Sieci komputerowe. Księga eksperta. Wydanie II poprawione i uzupełnione

Autor: Mark Sportack
Tłumaczenie: Zbigniew Gała
ISBN: 83-7361-503-2
Tytuł oryginału: Networkig Essentials Unleashed
Format: B5, stron: 616

Współczesne komputery dawno przestały być „samotnymi wyspami"; korzystanie z nich (zarówno do celów prywatnych, jak i na potrzeby wielkiego biznesu) nierozerwalnie wiąże się z dostępem do różnego rodzaju sieci, z internetem w roli głównej. W czasach kiedy wykorzystywanie sieci komputerowych stało się powszechne, podstawy ich działania powinny być znane każdemu współczesnemu informatykowi. Ta książka wykracza znacznie poza podstawy. Dostarcza kompletnego opisu technologii związanych z działaniem sieci, omówienia sposobów korzystania z sieci i praktycznych wskazówek dotyczących rozwiązywania problemów pojawiających się w ich funkcjonowaniu. Jeśli więc myślisz o projektowaniu, budowaniu, konfigurowaniu i (przede wszystkim) efektywnym użytkowaniu sieci komputerowych, to niniejsza książka okaże się nieocenioną pomocą, dzięki której zaoszczędzisz wiele czasu spędzonego na poszukiwaniach niezbędnych informacji.

Znajdziesz tu m.in. opis następujących zagadnień:

- Najważniejsze podstawy teoretyczne: model OSI, omówienie warstw sieci
- Tworzenie sieci lokalnych i sieci rozległych
- Opis sieciowych systemów operacyjnych
- Dokładne omówienie najnowocześniejszych technologii bezprzewodowych
- Administrowanie siecią i zagadnienia związane z bezpieczeństwem
- Ewoluowanie sieci komputerowych i działania związane z ustanawianiem standardów sieciowych
- Model odniesienia ISO i jego zastosowania
- Typy i topologie sieci
- Technologie i protokoły sieciowe
- Mechanizmy i media łączności w sieciach komputerowych
- Sieciowe systemy operacyjne i problemy związane z zarządzaniem i administrowaniem nimi
- Mechanizmy zabezpieczeń i ochrony integralności danych w sieciach
- Problemy wynikające z błędnego funkcjonowania sieci, metody ich rozwiązywania i zapobiegania im

Informacjom zawartym w książce zaufało już tysiące administratorów sieci komputerowych. Jeśli więc czujesz się niedoinformowany w tej dziedzinie, całą niezbędną wiedzę znajdziesz w tym kompletnym opracowaniu.
Książkę można z powodzeniem polecić studentom kierunków informatycznych i pokrewnych, którym może posłużyć jako podręcznik przygotowujący do egzaminów z zakresu sieci komputerowych.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 2.

Typy i topologie sieci LAN

Mark A. Sportack

Sieci lokalne (sieci LAN) rozpowszechniły się do dziś w bardzo wielu — zwłaszcza komercjalnych — środowiskach. Mimo że większość z nas miała już większą lub mniejszą styczność z sieciami, to niewiele osób wie, czym one są i w jaki sposób działają. Łatwo wskazać koncentratory czy przełączniki i powiedzieć, że to one są siecią. Ale one są jedynie częściami pewnego typu sieci.

Jak zostało to wyjaśnione w rozdziale 1. pt. „ABC sieci", sieci lokalne najłatwiej zrozumieć po rozłożeniu ich na czynniki pierwsze. Często składniki sieci dzielone są na *warstwy* w sposób określony przez model referencyjny OSI, który szczegółowo przedstawiony został w rozdziale 1. Każda warstwa tego modelu obsługuje inny zbiór funkcji.

Niezbędnym warunkiem wstępnym podziału sieci lokalnej na warstwy jest poznanie dwóch jej atrybutów: metodologii dostępu do sieci oraz topologii sieci. Metodologia dostępu do zasobów sieci LAN opisuje sposób udostępniania zasobów przyłączanych do sieci. Ten aspekt sieci często decyduje o jej typie. Dwoma najczęściej spotykanymi typami są: „każdy-z-każdym" oraz „klient-serwer".

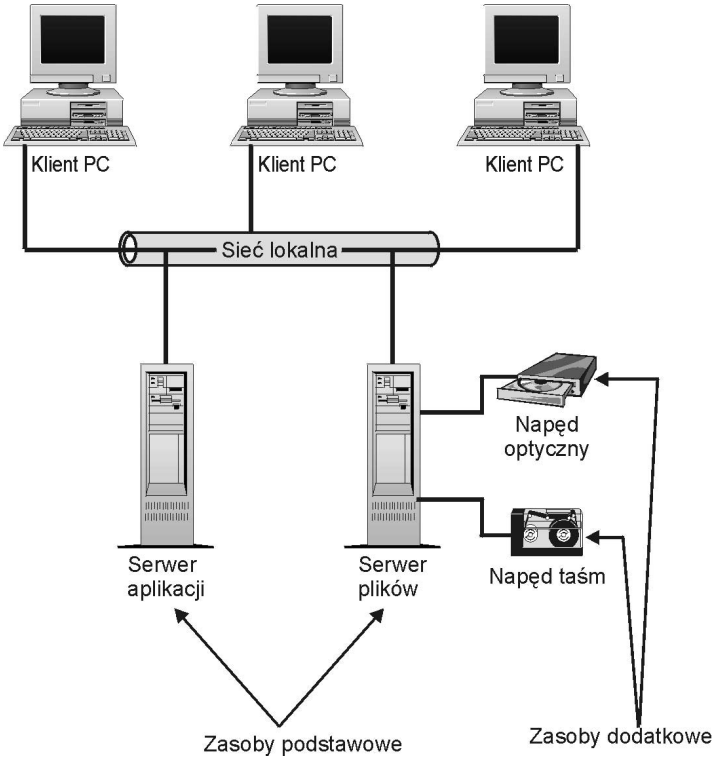
Natomiast topologia sieci LAN odnosi się do sposobu organizacji koncentratorów i okablowania. Topologiami podstawowymi sieci są: topologia magistrali, gwiazdy, pierścienia oraz przełączana (czyli komutowana). Wspomniane atrybuty tworzą zarys ułatwiający rozróżnianie warstw funkcjonalnych sieci LAN. Rozdział niniejszy bada wszystkie możliwe kombinacje typów i topologii sieci LAN. Przedstawione są również ich ograniczenia, korzyści z nich płynące oraz potencjalne zastosowania.

Urządzenia przyłączane do sieci LAN

Przed zanurzeniem się w morzu typów i topologii sieci LAN, warto zapoznać się z niektórymi podstawowymi zasobami dostępnymi w sieci LAN. Trzema najbardziej powszechnymi urządzeniami podstawowymi są klienci, serwery oraz drukarki. Urządzeniem podstawowym jest takie urządzenie, które może uzyskać bezpośredni dostęp do innych urządzeń lub umożliwić innym urządzeniom dostęp do siebie.

Serwer to dowolny komputer przyłączony do sieci LAN, który zawiera zasoby udostępniane innym urządzeniom przyłączonym do tej sieci. *Klient* to natomiast dowolny komputer,

który za pomocą sieci uzyskuje dostęp do zasobów umieszczonych na serwerze. Drukarki są oczywiście urządzeniami wyjścia tworzącymi wydruki zawartości plików. Do wielu innych urządzeń, takich jak napędy CD-ROM oraz napędy taśm, również można uzyskać dostęp za pomocą sieci, ale mimo to są one urządzeniami dodatkowymi. Wynika to z faktu, że bezpośrednio przyłączone są one do urządzeń podstawowych. Urządzenie dodatkowe (na przykład CD-ROM) znajduje się więc w stosunku *podporządkowania* wobec urządzenia podstawowego (na przykład serwera). Drukarki mogą być podporządkowanymi urządzeniom podstawowym urządzeniami dodatkowymi lub — w razie bezpośredniego podłączenia ich do sieci — urządzeniami podstawowymi.[1] Rysunek 2.1 przedstawia zasoby podstawowe, które można znaleźć w sieci lokalnej, a także zależności między zasobami podstawowymi i dodatkowymi.



Rysunek 2.1. *Podstawowe i dodatkowe zasoby sieci LAN*

Typy serwerów

„Serwer" to słowo ogólnie określające komputer wielodostępny (z którego jednocześnie korzystać może wielu użytkowników). Warto zauważyć, że serwery nie są identyczne, lecz stanowią grupę różnorodnych komputerów. Zwykle wyspecjalizowane są w wykonywaniu określonych funkcji, na które wskazuje przymiotnik dołączany do ich nazwy. Wyróżnić więc można serwery plików, serwery wydruków, serwery aplikacji i inne.

[1] Tu należy podkreślić różnicę między drukarką sieciową i zwykłą drukarką. Pierwsza jest urządzeniem podstawowym, natomiast druga — urządzeniem dodatkowym — *przyp. red.*

Serwery plików

Jednym z podstawowych i dobrze znanych rodzajów serwerów jest serwer plików. Serwer plików jest scentralizowanym mechanizmem składowania plików, z których korzystać mogą grupy użytkowników. Składowanie plików w jednym miejscu zamiast zapisywania ich w wielu różnych urządzeniach klienckich daje wiele korzyści, takich jak:

- **Centralna lokalizacja** — wszyscy użytkownicy korzystają z jednego, ustalonego magazynu współdzielonych plików. To z kolei daje korzyści dwojakiego rodzaju. Użytkownicy nie muszą przeszukiwać wielu miejsc, w których potencjalnie zapisany mógł zostać potrzebny im plik; pliki są bowiem składowane w jednym miejscu. Zwalnia to również użytkowników z obowiązku logowania się osobno do każdego z tych wielu miejsc i, tym samym, z konieczności pamiętania wielu różnych haseł dostępu. Dzięki temu dostęp do wszystkich potrzebnych plików umożliwia jedno wyłącznie logowanie (jedna rejestracja).
- **Zabezpieczenie źródła zasilania** — składowanie plików w centralnym serwerze umożliwia również wprowadzanie wielu technik pozwalających na ochronę danych przed zakłóceniami w dostawach prądu elektrycznego. Zmiany częstotliwości lub nawet całkowita przerwa w zasilaniu mogą uszkodzić zarówno dane, jak i sprzęt. Filtracja prądu oraz bateryjne zasilanie dodatkowe, możliwe dzięki zastosowaniu urządzeń „UPS" nieprzerywalnego podtrzymywania napięcia (ang. *Uninterruptible Power Supply*), jest dużo efektywniejsze ekonomicznie w przypadku stosowania ich względem jednego serwera. Podobny sposób ochrony w sieci równorzędnej spowodowałby nadmierne (w stopniu nie do zaakceptowania) podniesienie kosztów ze względu na większą liczbę komputerów wymagających ochrony.
- **Zorganizowane archiwizowanie danych** — składowanie udostępnianych plików w jednym, wspólnym miejscu znacznie ułatwia tworzenie ich kopii zapasowych; wystarcza bowiem do tego celu jedno tylko urządzenie i jedna procedura działania. Zdecentralizowane przechowywanie danych (na przykład w każdym komputerze osobno) oznacza, że kopie zapasowe danych znajdujących się w każdym komputerze musiałyby być tworzone indywidualnie. Kopie zapasowe są podstawowym sposobem ochrony przed utratą lub uszkodzeniem plików. Urządzeniami służącymi do tworzenia kopii zapasowych są napędy taśm, napędy dysków optycznych, a nawet napędy dysków twardych. Do zapisywania kopii zapasowych używać można również wielu napędów dysków, która to technika znana jest jako *porcjowanie.* Porcjowanie polega na wielokrotnych, jednoczesnych zapisach dokonywanych na różnych dyskach twardych. Mimo że technika ta używana jest głównie w celu uzyskania szybszego odczytu danych, to może ona być również stosowana do tworzenia nowych kopii zapasowych podczas każdej operacji zapisu.
- **Szybkość** — standardowy serwer stanowi dużo bardziej niż typowy komputer-klient niezawodną i w pełni konfigurowalną platformę. Przekłada się to bezpośrednio na znaczną, w stosunku do sieci równorzędnej, poprawę wydajności odczytywania plików.

Nie wszystkie pliki nadają się do przechowywania w serwerze plików. Pliki prywatne, zastrzeżone i nie nadające się do użycia przez osoby korzystające z sieci najlepiej zostawić na lokalnym dysku twardym. Przechowywanie ich w serwerze plików daje wszystkie uprzednio opisane korzyści, ale może też być powodem niepotrzebnych zagrożeń.

