiskową jednostką połączeniową (ang. MAU - MultiStation Access Unii). Wewnątrz MAU dane są przekazywane okrężnie od jednej stacji do drugiej.

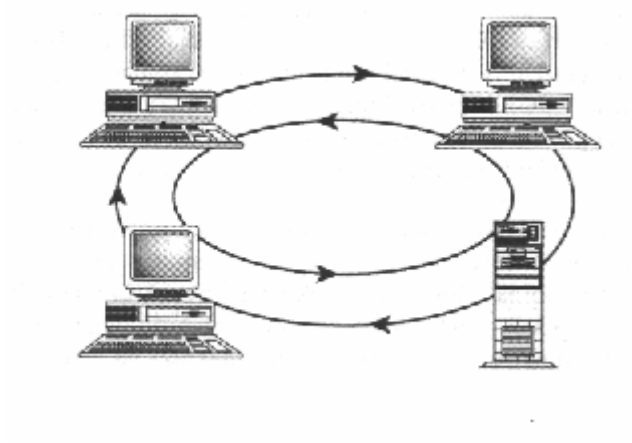
Zalety

- Możliwy do ustalenia czas odpowiedzi
- Niski koszt i łatwa rozbudowa
- Niewielka długość kabla

Wady

- Duża awaryjność - uszkodzenie jednej ze stacji roboczej natychmiast unieruchamia całą sieć
- Spadek wydajności wraz z dodaniem kolejnej stacji roboczej
- Trudna diagnostyka uszkodzeń

1.4.4 Topologia podwójnego pierścienia



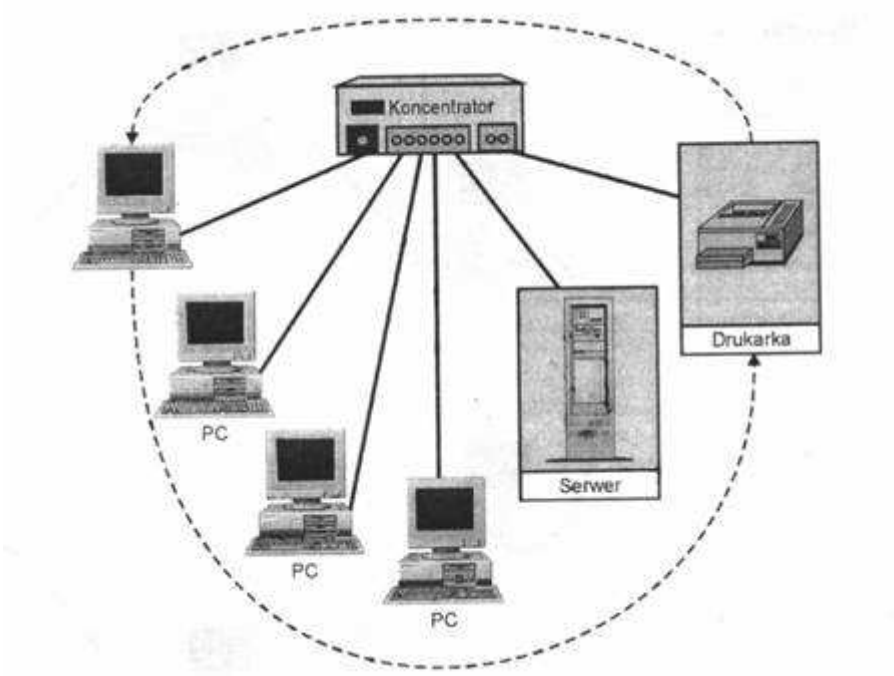
Rys.: Sieć o topologii podwójnego pierścienia

W tej topologii (dual-ring) są zazwyczaj tworzone sieci FDDI (ang. Fiber Distributed Data Interface - złącze danych sieci światłowodowych). Sieć FDDI może być wykorzystywana do przyłączania sieci lokalnych (LAN) do sieci miejskich (MAN). Pozwala tworzyć pierścienie o całkowitej długości sięgającej 115 km i przepustowości 100 Mb/s.

Na ruch w sieci o topologii podwójnego pierścienia składają się dwa podobne strumienie danych krążące w przeciwnych kierunkach.

Jeden z pierścieni jest nazywany głównym (primary), drugi - pomocniczym (secondary). W zwykłych warunkach wszystkie dane krążą po pierścieniu głównym, a pomocniczy pozostaje niewykorzystany. Krąg ten zostaje użyty wyłącznie wtedy, gdy pierścień główny ulega przerwaniu. Następuje wówczas automatyczna rekonfiguracja do korzystania z obwodu pomocniczego i komunikacja nie zostaje przerwana.

1.4.5. Sieć Token Ring



Rys.: Sieć Token-Ring

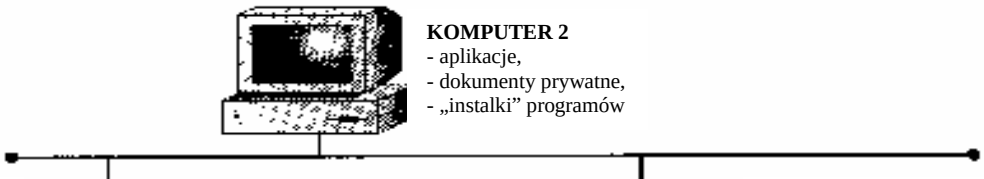
Pierścienie zostały wyparte przez sieci Token Ring firmy IBM, które z czasem znormalizowała specyfikacja IEEE 802.5. Sieci Token Ring odeszły od połączeń międzysieciowych każdy-z-każdym na rzecz koncentratorów wzmacniających. Wyeliminowało to podatność sieci pierścieniowych na zawieszanie się dzięki wyeliminowaniu konstrukcji każdy-z-każdym. Sieci Token Ring, mimo pierwotnego kształtu pierścienia (ang. ring - pierścień), tworzone są przy zastosowaniu topologii gwiazdy i metody dostępu cyklicznego.

Token w takiej sieci przesyłany jest do kolejnych punktów końcowych, mimo że wszystkie one są przyłączone do wspólnego koncentratora. Dlatego pojawiają się określenia sieci Token Ring jako mających "logiczną" topologię pierścienia, pomimo tego, że fizycznie ujęte są one w kształcie gwiazdy.

1.5 Typy połączeń sieciowych.

1.5.1 Połączenie sieciowe typu klient-klient.

Połączenie sieciowe klient-klient to taki typ, w którym komputery w sieci komunikują się ze sobą jak z równymi. Każdy komputer może udostępnić swoje zasoby innym komputerom w sieci. Do tych zasobów należą na przykład pliki, katalogi, aplikacje, czy też urządzenia takie jak drukarki, modemy, CD-ROMy itp. Każdy komputer jest również odpowiedzialny za zorganizowanie sobie i utrzymanie systemu bezpieczeństwa dla własnych zasobów. Aż w końcu, każdy komputer jest odpowiedzialny za korzystanie z zasobów sieci potrzebnych mu i dostępnych przez inny komputer w sieci klient-klient, za znajomość miejsca tych zasobów oraz zasad bezpieczeństwa umożliwiających dostęp do nich (hasła itp.).



KOMPUTER 2
- aplikacje,
- dokumenty prywatne,
- „instalki" programów

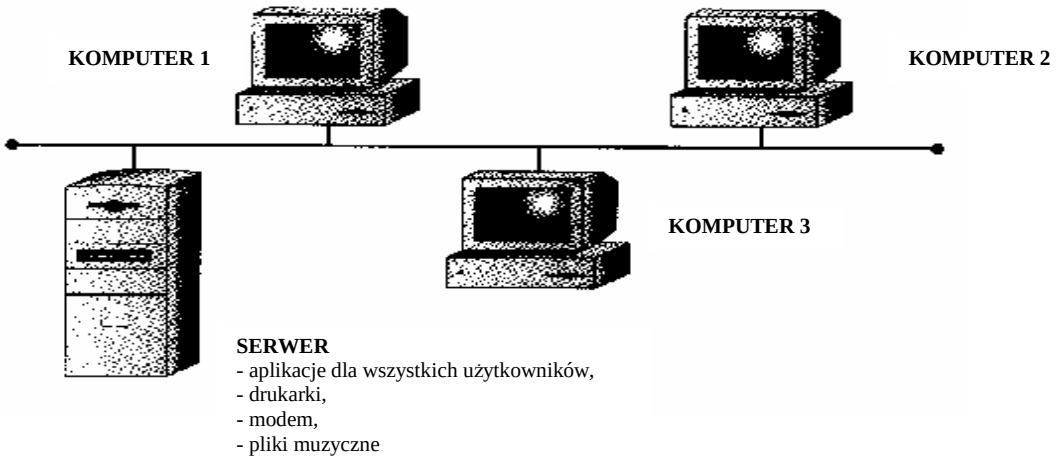
KOMPUTER 1
- aplikacje,
- dokumenty prywatne,
- pliki muzyczne,
- drukarka laserowa

KOMPUTER 3
- aplikacje,
- dokumenty prywatne,
- modem,
- drukarka atramentowa (kolorowa)

UWAGA: Nawet w sieciach wykorzystujących jedynie typ klient-klient możliwe jest przeznaczenie jednego komputera do specjalnych celów i umieszczenia na nim często wykorzystywanych zasobów. Można na przykład na pojedynczej stacji roboczej umieścić pliki aplikacji i pliki danych systemu księgowego, lub drukarkę po to, by zapewnić dużą wydajność i nie używać jej do zadań takich jak edytowanie tekstu. Komputer ten nadal działa na zasadzie klient-klient, ale po prostu nie jest używany do innych celów.

1.5.2 Połączenie sieciowe typu klient-serwer.

Połączenie sieciowe klient-serwer to taki typ, w którym istnieje rozróżnienie na komputery dające zasoby sieciowe (serwery) i komputery z tych zasobów korzystające (klienci - stacje robocze). W sieciach wykorzystujących jedynie typ klient-serwer wszystkie dostępne zasoby sieciowe, np. pliki, katalogi, aplikacje i wspólne urządzenia, są zarządzane i umieszczone w centrum, do którego mają dostęp komputery-klienci. Żaden komputer-klient nie dzieli swoich zasobów z innym komputerem-klientem lub serwerami; wprost przeciwnie - komputery-klienci są wyłącznie konsumentami tych zasobów.



KOMPUTER 1

KOMPUTER 2

KOMPUTER 3

SERWER
- aplikacje dla wszystkich użytkowników,
- drukarki,
- modem,
- pliki muzyczne

Serwery w sieci klient-serwer są odpowiedzialne za udostępnianie i zarządzanie odpowiednimi zasobami wspólnymi, oraz za ich bezpieczeństwo.

1.5.3 Porównanie sieci typu klient-klient i klient-serwer.

W praktyce większość sieci posiada cechy obu typów połączeń klient-klient jak i klient-serwer. Jest z całą pewnością możliwe, a czasem nawet pożądane wybranie tylko jednego typu połączenia, jednak najczęściej i tak uwzględnia się je oba. Projektując sieć, zanim podejmie się decyzję o budowaniu sieci opartej na jednym czy obu typach, musimy rozważyć argumenty każdego z rozwiązań i określić, w jaki sposób zamierzamy zrealizować potrzeby swoje i np. firmy.

Argumenty ZA siecią typu klient-klient:

- **Nie wymaga bardzo drogiego sprzętu komputerowego**: Sieci klient-klient są sprzętowo najmniej wymagającym rozwiązaniem. Zasoby są w nim rozłożone na wielu komputerach, nie ma więc potrzeby instalowania wysokiej klasy serwera. Obciążenie każdego z klientów jest zazwyczaj (ale nie zawsze!) względnie niewielkie.

