Piotr Ziniewicz

Sieci

Komputerowe

Wraz z dynamicznym rozwojem systemów komputerowych oraz ich możliwości pojawiła się konieczność łączenia wielu systemów w celu wymiany informacji pomiędzy nimi bez konieczności używania nośników wymiennych takich jak na przykład dyskietki. Połączenie komputerów między sobą za pomocą stałego medium przesyłającego dane nie tylko upraszcza wymianę informacji, ale również w znacznym stopniu ją przyspiesza. Tak powstały sieci komputerowe.

Sieć komputerowa – jest to grupa komputerów lub innych urządzeń z nimi współpracujących połączonych ze sobą w celu wymiany danych i/lub współdzielenia różnych zasobów informacyjnych. Sieci komputerowe umożliwiają korzystanie ze wspólnych urządzeń takich jak drukarki, skanery, macierze dyskowe przechowujące olbrzymie ilości plików. Dzięki sieciom możliwe jest korzystanie ze wspólnego oprogramowania operującego na zcentralizowanej bazie danych oraz przesyłanie informacji pomiędzy komputerami takich jak listy czy pliki. Szczególnym przypadkiem wspólnego oprogramowania może być dostęp do stron WWW gdzie często możemy znaleźć interesujące nas informacje na przykład o wydarzeniach na świecie bądź wszelkiego rodzaju informacje naukowe i techniczne.

We współczesnych sieciach komputerowych wyróżnić możemy trzy główne elementy składowe:

- Media sieciowe (służą do transportowania informacji na mniejsze i większe odległości),
- Protokoły komunikacyjne (określają logiczny i fizyczny format przesyłanej przez medium informacji),
- Urządzenia sieciowe (zarządzają trasą informacji odbierając ją z jednego medium i przekazując do innego).
- Urządzenia klienckie (komputery i inne urządzenia korzystające z zasobów sieci)

Medium (liczba mnoga **media**) – słowo to wywodzi się od łacińskiego słowa oznaczającego "coś pomiędzy". W przypadku sieci komputerowych oznacza nośnik służący do transmisji danych. W praktyce sprowadza się do przewodu łączącego ze sobą komputery i urządzenia sieciowe. Szczególnym przypadkiem medium mogą być fale radiowe, które mimo że nie mają namacalnej postaci fizycznej również mogą służyć jako medium sieciowe.

Rodzaj zastosowanego medium sieciowego jest bezpośrednio związany z innym terminem określającym szybkość przesyłania danych w sieci.

Przepustowość – jest to maksymalna ilość informacji mierzonej w bitach jaka może być przesłana przez dane łącze w jednostce czasu mierzonej w sekundach. Na łącze składają się fragment medium wraz z interfejsami na jego końcach. Interfejs to część komputera lub urządzenia sieciowego, za pośrednictwem którego dane mogą być nadawane do medium i odbierane z niego. Tak więc podstawową jednostką przepustowości jest **Bit na sekundę** (*ang. bps - bit per second*) oznaczany **b/s** bądź **bps**. Oczywiście jednostka taka jest zbyt mała aby można było się nią wygodnie posługiwać w praktyce dlatego też na bazie przedrostków dziesiętnych układu SI stworzono pokrewne – większe jednostki:

kb/s (**kbit/s**), **kilobit na sekundę**

$1\ kb/s = 10^3\ b/s = 1\ 000\ b/s.$

Mb/s (**Mbit/s**), **megabit na sekundę**

$1\ Mb/s = 10^6\ b/s = 1\ 000\ 000\ b/s.$

Gb/s, **gigabit na sekundę**

$1\ Gb/s = 10^9\ b/s = 1\ 000\ 000\ 000\ b/s.$

Zwrócić należy uwagę, że kilobit oznaczany jest małą literą k (kb/s) a każda następna jednostka już dużą (Mb/s, GB/s). duża litera K zarezerwowana jest bowiem dla przedrostków w układzie binarnym.

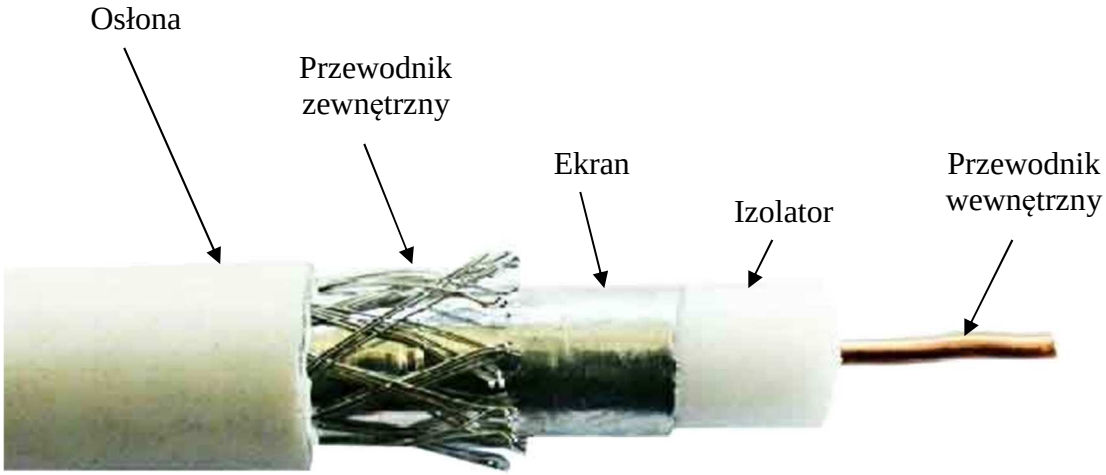
Jak łatwo policzyć przesłanie informacji o objętości 640 MB po łączu o przepustowości 10 Mb/s zajęło by niecałe 10 minut bo:
640 MB = 640 * 1024 * 1024 B = 671 088 640 B = 5 368 709 120 b
5 368 709 120 b / 10 000 000 bps = 536,870912 s = 8,9478485(3) min
Warto jednak zauważyć, że obliczenia te nie mogą dotyczyć ilości danych przesyłanych przez użytkownika. Spora porcja informacji przesyłanych przez medium to dane kontrolne i informacyjne zastosowanych protokołów przesyłu. W praktyce dane wysyłane przez użytkownika stanowią około 70% faktycznie przesyłanych informacji. Biorąc pod uwagę błędy, które mogą powstać w transmisji i konieczność powtórnej transmisji niektórych części informacji należy się liczyć z faktem, że rzeczywisty czas transmisji może wydłużyć się nawet dwukrotnie (zależy od jakości połączenia).

Z medium transmisyjnym wiąże się również inne pojęcie dotyczące sieci komputerowym. Jest nim **topologia sieci**. Pojęcie to można rozbić na dwa elementy ściśle ze sobą współpracujące.

Topologia Fizyczna – jest to układ przewodów (mediów transmisyjnych) jaki stosuje się do połączenia ze sobą komputerów i urządzeń w sieci. Jednym z warunków, jakie musi spełnić topologia fizyczna jest zapewnienie bezbłędnej transmisji danych.

Topologia Logiczna – Jest to część topologii sieci, która opisuje sposoby komunikowania się komputerów między sobą za pomocą urządzeń topologii fizycznej. Określa ona, który z komputerów w danej chwili może skorzystać z medium transmisyjnego

Jednym z podstawowych, szeroko stosowanych na przełomie latach osiemdziesiątych i dziewięćdziesiątych mediów sieciowych jest **kabel koncentryczny.** Składa się on z dwóch koncentrycznych (współosiowych) przewodów, skąd pochodzi jego nazwa [ryc.1]. Wewnętrzny przewód umieszczony w otoczce izolatora, na który nawinięta jest aluminiowa



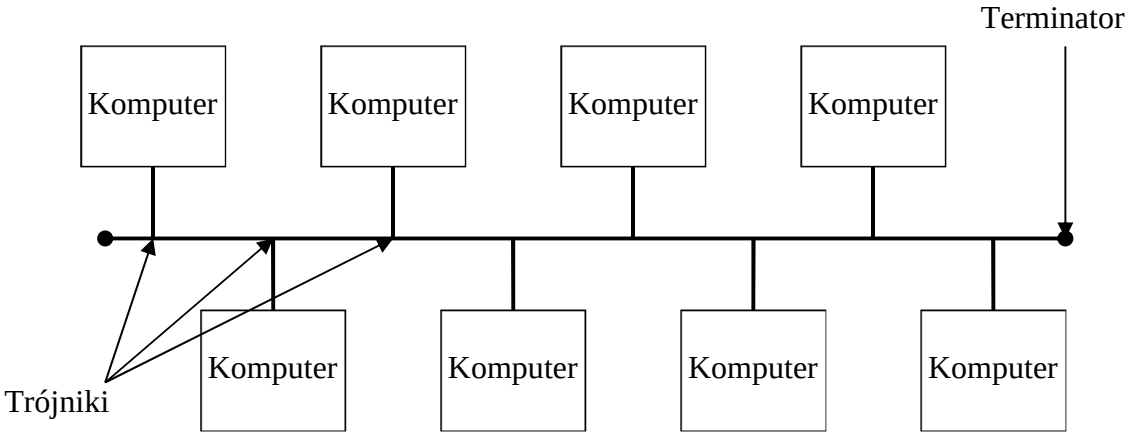
Ryc.1 Budowa kabla koncentrycznego

folia ekranująca. Jej zadaniem jest eliminowanie potencjalnych zakłóceń sygnału pochodzących ze środowiska zewnętrznego. Ekran otoczony jest z plecionką z drutu stanowiącą przewodnik zewnętrzny. Całość zamknięta jest w osłonie zabezpieczającej przed wpływem otoczenia. Kabel taki umożliwia prędkość transmisji do 10 Mb/s. Wadą kabla koncentrycznego jest jego wrażliwa na ostre zakręty i zgniatanie struktura. Łatwo ulega on uszkodzeniu, co powoduje pogorszenie sygnału owocujące spadkiem prędkości transmisji w wyniku zwiększenia się ilości błędów. Cena takiego przewodu jest również wyższa od obecnie używanej skrętki, co w połączeniu z jego większą średnicą spowodowało niemal całkowite zaniechanie jego stosowania pod koniec XX wieku.