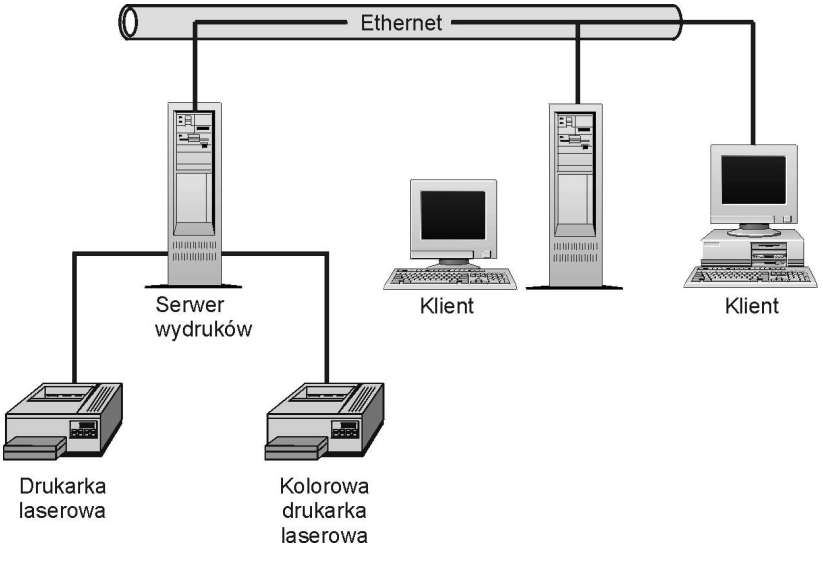
Zastosowanie serwera plików nie zawsze powoduje zwiększenie szybkości obsługi plików. Dostęp do danych zapisanych lokalnie (czyli w tym samym komputerze, który je odczytuje) uzyskać można dużo szybciej niż do plików zapisanych w komputerze zdalnym i pobieranych za pośrednictwem sieci lokalnej. Wspomniane zwiększenie szybkości zależy od szybkości, z jaką pliki mogą być uzyskiwane z innych urządzeń przyłączonych do sieci równorzędnej, a nie od szybkości, z jaką pliki mogą być pobierane z lokalnego dysku twardego.

Serwery wydruków

Serwery mogą być również używane do współdzielenia drukarek przez użytkowników sieci lokalnej. Mimo że ceny drukarek, zwłaszcza laserowych, od czasu wprowadzenia ich na rynek uległy znacznemu obniżeniu, to w mało której organizacji potrzebna jest drukarka na każdym biurku. Lepiej więc korzystać, za pośrednictwem serwera wydruków, z kilku lub nawet jednej tylko drukarki, udostępniając je (ją) w ten sposób każdemu użytkownikowi sieci.

Jedyną funkcją serwerów wydruków jest przyjmowanie żądań wydruków ze wszystkich urządzeń sieci, ustawianie ich w kolejki i „spoolowanie" (czyli wysyłanie) ich do odpowiedniej drukarki. Proces ten jest przedstawiony na rysunku 2.2.

Rysunek 2.2. *Prosty serwer wydruków*



Słowo „spool" jest akronimem wyrażenia „Simultaneous Peripheral Operations On- Line", oznaczającego po polsku „współbieżne bezpośrednie operacje peryferyjne". Operacje te polegają na tymczasowym buforowaniu (magazynowaniu) na nośniku magnetycznym programów i danych w postaci strumieni wyjściowych w celu późniejszego ich wyprowadzenia lub wykonania.[2]

[2] *Spooling* jest to organizowana przez system operacyjny jednoczesna praca procesów i urządzeń zewnętrznych. Polega on na symulowaniu w czasie rzeczywistym obsługi operacji wykonywanych przez urządzenia peryferyjne (np. drukarki) za pomocą plików dyskowych — *przyp. red.*

Każda drukarka przyłączona do serwera wydruków ma swoja własną listę kolejności, czyli kolejkę, która informuje o porządku, w jakim wszystkie żądania są tymczasowo zapisywane i czekają na wydrukowanie. Żądania zwykle przetwarzane są w kolejności, w jakiej zostały otrzymane. Systemy operacyjne klientów, takie jak Windows 95 oraz Windows NT dla stacji roboczej (NT Workstation) firmy Microsoft umożliwiają udostępnianie (współdzielenie) drukarek.

Drukarkę można do sieci LAN przyłączyć również bezpośrednio, czyli bez pośrednictwa serwera wydruków. Umożliwiają to *karty sieciowe*, za pomocą których drukarki mogą być konfigurowane tak, aby były jednocześnie serwerami kolejek wydruków. W takiej sytuacji serwer wydruków nie jest potrzebny, a wystarczy jedynie przyłączyć odpowiednio skonfigurowane drukarki bezpośrednio do sieci LAN — będzie to wystarczające, o ile nie zamierzamy zbytnio obciążać ich czynnościami drukowania.[3]

Serwery aplikacji

Równie często serwery służą jako centralne składy oprogramowania użytkowego. Serwery aplikacji, mimo że na pierwszy rzut oka podobne do serwerów plików, różnią się jednak od nich znacznie. *Serwer aplikacji* jest miejscem, w którym znajdują się wykonywalne programy użytkowe. Aby móc uruchomić określony program, klient musi nawiązać w sieci połączenie z takim serwerem. Aplikacja jest następnie uruchamiana, ale nie na komputerze-kliencie, lecz na rzeczonym serwerze. Serwery umożliwiające klientom pobieranie kopii programów do uruchomienia na komputerach lokalnych to *serwery plików*. Pliki w ten sposób wysyłane są co prawda plikami aplikacji, ale serwery spełniają w takim przypadku funkcje serwerów plików.

Serwery aplikacji umożliwiają organizacji zmniejszenie kosztów zakupu oprogramowania użytkowego. Koszty nabycia i konserwacji jednej, wielodostępnej kopii programu są zwykle dużo niższe od kosztów nabycia i konserwacji kopii instalowanych na pojedynczych komputerach.

Instalowanie zakupionego pakietu oprogramowania użytkowego przeznaczonego dla pojedynczej stacji w serwerze plików może być niezgodne z warunkami umowy jego zakupu. W podobny bowiem sposób, w jaki użytkownicy mogą przekazywać sobie nośnik z oryginalną wersją oprogramowania, również serwer udostępnia pojedynczą kopię programu wszystkim użytkownikom sieci, do której jest przyłączony. Uznawane jest to za piractwo komputerowe. Warto zatem upewnić się, że każdy pakiet oprogramowania instalowany na serwerze zakupiony został na podstawie umowy umożliwiającej korzystanie z niego wielu użytkownikom.

Mimo że w zasadzie oprogramowanie użytkowe warto składować na innych serwerach niż pliki danych (na przykład aplikacje na serwerze aplikacji, a pliki na serwerze plików), od zasady tej odnotować należy jeden, istotny wyjątek.

Niektóre aplikacje tworzą i obsługują duże relacyjne bazy danych. Aplikacje te i ich bazy danych powinny znajdować się obok siebie w serwerze aplikacji.

[3] Jak już wspomniano przy klasyfikowaniu urządzeń sieciowych, obecnie dostępne są zaawansowane drukarki sieciowe z wbudowanymi printserwerami, które można bezpośrednio dołączyć do sieci — *przyp. red.*

Przyczyna tego jest dość prosta: zasady pobierania danych z bazy danych różnią się znacznie od sposobu korzystania z plików Worda czy Excela. Aplikacja relacyjnej bazy danych udostępnia żądane dane, zatrzymując wszystkie pozostałe w bazie danych. Aplikacje automatyzujące pracę w biurze takie jak Word czy Excel, wszystkie informacje zapisują w odrębnych plikach, które zwykle nie są wzajemnie zależne, a na pewno nie w złożony sposób. Inaczej w przypadku aplikacji relacyjnych baz danych, które są bezpośrednio odpowiedzialne za integralność zarówno samych baz danych, jak i ich indeksów. A zarządzanie bazami danych w sieci zwiększa ryzyko uszkodzenia ich indeksów i całej aplikacji.[4]

Typy sieci

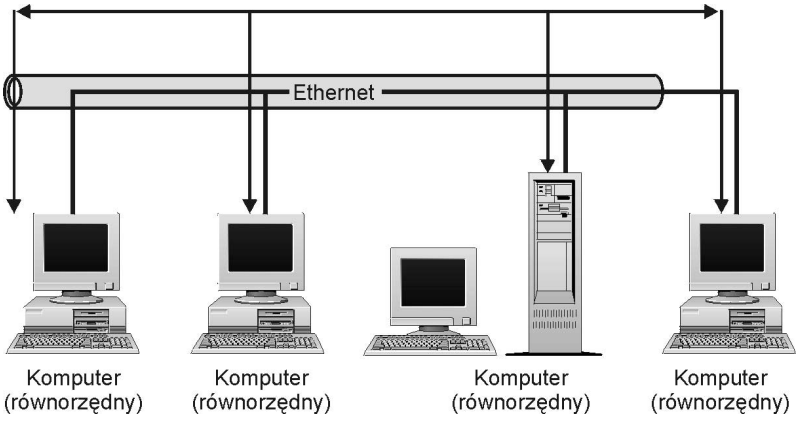
Typ sieci opisuje sposób, w jaki przyłączone do sieci zasoby są udostępniane. Zasobami mogą być klienci, serwery lub inne urządzenia, pliki itd., które do klienta lub serwera są przyłączone. Zasoby te udostępniane są na jeden z dwóch sposobów: równorzędny i serwerowy.

Sieci równorzędne (każdy-z-każdym)

Sieć typu każdy-z-każdym obsługuje nieustrukturalizowany dostęp do zasobów sieci. Każde urządzenie w tego typu sieci może być jednocześnie zarówno klientem, jak i serwerem. Wszystkie urządzenia takiej sieci są zdolne do bezpośredniego pobierania danych, programów i innych zasobów. Innymi słowy, każdy komputer pracujący w takiej sieci jest *równorzędny* w stosunku do każdego innego — w sieciach tego typu nie ma hierarchii.

Rysunek 2.3 przedstawia sieć typu każdy-z-każdym.

Rysunek 2.3. *Sieć typu każdy-z-każdym*



[4] Warto podkreślić, że w zasadzie wielodostępne pliki (np. tekstowe) powinny być przechowywane na serwerach plików, natomiast pliki danych wykorzystywanych przez serwery aplikacji powinny być przechowywane na serwerach aplikacji. Użycie sformułowania „w zasadzie" oznacza, że w dobie sieciowych macierzy dyskowych nie musi tak być! — *przyp. red.*

Korzyści

Korzystanie z sieci równorzędnej daje cztery główne korzyści.

- Sieci typu każdy-z-każdym **są w miarę łatwe do wdrożenia i w obsłudze**. Są bowiem niczym więcej jak tylko zbiorem komputerów-klientów, obsługiwanych przez sieciowy system operacyjny umożliwiający udostępnianie równorzędne. Tworzenie sieci każdy-z-każdym wymaga jedynie dostarczenia i zainstalowania koncentratora (lub koncentratorów) sieci LAN, komputerów, okablowania oraz systemu operacyjnego pozwalającego na korzystanie z tej metody dostępu do zasobów.
- Sieci typu każdy-z-każdym **są bardzo tanie w eksploatacji**. Nie wymagają one drogich i skomplikowanych serwerów dedykowanych, nad którymi należy roztaczać administracyjną opiekę i które trzeba klimatyzować. Brak dedykowanych serwerów eliminuje również towarzyszące im wydatki związane z zatrudnianiem i szkoleniem pracowników, jak również z dodatkowymi kosztami tworzenia pomieszczeń klimatyzowanych wyłącznie dla serwerów. Każdy komputer znajduje się przy biurku lub na nim, a pod opieką korzystającego zeń użytkownika.
- Sieci typu każdy-z-każdym **mogą być ustanawiane przy wykorzystaniu prostych systemów operacyjnych**, takich jak Windows for Workgroups, Windows 95 czy Windows NT.
- Brak hierarchicznej zależności sprawia, że sieci każdy-z-każdym **są dużo odporniejsze na błędy** aniżeli sieci oparte na serwerach. Teoretycznie w sieci typu klient-serwer serwer jest *pojedynczym punktem defektu*. Pojedyncze punkty defektu są miejscami, których niesprawność spowodować może awarię całej sieci. W sieciach typu każdy-z-każdym uszkodzenie jednego komputera powoduje niedostępność jedynie przyłączonej do niego części zasobów sieci.

Ograniczenia

Sieci każdy-z-każdym niosą ze sobą również ryzyko i ograniczenia. Niektóre z nich dotyczą sfer bezpieczeństwa, wydajności i administracji.

Sieć każdy-z-każdym charakteryzuje się następującymi słabościami z zakresu bezpieczeństwa.

- **Użytkownicy muszą pamiętać wiele haseł**, zwykle po jednym dla każdego komputera wchodzącego w skład sieci.
- **Brak centralnego składu udostępnianych zasobów** zmusza użytkownika do samodzielnego wyszukiwania informacji. Niedogodność ta może być ominięta za pomocą metod i procedur składowania, przy założeniu jednak, że każdy członek grupy roboczej będzie się do nich stosować. Użytkownicy obmyślają bardzo twórcze sposoby radzenia sobie z nadmiarem haseł. Większość tych sposobów bezpośrednio obniża bezpieczeństwo każdego komputera znajdującego się w sieci równorzędnej.

- Jak każdy zasób sieciowy, również **bezpieczeństwo jest w sieci równorzędnej rozdysponowane równomiernie**. Na środki bezpieczeństwa charakterystyczne dla tego typu sieci zwykle składają się: identyfikacja użytkownika za pomocą identyfikatora ID i hasła oraz szczegółowe zezwolenia dostępu do określonych zasobów. Struktura zezwoleń dla wszystkich pozostałych użytkowników sieci zależy od „administratora" komputera, dla jakiego są one ustalane.