- **Łatwy do administrowania**: Sieci klient-klient są przede wszystkim najłatwiejsze do zbudowania i administrowania. Ponieważ każda z maszyn sama się administruje - zazwyczaj w zakresie pewnych ograniczonych zasobów - trud administrowania siecią rozkłada się pomiędzy wielu różnych ludzi.

- **Nie wymaga sieciowego systemu operacyjnego**: Sieć klient-klient można zbudować tylko przy użyciu Windows 95 lub 98 na wszystkich stacjach roboczych, albo użyć w tym celu komputerów Macintosh. Oba te systemy operacyjne wyposażone są w konieczne do tego funkcje. Podobnie, możliwe jest stworzenie sieci klient-klient za pomocą komputerów opartych na UNIX (LINUX), co jest jednak czynnością zdecydowanie bardziej złożoną z powodu złożoności tegoż systemu operacyjnego.

- Więcej wbudowanej nadmiarowości: Załóżmy, że mamy do czynienia z małą siecią o 10-20 stacjach roboczych i na każdej z nich znajdują się bardzo ważne informacje. Jeśli wystąpi awaria jednej, większość wspólnych zasobów jest nadal dostępna. Sieć klient-klient oferuje znacznie większy stopień nadmiarowości niż sieć klient-serwer, ponieważ awarie pojedynczych elementów nie mają aż tak dużego wpływu na całą sieć i jej użytkowników.

Argumenty PRZECIW sieci klient-klient

- **Może obniżyć wydajność pracy użytkownika:** Jeśli któraś stacja robocza dysponuje zasobami wykorzystywanymi często i przez wiele osób, praca na takim komputerze będzie utrudniona.

- **Brakuje jej bezpieczeństwa:** Sieci klient-klient nie są nawet w małym stopniu tak bezpieczne jak sieci klient-serwer, ponieważ nie można zagwarantować, niezależnie jak dobrzy są użytkownicy sieci, że będą oni odpowiednimi administratorami dla swoich komputerów. Prawdę mówiąc, obojętnie jaki jest rozmiar sieci (załóżmy, że ponad 10 użytkowników), zawsze znajdzie się przynajmniej kilka osób, które nie będą postępowały zgodnie z poprawnymi zasadami administrowania. Ponadto systemy operacyjne, na których opiera się sieci klient-klient, takie jak Windows 98 lub Macintosh, z zasady nie są tworzone do zachowania ścisłego bezpieczeństwa.

- **Jest niełatwa do archiwizacji:** Niezawodna archiwizacja wszystkich danych na wszystkich stacjach roboczych jest trudnym zadaniem, a doświadczenie pokazuje, że pozostawianie tak istotnej czynności użytkownikom oznacza, że nie zostanie ona wykonana.

Argumenty ZA siecią klient-serwer

Sieci klient-serwer oferują z kolei scentralizowaną administrację, opartą na sprzęcie lepiej przystosowanym do zarządzania i udostępniania zasobów. Ten typ jest prawie zawsze rozwiązaniem stosowanym w przypadku sieci obsługujących mniej więcej ponad 10 użytkowników, a istnieje ku temu kilka słusznych powodów:

- **Jest bardzo bezpieczna:** Bezpieczeństwo sieci klient-serwer ma swoje uzasadnienie w kilku właściwościach tej sieci. Po pierwsze, w związku z tym, że wspólne zasoby mieszczą się w jednym, scentralizowanym punkcie, właśnie tam mogą być administrowane. A zarządzanie sporą ilością zasobów jest przecież znacznie łatwiejsze, gdy są one umieszczone na jednym czy dwóch serwerach niż rozrzucone na dziesięciu czy stu stacjach roboczych. Po drugie, serwery są zazwyczaj w fizycznie bezpiecznych miejscach, jak na przykład zamykanych szafach serwera. Fizyczne bezpieczeństwo jest bardzo istotnym sposobem ochrony sieci i jest nieosiągalne w przypadku sieci klient-klient. Po trzecie, systemy operacyjne obsługujące sieci klient-serwer są zaprojektowane jako systemy bezpieczne i są wyposażone w funkcje zapewniające ścisłą ochronę. Jeśli więc przestrzega się zasad bezpieczeństwa i poprawnego administrowania, włamanie do serwera nie jest wcale łatwe.

- **Sprawniej funkcjonuje:** Chociaż komputery pracujące jako serwery sieciowe są znacznie droższe od standardowych stacji roboczych, gwarantują jednak stosunkowo większą wydajność i są zaprojektowane, by w optymalny sposób równocześnie realizować potrzeby wielu użytkowników.

- **Scentralizowana archiwizacja:** Archiwizowanie bardzo ważnych danych przedsiębiorstwa jest znacznie łatwiejsze, gdy prowadzi się je na scentralizowanym serwerze. Często polecenie archiwizacji wydaje się na okres nocy, gdy serwer nie jest używany, a dane pozostają statyczne. Naturalnie, możliwe jest archiwizowanie zdecentralizowanych danych, zwłaszcza, że istnieją służące do tego narzędzia, jednak archiwizacja scentralizowana jest znacznie szybsza i bardziej wiarygodna.

- **Jest niezawodna**: Wprawdzie w sieciach klient-klient faktycznie jest więcej wbudowanej nadmiarowości, jednak nie można zapominać, że dobra sieć klient-serwer będzie bardziej niezawodna. Komputery przeznaczone na serwery charakteryzują się często zdecydowanie większą wewnętrzną nadmiarowością niż stacje robocze - potrafią poradzić sobie z awarią twardego dysku, procesora czy chwilowym brakiem dopływu prądu, i nie przerwać pracy do momentu, kiedy można usunąć usterki. Dodatkowo, ponieważ serwery mają tylko jedno względnie łatwe zadanie do wykonania, rezygnuje się z ich złożoności na rzecz niezawodności. Należy to porównać z sieciami klient-klient, gdzie czynności wykonywane przez użytkowników mogą się przyczynić do drastycznego wzrostu zawodności stacji roboczych. Przykładowo, konieczność restartowania komputera z Windows 9x co kilka dni nie jest wcale rzadkością, podczas gdy komputery w funkcji serwera mogą pracować przez wiele miesięcy bez żadnego zawieszenia się systemu.

Argumenty PRZECIW sieci klient-serwer

Rozważając argumenty za sieciami klient-serwer, należy zdać sobie sprawę, że istnieją również przeciwwskazania, zwłaszcza dla firm nie posiadających swoich własnych administratorów lub chcących jak najbardziej ograniczyć wydatki związane z siecią. Do argumentów przeciw sieci klient-serwer należą:

- **Wymaga profesjonalnego administrowania:** Sieci klient-serwer wymagają przynajmniej w pewnym stopniu profesjonalnego administrowania, nawet w przypadku małych sieci. Administratora można zatrudnić, bądź skorzystać z usług sieciowych świadczonych przez firmę specjalizującą się w administrowaniu, pamiętając w obu przypadkach, że niezbędny jest profesjonalizm. Poznanie wszystkich zagadek sieciowego systemu operacyjnego jest ważne i wymaga doświadczenia i przeszkolenia.

- **Jest bardziej zaawansowana sprzętowo**: Oprócz komputerów-klientów, w sieci niezbędny jest również komputer-serwer, zazwyczaj bardzo „naszpikowany", z dużą pamięcią i dyskiem SCSI. Dodatkowo potrzebny jest sieciowy system operacyjny i odpowiednia liczba licencji dla klientów. Te wymogi to nieraz przynajmniej dodatkowe kilkanaście tysięcy złotych do kosztów serwera, a dla naprawdę dużych sieci dziesiątki tysięcy złotych.

1.5.4 Rodzaje serwerów programowych.

Wyróżnia się kilka rodzajów serwerów (klasyfikacja zaczerpnięta z książki B. Komara: "TCP/IP dla każdego"):

Serwery katalogów
Dostarczają scentralizowanej usługi katalogowej, służącej do zarządzania kontami użytkowników, grup i stacji sieciowych oraz umożliwiającej scentralizowanie procedur uwierzytelniania i autoryzacji.

Serwery plików i drukarek
Zapewniają bezpieczne składowanie wszystkich danych. Mogą również obsługiwać kolejki drukowania, które zapewniają dostęp do urządzeń drukujących udostępnianych w sieci.

Serwery aplikacji
Pełnią funkcję serwera aplikacji typu klient-serwer. W środowisku typu klient-serwer, na kliencie uruchamiana jest jedynie niewielka wersja programu (tzw. procedura pośrednicząca), która zapewnia możliwość łączenia się z serwerem. Aplikacja po stronie serwera jest wykorzystywana do wykonywania silnie obciążających procesor zapytań klienta. Przykładami serwerów aplikacji mogą być serwery WWW i serwery baz danych.

Serwery pocztowe
Zapewniają klientom sieci możliwość korzystania z poczty elektronicznej. Wykorzystanie bram pozwala przekazywać pocztę pomiędzy różnorodnymi systemami pocztowymi.

Serwery bezpieczeństwa
Zabezpieczają sieć lokalną, gdy jest ona połączona z większymi sieciami, takimi jak Internet. Do tej grupy należą firewalle i serwery proxy.

Serwery dostępu zdalnego
Ich zadaniem jest umożliwienie przepływu danych między siecią a odległymi klientami. Klient odległy (zdalny) może używać modemu do uzyskania połączenia telefonicznego z siecią lokalną. Może również wykorzystać technikę tunelowania (VPN) i połączyć się z siecią lokalną za pośrednictwem sieci publicznej, takiej jak Internet. System, który umożliwia te formy dostępu do sieci to serwer dostępu zdalnego. Może on zostać wyposażony w jeden lub więcej modemów służących zapewnieniu zewnętrznego dostępu do sieci albo też w porty wirtualne, wykorzystane przez połączenia tunelowane. Po połączeniu klienta z siecią może on funkcjonować w podobny sposób jak przy bezpośrednim przyłączeniu do sieci przez kartę sieciową.