Sieci komputerowe oparte na technologii kabla koncentrycznego wykorzystują najczęściej **topologię magistrali (szynową)**. W topologii tej wszystkie elementy sieci są

Ryc.2 Trójnik i wtyczka BNC stosowane przy łączeniu kabla koncentrycznego

podłączone do jednego kabla koncentrycznego. Poszczególne elementy sieci są podłączane do kabla za pomocą specjalnych trójników umożliwiających odgałęzienie przewodu w celu podłączenia do karty sieciowej komputera [ryc.2]. Magistralę (kabel) przecina się w miejscu przyłączenia komputera lub innego urządzenia a na obu końcach umieszcza się wtyczki. Wtyczki te mocuje się z obu stron do trójnika a jego trzecie odgałęzienie mocuje się do karty sieciowej komputera. Na obu końcach magistrali powinny znajdować się oporniki (tzw. terminatory), które zapobiegają odbijaniu się impulsu elektrycznego, który uniemożliwiłby transmisje poprzez wprowadzanie nakładających się na siebie zakłóceń. Maksymalna długość



Ryc.3 Schemat sieci w topologii magistrali

magistrali bez dodatkowych urządzeń wzmacniających sygnał zależy od klasy wykorzystywanego kabla i waha się od 185 do 1800 metrów. W celu przedłużenia magistrali konieczne jest połączenie jej segmentów za pomocą urządzeń „odświeżających” sygnał.

Do zalet zastosowania tego typu topologii należy:

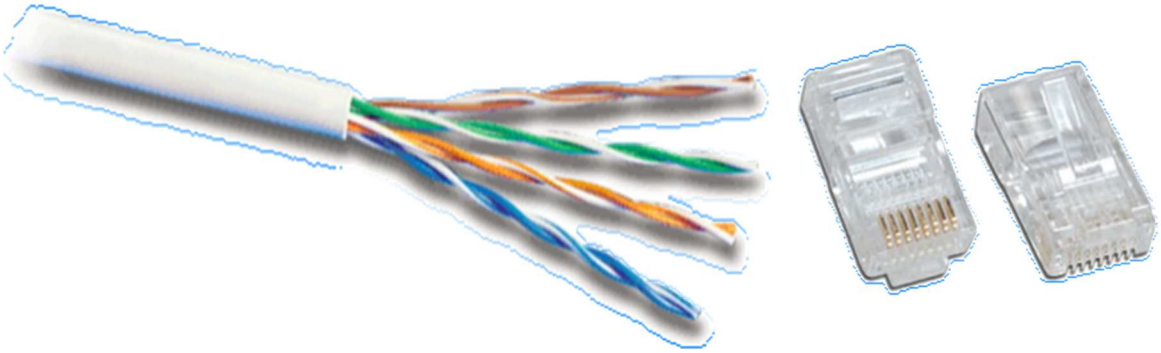
- Mała ilość użytego przewodu a co z tym idzie niska cena sieci
- Brak dodatkowych urządzeń sieciowych służących zarządzaniu ruchem w sieci, co dodatkowo obniża koszty.
- Łatwość montażu – nawet we własnym amatorskim zakresie
- Awaria pojedynczej stacji roboczej nie powoduje unieruchomienia całej sieci

Instalacja taka ma niestety również poważne wady:

- Przerwanie kabla w którymkolwiek miejscu powoduje unieruchomienie całego segmentu sieci. W miejscu przerwania magistrala dzieli się na dwie, w których jeden koniec nie jest zakończony terminatorem, co wprowadza zbyt duże zakłócenia, aby którakolwiek z nich mogła działać prawidłowo.
- Trudna lokalizacja usterek, o ile na kablu brak widocznych śladów przerwania konieczne jest sprawdzenie wszystkich odcinków w celu znalezienia uszkodzonego.

- W danej chwili możliwa jest tylko jedna transmisja danych. Tylko jeden komputer może nadawać, podczas gdy inne muszą nasłuchiwać i czekać aż skończy.
- Bardzo małe możliwości rozbudowy sieci
- Niskie bezpieczeństwo informacji – gdy jeden komputer nadaje wszystkie go słuchają. Choć tylko komputer docelowy interpretuje wysyłane informacje, inne mogą również podszyć się pod adresata i „podsłuchać" wysyłane informacje

Obecnie najpopularniejszym medium, jeśli chodzi o sieci lokalne jest **Skrętka dwużyłowa**. Składa się ona z dwóch dość cienkich przewodów pokrytych cienką warstwą polichlorku winylu i skręconych razem. Skręcenie przewodów równoważy promieniowanie, na jakie



Ryc.4 Budowa kabla opartego na skrętce dwużyłowej oraz wtyczki RJ-45

wystawiony jest każdy z nich znosząc w ten sposób zakłócenia elektromagnetyczne, które inaczej zakłócałyby sygnał. W sieciach komputerowych najczęściej stosowane są cztery pary przewodów połączone razem w wiązki, które osłonięte są wspólną koszulką z PCW lub teflonu. Istnieje również skrętka ekranowana, w której wszystkie pary owinięte są folią aluminiową a dopiero na jej wierzchu znajduje się koszulka [ryc.4]. Zaletą tego typu przewodu jest możliwość osiągnięcia wysokiej prędkości transmisji (do 1 Gb/s). Niestety umożliwia on transmisję na znacznie mniejszą odległość niż kabel koncentryczny (do 100m) i podobnie jak on jest bardzo wrażliwy na uszkodzenia mechaniczne.

Sieci komputerowe budowane na bazie skrętki wykorzystują najczęściej **topologię gwiazdy**. W sieci takiej wszystkie komputery i urządzenia podłączone są za pomocą kabli z urządzeniem sieciowym, które znajduje się w centrum gwiazdy. Urządzeniem tym jest koncentrator *(ang. hub)* lub przełącznik *(ang. switch)*. Zarządza ono całym ruchem w sieci. W zależności od typu urządzenia wyróżniamy dwa rodzaje topologii gwiazdy:

Aktywna – sygnał w urządzeniu jest regenerowany i wzmacniany, dzięki czemu zwiększa się odległość, na jaką może być przesyłany pomiędzy poszczególnymi komputerami. Dodatkowo sygnał odebrany z jednego kabla może być skierowany od razu do kabla, którym jest podłączony komputer adresata. Ogranicza to możliwość podsłuchu oraz obciążenie sieci ruchem pakietów.

Bierna – urządzenie działa jednie jako rozgałęźnik sygnału, nie regeneruje go ani nie wzmacnia. Dodatkowo sygnał powielany jest na wszystkie interfejsy, więc sieć pracuje przy identycznym obciążeniu jak w przypadku magistrali – tylko jeden komputer może nadawać w danej chwili.

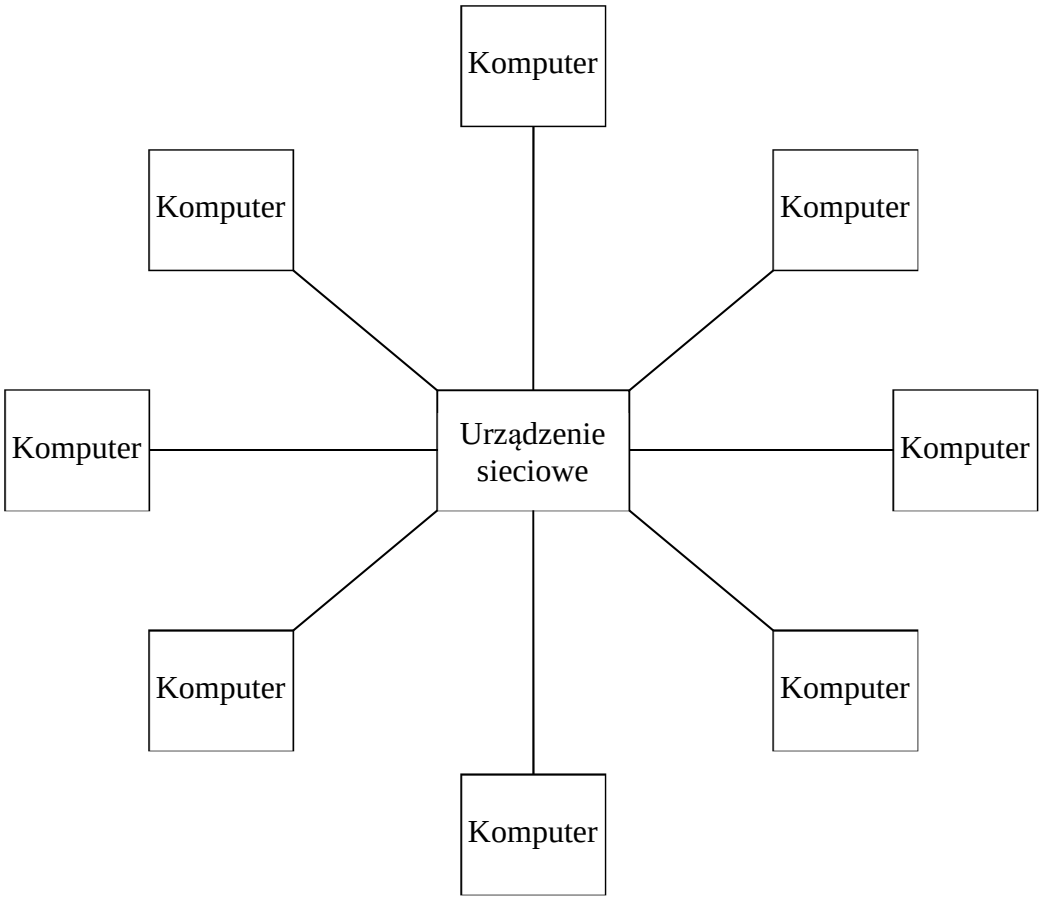
Do zalet zastosowania tego typu topologii należy:

- Łatwość rozbudowy sieci – wystarczy do urządzenia sieciowego podłączyć dodatkowy kabel prowadzący do nowego komputera lub innego urządzenia sieciowego.
- Przerwanie pojedynczego kabla nie powoduje unieruchomienia całej sieci a jedynie komputera, którym był on do niej przyłączony.
- Łatwość wykrywania usterek. W razie braku dostępu do sieci z któregoś komputera oczywiste jest, który przewód uległ uszkodzeniu.

