

## Moduł 2: Podstawy działania sieci komputerowych Wprowadzenie

Szerokość pasma ma zasadnicze znaczenie dla działania sieci komputerowej. Decyzje dotyczące szerokości pasma są jednymi z najważniejszych, które trzeba podjąć podczas projektowania sieci. W niniejszym module omówiono znaczenie szerokości pasma, wyjaśniono sposoby jego obliczania oraz pomiaru.

Funkcje sieci są opisywane przy użyciu modeli warstwowych. W module 2 omówiono dwa najważniejsze modele, tj. model OSI (ang. *Open System Interconnection*) i model TCP/IP (ang. *Transmission Control Protocol/Internet Protocol*).

Przedstawiono także różnice i podobieństwa między nimi.

### 2.1 Terminologia sieciowa

#### 2.1.1 Sieci danych

Rozwój sieci danych zawdzięczamy faktowi stosowania na mikrokomputerach aplikacji biznesowych. Z początku, mikrokomputery nie były ze sobą połączone, podobnie jak terminale komputerów klasy mainframe, nie istniała więc wygodna metoda wymiany danych między wieloma mikrokomputerami. Stało się oczywiste, że przenoszenie danych przy użyciu dyskietek (stosowanie sieci Sneakernet) nie jest ani na tyle wydajne, ani oszczędne, aby nadawało się do zastosowań w biznesie. Taki sposób przenoszenia danych sprawiał, że były one przechowywane w wielu kopiach. Każda modyfikacja pliku pociągała za sobą konieczność jego ponownego rozpowszechnienia wśród pracowników, którym był potrzebny. W przypadku jednoczesnego zmodyfikowania pliku przez dwie osoby próba rozpowszechnienia zmian mogła powodować utratę jednego zbioru modyfikacji. Przedsiębiorstwa potrzebowały dobrego rozwiązania trzech następujących problemów:

Jak uniknąć powielania urządzeń i zasobów? Jak wydajnie się komunikować? Jak zbudować sieć i zarządzać nią? Zorientowano się, że technika sieciowa może zwiększyć wydajność przy jednoczesnym obniżeniu kosztów. Prędkość wdrażania i upowszechniania się sieci zaczęła dorównywać tempu wprowadzania nowych technologii i produktów sieciowych na rynek. We wczesnych latach 80. XX w. nastąpiło masowe upowszechnienie sieci komputerowych, pomimo tego, że początkowo ich rozwój nie był zorganizowany.

W połowie lat 80. pojawiające się technologie sieciowe były tworzone na bazie różnego sprzętu i oprogramowania. Każda firma produkująca urządzenia i oprogramowanie sieciowe stosowała własne standardy. Tworzenie indywidualnych standardów wynikało z panującej na rynku konkurencji. W wyniku tego wiele technologii sieciowych było ze sobą niezgodnych. Wzajemna komunikacja sieci opartych na różnych specyfikacjach stawała się coraz trudniejsza. Wdrożenie nowego sprzętu często powodowało konieczność wymiany starych urządzeń sieciowych.

Jednym z wczesnych rozwiązań tych problemów było utworzenie standardów sieci lokalnych LAN. Ze względu na to, że standardy LAN zawierały otwarty zbiór wytycznych dotyczących projektowania sprzętu i oprogramowania sieciowego, urządzenia produkowane przez różne firmy mogły stawać się zgodne z systemami konkurencji. Pozwoliło to na ustabilizowanie się implementacji sieci LAN.

W systemie LAN każdy dział firmy jest rodzajem elektronicznej wyspy. Wraz ze wzrostem znaczenia komputerów dla przedsiębiorstw stało się jasne, że sieci LAN nie są rozwiązaniem wystarczającym.

Pojawiła się potrzeba opracowania sposobu szybkiej i wydajnej wymiany informacji nie tylko w ramach jednej firmy, ale także między przedsiębiorstwami. Rozwiązaniem stało się utworzenie sieci miejskich MAN (ang. *metropolitan-area network*) i sieci rozległych WAN (ang. *wide-area network*). Ponieważ sieci WAN pozwalały na łączenie użytkowników rozproszonych na dużych obszarach geograficznych, możliwa stała się wzajemna komunikacja na wielkie odległości.

#### 2.1.2 Historia sieci komputerowych

Historia sieci komputerowych jest złożona. W rozwój sieci w ciągu ostatnich 35 lat było zaangażowanych wielu ludzi z całego świata. W tym miejscu przedstawiono skrócony opis rozwoju Internetu. Procesy tworzenia nowych rozwiązań i ich wprowadzania na rynek są daleko bardziej skomplikowane, ale spojrzenie na podstawy rozwoju jest bardzo pomocne.

W latach 40. XX w. komputery były łatwo psującymi się, ogromnymi urządzeniami elektromechanicznymi. Wynalezienie w 1947 roku tranzystora półprzewodnikowego otworzyło wiele możliwości budowania mniejszych i bardziej niezawodnych komputerów. W latach pięćdziesiątych komputery klasy mainframe, które wykonywały programy zapisane na kartach perforowanych, zaczęły być wykorzystywane przez duże instytucje. W późnych latach pięćdziesiątych wynaleziono układ scalony, który składał się z kilku, później wielu, a obecnie z milionów tranzystorów umieszczonych na małym kawałku półprzewodnika. W latach 60. komputery mainframe z terminalami nie były niczym niezwykłym i upowszechniły się układy scalone. W późnych latach 60. i w trakcie następnej dekady powstały mniejsze komputery nazywane minikomputerami.

Jednak nawet tamte minikomputery były ogromne według współczesnych standardów. W roku 1977 firma Apple Computer Company przedstawiła mikrokomputer nazywany także komputerem osobistym. W roku 1981 firma IBM zaprezentowała swój pierwszy komputer osobisty. Przyjazny użytkownikowi komputer Mac, otwarta architektura komputera IBM PC i dalsza miniaturyzacja układów scalonych doprowadziły do rozpowszechnienia się komputerów osobistych w domu i w biznesie. W połowie lat 80. XX w. użytkownicy autonomicznych komputerów zaczęli wykorzystywać modemy do łączenia się z innymi komputerami i wymiany plików. Nazywano to komunikacją punkt-punkt lub komunikacją komutowaną (dial-up). Pomysł ten rozwinęto, wykorzystując komputery jako centralne punkty komunikacji w połączeniach komutowanych. Komputery te nazywano biuletynami BBS (ang. *bulletin boards*). Użytkownicy mogli połączyć się z biuletynem BBS i pozostawić tam lub pobrać stamtąd wiadomości bądź pliki. Wadą takiego systemu było to, że komunikacja bezpośrednia była ograniczona i dotyczyła tylko tych, którzy wiedzieli o danym biuletynie BBS. Inne ograniczenie stanowił fakt, że komputer BBS wymagał jednego modemu do każdego połączenia. Tak więc jednoczesne połączenie pięciu użytkowników wymagało pięciu modemów podłączonych do pięciu odrębnych linii telefonicznych. Wraz ze wzrostem liczby osób chcących korzystać z systemu obsłużenie wszystkich zgłoszeń stawało się niemożliwe. Wystarczy wyobrazić sobie sytuację, w której 500 osób chce połączyć się w tej samej chwili. W latach 60. XX w. Departament Obrony USA rozpoczął

tworzenie dużych i niezawodnych sieci WAN do celów wojskowych i naukowych. Ich rozwój był kontynuowany przez trzy następne dekady. Ta technologia różniła się od komunikacji punkt-punkt wykorzystywanej w biuletynach BBS.

Umożliwiała wspólne połączenie wielu komputerów przy użyciu różnych ścieżek. Sposób przenoszenia danych między komputerami był określany przez sieć. Wprowadzono możliwość komunikacji między wieloma komputerami przy użyciu tego samego połączenia, podczas gdy wcześniej możliwa była komunikacja z zaledwie jednym komputerem w danej chwili. Sieć WAN Departamentu Obrony USA ostatecznie przekształciła się w Internet.

### 2.1.3 Urządzenia sieciowe

Urządzenia przyłączane bezpośrednio do segmentu sieci dzielą się na dwie klasy. Pierwszą klasę stanowią urządzenia końcowe. Są to komputery, drukarki, skanery i inne urządzenia, które wykonują usługi bezpośrednio dla użytkownika. Drugą klasę stanowią urządzenia sieciowe. Są to wszystkie urządzenia, które łączą urządzenia końcowe, umożliwiając komunikację między nimi.

Urządzenia końcowe, które umożliwiają użytkownikom połączenie z siecią, są również nazywane hostami. Urządzenia takie pozwalają użytkownikom na współdzielenie, tworzenie i uzyskiwanie informacji. Hosty mogą istnieć bez sieci, ale wtedy ich możliwości są znacznie ograniczone. Hosty są fizycznie przyłączone do mediów sieciowych przy użyciu karty sieciowej. Połączenie to jest wykorzystywane do wykonywania takich zadań, jak wysyłanie poczty elektronicznej, drukowanie dokumentów, skanowanie obrazów i uzyskiwanie dostępu do bazy danych. Karta sieciowa może mieć postać płytki z obwodem drukowanym, który pasuje do złącza rozszerzeń na magistrali płyty głównej komputera, może także występować w postaci urządzenia peryferyjnego. Inna nazwa karty sieciowej to adapter sieciowy. Karty sieciowe komputerów przenośnych mają zwykle rozmiar karty PCMCIA. Do każdej karty sieciowej jest przypisany unikatowy kod nazywany adresem MAC. Jest on używany do sterowania komunikacją hosta w sieci. Więcej informacji o adresie MAC zostanie przedstawionych później. Jak sama nazwa wskazuje, karta sieciowa steruje dostępem hosta do medium.