Mimo że użytkownik każdego komputera w sieci równorzędnej uważany może być za jego administratora, rzadko kiedy posiada on wiedzę i umiejętności potrzebne do sprawnego wykonywania czynności administracyjnych. Jeszcze rzadziej zdarza się, by poziom tych umiejętności był równy dla małej nawet grupy roboczej. Owa nierówność często staje się przyczyną wielu problemów występujących podczas korzystania z sieci typu każdy-z-każdym.

- Niestety, umiejętności techniczne uczestników grupy roboczej nie są zwykle jednakowe. W związku z tym **bezpieczeństwo całej sieci jest wprost proporcjonalne do wiedzy i umiejętności jej technicznie najmniej biegłego uczestnika**. Jedną z lepszych metafor, za pomocą której opisać można taką sytuację jest porównanie sieci równorzędnej do łańcucha. Łańcuch mianowicie jest tak mocny, jak jego najsłabsze ogniwo. Również sieć typu każdy-z-każdym jest tak bezpieczna, jak jej najsłabiej zabezpieczony komputer.

Mimo że obciążenie czynnościami administracyjnymi w sieci każdy-z-każdym jest mniejsze niż w sieci klient-serwer, to jest ono rozłożone na wszystkich członków grupy. Jest to przyczyną powstawania niektórych problemów logistycznych. Najpoważniejszymi z nich są:

- **Nieskoordynowane i niekonsekwentne tworzenie kopii zapasowych danych oraz oprogramowania.** Każdy użytkownik jest odpowiedzialny za swój komputer, w związku z czym jest bardzo możliwe, że każdy będzie wykonywać kopie zapasowe plików w czasie wolnym, wtedy gdy sobie o tym przypomni i gdy będzie mu się chciało (ci, co to już robili, wiedzą, że nie zawsze się chce...).
- **Zdecentralizowana odpowiedzialność za trzymanie się ustalonych konwencji nazywania i składowania plików**. Zakładając, że nie ma jednego miejsca, w którym informacja byłaby centralnie składowana, ani innego systemu logicznego, za pomocą którego zorganizowane byłyby zasoby przyłączone do sieci LAN, orientowanie się w tym, co jest zapisywane w jakim miejscu może stanowić nie lada wyzwanie. Jak wszystko inne w sieciach każdy-z-każdym, również efektywność całej sieci zależna jest bezpośrednio od stopnia, do jakiego ustalone metody i procedury są przestrzegane przez wszystkich jej uczestników.

Mniejsza jest również wydajność tego typu sieci, czego przyczyną jest wielodostępność każdego z komputerów tworzących sieć równorzędną. Komputery standardowe, z jakich zwykle składa się sieć każdy-z-każdym, przeznaczone są bowiem do użytku jako klienci przez pojedynczych użytkowników, w związku z czym nie są najlepiej dostosowane do obsługi wielodostępu. Ze względu na to, wydajność każdego komputera postrzegana przez jego użytkownika zmniejsza się zauważalnie zawsze, gdy użytkownicy zdalni współdzielą jego zasoby.

Pliki i inne zasoby danego hosta są dostępne tylko na tyle, na ile dostępny jest ów host. Innymi słowy, jeśli użytkownik wyłączył swój komputer, jego zasoby są niedostępne dla

reszty komputerów znajdujących się w sieci. Problem ten może być rozwiązany przez nie wyłączanie komputerów, co z kolei rodzi wątpliwości dotyczące innych zagadnień, takich jak bezpieczeństwo.

Innym, bardziej subtelnym aspektem wydajności jest skalowalność. Sieć typu każdy-z-każdym jest z natury nieskalowalna. Im większa liczba komputerów przyłączona jest do sieci równorzędnej, tym bardziej staje się ona „krnąbrna" i nieposłuszna

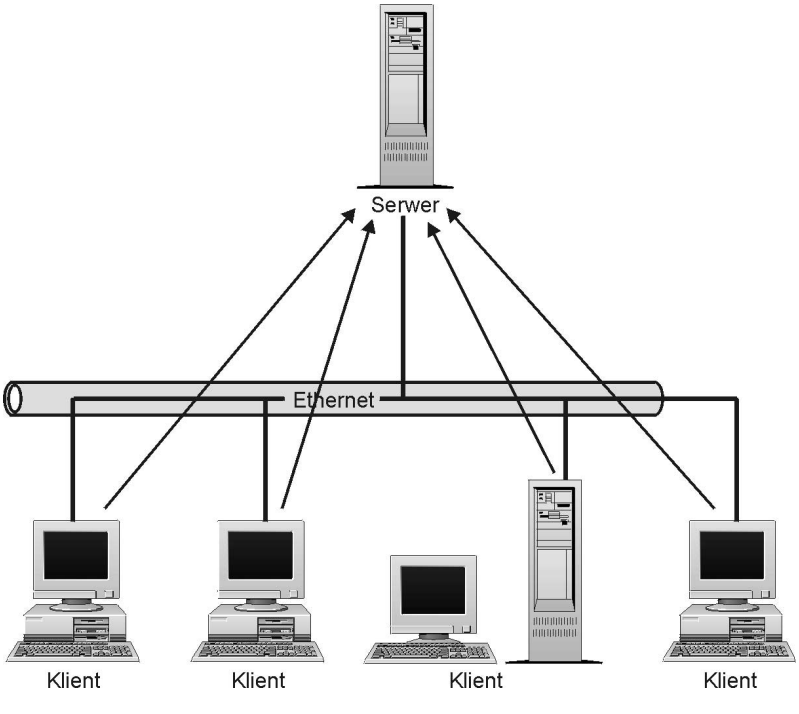
Zastosowania

Sieci typu każdy-z-każdym mają dwa główne zastosowania. Pierwsze — są one idealne dla małych instytucji z ograniczonym budżetem technologii informacyjnych i ograniczonymi potrzebami współdzielenia informacji. Drugie — to zastosowanie tego rodzaju sieci do ściślejszego współdzielenia informacji w ramach grup roboczych wchodzących w skład większych organizacji.

Sieci oparte na serwerach (klient-serwer)

Sieci oparte na serwerach wprowadzają hierarchię, która ma na celu zwiększenie sterowalności różnych funkcji obsługiwanych przez sieć w miarę, jak zwiększa się jej skala. Często sieci oparte na serwerach nazywa się sieciami typu klient-serwer. Rysunek 2.4 ilustruje ową hierarchię klientów i serwerów.

Rysunek 2.4.
Sieć typu klient-serwer



W sieciach klient-serwer zasoby często udostępniane gromadzone są w komputerach odrębnej warstwy zwanych serwerami. Serwery zwykle nie mają użytkowników bezpośrednich. Są one raczej komputerami wielodostępnymi, które regulują udostępnianie swoich

zasobów szerokiej rzeszy klientów. W sieciach tego typu z klientów zdjęty jest ciężar funkcjonowania jako serwery wobec innych klientów.

Korzyści

Wiele jest korzyści płynących z opartego na serwerach podejścia do współdzielenia zasobów sieci. Korzyści te bezpośrednio odpowiadają ograniczeniom sieci każdy-z-każdym. Obszarami, w których zastosowanie sieci serwer-klient przynosi korzyści, są więc bezpieczeństwo, wydajność oraz administracja.

- **Sieci oparte na serwerach są dużo bezpieczniejsze niż sieci równorzędne.** Przyczynia się do tego wiele czynników. Po pierwsze, bezpieczeństwem zarządza się centralnie. Zasoby przyłączone do sieci nie podlegają już zasadzie „najsłabszego ogniwa w łańcuchu", która stanowi integralną część sieci każdy-z-każdym.

Zamiast tego wszystkie konta użytkowników i ich hasła zarządzane są centralnie i tak są weryfikowane przed udostępnieniem zasobu użytkownikowi. Ułatwia to przy okazji życie użytkownikom, zmniejszając znacznie liczbę haseł, które muszą oni pamiętać (najczęściej do jednego).

Inną korzyścią wynikającą z owej centralizacji zasobów jest fakt, że zadania administracyjne, takie jak tworzenie kopii zapasowych, mogą być przeprowadzane stale i w sposób wiarygodny.

- **Sieci oparte na serwerach charakteryzują się większą wydajnością** wchodzących w jej skład komputerów ze względu na kilka czynników. Po pierwsze — z każdego klienta zdjęty jest ciężar przetwarzania żądań innych klientów. W sieciach opartych na serwerach każdy klient musi przetwarzać jedynie żądania pochodzące wyłącznie od jego głównego użytkownika.

Co więcej, przetwarzanie to jest wykonywane przez serwer, który jest skonfigurowany specjalnie do wykonywania tej usługi. Zwykle serwer cechuje się większą mocą przetwarzania, większą ilością pamięci i większym, szybszym dyskiem twardym niż komputer-klient. Dzięki temu żądania komputerów-klientów mogą być obsłużone lepiej i szybciej.

Taki sposób organizacji sieci oszczędza również syzyfowego trudu zapamiętywania miejsc w sieci, w których przechowywane są różne zasoby. W sieciach opartych na serwerach liczba „kryjówek", w których dane mogą się przed nami schować, jest ograniczona do liczby serwerów. W środowisku Windows NT zasoby serwerów mogą być łączone z każdym komputerem jako jego osobny dysk logiczny (taki sposób ich łączenia nazywa się mapowaniem). Po zmapowaniu dysku sieciowego można korzystać z jego (zdalnych z perspektywy mapującego) zasobów w taki sam sposób, w jaki korzysta się z zasobów znajdujących się na dysku lokalnym.

- **Łatwo również zmieniać rozmiary sieci serwerowych**, czyli je skalować. Niezależnie od liczby przyłączonych do sieci klientów, jej zasoby znajdują się bowiem zawsze w jednym, centralnie położonym miejscu. Zasoby te są również centralnie zarządzane i zabezpieczane. W związku z tym wydajność sieci jako całości nie zmniejsza się wraz ze zwiększaniem jej rozmiaru.

Ograniczenia

- Sieć serwerowa ma jedno tylko ograniczenie: **zainstalowanie i obsługa tego rodzaju sieci kosztuje dużo więcej niż sieci typu każdy-z-każdym**. Owa różnica w cenie ma kilka powodów.

Przede wszystkim, koszty sprzętu i oprogramowania są dużo wyższe ze względu na potrzebę zainstalowania dodatkowego komputera, którego jedynym zadaniem będzie obsługa klientów. A serwery najczęściej są dosyć skomplikowanymi — czyli drogimi — urządzeniami.

Również koszty obsługi sieci opartych na serwerach są dużo wyższe. Wynika to z potrzeby zatrudnienia wyszkolonego pracownika specjalnie do administrowania i obsługi sieci. W sieciach każdy-z-każdym każdy użytkownik odpowiedzialny jest za obsługę własnego komputera, w związku z czym nie trzeba zatrudniać dodatkowej osoby specjalnie do realizacji tej funkcji.

Ostatnią przyczyną wyższych kosztów sieci serwerowej jest większy koszt ewentualnego czasu przestoju. W sieci każdy-z-każdym wyłączenie lub uszkodzenie jednego komputera powoduje niewielkie jedynie zmniejszenie dostępnych zasobów sieci lokalnej. Natomiast w sieci lokalnej opartej na serwerze, uszkodzenie serwera może mieć znaczny i bezpośredni wpływ na praktycznie każdego uczestnika sieci. Powoduje to zwiększenie potencjalnego ryzyka użytkowego sieci serwerowej. W celu jego zmniejszenia stosowane są więc różne podejścia, z grupowaniem serwerów w celu uzyskania nadmierności włącznie. Każde z tych rozwiązań — niestety — dalej zwiększa koszty sieci serwerowej.

Zastosowania

Sieci oparte na serwerach są bardzo przydatne, zwłaszcza w organizacjach dużych oraz wymagających zwiększonego bezpieczeństwa i bardziej konsekwentnego zarządzania zasobami przyłączonymi do sieci. Koszty dodane sieci opartych na serwerach mogą jednak przesunąć je poza zasięg możliwości finansowych małych organizacji.

Sieci mieszane

Różnice między sieciami każdy-z-każdym a sieciami opartymi na serwerach nie są tak oczywiste jak sugerują to poprzednie podpunkty. Przedstawione one w nich zostały specjalnie jako odmienne typy sieci, dla tzw. potrzeb akademickich, czyli dla lepszego ich opisania i zrozumienia. W rzeczywistości różnice między typami sieci uległy rozmyciu ze względu na wielość możliwości udostępnianych przez różne systemy operacyjne.

Obecnie standardowo zakładane są sieci będące mieszanką sieci równorzędnych (każdy-z-każdym) i serwerowych (opartych na serwerze). Przykładem tego rodzaju sieci jest sieć o architekturze serwerowej grupującej centralnie zasoby, które powinny być ogólnodostępne. W ramach takiej organizacji sieci, udostępnianie zasobów wewnątrz lokalnych grup roboczych może nadal odbywać się na zasadzie dostępu równorzędnego.

