Futura – Policealna Szkoła dla Dorosłych w Lublinie

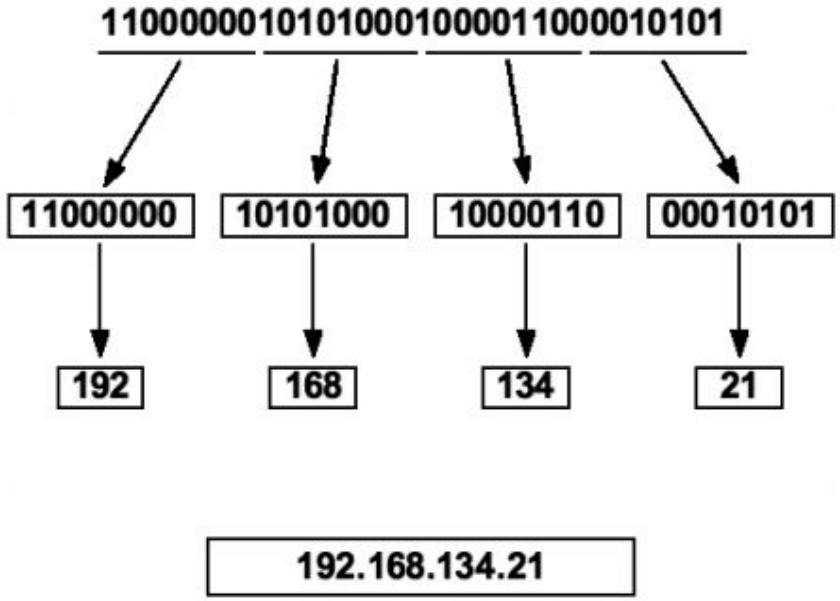
Kierunek: technik informatyk 351203
Semestr: I
Przedmiot: Sieci komputerowe
Nauczyciel: Mirosław Ruciński