W przemyśle sieciowym nie zostały ustalone zestandaryzowane oznaczenia **urządzeń końcowych**. Przypominają one kształtem rzeczywiste urządzenia, aby można je było szybko rozpoznać.

**Urządzenia sieciowe** zapewniają transmisję danych przeznaczonych do przesłania między urządzeniami końcowymi. Urządzenia sieciowe umożliwiają rozszerzenie skali możliwych połączeń kablowych, koncentrację połączeń, konwersję formatu danych i zarządzanie przesyłem informacji. Przykładami urządzeń spełniających takie funkcje są: wtórniki, koncentratory, mosty, przełączniki i routery.

Wszystkie wymienione urządzenia sieciowe będą szczegółowo opisane w dalszej części kursu. W tym miejscu zostaną one omówione w skrócie.

Wtórnik jest urządzeniem sieciowym używanym do regenerowania sygnału. Wtórniki regenerują sygnał analogowy lub cyfrowy zniekształcony przez straty transmisji powstałe w wyniku tłumienia. Wtórnik nie podejmuje decyzji odnośnie przekazywania pakietów, jak router lub most.

Koncentratory służą do koncentrowania połączeń. Innymi słowy, dzięki nim grupa hostów jest postrzegana od strony sieci jako pojedyncza jednostka. Koncentracja jest wykonywana pasywnie i nie ma żadnego innego wpływu na transmisję danych. Koncentratory aktywne nie tylko koncentrują hosty, lecz także regenerują sygnał. Mosty przekształcają formaty sieciowej transmisji danych oraz realizują podstawowe funkcje zarządzania nią. Mosty, jak sugeruje nazwa, stanowią połączenie między sieciami LAN. Nie tylko łączą one sieci LAN, ale także sprawdzają dane w celu określenia, czy powinny one zostać przesłane na drugą stronę mostu, czy też nie. Dzięki temu poszczególne części sieci funkcjonują wydajniej.

Przełączniki grup roboczych wykonują bardziej zaawansowane funkcje zarządzania przesyłaniem danych. Nie tylko określają, czy informacje powinny pozostać w danej sieci LAN, czy nie, ale także mogą przesłać dane tylko do tego połączenia, w którym są one potrzebne. Inną różnicę między mostem a przełącznikiem stanowi fakt, że przełącznik nie przekształca formatów transmisji danych.

Routery dysponują wszystkimi wymienionymi wcześniej możliwościami. Mogą one regenerować sygnały, koncentrować wiele połączeń, przekształcać formaty transmisji danych i zarządzać transferem danych. Umożliwiają również połączenie z siecią WAN, co pozwala na łączenie znacznie od siebie oddalonych sieci lokalnych. Żadne z pozostałych urządzeń nie zapewnia takiego połączenia.

Urządzenia końcowe	
Komputer PC 	Drukarka 
Apple Macintosh 	Serwer plików 
Komputer przenośny 	Komputer mainframe 
Urządzenia sieciowe	
Wtórnik 	Most 
Koncentrator 10BASE-T 	Przełącznik grupy roboczej 
Koncentrator (100BASE-T Hub) 	Router 
Koncentrator 	Chmura obrazująca sieć 

## 2.1.4 Topologia sieci

Topologia sieci określa jej strukturę. Jedną częścią definicji topologii jest topologia fizyczna, która stanowi rzeczywisty układ przewodów lub medium transmisyjnego. Drugą częścią jest topologia logiczna, która określa sposób dostępu hosta do medium w celu wysłania danych. Powszechnie stosowane są następujące odmiany topologii fizycznej:

**Topologia magistrali**, w której wykorzystywany jest pojedynczy kabel szkieletowy na obu końcach wyposażony w terminatory. Wszystkie hosty są podłączone bezpośrednio do tego szkieletu.

**Topologia pierścienia**, w której każdy host jest podłączony do następnego, a ostatni host jest podłączony do pierwszego. W ten sposób tworzony jest pierścień okablowania.

**Topologia gwiazdy**, w której wszystkie kable łączą się w jednym punkcie centralnym.

**Topologia gwiazdy rozszerzonej**, w której pojedyncze gwiazdy są powiązane poprzez połączenie koncentratorów lub przełączników. Ta topologia umożliwia rozszerzenie zasięgu i obszaru sieci.

**Topologia hierarchiczna** jest podobna do rozszerzonej gwiazdy. Jednak zamiast łączyć razem koncentratory lub przełączniki, system jest podłączony do komputera, który steruje ruchem w tej topologii.

**Topologia siatki** w możliwie największym stopniu zabezpiecza przed przerwami w dostępie do usług. Świetnym przykładem może być zastosowanie topologii siatki w sieciowym systemie sterowania elektrownią atomową. Jak widać na rysunku, każdy host dysponuje połączeniami z wszystkimi innymi hostami. Chociaż w Internecie istnieje wiele ścieżek do każdego miejsca, nie mamy w nim do czynienia z pełną topologią siatki.

**Topologia logiczna** sieci to sposób, w jaki hosty komunikują się ze sobą za pośrednictwem medium. Dwie najpowszechniejsze topologie logiczne to rozgłaszanie i przekazywanie tokenu.

**Topologia rozgłaszania** oznacza po prostu, że każdy host wysyła przekazywane dane do wszystkich hostów podłączonych do medium sieciowego. Nie ma określonej kolejności korzystania z sieci przez poszczególne stacje. Host, który jako pierwszy wyśle dane, jest obsługiwany jako pierwszy (ang. *first come, first serve*). W ten sposób działa sieć Ethernet, co zostanie omówione w dalszej części kursu.

Drugą odmianą topologii logicznej jest przekazywanie tokenu. W tej topologii dostęp do sieci jest kontrolowany przez przekazywanie elektronicznego tokenu kolejno do każdego hosta. Gdy host odbierze token, może wysyłać dane przez sieć. Jeśli nie ma danych do wysłania, przekazuje token do następnego hosta i proces się powtarza. Przykładami sieci, w których jest wykorzystywane przekazywanie tokenu, są Token Ring i FDDI. Odmianą sieci Token Ring i FDDI jest sieć Arcnet. W sieci Arcnet token jest przekazywany w ramach topologii magistrali.

Diagram na rysunku przedstawia wiele różnych topologii w połączeniu z urządzeniami sieciowymi. Prezentuje on typową dla szkoły lub małej firmy sieć o średnim stopniu złożoności. Znajduje się na nim wiele symboli i wiele rozwiązań sieciowych, których poznanie będzie wymagało czasu.

## 2.1.5 Protokoły sieciowe

Zestawy protokołów są to zbiory protokołów, które umożliwiają sieciową komunikację między hostami. Protokół jest formalnym opisem zestawu reguł i konwencji regulujących szczególny aspekt komunikacji między urządzeniami w sieci. Protokoły określają format informacji, zależności czasowe, kolejność transmisji i sposób wykrywania oraz reagowania na błędy występujące podczas komunikacji. Bez znajomości protokołów komputer nie mógłby przywrócić początkowej postaci strumienia bitów przychodzących z innego komputera.

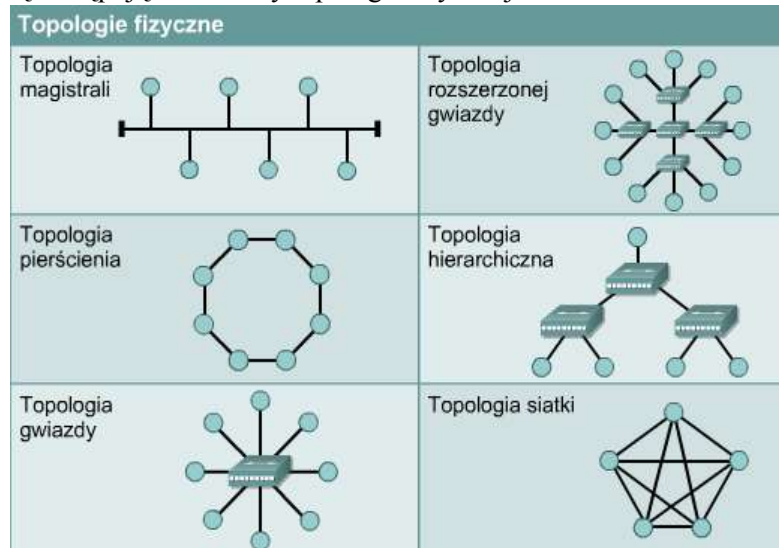
Protokoły regulują wszystkie aspekty komunikacji danych. Należą do nich:

- budowa sieci fizycznej,
- sposoby łączenia komputerów z siecią,
- sposoby formatowania danych do transmisji,
- sposoby wysyłania danych,
- sposoby obsługi błędów.