- Przy zastosowaniu odpowiednio zaawansowanej technologii w urządzeniu sieciowym (np. Przełącznik) możliwa jest jednoczesna transmisja danych pomiędzy wieloma komputerami do niego podłączonymi. Wzrasta także bezpieczeństwo danych gdyż wyeliminowana zostaje możliwość podsłuchu (sygnał wysyłany jest przez przełącznik tylko do jego adresata).

Instalacja taka ma niestety również swoje wady:

- Stosunkowo wysoki koszt spowodowany dużą ilością kabla oraz koniecznością zakupu urządzenia sieciowego.
- W przypadku awarii urządzenia sieciowego cała sieć zostaje unieruchomiona do momentu jego wymiany lub naprawy w profesjonalnym serwisie.



Ryc.5 Schemat sieci w topologii gwiazdy

Kolejnym medium sieciowym jest kabel światłowodowy. Używany on jest do łączenia mniejszych sieci lokalnych w większe grupy i może być stosowany na duże odległości.

Kabel światłowodowy - giętkie włókno szklane, przez które dane są przesyłane z wykorzystaniem światła. Cienkie włókna szklane zamykane są w plastikowe osłony, co umożliwia ich zginanie nie powodując łamania. Nadajnik na jednym końcu światłowodu wyposażony jest w diodę świecącą lub laser, które służą do generowania impulsów świetlnych przesyłanych włóknem szklanym. Odbiornik na drugim końcu używa światłoczułego tranzystora do wykrywania tych impulsów. Najnowsze technologie zapewniają transmisję po takim kablu na odległości sięgające 100 km bez konieczności stosowania regeneratorów sygnału. Prędkości transmisji zależą od zastosowanych urządzeń transmisyjnych i mogą sięgać 10Gb/s. W praktyce do łączenia urządzeń znajdujących się w dużej odległości używa się wiązek kilkunastu lub nawet kilkuset światłowodów umieszczonych w jednej osłonie. Kable takie są bardzo grube i wykorzystuje je się z dwóch powodów. Po pierwsze istnieje możliwość realizacji

połączenia między dwoma urządzeniami sieciowymi za pośrednictwem kilku wiązek, co mocno zwiększa przepustowość kabla. Po drugie kabel taki kładziony jest raz przez specjalną ekipę a później istnieje możliwość wykorzystania nadmiarowych wiązek do zestawienia

Ryc.5 Światłowodowy kabel oraz przykład stosowanych wtyczek

nowych połączeń bez potrzeby wykonywania kolejnych prac ziemno-budowlanych. Na ryc.5 widzimy prosty przewód służący do łączenia urządzeń sieciowych na krótkie odległości (w ramach jednej szafy rozdzielczej). Przewody takie mają wiele standardów i stosowane są różne rodzaje wtyczek.

Do zalet wynikających z zastosowania tego rodzaju medium zaliczyć należy:

- Możliwość łączenia urządzeń znajdujących się w bardzo odległych punktach
- Brak wywoływania interferencji elektrycznej w innych kablach, oraz brak podatności na tego typu interferencje
- Możliwość łączenia światłowodów w większe wiązki zwiększając w ten sposób ich przepustowość przy zachowaniu niewielkiej grubości przewodu sprawia, że są one stosowane bardzo powszechnie do zestawiania szkieletowych połączeń międzynarodowych oraz międzykontynentalnych.

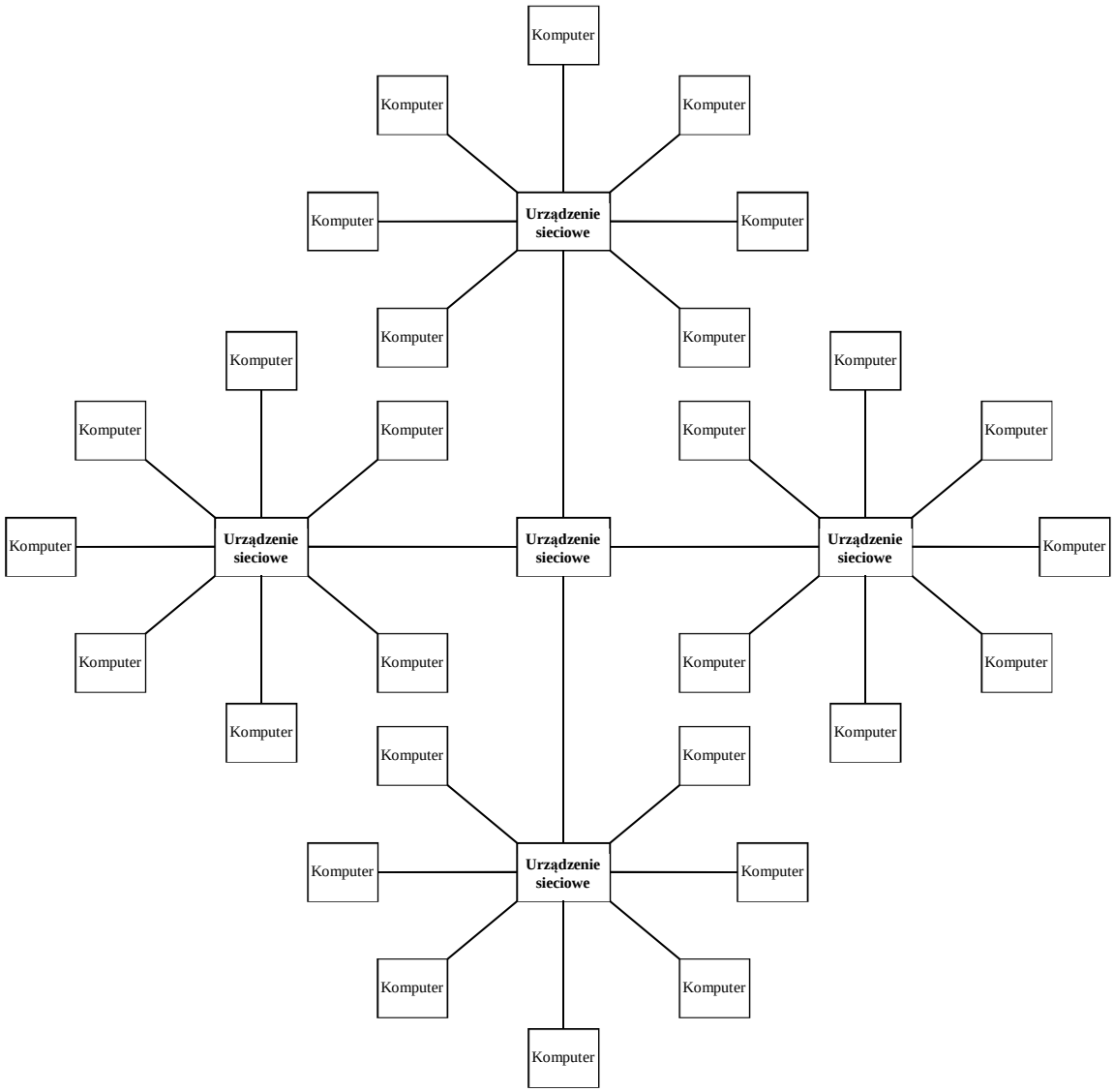
Niestety kable światłowodowe mają wiele wad:

- Najważniejszą z nich jest wysoka cena urządzeń jak i samych kabli. W praktyce nie używa się ich więc do podłączania pojedynczych komputerów lecz do zestawiania połączeń między większymi sieciami wewnątrz których stosowana jest skrętka lub inne medium
- Przy instalowaniu światłowodów konieczny jest specjalny sprzęt do ich łączenia oraz zakładania na nie wtyczek. Sprzęt ten jest tak drogi, że często stosuje się strategię jego wypożyczania wraz z obsługą zamiast zakupu urządzenia, które potrzebne jest praktycznie tylko do zbudowania sieci a w dalszym etapie staje się zbędne.
- Gdy włókno zostanie złamane wewnątrz plastikowej osłony, znalezienie miejsca zaistniałego problemu jest trudne. Sytuacja taka ma miejsce zwłaszcza, gdy kabel jest długi i leży pod ziemią. Istnieją urządzenia umożliwiające mniej lub bardziej precyzyjne określenie miejsca przerwania jednak same prace polegające na odkopaniu światłowodu i ponownym połączeniu są tak drogie, że w praktyce wykorzystuje się inny światłowód z tej samej wiązki, aby zastąpić uszkodzony.
- Naprawa złamanego włókna jest trudna ze względu na konieczność użycia specjalnego sprzętu. Możliwe jest ponowne połączenie przerwanego światłowodu metodą jego spawania. Metoda ta wymaga takich samych urządzeń jak przy instalacji światłowodu i jest dosyć droga. Jednak stosuje się ją w sytuacjach kiedy kabel biegnie w budynku i

jego całkowita wymiana byłaby droższa od naprawy. Kabel taki po naprawie nie uzyskuje całkowitej sprawności nowego przewodu, jednak jest ona na tyle satysfakcjonująca, że warto wziąć taką możliwość pod uwagę w przypadku awarii.

Omawiając łącza światłowodowe oraz łączenie mniejszych sieci w większe warto jest wspomnieć o **topologii gwiazdy rozgałęzionej.** Jest ona oparta na topologii gwiazdy, w której zamiast komputerów są kolejne urządzenia sieciowe stanowiące urządzenia centralne gwiazdy, dla komputerów i/lub kolejnych urządzeń sieciowych.