Topologie sieci lokalnych

Topologie sieci LAN mogą być opisane zarówno na płaszczyźnie fizycznej, jak i logicznej. Topologia fizyczna określa geometryczną organizację sieci lokalnych. Nie jest ona jednak mapą sieci. Jest natomiast teoretyczną strukturą graficznie przedstawiającą kształt i strukturę sieci LAN.

Topologia logiczna opisuje wszelkie możliwe połączenia między parami mogących się komunikować punktów końcowych sieci. Za jej pomocą opisywać można, które punkty końcowe mogą się komunikować z którymi, a także ilustrować, które z takich par mają wzajemne, bezpośrednie połączenie fizyczne. Rozdział niniejszy koncentruje się tylko na topologii fizycznej.

Do niedawna istniały trzy podstawowe topologie fizyczne:

- magistrali,
- pierścienia,
- gwiazdy.

Rodzaj topologii fizycznej wynika z rodzaju zastosowanych technologii sieci LAN. Na przykład, dla sieci Token Ring, z definicji, stosowane były topologie pierścienia. Jednak koncentratory, znane również jako *jednostki dostępu do stacji wieloterminalowych* (ang. *MSAU — Multi-Station Access Units*) sieci Token Ring, rozmyły różnice między topologią pierścienia a topologią gwiazdy dla sieci Token Ring. W wyniku wprowadzenia tychże koncentratorów powstały sieci o topologii *pierścieni gwiaździstych.* Podobnie wprowadzenie przełączania sieci LAN zmieniło sposób klasyfikowania topologii. Lokalne sieci przełączane, niezależnie od rodzaju ramki i metody dostępu, są topologicznie podobne. Pierścień jednostki dostępu do stacji wieloterminalowej, który do niedawna używany był do przyłączania — na poziomie elektroniki — wszelkich urządzeń do sieci Token Ring, nie pełni już tej funkcji. Zamiast niego każde z przyłączanych urządzeń ma własny minipierścień, do którego przyłączone są tylko dwa urządzenia: ono samo oraz port przełączania. W związku z tym słowo „przełączane" powinno być dodane do triady nazw podstawowych fizycznych topologii sieci LAN, na określenie kolejnego, czwartego już ich typu.

Przełączniki wprowadzają topologię gwiazdy, bez względu na rodzaj protokołu warstwy łącza danych dla którego są zaprojektowane. Ze względu na przyjęcie terminu „przełącznik" (dzięki nieustannym kampaniom reklamowym producentów przełączników), sieci częściej określa się mianem „przełączanych" (lub „komutowanych") niż „gwiaździstej magistrali" (ang. *star bus*) czy „gwiaździstego pierścienia"(ang. *star ring*). W związku z tym przełączanie może być uważane za rodzaj topologii. Mimo to na ewentualnym egzaminie MCSE lepiej jednak zaznaczyć odpowiedź „gwiaździsta magistrala (star bus)" i „gwiaździsty pierścień (star ring)".

Przełączanie rozdzieliło dotychczasowe nierozłączki: topologię i technologię sieci LAN. Obecnie bowiem dosłownie wszystkie technologie LAN mogą być zakupione w wersji przełączanej. Ma to niebagatelny wpływ na sposób uzyskiwania dostępu do sieci i, tym

samym, na jej ogólną sprawność. Wpływ ten przedstawiony jest bardziej szczegółowo w dalszym punkcie tego rozdziału zatytułowanym „Topologia przełączana".

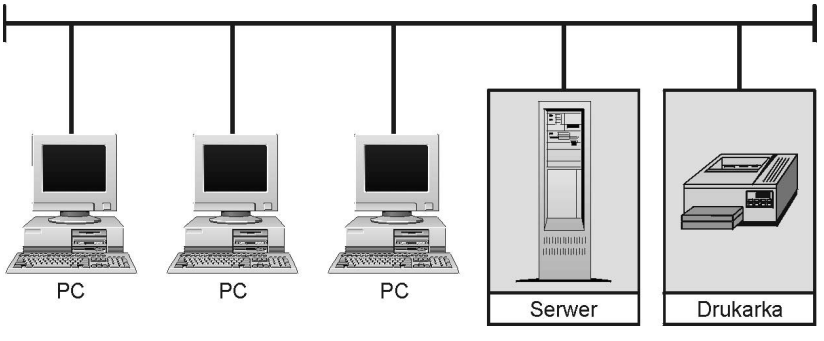
Mimo że kupić można przełączniki dla sieci lokalnych o dowolnej technologii, na przykład Ethernet, Token Ring, FDDI itd., to przełączniki te nie pełnią funkcji mostków translacyjnych. Oznacza to, że nie są one zdolne do przełączania ramek pomiędzy sieciami lokalnymi o różnych architekturach.

Topologia magistrali

Topologię magistrali wyróżnia to, że wszystkie węzły sieci połączone są ze sobą za pomocą pojedynczego, otwartego (czyli umożliwiającego przyłączanie kolejnych urządzeń) kabla. 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.[5] 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. Przykładowa topologia magistrali przedstawiona jest na rysunku 2.5.

Rysunek 2.5. *Standardowa topologia magistrali*



Typowa magistrala składa się z pojedynczego kabla łączącego wszystkie węzły w sposób charakterystyczny dla sieci równorzędnej. Kabel ten nie jest obsługiwany przez żadne urządzenia zewnętrzne. Zatem wszystkie urządzenia przyłączone do sieci słuchają transmisji przesyłanych magistralą i odbierają pakiety do nich zaadresowane. Brak jakichkolwiek urządzeń zewnętrznych, w tym wzmacniaków, sprawia, że magistrale sieci lokalnych są proste i niedrogie. Jest to również przyczyną dotkliwych ograniczeń dotyczących odległości, funkcjonalności i skalowalności sieci.

[5] W kablach koncentrycznych jeden z terminatorów dodatkowo jest łączony z uziemieniem — *przyp. red.*

Topologia ta jest więc praktyczna jedynie dla najmniejszych sieci LAN. Wobec tego obecnie dostępne sieci lokalne o topologii magistrali są tanimi sieciami równorzędnymi udostępniającymi podstawowe funkcje współdziałania sieciowego. Produkty te są przeznaczone do użytku w domach i małych biurach.

Jedynym od tego wyjątkiem jest specyfikacja IEEE 802.4 magistrali Token Bus sieci LAN. Technologia ta charakteryzuje się względnie dużą odpornością na błędy, dość wysokim stopniem determinizmu i ogólnym podobieństwem do sieci lokalnej Token Ring. Deterministyczne sieci LAN oferują administratorom wysoki stopień kontroli przez określanie maksymalnej ilości czasu, podczas którego ramka danych może znajdować się w transmisji. Podstawową różnicę stanowi oczywiście fakt, że magistrala Token Bus została wdrożona na podstawie topologii magistrali.

Magistrala Token Bus spotkała się z wyjątkowo chłodnym przyjęciem rynku. Jej zastosowanie było ograniczone do linii produkcyjnych zakładów pracy. Topologie magistralowe rozwinęły się jednak w tysiące innych form. Na przykład dwoma wczesnymi formami Ethernetu były 10Base2 oraz 10Base5, oparte na topologii magistrali oraz kablu koncentrycznym. Magistrale stały się również technologią ważną stosowaną do łączenia składników poziomu systemowego i urządzeń peryferyjnych w ramach wewnętrznych architektur komputerów.[6]

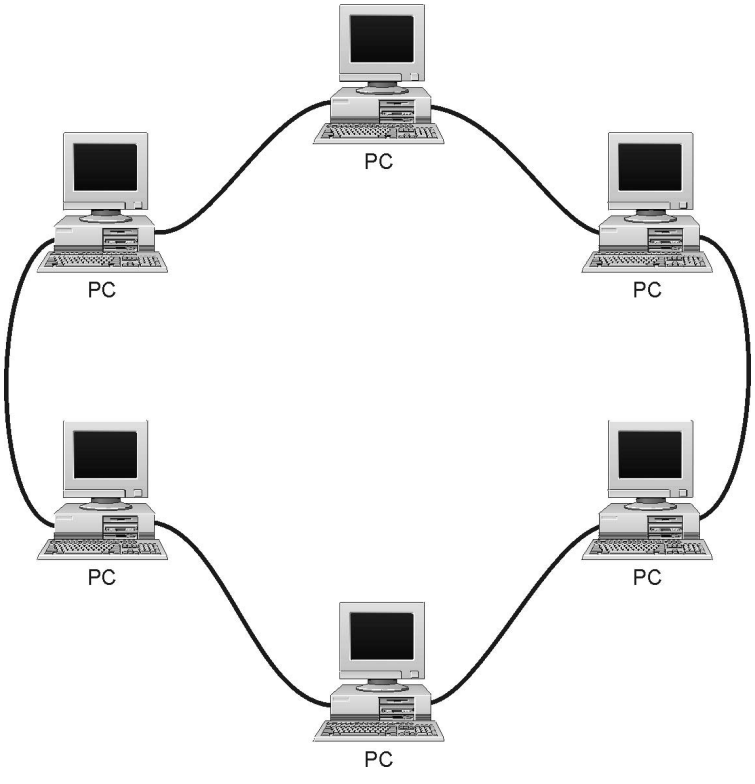
Topologia pierścienia

Pierwszą topologią pierścieniową była topologia prostej sieci równorzędnej. Każda przyłączona do sieci stacja robocza ma w ramach takiej topologii dwa połączenia: po jednym do każdego ze swoich najbliższych sąsiadów (patrz rysunek 2.6). Połączenie takie musiało tworzyć fizyczną pętlę, czyli pierścień. Dane przesyłane były wokół pierścienia w jednym kierunku. Każda stacja robocza działała podobnie jak wzmacniak, pobierając i odpowiadając na pakiety do niej zaadresowane, a także przesyłając dalej pozostałe pakiety do następnej stacji roboczej wchodzącej w skład sieci.

Pierwotna, pierścieniowa topologia sieci LAN umożliwiała tworzenie połączeń równorzędnych między stacjami roboczymi. Połączenia te musiały być zamknięte; czyli musiały tworzyć pierścień. Korzyść płynąca z takich sieci LAN polegała na tym, że czas odpowiedzi był możliwy do ustalenia. Im więcej urządzeń przyłączonych było do pierścienia, tym dłuższy był ów czas. Ujemna strona tego rozwiązania polegała na tym, że uszkodzenie jednej stacji roboczej najczęściej unieruchamiało całą sieć pierścieniową.

Owe prymitywne pierścienie zostały wyparte przez sieci Token Ring firmy IBM, które z czasem znormalizowała specyfikacja IEEE 802.5. Sieci Token Ring odeszły od połączeń

[6] Topologia magistrali jest ciągle stosowana w małych sieciach biurowych i domowych. Są dwa szeroko znane standardy tego typu: TOKEN BUS (IEEE 802.4) i Ethernet w wersji 10BASE2 i 10BASE5 (IEEE 802.3) bazujący na kablach koncentrycznych. Standardy Ethernetu koncentrycznego w pewnym momencie dominowały na rynku sieci LAN, natomiast Token Bus nigdy nie zdobył szerszego uznania, chociaż był i jest chętnie stosowany w sieciach przemysłowych do przesyłania danych między stacjami operatorskimi a regulatorami cyfrowymi. W takich zastosowaniach ma wyraźną przewagę nad innymi standardami, ponieważ jest prosty w budowie, odporny na zakłócenia elektromagnetyczne i można w nim określić maksymalny czas oczekiwania na dostęp do magistrali — *przyp. red.*

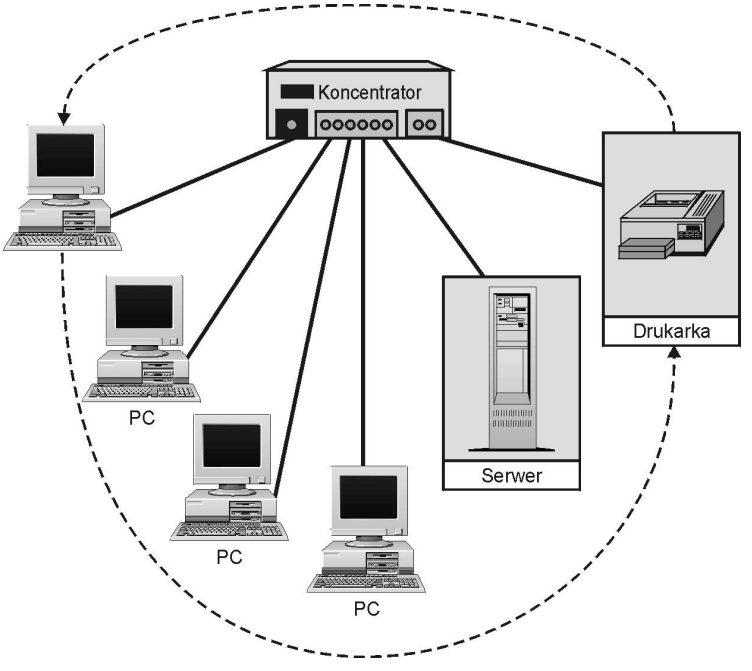


Rysunek 2.6. *Topologia równorzędna każdy-z-każdym*

międzysieciowych każdy-z-każdym na rzecz koncentratorów wzmacniających. Wyeliminowało to podatność sieci pierścieniowych na zawieszanie się przez wyeliminowanie konstrukcji każdy-z-każdym pierścienia. Sieci Token Ring, mimo pierwotnego kształtu pierścienia (stąd nazwa ang. *ring — pierścień*), tworzone są przy zastosowaniu topologii gwiazdy i metody dostępu cyklicznego, co przedstawia rysunek 2.7.