Konwertowanie adresów IP na postać binarną

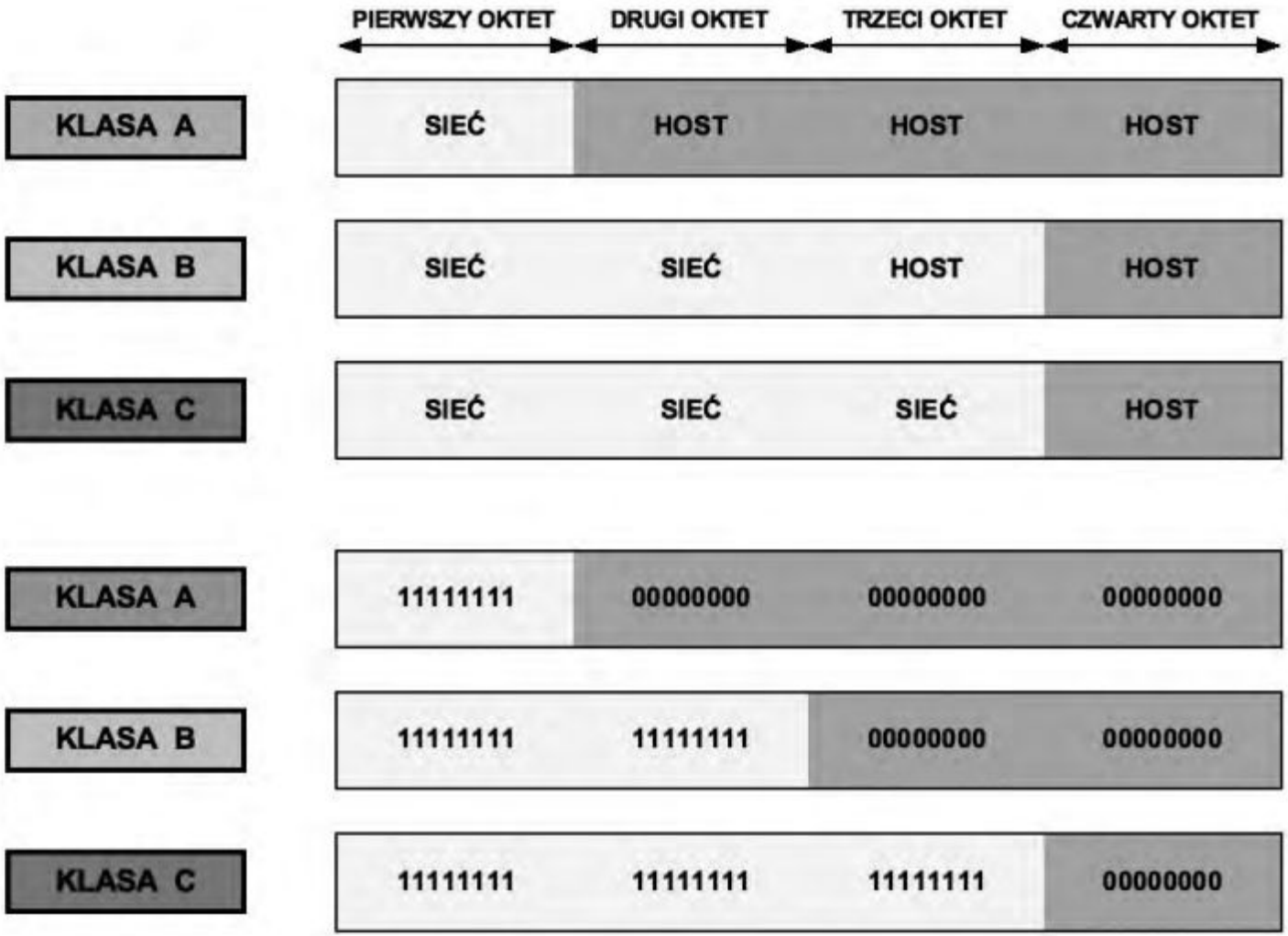
Podział sieci na podsieci

Notacja kropkowo dziesiętna adresu IPv4

32 bitowa liczba binarna adresu IPv4 składa się z cztery grupy liczb dziesiętnych rozdzielonych kropkami, w notacji kropkowo-dziesiętnej.



Standardowe maski podsieci – zapisane w notacji binarnej

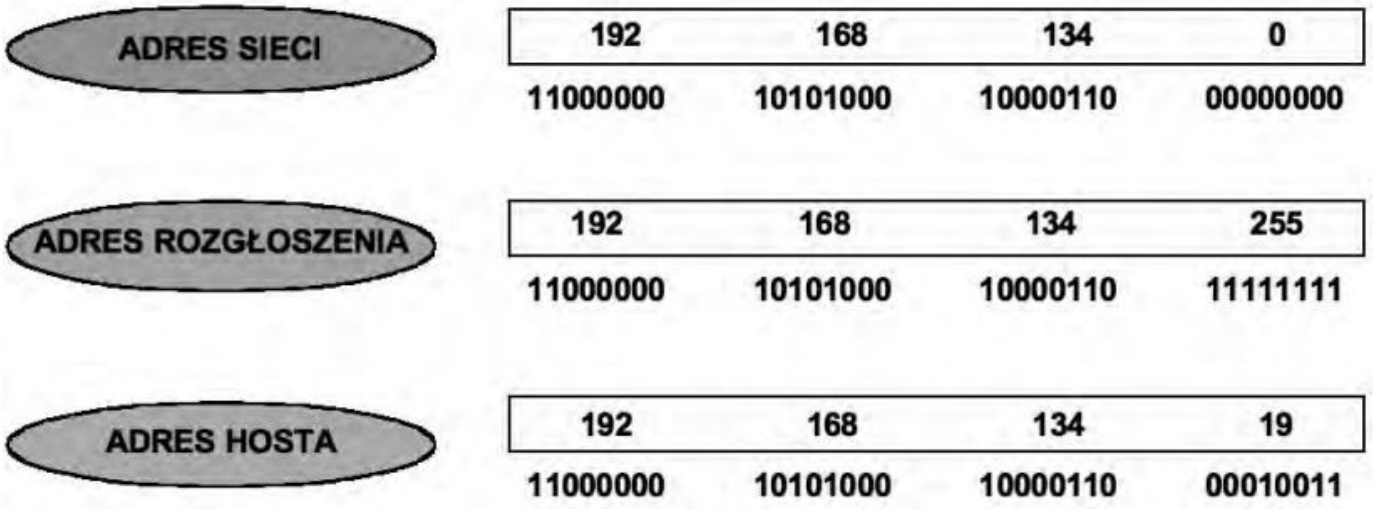


Adresy IP v4 klasy C z maską 255.255.255.0 zapisane w notacji dziesiętno kropkowej i binarnej

Adres sieci – charakteryzuje się tym, że w części hostowej ma same zera.

Adres rozgłoszenia - charakteryzuje się tym, że w części hostowej ma same jedynki.