Przykład takiej sieci przedstawia ryc.6. Mamy tu jedno urządzenie centralne łączące 4

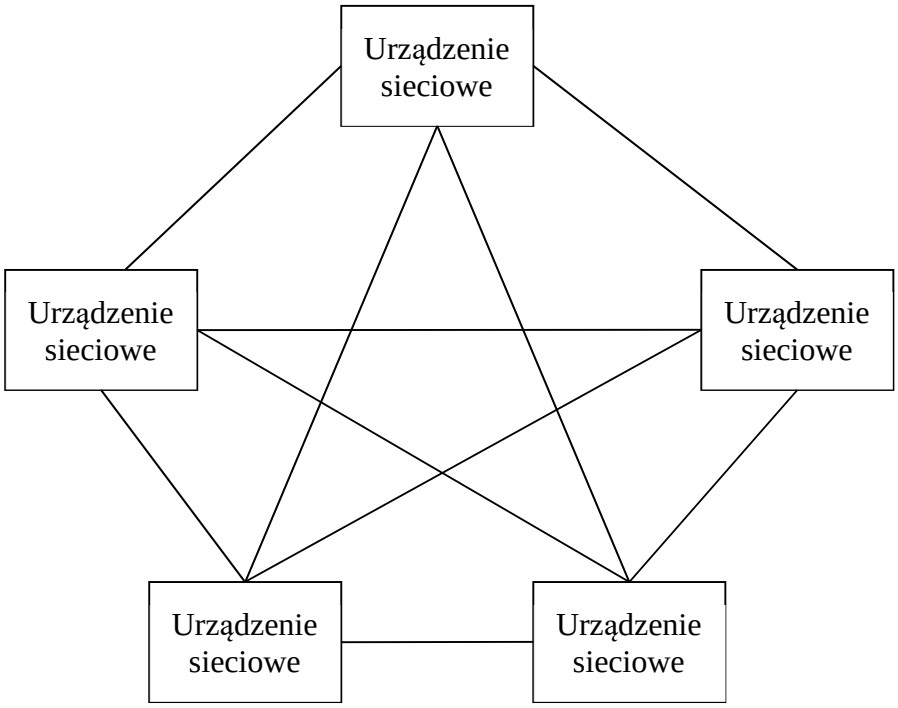


Ryc.6 Schemat sieci w topologii gwiazdy rozgałęzionej

urządzenia sieciowe. Urządzenia te z kolei są centralne dla 4 różnych gwiazd. Jest to topologia o charakterze hierarchicznym i przy odpowiednim skonfigurowaniu urządzeń możliwe jest takie ukierunkowanie ruchu pakietów, aby trafiały one tylko do swojego adresata bez względu na to, w której gwieździe się on znajduje. Połączenia między poszczególnymi urządzeniami sieciowymi realizowane są najczęściej właśnie za pomocą światłowodów.

Dzięki topologii takiej możemy łączyć ze sobą wiele sieci o różnych topologiach i różnych rodzajach zastosowanych mediów umożliwiając płynny przepływ informacji od źródła do celu. Na przykład zamiast jednego z komputerów może zostać dołączona magistrala na kablu

koncentrycznym z podłączonymi kilkoma komputerami. Zamiast innego komputera może zostać podłączone urządzenie sieciowe centralne dla kolejnej gwiazdy.
W praktyce pojedyncza gwiazda jest stosowana w obrębie jednego budynku bądź innego wydzielonego obiektu architektonicznego. Urządzenie centralne tej gwiazdy staje się ramieniem większej gwiazdy łączącej urządzenia sieciowe z budynków całego osiedla za pomocą kolejnego urządzenia centralnego, które z kolei staje się ramieniem gwiazdy łączącej wszystkie osiedla w mieście. Postępując w górę tej hierarchii łączącej ze sobą kolejno coraz większe sieci z coraz większych obszarów zauważymy, że coraz rzadziej jako elementy gwiazd pojawiają się komputery a coraz więcej pojawia się gwiazd z samymi urządzeniami sieciowymi. Ze zjawiskiem ten związany jest termin sieci szkieletowej.
Sieć szkieletowa *(ang. backbone network)* - Sieć telekomunikacyjna, w tym sieć komputerowa, przez którą przesyłana jest największa liczba informacji. Łączy zwykle mniejsze sieci (sieci lokalne), sieci rozległe. Urządzenia wchodzące w strukturę sieci szkieletowej z reguły odpowiedzialne są za funkcjonowanie całej sieci na określonym obszarze.
Należy zauważyć, że w przypadku uszkodzenia któregoś z łączy pomiędzy urządzeniami sieciowymi następuje całkowite odcięcie od reszty sieci jej fragmentu. Wewnątrz odciętego fragmentu komputery komunikują się bez problemu, jednak nie możliwa jest transmisja danych do komputerów spoza tego fragmentu. Na przykład w przypadku awarii przewodu łączącego centralne urządzenie sieciowe jakiegoś miasta z centralnym urządzeniem sieciowym dla całego kraju, całe te miasto zostaje odcięte od dostępu do zasobów sieciowych innych miast. Taka sytuacja jest niedopuszczalna i żeby ją wyeliminować stosuje się **topologię siatki**. W topologii takiej każdy komputer bądź urządzenie sieciowe połączone jest bezpośrednio z pozostałymi komputerami lub urządzeniami sieciowymi. Wyobraźmy sobie teraz przypadek z ryc.6, w którym urządzenia sieciowe połączone są nie za pomocą topologii gwiazdy a przy użyciu siatki [ryc.7]. Urządzenie sieciowe znajdujące się na górze ryc.7 to nasze dawne urządzenie centralne



Ryc.7 Schemat urządzeń sieciowych połączonych w topologii siatki

z ryc.6 i jest ramieniem gwiazdy nadrzędnej w stosunku do naszej (dzięki niemu zapewniona jest komunikacja z innymi częściami sieci). Pozostałe 4 urządzenia sieciowe są urządzeniami centralnymi swoich gwiazd i są do nich podłączone komputery (których na ryc.7 nie widać). W

takiej topologii przerwanie jednego połączenia nie zakłóca pracy sieci gdyż sygnał ma jeszcze 3 inne drogi do centralnego urządzenia poprzez pozostałe urządzenia sieciowe. Topologia taka może być stosowane na różnych poziomach łącząc na przykład wszystkie osiedla w obrębie miasta lub wszystkie kraje w obrębie kontynentu. W praktyce pełna siatka jest rzadko stosowana, zastępuje ją siatka częściowa gdzie urządzenia nie są połączone „Każdy z każdym" jednak z każdego urządzenia są przynajmniej dwie drogi do urządzenia nadrzędnego łączącego z resztą świata. Zwróciwszy uwagę na wygląd połączeń w sieciach rozległych opartych na topologii siatki nasuwa się oczywiste spostrzeżenie skąd wzięło się określenie „Sieć komputerowa". Warto wspomnieć że obecność wielu dróg do adresata wymusza na sieci wybór jednej która jest najlepsza w danym momencie. Najczęściej stosowanym tutaj kryterium jest czas trwania transmisji. Proces wyboru drogi transmisji nazywamy trasowaniem i jest on wykonywany przez specjalne urządzenia sieciowe nazywane Routerami.
Ostatnim medium transmisyjnym, którego popularność w ostatnich czasach bardzo wzrosła są **fale radiowe**. Fale elektromagnetyczne mogą być wykorzystywane nie tylko do nadawania programów telewizyjnych i radiowych, ale i do transmisji danych komputerowych. Sieci takie nie wymagają bezpośredniego fizycznego połączenia między komputerami. Każdy uczestniczący w łączności komputer jest podłączony do anteny, która zarówno nadaje, jak i odbiera fale. Prędkość transmisji obecnie utrzymuje się na poziomie 54 Mb/s, choć oczywiście

Ryc.8 Bezprzewodowa karta sieciowa oraz punkt dostępowy

urządzenia do zastosowań profesjonalnych osiągają znacznie wyższe prędkości. Zasięg działania połączenia dla urządzeń do użytku domowego wynosi około 100 metrów i uzależniony jest warunków architektonicznych. W przypadku ścian oddzielających pomieszczenia, w którym znajduje się komputer i urządzenie sieciowe zasięg drastycznie spada. Przy słabej jakości połączenia (zbyt duża odległość lub zakłócenia) spada również przepustowość takiej sieci. Oczywiście konstruowane są urządzenia o dużo większym zasięgu, wymagają jednak odpowiednio dużej anteny zarówno w urządzeniu jak i przy komputerze. Urządzenia takie służą zazwyczaj do udostępniania dostępu do sieci na obszarach o niskim zaludnieniu i rozrzuconej zabudowie.
W sieciach bezprzewodowych stosuje się najczęściej topologię gwiazdy, w centrum której znajduje się punkt dostępowy (AccessPoint) podłączony do sieci zewnętrznej za pomocą tradycyjnego przewodowego medium, lub za pomocą fal radiowych o większym zasięgu – a więc wymagających urządzeń z odpowiednio dużą anteną i mocą.
Do zalet sieci bezprzewodowych należą:

- Brak konieczności układania okablowania, co w niektórych przypadkach może być dużą oszczędnością.
- W przypadku komputerów przenośnych możliwe jest podłączenie do Internetu w miejscach publicznych. W miejscach takich znajdują się punkty dostępowe i możliwe jest podłączenie do sieci każdego komputera przenośnego wyposażonego w

bezprzewodową kartę sieciową. Możliwe jest więc na przykład surfowanie w Internecie na dworcu kolejowym w oczekiwaniu na pociąg.

Wady tego typu połączeń to:

- Stosunkowo niska przepustowość uzależniona często od warunków architektonicznych i pogodowych.
- Mała stabilność połączenia – jest ono często zrywane a przepustowość waha się w czasie.
- Konieczność stosowania skomplikowanych mechanizmów bezpieczeństwa dla zapewnienia poufności transmisji. Ze względu na to, że sygnał jest rozprzestrzeniany w każdym kierunku możliwe jest jego podsłuchanie. Koniecznym jest więc zastosowanie mechanizmów szyfrowania i autoryzacji dostępu do sieci po to aby podsłuchujący nie był w stanie odszyfrować transmisji bez odpowiedniego hasła-klucza.

Drugim bardzo ważnym elementem składowym sieci komputerowej są **Protokoły komunikacyjne** stanowiące zbiór ścisłych reguł i kroków postępowania, które są automatycznie wykonywane przez urządzenia komunikacyjne w celu nawiązania łączności i wymiany danych. Dzięki temu, że połączenia z użyciem protokołów odbywają się całkowicie automatycznie typowy użytkownik zwykle nie zdaje sobie sprawy z ich istnienia i nie musi o nich nic wiedzieć. Całkowita postać informacji przesyłanej w sieci określana jest przez protokoły począwszy od jej logicznej postaci (struktury) oraz formy dostępu do niej aż po poziomy napięć i charakterystykę sygnału w medium.

