

## Topologia sieci

Topologia to sposób wykonania sieci na danym obszarze, czyli połączenia urządzeń komputerowych w jeden zbiór za pomocą medium transmisyjnego. W trakcie projektowania sieci trzeba wziąć pod uwagę kilka czynników, z których najważniejszymi są poniższe trzy:

- koszty instalacji okablowania, sprzętu sieciowego oraz kart sterujących
- elastyczność architektury sieciowej, która daje możliwość rekonfiguracji oraz wprowadzania dodatkowych węzłów sieci (urządzeń peryferyjnych, komputerów)
- niezawodność przeprowadzania zadań informatycznych, realizowanych w sieci, uzyskiwana przez redundancję komunikacji pomiędzy poszczególnymi węzłami sieci oraz dodatkowe węzły w sieci stosowane zależnie od rangi procesów informatycznych

Rozróżnia się dwa rodzaje topologii sieci komputerowych, zależnie od tego, czy chodzi o sieć lokalną (ang. **LAN**), czy sieć złożoną, czyli zbiory sieci lokalnych złączonych ze sobą przy pomocy routerów i mostów (ang. WAN, WLAN, MAN).

**WAN (ang. Wide Area Network)** - to rozległa sieć działająca w oparciu o połączenia telefoniczne, zbudowana z urządzeń znacznie oddalonych od siebie (np. sieć łącząca użytkowników poczty internetowej na danym obszarze). W przypadku sieci WAN niezbędny jest udział publicznej sieci teleinformatycznej, WAN łączy ze sobą sieci miejskie (MAN) oraz lokalne (LAN). Sieci rozległe łączą płaszczyznę informatyczną i telefoniczną. Rozwiązania zastosowane w przypadku tych sieci muszą gwarantować odpowiednią szybkość przesyłu danych, bezawaryjność łączy a także bezpieczeństwo transmitowanych informacji, dlatego sieci rozległe wymagają zastosowania urządzeń najnowszej generacji. Sieć WAN zakłada implementację takich procesów telekomunikacyjnych jak: przesyłanie danych komputerowych, dzielenie plików, konferencje wideo, przekazywanie połączeń do maszyn spoza sieci, do firmy, domu, samochodu oraz w inne miejsca. Połączenia w sieciach WAN realizuje się przy pomocy routerów, które mają za zadanie tworzenie pomostów pomiędzy różnymi, oddalonymi od siebie sieciami a także realizowanie połączeń z siecią Internet. Bezpieczeństwo routerów od strony sieci komputerowych nadzorowane jest przez procedury autoryzacyjne, które kontrolują dostęp użytkowników do routera. W sieciach WAN mogą być wykorzystane łącza: kablowe, satelitarne, mikrofalowe oraz światłowodowe.

**MAN (ang. Metropolitan Area Network)** - to sieci funkcjonujące w dużych metropoliach, charakteryzujące się dużą przepustowością, używane są głównie przez urządzenia badawcze a także do zastosowań komercyjnych o wysokim przepływie informacji. Sieci MAN zbudowane są z połączony w zróżnicowany sposób sieci lokalnych LAN.

**WLAN (ang. Wireless Local Area Network)** - to bezprzewodowa sieć, mająca zastosowanie w domach, biurach, czyli wszędzie tam, gdzie występuje potrzeba połączenia w sieć wielu urządzeń jak komputery, modemy czy drukarki, ale układ pomieszczeń utrudnia bądź uniemożliwia położenie klasycznego okablowania. Urządzenia działające bezprzewodowo eliminują stosowanie kabli, będąc przydatne szczególnie tam, gdzie estetyka pomieszczeń nie pozwala na zastosowanie okablowania. Sieć taka zapewnia komunikację przez podłogi, ściany i inne obiekty w promieniu kilkunastu do kilkudziesięciu metrów, umożliwiając jednocześnie wspólne użytkowanie takich urządzeń jak modemy czy drukarki. Drukarka podłączona do sieci bezprzewodowej może być używana przez dowolnego użytkownika podłączonego do sieci, bez względu na to, gdzie się aktualnie znajduje. Modem wpięty do sieci bezprzewodowej może łączyć do Internetu wielu użytkowników na raz bez względu na fakt, jak daleko znajdują się od gniazdka telefonicznego.