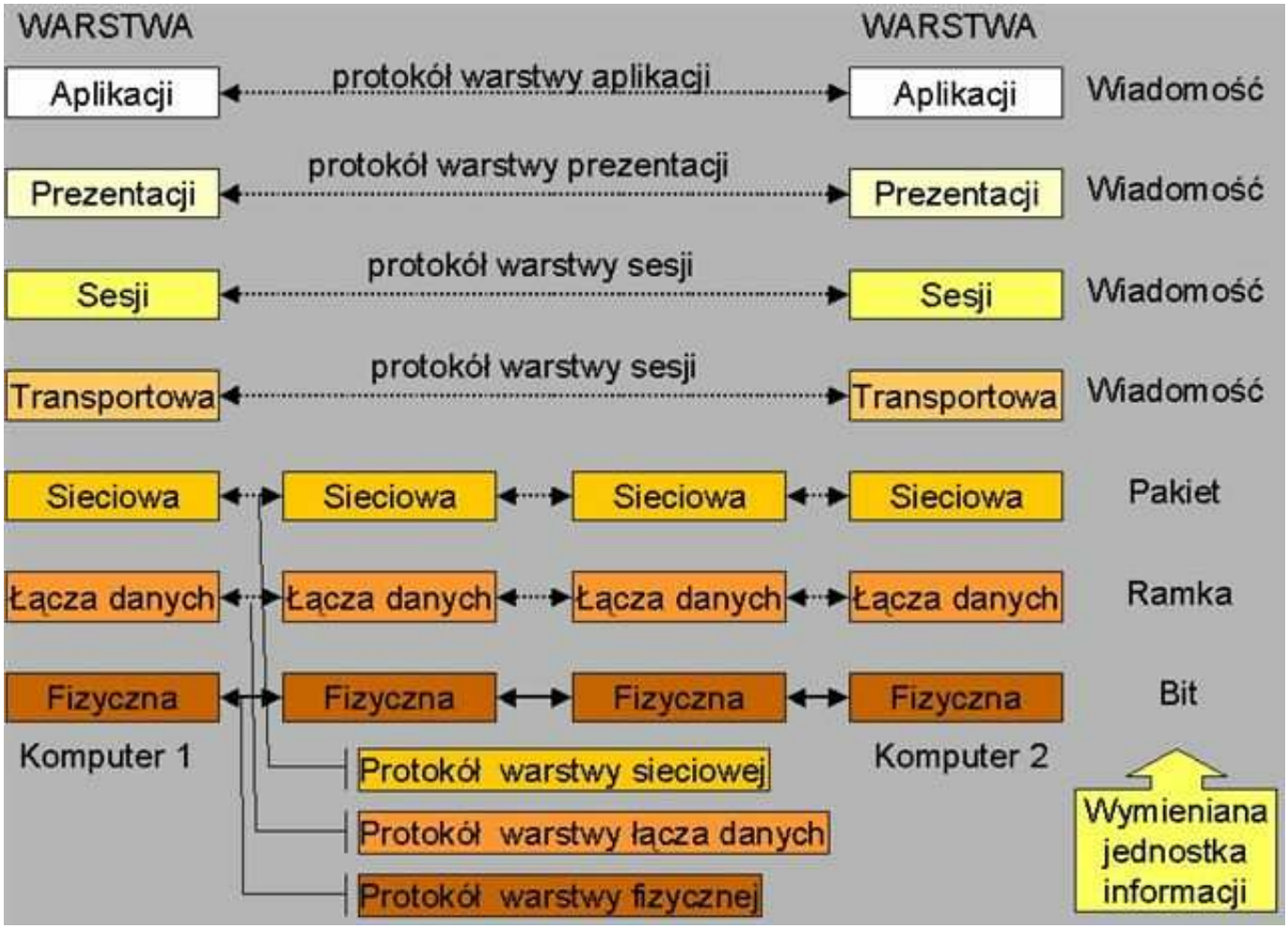
1.6 Sieciowy model OSI.

Model OSI (ang. *Open Systems Interconnection* – otwarte odniesienie systemowe) definiuje wszystkie metody i protokoły (*protokół* - zbiór zasad, wg. których może odbywać się komunikacja w sieci) niezbędne do podłączenia jednego komputera z innym za pomocą sieci.

Stworzony został przez organizację International Organization for Standardization (ISO). Jest on zbiorem zasad komunikowania się urządzeń sieciowych. Podzielony jest na siedem warstw, z których każda zbudowana jest na bazie warstwy poprzedniej. Model ten nie określa fizycznej budowy poszczególnych warstw, a koncentruje się na sposobach ich współpracy. Takie podejście do problemu sprawia, że każda warstwa może być implementowana przez producenta na swój sposób, a urządzenia sieciowe od różnych dostawców będą poprawnie współpracować. Poszczególne warstwy sieci stanowią niezależne całości i chociaż nie potrafią wykonywać żadnych widocznych zadań w odosobnieniu od pozostałych warstw, to z programistycznego punktu widzenia są one odrębnymi poziomami.

1.6.1 Warstwy OSI.

Komunikacja pomiędzy komputerami odbywa się na poziomie odpowiadających sobie warstw i dla każdej z nich powinien zostać stworzony własny protokół komunikacyjny. W rzeczywistej sieci komputerowej komunikacja odbywa wyłącznie się na poziomie warstwy fizycznej (*linia ciągła na rysunku poniżej*). W tym celu informacja każdorazowo przekazywana jest do sąsiedniej niższej warstwy aż do dotarcia do warstwy fizycznej.
Tak, więc pomiędzy wszystkimi warstwami z wyjątkiem fizycznej istnieje komunikacja wirtualna (linie przerywane na rysunku), możliwa dzięki istnieniu połączenia fizycznego.



1.6.2 Zadania poszczególnych warstw.

Warstwa fizyczna - odpowiada za transmisje sygnałów w sieci. Realizuje ona konwersje bitów informacji na sygnały, które będą przesyłane w kanale z uwzględnieniem maksymalizacji niezawodności przesyłu. W warstwie fizycznej określa się parametry amplitudowe i czasowe przesyłanego sygnału, fizyczny kształt i rozmiar łączy, znaczenie ich poszczególnych zestyków i wartości napięć na nich występujących, sposoby nawiązywania połączenia i jego rozłączania po zakończeniu transmisji.
Połączenie fizyczne można uzyskać pomiędzy dwoma punktami (*point-to-point*) lub po między wieloma punktami i może przebiegać w trybie *half-duplex* (w jednym kierunku) lub *full-duplex* (w obu kierunkach równocześnie)

Warstwa łącza danych – definiuje standardy, które nadają znaczenie poszczególnym bitom przesyłanym w warstwie fizycznej. Odpowiedzialna jest za odbiór i konwersję strumienia bitów pochodzących z urządzeń transmisyjnych w taki sposób, aby nie zawierały one błędów. Warstwa ta postrzega dane jako grupy bitów zwane ramkami. Warstwa łącza danych tworzy i rozpoznaje granice ramki. Ramka tworzona jest przez dołączenie do jej początku i końca grupy specjalnych bitów. Kolejnym zadaniem warstwy jest eliminacja zakłóceń, powstałych w trakcie transmisji informacji po kanale łączności. Ramki, które zostały przekazane niepoprawnie, są przesyłane ponownie. Ponadto warstwa łącza danych zapewnia synchronizację szybkości przesyłania danych oraz umożliwia ich przesyłanie w obu kierunkach.

Warstwa sieciowa – tu odbywa się najwięcej operacji w większości sieci. Steruje działaniem podsieci transportowej. Jej podstawowe zadania to przesyłanie danych pomiędzy węzłami sieci wraz z wyznaczaniem trasy przesyłu, określanie charakterystyk sprzęgu węzeł-komputer obliczeniowy, łączenie bloków informacji w ramki na czas ich przesyłania a następnie stosowny ich podział. W najprostszym przypadku określanie drogi transmisji pakietu informacji odbywa się w oparciu o stałe tablice opisane w sieci (tzw. *routing statyczny*). Istnieje również możliwość dynamicznego określania trasy na bazie bieżących obciążeń linii łączności (tzw. *routing dynamiczny*). Stosując drugie rozwiązanie mamy możliwość uniknięcia przeciążeń sieci na trasach, na których pokrywają się drogi wielu pakietów.

Warstwa transportowa – organizuje przepływ informacji z jednego punktu sieci do innego. Nadzoruje, by pakiety były dekodowane w prawidłowej kolejności i by wszystkie dotarły do miejsca przeznaczenia. Podstawową funkcją tej warstwy jest obsługa danych przyjmowanych z warstwy sesji. Obejmuje ona opcjonalne dzielenie danych na mniejsze jednostki, przekazywanie zblokowanych danych warstwie sieciowej, otwieranie połączenia stosownego typu i prędkości, realizacja przesyłania danych, zamykanie połączenia. Ponadto mechanizmy wbudowane w warstwę transportową pozwalają rozdzielać logicznie szybkie kanały łączności pomiędzy kilka połączeń sieciowych. Możliwe jest także udostępnianie jednego połączenia kilku warstwom sieciowym, co może obniżyć koszty eksploatacji sieci. Celem postawionym przy projektowaniu warstwy transportowej jest zapewnienie pełnej jej niezależności od zmian konstrukcyjnych sprzętu.

Warstwa sesji – definiuje połączenie użytkownika (klienta) z serwerem z serwerem bądź jednego klienta sieci z drugim. Po nawiązaniu stosownego połączenia (czyli właśnie sesji) warstwa sesji pełni szereg funkcji zarządzających, związanych m. in. z „taryfikacją" usług w sieci. W celu otwarcia połączenia pomiędzy komputerami (sesji łączności) poza podaniem stosownych adresów warstwa sprawdza, czy obie warstwy (nadawcy i odbiorcy) mogą otworzyć połączenie. Następnie obie komunikujące się strony muszą wybrać opcje obowiązujące w czasie trwania sesji. Dotyczy to na przykład rodzaju połączenia (simpleks, dupleks) i reakcji warstwy na zerwanie połączenia (rezygnacja, ponowne odtworzenie). Przy projektowaniu warstwy zwraca się uwagę na zapewnienie bezpieczeństwa przesyłanych danych. Przykładowo, jeżeli zostanie przerwane połączenie, którego zadaniem była aktualizacja bazy danych, to w rezultacie tego zawartość bazy może okazać się niespójna. Warstwa sesji musi przeciwdziałać takim sytuacjom.

Warstwa prezentacji - jej zadaniem jest obsługa formatów danych. Odpowiada ona więc za kodowanie i dekodowanie zestawów znaków oraz wybór algorytmów, które do tego będą użyte. Przykładową funkcją realizowaną przez warstwę jest kompresja przesyłanych danych, pozwalająca na zwiększenie szybkości transmisji informacji. Ponadto warstwa udostępnia mechanizmy kodowania danych w celu ich utajniania oraz konwersję kodów w celu zapewnienia ich mobilności.

Warstwa aplikacji - zapewnia programom użytkowym (np. MS Word, IE) usługi komunikacyjne. Określa ona formaty wymienianych danych i opisuje reakcje systemu na podstawowe operacje komunikacyjne. Warstwa stara się stworzyć wrażenie przezroczystości sieci. Jest to szczególnie ważne w przypadku obsługi rozproszonych baz danych, w których użytkownik nie powinien wiedzieć, gdzie zlokalizowane są wykorzystywane przez niego dane lub gdzie realizowany jest jego proces obliczeniowy.

1.6.3 Przemieszczanie się danych pomiędzy poszczególnymi warstwami OSI.

Dane przemieszczają się z aplikacji lub systemu operacyjnego, za pomocą protokołów i urządzeń tworzących siedem warstw modelu OSI, po kolei, aż w końcu dostają się do warstwy fizycznej i zostają przesłane przez połączenie sieciowe. Komputer przyjmujący je odwraca kolejność tych procesów, a więc przyjmowane są w warstwie fizycznej, przechodzą w górę przez wszystkie pozostałe warstwy, aż w końcu w warstwie aplikacji zostaną wykorzystane przez system operacyjny i jego aplikacje.
Na każdym etapie modelu OSI dane są „opakowywane" w kolejne informacje kontrolne, związane z operacjami wykonanymi w poszczególnych warstwach, przy czym informacje z poprzednich warstw pozostają nietknięte, a jedynie „opakowane" w dodatkowe dane kontrolne. W każdej warstwie są to inne informacje, ale wszystkie zawierają *nagłówki, trailery, preambułę i postambułę*.
Kiedy więc przykładowo dane docierają do oprogramowania sieciowego i części składowych modelu OSI, swoją drogę rozpoczynają w warstwie aplikacji, zawierając nagłówek aplikacji i dane aplikacji (prawdziwe dane, które zostały wysłane). Następnie, w warstwie prezentacji, nagłówek prezentami zostaje „owinięty" dookoła naszych danych i wszystko jest dalej przekazane do warstwy sesyjnej, gdzie znowu nagłówek sesyjny „owija" się wokół danych, i tak dalej, aż dotrą one do warstwy fizycznej. W komputerze przyjmującym dane, cały proces jest odwracany, przy czym każda warstwa „odwija" odpowiednią informację kontrolną, wykonuje zadania wskazane przez tę informację i przekazuje dane do wyższej warstwy.