Reguły funkcjonowania sieci są opracowywane i nadzorowane przez wiele różnych organizacji i komitetów. Należą do nich: Institute of Electrical and Electronic Engineers (IEEE), American National Standards Institute (ANSI), Telecommunications Industry Association (TIA), Electronic Industries Alliance (EIA) i International Telecommunications Union (ITU), dawniej znana pod nazwą Comité Consultatif International Téléphonique et Télégraphique (CCITT).

**2.1.6 Sieci LAN** składają się z następujących elementów:

- komputery,
- urządzenia peryferyjne,
- urządzenia sieciowe,
- karty sieciowe,
- media sieciowe,



Sieci LAN umożliwiają efektywne wykorzystanie technologii komputerowych w biznesie do lokalnego współdzielenia plików i zapewnienia wewnętrznej komunikacji. Dobrym przykładem takiego rozwiązania jest poczta elektroniczna. Sieci LAN wiążą razem dane, lokalną komunikację i urządzenia komputerowe. Najpowszechniej stosowanymi technologiami sieci LAN są:

Ethernet                      Token  
RingFDDI

### 2.1.7 Sieci WAN

Sieci WAN łączą sieci LAN, co umożliwia dostęp do komputerów lub serwerów plików znajdujących się w innych miejscach. Ze względu na to, że sieci WAN łączą sieci na dużych obszarach geograficznych, umożliwiają komunikację między firmami na duże odległości. Sieci WAN umożliwiają współdzielenie komputerów, drukarek i innych urządzeń znajdujących się w sieci LAN z maszynami znajdującymi się w odległych miejscach. Pozwalają one na szybką komunikację na dużych obszarach geograficznych.

Oprogramowanie do pracy zespołowej umożliwia dostęp do informacji i zasobów w czasie rzeczywistym, co pozwala na zdalne uczestnictwo w spotkaniach, które wcześniej wymagały fizycznej obecności uczestników. Sieci rozległe spowodowały powstanie nowej klasy pracowników zwanych telepracownikami, którzy nie muszą wychodzić z domu, aby wykonywać swoją pracę.

Zadania sieci WAN prezentują się następująco:

- działanie na dużych, odległych geograficznie obszarach;
- umożliwienie użytkownikom komunikacji w czasie rzeczywistym;
- udostępnienie stałego połączenia zdalnych zasobów i lokalnych usług; dostęp do poczty elektronicznej, sieci WWW, usług przesyłania plików i handlu elektronicznego.

Najpowszechniej stosowanymi technologiami WAN są:

- sieci komutowane
- sieci ISDN (ang. *Integrated Services Digital Network*)
- linie DSL (ang. *Digital Subscriber Line*)
- sieci Frame Relay
- sieci Carrier Series w USA (T) i w Europie (E): sieci T1, E1, T3 i E3
- sieci SONET (ang. *Synchronous Optical Network*)

### 2.1.8 Sieci MAN

Sieć MAN obejmuje swoim zasięgiem obszar miejski, taki jak centrum miasta lub przedmieście. Sieć MAN zwykle składa się z dwóch lub więcej sieci LAN znajdujących się na wspólnym obszarze geograficznym. Sieć MAN może być na przykład wykorzystywana przez bank mający kilka oddziałów. Zwykle dostawca usług łączy dwie lub więcej sieci LAN przy użyciu własnych linii komunikacyjnych lub usług światłowodowych. Sieć MAN można także utworzyć przy użyciu bezprzewodowych mostów, przesyłając sygnały przez obszary publiczne.

### 2.1.9 Sieci SAN

Sieć SAN jest wydzieloną, wysoko wydajną siecią używaną do przenoszenia danych między serwerami i zasobami służącymi do przechowywania informacji. Ponieważ jest to odrębna, wydzielona sieć, nie występują w jej przypadku kolizje w ruchu między serwerami i klientami.

Technika SAN umożliwia szybką łączność serwer-pamięć, pamięć-pamięć i serwer-serwer. Metoda ta polega na wykorzystaniu odrębnej infrastruktury sieci, co wyklucza problemy związane z łącznością w istniejącej sieci. Sieci SAN mają następujące cechy:

**Wydajność:** Sieci SAN umożliwiają współbieżny szybki dostęp dwóch lub więcej serwerów do macierzy dyskowych lub taśmowych, zapewniając większą wydajność systemu.

**Dostępność:** Sieci SAN mają wbudowaną odporność na awarie, ponieważ pozwalają na utworzenie lustrzanej kopii danych przy użyciu sieci SAN w odległości do 10 km.

#### Sieci LAN:

- Działają na ograniczonym obszarze geograficznym.
- Umożliwiają jednoczesny dostęp wielu urządzeń do medium o dużej szerokości pasma.
- Pozwalają na lokalne administrowanie siecią.
- Zapewniają stały dostęp do lokalnych usług.
- Zapewniają połączenie fizycznie sąsiadujących urządzeń.

#### Wykorzystanie:



#### Sieci WAN:

- Działają na dużych obszarach geograficznych.
- Umożliwiają dostęp przez relatywnie wolne interfejsy szeregowo.
- Zapewniają łączność w pełnym lub ograniczonym wymiarze czasowym.
- Łączą urządzenia znacznie od siebie oddalone, które mogą się znajdować w różnych częściach globu.

#### Wykorzystanie:



**Skalowalność:** Jak w przypadku sieci LAN i WAN, tak i tu można korzystać z różnych technologii sieciowych. Pozwala to na łatwe przenoszenie kopii zapasowych i plików, realizowanie różnych operacji i replikację danych między systemami.

### 2.1.10 Sieć VPN

Sieć VPN to prywatna sieć utworzona w ramach infrastruktury sieci publicznej, takiej jak światowa sieć Internet. Przy użyciu sieci VPN telepracownik może za pośrednictwem Internetu uzyskać dostęp do sieci komputerowej znajdującej się w centrali firmy, tworząc zabezpieczony tunel między własnym komputerem a routerem VPN w siedzibie firmy

### 2.1.11 Zalety sieci VPN

Produkty firmy Cisco obsługują najnowsze rozwiązania z zakresu technologii VPN. Sieć VPN jest usługą, która zapewnia bezpieczną i niezawodną komunikację poprzez wspólną sieć publiczną, taką jak Internet. Reguły zabezpieczeń i zarządzania w sieciach VPN są takie same jak w sieci prywatnej. Sieci te są najbardziej wydajną metodą nawiązywania połączeń punkt-punkt między zdalnymi użytkownikami i siecią klienta firmy.

Wyróżnia się trzy główne typy sieci VPN:

**Dostępowe sieci VPN:** Dostępowe sieci VPN zapewniają łączność zdalnych pracowników i małych biur z centralą intranetu lub ekstranetu za pośrednictwem wspólnej infrastruktury. W przypadku dostępowych sieci VPN do bezpiecznej komunikacji przemieszczających się pracowników, telepracowników i biur terenowych używane są techniki analogowe, komutowane, ISDN, DSL, mobile IP i kablowe.

**Intranetowe sieci VPN:** Intranetowe sieci VPN łączą regionalne i zdalne biura z centralą sieci wewnętrznej za pośrednictwem wspólnej infrastruktury korzystającej z dedykowanych połączeń. Intranetowe sieci VPN różnią się od ekstranetowych sieci VPN tym, że umożliwiają dostęp tylko pracownikom danej firmy.

**Ekstranetowe sieci VPN:** Ekstranetowe sieci VPN łączą partnerów firmy z centralą sieci za pośrednictwem wspólnej infrastruktury korzystającej z dedykowanych połączeń. Ekstranetowe sieci VPN różnią się od intranetowych sieci VPN tym, że umożliwiają dostęp użytkownikom spoza firmy

### 2.1.12 Intranety i ekstranety

Jedną z powszechnie stosowanych konfiguracji sieci LAN jest Intranet. Intranetowe serwery WWW różnią się tym od publicznych serwerów WWW, że aby uzyskać dostęp z zewnątrz do Intranetu danej organizacji trzeba mieć odpowiednie uprawnienia i hasła. Intranety są projektowane w taki sposób, aby umożliwiałały dostęp tym użytkownikom, którzy mają uprawnienia dostępu do wewnętrznej sieci LAN firmy. W intranecie są instalowane serwery WWW. Przeglądarki są wykorzystywane jako wspólny mechanizm dostępu (fronton) do informacji przechowywanych na tych serwerach, takich jak dane lub wykresy finansowe bądź dane tekstowe.