### Topologia gwiazdy (ang. Star)

To sieć, która zawiera jeden główny węzeł (serwer), gdzie przyłączona jest reszta elementów składowych sieci przy pomocy koncentratora. Taki układ jest odporny na awarię, gdyż awaria

pojedynczego łącza nie oznacza awarii całej sieci. Topologii gwiazdy używa się do łączenia urządzeń w obrębie jednego budynku, instytucji. Większa część zasobów sieci umiejscowiona jest w centralnym serwerze, który zarządza pracą sieci. Reszta urządzeń to terminale, które służą do wprowadzania danych i posiadają zwykle niewielką moc obliczeniową. Wszelkie dane są przetwarzane przez centralny serwer. Topologia gwiazdy może zostać określona jako drzewo z tylko jednym poziomem połączeniowym. Okablowanie wykorzystywane w tym rodzaju sieci to UDP oraz światłowody.

#### **Zalety topologii gwiazdy:**

- łatwa konserwacja oraz lokalizacja uszkodzeń
- prosta rekonfiguracja
- łatwe i szybkie oprogramowanie sieci
- centralne sterowanie oraz centralna diagnostyka sieci
- wysokie prędkości transmisji (pod warunkiem szybkiego komputera centralnego).

#### **Wady topologii gwiazdy:**

- duża ilość okablowania
- wszystkie maszyny muszą być podłączone do centralnego komputera
- ograniczona możliwość rozbudowywania sieci
- zależność funkcjonowania sieci od sprawności centralnego serwera
- ograniczenie odległości komputerów od koncentratora
- w momencie awarii koncentratora przestaje funkcjonować cała sieć.

#### **Topologia drzewa (ang. Tree)**

Jest to rodzaj okablowania, który przypomina swym kształtem mocno rozgałęzione drzewo. Jego gałęzie dzielą się na mniejsze elementy zwane podgałęziami, te z kolei dzielą się ponownie. W każdym miejscu podziału komputer rozsyła określone sygnały. Topologia drzewa jest mocno elastyczna i w pewnych systemach transportu sieciowego, może umożliwić praktycznie nieograniczone sposoby konfiguracji.

#### **Zalety topologii drzewa:**

- łatwe rozbudowywanie sieci komputerowych poprzez dodawanie rozgałęźników
- prostota rekonfiguracji sieci
- sieć zazwyczaj może przetrwać zniszczenie kabla bądź komputera

#### **Wady topologii drzewa:**

- spora ilość okablowania
- utrudniona lokalizacja błędów

#### **Topologia magistrali (ang. Bus)**

Topologię tą można traktować jak "autostradę", która służy przesyłaniu danych oraz łączy dane stacje sieci. Informacje, zanim dotrą do celu, przechodzą na swej drodze przez wszystkie inne stacje. W tym rozwiązaniu, do wspólnego kabla, którym przebiega transmisja podłączone zostają komputery, które dzielą dostęp do danego medium transmisyjnego. Każdy komputer przyłączony jest do kanału, przekazywane sygnały dochodzą do wszystkich stacji, lecz pakiety odbierane zostają tylko przez tę stację, do której zostały adresowane, gdyż każda stacja przeprowadza kontrolę, czy dane skierowane są właśnie do niej. Topologia ta stanowi jedną z najpopularniejszych modeli sieci komputerowych.