Sieci LAN mogą być wdrażane w topologii gwiazdy, przy zachowaniu — mimo to — metody dostępu cyklicznego. Sieć Token Ring zilustrowana na rysunku 2.7 przedstawia pierścień wirtualny tworzony za pomocą metody dostępu cyklicznego zwanej *round-robin*. Linie pełne reprezentują połączenia fizyczne, podczas gdy linie przerywane — logiczny przebieg sterowanego dostępu do nośnika.

Token w takiej sieci przesyłany jest do kolejnych punktów końcowych, mimo że wszystkie one są przyłączone do wspólnego koncentratora. I to pewnie dlatego wielu z nas nie potrafi oprzeć się pokusie określenia sieci Token Ring jako mających „logiczną" topologię pierścienia, nawet mimo tego, że fizycznie ujęte są one w kształcie gwiazdy. Pokusie tej ulegli na przykład twórcy kursu i egzaminu Microsoft Networking Essentials. Uważają oni sieć Token Ring za mającą topologię pierścienia, a nie — jak jest w istocie — topologię gwiazdy. Co prawda pierścień występuje, ale na poziomie elektroniki, wewnątrz koncentratora Token Ring, czyli *jednostki dostępu do stacji wieloterminalowej*.



Rysunek 2.7. *Topologia pierścieniowa o kształcie gwiazdy*

Topologia gwiazdy

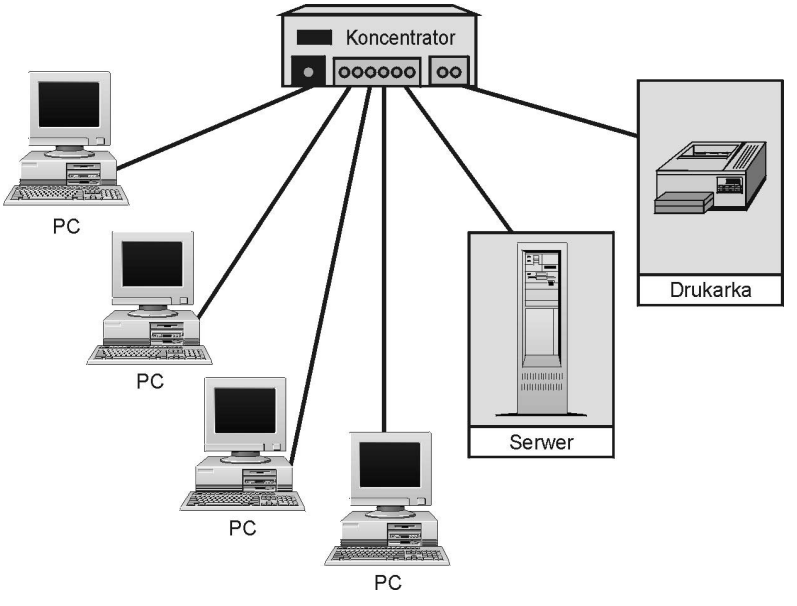
Połączenia sieci LAN o topologii gwiazdy z przyłączonymi do niej urządzeniami rozchodzą się z jednego, wspólnego punktu, którym jest *koncentrator*, co przedstawia rysunek 2.8. Odmiennie niż w topologiach pierścienia — tak fizycznej, jak i wirtualnej — każde urządzenie przyłączone do sieci w topologii gwiazdy może uzyskiwać bezpośredni i niezależny od innych urządzeń dostęp do nośnika. W tym celu urządzenia te muszą współdzielić dostępne szerokości pasma koncentratora. Przykładem sieci LAN o topologii gwiazdy jest 10BaseT Ethernet.

Połączenia w sieci LAN o małych rozmiarach i topologii gwiazdy rozchodzą się z jednego wspólnego punktu. Każde urządzenie przyłączone do takiej sieci może inicjować dostęp do nośnika niezależnie od innych przyłączonych urządzeń. Topologie gwiazdy stały się dominującym we współczesnych sieciach LAN rodzajem topologii. Są one elastyczne, skalowalne i stosunkowo tanie w porównaniu z bardziej skomplikowanymi sieciami LAN o ściśle regulowanych metodach dostępu. Gwiazdy przyczyniły się do dezaktualizacji magistral i pierścieni, formując tym samym podstawy pod ostateczną (obecnie przynajmniej) topologię sieci LAN — topologię przełączaną.

Topologia przełączana

Przełącznik jest urządzeniem warstwy łącza danych (warstwy 2 modelu referencyjnego OSI), zwanym również wieloportem. Przełącznik „uczy się" adresów sterowania dostępem do nośnika i składuje je w wewnętrznej tablicy przeglądowej (w tablicy wyszukiwania). Tymczasowo, między nadawcą ramki i jej zamierzonym odbiorcą, tworzone są ścieżki

Rysunek 2.8.
Topologia gwiazdy



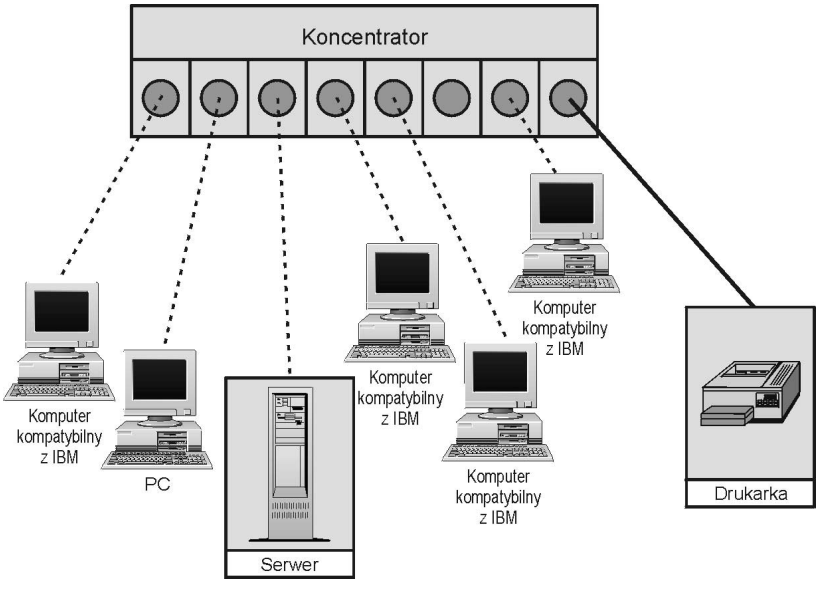
przełączane (czyli inaczej komutowane), a następnie ramki te są przesyłane dalej wzdłuż owych tymczasowych ścieżek.[7]

Typowa sieć LAN o topologii przełączanej pokazana jest na rysunku 2.9, na którym widać wiele połączeń urządzeń z portami koncentratora przełączającego. Każdy port oraz urządzenie, które jest doń przyłączone, ma własną dedykowaną szerokość pasma. Choć pierwotnie przełączniki przesyłały dalej ramki na podstawie ich adresów fizycznych, to postęp technologiczny szybko zmienia ten stan rzeczy. Obecnie dostępne są przełączniki, które potrafią przetwarzać komórki, ramki, a nawet pakiety używające adresów warstwy 3, takie jak protokół IP.

Ramka jest ciągiem bitów zmiennej długości i jednoznacznie zdefiniowanej budowie strukturą, która zawiera przesyłane dane, adresy nadawcy i adresata odbiorcy oraz inne dodatkowe pola danych pomocnicze niezbędne do przesyłania dalej ramek w sieci z wykorzystaniem mechanizmów adresowania w warstwie 2 modelu referencyjnegoOSI. Komórki są podobne do ramek, z jednym wyjątkiem — są one strukturami nie o zmiennej, lecz o niezmiennej — to ramki o jednakowej, ściśle zdefiniowanej długości dla danego typu sieci. Pakiety natomiast są układami protokołów działających na poziomie warstwy 3 modelu referencyjnego OSI. IP oraz IPX to dwa przykłady protokołów warstwy 3, które używają pakietów do opakowywania danych przesyłanych do domen zdalnych.[8]

[7] Przełącznik realizuje transmisję w trzech etapach: odbiera dane od nadawcy (na jego żądanie), określa odbiorcę (port, do którego dołączona jest karta odbiorcy) i przesyła dane ze swojego portu wyjściowego do odbiorcy. Aby cały ten proces przebiegał prawidłowo, przełącznik w chwili pierwszego włączenia identyfikuje topologię sieci i zapamiętuje adresy kart sieciowych (MAC-adresy) w odpowiednich tablicach trasowania — *przyp. red.*

[8] Pakietami nazywamy struktury danych przesyłane przez protokoły pracujące w warstwie trzeciej OSI. Ciąg bitów tworzący pakiet ma ustalony format, a w jego skład wchodzą: nagłówek sterujący, dane i suma kontrolna — *przyp. red.*



Rysunek 2.9. *Topologia przełączana*

Przełączniki poprawiają sprawność sieci LAN na dwa sposoby. Pierwszy polega na zwiększaniu szerokości pasma dostępnego w sieci. Na przykład, przełączany koncentrator Ethernetu o 8 portach zawiera 8 odrębnych domen kolizji, z których każda przesyła dane z prędkością 10 Mbps, co daje łączną szerokość pasma rzędu 80 Mbps.

Drugi sposób zwiększania sprawności przełączanych sieci LAN polega na zmniejszaniu liczby urządzeń, wymuszających udostępnianie wszystkich segmentów pasma szerokości. Każda przełączana domena kolizji składa się jedynie z dwóch urządzeń: urządzenia sieciowego oraz portu koncentratora przełączanego, z którym urządzenie to jest połączone. Wyłącznie te dwa urządzenia mogą rywalizować o szerokość pasma 10 Mbps w segmencie, w którym się znajdują. W sieciach, które nie korzystają z metody dostępu do nośnika na zasadzie rywalizacji o szerokość pasma — takich jak Token Ring lub FDDI — tokeny krążą między dużo mniejszą liczbą urządzeń sieciowych niż ma to zwykle miejsce w sieciach o dostępie opartym na zasadzie rywalizacji.

Jedyny problem dużych sieci przełączanych (komutowanych) polega na tym, że przełączniki nie rozróżniają rozgłoszeniowych transmisji danych. Zwiększenie sprawności sieci jest wynikiem segmentacji wyłącznie domeny kolizji, a nie domeny rozgłaszania. Nadmierne natężenie rozgłaszania może więc znacznie i niekorzystnie wpłynąć na wydajność sieci LAN.

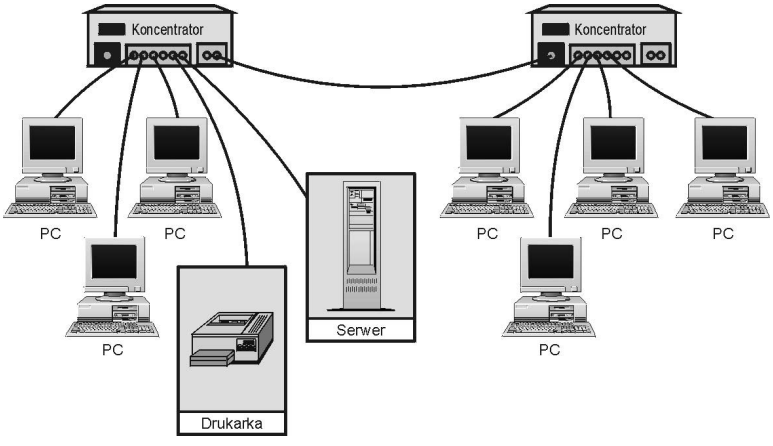
Topologie złożone

Topologie złożone są rozszerzeniami i/lub połączeniami podstawowych topologii fizycznych. Topologie podstawowe są odpowiednie jedynie do bardzo małych sieci LAN. Skalowalność topologii podstawowych jest bardzo ograniczona. Topologie złożone tworzone są z elementów składowych umożliwiających uzyskanie topologii skalowalnych odpowiadających zastosowaniom.

Łańcuchy

Najprostszą z topologii złożonych otrzymać można w wyniku połączenia szeregowego wszystkich koncentratorów sieci tak, jak przedstawia to rysunek 2.10. Taki sposób łączenia znany jest jako *łańcuchowanie.* Wykorzystuje ono porty już istniejących koncentratorów do łączenia ich z kolejnymi koncentratorami. Dzięki temu uniknąć można ponoszenia kosztów dodatkowych związanych z tworzeniem odpowiedniego szkieletu.

Rysunek 2.10. *Koncentratory łańcuchujące*



Małe sieci LAN mogą być zwiększane (skalowane dodatnio) przez łączenie koncentratorów w łańcuchy (łańcuchowania ich). Łańcuchy dają się łatwo tworzyć i nie wymagają żadnych specjalnych umiejętności administracyjnych. Łańcuchy stanowiły alternatywną, wobec sieci LAN pierwszej generacji, metodę przyłączania urządzeń.