Klasyczne protokoły, składają się z trzech części:

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

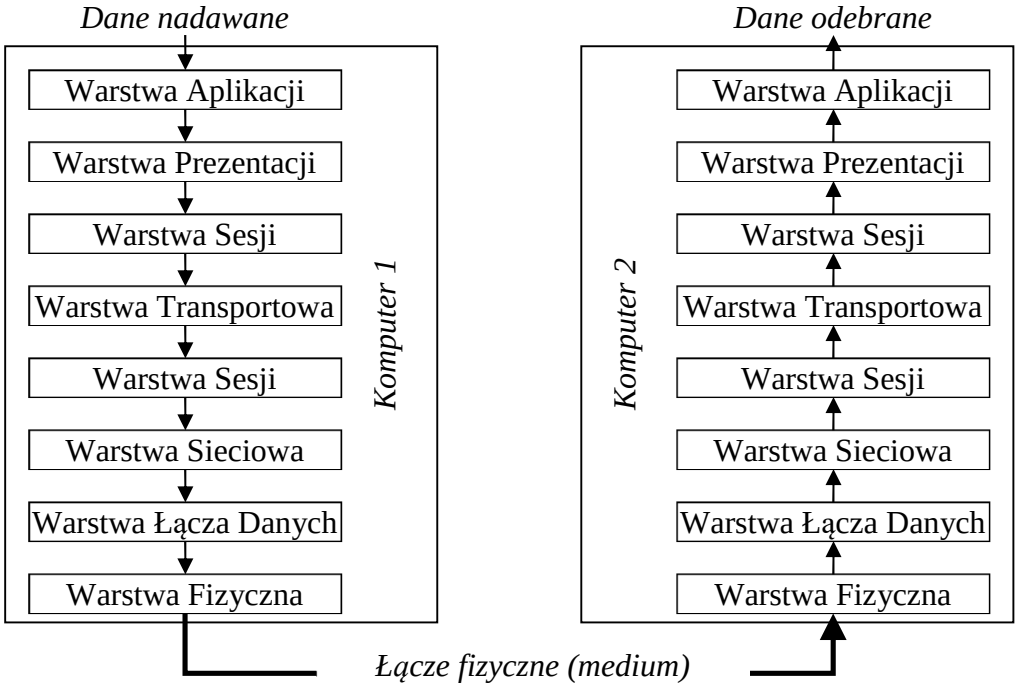
Na uwagę zasługuje fakt, że informacja może być porcjowana, szyfrowana i kompresowana na potrzeby przesyłu przez medium. Protokoły muszą więc posiadać możliwości jej rozszyfrowania, dekompresji a co najważniejsze poskładania w całość z mniejszych porcji które mogą dochodzić do adresata w kolejności różnej od kolejności wysyłania.

Na potrzeby konstrukcji protokołów oraz ich implementacji podzielono je na rodzaje (tzw. warstwy) a podział ten opisano standardem Modelu OSI.

Model OSI (pełna nazwa **ISO OSI RM**, ang. *ISO Open System Interconnection Reference Model* - model odniesienia łączenia systemów otwartych) jest to standard zdefiniowany przez ISO oraz ITU-T opisujący strukturę komunikacji sieciowej. Podstawowym założeniem modelu jest podział systemów sieciowych na 7 warstw (ang. *layers*) współpracujących ze sobą w ściśle określony sposób. Warstwy te uporządkowane są od najbardziej logicznej (najwyższej) do najbardziej fizycznej (najniższej). W założeniu informacja wysyłana przez sieć jest kolejno obrabiana przez protokoły od warstwy najwyższej do warstwy najniższej skąd przesyłana jest do medium. Podczas odbierania informacja przechodzi od warstwy najniższej do warstwy najwyższej skąd prezentowana jest na ekranie lub innym urządzeniu w oczekiwany przez użytkownika sposób.

Model OSI definiuje, jakie zadania oraz rodzaje danych mogą być przesyłane między warstwami w całkowitym oderwaniu od ich fizycznej i algorytmicznej realizacji, wokół tych warstw orientuje specyficzne dla nich protokoły, realizowane przez te protokoły usługi świadczone wyższym warstwom oraz posiadane interfejsy, umożliwiające dostęp do warstwy przez procesy z innych warstw. Mimo, iż **każda z warstw sama nie jest funkcjonalna**, to możliwe jest projektowanie warstwy w całkowitym oderwaniu od pozostałych. Jest to realne,

dzięki wcześniej zdefiniowanym protokołom wymiany danych pomiędzy poszczególnymi warstwami. Tak więc jeżeli chcemy wymienić medium za pomocą którego nasz komputer jest podłączony do Internetu, nie ma konieczności wymiany przeglądarki internetowej czy innych programów z nim współpracujących. Jedyne co należy zrobić to wymiana protokołów najniższych warstw zajmujących się bezpośrednio transmisją sygnału przez medium. Dzięki



Ryc.9 Schemat przepływu danych przez 7 warstwowy Model OSI

modelowi OSI istnieje pewność, że nowe protokoły będą współpracowały z protokołami wyższych warstw tak samo sprawnie jak poprzednie. W praktyce operacja ta sprowadza się do wymiany sterowników karty sieciowej.

Górne warstwy modelu OSI:

- Warstwa aplikacji,
- Warstwa prezentacji,
- Warstwa sesji,

Warstwy dolne modelu OSI:

- Warstwa Transportowa,
- Warstwa Sieciowa,
- Warstwa łącza danych,
- Warstwa fizyczna,

Przykładem konkretnego protokołu sieciowego jest **Protokół TCP/IP** wykorzystywany we współczesnym Internecie. W ramach tego protokołu, dowolna maszyna kliencka (uczestnicząca w wymianie danych lub je udostępniająca) nazywana jest **Host**em.

TCP/IP - *(ang. Transmission Control Protocol / Internet Protocol)* jest pakietem najbardziej rozpowszechnionych protokołów komunikacyjnych współczesnych sieci komputerowych. Został stworzony przez ***Agencję Zaawansowanych Projektów Badawczych Obrony Departamentu Obrony Stanów Zjednoczonych*** we wczesnych latach 70. Obecnie najczęściej wykorzystywany standard sieciowy, stanowiący podstawę współczesnego Internetu. Nazwa pochodzi od dwóch najważniejszych jego protokołów: **TCP** oraz **IP**.

IP *(ang. Internet Protocol)* to protokół komunikacyjny warstwy sieciowej modelu OSI Używany powszechnie w Internecie i sieciach lokalnych. Dane w sieciach IP są wysyłane w formie bloków określanych mianem pakietów. W przypadku protokołu IP, przed rozpoczęciem transmisji **nie jest** zestawiana żadna sesja komunikacyjna pomiędzy dwoma hostami. Protokół IP jest przez to protokołem zawodnym - nie gwarantuje dotarcia pakietów do adresata, braku ich zdublowania, ani ich odpowiedniej kolejności.
TCP *(ang. Transmission Control Protocol - protokół kontroli transmisji)* – strumieniowy protokół komunikacji między dwoma komputerami. W modelu OSI TCP odpowiada warstwie Transportowej. Zapewnia wiarygodne połączenie dla wyższych warstw komunikacyjnych. Charakterystyczne dla tego protokołu jest zestawianie wirtualnego połączenia pomiędzy dwoma hostami przesyłającymi między sobą dane. Podczas przesyłu pakietów, przy pomocy sum kontrolnych weryfikowana jest ich poprawność a dzięki numerom sekwencyjnym możliwe jest ułożenie pakietów we właściwej kolejności po odebraniu. W przypadku brakujących lub błędnych pakietów wysyłane są żądania ponownego ich przesłania. TCP jako protokół wyższego poziomu wykorzystuje IP do przesyłu pakietów przez sieć, rozwijając jednocześnie jego możliwości o mechanizm portów umożliwiający zestawienie wielu połączeń (np. dla różnych aplikacji) na komputerze/hoscie o jednym adresie IP. Numery portów reprezentowane są przez liczby z zakresu od 0 do 65535. Część portów (od 0 do 1023) jest zarezerwowana na standardowo przypisane do nich usługi takie jak strony WWW czy poczta elektroniczna. Przydzielaniem i rezerwacją numerów portów zajmuje się organizacja IANA (*ang. Internet Assigned Numbers Authority*) a aktualna ich lista znajduje się pod adresem ***http://www.iana.org/assignments/port-numbers***. Zdarza się że niektóre usługi korzystają z dwóch lub więcej różnych portów które używane są do realizacji różnych zadań. Przykładem może być usługa FTP (przesyłania plików) która wykorzystuje port 20 do przesyłania danych z plików i port 21 do przesyłania informacji kontrolnych i poleceń. Porty od 1024 do 65535 mogą być wykorzystywane do zestawiania połączeń, w zależności od potrzeb aplikacji korzystającej z protokołu.
Na uwagę zasługuje jeszcze jeden protokół wchodzący w skład TCP/IP, mianowicie UDP
UDP *(ang. User Datagram Protocol - Datagramowy Protokół Użytkownika)* – protokół ten działa w warstwie transportu modelu OSI. W protokole tym nie są nawiązywane połączenia oraz brak kontroli przepływu pakietów i ich retransmisji, można więc powiedzieć że jest to uproszczony protokół TCP. Dzięki takiemu uproszczeniu możliwa jest większa szybkość transmisji danych i brak dodatkowych zadań, którymi musi zajmować się host. Z tych względów UDP jest często używany w takich zastosowaniach jak konferencje wideo i gry sieciowe. W takich przypadkach dane muszą być przesyłane możliwie szybko, a poprawianiem błędów zajmują się protokoły innych warstw modelu OSI. Podobnie jak TCP, UDP wykorzystuje mechanizm portów, aby umożliwić identyfikację punktów końcowych (aplikacji lub usług) w obrębie jednego hosta. UDP zajmuje się jednak dostarczaniem pojedynczych pakietów, a nie strumieni danych tak jak TCP. Kolejną cechą odróżniającą UDP od TCP jest możliwość transmisji do kilku adresów docelowych na raz – multicast. Mechanizm numerowania portów UDP jest identyczny jak w przypadku TCP, warto jednak zauważyć, że porty UDP o tych samych numerach, co TCP nie są tożsame i stanowią odrębne punkty końcowe. W związku z tym ten sam numer portu może być wykorzystywany przez dwie różne usługi pod warunkiem, że jedna z nich wykorzystuje tylko protokół UDP a druga tylko TCP. Zdarzają się również usługi korzystające z obydwu protokołów i tego samego numeru portu – na przykład usługa DNS korzysta z portu 53 za pomocą TCP i UDP jednocześnie.