#### **Zalety topologii magistrali:**

- niewielkie zużycie kabla
- łatwa instalacja
- niewielka cena instalacji

- łatwa rozbudowa sieci
- proste łączenie segmentów danej sieci w spójny system (bez zmiany oprogramowania komunikacyjnego)
- każde urządzenie podłączony jest tylko jednym kablem
- pojedyncze uszkodzenie (awaria komputera bądź uszkodzenie kabla) nie spowoduje awarii całej sieci

#### **Wady topologii magistrali:**

- konkurencja dotycząca dostępu - wszystkie komputery skazane są na dzielenie się kablem
- utrudnione wykrywanie błędów z powodu nieobecności centralnego systemu do zarządzania siecią
- rozproszenie działań realizujących zarządzanie siecią, co w pewnych przypadkach może niekorzystnie wpłynąć na szybkość realizowania określonych zadań informatycznych
- przeważnie w celu uniknięcia zakłóceń sygnału należy zachować określoną odległość pomiędzy punktami przyłączenia danych stacji

#### **Topologia łańcucha priorytetów (ang. Priority)**

Istnieje pewne podobieństwo do układu pierścieniowego, lecz z przerywanym połączeniem pomiędzy jedną parą urządzeń. Każdy komputer podłączony jest do dwóch pozostałych, za wyjątkiem komputerów znajdujących się na końcu łańcucha. Możliwe jest powstanie sieci opartych o połączenie obu wymienionych wcześniej topologii np. gwiazda-magistrala, pierścień-drzewo. Topologia ta jest niezbyt popularna z powodu możliwości rozczłonkowania się sieci w razie awarii.

#### **Zalety topologii łańcucha priorytetów:**

- prostota okablowania
- niewielka ilość kabla

#### **Wady topologii łańcucha priorytetów:**

- uszkodzenie kabla bądź awaria komputera spowoduje podzielenie się sieci na dwa niezależne części

#### **Topologia pierścienia (ang. Ring)**

Topologia pierścieniowa posiada wiele zalet. Działanie sieci nie będzie przerwane nawet w przypadku awarii centralnego komputera, ponieważ jego zadania mogą zostać przejęte przez inną stację. Dzięki połączeniu obejściowemu (ang. bypass), wyłączona może zostać dowolna stacja w celu uniknięcia awarii sieci. Dowolny węzeł sieci włączony jest bezpośrednio w proces transmisji danych, będąc połączony jednocześnie z dwoma "sąsiadami". Węzły, które połączone są w pierścień, przesyłają komunikaty sterujące (tzw. tokeny) do następnych węzłów. Węzeł posiadający aktualnie token, może przesyłać komunikat. Używając terminu "token ring", bardzo często ma się na myśli standard IEEE 802.5 (ang. Institute of Electrical and Electronics Engineers), sieci token ring, będący najbardziej rozpowszechnionym typem sieci o charakterze token ring. Początkowy standard przewidywał transmisję z prędkością 4 Mb/s, natomiast obecne sieci osiągają prędkości rzędu 16 Mb/s. Dane wędrują w danym kierunku i po przekroczeniu wszystkich węzłów wracają do miejsca, skąd zostały nadane. Interfejs sieciowy w każdym komputerze musi odbierać informacje od pierwszego sąsiada, a następnie przesyłać je do kolejnego. W trakcie przechodzenia przez poszczególne węzły sieci, sygnał jest wzmacniany na każdym z nich.

#### **Zalety topologii pierścienia:**

- niewielkie zużycie okablowania
- możliwe zastosowanie łącz optoelektronicznych, wymagających bezpośredniego nadawania oraz odbierania transmitowanych danych

- możliwe do osiągnięcia wysokie osiągi, gdyż każdy kabel jest połączeniem dwóch konkretnych komputerów

#### *Wady topologii pierścienia:*

- uszkodzenie pojedynczego kabla bądź komputera spowoduje przerwanie działania całej sieci, jeżeli nie zainstalowano dodatkowego sprzętu
- skomplikowana diagnostyka sieci (usprawnienie może być zrealizowane poprzez wyposażenie węzłów w procedury samotestujące)
- utrudniona lokalizacja awarii
- trudna zmiana parametrów sieci
- wymagane są specjalne procedury do transmisji
- dołączenie dodatkowych stacji jest mocno utrudnione, jeżeli w pierścieniu znajduje się już duża ilość stacji