2. Protokoły transmisji

Protokoły komunikacyjne to zbiór ścisłych reguł i kroków postępowania, które są automatycznie wykonywane przez urządzenia komunikacyjne w celu nawiązania łączności i wymiany danych. Dzięki temu, że połączenia z użyciem protokołów odbywają się całkowicie automatycznie typowy użytkownik zwykle nie zdaje sobie sprawy z ich istnienia i nie musi o nich nic wiedzieć.

Klasyczne protokoły, których pierwowzorem był protokół teleksu składają się z trzech części:

- procedury powitalnej (tzw. "handshake") która polega na przesłaniu wzajemnej podstawowej informacji o łączących się urządzeniach, ich adresu (np. nr telefonu), szybkości i rodzaju transmisji itd, itp,
- właściwego przekazu danych,
- procedury analizy poprawności przekazu (np. sprawdzania sum kontrolnych) połączonej z procedurą pożegnania, żądaniem powtórzenia transmisji lub powrotem do procedury powitalnej

Przesyłana informacja może być porcjowana - protokół musi umieć odtworzyć informację w postaci pierwotnej.

Protokołami tego rodzaju posługują się:

- teleksy,
- faksy,
- modemy,
- programy komputerowe,
- wiele innych urządzeń, włącznie z np. pilotami do telewizorów.

Warstwy Przesyłanie danych komputerowych to niezwykle trudny proces, dlatego rozdzielono go na kilka "etapów", warstw. Warstwy oznaczają w istocie poszczególne funkcje spełniane przez sieć. Najbardziej powszechny sposób organizacji warstw komunikacji sieciowej to Model OSI.(omawiany wcześniej)

2.1 Protokół TCP/IP – wprowadzenie.

TCP/IP *(Transmission Control Protocol / Internet Protocol*) jest pakietem najbardziej rozpowszechnionych protokołów komunikacyjnych współczesnych sieci komputerowych. Następca protokołu NCP. Najczęściej obecnie wykorzystywany standard sieciowy, stanowiący podstawę współczesnego Internetu. Nazwa pochodzi od dwóch najważniejszych jego protokołów: TCP oraz IP.

TCP (ang. *Transmission Control Protocol* - protokół kontroli transmisji) – strumieniowy protokół komunikacji między dwoma komputerami. Został stworzony przez Vintona Cerfa i Roberta Kahna. Jest on częścią większej całości określanej jako stos TCP/IP. W modelu OSI TCP odpowiada warstwie Transportowej.

IP (ang. *Internet Protocol*) to protokół komunikacyjny warstwy sieciowej modelu OSI (warstwy internet w modelu TCP/IP). Używany powszechnie w Internecie i sieciach lokalnych.

Dane w sieciach IP są wysyłane w formie bloków określanych mianem pakietów. W przypadku protokołu IP, przed rozpoczęciem transmisji nie jest zestawiana wirtualna sesja komunikacyjna pomiędzy dwoma hostami, które nie komunikowały się ze sobą wcześniej

Host: Każdy komputer podłączony do Internetu lub innej sieci używającej protokołu TCP/IP i posiadający unikalny adres IP

Protokół IP jest protokołem zawodnym - nie gwarantuje, że pakiety dotrą do adresata, nie zostaną pofragmentowane, czy też zdublowane, a ponadto mogą dotrzeć do odbiorcy w innej kolejności niż zostały nadane. Niezawodność transmisji danych jest zapewniana przez protokoły warstw wyższych (np. TCP), znajdujących się w hierarchii powyżej warstwy sieciowej.

TCP/IP jest standardem komunikacji otwartej. Otwartość oznacza tu możliwości komunikacji miedzy dowolnymi typami urządzeń, bez względu na ich fizyczną różnorodność. TCP/IP zwany jest także stosem protokołów ze względu na strukturę warstwową, w której ramka protokołu wyższej warstwy jest zawarta jako dane w protokole warstwy niższej.

2.2 Adresy IP

Adresy IP są niepowtarzalnymi identyfikatorami wszystkich stacji należących do intersieci TCP/IP. Stacją może być komputer, terminal, router, a także koncentrator. "Stację" można najprościej zdefiniować jako dowolne urządzenie w sieci, występujące jako przedmiot jednego z trzech działań:

- uzyskiwania dostępu do innych urządzeń w sieci,
- łączenia się z nim jako udostępnionym składnikiem sieci,
- administrowania niezbędnego dla poprawnego funkcjonowania sieci.

Każda stacja wymaga adresu niepowtarzalnego w całej intersieci TCP/IP; żadnej ze stacji nie można przypisać adresu już istniejącego. W światowej sieci, jaką jest Internet, rolę organu przydzielającego adresy IP pełni Internet Assigned Number Authority (IANA - Rada ds. Nadawania Numerów). Określa ona zasady przydzielania adresów.

2.3 Sposoby zapisywania adresów IP

Każdy z adresów IP jest ciągiem trzydziestu dwóch zer i jedynek. Obecna wersja adresowania IP jest więc nazywana adresowaniem 32-bitowym. Nie jest ono, w gruncie rzeczy, zbyt wygodne. Stąd powszechne używanie notacji dziesiętnej z kropkami.

Na 32-bitowy adres IP składają się 4 oktety. Każdy oktet można zapisać w postaci liczby dziesiętnej.

Przykładowy adres:	01111111 00000000 00000000 00000001
Jest zapisywany jako:	127.0.0.1

Jest to tzw. adres pętli zwrotnej (ang. loopback address), reprezentujący stację lokalną, czyli tę, przy której siedzimy. Jest to adres zarezerwowany i wysyłane doń dane nigdy nie są przekazywane do sieci.

Przekształcenie polega na zapisaniu każdego z oktetów postaci liczby dziesiętnej i wstawieniu pomiędzy nie kropek.

2.4 Klasy adresów IP

A	0	Sieć . Stacja . Stacja . Stacja
B	10	Sieć . Sieć . Stacja . Stacja
C	110	Sieć . Sieć . Sieć . Stacja
D	1110	Adres multiemisji
E	11110	Zarezerwowany do użycia w przyszłości

Rys 2.4.: Pięć klas adresów IP

Każda z pięciu klas adresów IP jest oznaczona literą alfabetu: klasa A, B, C, D oraz E. Każdy adres składa się z dwóch części: adresu sieci i adresu hosta (stacji). Klasy prezentują odmienne uzgodnienia dotyczące liczby obsługiwanych sieci i hostów.

Adres IP klasy A

Pierwszy bit adresu (8 bajtów) klasy A jest zawsze ustawiony na "O". Następne siedem bitów identyfikuje numer sieci. Ostatnie 24 bity (np. trzy liczby dziesiętne oddzielone kropkami) adresu klasy A reprezentują możliwe adresy hostów.
Wzorzec binarny tej klasy to: 0#######.
Adresy klasy A mogą mieścić się w zakresie od 1.0.0.1 do 127.255.255.254.
Każdy adres klasy A może obsłużyć 16777214 unikatowych adresów hostów.

Adres IP klasy B

Pierwsze dwa bity adresu klasy B to "10". 16 bitów identyfikuje numer sieci, zaś ostatnie 16 bitów identyfikuje adresy potencjalnych hostów.
Wzorcem binarnym jest: 10######.
Adresy klasy B mogą mieścić się w zakresie od 128.0.0.1 do 191.255.255.254.
Każdy adres klasy B może obsłużyć 65534 unikatowych adresów hostów.

Adres IP klasy C

Pierwsze trzy bity adresu klasy C to "110". Następne 21 bitów identyfikuje numer sieci. Ostatni oktet służy do adresowania hostów.
Wzorzec binarny: 110#####.
Adresy klasy C mogą mieścić się w zakresie od 192.0.0.1 do 223.255.255.254. Każdy adres klasy C może obsłużyć 254 unikatowe adresy hostów.

Adres IP klasy D

Pierwsze cztery bity adresu klasy D to "1110". Adresy te są wykorzystywane do multicastingu, ale ich zastosowanie jest ograniczone. Adres multicast jest unikatowym adresem sieci, kierującym pakiety do predefiniowanych grup adresów IP. Adresy klasy D mogą pochodzić z zakresu 224.0.0.0 do 239.255.255.254.

Adres IP klasy E

Faktycznie - zdefiniowano klasę E adresu IP, ale InterNIC zarezerwował go dla własnych badań. Tak więc żadne adresy klasy E nie zostały dopuszczone do zastosowania w Internecie.

2.5 Ogólne zasady adresowania IP

Podczas nadawania adresów IP należy przestrzegać następujących reguł:

- Wszystkie stacje w jednym fizycznym segmencie sieci powinny mieć ten sam identyfikator sieci
- Część adresu IP określająca pojedynczą stację musi być odmienna dla każdej stacji w segmencie sieci
- Identyfikatorem sieci nie może być 127 - wartość ta jest zarezerwowana do celów diagnostycznych
- Identyfikator stacji nie może składać się z samych jedynek - jest to adres rozgłaszania dla sieci lokalnej
- Identyfikator sieci nie może składać się z samych zer - jest to oznaczenie sieci lokalnej
- Identyfikator stacji również nie może składać się z samych zer - jest to oznaczenie sieci wskazanej przez pozostałą część adresu i nie może zostać przypisane pojedynczej stacji

2.6 Specjalne adresy IP

Pewne adresy IP zostały zarezerwowane i nie mogą zostać wykorzystane do oznaczania stacji lub sieci.

- Adresy poszczególnych sieci powstają ze złożenia identyfikatora sieci oraz zer w miejscu identyfikatora stacji

Klasa	ID Sieci
A	w.0.0.0
B	w.x.0.0
C	w.x.y.0

Rys.: Adresy sieci według klas

- Identyfikatory sieci połączone z binarnymi jedynkami w miejscu identyfikatora stacji są adresami rozgłaszania

Klasa	Adres rozgłaszania
A	w.255.255.255
B	w.x.255.255
C	w.x.y.255

Rys.: Adresy rozgłaszania według klas

- Adres IP 255.255.255.255 jest zarezerwowany jako adres ograniczonego rozgłaszania. Może on zostać użyty zawsze, gdy stacja nie zna jeszcze identyfikatora sieci. Ogólną zasadą konfiguracji routerów jest uniemożliwienie przesyłania tego rozgłoszenia poza lokalny segment sieci
- Adres sieci 127 jest zarezerwowany dla celów diagnostycznych (tzw. adres pętli zwrotnej)
- Adres IP 0.0.0.0 oznacza "niniejsza stacja". Wykorzystywany jest jedynie w takich sytuacjach jak uruchomienie klienta DHCP, który nie otrzymał jeszcze własnego adresu IP

2.7 Znaczenie masek podsieci

Maska podsieci (ang. SNM - subnet mask) jest wykorzystywana do określania, ile bitów adresu IP wskazuje sieć, a ile stację w tej sieci. Dla adresów klas A, B i C wykorzystywane są maski domyślne:

- klasa A - 255.0.0.0
- klasa B - 255.255.0.0
- klasa C - 255.255.255.0

Maska podsieci klasy A wskazuje, że sieciowa część adresu to pierwsze 8 bitów. Pozostałe 24 bity określają stację w tej sieci. Jeżeli adresem stacji jest 11.25.65.32, to wykorzystanie maski domyślnej określa adres sieci jako 11.0.0.0. Częścią adresu wskazującą stację jest 25.65.32.