W celu jednoznacznej identyfikacji hostów protokół IP wykorzystuje adresy IP. Istnieje klika wariantów adresacji IP jednak najpopularniejszym z nich jest **IPv4** i właśnie nim się zajmiemy w dalszej części skryptu.

Adres IP – jest to unikatowy numer przyporządkowany komputerowi/hostowi wykorzystującemu protokół IP do komunikacji. Zapisywany jest on w postaci czterech ośmiobitowych liczb prezentowanych w postaci dziesiętnej i oddzielonych kropkami. Przez urządzenia sieciowe traktowany jest jednak jako jedna liczba 32-bitowa. Przykładowy adres IP widzimy poniżej:

Reprezentacja dziesiętna:	**212.33.76.124**
Reprezentacja binarna:	11010100 . 00100001 . 01001100 . 01111100
Liczba 32-bitowa:	11010100001000010100110001111100 (= 3558952060)

Użytkownicy Internetu nie muszą znać adresów IP dzięki usłudze DNS zajmującej się tłumaczeniem znanych powszechnie nazw domenowych (np. *www.umwb.edu.pl*) na odpowiadające im adresy IP.

Adresy IP przyznawane są poszczególnym hostom przez ich dostawcę Internetu. Proces ten może mieć charakter statyczny lub dynamiczny. W przypadku statycznego przyznawania adresu IP najczęściej jest on wpisywany w oknie konfiguracji sieci systemu operacyjnego hosta. Procesem dynamicznego przyznawania adresów zajmuje się usługa serwera DHCP *(ang. Dynamic Host Configuration Protocol - protokół dynamicznego konfigurowania węzłów).*

Kombinację adresu IP hosta oraz numeru portu określamy jako **Gniazdo** (*ang. Socket*). Gniazda zapisywane są w postaci adresu IP oraz numeru portu oddzielonych znakiem dwukropka (np. 212.33.76.124:5476). Właściwa komunikacja w protokołach TCP i UDP następuje pomiędzy gniazdami hostów. Komputer wysyłający żądanie dostępu do usługi pracującej na określonym porcie tworzy gniazdo używając swojego adresu IP i pierwszego wolnego portu. Z gniazda tego wysyłane są pakiety do gniazda serwera usługi składającego się z jego adresu IP i portu, na którym pracuje ta usługa. Jak widać nie ma konieczności aby numery portów w komputerze i serwerze były zgodne. Ważne jest żeby komputer znał gniazdo serwera a serwer gniazdo komputera, z którym wymienia dane.

Z adresowaniem IP ściśle wiąże się pojęcie **maski sieciowej**. Umożliwia ono określenie przynależności określonych komputerów do jednej sieci lokalnej lub jej podsieci. Zakładamy, że pewna określona ilość pierwszych bitów adresu IP pozostaje niezmienna i określa adres podsieci. Pozostałe bity określają precyzyjnie hosta w danej sieci. Maskę sieciową zapisujemy w takiej samej postaci jak adres IP. Rozpatrzmy następujący przykład:

Adres IP:	192.168.10.12	11000000.10101000.00001010.00001100
Maska sieci:	255.255.255.0	11111111.11111111.11111111.00000000

Na odpowiadających sobie bitach adresu i maski wykonujemy operację koniunkcji w wyniku której otrzymujemy adres sieci do której przynależy komputer:

Adres sieci:	192.168.10.0	11000000.10101000.00001010.00000000

Bardziej praktycznym sposobem wyliczania maski jest po prostu wyzerowanie tych bitów w adresie IP, dla których odpowiadające bity w masce mają wartość 0. Operacja ta daje nam dokładnie ten sam wynik, co logiczna operacja koniunkcji. Rozpatrywany przykład jest dość prosty i już „na oko” można stwierdzić, jaki jest adres sieci, ponieważ widzimy, że pierwsze 3 liczby są zachowywane w całości a czwarta jest odrzucana. Rozpatrzmy teraz nieco bardziej skomplikowany przykład:

Adres IP:	192.168.10.12	11000000.10101000.00001010.00001100
Maska sieci:	255.255.248.0	11111111.11111111.11111000.00000000
Adres sieci:	192.168.8.0	11000000.10101000.00001000.00000000

Pamiętajmy o tym, że w adresie sieci pozostają jedynie te bity, dla których odpowiadający bit maski jest jedynką.

Maska sieciowa nabiera prawdziwego znaczenia w momencie, gdy komputery danej sieci lokalnej o określonym adresie mają łączyć się z Internetem. Gdy urządzenie sieciowe porównując adres sieci docelowej danego pakietu stwierdzi, że różni się on od adresu sieci lokalnej wysyła go do urządzenia zwanego bramą, które pośredniczy w wymianie pakietów

pomiędzy siecią lokalną a Internetem. Do wyliczania adresu sieci docelowej używana jest oczywiście maska sieci lokalnej.
Znając maskę sieciową możemy również wyliczyć zakres adresów IP używanych przez daną sieć lokalną. Dolnym ograniczeniem zakresu będzie oczywiście nasz adres sieci. Żeby wyliczyć górne ograniczenie zakresu należy ustawić w adresie sieci na 1 te bity, które odpowiadają wartości 0 w masce sieciowej. Rozpatrzmy to na przykładzie:

Maska sieci:	255.255.248.0	11111111.11111111.11111000.00000000
Adres sieci:	192.168.8.0	11000000.10101000.00001000.00000000
Adres od:	192.168.8.0	11000000.10101000.00001000.00000000
Adres do:	192.168.15.255	11000000.10101000.00001111.11111111

Nasz zakres adresów w tym przypadku to 192.168.8.0 – 192.168.15.255

W zależności od wielkości sieci oraz przeznaczenia adresu IP wyróżniamy następujące grupy adresów sieci nazywane klasami:

Klasa A

Zakresy adresów sieci: **1.0.0.0 - 126.0.0.0**

Najstarszy bit pierwszego bajtu adresu jest zawsze równy zeru, poza tym liczby 0 i 127 są zarezerwowane. Klasa ta przeznaczona jest dla wyjątkowo dużych sieci (ponad 16 milionów hostów dla każdej sieci).

Klasa B

Zakresy adresów sieci: **128.1.0.0 - 191.254.0.0**

Najstarsze dwa bity pierwszego bajtu adresu to 10. Klasa ta przeznaczona jest dla średnich i dużych sieci (ponad 60 tysięcy hostów dla każdej sieci).

Klasa C

Zakresy adresów sieci: **192.0.1.0 - 223.255.254.0**

Najstarsze trzy bity pierwszego bajtu adresu to 110. Klasa ta przeznaczona jest dla małych sieci (ponad 250 hostów dla każdej sieci).

Klasa D

Zakresy adresów sieci: **224.0.0.0 - 239.255.255.254**

Najstarsze cztery bity pierwszego bajtu adresu to 1110. Ta przestrzeń adresowa została utworzona w celu umożliwienia rozsyłania grupowego do zdefiniowanej wcześniej grupy adresów IP. Grupa ta określana jest unikatowym adresem IP z tej klasy. Dzięki temu pojedynczy komputer może przesyłać jeden strumień danych równocześnie do wielu odbiorców.

Klasa E

Zakresy adresów sieci: **240.0.0.0 - 255.255.255.255**

Najstarsze cztery bity pierwszego bajtu adresu to 1111. Adresy tej klasy zostały zarezerwowane przez Internet Engineering Task Force (IETF) do potrzeb badawczych i nie są dostępne do publicznego użytku.

Pośród całkowitej puli adresów IP występują adresy specjalne nie używane do normalnej adresacji hostów. Wymienimy teraz kilka z nich:

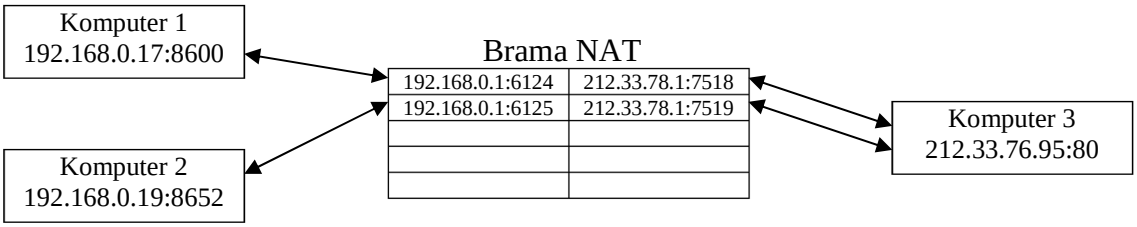
Loopback – czyli pętla zwrotna. Adres 127.0.0.1 używany jest do wymiany informacji w obrębie jednego hosta. Pakiety wysłane na ten adres trafiają z powrotem do urządzenia, które je wysłało nawet, jeśli nie jest ono podłączone do żadnej sieci. Adres ten wykorzystywany jest w celach testowych oraz w aplikacjach sieciowych zainstalowanych na pojedynczej stacji roboczej niepodłączonej do sieci. W przypadku aplikacji, które wymagają na przykład serwera bazodanowego istnieje możliwość instalacji go na tym samym komputerze, na którym będzie wykorzystywana aplikacja. Jeżeli komputer nie jest podłączony do sieci należy jako adres serwera w konfiguracji aplikacji podać właśnie 127.0.0.1.