Terminem „ekstranet” określa się aplikacje i usługi oparte na intranecie i korzystające z rozszerzonego, zabezpieczonego dostępu do zewnętrznych użytkowników lub firm. Dostęp ten zwykle uzyskuje się przy użyciu haseł, identyfikatorów i innych zabezpieczeń na poziomie aplikacji. Tak więc ekstranet jest rozszerzeniem dwóch lub kilku intranetów z zapewnieniem bezpiecznej interakcji między współpracującymi firmami i ich intranetami

## 2.2 Przepustowość

### 2.2.1 Znaczenie szerokości pasma

Szerokość pasma jest zdefiniowana jako ilość informacji, które można przesłać siecią w określonym czasie. Zrozumienie istoty szerokości pasma podczas poznawania zagadnień sieciowych jest bardzo ważne z następujących powodów:

**Szerokość pasma jest skończona.** Innymi słowy, niezależnie od medium użytego do budowy sieci ilość informacji przenoszonych przez tę sieć jest ograniczona. Szerokość pasma jest ograniczona prawami fizyki i technologiami umieszczania informacji w medium. Szerokość pasma zwykłego modemu jest na przykład ograniczona do około 56 kb/s przez fizyczne właściwości skłębki telefonicznej i technologię modemu. Ta sama skłębka telefoniczna jest wykorzystywana przez urządzenia technologii DSL, która zapewnia znacznie większą szerokość pasma. Czasami nawet ograniczenia wynikające z praw fizyki trudno jest opisać. Światłowód daje fizyczną możliwość uzyskania praktycznie nieograniczonej szerokości pasma. Pomimo tego nie jesteśmy w stanie w pełni wykorzystać możliwości światłowodu, ponieważ technologie, które pozwoliłyby na wykorzystanie całego jego potencjału, nie zostały jeszcze opracowane.

**Im większa szerokość pasma, tym większy koszt.** Można kupić sprzęt dla sieci LAN, który zapewni niemal nieograniczoną szerokość pasma przez długi czas. W przypadku połączeń WAN prawie zawsze trzeba kupić szerokość pasma od dostawcy usług. W obu przypadkach zrozumienie, czym jest szerokość pasma i skąd biorą się zmiany zapotrzebowania na szerokość pasma w danej chwili, może pozwolić danej osobie lub firmie na znaczące oszczędności. Menedżer sieci musi podejmować właściwe decyzje dotyczące tego, które urządzenia i usługi zakupić.

**Szerokość pasma ma kluczowe znaczenie dla analizy wydajności sieci, projektowania nowych sieci i zrozumienia zasad działania Internetu.** Osoba zawodowo zajmująca się sieciami komputerowymi musi rozumieć ogromny wpływ, jaki na wydajność i projekt sieci ma przepustowość i szerokość pasma. Informacje są przesyłane między komputerami na całym świecie jako ciągi bitów. Bity te reprezentują ogromne ilości

informacji przepływających przez kulę ziemską w ciągu pojedynczych sekund lub jeszcze szybciej. W pewnym sensie można powiedzieć, że Internet to pasmo.

**Popyt na szerokość pasma nieustannie rośnie.** Wraz z powstaniem technologii i infrastruktur sieciowych zapewniających szersze pasmo tworzone są aplikacje korzystające z tych możliwości. Przesyłanie siecią bogatych treści medialnych, w tym strumieni wideo i audio, wymaga bardzo szerokiego pasma. Zamiast tradycyjnych systemów głosowych instaluje się obecnie często systemy telefonii IP, co dodatkowo zwiększa zapotrzebowanie na szerokość pasma. Dla specjalistów w dziedzinie sieci komputerowych kluczem do sukcesu jest przewidywanie zwiększającego się zapotrzebowania na szerokość pasma i podejmowanie zgodnych z tą tendencją działań.

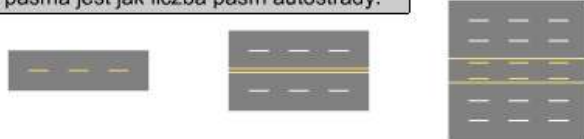
### 2.2.2 Pulpit

Szerokość pasma jest zdefiniowana jako ilość informacji, które można przesłać siecią w określonym czasie. Idea przepływu informacji sugeruje dwie analogie, które ułatwiają zobrazowanie szerokości pasma sieci. Ponieważ pojęcie przepływu opisuje zarówno wodę, jak i ruch uliczny, należy rozważyć następujące analogie:

**Szerokość pasma jest jak liczba pasm autostrady.**

Sieć dróg funkcjonuje w każdym dużym mieście lub miejscowości. Ogromne wielopasmowe autostrady są połączone mniejszymi drogami o mniejszej liczbie pasm. Drogi te prowadzą do jeszcze mniejszych, węższych dróg, które w końcu łączą się z dojazdami do domów i firm. Gdy systemem dróg porusza się mało samochodów, każdy pojazd może jechać bez ograniczeń prędkości. Gdy ruch jest większy, pojazdy poruszają się wolniej. Dzieje się tak szczególnie na drogach o mniejszej liczbie pasm dla samochodów. Gdy natężenie ruchu w systemie dróg zwiększy się jeszcze bardziej, nawet wielopasmowe autostrady staną się zatłoczone i powolne. Sieć danych bardzo przypomina system dróg. Pakiety danych można porównać do pojazdów, a szerokość pasma do liczby pasm autostrady. Gdy na sieć danych patrzy się jak na sieć dróg, można łatwo zaobserwować, w jaki sposób połączenia o wąskim paśmie powodują przeciążenia ruchu w całej sieci.

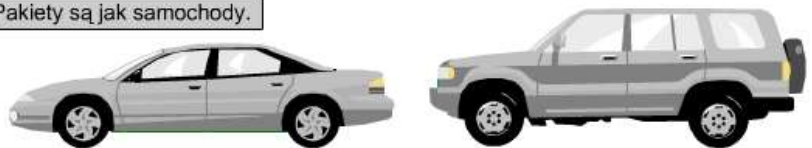
Szerokość pasma jest jak liczba pasm autostrady.



Urządzenia sieciowe można porównać do bramek, sygnalizacji świetlnej, znaków i map.



Pakiety są jak samochody.



### 2.2.3 Pomiary

W systemach cyfrowych podstawową jednostką szerokości pasma są bity na sekundę (b/s). Szerokość pasma jest miarą tego, jaka ilość informacji lub bitów może przepłynąć z jednego miejsca do innego w danym czasie. Choć szerokość pasma można określić w bitach na sekundę, zwykle używana jest wielokrotność tej jednostki. Innymi słowy, pasmo

sieciowe jest zwykle opisane przy użyciu tysięcy bitów na sekundę (kb/s), milionów bitów na sekundę (Mb/s), miliardów bitów na sekundę (Gb/s) i bilionów bitów na sekundę (Tb/s). Choć pojęcia szerokości pasma i szybkości są często używane zamiennie, nie oznaczają one tego samego. Ktoś może na przykład powiedzieć, że połączenie T3 o paśmie 45 Mb/s działa szybciej niż połączenie T1 o paśmie 1,544 Mb/s. Jeśli jednak wykorzystywana jest tylko niewielka część ich możliwości, oba typy połączeń będą przysyłały dane z mniej więcej tą samą szybkością. Na przykład, niewielka ilość wody będzie przepływała z tą samą szybkością zarówno przez rurę o dużej, jak i o małej średnicy. A więc bardziej ściśle jest stwierdzenie, że połączenie T3 ma szersze pasmo niż połączenie T1. Jest to spowodowane tym, że połączenie T3 może przenieść więcej informacji w tym samym czasie, a nie tym, że jest szybsze.

### 2.2.4 Ograniczenia

Szerokość pasma zależy od typu użytego medium oraz od użytej technologii sieci LAN lub WAN. Niektóre różnice wynikają z fizycznych właściwości medium. Sygnały są przysyłane miedzianą skrętką, kablem koncentrycznym, światłowodem lub za pomocą łącza bezprzewodowego. Fizyczne różnice w sposobie przysyłania sygnału są źródłem

Jednostka szerokości pasma	Skrót	Odpowiednik
Bity na sekundę	bps	1 b/s = podstawowa jednostka szerokości pasma
Kilobity na sekundę	kbps	1 kbps = 1,000 bps = $10^3$ bps
Megabity na sekundę	Mbps	1 Mbps = 1,000,000 bps = $10^6$ bps
Gigabity na sekundę	Gbps	1 Gbps = 1,000,000,000 bps = $10^9$ bps
Terabity na sekundę	Tbps	1 Tbps = 1,000,000,000,000 bps = $10^{12}$ bps

podstawowych ograniczeń przepustowości danego medium. Rzeczywista szerokość pasma sieci jest jednak zależna od dwóch czynników: rodzaju medium fizycznego oraz technologii służących do sygnalizacji i wykrywania sygnałów sieciowych. Na przykład aktualna wiedza dotycząca fizycznych właściwości miedzianej skrętki nieekranowanej (UTP) wyznacza teoretyczną granicę szerokości pasma równą jednemu gigabitowi na sekundę (Gb/s). Jednak w praktyce szerokość pasma zależy od tego, czy zostanie użyta sieć Ethernet typu 10BASE-T, 100BASE-TX czy 1000BASE-TX. Innymi słowy, rzeczywista szerokość pasma jest określana poprzez wybrane metody sygnalizacji, rodzaje kart sieciowych i inne elementy sieci. Szerokość pasma nie wynika więc wyłącznie z ograniczeń medium.