Maska podsieci klasy B wskazuje, że sieć jest określona przez pierwszych 16 bitów adresu. Pozostałe 16 bitów wyznacza konkretną stację. Dla adresu stacji 172.16.33.33, sieć wskazuje adres 172.16.0.0, a składnikiem określającym stację jest 33.33.

Maska podsieci klasy C wskazuje, że część adresu określająca sieć to pierwsze 24 bity, a pozostałe 8 określa należącą do niej stację. Dla adresu stacji 192.168.2.3 wskazaniem sieci jest 192.168.2.0, zaś składnikiem określającym stację jest 3.

2.8 Adresy w sieci lokalnej

Trzy następujące pule adresów IP zostały zarezerwowane do użytku w sieciach lokalnych, oddzielonych serwerami proxy lub zaporami firewall:

- od 10.0.0.0 do 10.255.255.255
- od 172.16.0.0 do 172.31.255.255
- od 192.168.0.0 do 192.168.255.255

Celem ich utworzenia było zapewnienie sieciom nie przyłączonym do Internetu puli adresów niewchodzących w konflikt z żadnymi adresami będącymi w użyciu w Internecie (tzw. adresy nieroutowalne).

Sieciom korzystającym z tych pul nie zagraża, w razie późniejszego przyłączenia do Internetu, przypadkowy konflikt z inną siecią obecną w Internecie.

Poza zabezpieczeniem przed konfliktem, prywatne adresowanie sieci przyczynia się istotnie do ograniczenia zapotrzebowania na adresy publiczne. Przy wysyłaniu danych z sieci prywatnej do publicznej, pierwotny adres źródłowy zostaje zamieniony na adres zewnętrzny, uzyskany od ISP. Procedury tego rodzaju określane są jako translacja adresów sieciowych (NAT - network address translation).

Adresy NAT mogą być wykorzystywane wyłącznie za zaporami firewall albo serwerami proxy, które ukrywają przed Internetem własne schematy adresowania. Utrudnia to dostęp do sieci osobom nieuprawnionym i umożliwia współużytkowania jednego adresu publicznego przez wiele stacji.

2.9 Protokół Internetu, wersja 6 (IPv6)

CDN...

(DO POPRAWY i UZUPEŁNIENIA)

1.7 Podstawowe komponenty sprzętu sieciowego – wprowadzenie.

1.7.1 Serwery.

Serwer jest to komputer wykonujący funkcje sieciowe dla innych komputerów. Funkcje te można zakwalifikować do kilku kategorii, w tym do następujących:

- ***Serwery plików*** i drukowania, umożliwiające współdzielenie plików i drukarek sieciowych.
- ***Serwery aplikacji***, świadczące specjalne usługi dla programów. Przykładem jest serwer, który uruchamia bazę danych, by mogła z niej korzystać aplikacja rozprowadzona w sieci.
- ***Serwery pocztowe***, umożliwiające przechowywanie poczty elektronicznej i połączenia pomiędzy komputerami-klientami.
- ***Serwery sieciowe***, będące punktem wyjścia do różnych usług sieciowych. Do usług tych należą między innymi automatyczne przyznawanie adresów TCP/ IP (serwery DHCP), nakierowywanie pakietów z jednej sieci do drugiej (serwery routujące), kodowanie/dekodowanie i inne funkcje bezpieczeństwa. W grupie tej znajdują się też serwery obsługujące wirtualne sieci prywatne VPN i wiele innych.
- ***Serwery internetowe***, obsługujące strony internetowe, grupy dyskusyjne (NNTP) i pocztę elektroniczną w Internecie.
- ***Serwery zdalnego dostępu***, umożliwiające zdalnym użytkownikom dostęp do sieci lokalnych

Serwery zazwyczaj są obsługiwane przez jakiś rodzaj sieciowego systemu operacyjnego, np. *Windows NT Server, 2000 Server, Novell NetWare lub UNIX*. W zależności od tego, który z systemów został wybrany, wyżej wspomniane funkcje mogą być umieszczone na jednym lub kilku serwerach. Ponadto należy pamiętać, że nie we wszystkich sieciach te funkcje są niezbędne.
Serwerami mogą zostać prawie wszystkie komputery, ale na dzień dzisiejszy są to zazwyczaj wysokiej klasy komputery osobiste o architekturze Intela produkowane w seriach przez markowych producentów***.

Kilka cech odróżnia komputer zbudowany, by służyć jako serwer od komputera-klienta. Należą do nich wbudowana nadmiarowość realizowana za pomocą wielu źródeł prądu i wiatraków (przykładowo), które zapewniają, że w razie jakiejś awarii, komputer nie przestanie działać. Przewidziane są również najwyższej jakości rozwiązania podsystemów dysku (SCSI, RAID), pamięci (ECC) i podsystemów sieciowych, optymalizujące przepływ danych do i od serwera, sieci i komputerów-klientów. Aż w końcu, zawierają zazwyczaj specjalne oprogramowanie i sprzęt monitorujący, które zapewniają dobre działanie serwera, ostrzegając o możliwości powstania awarii zanim jeszcze do niej dojdzie. Dzieje się tak na przykład przy monitorowaniu temperatury (większość serwerów jest wyposażona w termometry); jeśli podnosi się zbyt wysoko, pojawia się komunikat i problem zostaje rozwiązany jeszcze zanim awarii ulegnie któraś z części serwera (można tu także wspomnieć o specjalnie przygotowanych pomieszczeniach, w których znajdują się serwery).

1.7.2 Koncentratory, routery i przełączniki

Koncentratory, routery i przełączniki to najczęściej spotykane „wyłącznie" sieciowe elementy sprzętu komputerowego. („Wyłącznie" zostało tutaj użyte w takim sensie, że funkcjonują one tylko w sieciach i nigdzie indziej.) Często tę grupę sprzętu nazywa się „urządzeniami wewnątrzsieciowymi", ponieważ właśnie do tego służą. To właśnie one łączą ze sobą całe okablowanie sieci i przesyłają dane w warstwach: fizyczne, łącza danych lub sieciowej modelu OSI.

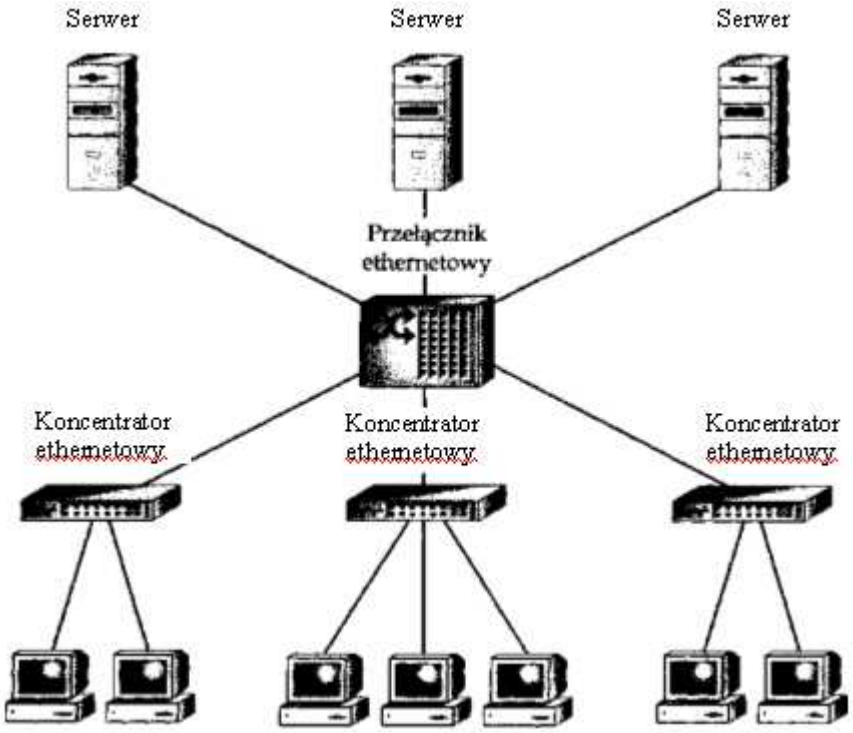
Koncentrator (ang. hub, concentrator) jest urządzeniem, które podłącza kable sieciowe wychodzące z komputerów-klientów do sieci. Koncentratory występują w wielu różnych rozmiarach, od małych, obsługujących po prostu dwa komputery, aż do naprawdę dużych z 60 lub jeszcze większą liczbą portów. (Najpopularniejsze są koncentratory 24-portowe.) Wszystkie łącza sieciowe jednego koncentratora mają jedną wspólną domenę kolizji, co jest wyszukanym terminem na opisanie sytuacji, w której wszystkie połączenia do koncentratora „rozmawiają" przez jeden kabel logiczny i podlegają interferencjom z innych komputerów podłączonych do tego samego koncentratora.

Przełącznik (ang. switch) jest okablowany w sposób bardzo podobny do koncentratora i właściwie wygląda jak koncentrator. Jednak w przełączniku wszystkie połączenia są na swojej własnej domenie kolizji. Sprawia on, że każde połączenie sieciowe staje się połączeniem prywatnym, a następnie zbiera dane z wszystkich pojedynczych

połączeń i przesyła je do szkieletu sieci, która operuje zazwyczaj na dużo większej prędkości niż pojedyncze łącze między przełącznikami. Często przełączników używa się do przyłączania koncentratorów do szkieletu sieci.

Router kieruje pakiety danych z jednej sieci do drugiej. Dwie sieci podłączają się do routera przy pomocy swojego własnego typu okablowania i typu połączenia. Przykładowo, router łączący sieć 10Base-T z linią telefoniczną ISDN będzie miał dwa łącza: jedno prowadzące do sieci 10Base-T i jedno do linii ISDN dostarczonej przez firmę telekomunikacyjną. Routery mają bardzo często dodatkowe łącze, na końcu którego znajdzie się terminal, używane do programowania, utrzymania i serwisowania routera.

Rys. 1.7.2 Zastosowanie przełączników i koncentratorów.



1.7.3 Okablowanie i infrastruktura sieciowa

Na rynku dostępne jest wiele rodzajów kabli sieciowych, ale niezbędna jest znajomość tylko kilku najważniejszych. Najpopularniejszym kablem dla sieci LAN jest **kabel skręcany** (*skrętka*) Category 3 (Cat-3). Kabel ten przesyła sygnały w sieci przez cztery żyły (dwie skręcone pary). Kabla Cat-3 używa się do sieci 10Base-T Ethernet. (UWAGA: Skręcenie każdej pary wewnątrz kabla zmniejsza szansę wpływu interferencji elektrycznych na kabel)
Większymi możliwościami i wyższą jakością w porównaniu do kabla Cat-3 cechuje się kabel Category 5 (Cat-5). Kabel ten jest podobny - również zbudowany z zestawów skręconych par żył, tyle że par tych jest dwa razy więcej. Kabel Cat-5 jest niezbędnym elementem sieci 100Base-T, a może być również wykorzystany do uzyskania dwóch równoczesnych połączeń Cat-3.

Do nowych instalacji nie używa się już **kabla koncentrycznego**, jednak można się jeszcze na niego natknąć w starszych konstrukcjach. Ma on miedziany rdzeń (tzw. wiązka przewodząca) owinięty warstwą plastikową, która z kolei jest otoczona metalowym splotem, zwanym osłoną), a ostatnią warstwę stanowi plastikowa otoczka.