Adres Sieci – omówiony już wcześniej nie może być przypisany do żadnego konkretnego hosta. Służy on jedynie celom związanym z rozpoznaniem, z jakiej podsieci pochodzi komputer o konkretnym adresie IP.
Broadcast – Adres służący rozsyłaniu pakietów do wielu hostów w obrębie danej posieci. Jest on wyliczany na podstawie adresu hosta wysyłającego oraz maski sieci. W istocie jest to po prostu górny zakres adresów używanych przez daną podsieć i wylicza się go w identyczny sposób (ustawiając na 1 bity adresu IP którym odpowiadają bity zerowe w masce). Teoretycznie możliwe jest rozsyłanie broadcastów poza podsieć jednak w praktyce są one odbierane przez bramę, która jest skonfigurowana do ich odrzucania.
Adresy prywatne
Z założenia każdy adres IP musi być unikatowy i jednoznacznie identyfikować hosta. Jak łatwo zauważymy istnieje 4 294 967 296 kombinacji adresu IP z czego spora część to adresy specjalne które nie mogą być wykorzystywane do adresacji urządzeń. Przy obecnym rozwoju komputeryzacji na świecie liczba ta jest bardzo mała i może ograniczać rozwój Internetu, choć w czasach jego powstawania była wystarczająco duża. W celu zniwelowania tego efektu zaproponowano kilka rozwiązań. Jednym z nich jest wprowadzenie adresacji IPv6 przewidującej zapis pojedynczego adresu IP na 128 bitach. Rozwiązanie te aczkolwiek radykalne i bardzo nowoczesne obarczone jest problemem wdrożenia do istniejącej rozległej sieci Internetowej. Innym ciekawym i powszechnie stosowanym rozwiązaniem jest stosowanie adresów prywatnych. Polega ono na wyznaczeniu określonej puli adresów IPv4 która ignorowana jest przez infrastrukturę Internetu. Adresy te wykorzystywane są w sieciach lokalnych a ich unikatowość ogranicza się jedynie do obszaru każdej z nich. Oto wykaz adresów prywatnych zarezerwowanych dla każdej klasy sieci:

- 10.0.0.0 - 10.255.255.255 - dla sieci prywatnych klasy A (maska: 255.0.0.0)
- 172.16.0.0 - 172.31.255.255 - dla sieci prywatnych klasy B (maska: 255.240.0.0)
- 192.168.0.0 - 192.168.255.255 - dla sieci prywatnych klasy C (maska: 255.255.255.0)

Nie ma możliwości wysłania bezpośrednio pakietu do urządzenia posiadającego adres prywatny, chyba że urządzenie go wysyłające należy do tej samej sieci lokalnej. Takie wydzielone sieci komunikują się z resztą świata przy użyciu jednego adresu publicznego przypisanego bramie. Brama jest to urządzenie pośredniczące w wymianie pakietów pomiędzy siecią lokalną a Internetem i posiada dwa adresy IP – jeden wewnętrzny – w naszym przypadku prywatny należący do sieci lokalnej oraz zewnętrzny – publiczny a więc widziany przez infrastrukturę Internetu. Proces taki nazywamy translacją adresów – **NAT** (*ang. Network Address Translation*). Wyróżniamy dwa podstawowe rodzaje translacji adresów:
SNAT (*Source Network Address Translation*) stosowana w celu umożliwienia komputerom o adresach prywatnych komunikacji z Internetem.
DNAT (*Destination Network Address Translation*) stosowana w celu umożliwienia dostępu z Internetu do komputera o adresie prywatnym (jeżeli chcemy na przykład wykorzystać go jako serwer)

Proces komunikacji z Internetem komputerów o adresach prywatnych komplikuje się nieco, jeśli założymy, że komputer ma nie tylko wysłać informację do jakiegoś hosta spoza sieci ale również odebrać od niego odpowiedź. Logicznym jest, że brama realizująca translację adresów musi zapamiętać spod jakiego adresu odebrała pakiet przesłany później do hosta docelowego,



Ryc.14 Uproszczony schemat działania translacji adresów

aby po odebraniu odpowiedzi móc przekazać ją do właściwego nadawcy. Na Ryc.14 mamy przedstawioną schematycznie zasadę działania tego typu operacji. Na schemacie oznaczono również numery portów – znajdują się one za adresem IP po dwukropku. Dwa komputery znajdujące się w sieci lokalnej na prywatnych adresach IP zgłaszają do serwera WWW znajdującego się na komputerze 3 prośbę o przesłanie zawartości strony. Komputer 3 znajduje się za bramą realizującą translację adresów i ma adres publiczny. Brama od strony sieci lokalnej ma adres 192.168.0.1 a od strony Internetu 212.33.78.1. Nawiązuje ona połączenia z komputerami 1 i 2 na dowolnie wybranych wolnych portach. W odebranych pakietach zmienia adres nadawcy na swój zewnętrzny adres i numer portu nadawcy na pierwszy wolny port. Dokonane zmiany są zapisywane w tablicy stanów NAT. Następnie pakiety są przesyłane do adresata, który je przetwarza i odsyła na adres nadawcy, czyli naszej bramy. Brama na podstawie tablicy stanów zamienia adres odbiorcy na właściwy i wysyła je do sieci lokalnej. Widać, że komputer 3 nawet nie „wie” o istnieniu komputerów 1 i 2 gdyż realizuje po prostu żądania bramy spod adresu 212.33.78.1.

Zapora Internetowa

Ważnym pojęciem z zakresu bezpieczeństwa sieci jest Zapora Internetowa (*ang. Firewall – „ściana ogniowa”*). Zajmuje się ona filtrowaniem pakietów przepływających przez nią oraz zapisywaniem informacji o podejrzanych połączeniach. Termin ten może odnosić się zarówno do samodzielnego urządzenia sieciowego ustawianego najczęściej przed bramą sieci lokalnej jak i do oprogramowania instalowanego na komputerach – stacjach roboczych. Podstawowym zadaniem zapory jest blokowanie dostępu do określonych portów komputera lub komputerów. Blokada ta może dotyczyć wszystkich hostów lub tylko wybranych. Tak więc możliwe jest takie skonfigurowanie zapory aby dostęp do konkretnego portu określonego komputera miały tylko komputery będące z nim w sieci lokalnej o tym samym adresie, zapobiegając w ten sposób wypływowi poufnych danych na zewnątrz sieci. Zaporę internetową można też skonfigurować w taki sposób, aby komputery z sieci lokalnej nie miały dostępu do określonego portu komputerów spoza sieci wyłączając na przykład możliwość korzystania z komunikatorów oraz czata, co często praktykowane jest w prywatnych firmach w celu podniesienia wydajności pracownika. Ponadto wszelkie próby zakazanego dostępu mogą być zapisywane w pliku nazywanym logiem firewalla. Administrator po przejrzeniu takiego loga ma możliwość wykrycia potencjalnych prób włamania do systemu lub sieci. Najbardziej zaawansowane zapory internetowe mają możliwość analizowania zawartości przesyłanych stron WWW i filtrowania ich w celu zapobieżenia wyświetlaniu wulgaryzmów i innych niecenzuralnych treści. Współcześnie działające zapory sieciowe pracują w warstwach modelu OSI od łącza danych aż po warstwę aplikacji.

Nazwa domenowa jest adresem komputera – najczęściej serwera w sieci, zapisanym w łatwej do zapamiętania formie. Składa się ona z dwóch lub więcej części oddzielonych kropkami (np. www.umwb.edu.pl). W skład nazwy mogą wchodzić litery (a…z), cyfry (0…9) oraz znak myślnika (-) który jednak nie może być użyty ani na początku ani na końcu żadnej części nazwy domenowej. Znaki narodowe również nie mogą wchodzić w skład nazwy domenowej (niedopuszczalne jest na przykład użycie www.białystok.pl). Nazwy domenowe w pewien sposób odzwierciedlają strukturę sieci, nie jest to jednak struktura fizyczna a administracyjna. Części wchodzące w skład nazwy posiadają pewną hierarchię pozwalającą zorientować się co do kraju i charakteru instytucji do której należy dana nazwa domenowa:
Domena najwyższego poziomu jest to część znajdująca się na końcu nazwy domenowej. Wyróżniamy dwie grupy domen najwyższego poziomu: znaczeniowe oraz narodowe. **Domeny znaczeniowe** opisują rodzaj instytucji lub organizacji. Do najczęściej spotykanych należą:
.com – instytucje i firmy o charakterze komercyjnym
.edu – instytucje o charakterze edukacyjnym
.gov – instytucje rządowe
.int – międzynarodowe instytucje rządowe i pozarządowe
.net – instytucje i firmy związane z Internetem
.org – instytucje, organizacje, stowarzyszenia pozarządowe
.mil – instytucje o charakterze wojskowym
Trzy z pośród nich (.edu , .gov , .mil) są zarezerwowane wyłącznie dla organizacji działających na terenie Stanów Zjednoczonych. Organizacje tego typu działające w innych krajach muszą używać kombinacji domen z obu grup dodając na końcu domeny znaczeniowej domenę narodową (np. *www.umwb.**edu.pl***).
Domeny narodowe opisują kraj, na terenie którego znajduje się instytucja. Domena ta składa się zawsze z dwóch liter jednoznacznie identyfikujących kraj. Własną domenę posiada każdy kraj niezależnie od tego czy jest on podłączony do Internetu czy nie (niektóre państwa afrykańskie). W przypadku Stanów Zjednoczonych domena kraju jest często pomijana. Przykładowe domeny narodowe to:
.pl – Polska
.fr – Francja
.ru – Rosja
.de – Niemcy
.uk – Wielka Brytania
Domena drugiego poziomu umieszczana jest przed domeną najwyższego poziomu i oddzielana od niej kropką. Określa ona instytucje, do której należy dany adres domenowy (np. ***microsoft**.com*) lub region którego dotyczy dany adres (np. ***bialystok**.pl*). W przeciwieństwie do domeny najwyższego poziomu stosowane tutaj nazewnictwo nie jest ustandaryzowane i jako domeny drugiego poziomu możemy użyć dowolnej przedmiotowej nazwy. Szczególnym przypadkiem domeny drugiego poziomu są nazwy dublujące 7 domen znaczeniowych najwyższego poziomu (przypadek ten był omówiony wcześniej)
Poddomena jest alternatywnym składnikiem adresu domenowego umieszczanym przed domeną drugiego poziomu. Duże instytucje dysponujące takimi domenami automatycznie uzyskują prawo do zarządzania nimi i tworzenia w ich ramach kolejnych poddomen. Mogą one określać odłamy firmy bądź jednostki organizacyjne (np. ***sklep**.firma.com.pl* lub ***biuro**.firma.com.pl*). Poddomeny mogą być również udostępniane odpłatnie innym instytucjom.
Składnikiem adresu domenowego o najniższym poziomie występującym na początku nazwy domenowej jest nazwa konkretnego komputera bądź usługi którą komputer ten udostępnia (np. ***www**.amb.edu.pl*)