### 2.2.5 Przepustowość

Szerokość pasma jest miarą ilości informacji, które można przesłać siecią w danym czasie. Z tego powodu szerokość dostępnego pasma jest jednym z najważniejszych elementów specyfikacji sieci komputerowej. Typowa sieć LAN może być tak skonstruowana, aby zapewniała pasmo 100 Mb/s dla każdej stacji roboczej, ale to nie znaczy, że dowolny użytkownik będzie mógł w rzeczywistości przesłać siecią sto megabitów danych w każdej sekundzie korzystania z niej. Byłoby to możliwe tylko w warunkach idealnych. Pojęcie przepustowości może pomóc w wyjaśnieniu powodu takiego stanu rzeczy. Przepustowość oznacza rzeczywistą szerokość pasma zmierzoną o określonej porze dnia, przy użyciu określonych tras internetowych i podczas transmisji siecią określonych zbiorów danych. Niestety z wielu powodów przepustowość jest często znacznie mniejsza niż maksymalna możliwa szerokość pasma cyfrowego używanego medium. Niektórymi spośród czynników mających wpływ na przepustowość są:

- urządzenia intersieciowe
- typ przesyłanych danych
- topologia sieci
- liczba użytkowników sieci
- komputer użytkownika
- komputer pracujący jako serwer
- warunki zasilania

Teoretyczna szerokość pasma jest ważnym czynnikiem podczas projektowania sieci, ponieważ nigdy nie przekroczy ona wartości granicznych związanych z wyborem medium i technologii sieciowych. Jednak równie ważne dla projektanta sieci i administratora jest wzięcie pod uwagę czynników, które mogą wpłynąć na rzeczywistą przepustowość. Dzięki okresowym pomiarom przepustowości administrator sieci będzie miał świadomość zmian wydajności sieci i potrzeb jej użytkowników. Sieć można dzięki temu dostosowywać do aktualnych wymagań.

### 2.2.6 Obliczanie parametrów przesyłania danych

Projektanci i administratorzy sieci muszą często podejmować decyzje dotyczące szerokości pasma. Przykładem takiej decyzji może być podwyższenie parametrów połączenia WAN w celu obsługi ruchu związanego z nową bazą danych. Inna decyzja może być związana z określeniem, czy aktualna sieć szkieletowa LAN ma szerokość pasma wystarczającą dla szkoleniowego programu wideo. Odpowiedzi na takie pytania nie zawsze są łatwe, ale analizę należy zacząć od prostego obliczenia parametrów przesyłania danych. Korzystając ze wzoru: czas przesyłania = rozmiar pliku / szerokość pasma ( $C=R/P$ ), administrator sieci może oszacować kilka ważnych elementów składowych wydajności sieci. Jeśli typowy rozmiar pliku dla danej aplikacji jest znany, podzielenie tej wartości przez szerokość pasma sieci daje dobre przybliżenie najkrótszego czasu przesyłania takiego pliku. Wykonując takie obliczenia, należy wziąć pod uwagę dwie sprawy.

- Wynik jest tylko przybliżeniem, ponieważ rozmiar pliku nie obejmuje dodatkowych danych dołączonych podczas enkapsulacji.
- Wynik będzie najprawdopodobniej dotyczył najbardziej korzystnego przypadku, ponieważ dostępna szerokość pasma najczęściej nie jest równa maksymalnej szerokości pasma dla sieci danego typu.

Dokładniejsze oszacowanie można otrzymać, podstawiając we wzorze przepustowość w miejsce szerokości pasma. Chociaż obliczenie transferu danych jest całkiem proste, należy zwracać uwagę na to, by w równaniu posługiwać się tymi samymi jednostkami. Innymi słowy, jeśli szerokość pasma jest mierzona w megabitach na sekundę (Mb/s), rozmiar pliku należy podać w megabitach (Mb), a nie w megabajtach (MB). Ponieważ rozmiary plików są zwykle podawane w megabajtach, może być konieczne przemnożenie liczby megabajtów przez osiem, aby przekształcić je w megabity.

<b>Najlepszy czas pobierania</b>  $T = \frac{S}{BW}$	<b>Typowy czas pobierania</b>  $T = \frac{S}{P}$	BW	Maksymalna teoretyczna szerokość pasma najwolniejszego łącza między hostem źródłowym i docelowym (mierzona w bitach na sekundę)
		P	Rzeczywista przepustowość w momencie przesyłania (mierzona w bitach na sekundę)
		T	Czas przesyłania pliku (mierzony w sekundach)
		S	Rozmiar pliku w bitach

### 2.2.7 Transmisja cyfrowa a analogowa

Sygnały radiowe, telewizyjne i telefoniczne były do niedawna przesyłane drogą radiową oraz za pomocą transmisji przewodowej przy użyciu fal elektromagnetycznych. Fale te są nazywane analogowymi, ponieważ mają taki sam kształt jak fale świetlne i dźwiękowe wytwarzane przez nadajniki. Sygnał elektryczny przenoszący informacje zmienia się proporcjonalnie do zmian natężenia i kształtu transmitowanych fal świetlnych i dźwiękowych. Innymi słowy, fale elektromagnetyczne są analogią fal świetlnych i dźwiękowych.

Pasmo analogowe jest mierzone poprzez określenie, jaką część widma elektromagnetycznego zajmuje każdy sygnał. Podstawową jednostką pasma analogowego jest herc (Hz) lub liczba cykli na sekundę. Najczęściej używane są

wielokrotności jednostki podstawowej, jak dzieje się to w przypadku pasma cyfrowego. Powszechnie używanymi jednostkami są: kiloherc (kHz), megaherc (MHz) i gigaherc (GHz). Są to jednostki używane do opisania częstotliwości telefonów bezprzewodowych, które zwykle działają w zakresie 900 MHz lub 2,4 GHz. Są to także jednostki używane do opisu częstotliwości sieci bezprzewodowych 802.11a i 802.11b, wynoszących odpowiednio 5 GHz i 2,4 GHz. Chociaż sygnały analogowe mogą przenosić zróżnicowane informacje, mają one pewne znaczące wady w porównaniu z transmisją cyfrową. Analogowego sygnału wideo, którego transmisja wymaga szerokiego zakresu częstotliwości, nie można przesłać w węższym paśmie. Z tego powodu, jeśli wymagane pasmo analogowe nie jest dostępne, sygnału nie można wysłać. W przypadku sygnału cyfrowego wszystkie dane są przesyłane w postaci bitów niezależnie od rodzaju informacji.

Głos, sygnał wideo i dane przygotowane do transmisji w medium cyfrowym stają się strumieniami bitów. Taki sposób transmisji zapewnia istotną przewagę pasma cyfrowego nad analogowym. Kanałem cyfrowym o najwyższym nawet paśmie można przesłać nieograniczone ilości informacji. Niezależnie od tego, ile czasu trwa przesłanie informacji cyfrowej do miejsca docelowego i jej ponowne złożenie, może ona zostać wyświetlona, odsłuchana, odczytana lub przetworzona w oryginalnej postaci.

Zrozumienie różnic i podobieństw między pasmem cyfrowym i analogowym jest bardzo ważne. Oba typy pasm bardzo często występują w dziedzinie technik informacyjnych. Ponieważ jednak ten kurs dotyczy głównie cyfrowych sieci komputerowych, termin „pasma” będzie odnosił się do pasma cyfrowego

Szerokość pasma (cyfrowego) jest podobna do szerokości pasma analogowego.



Urządzenia sieciowe są jak telefony, radioodbiorniki AM/FM i odtwarzacze płyt CD.



Pakiety są jak muzyka.



## 2.3 Modele działania sieci komputerowych

### 2.3.1 Używanie warstw do analizy problemów związanych z przepływem informacji

W celu opisanie komunikacji między komputerami stosuje się koncepcję warstw. Na rysunku (obok) przedstawiono zbiór zagadnień związanych z przepływem, który jest zdefiniowany jako ruch fizycznych lub logicznych obiektów w systemie. Zagadnienia te ilustrują, w jaki sposób koncepcja warstw pomaga w opisie szczegółów procesu przepływu. Proces ten może być przepływem dowolnego rodzaju, od ruchu ulicznego w systemie dróg do przepływu danych w sieci komputerowej.

Rozmowa między dwiema osobami jest dobrą okazją do przedstawienia podejścia warstwowego w celu analizy przepływu informacji. Podczas rozmowy każda osoba, która chce coś powiedzieć, rozpoczyna od stworzenia myśli. Następnie podejmowana jest decyzja, w jaki sposób prawidłowo tę myśl przekazać. Można na przykład mówić, śpiewać lub krzyczeć oraz użyć określonego języka. W końcu myśl jest przekazywana. Osoba wydaje dźwięk, który przynosi wiadomość. Proces ten można podzielić na kilka odrębnych warstw, które mają zastosowanie do wszystkich rozmów. Górna warstwa jest myślą, która będzie przekazywana. Warstwa środkowa to decyzja dotycząca sposobu przekazania myśli.

Warstwa najniższa odpowiada za wytworzenie dźwięku, który przynosi informację. Ta sama metoda dzielenia na warstwy wyjaśnia, w jaki sposób sieć komputerowa przekazuje informacje od źródła do miejsca docelowego. Gdy komputery wysyłają informacje poprzez sieć, cała komunikacja rozpoczyna się u źródła, a kończy w miejscu docelowym. Informacje przenoszone w sieci są zwykle nazywane danymi lub pakietami. Pakiet jest logiczną grupą informacji, która przemieszcza się między systemami komputerowymi. Gdy dane są przekazywane między warstwami, każda warstwa dodaje do nich informacje, które umożliwiają efektywną komunikację z odpowiadającą jej warstwą na drugim komputerze. Sposób przesyłania danych między komputerami można wyjaśnić przy użyciu warstw modeli OSI i TCP/IP. Modele te różnią się liczbą i funkcjami warstw. Mimo to, każdego z nich można użyć do opisu i przedstawienia szczegółów przepływu informacji od źródła do celu.