1.7.3 Stacje robocze
O komputerach w sieci, używanych przez pracowników mówi się zazwyczaj jako o **sieciowych stacjach roboczych** (ang. workstation). Niekiedy nazywa sieje również klientami sieci. Zazwyczaj klient jest komputerem osobistym PC, pracującym na którejś z wersji Windows, z zainstalowaną kartą sieciową i oprogramowaniem sieciowym dla klienta, które to lementy umożliwiają stacji pracę w sieci. Sieciowe stacje robocze mogą być również jakimkolwiek innym typem komputera, wyposażonym w niezbędny sprzęt i oprogramowanie, a do tej grupy będą należeć na przykład Macintosh firmy Apple, czy niektóre komputery o architekturze LINUX.

2. Okablowanie sieciowe.

2.1 Topologia okablowania.

Ponieważ słowo topologia znaczy w zasadzie kształt, termin topologia sieci odnosi się do kształtu sieci. Okablowanie sieci wykonywane jest na podstawie kilku różnych topologii, a wybór jednej z nich jest jedną z najważniejszych decyzji, jakie należy podjąć podczas budowy sieci. Różnią się one kosztami (instalacji i utrzymania), stopniem funkcjonalności i niezawodności.

2.1.1 Topologia liniowa.

Topologia liniowa (ang. *bus topology*), jest siecią, gdzie jednego pojedynczego kabla używa się od początku do końca sieci, a różne urządzenia sieciowe (tzw. węzły sieciowe) są podłączone do niego.

Próba definicji segmentu sieci.

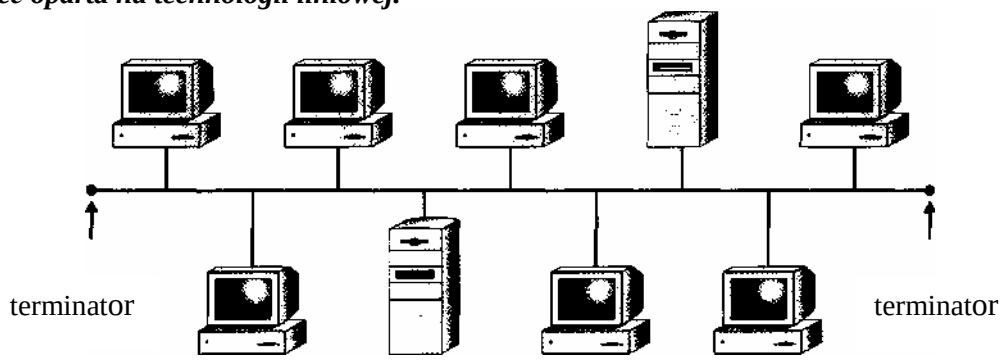
Segment sieci to grupa komputerów połączonych okablowaniem. Pakiet wysłany w obrębie grupy nie będzie odebrany przez komputer spoza segmentu dopóty, dopóki nie zostanie odpowiednio skonfigurowane połączenie między nimi.

Segment jest pojedynczą długością kabla, do którego przyłączone są węzły sieciowe. Tak naprawdę, segment nie jest jednym kawałkiem kabla, ponieważ jest przerywany we wszystkich punktach, gdzie komputery łączą się z siecią za pomocą łącznika zezwalającego na przyłączenie węzła do kabla sieciowego. Jednak segment jest jednym kablem pod względem elektryczności. W każdym segmencie wszystkie przejawy ruchu sieciowego są „widziane" przez wszystkie węzły sieciowe w tym segmencie. Należy to wziąć pod uwagę planując liczbę węzłów, które będą podłączone do jednego segmentu. Przy 20 komputerach w pełni korzystających z jednego segmentu w tym samym czasie, przepustowość, jaką każdy z nich będzie mógł maksymalnie osiągnąć, będzie wynosiła zaledwie około 1/20

Różne typy sieci liniowych mają inne specyfikacje. Wszystkie biorą pod uwagę następujące czynniki:

- Ile węzłów sieciowych może się znaleźć w pojedynczym segmencie?
- Ile segmentów można połączyć za pomocą regeneratorów?
- Jak blisko siebie mogą znaleźć się węzły sieciowe?
- Jaka jest całkowita długość segmentu?
- Jaki rodzaj kabla koncentrycznego jest wymagany?
- Jak należy zakończyć linię?

Rys 2.1.1 Prosta sieć oparta na technologii liniowej.



W chwili obecnej nowe sieci rzadko opierają się na topologii liniowej, jednak wśród starszych sieci jest ona popularna. Używają one kabla koncentrycznego. Wyróżniamy trzy typy sieciowych kabli koncentrycznych:

- Ethernet cienki o impedancji falowej 50 omów i grubości 1/4", powszechnie stosowany w małych sieciach lokalnych (max. odległość między końcami sieci 185m).
- Ethernet gruby o impedancji falowej 50 omów i grubości 1/2", praktycznie wyszedł z użycia, czasem stosowany jako rdzeń sieci (max. odległość między końcami sieci do 500m).
- Arcnet o impedancji falowej 93 omy i grubości 1/3"(max. odległość między końcami sieci do 300m).

Kable koncentryczne powinny być zakończone terminatorami (specjalne końcówki o rezystancji dostosowane do impedancji falowej kabla).

Zalety kabla koncentrycznego:

- jest mało wrażliwy na zakłócenia i szumy

- nadaje się do sieci z przesyłaniem modulowanym (szerokopasmowym)
- zapewnia większe prędkości niż nie ekranowany kabel skręcany (pojedyncza skrętka)
- jest tańszy niż ekranowany kabel skręcany (znacznie mniejsza ilość tego kabla jest zużywana do budowy sieci)

Wady kabla koncentrycznego:

- łatwo ulega uszkodzeniom (awaria jednej części segmentu powoduje awarię całego segmentu)
- możliwość zastosowania danego typu kabla ogranicza impedancja falowa
- trudności przy lokalizowaniu usterki

Analizując wady i zalety można stwierdzić, że projektując małą sieć (mała ilość komputerów) zajmującą np. jedno pomieszczenie, można podjąć decyzję o wykorzystaniu topologii liniowej. Jednak myśląc o ewentualnej rozbudowie takiej sieci należy wybrać sieć opartą na topologii gwiazdy z zastosowaniem skrętki.

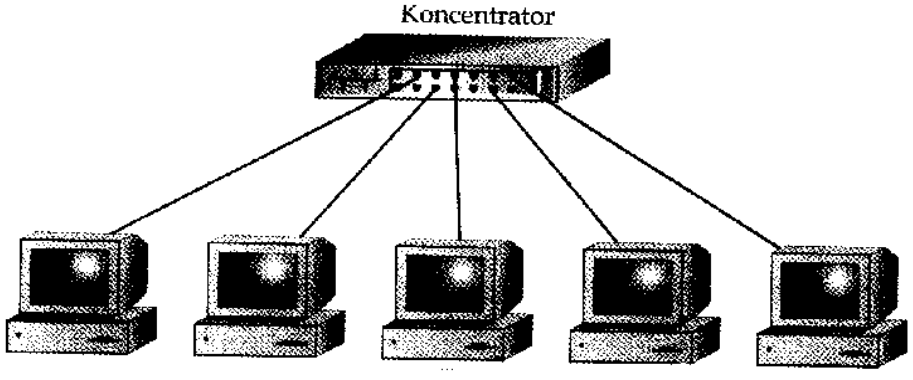
2.1.2 Topologia gwiazdy.

Topologia gwiazdy to taki kształt sieci, w którym centralną jednostką jest koncentrator z podłączonym do niego zestawem kabli odchodzących do wszystkich stacji sieciowych.

Każdy koncentrator mieści zazwyczaj około 24 węzłów sieciowych, choć są i takie, do których można podłączyć od dwu do 96 węzłów. Bez względu na rozmiar koncentratora, można do niego podłączać wiele węzłów w celu rozwijania sieci w pożądanym kierunku.

Cały ruch sieciowy na jednym z połączeń do koncentratora jest powtarzany pozostałym węzłom sieciowym przyłączonym akurat do tego koncentratora. Z tego też powodu, połączenie jednego węzła sieciowego dzieli swoją przepustowość ze wszystkimi pozostałymi połączeniami innych węzłów sieciowych. Przykładowo, jeśli jeden węzeł podłączony do koncentratora używa połowy dostępnej przepustowości, pozostałe węzły również będą mogły pracować tylko przy takiej przepustowości. Innymi słowy, jeśli używa się typu sieci o prędkości 10 Mbps, jest to całkowita wartość przepustowości udostępniona wszystkim węzłom sieciowym w sumie umieszczonym na wspólnym koncentratorze.

Rys. 2.1.2 Układ sieci połączonej zgodnie z topologią gwaizdy.



UWAGA: Sieci, które fizycznie są oparte na topologii gwiazdy, logicznie są sieciami liniowymi bądź pierścieniowymi. Oznacza to, że pomimo wyglądu gwiazdy, sieć i tak „zachowuje się" jak linia lub pierścień. Sieci Ethernetowe okablowane na topologii gwiazdy są logicznie linią, natomiast sieci Token Ring są logicznie pierścieniem.

DEFINICJA! Fizyczny czy logiczny

Terminy „fizyczny" i „logiczny" pojawiają się często w trakcie dyskusji o zagadnieniach sieciowych. Używa się ich w odniesieniu do kilku różnych kwestii. Fizyczny w odniesieniu do sieci komputerowych oznacza faktyczną fizyczną rzecz - to, co można zobaczyć i poczuć. Logiczny określa sposób funkcjonowania - pomimo wyglądu.

Sieci o topologii gwiazdy mogą użyć jednej z wielu form Ethernetu. Najbardziej popularny jest l0Base-T Ethernet o przepustowości 10 Mbps. Obecnie coraz częściej spotyka się l00Base-T Ethernet o przepustowości 100 Mbps. 10Base-T wymaga skrętki Category 3 (Cat-3), natomiast l00Base-T wymaga

kabla Category 5 (Cat-5) (l0Base-T może również użyć kabla Cat-5, ale l00Base-T nie może wykorzystać kabla Cat-3). Kabel i złącza Cat-5 są również bardziej niezawodnie niż komponenty Cat-3.

Okablowanie sieci **l0Base-T** ma następującą charakterystykę:

- Wymaga czterech przewodów (dwie skręcone pary w osłonie); może to być zarówno skrętka nieekranowana (UTP), jak i ekranowana (STP).
- Może być zbudowane przy użyciu kabla Cat-3 lub Cat-5 (kabel Cat-5 posiada osiem żył - cztery skręcone pary - i może dzięki temu uzyskać przyłączenie dwóch węzłów sieciowych za pomocą jednego kabla).
- Maksymalna długość połączenia węzłów sieciowych wynosi 100 metrów.
- Liczba węzłów sieciowych w jednym segmencie logicznym nie jest ograniczona.
- Dla wszystkich połączeń używa złączy RJ-45 (ten typ złącza jest podobny do modułowego złącza telefonicznego, jednak RJ-45 jest większy).