Ograniczenia nakładane przez łańcuchowanie określić można na wiele sposobów. Specyfikacje technologii LAN, takie jak 802.3 Ethernet, ograniczały maksymalny rozmiar sieci LAN ze względu na maksymalną liczbę koncentratorów i/lub wzmacniaków, które można łączyć ze sobą szeregowo. Maksymalna długość kabla określona przez wymogi warstwy fizycznej pomnożonej przez maksymalną liczbę urządzeń dających się łączyć szeregowo określała maksymalny rozmiar sieci LAN. Rozmiar ten nazywany jest *maksymalną średnicą sieci.* Zwiększanie rozmiaru sieci ponad tę wartość wpływa negatywnie na działanie sieci LAN. Nowoczesne, wysokowydajne sieci lokalne, takie jak Fast Ethernet, nakładają ścisłe ograniczenia dotyczące średnicy sieci i liczby połączonych w jej ramach wzmacniaków.

Wzmacniak Regenerator jest urządzeniem, które odbiera przychodzące sygnały, wzmacnia je do poziomu ich pierwotnej siły i umieszcza z powrotem w sieci. Zwykle funkcje wzmocnienia i powtórzenia sygnału są dołączane również do koncentratorów. Terminy „wzmacniakregenerator" oraz „koncentrator" są więc synonimami i jako takie mogą być używane zamiennie.[9]

[9] Regenerator jest urządzeniem, które na podstawie zakłóconego i stłumionego wejściowego sygnału cyfrowego odtwarza jego pierwotny kształt. Obecnie regeneracja i rozdzielanie sygnałów nie jest realizowane przez dedykowane urządzenia, ale przez koncentrator (hub) lub przełącznik (switch) — *przyp. red.*

Sieci łańcuchowane korzystające z dostępu do nośnika na zasadzie rywalizacji mogą powodować problemy na długo przed osiągnięciem maksymalnej średnicy sieci. Łańcuchowanie zwiększa liczbę połączeń i tym samym również liczbę urządzeń możliwych do przyłączenia do sieci LAN. Nie powoduje to zwiększenia całkowitej szerokości pasma ani domen kolizji. Łańcuchowanie zwiększa po prostu liczbę urządzeń współdzielących dostępne w sieci pasmo szerokości. Zbyt wiele urządzeń konkurujących o ten sam zakres pasma może powodować kolizje i szybko uniemożliwić poprawne działanie sieci LAN.

Topologia ta sprawdza się najlepiej w sieciach lokalnych, w skład których wchodzi garstka jedynie koncentratorów i — co najwyżej –niewielkie współdziałanie w ramach sieci rozległych.

Hierarchie

Topologie hierarchiczne składają się z kilku (więcej niż jednej) warstw koncentratorów. Każda z tych warstw realizuje inną funkcję sieci. Warstwa podstawowa jest w tego rodzaju topologii zarezerwowana dla komunikacji między stacją roboczą a serwerem. Poziomy wyższe umożliwiają grupowanie wielu poziomów użytkownika. Innymi słowy, wiele koncentratorów poziomu użytkownika połączonych jest za pomocą mniejszej liczby koncentratorów wyższego poziomu. Wszystkie koncentratory, niezależnie od poziomu, na którym się znajdują, najczęściej są urządzeniami identycznymi. Różni je tylko warstwa, na której się znajdują, a tym samym ich zastosowanie. Organizacja hierarchiczna jest najodpowiedniejsza dla sieci LAN o rozmiarach średnich do dużych, w których rozwiązuje ona problemy skalowalności i agregacji ruchu w sieci.

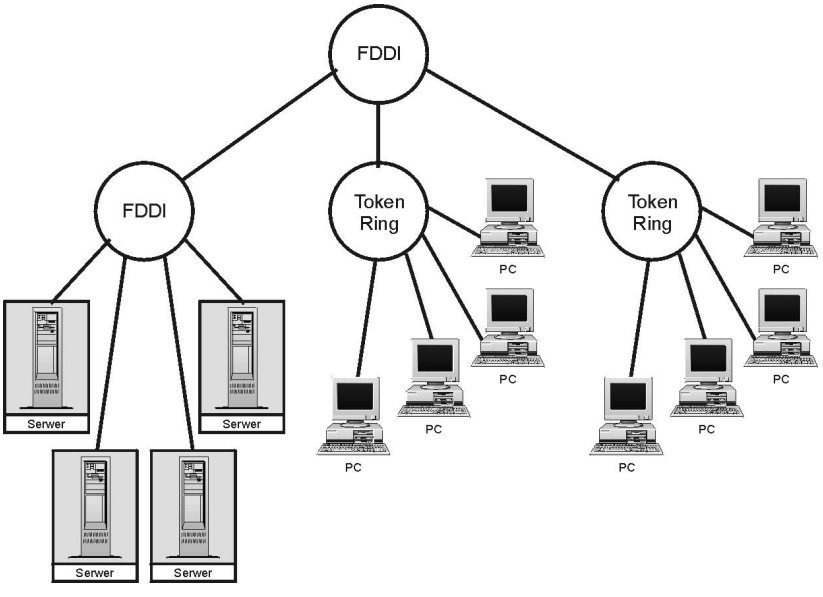
Hierarchiczne pierścienie

Rozmiary sieci pierścieniowych mogą być zwiększane przez łączenie wielu pierścieni w sposób hierarchiczny, tak jak przedstawia to rysunek 2.11. Łączność między stacją roboczą a serwerem może być realizowana za pomocą tylu pierścieni o ograniczonych rozmiarach, ile potrzeba do uzyskania odpowiedniego poziomu sprawności. Pierścień poziomu drugiego, zarówno w sieciach Token Ring, jak i FDDI, może być używany do wzajemnego łączenia wszystkich pierścieni poziomu użytkownika oraz do umożliwienia zagregowanego dostępu do sieci rozległych (sieci WAN).

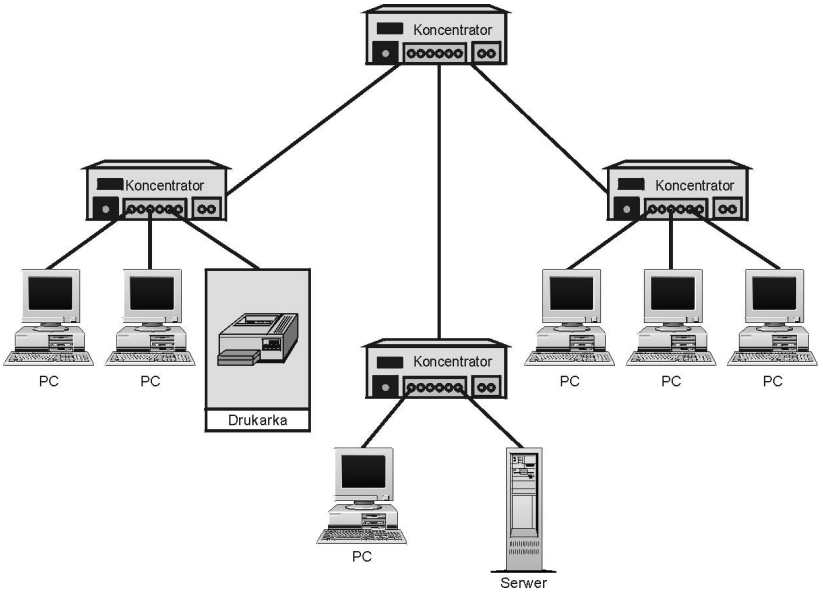
Sieci lokalne o małych pierścieniach można skalować, dodając hierarchicznie kolejne pierścienie. Rysunek 2.11 ilustruje dwa odrębne pierścienie Token Ring o szybkości przesyłania danych rzędu 16 Mbps każdy (przedstawione logicznie jako pętle), które używane są do łączenia komputerów użytkowników oraz odrębną pętlę FDDI używaną do łączenia serwerów i tworzenia szkieletu.

Hierarchiczne gwiazdy

Topologie gwiazdy również mogą być organizowane hierarchicznie w wiele gwiazd, co przedstawia rysunek 2.12. Hierarchiczne gwiazdy mogą być realizowane jako pojedyncze domeny kolizji lub dzielone przy użyciu przełączników, routerów i mostków na segmenty, z których każdy jest domeną kolizji.



Rysunek 2.11. *Topologia hierarchiczna pierścienia*



Rysunek 2.12. *Topologia hierarchiczna gwiazdy*

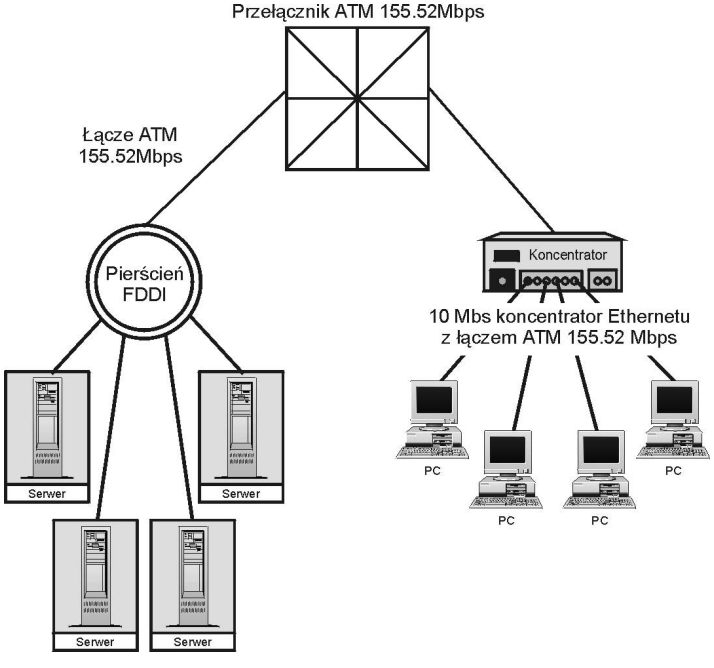
Domena kolizji składa się ze wszystkich urządzeń konkurujących o prawo do transmisji przy użyciu współdzielonego nośnika. Przełączniki, mostki oraz routery dzielą domeny kolizji tworząc w ten sposób wiele mniejszych domen kolizji.

Topologia hierarchiczna gwiazdy używa jednego poziomu do łączenia użytkownika z serwerem, a drugiego — jako szkielet.

Hierarchiczne melanże

Ogólna sprawność sieci może być zwiększona przez nie wypełnianie wszystkich wymagań funkcjonalnych sieci lokalnej na siłę w ramach jednego rozwiązania. Dzisiejsze nowoczesne koncentratory przełączające umożliwiają łączenie wielu różnych technologii.[10]

Nowe topologie mogą być wprowadzane przez wstawianie odpowiednich płytek logicznych w obudowę koncentratora przełączającego o wielu gniazdach. Topologię hierarchiczną wykorzystywać można do tworzenia topologii mieszanych, co przedstawia rysunek 2.13.



Rysunek 2.13. *Topologia hierarchiczna mieszana*

W przedstawionym przykładzie topologii hierarchicznej mieszanej do łączenia koncentratorów poziomu użytkownika używany jest szkielet ATM asynchronicznego trybu przesyłania (ang. — *Asynchronous Transfer Mode*), do łączenia serwerów — sieć FDDI, a do łączenia stacji roboczych — sieć Ethernet. W podejściu tym sieć LAN dzielona jest na jej składniki funkcjonalne (przyłączania stacji roboczej, przyłączania serwera oraz szkieletu), co umożliwia zastosowanie odpowiedniej technologii dla każdej z realizowanych funkcji. Wspomniane obszary funkcjonalne opisane są szerzej w podrozdziale następnym.

[10] Sprawność sieci można zwiększać dodatkowo nie tylko przez podwyższenie wymagań funkcjonalnych na określone urządzenia w danym typie sieci (np. wymiana urządzeń 10 Mbps Ethernet na 100 Mbps lub 1000 Mbps), ale przede wszystkim na wykorzystywaniu zalet różnych technologii. Na rysunku 2.13 pokazano sieć łączącą technologie ATM, Token Ring i Ethernet, która może być znacznie wydajniejsza dla określonego zastosowania niż jakakolwiek sieć homogeniczna. Należy podkreślić, że współczesne przełączniki z zaimplementowaną obsługą warstwy trzeciej OSI umożliwiają łatwe łączenia wielu technologii — *przyp. red.*

Obszary funkcjonalne sieci LAN

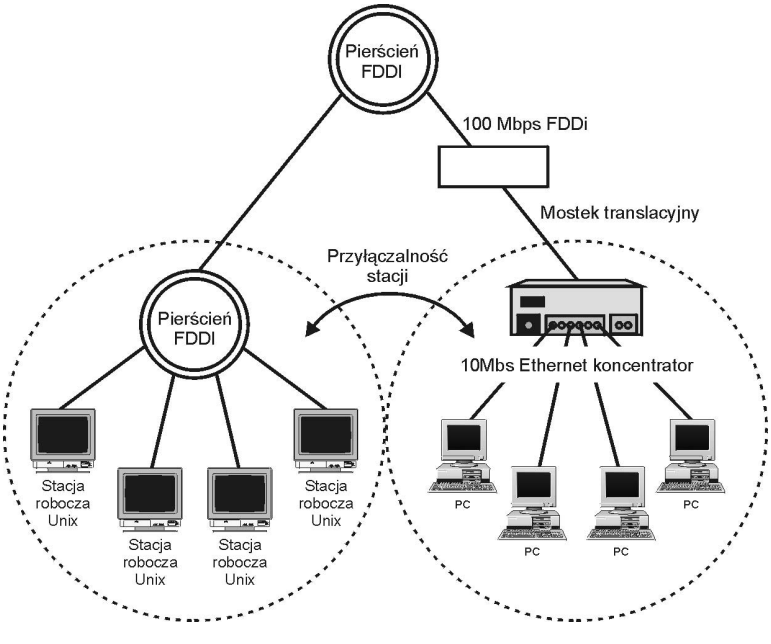
Topologiczne wariacje mogą stanowić ważny sposób optymalizowania wydajności każdego z obszarów funkcjonalnych sieci LAN. Sieci lokalne składają się z czterech odrębnych obszarów funkcjonalnych: przyłączenia stacji (komputera), przyłączenia serwera, przyłączenia sieci WAN oraz ze szkieletu. Każdy obszar funkcjonalny jest najlepiej obsługiwany przez odpowiednie topologie podstawowe i złożone.