Nie wszystkie komputery muszą posiadać nazwę domenową gdyż jest ona najczęściej przypisywana serwerom udostępniającym w Internecie różnego rodzaju usługi. Najważniejszym zadaniem nazwy domenowej jest ułatwienie nawigacji w sieci przeciętnemu użytkownikowi i odizolowanie go od konieczności zapamiętywania adresów IP. Adresy domenowe zanim zostaną użyte muszą być zarejestrowane i w ten sposób niejako zarezerwowane, aby zapobiec ponownemu ich użyciu przez inne instytucje lub osoby. Są one jednoznacznie tłumaczone na adresy IP przez serwery udostępniające w sieci usługę **DNS** (*ang.* ***Domain Name System***, *system nazw domenowych*). Serwery takie przechowują tablicę translacji znanych im adresów domenowych na adresy IP. W przypadku otrzymania żądania przetłumaczenia adresu sprawdzają ją a jeśli nie znajdują odpowiadającemu żądaniu wpisu rozsyłają żądanie do innych serwerów DNS. W zależności od konfiguracji serwera po otrzymaniu żądanego tłumaczenia, serwer może uzupełnić lub nie swoją tablicę translacji, ale w każdym wypadku zwraca odpowiedź do komputera, od którego żądanie otrzymał. Żądanie translacji wysyłanie jest w momencie użycia adresu domenowego (np. po wpisaniu go do przeglądarki internetowej)

Trzecim elementem składowym sieci komputerowych są **Urządzenia Sieciowe**. Umożliwiają one łączenie mniejszych elementów sieci w większe oraz zarządzają przepływem pakietów tak, aby zminimalizować ruch i obciążenie sieci. Urządzenia sieciowe dają możliwość łączenia ze sobą sieci o różnych topologiach a nawet o różnym zastosowanym w nich medium sieciowym. Istnieje wiele rodzajów urządzeń, my jednak skupimy się na najważniejszych z nich:
Wtórnik (*także* ***regenerator*** *lub* ***wzmacniak*** *ang. repeater***)** - jest to urządzenie wzmacniające sygnał (regeneruje sygnały sieciowe przedłużając w ten sposób odległość na jaką mogą być przesyłane). Na przykład, jeśli jest sieć zrobiona na skrętce UTP kategorii 5 Ethernet to maksymalna długość, na którą można wysyłać dane wynosi 100 metrów. Wtórnik może być użyty do powiększenia tej długości o następne 100 metrów. Szczególnym przypadkiem

Ryc.10 Przykładowy koncentrator z możliwością dołączenia dwóch rodzajów mediów

wtórnika jest **Konwerter** (*ang. Transceiver*) umożliwiający połączenie ze sobą dwóch różnych mediów sieciowych. Wtórnik wyposażony jest w dwa porty, do których podłączamy media sieciowe oraz własne zasilanie. Pracuje w warstwie fizycznej Modelu OSI i nie wnosi żadnych zmian do zawartości przysyłanych przez niego informacji.
Koncentrator *(ang. hub)* - jest urządzeniem podobnym do wtórnika. W zasadzie w wersji aktywnej jest to wieloportowy wtórnik. Koncentratory wysyłają odebrany sygnał na wszystkie swoje porty, powielając w ten sposób otrzymaną porcję danych na wszystkie przyłączone do niego media. W wersji pasywnej sygnał nie jest wzmacniany a jedynie powielany, więc tego typu urządzenia stosuje się zazwyczaj w zastosowaniach domowych. Koncentrator w wersji

aktywnej może być stosowany jako centralne urządzenie sieciowe w małych sieciach o topologii gwiazdy. Ze względu na fakt powielania informacji na wszystkie swoje porty wywołuje dość duże obciążenie sieci ruchem, co eliminuje go z zastosowań w bardziej rozległych sieciach o dużej ilości przyłączonych komputerów. Podobnie jak wtórnik pracuje jedynie w warstwie fizycznej Modelu OSI i ma również możliwość łączenia sieci o różnych mediach sieciowych.

Most *(ang. bridge)* - tworzy dwa lub więcej segmentów sieci. Na bieżąco identyfikuje swoje porty i kojarzy konkretne komputery. Pozwala na podniesienie wydajności i zwiększenie maksymalnych długości sieci. Gdy więc komputer z jednego segmentu wysyła wiadomość, mostek analizuje zawarte w niej adresy i jeśli nie jest to konieczne nie rozsyła jej do innego segmentu. W sieci nie krążą wtedy zbędne pakiety co ogranicza jej obciążenie. Bridge nie potrafi jednak zablokować pakietów uszkodzonych. Operuje nie tylko w warstwie fizycznej ale

Ryc.11 Przykładowy Most w wersji do zamontowania w szafie sieciowej

i łącza danych. Umożliwia chociaż częściowe ograniczenie zbędnego ruchu pomiędzy dwoma sieciami.

Przełącznik *(ang switch)* – podobnie jak mosty służą do separacji segmentów sieci. W przypadku przełączników segment sieci jest jednak najczęściej pojedynczą stacją roboczą co znacznie ogranicza ruch w sieci. Dzięki nim wysyłana informacja jest przesyłana tylko do jej adresata. Przełączniki mają wiele portów (najczęściej stosowane około 32) do których można podłączać komputery oraz inne urządzenia sieciowe w celu rozbudowy sieci. Tak naprawdę można je traktować jako wysoko wyspecjalizowane komputery z dużą ilością kart sieciowych. Oprogramowanie tych komputerów umożliwia bardzo zaawansowane kierowanie ruchem w sieci łącznie z jej wirtualnym podziałem na mniejsze niezależne sieci. Profesjonalne urządzenia tego rodzaju potrafią być bardzo drogie dlatego znajdują zastosowanie w dość rozbudowanych

Ryc.12 Przykładowy Przełącznik z możliwością dokładania modułów

sieciach lokalnych, gdzie istnieje konieczność ograniczenia ruchu ze względu na dużą ilość komputerów. Innym aspektem zastosowania Przełączników jest bezpieczeństwo informacji, która trafia jedynie do adresata, więc nie może być podsłuchana przez inne komputery. Zaawansowane modele przełączników posiadają często gniazda rozszerzeń umożliwiające instalację dodatkowych modułów do obsługi innych rodzajów mediów – na przykład światłowodów. Przełączniki potrafią magazynować odebrane informacje i wysyłać je wtedy, gdy właściwe medium jest na tyle mało obciążone, że istnieje niewielkie ryzyko kolizji z

pakietami wysyłanymi przez inny komputer lub urządzenie sieciowe. Opóźnienie w przesyle jest najczęściej niezauważalne a gwarantuje sprawny przepływ pakietów w sieci. Oczywiście jeśli to tylko możliwe przełącznik wysyła informacje zaraz po ich odebraniu. Ponadto Switch ma możliwość kontroli poprawności pakietów i odrzucania błędnych co dodatkowo eliminuje zbędny ruch w sieci. Tak samo jak most, pracuje w warstwie fizycznej i warstwie łącza danych.
Router - jest to urządzenie, które wyznacza drogę pakietu w sieci. Routery mają fundamentalne znaczenie w sieciach o topologii siatki gdzie do adresata może prowadzić wiele dróg. W sieciach rozległych dane przesyłane są z jednego węzła do konkretnego drugiego, a nie do wszystkich. Do kierowania danych routery używają tzw. tablicę routingu, zawierającą informacje o sąsiadujących routerach i sieciach lokalnych. Służy ona do wyszukania optymalnej drogi od obecnego położenia pakietu do innego miejsca sieci. Tablica

Ryc.13 Przykładowe Routery

routingu może być statyczna lub dynamiczna. Zaletą dynamicznej tablicy routingu jest to, że w wypadku zablokowania sieci z powodu ruchu o dużym natężeniu lub uszkodzenia medium oprogramowanie routera może zaktualizować tablicę, tak aby poprowadzić pakiety drogą omijającą zator. Routery pracują w warstwach fizycznej, łącza danych i sieciowej.

Ze względu na obszar objęty siecią komputerową możemy wyróżnić kilka jej rodzajów:
Sieć lokalna *(ang. Local Area Network* stąd używany także w języku polskim skrót ***LAN)*** - najmniej rozległa postać sieci komputerowej, zazwyczaj ogranicza się do jednego budynku lub kilku pobliskich budynków.
Technologie stosowane w sieciach lokalnych można podzielić na rozwiązanie oparte na przewodach (kable miedziane, światłowody) lub komunikacji radiowej (bezprzewodowe).
W sieciach lokalnych przewodowych najczęściej używaną technologią jest Ethernet (za pośrednictwem skrętki i urządzenia pośredniczącego koncentratora lub switcha). Najczęściej spotykaną obecnie topologią jest topologia gwiazdy. W większych sieciach lokalnych stosuje się również topologię gwiazdy rozgałęzionej. W sieciach lokalnych bezprzewodowych najczęściej używaną technologią jest WLAN, zwany także Wi-Fi.
Sieć miejska *(ang. Metropolitan Area Network* - ***MAN)*** to duża sieć komputerowa, której zasięg obejmuje aglomerację lub miasto. Tego typu sieci używają najczęściej połączeń światłowodowych do komunikacji pomiędzy wchodzącymi w jej skład rozrzuconymi sieciami LAN. Sieci miejskie są budowane przede wszystkim przez duże organizacje rządowe, edukacyjne lub prywatne, które potrzebują szybkiej i pewnej wymiany danych pomiędzy punktami w ramach miejscowości bez udziału stron trzecich. W tego typu sieciach najczęściej spotykaną topologią jest topologia gwiazdy rozgałęzionej oraz rzadziej – siatki. Do technologii używanych przy budowaniu takich sieci należą ATM (oparty na światłowodach) oraz ostatnio Gigabit Ethernet. Tam gdzie niemożliwe jest użycie połączeń światłowodowych często stosuje się bezprzewodowe połączenia radiowe.

Sieć rozległa *(z ang. Wide Area Network - WAN)* - jest to sieć znajdująca się na obszarze wykraczającym poza jedno miasto (bądź kompleks miejski). Łączy ze sobą urządzenia rozmieszczone na dużych obszarach geograficznych (np. kraju, kontynentu). W celu zestawienia łącza lub połączenia między dwoma miejscami korzysta się z usług operatorów. Sieci WAN łączą ze sobą sieci LAN, które są zazwyczaj rozproszone na dużych obszarach geograficznych. Sieci takie budowane są w oparciu o topologię siatki i Wykorzystują różne rodzaje mediów transmisyjnych włączając w to drogę radiową.