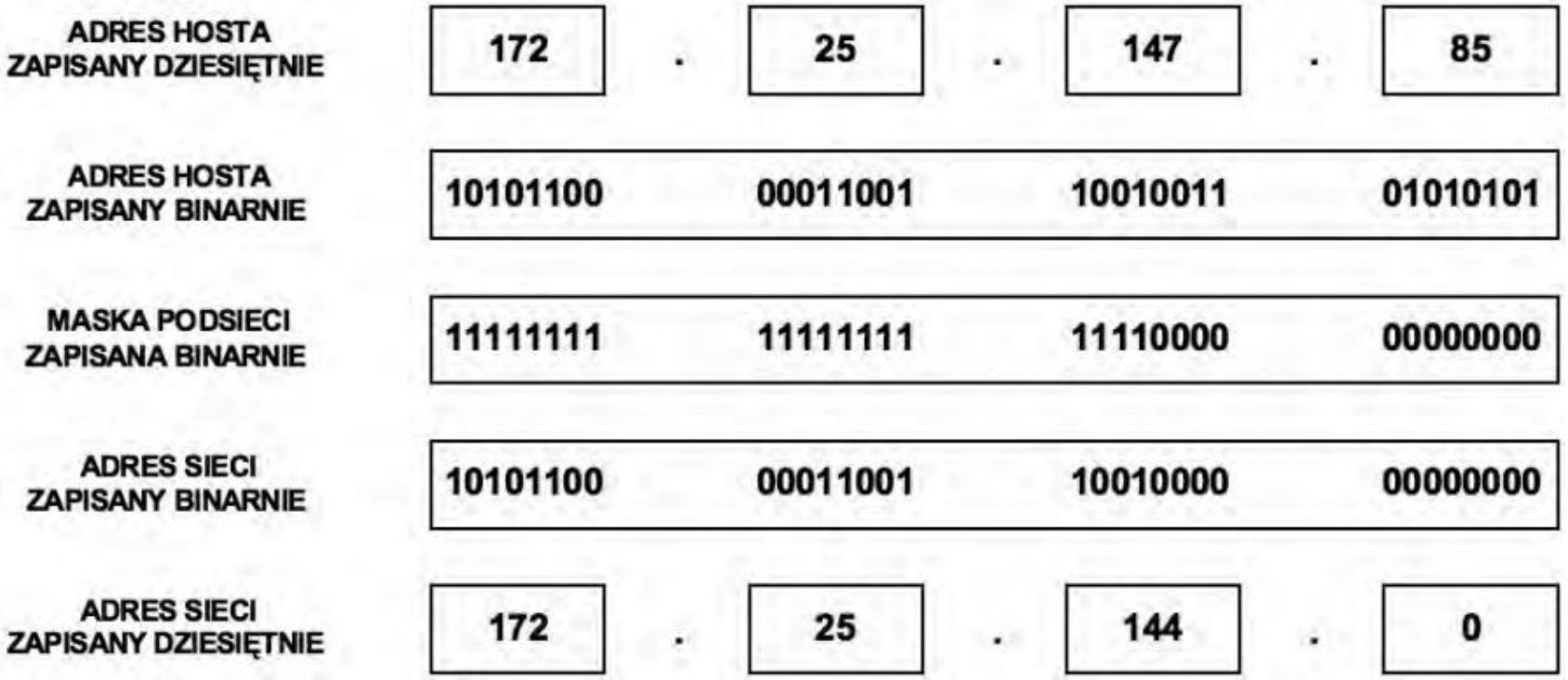
Adres hosta – jest zakresem pomiędzy adresami sieci i adresem rozgłoszenia.



Określenie identyfikatora sieci

Aby określić sieć, do której należy adres IPv4, zamieniamy zapis dziesiętny na binarny. Następnie używając operacji logicznej AND porównujemy odpowiadające sobie bity IP hosta i maski podsieci. Wynik jest równy 1, gdy oba porównywane bity są równe 1, w przeciwnym wypadku wynik jest równy 0.

Host o adresie 172.25.147.85 z maską podsieci 255.255.240.0 Otrzymany identyfikator sieci jest równy 172.25.144. 0



Adresowanie bezklasowe – część maski podsieci z samymi jedynkami określa sieć, część maski określa liczbę sieci do zaadresowania.

Podział na podsieć z maską 25 bitową – można wydzielić 2 podsieci, dla każdej z nich przypisać 126 adresów IP.

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	10000000
	255	255	255	128

Podział na podsieć z maską 26 bitową - można wydzielić 4 podsieci, dla każdej z nich przypisać 62 adresów IP.

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11000000
	255	255	255	192

Podział na podsieć z maską 27 bitową - można wydzielić 8 podsieci, dla każdej z nich przypisać 30 adresów IP.

	SIEĆ	SIEĆ	SIEĆ	HOST PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11100000
	255	255	255	224

Podział na podsieć z maską 28 bitową - można wydzielić 16 podsieci, dla każdej z nich przypisać 14 adresów IP.

	SIEĆ	SIEĆ	SIEĆ	HOST PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11110000
	255	255	255	240

Podział na podsieć z maską 29 bitową - można wydzielić 32 podsieci, dla każdej z nich przypisać 6 adresów IP.