Przyłączanie stacji

Podstawową funkcją większości sieci LAN jest przyłączanie stacji. Jak nazwa wskazuje, jest to ta część sieci LAN, która używana jest do przyłączania stacji roboczych użytkowników do sieci. Ten obszar funkcjonalny ma zwykle najmniejsze ze wszystkich obszarów wymagania odnośnie właściwości sieci LAN. Istnieją oczywiście wyjątki od tej tendencji, takie jak stacje robocze CAD/CAM, konferencje wideo itp. Ogólnie jednak rzecz biorąc, oszczędności dotyczące kosztów i wydajności poczynione w tym obszarze funkcjonalnym mają mniejsze prawdopodobieństwo negatywnego wpływu na sprawność sieci.

Przyłączanie urządzeń mających różne wymagania względem wydajności sieci może wymagać korzystania z wielu technologii LAN, co przedstawia rysunek 2.14. Na szczęście, obecnie produkowane koncentratory mimo nie dającej się modyfikować obudowy obsługują wiele różnych technologii.

Rysunek 2.14.
Przyłączalność stacji w sieci LAN



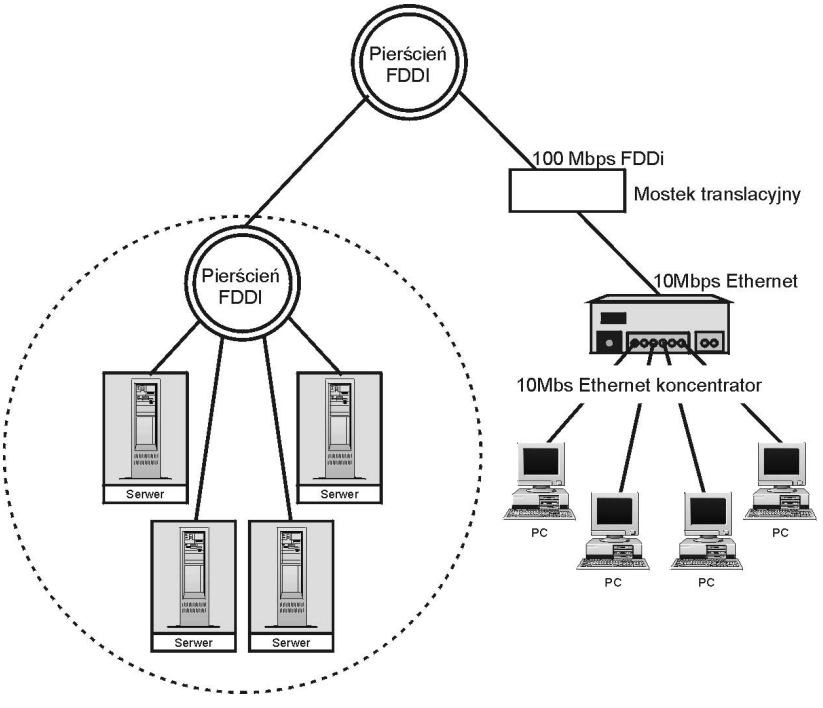
Sieci LAN są podstawowym sposobem łączenia stacji roboczych i ich urządzeń peryferyjnych. Różne wymagania stacji roboczych odnośnie właściwości sieci mogą wymagać stosowania mieszanych rozwiązań topologiczno-technologicznych.

Przyłączanie serwera

Serwery są zwykle solidniejsze od stacji roboczych użytkowników. Na ogół są one miejscami dużego natężenia ruchu i muszą obsługiwać wielu klientów i/lub innych serwerów. W przypadku serwerów o dużej przepustowości agregowanie ruchu musi być ujęte w projekcie topologii sieci LAN; inaczej wydajność sieci ulegnie obniżeniu. Również przyłączalność serwerów powinna być bardziej niezawodna niż przyłączalność stacji roboczych, zwłaszcza w zakresie dostępnych szerokości pasma oraz metody dostępu.

Topologie sieci LAN mogą również być zmieniane w celu dostosowania ich do zwiększonych wymagań serwerów i ich grup. Na rysunku 2.15 przedstawiona jest taka przykładowa łączona topologia hierarchiczna. Grupa serwerów połączona jest za pomocą małej pętli FDDI; mniej niezawodne stacje robocze są tu połączone za pomocą Ethernetu.

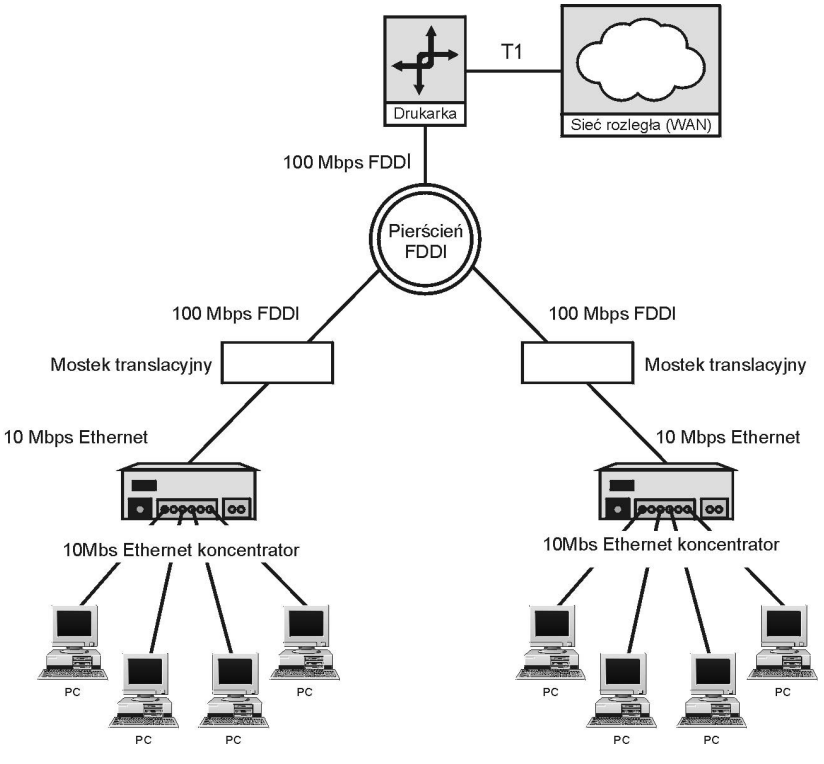
Rysunek 2.15. *Przyłączalność serwera sieci LAN*



Przyłączanie do sieci WAN

Często pomijanym aspektem topologii sieci lokalnych (sieci LAN) jest możliwość łączenia ich z sieciami rozległymi (z sieciami WAN). W wielu przypadkach sieć WAN jest przyłączana za pomocą pojedynczego łącza szkieletu z routerem, tak jak przedstawia to rysunek 2.16.

Połączenie sieci LAN z routerem umożliwiające dostęp do sieci WAN stanowi podstawowe ogniwo całej konstrukcji sieci LAN. Wybór nieodpowiedniej technologii w tak krytycznym miejscu może spowodować znaczne obniżenie poziomu wydajności w obsłudze ruchu



Rysunek 2.16. *Przyłączanie sieci WAN*

przychodzącego do sieci LAN i wychodzącego z niej. Technologie LAN używające dostępu do nośnika na zasadzie rywalizacji są zdecydowanie nieodpowiednie do wykonywania tej funkcji.

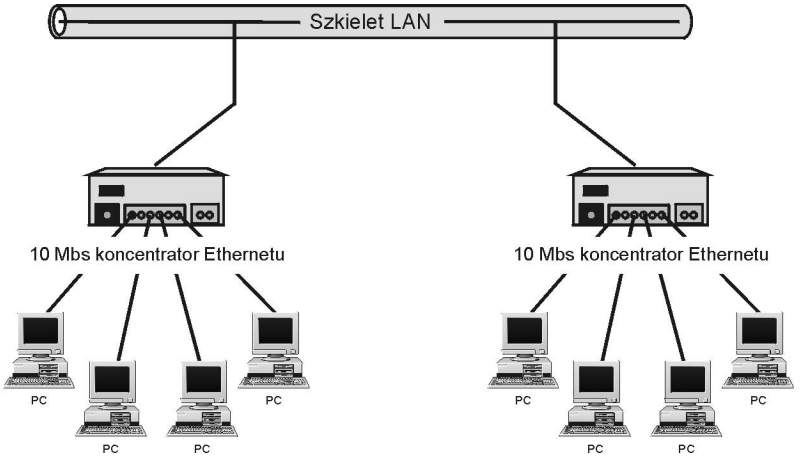
Sieci obsługujące znaczne natężenia ruchu z sieci WAN do LAN i z LAN do WAN wymagają najbardziej niezawodnych z dostępnych połączeń. Wybrana technologia powinna być niezawodna pod względem jej nominalnej szybkości transmisji oraz stosowanej metody dostępu. Za wszelką cenę powinno się tu unikać technologii o dostępie opartym na zasadzie rywalizacji. Stosowanie rywalizacji, nawet w połączeniu z dedykowanym portem przełączanym może powodować problemy w sieciach o dużym natężeniu ruchu. Rozwiązanie takie będzie powodowało zatykanie się sieci LAN.

Przyłączanie do szkieletu

Szkielet sieci LAN tworzą urządzenia używane do łączenia koncentratorów. Szkielet może być tworzony w różnych topologiach za pomocą różnorodnych składników sieciowych, co przedstawia rysunek 2.17.

Szkielet sieci LAN realizuje funkcję krytyczną. Łączy on wszystkie zasoby sieci lokalnej oraz ewentualnie sieć lokalną z siecią rozległą. Logiczny opis szkieletu przedstawiony jest na rysunku 2.17. Może on być zrealizowany na jeden z wielu sposobów.

Wybór najodpowiedniejszej topologii szkieletu dla zadanej sieci LAN nie jest łatwy. Niektóre opcje są łatwiejsze do opracowania, dostępniejsze cenowo i łatwiejsze w obsłudze.

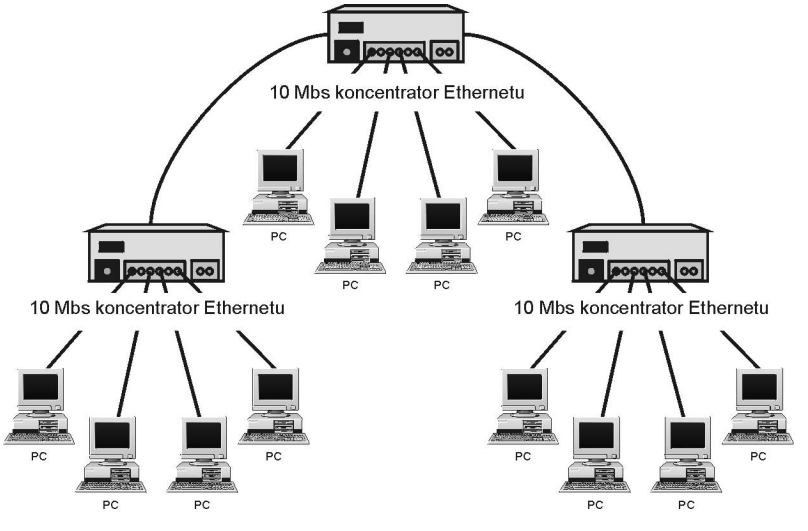


Rysunek 2.17.
Szkielet LAN

Inne mogą być z kolei kosztowne: zarówno do nabycia, jak i w obsłudze. Kolejna ważna różnica polega na skalowalności różnych topologii szkieletu. Rozmiary niektórych można łatwo zwiększać aż do pewnej granicy, po przekroczeniu której wymagają one ponownej inwestycji w celu utrzymania akceptowalnych poziomów wydajności. Każda opcja musi być sprawdzona indywidualnie stosownie do istniejącej sytuacji oraz wymagań technicznych.

Szkielet szeregowy

Szkielet szeregowy, przedstawiony na rysunku 2.18, jest szeregiem koncentratorów połączonych ze sobą łańcuchowo. Jak zostało to opisane w poprzednich punktach, topologia ta jest odpowiednia wyłącznie do zastosowań w małych sieciach.