### 2.3.2 Wykorzystanie warstw do opisu komunikacji danych

Aby możliwe było przesyłanie pakietów danych z miejsca źródłowego do docelowego, wszystkie urządzenia w sieci muszą używać tego samego języka lub protokołu. Protokół jest zestawem reguł, które komunikację w sieci czynią bardziej efektywną. Na przykład podczas lotu samolotem piloci stosują się do specjalnych zasad komunikacji z innymi samolotami i kontrolą lotów.

Protokół komunikacji danych jest zestawem reguł lub umową, która określa format i zasady transmisji danych.

Warstwa 4 w komputerze źródłowym komunikuje się z warstwą 4 w komputerze docelowym. Reguły i konwencje używane w tej warstwie są nazywane protokołami warstwy 4. Należy pamiętać o tym, że protokoły przygotowują dane liniowo.





Protokół w jednej warstwie, przygotowując dane do przesłania siecią, wykonuje na danych pewien zestaw operacji. Dane te są następnie przekazywane do kolejnej warstwy, w której następny protokół wykonuje inny zestaw operacji.

Gdy pakiet dotrze do miejsca docelowego, protokoły dokonują dekonstrukcji pakietu, który został zbudowany po stronie źródłowej. Wykonywane jest to w odwrotnej kolejności. Protokoły każdej warstwy w komputerze docelowym przywracają oryginalną postać informacji, aby aplikacja mogła je we właściwy sposób odczytać.

### 2.3.3 Model OSI

Wczesny rozwój sieci komputerowych był pod wieloma względami niezorganizowany. We wczesnych latach 80. XX w. nastąpił ogromny wzrost liczby i rozmiarów sieci. Gdy tylko w firmach zdano sobie sprawę z korzyści wynikających ze stosowania technologii sieciowych, prędkość wdrażania i rozpowszechniania się sieci dorównała tempu wprowadzania nowych technologii i produktów sieciowych na rynek. W połowie lat 80. w firmy zaczęły odczuwać problemy wynikające z tak gwałtownego rozwoju. Podobnie jak dzieje się to w przypadku ludzi, którzy mają problemy z porozumiewaniem się, ponieważ nie mówią tym samym językiem, w sieciach komputerowych zbudowanych na podstawie różnych specyfikacji i implementacji wystąpiły problemy z wymianą informacji. Te same problemy dotyczyły firm, które rozwijały prywatne lub zastrzeżone technologie sieciowe. Słowo „zastrzeżone” oznacza, że tylko jedna firma lub grupa firm miały kontrolę nad wykorzystaniem określonej technologii. Wzajemna komunikacja systemów opartych na ścisłej realizacji własnych, zastrzeżonych zasad nie była możliwa. W celu rozwiązania problemu niezgodności sieci organizacja ISO (ang. *International Organization for Standardization*) zbadała modele sieciowe, takie jak DECnet (ang. *Digital Equipment Corporation net*), SNA (ang. *Systems Network Architecture*) i TCP/IP, aby określić możliwy do ogólnego zastosowania zestaw zasad dla wszystkich sieci. Wykorzystując te badania, organizacja ISO utworzyła model sieciowy, który umożliwił producentom wytwarzanie wzajemnie zgodnych sieci. Model odniesienia OSI (ang. *Open System Interconnection*) wydany w roku 1984 był opisowym modelem sieci, który powstał w organizacji ISO. Zawierał on zestaw standardów przeznaczonych dla producentów, które zapewniły większą zgodność i możliwość współdziałania różnych technologii sieciowych wytwarzanych przez firmy na całym świecie. Model odniesienia OSI stał się głównym modelem komunikacji sieciowej. Chociaż istnieją inne modele, większość producentów sieci wykorzystuje w swoich produktach model odniesienia OSI. Dzieje się tak

w szczególności w przypadku szkolenia użytkowników ich produktów. Model ten jest uważany za najlepsze dostępne narzędzie służące do nauczania zagadnień związanych z wysyłaniem i odbieraniem danych w sieci.

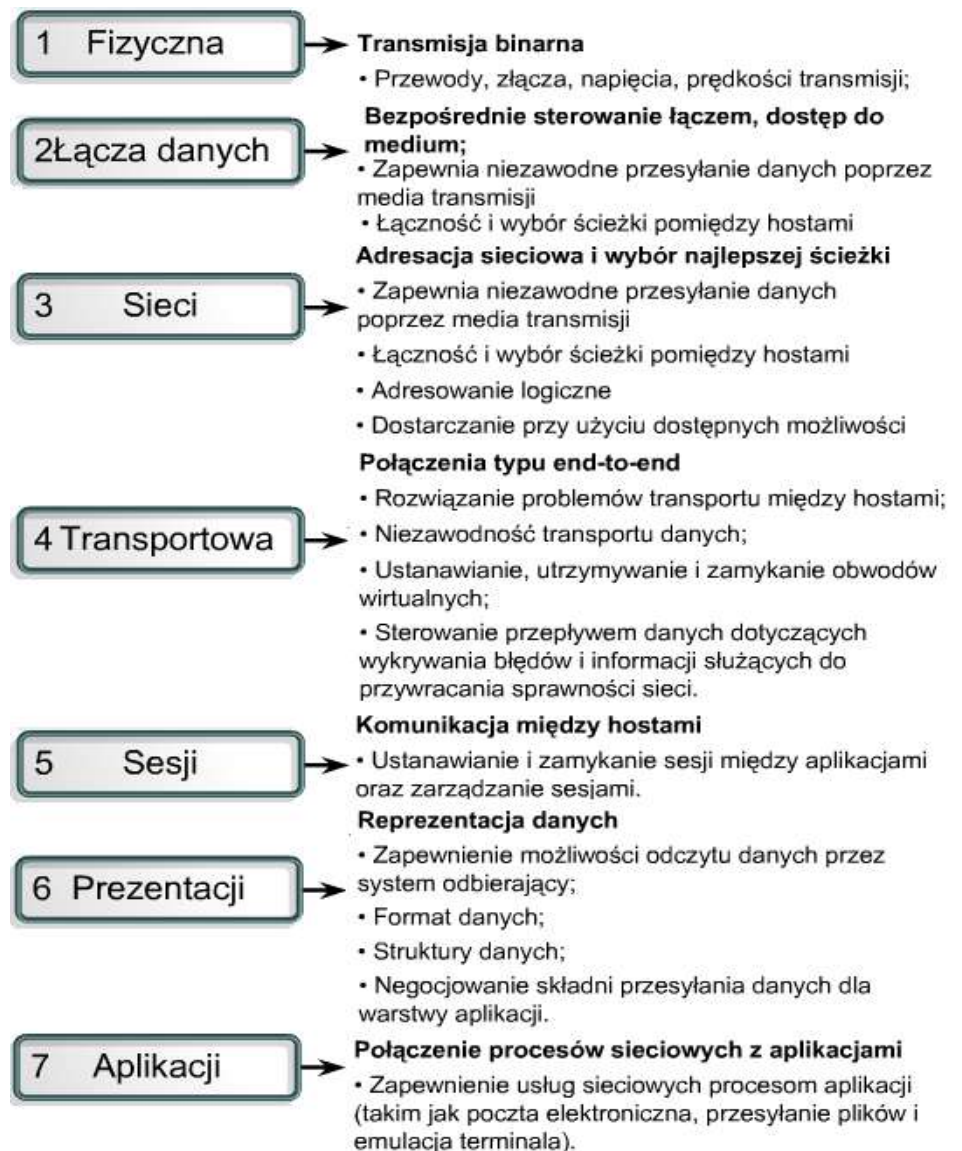
### 2.3.4 Warstwy OSI

Model odniesienia OSI jest szkieletem używanym do poznania mechanizmów przesyłania informacji w sieci. Przy użyciu tego modelu można wyjaśnić, w jaki sposób pakiet przechodzi przez różne warstwy do innego urządzenia w sieci, nawet jeśli nadawca i odbiorca dysponują różnymi typami medium sieciowego. W modelu odniesienia OSI jest siedem warstw, z których każda dotyczy pewnej funkcji sieci. – Podział sieci na warstwy przynosi następujące korzyści:

- dzieli proces komunikacji sieciowej na mniejsze, łatwiejsze do zarządzania elementy składowe;
- tworzy standardy składników sieci, dzięki czemu składniki te mogą być rozwijane i obsługiwane przez różnych producentów;
- umożliwia wzajemną komunikację sprzętu i oprogramowania sieciowego różnych rodzajów;
- zmiany wprowadzone w jednej warstwie nie dotyczą innych warstw;
- dzieli proces komunikacji sieciowej na mniejsze składowe, co pozwala na łatwiejsze jego zrozumienie.