	SIEĆ	SIEĆ	SIEĆ	HOST PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11111000
	255	255	255	248

Podział na podsieć z maską 30 bitową - można wydzielić 64 podsieci, dla każdej z nich przypisać 2 adresów IP.

	SIEĆ	SIEĆ	SIEĆ	HOST PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11111100
	255	255	255	252

Podział na podsieć z maską 31 bitową - można wydzielić 128 podsieci, ale dla każdej z nich nie można przypisać nawet jednego użytecznego adresu IP.

	SIEĆ	SIEĆ	SIEĆ	HOST PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	0000000**0**
MASKA	11111111	11111111	11111111	1111111**0**
	255	255	255	254

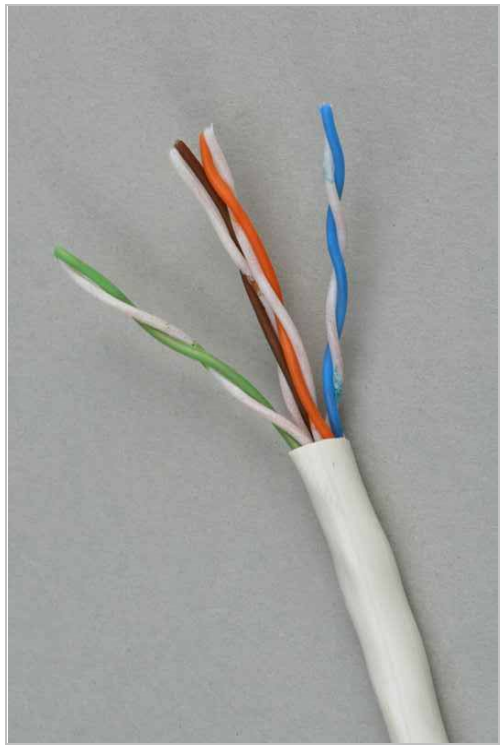
<u>Media transmisyjne.</u>

Skrętka nieekranowana (UTP – Unshielded Twisted Pair)
Skrętka foliowana (FTP – Foiled Twisted Pair)
Skrętka ekranowana (STP – Shielded Twisted Pair)
Kategorie skrętek miedzianych
Kabel światłowodowy
Kabel współosiowy (koncentryczny)

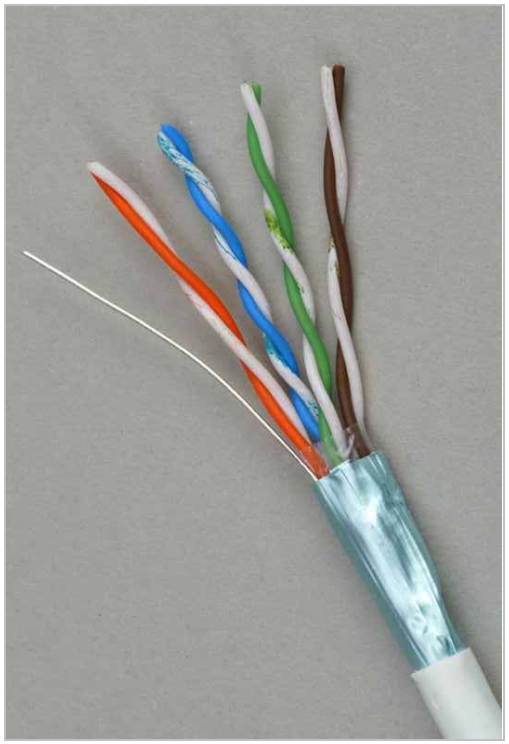
Skrętka - stosowana w standardach **10BASE-T**, **100BASE-T lub 1000BASE-T** to obecnie najpopularniejsze medium transmisyjne sieci LAN. Wyróżniamy skrętkę, **ekranowaną (STP, FTP)** i **nieekranowaną (UTP)**. Różnią się one tym, iż

przewód ekranowany posiada folie lub siatkę metalową ekranującą, więc zapewniają większą odporność na zakłócenia. Powszechnie stosuje się skrętkę UTP.