Sieć **l00 Base-T** jest podobna do sieci l0Base-T i ma następującą charakterystykę:

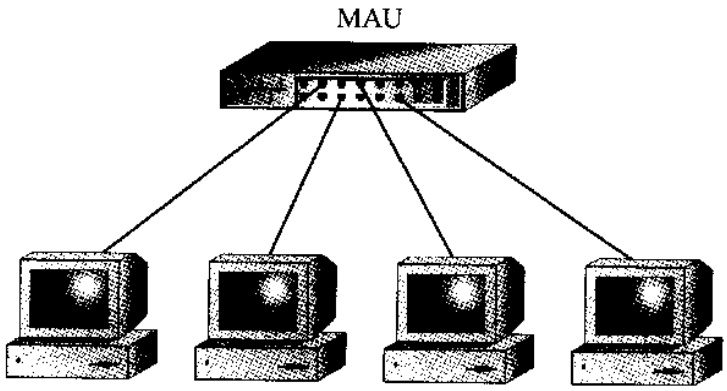
- Wymaga ośmiu żył (cztery skręcone pary w jednej osłonie).
- Musi być zbudowana przy użyciu kabla Cat-5 lub lepszego. (Ulepszona wersja kabla standardowego Cat-5 to Cat-5E, gdzie E oznacza „wzmocniony, ulepszony" (ang. enhanced). Cat-5E wnosi różnorodne, znaczące ulepszenia do podstawowej wersji kabla Cat-5.)
- Maksymalna długość połączenia węzłów sieciowych wynosi 100 metrów.
- Liczba węzłów sieciowych w jednym segmencie logicznym nie jest ograniczona.
- Dla wszystkich połączeń używa złączy RJ-45.

Porównując topologię gwiazdy z liniową, należy wziąć pod uwagę dwa minusy. Po pierwsze, sieć oparta na topologii gwiazdy jest droższa. Wymaga znacznie więcej okablowania i nakładu pracy na jego instalację, a konieczne koncentratory pociągają za sobą dodatkowy koszt. Po odsunięciu jednak kwestii kosztów na bok, dochodzimy do wniosku, że topologie gwiazdy są daleko bardziej niezawodne - w ich przypadku, gdy przestanie funkcjonować jedno z połączeń sieciowych (to znaczy przerwie się lub coś zostanie uszkodzone), problem dotyczyć będzie wyłącznie tego jednego połączenia. Dzieje się tak dlatego, że nawet jeśli koncentratory przesyłają wszystkie dane dalej do kolejnych stacji sieciowych, to posiadają one również funkcję odcinania niepoprawnie działających przyłączeń węzłów sieciowych - jedno zepsute jabłko nie będzie psuć całej reszty. Dodatkowo, ponieważ każdy kabel biegnie bezpośrednio od koncentratora do węzła sieciowego, sieci oparte na topologii gwiazdy sprzyjają szybkiemu odnajdywaniu i reagowaniu na jakiekolwiek problemy; nie trzeba mozolnie analizować sieci w całym budynku, żeby znaleźć awarię.

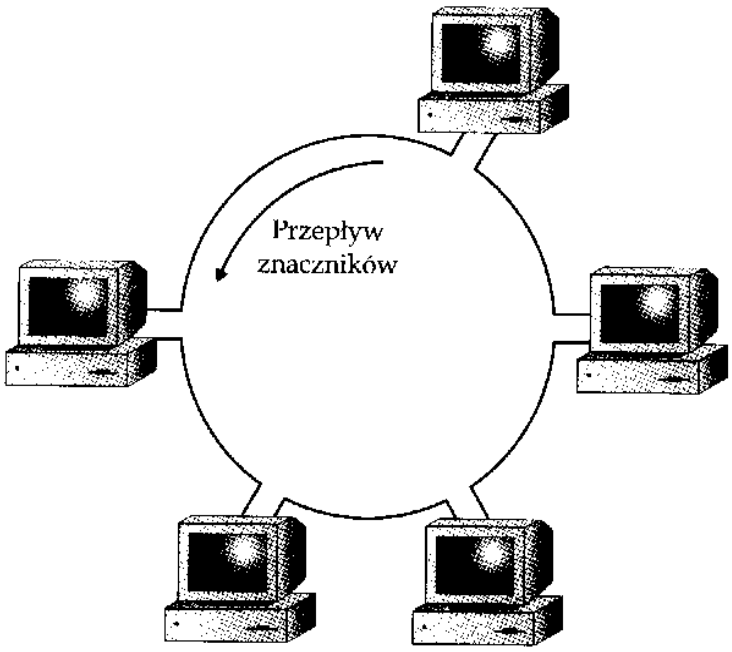
2.1.3 Topologia pierścienia.

Topologia pierścienia, jak się można domyślić, nie jest fizycznym planem okablowania sieci komputerowej. Mamy tutaj do czynienia z ustawieniem logicznym; samo okablowanie zrobione jest na kształt gwiazdy, z wszystkimi węzłami sieciowymi podłączonymi ich własnymi kablami do koncentratora (MAU). Jednak elektrycznie sieć zachowuje się jak pierścień, w którym wszystkie sygnały wędrują po pierścieniu trafiając po kolei do wszystkich węzłów sieciowych. Rysunek 2.1.3 przedstawia przykładową sieć opartą na topologii pierścienia. Sieci LAN o topologii pierścienia oparte są na sieci Token Ring, a nie Ethernecie. Niektóre mogą posługiwać się również technologią FDDI (ang. Fiber Distributed Data Interface) - światłowodową siecią o przepustowości 100 Mbps. Pierścienie są również stosowane w niektórych większych sieciach telekomunikacyjnych, jak na przykład w sieci SONET (ang. Synchronous Optical Network).

Rys 2.1.3 Przykładowa sieć oparta na topologii pierścienia.



Topologia pierścienia, reprezentacja fizyczna



Topologia pierścienia, reprezentacja logiczna

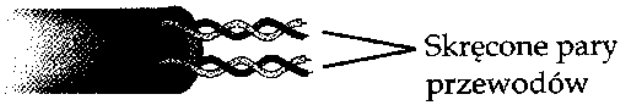
2.2 Podstawowe typy kabli.

Okablowanie sieciowe potrafi być strasznie skomplikowane. Nie tylko istnieją liczne różniące się od siebie typy kabli sieciowych, każde o innej nazwie i charakterystyce, ale też często można wybrać różne typy kabli do jednego typu sieci. Przykładowo, do sieci ethernetowych stosuje się zdumiewającą liczbę kabli, od koncentrycznego począwszy, przez gruby koncentryczny, ekranowany i nieekranowany skręcany, aż do światłowodu. Aby zaprojektować i utrzymać którąkolwiek z sieci, musimy wiedzieć, jakie mamy kable do wyboru i jak je utrzymać.

Pośród wielu różnych typów kabli, do najczęstszych należą kable nieekranowane skręcane (UTP, ang. Unshielded Twisted-Pair) oraz koncentryczne, przy czym UTP daleko wyprzedza swoich rywali. Następnymi w kolejce są skrętki ekranowane i światłowody.

2.2.1 Skrętka nieekranowana.

Skrętka nieekranowana składa się z dwóch lub więcej par wiązek przewodzących izolowanych plastikiem umieszczonych w osłonie (zrobionej z winylu bądź teflonu). W każdej parze wiązki przewodzące są skręcone, co pomaga kablowi obronić się przed interferencjami elektrycznymi. Ostre regulacje określają, jak kabel ten ma być wykonywany, w tym na przykład dotyczą właściwej odległości pomiędzy dwoma skrętami pary żył. Rysunek 2.2.1 ilustruje przykładowy kabel UTP.



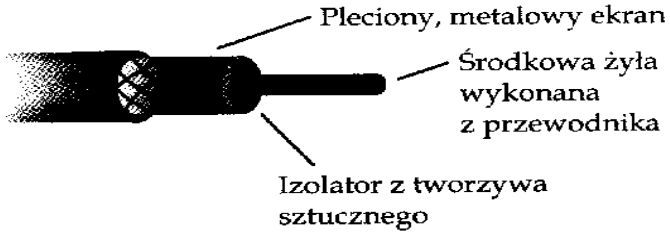
Rys. 2.2.1 Skrętka nieekranowana.

2.2.2 Skrętka ekranowana.

Skrętka ekranowana (STP, ang. Shielded Twisted-Pair) jest podobna do swojego odpowiednika nieekrowanego, posiada jednak osłonę z plecionego metalu, która otacza skręcone pary żył, aby jeszcze skuteczniej ochronić kabel przed interferencjami źródeł elektryczności na zewnątrz kabla.

2.2.3 Kabel koncentryczny.

Kabel koncentryczny składa się z kolei z miedzianej wiązki przewodzącej owiniętej w plastikowy materiał izolacyjny, co następnie jest otoczone osłoną z plecionych przewodów, aż w końcu umieszczone w plastikowej osłonie. (Kabel koncentryczny używany do telewizorów jest bardzo podobny.) Jego dwie podstawowe odmiany używane są do okablowania sieciowego. Cienki Ethernet (10Base-2) stosuje kable RG-58/AU lub RG-58/CU, natomiast Gruby Ethernet (10Base-5) stosuje - jak się można domyślić - znacznie grubszy kabel koncentryczny RG-8. Rysunek 2.2.3 ilustruje przykładowy kabel koncentryczny.



Rys. 2.2.3 Kabel koncentryczny.

2.2.4 Kabel światłowodowy.

Do budowy kabli światłowodowych korzysta się z włókna optycznego, a przesyłają one sygnały w postaci światła, a nie elektryczności. Kable światłowodowe były używane w sieciach o większych prędkościach przesyłu, ale to podejście się zmienia. Już teraz pojawia się sprzęt przesyłający dane z szybkością l Gbps za pomocą miedzianego kabla, tym samym zanika więc tak silna potrzeba stosowania światłowodów. Jest to pocieszające, bowiem kable światłowodowe są wyjątkowo drogie w zakupie, instalacji i utrzymaniu. Niemniej istnieje jedna ich cecha, której kable miedziane nie posiadają: mogą łączyć niezwykle duże odległości. Bez problemu pokonują przeszło 3 km z prędkością 100 Mbps. Z tego powodu światłowody są często stosowane przy łączeniu siecią budynków na terenach takich jak kampusy studenckie. Jednak oprócz tego typu sytuacji, gdy istnieje potrzeba rozciągania sieci na duże odległości, należy unikać posługiwania się kablami światłowodowymi.

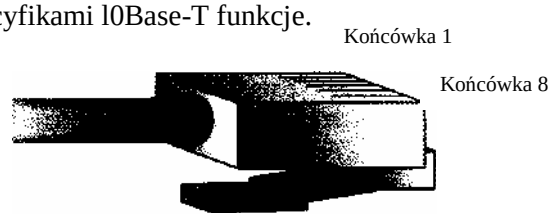
2.3 Kabel skręcany – cd.

Przez ostatnie kilka lat prawie wszystkie nowe sieci są budowane przy użyciu którejś z form kabla skręcanego. Zazwyczaj korzysta się ze skrętek Category 5, chociaż istnieje jeszcze całkiem sporo sieci opierających się na kablu Category 3.

Prawie we wszystkich przypadkach używa się kabla nieekranowanego zamiast ekranowanego, ponieważ jest tańszy, łatwiejszy do zainstalowania i utrzymania, i wcale tak bardzo nie podlega interferencjom elektrycznym. Zarówno sieci Ethernet, jak i Token Ring budowane są przy pomocy skrętek. Należy jednak zwrócić uwagę, że różne typy Ethernetu wymagają różnych typów kabli, w tym sieci o większych prędkościach - kabli ekranowanych.

Kiedy instalujemy nową sieć w oparciu o skrętki, całkowite przyłączenie stacji roboczej do koncentratora jest warunkowane przez kilka różnych komponentów okablowania. Jak pokazano na rysunku 2.2.5, okablowanie zaczyna się przy koncentratorze, gdzie kabel krosowy (zazwyczaj 2-3 metrowy) podłącza port na koncentratorze do panelu krosowego za pomocą złączy RJ-45 na każdym końcu. Po drugiej stronie panelu krosowego może wychodzić na stałe przytwierdzony kabel skręcany, który biegnie do gniazdka sieciowego w ścianie, gdzie jest również przytwierdzony na stałe. Gniazdko to po drugiej stronie jest wyposażone w złącze RJ-45, do którego przyłącza się kolejny kabel krosowy. Kabel ten zostaje następnie podłączony do karty sieciowej stacji roboczej.