#### Korzyści ze stosowania modelu OSI:

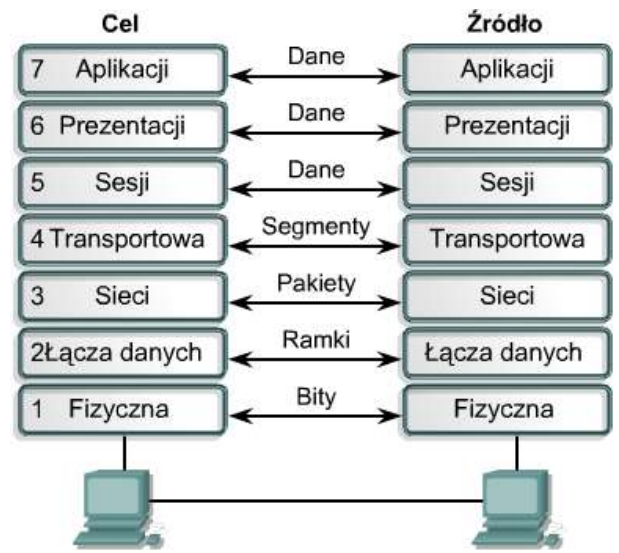
- Mniejsza złożoność
- Ustandaryzowanie interfejsów
- Projektowanie modułowe
- Zapewnienie współdziałania technologii
- Przyspieszony rozwój
- Uproszczenie procesu nauczania



### 2.3.5 Komunikacja węzłów równorzędnych

Aby dane mogły zostać przesłane ze źródła do miejsca docelowego, każda warstwa modelu OSI w miejscu źródłowym musi porozumieć się z równorzędną jej warstwą w miejscu docelowym. Taka forma komunikacji jest nazywana komunikacją równorzędną (ang. *peer-to-peer*). Podczas tego procesu protokoły każdej warstwy wymieniają informacje nazywane jednostkami danych protokołu (ang. *protocol data unit, PDU*). Każda warstwa komunikacyjna w komputerze źródłowym komunikuje się przy użyciu określonych jednostek PDU z równorzędną jej warstwą w komputerze docelowym, co przedstawiono na rysunku.

Pakiety danych w sieci są wysyłane ze źródła i trafiają do miejsca docelowego. Każda warstwa zależy od funkcji usługowej realizowanej przez warstwę OSI znajdującą się poniżej. W warstwie niższej następuje enkapsulacja jednostek PDU wyższej warstwy w polu danych warstwy niższej, po czym dodawane są nagłówki i stopki wymagane do wykonania funkcji tej warstwy. Następnie do danych przesyłanych w dół przez kolejne warstwy modelu OSI dodawane są kolejne nagłówki i stopki. Po dodaniu informacji w warstwach 7, 6 i 5 kolejne informacje zostaną dodane w warstwie 4. Taka grupa danych, jednostka PDU warstwy 4, jest nazywana segmentem. Warstwa sieciowa świadczy usługi warstwie transportowej, która dostarcza dane do podsystemu intersieci. Zadaniem warstwy sieciowej jest przesyłanie danych intersięcią. Zadanie to jest wykonywane poprzez enkapsulację danych i dodanie nagłówka, co powoduje utworzenie pakietu (jednostka PDU warstwy 3). Nagłówek zawiera informacje wymagane do realizacji przesłania, takie jak źródłowy i docelowy adres logiczny. Warstwa łącza danych świadczy usługi warstwie sieciowej. Umieszcza informacje pochodzące z warstwy sieciowej w ramce (jednostka PDU warstwy 2). Nagłówek ramki zawiera informacje (na przykład adresy fizyczne) wymagane do realizacji funkcji łącza danych. Warstwa łącza danych świadczy usługi warstwie sieciowej, umieszczając informacje pochodzące z tej warstwy w ramce. Warstwa fizyczna z kolei świadczy usługi warstwie łącza danych. W warstwie fizycznej następuje kodowanie ramki łącza danych na ciąg zer i jedynek (bitów) w celu przesłania ich przez medium (zwykle kabel) w warstwie 1.



### 2.3.6 Model TCP/IP

Model TCP/IP jest historycznym i technicznym standardem sieci Internet. Model odniesienia TCP/IP został utworzony w Departamencie Obrony USA jako projekt sieci, która przetrwałaby w każdych warunkach, nawet podczas wojny nuklearnej. W departamencie sformułowano wymaganie, aby transmisja pakietów była możliwa zawsze i w każdych warunkach przy wykorzystaniu różnych mediów komunikacyjnych, takich jak przewody miedziane, mikrofały, światłowody i łącza satelitarne. Postawienie tego trudnego problemu zaowocowało utworzeniem modelu TCP/IP. W przeciwieństwie do zastrzeżonych technologii sieciowych opisanych wcześniej, model TCP/IP został opracowany jako ogólnodostępny standard otwarty. Oznaczało to, że każdy mógł korzystać z modelu TCP/IP. Pozwoliło to na przyspieszenie rozwoju modelu TCP/IP jako standardu. Model TCP/IP składa się z następujących czterech warstw:

- warstwa aplikacji**
- warstwa transportowa**
- warstwa internetowa**
- warstwa dostępu do sieci**

Chociaż niektóre warstwy modelu TCP/IP nazywają się tak samo jak warstwy modelu OSI, oba modele nie do końca sobie odpowiadają. Największa różnica polega na tym, że warstwy aplikacji obu modeli realizują inne funkcje. Projektanci modelu TCP/IP uważali, że warstwa aplikacji powinna obejmować warstwy sesji i prezentacji modelu OSI. Stworzyli warstwę aplikacji, która obsługuje prezentację, kodowanie i sterowanie konwersacją. **Warstwa transportowa** jest odpowiedzialna za sprawy związane z jakością usług, co obejmuje niezawodność transmisji, sterowanie przepływem i korekcję błędów. Jeden z jej protokołów, protokół TCP, posiada efektywne i elastyczne sposoby realizowania niezawodnej komunikacji sieciowej o niskiej stopie błędów i wysokiej przepustowości. **Protokół TCP** jest protokołem zorientowanym połączeniowo. Obsługuje on konwersację między miejscem źródłowym a docelowym, pakując informacje pochodzące z warstwy aplikacji w jednostki nazywane segmentami. Nazwa „zorientowany połączeniowo” nie oznacza, że między komunikującymi się komputerami istnieje obwód. Oznacza to, że segmenty warstwy 4 są przenoszone tam i z powrotem między hostami, potwierdzając logiczne istnienie połączenia przez określony czas. Zadaniem warstwy internetowej jest podzielenie segmentów TCP na pakiety i przesłanie ich dowolną siecią. Pakiety trafiają do sieci docelowej niezależnie od przebytej drogi. Protokołem, który zarządza tą warstwą, jest protokół IP. W tej warstwie następuje określenie najlepszej ścieżki i przełączanie pakietów. Związek między protokołem IP i protokołem TCP jest bardzo istotny. Protokół IP określa drogę dla pakietów, a protokół TCP zapewnia niezawodny transport. Pojęcie warstwy dostępu do sieci jest szerokie i w pewnym stopniu mylące. Jest ona także nazywana warstwą łącza host-sieć. W warstwie tej są obsługiwane wszystkie fizyczne i logiczne składniki potrzebne do utworzenia fizycznego łącza. Obejmuje ona szczegółowe rozwiązania dotyczące technologii sieciowej, łącznie ze szczegółami warstwy fizycznej i łącza danych modelu OSI.

**Na rysunku** przedstawiono niektóre spośród popularnych protokołów zdefiniowanych przy użyciu warstw modelu odniesienia TCP/IP. Najczęściej stosowane protokoły warstwy aplikacji to:

protokół FTP (ang. *File Transfer Protocol*)

protokół HTTP (ang. *Hypertext Transfer Protocol*)  
 protokół SMTP (ang. *Simple Mail Transfer Protocol*)  
 protokół DNS (ang. *Domain Name System*)  
 protokół TFTP (ang. *Trivial File Transfer Protocol*)

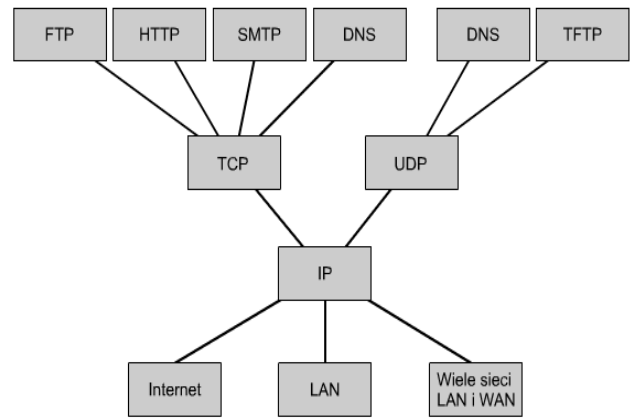
Najczęściej stosowane protokoły warstwy transportowej to:

protokół TCP (ang. *Transport Control Protocol*)  
 protokół UDP (ang. *User Datagram Protocol*)

Główny protokół warstwy internetowej to

protokół IP (ang. *Internet Protocol*)

Warstwa dostępu do sieci dotyczy określonej technologii używanej w danej sieci. Niezależnie od dostępnych usług aplikacji sieciowej i używanego protokołu istnieje tylko jeden protokół internetowy — protokół IP. Jest to świadoma decyzja projektowa. Protokół IP jest uniwersalnym protokołem umożliwiającym dowolnemu komputerowi komunikację w dowolnej chwili i w dowolnym miejscu.