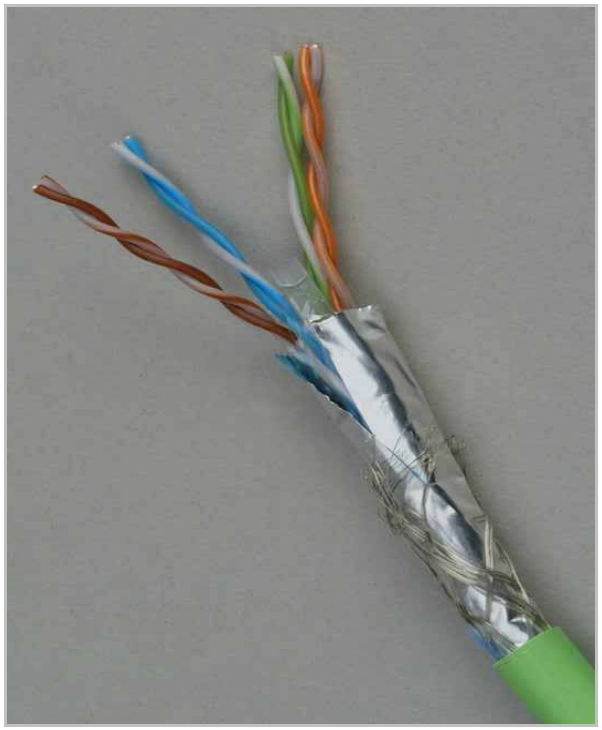
Przepustowość skrętki zależna jest od tzw. **kategorii**. Skrętka kategorii 1 to kabel telefoniczny, kategorii 2 przeznaczona jest do transmisji danych z szybkością 4 Mb/s, kategorii 3 do transmisji o przepustowości do 10 Mb/s, kategorii 4 do 16 Mb/s, kategorii 5 do ponad 100 Mb/s - ten typ ma zastosowanie w szybkich sieciach np. **Fast Ethernet**, natomiast kategorii 6 - 622 Mb/s przeznaczony jest dla sieci **ATM**.



"UTP"
Unshielded Twisted Pairs
Nieekranowana skrętka



"FTP"
Foiled Twisted Pairs
Ekranowana folią skrętka



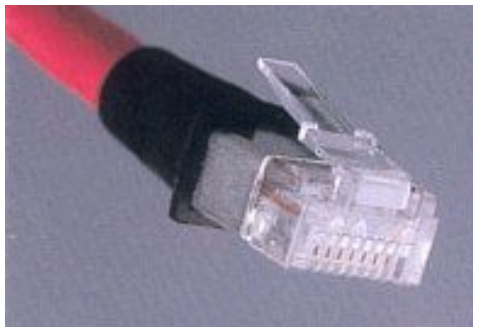
"SFTP"
Shielded Foiled Twisted Pairs
Ekranowana i foliowana skrętka

Maksymalna długość połączeń dla UTP wynosi 100 m, natomiast dla STP 250 m. Limit ten można oczywiście przekroczyć używając **repeatera**. Obydwa rodzaje skrętki posiadają **impedancję** 100 ohmów.

Sieć oparta na skrętce z odległą stacją.

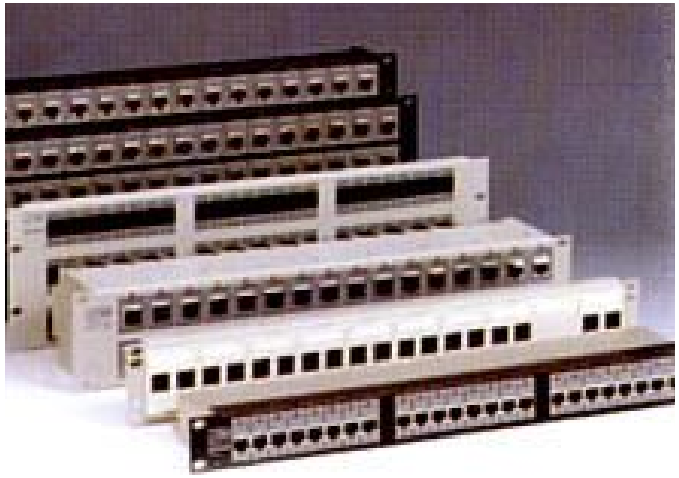
W sieciach opartych na skrętce podobnie jak w pozostałych okablowaniach standardu **Ethernet** obowiązuje zasada, iż sygnał może przejść tylko przez 4 repeatery.

Do karty sieciowej skrętkę przyłączą sie za pomocą złącza RJ-45.



Złącze RJ-45

Skrętkę stosuje się przede wszystkim w sieciach o **topologii gwiazdy**. Instalacja okablowania jest bardzo prosta dzięki zastosowaniu połączeń zaciskowych. W celu zmniejszenia awaryjności sieci, zaleca sie stosowanie tzw. **paneli przyłączeniowych** (krosownic).