Odległość pomiędzy złączem na koncentratorze a złączem w karcie sieciowej komputera nie może być większa niż 100 metrów długości kabla.
Wszędzie, gdzie skrętki nie są przytwierdzone na stałe, używa się modułowych złączy RJ-45. Są to złącza bardzo podobne do swoich odpowiedników telefonicznych, te jednak są większe i przystosowane nawet do ośmiu żył. 10Base-T używa czterech żył (dwie pary: jedna do wysyłania, druga do przyjmowania), a l00Base-T używa ich osiem.
Owe osiem żył w złączu RJ-45 są ponumerowane od l do 8. Chwytając to złącze w lewej dłoni, ustawiamy je tak, by jego końcówki skierowane były do przodu i do góry, wtedy końcówka nr l to ta znajdująca się najdalej (patrz rysunek 2.3.a). Tabela 2.3.b przedstawia standardowe kolory żył kabla Cat-5 i jak mają być podłączone do końcówek, oraz przypisane im w specyfikami l0Base-T funkcje.



Rys.2.3.a Wtyczka RJ 45.

Numery końcówek	**Kolor podstawowy przewodu**	**Kolor pasków przewodu**	**Wykorzystanie**
1	Biały	Pomarańczowy	Transmisja -
2	Pomarańczowy	Biały	Transmisja +
3	Biały	Zielony	Odbiór -
4	Niebieski	Biały	Nie dotyczy
5	Biały	Niebieski	Nie dotyczy
6	Zielony	Biały	Odbiór +
7	Biały	Brązowy	Nie dotyczy
8	Brązowy	Biały	Nie dotyczy

Tab. 2.3.b 10Base – funkcje poszczególnych żył.

Większość urządzeń komunikacyjnych i sieciowych, w tym te przeznaczone do korzystania ze złączy RJ-45, dzieli się na sprzęt komunikujący (ang. Data Communications Eąuipment - DCE) oraz sprzęt terminalowy (ang. Data Terminal Eąuipment - DTE). Jeśli na jednym końcu znajduje się sprzęt DTE, na drugim końcu potrzebujemy sprzęt DCE. W pewnym sensie wygląda to tak samo jak w przypadku śrub i nakrętek. Nie można bezpośrednio połączyć dwóch śrub czy dwóch nakrętek. Ta sama zasada stosuje się w przypadku sprzętu komputerowego: urządzenia DCE i DTE nie mogą łączyć się bezpośrednio z urządzeniami tego samego typu.

Złącze RJ-45 na koncentratorze jest urządzeniem DCE, podczas gdy złącze RJ-45 w karcie sieciowej komputera jest urządzeniem DTE. Nie można uzyskać połączenia pomiędzy urządzeniami DCE i DCE czy urządzeniami DTE i DTE, za pomocą standardowej skrętki/kabla RJ-45, który został podłączony jak zostało to opisane w tabeli 2.3.b. Nie można, przykładowo, posłużyć się standardową skrętką krosową, by połączyć bezpośrednio serwer sieciowy ze stacją, bądź dwie stacje ze sobą, ponieważ są to wszystko urządzenia DTE. Zamiast tego należy kupić bądź przygotować kabel krzyżowy, który umożliwi nam połączenie dwóch urządzeń tego samego typu. Tabela 2.3.c pokazuje schemat połączeń kabla krzyżowego.

2.3.1 Standardy Ethernetu.

Standardy Ethernetu, występujące pod nazwami m.in. 10Base-2, l0Base-T, l00Base-T, zawierają w swoich nazwach wszystkie istotne informacje o swoim przeznaczeniu. Pierwsza część - liczba - może to być 10,100 lub 1000, wskazuje na prędkość (w Mbps), z jaką ten standard przesyła dane. Słowo Base oznacza, że sieć jest *baseband* (o paśmie podstawowym), a nie *broadband* (szerokopasmowa). (Połączenie o paśmie podstawowym przesyła tylko jeden sygnał w danej chwili, a połączenie wielopasmowe przesyła równocześnie bardzo wiele sygnałów.) Kończąca nazwę litera lub cyfra wskazuje na rodzaj użytego kabla, gdzie T oznacza skrętkę (od ang.

twisted-pair), 2 cienki kabel koncentryczny, a 5 gruby koncentryczny. Poniżej znajduje się krótki przewodnik po często spotykanych standardach:

10Base-2 10 Mbps, kabel koncentryczny (RG-58)
10Base-5 10 Mbps, kabel koncentryczny (RG-8)
10Base-T 10 Mbps, skrętka (dwie pary, Cat-3 lub wyższa)
100Base-T 100 Mbps, skrętka (cztery pary, Cat-5), również nazywany 100Base-T4 w celu zaznaczenia czterech par
100Base-TX 100 Mbps, skrętka (dwie pary, Cat-5)
100Base-FX 100 Mbps, kabel światłowodowy
l000Base-T l Gbps, skrętka (cztery pary, Cat-5)

Końcówka	*Kolor podst. przewod.*	*Kolor pasków przew.*	*Końcówka*	*Kolor podst. przewod.*	*Kolor pasków przew.*
1	*Biały*	*Pomarańczowy*	***1***	*Biały*	*Zielony*
2	*Pomarańczowy*	*Biały*	***2***	*Zielony*	*Biały*
3	*Biały*	*Zielony*	***3***	*Biały*	*Pomarańczowy*
6	*Zielony*	*Biały*	***6***	*Pomarańczowy*	*Biały*

Tab. 2.3.c Schemat kabla krzyżowego.

2.3.2 Kategorie kabli.

Skręcane kable sieciowe dzieli się ze względu na ich możliwości przesyłania ruchu sieciowego. Podział na kategorie został opracowany przez organizację Electronics Industry Association (ELA), a w jego wyniku otrzymujemy Level l i 2 oraz Gategory 3,4 i 5, które nazywamy w skrócie Cat-3, Cat-4 i Cat-5. Tabela 2.3.5 ilustruje wskazaną wydajność każdego z poziomów i kategorii.

Poziom lub kategoria	**Wskazana wydajność**
Level 1	Nie podana
Level 2	1 Mbps
Category 3	10Mbps
Category 3	16Mbps
Category 3	**100Mbps**

Tab 2.3.5 Wydajność skrętki.

3. Instalatorstwo i konfiguracja sieci opartej na skrętce – sieć równouprawniona Windows (bez serwera).

3.1 Instalacja okablowania sieci 100Base-T

Sieć oficjalnie nazwana Ethernet 100 Base-T to popularna sieć oparta na skrętce. Kabelki od wszystkich komputerów zbiegają się w jednym punkcie, w którym znajduje się HUB (koncentrator).
Jest to tak zwana topologia gwiazdy, gdyż wszystkie kabelki zbiegają się do jednego punktu. Należy pamiętać, że maksymalna odległość komputera od HUB-a to 100m.

3.1.1. Dlaczego często buduje się sieć zbudowana na skrętce/RJ-45 ?

Zalet jest wiele (dla przypomnienia):

- ✓ Wszystkie kable zbiegają się w jednym punkcie
- ✓ Awaria jednej końcówki nie odcina całej sieci
- ✓ Wszystkie kabelki są podłączone do HUBa (koncentratora) lub switcha (przełącznika)
- ✓ Taką sieć bardzo łatwo podłączyć do Internetu korzystając z tzw. Internet Sharing Hub – Internet Router (jest to specjalny rodzaj Huba podłączanego bezpośrednio do użądzenia dostępowego, nie musimy w takim przypadku ustawiać serwera)
- ✓ Możliwość łączenia kilku HUBów bezpośrednio ze sobą, co pozwala połączyć łatwo np. dwa budynki

Niestety główną wadą takiego rozwiązania są jego koszty. Zakup HUBa to wydatek rzędu 150-300 zł za jednostkę z 8 wejściami (używane na 4 komputery można kupić dużo taniej). Taka struktura zapewnia prędkość 100 mbit/s, czyli wiecej niż sieć oparta na koncentryku.

3.1.2 Instalacja

Będą nam potrzebne następujące elementy:

- ➢ Okablowanie strukturalne UTP kategorii 5 , czyli popularna skrętka
- ➢ Końcówki RJ-45
- ➢ Specjalny zaciskacz do końcówek, cena ok. 100 zł
- ➢ Koncentrator lub przełącznik z odpowiednią ilością wejść (przy dużych sieciach zalecany przełącznik nie hub)

- Przygotowujemy kabel o odpowiedniej długości (od komputera do koncentratora)
- Na końcówce kabla ściągamy izolację, ze szczególną ostrożnością, by nie uszkodzić izolacji wewnętrznych przewodów
- Układamy pojedyncze przewody skrętki zgodnie z opisem (Rys 2.3.a)
- Wciskamy ułożone przewody w końcówkę RJ-45
- Wkładamy końcówkę RJ-45 z włożonymi doń przewodami do zaciskarki i ściskamy, dzięki czemu przewody w końcówce zostają przymocowane blaszkami, znajdującymi się w samej końcówce

3.1.3 Łączenie kilku koncentratorów

Dwa koncentratory można połączyć na dwa sposoby:

Łącząc je korzystając z portu UPLINK, który często znajduje się w koncentratorze. Wtedy HUB-y łączymy dokładnie tak samo jak zwykłe komputery w sieci 100Base-2, tzn. z jednej strony kabla UPLINK jednego koncentratora, z drugiej zwykły port drugiego. UWAGA najczęściej port UPLINK jest współdzielony z jednym z zwykłych porów RJ45 i nie da się ich razem używać. Tu też obowiązuje ograniczenie maksymalnej długości magistrali do ponad 100m.

Łącząc je korzystając z portów RJ-45. Po prostu jedną końcówkę kabelka wpinamy do jednego HUB-a (switcha), a drugą do drugiego. Będzie działać bez problemów. Należy jedynie pamiętać o zastosowaniu kabelka typu crossover.

Nie należy też przesadzać z ilością HUB-ów w sieci gdyż sieć po prostu szybko się zapcha (większe HUB-y, a najlepiej zamiast HUB-ów SWITCHE!).

3.1.4 Łączenie dwóch komputerów za pomocą skrętki bez koncentratora.
Opisana metoda może być przydatna dla posiadaczy karty sieciowej, która ma tylko wyjście na skrętkę a sieć nie posiada HUB-a.
Używając skrętki można połączyć dwie maszyny bez koncentratora za pomocą skrosowanej skrętki.

Jeżeli komputer ma zainstalowany system WinNT/XP (ten system ma możliwość przekazywania danych z komputera dołączonego do jednej z kart do komputera na drugiej z kart) to można w ten sposób podłączyć do niego tyle komputerów ile jest w nim kart sieciowych (jeden komputer do każdej z kart) ale to już jest raczej nie ekonomiczne i koncentrator jest lepszym rozwiązaniem.

Literatura:

- Komar, B. (2002). TCP/IP dla każdego. Gliwice: Helion.
- Sportack, M. (1999). Sieci komputerowe - księga eksperta. Gliwice: Helion.
- Informatyka (podstawy). Praca zbiorowa pod redakcją Henryka Sroki. AE, Katowice 1998.
- "Chip Special". Nr 6 (75)/2003.
- "NetWorld". Nr 11/2003 (95).