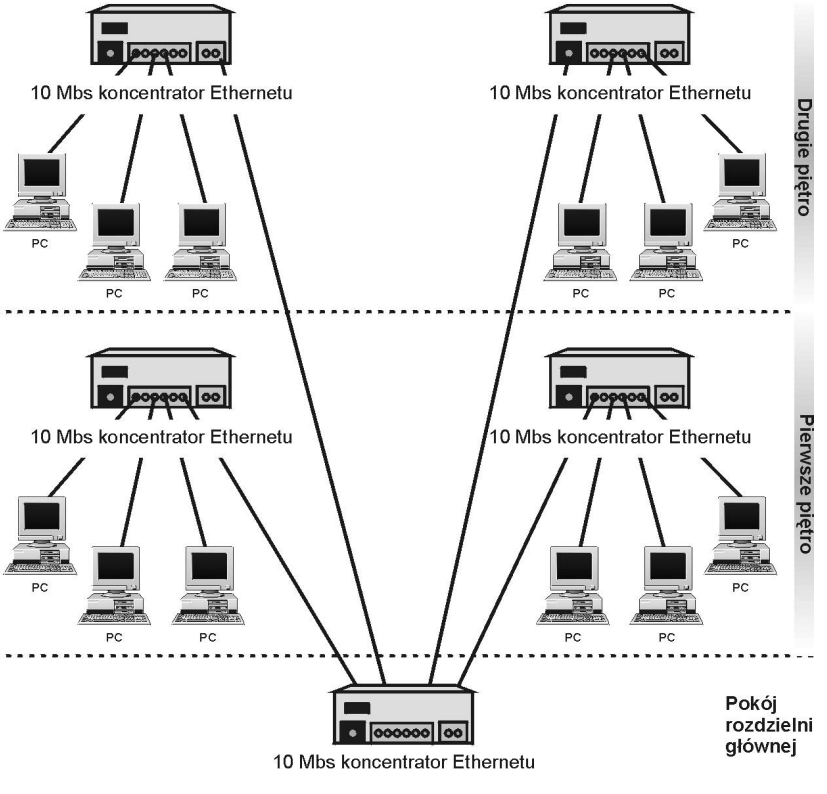
Rysunek 2.18.
Szkielet szeregowy

Szkielet rozproszony

Szkielet rozproszony jest rodzajem topologii hierarchicznej, która może być utworzona przez zamontowanie koncentratora szkieletowego w centralnym miejscu sieci. Zwykle

centrum topologii okablowania znajduje się w pokoju rozdzielni telefonicznej. Miejsce to jest idealne w celu umieszczenia tam również koncentratora szkieletu rozproszonego. Połączenia wychodzące z tego koncentratora biegną do innych koncentratorów znajdujących się w budynku (w którym sieć jest montowana), co przedstawia rysunek 2.19.

Rysunek 2.19.
Szkielet rozproszony



Szkielet rozproszony może być utworzony przez centralne umieszczenie koncentratora szkieletowego. Połączenia rozchodzą się z tego koncentratora do innych koncentratorów znajdujących się w budynku. Szkielet o topologii rozproszonej, w odróżnieniu od szkieletu szeregowego, umożliwia pokrycie siecią LAN dużych budynków bez obaw o przekroczenie maksymalnych średnic sieci.

Jeśli rozważamy utworzenie szkieletu rozproszonego, upewnijmy się najpierw, że znamy topologię okablowania budynku i ograniczenia długości poszczególnych nośników sieci LAN. Dla sieci o rozmiarach średnich do dużych i szkielecie rozproszonym jedynym nośnikiem wartym wzięcia pod uwagę jest kabel światłowodowy.

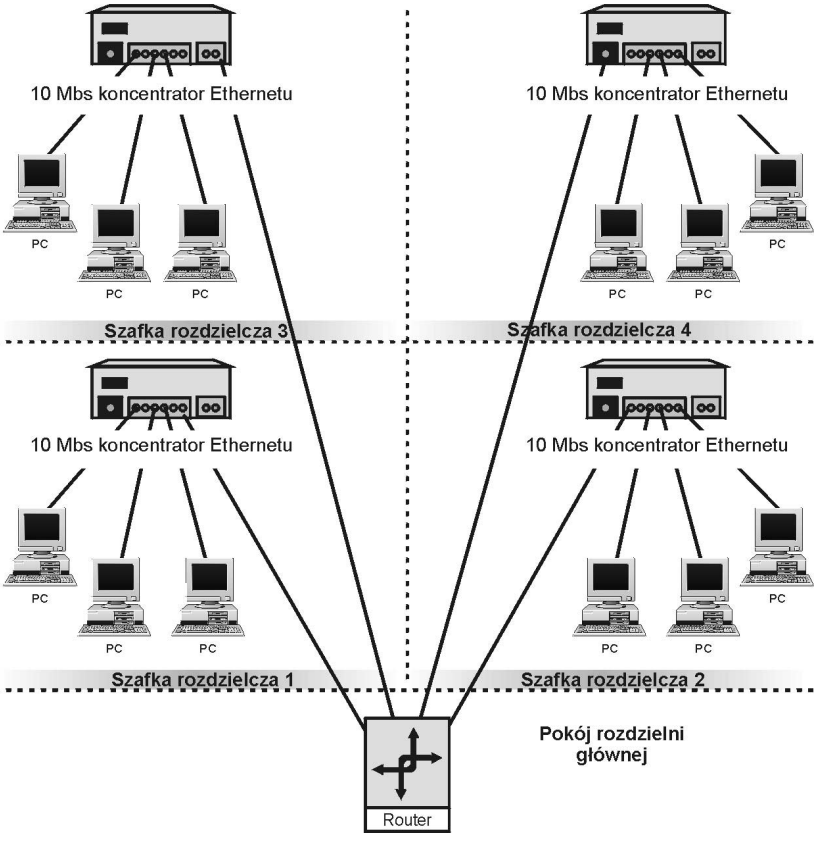
Szkielet segmentowy

Topologia szkieletu segmentowego oparta jest na centralnie umieszczonym routerze łączącym wszystkie segmenty sieci LAN w danym budynku. Router skutecznie tworzy wiele domen kolizji i rozgłaszania zwiększając w ten sposób wydajność każdego z segmentów sieci LAN. Routery działają na poziomie warstwy 3 modelu referencyjnego OSI.

Funkcjonują one wolniej od koncentratorów. W związku z tym mogą ograniczać efektywną wydajność każdej transmisji rozpoczynającej się w jednym i kończącej się w drugim segmencie sieci LAN.

Szkielety segmentowe, jak widać na rysunku 2.20 również wprowadzają pojedynczy punkt defektu sieci LAN. Nie jest to poważna wada. Wiele innych topologii również wprowadza pojedynczy punkt defektu do sieci LAN. Jest to natomiast niedomaganie, które trzeba brać pod uwagę podczas planowania topologii sieci.

Rysunek 2.20.
Szkielet segmentowy

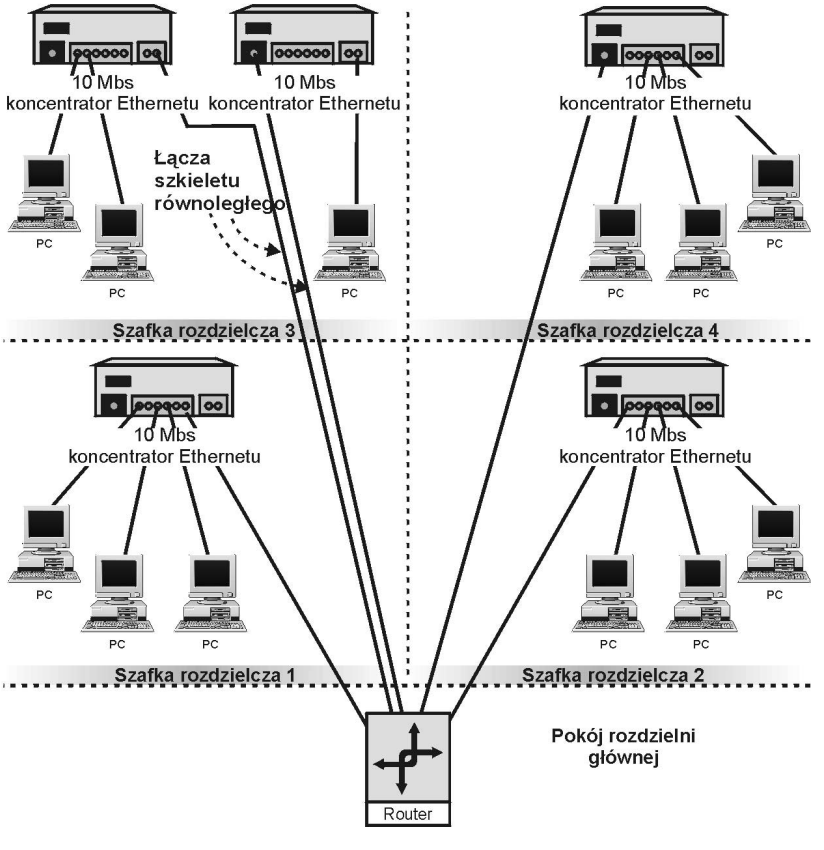


Ważnym aspektem topologii szkieletów segmentowych jest fakt, że użytkownicy rzadko kiedy zgrupowani są w określonych miejscach budynku. Raczej porozrzucani są w różnych, zwykle odległych jego miejscach. Oznacza to, że często znajdują się również po przeciwnych stronach routera szkieletu segmentowego sieci. W takiej sytuacji nawet proste zadania sieciowe wykonywane między uczestnikami jednej grupy roboczej będą często przechodzić przez jej router. W związku z tym podczas projektowania segmentowych szkieletów sieci LAN należy zwrócić szczególną uwagę na minimalizowanie natężenia ruchu przechodzącego przez takie routery i używać je jako agregatory ruchu dla zasobów poziomu LAN, takich jak urządzenia sieci WAN, lecz nie jako mostek.

Szkielet równoległy

W niektórych sytuacjach, w których szkielety segmentowe stanowią rozwiązanie niepożądane, ich zmodyfikowana wersja może okazać się idealna. Wersja ta nazywana jest szkieletem równoległym. Powodów, dla których warto utworzyć szkielet równoległy, jest wiele. Grupy użytkowników mogą być rozrzucone po całym budynku. Niektóre z nich oraz niektóre aplikacje mogą mieć wysokie wymagania odnośnie bezpieczeństwa sieciowego. Jednocześnie również potrzebny może być wysoki stopień dostępu do sieci. Niezależnie od przyczyny, poprowadzenie połączeń równoległych od routera szkieletu segmentowego do szafki rozdzielczej umożliwia obsługę z tej szafki wielu segmentów, co przedstawione jest na rysunku 2.21.

Rysunek 2.21. *Topologia szkieletu równoległego*



Topologia szkieletu równoległego jest modyfikacją szkieletu segmentowego. Zarówno sam pokój rozdzielni jak i pojedyncza szafka rozdzielcza mogą obsługiwać wiele segmentów. Powoduje to nieznaczne podniesienie kosztu utworzenia sieci, ale umożliwia zwiększenie wydajności każdego segmentu i zaspokaja zwiększone wymagania wobec sieci, takie jak wymogi bezpieczeństwa.

Dokładne zrozumienie potrzeb i wymagań klienta odnośnie każdego z obszarów funkcjonalnych sieci LAN jest kluczowe do utworzenia idealnej topologii. Potencjalne sposoby łączenia różnych składników sieci ogranicza jedynie wyobraźnia. Ciągłe innowacje

technologiczne będą stale zwiększać różnorodność topologiczną rozwiązań dostępnych dla projektantów sieci.

Wiele spośród technologii złożonych przedstawionych jest w niniejszym rozdziale wyłącznie w celu pogłębienia wiedzy praktycznej.. Wielu producentów używa i tak innych nazw na określenie tych technologii, więc zamiast koncentrować się na nazwach, lepiej skupić się na ich właściwościach (mocnych i słabych stronach) oraz na zasadach ich działania.

Podsumowanie

Ważnym aspektem sieci LAN jest sposób obsługi dostępu do nośnika. I choć jest on bardziej funkcją sieciowych systemów operacyjnych aniżeli sprzętu sieciowego, to wpływa bezpośrednio na przebieg ruchu i sprawność sieci LAN.

Również topologia LAN jest zależna bezpośrednio od skuteczności sieci LAN. Istnieją cztery podstawowe topologie, które można mieszać, dopasowywać, układać i łączyć na bardzo wiele różnych sposobów. Zrozumienie korzyści i ograniczeń topologii podstawowych, a także potrzeb i wymagań użytkowników, jest istotne przy wyborze tej, która najlepiej je zaspokaja.

Tematy zaprezentowane w niniejszym rozdziale powinny udowodnić, że sieć składa się z więcej niż tylko sprzętu i okablowania. Równie ważnymi jak składniki fizyczne elementami składowymi sieci są sposób zorganizowania owych składników fizycznych oraz sposób dostępu do urządzeń przyłączonych do sieci.