### **Sieci Peer to Peer**

Istnieje dużo definicji, czym naprawdę jest sieć P2P. Jednak do tej chwili nie udało się ustalić stałego jej pojęcia. Różne firmy kreują swoje definicje tego określenia. P2P jest architekturą sieciową, która wykorzystuje bezpośrednie komunikowanie się osób (ang. Person to Person). Dokładniejszą definicję tego pojęcia zaproponowała firma Intel: Peer to peer to współdzielenie usług oraz zasobów komputerowych poprzez bezpośrednią wymianę. Architektura sieci P2P różni się zasadniczo od architektury klient-serwer (która do tej pory dominowała w świecie internetowej transmisji danych) tym, że nie potrzebuje serwera, a w samej komunikacji udział biorą dwie bądź więcej samodzielnych jednostek, najczęściej będącymi komputerami PC.

Współczesne sieci P2P wykorzystuje się głównie do poszukiwania oraz wymiany plików między użytkownikami, którzy korzystają ze stworzonych w tym celu programów jak: WinMX, Direct Connect, Blubster, iMesh, Filenavigator, Edonkey, eMule, KaZaA, Bit Torrent. Jednym z pionierów sieci P2P była aplikacja o nazwie Napster, wykorzystująca centralny serwer, gdzie gromadzone były informacje na temat zbiorów udostępnianych przez wszystkich użytkowników. Dotychczasowo wszelkie programy działające w sieci P2P używają jednego protokołu, którym jest Gnutella. Jest to najbardziej przyjazny użytkownikowi protokół, ponieważ nie kontroluje go żadna konkretna firma, oraz dodatkowo nie ma on zaimplementowanych ograniczeń, które uniemożliwiłyby ściąganie np. pirackiej muzyki, filmów czy gier. W nowoczesnych sieciach porzucono strukturę scentralizowaną, dążąc do uniezależnienia się od wszelkich punktów centralnych, które mogłyby spowodować unieruchomienie sieci. Jedną z pierwszych sieci rozproszonych była Gnutella, działająca w oparciu o protokół o takiej samej nazwie. Ta sieć nie ma żadnych wyróżnionych punktów. Możliwym jest transfer plików dowolnej wielkości i typu. Sieć ta nie posiada centralnego serwera, więc wszystkie maszyny są zarazem klientami i serwerami. Niemożliwym więc staje się zlikwidowanie jednego serwera wyłączając przez to całą sieć. Brak centralnych serwerów spowodowało jednak znaczne obniżenie prędkości wyszukiwania.

#### *Schemat sieci Gnutella:*

Komputer przesyła zapytanie do komputerów znajdujących się najbliżej w sieci. Następnie komputery te przekazują zapytanie dalej, pomniejszając parametr TTL (ang. Time To Live) danego zapytania. Kiedy TTL spadnie do zera, zapytanie przestaje być wysyłane dalej.

Komputery, dysponujące poszukiwanym plikiem, udzielają odpowiedzi na zapytanie.

Po wybraniu jednej z kilku odpowiedzi, zostaje nawiązane bezpośrednie połączenie z komputerem, który jest jej nadawcą, a następnie pobierany jest dany plik (przy pomocy protokołu HTTP oraz Gnutella).

W celu zredukowania czasu potrzebnego na przeszukanie sieci oraz zwiększenia możliwości przeszukiwania, zdecydowano się w innych aplikacjach na rozwiązanie pośrednie: utworzono sieć, która oparta jest na niezależnych, pośredniczących serwerach, które mogą być zakładane przez dowolnych użytkowników sieci i pełnią zadanie punktów informacyjnych. Znajdują się w nich listy udostępnianych plików oraz adresy komputerów użytkowników, którzy podłączają się do określonego serwera. Taki sposób przyspiesza oraz zwiększa możliwości wyszukiwania zasobów (sposób ten zastosowany został pierwszy raz w sieci eDonkey).