Krosownice

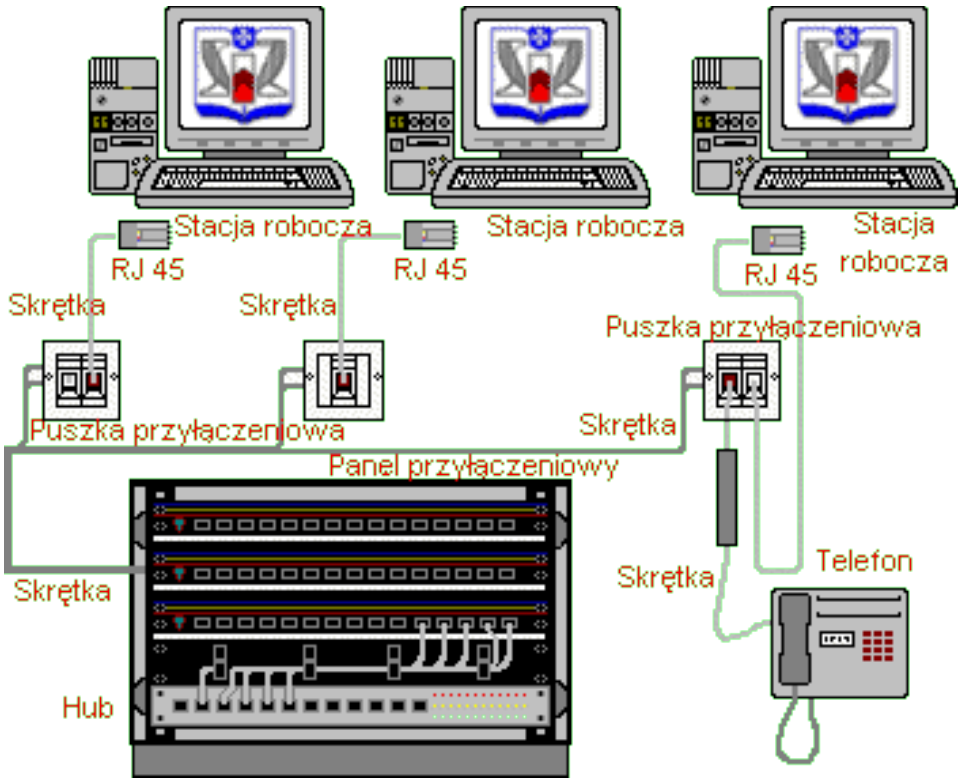
Dla większości zastosowań nieekranowane okablowanie UTP kat 5 jest wystarczające. Skrętkę ekranową stosujemy w:

- środowisku z dużym poziomem zakłóceń elektromagnetycznych (np. lotniska)
- środowiska wrażliwe na emisję pochodzącą z okablowania informatycznego (np. laboratoria, szpitale)
- budynki, w których istnieje potrzeba zapewnienia zgodności elektromagnetycznej według międzynarodowych lub lokalnych regulacji prawnych.

Ogromną zaletą skrętki jest też uniwersalność, można ją stosować dla różnych typów sygnałów, np. informatycznych i

telefonicznych. Skrętkę stosuje sie także w nowych sieciach Fast Ethernet (100BASE-T) i **Gigabit Ethernet** (1000BASE-T).

W przypadku przejścia z technologii Ethernet na Fast Ethernet okablowanie nie musi być zmieniane. Skrętka jest tania i prosta w ułożeniu. Wadą jest duża ilość kabli potrzebna do wykonania sieci oraz niska odporność na zakłócenia. Skrętkę stosuje sie powszechnie w **okablowaniu poziomym** na krótkich odcinkach i w środowiskach o niskim poziomie zakłóceń.

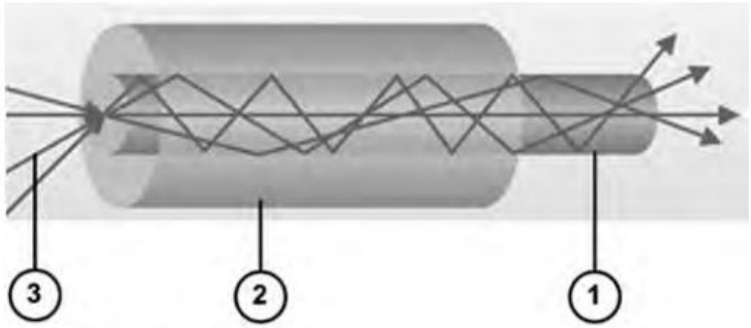


Przykład wykonania sieci LAN w topologii gwiazdy z zastosowaniem przewodu UTP kat 5

Światłowód - W światłowodach do transmisji informacji wykorzystywana jest **wiązka światła**, która jest odpowiednikiem prądu w kablach miedzianych. Wiązka ta jest modulowana zgodnie z treścią przekazywanych informacji. Właściwie dobrany kabel może przebiegać w każdym środowisku. Szybkość transmisji może wynosić nawet 3 Tb/s. Sieci oparte na światłowodach zwane są **FDDI.**
Światłowód wykonany ze ***szkła kwarcowego***, składa się z ***rdzenia*** (złożonego z jednego lub wielu włókien), okrywającego go ***płaszcza*** oraz ***warstwy ochronnej***. ***Dielektryczny*** kanał informatyczny eliminuje konieczność ekranowania.