**Porównanie modeli OSI i TCP/IP wykaże niektóre podobieństwa i różnice.**

**Podobieństwa są następujące:**

- Obydwa modele mają budowę warstwową.
- Oba protokoły mają warstwy aplikacji, chociaż świadczą one bardzo różne usługi.
- Oba mają porównywalne warstwy sieciowe i transportowe.
- Oba modele muszą być znane osobom zawodowo zajmującym się sieciami komputerowymi.
- W obu protokołach założeniem jest przełączanie pakietów. Oznacza to, że poszczególne pakiety mogą do tego samego miejsca docelowego trafić różnymi ścieżkami. Inaczej niż w sieci z komutacją łączy, gdzie wszystkie pakiety pokonują tę samą ścieżkę.

**Różnice są następujące:**

- W protokole TCP/IP zadania warstwy prezentacji i sesji są realizowane w warstwie aplikacji.
- W warstwie dostępu do sieci protokołu TCP/IP połączono funkcje warstw łącza danych i fizycznej modelu OSI.



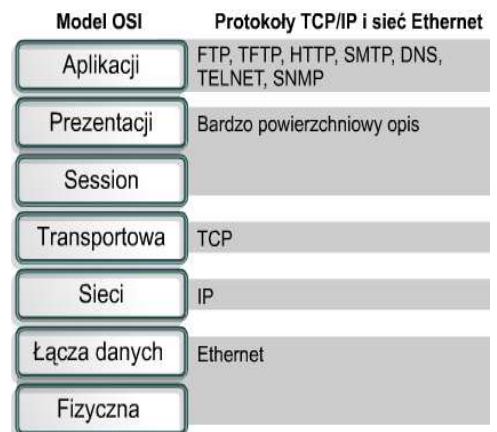
**Protokół TCP/IP wydaje się prostszy, bo ma mniej warstw.** Protokoły TCP/IP są standardem, wokół którego powstał Internet, więc model TCP/IP zyskał na znaczeniu właśnie dzięki tym protokołom. W przeciwieństwie do modelu TCP/IP model OSI nie jest zwykle bazą do tworzenia sieci, pomimo tego, że jest on używany jako podstawa teoretyczna. Chociaż protokoły TCP/IP są standardami, które przyczyniły się do rozwoju Internetu, w programie szkolenia będzie używany model OSI. Powody tego są następujące:

- Jest to podstawowy, niezależny od protokołów standard.
- Jest bardziej szczegółowy, co sprawia, że jest bardziej pomocny w nauce.
- Większa szczegółowość może być pomocna w przypadku rozwiązywania problemów.

Osoby zawodowo zajmujące się sieciami komputerowymi różnią się w opiniach, który model powinien być używany. W związku z naturą tej gałęzi przemysłu trzeba dobrze znać oba modele. Zarówno model OSI, jak i model TCP/IP będą przywoływane w trakcie trwania całego kursu. Nacisk zostanie położony na:

- protokół TCP jako protokół warstwy 4 modelu OSI;
- protokół IP jako protokół warstwy 3 modelu OSI;
- sieć Ethernet jako technologię obejmującą warstwy 2 i 1.

Należy pamiętać o tym, że między modelem a rzeczywistym protokołem używanym w sieci jest różnica. Model OSI będzie używany do opisu protokołów TCP/IP.



### 2.3.7 Szczegóły procesu enkapsulacji

Dane w komunikacji sieciowej są wysyłane ze źródła i trafiają do miejsca docelowego. Informacje przesyłane siecią są nazywane danymi lub pakietami danych. Jeśli dane mają być przesłane z jednego komputera (host A) do drugiego komputera (host B), muszą najpierw zostać opakowane w procesie zwanym enkapsulacją. W procesie enkapsulacji dane przed przesłaniem siecią są uzupełniane o potrzebne informacje związane z używanymi protokołami. Dlatego do pakietu danych przekazywanego w dół przez warstwy modelu OSI dodawane są nagłówki, stopki i inne informacje. Sposób przeprowadzania enkapsulacji można zaobserwować, patrząc na wędrówkę danych przez poszczególne warstwy, co przedstawiono na rysunku. Dane wysłane ze źródła przechodzą przez warstwę aplikacji w dół do kolejnych warstw. Opakowanie i przepływ wymienianych danych zmienia się, w miarę jak w kolejnych warstwach realizowane są usługi dla użytkowników końcowych. Jak przedstawiono to na rysunku, sieć musi przeprowadzić pięć następujących etapów konwersji, aby dokonać enkapsulacji danych:

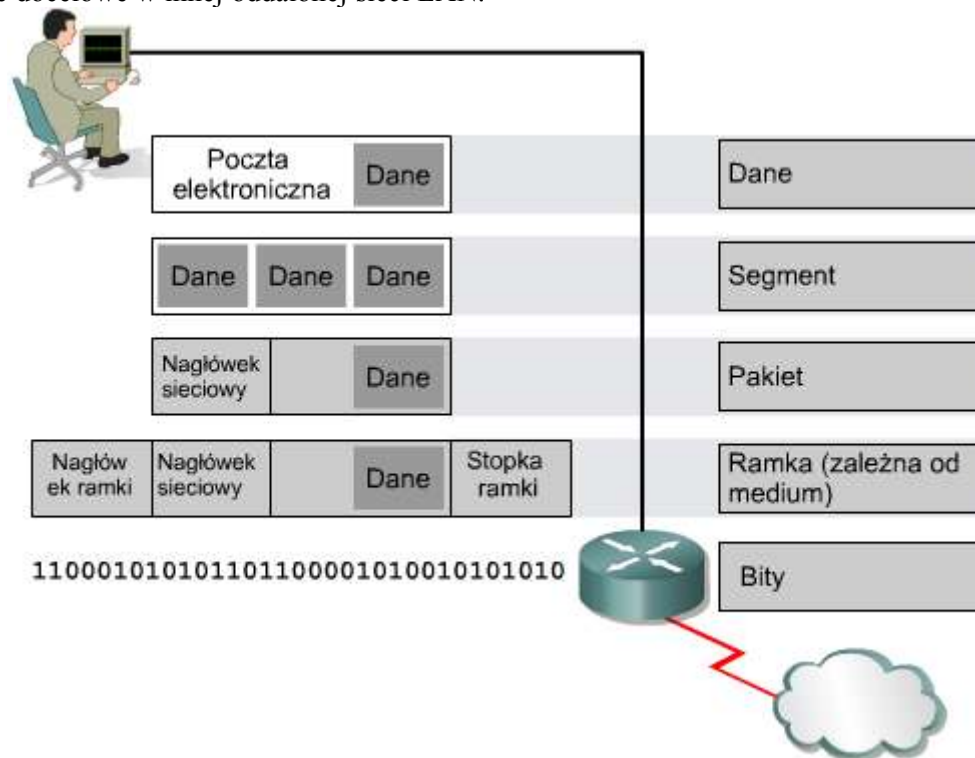
**Utworzenie danych.** Gdy użytkownik wysyła wiadomość e-mail, znaki alfanumeryczne są przekształcane w dane, które można przesłać intersiecią.

**Opakowanie danych do transportu end-to-end.** Dane są opakowywane w celu przesłania ich w intersieci. Funkcja transportowa dzięki użyciu segmentów zapewnia niezawodną komunikację hostów wiadomości po obu stronach systemu poczty elektronicznej.

**Dodanie sieciowego adresu IP do nagłówka.** Dane są umieszczane w pakiecie lub datagramie, który zawiera nagłówek z logicznym adresem źródłowym i docelowym. Adresy te umożliwiają urządzeniom sieciowym przesyłanie pakietów siecią wzdłuż wybranej ścieżki.

**Dodanie nagłówka i stopki warstwy łącza danych.** Każde urządzenie sieciowe musi umieścić pakiet w ramce. Ramka umożliwia połączenie z najbliższym bezpośrednio połączonym urządzeniem sieciowym na łączu. Każde urządzenie znajdujące się na wybranej ścieżce sieciowej musi obsługiwać ramki, aby możliwe było połączenie z następnym urządzeniem.

**Przekształcenie na bity w celu ich transmisji.** Ramkę trzeba przekształcić w ciąg zer i jedynek (bitów) w celu ich transmisji poprzez medium. Funkcja taktowania umożliwia urządzeniom rozróżnienie bitów przesyłanych przez medium. Medium w intersieci fizycznej może zmieniać się wzdłuż używanej ścieżki. Na przykład wiadomość e-mail może zostać wysłana z sieci LAN, przejść przez sieć szkieletową kampusu i zostać wprowadzona do sieci WAN, aż osiągnie miejsce docelowe w innej oddalonej sieci LAN.



## Podsumowanie

- Karty sieciowe, wtórniki, koncentratory, mosty, przełączniki i routery są powszechnie stosowanymi urządzeniami sieciowymi.
- Niektóre spośród popularnych typów sieci to: sieci LAN, WAN, MAN, SAN i VPN.
- Szerokość pasma jest zdefiniowana jako ilość informacji, które można przesłać siecią w określonym czasie.
- Dwa najbardziej znane modele sieci to: model odniesienia OSI i model TCP/IP.