### *Schemat sieci eDonkey:*

Sieci eDonkey wykorzystują do działania protokół MFTP (ang. Multisource File Transfer Protocol). Sieć tworzona jest przez dwa rodzaje oprogramowania: serwery oraz klienty. Po uruchomieniu aplikacji, klienckiej, następuje połączenie z określonym serwerem, zawierającym informacje na temat danych udostępnianych przez użytkowników. W chwili otrzymania zapytania, komputer centralny przeszukuje spis dostępnych plików, odsyłając do komputera pytającego odpowiedź, kto jest w posiadaniu poszukiwanych danych. Możliwe jest również skorzystanie z wyszukiwania rozszerzonego, gdzie zapytanie zostaje rozesłane do wielu serwerów, z którymi nie mamy bezpośredniego połączenia.

### *Hashowanie*

W przypadku wielu sieci P2P zdarza się pobranie pliku o zawartości, która nie odpowiada nazwie. Autorzy programów P2P stworzyli technologię zapobiegającą takim zdarzeniom. W eDonkey'u używana jest technika zwaną hashowaniem, która polega na stworzeniu sumy kontrolnej w oparciu o zawartość pliku. Liczba ta zostaje wygenerowana w wyniku zastosowania skomplikowanych algorytmów i jeżeli w pliku zostałby zmieniony zaledwie jeden bajt, suma kontrolna zmieni swą wartość.

Takie rozwiązanie pozwala na doskonałe poszukiwanie błędów w plikach. Pobierany jest plik oraz jego suma kontrolna, następnie tworzona jest ona z pliku, który znajduje się na dysku twardym. Jeżeli wartości sum kontrolnych są różne, oznacza to, że plik uległ uszkodzeniu. Dzięki tej technologii eDonkey sprawdza też w bardzo prosty sposób, czy dwóch użytkowników udostępniła rzeczywiście ten sam zbiór.

Hashowanie stwarza również inne możliwości. Wykorzystywane jest w technice zwanej ICH (ang. Intelligent Corruption Handling - co przetłumaczyć można jako: "inteligentne rozwiązywanie problemów z transmisją"). Rozwiązanie to umożliwia zmniejszenie ilości informacji, które muszą zostać ponownie skopiowane w sytuacji wystąpienia błędów w transmisji. Zwykle, jeżeli plik jest uszkodzony, należy go pobrać od nowa. Jednak w większości przypadków niepoprawnych jest zaledwie kilka bajtów. Oprogramowanie wykorzystujące ICH, plik pobierany jest ponownie bajt po bajcie. Na nowo skopiowane dane dodawane są do pliku, po czym następuje ponowne wyliczenie sumy kontrolnej - do momentu, aż okaże się, iż plik został naprawiony. Naturalnie może okazać się, iż błąd wystąpił na samym końcu zbioru, wtedy koniecznym staje się ponowne pobranie całości. Lecz często uszkodzenia występują wcześniej i w takich sytuacjach technika ICH znacznie skraca czas, który potrzebny jest na naprawienie pliku.

### *Wznawianie połączeń.*

Technika wznowiania przerywanych pobrań (ang. resumimg) znana jest już od dłuższego czasu. Niektóre aplikacje P2P stosują ją, aby pobrać plik od wielu osób w tym samym czasie. Technika ta funkcjonuje w następujący sposób:

- najpierw pliki sprawdzane są przy pomocy metody hashowania pod względem identyczności
- następnie udostępniony plik jest dzielony na części o określonym przez sieć rozmiarze
- każda część może być pobrana z wielu komputerów, przez co pobieranie pliku ulega przyspieszeniu

Wykorzystując technologie podziału pliku na części podczas jego pobierania sprawia, iż informacje szybciej się rozchodzą się po sieci. Przykładowo: użytkownik A posiada wszystkie części pliku. Użytkownicy oznaczeni literami K, L i M chcą ściągnąć ten plik. Jeżeli L oraz M dysponują już pewnymi częściami pobieranego pliku, to mogą skopiować je tak samo od użytkownika A, jak również od siebie wzajemnie.