Transmisja światłowodowa polega na przepuszczeniu przez ***szklane włókno wiązki światła*** generowanej przez ***diodę lub laser***. Wiązka ta, to zakodowana informacja binarna, rozkodowywana następnie przez ***fotodekoder*** na końcu kabla. Światłowód w przeciwieństwie do kabli miedzianych, nie wytwarza pola elektromagnetycznego, co uniemożliwia podsłuch transmisji. Główną wadą tego medium jest łatwa możliwość przerwania kabla oraz mała odporność na zginanie. Można wyróżnić światłowody do połączeń zewnętrznych i wewnętrznych oraz wielomodowe i jednomodowe. Rdzeń kabla otoczony jest specjalnym oplotem oraz odporną na wilgoć i promienie słoneczne polietylenową koszulką zewnętrzną. Kable ***wewnętrzne*** przeznaczone są do układania wewnątrz budynku. Posiadają cieńszą warstwę ochronną i nie są tak odporne jak kable zewnętrzne. Światłowody ***wielomodowe*** przesyłają wiele modów (fal) o różnej długości co powoduje rozmycie impulsu wyjściowego i ogranicza szybkość lub odległość transmisji. Źródłem światła jest tu dioda LED. Światłowody ***jednomodowe*** są efektywniejsze i pozwalają transmitować dane na odległość 100 km bez wzmacniacza. Jednak ze względu na wysoki koszt interfejsów przyłączeniowych jest to bardzo drogie rozwiązanie. Źródłem światła jest tu laser.

Budowa światłowodu jednomodowego

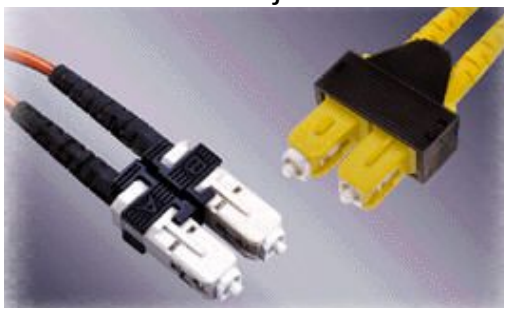


1 – rdzeń
2 – płaszcz
3 – wiele promieni światła

Rozchodzenie się promieni świetlnych w światłowodzie wielodomowym.

Światłowód to włókno szklane z centralnie umieszczonym rdzeniem przewodzącym światło, otoczonym cylindrycznym płaszczem odbijającym promienie świetlne i zewnętrzną powłoką lakierniczą, nadającą włóknu odpowiednią odporność i wytrzymałość mechaniczną. Rdzeń wykonany ze szkła krzemionkowego SiO 2, czyli tzw. szkła kwarcowego. Płaszcz otaczający rdzeń jest wykonany z czystego szkła kwarcowego.

Do karty sieciowej światłowód przyłącza się za pomocą złącza ***fiber connector***. Może ono wyglądać różnie, w zależności od rodzaju.

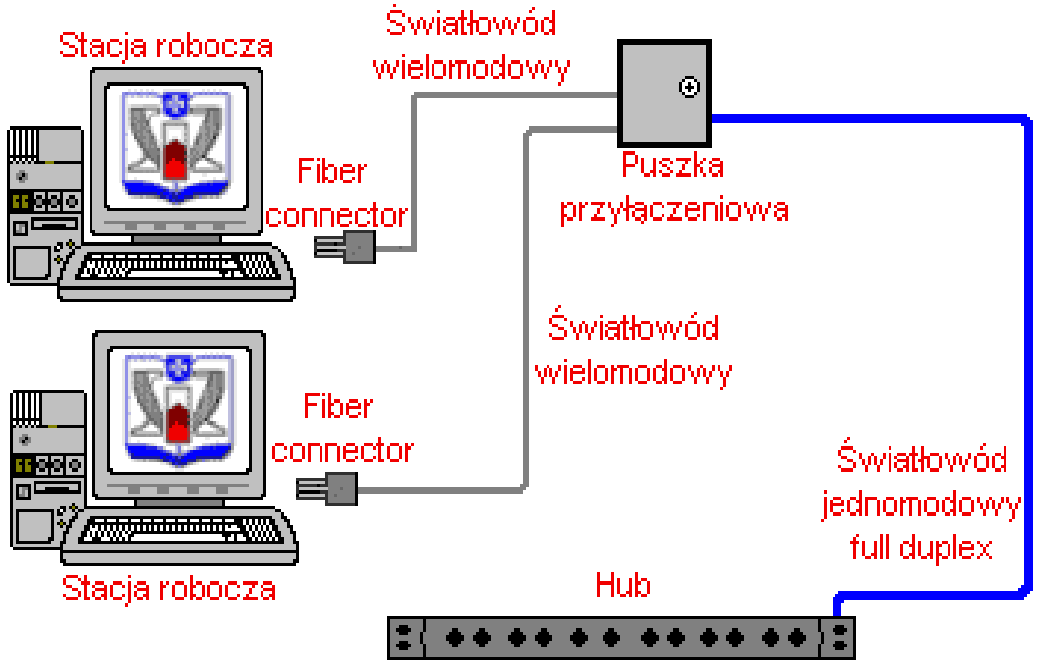


Złącza fiber connector full duplexowe wielomodowe

Światłowody umożliwiają stosowanie wielu ***protokołów*** jednocześnie co zapewnia wysokoefektywny transfer danych, przepływ danych jest zabezpieczony przed niepowołanym dostępem - nie wytwarzają własnego pola magnetycznego w

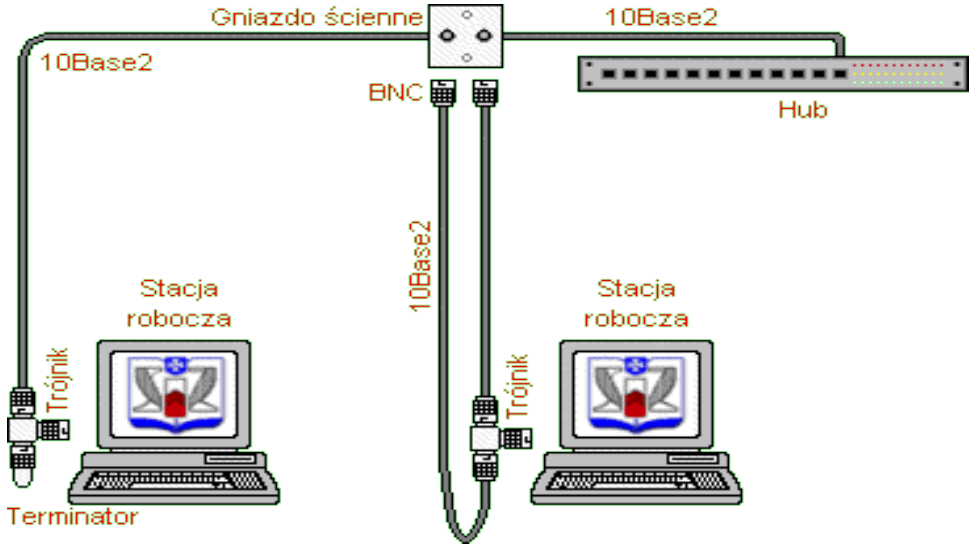
związku z czym niemożliwe jest podsłuchanie transmisji, długość światłowodu jest praktycznie niegraniczona i zależy wyłącznie od parametrów tłumienościowych kabla w porównaniu do innych kabli światłowody zapewniają minimalne straty sygnału . ***Do wad zaliczyć należy złożoność*** instalacji - wymagane jest stosowanie kosztownych, specjalistycznych narzędzi oraz bardzo wysoką cenę nie tyle samego kabla, ale i urządzeń dostępowych i montażowych.

Światłowody stosuje się w dużych sieciach ***lokalnych*** *i* ***metropolitarnych***, wymagających długich odcinków połączeniowych, w środowiskach o średnim i dużym poziomie zakłóceń elektromagnetycznych oraz w połączeniach wymagających wysokiej niezawodności, np. serwerów do sieci.Przykład zastosowania kabla światłowodowego.



Przewód koncentryczny – stosowany jest w sieci typu **magistrala,** standard **10 Base 2**, **10 Base 5** w oparciu o ten standard należy stosować gniazda typu BNC, trójniki do podłączenia poszczególnych stacji roboczych oraz terminatory na końcach przewodów. Instalacja terminatorów jest bardzo ważna, jego uszkodzenie doprowadza do awarii całej sieci. Podstawowe zalety cienkiego Ethernetu (10 Base -2) to niski koszt i prostota instalacji. Głównea wady to: ograniczona współpraca z nowoczesnymi technologiami - medium to działa tylko przy prędkości do 10 Mb/s, nieodporność na uszkodzenia - przerwanie okablowania w dowolnym miejscu powoduje paraliż całej sieci, słaba skalowalność - rozbudowa sieci jest stosunkowo niewygodna. Poza tym różne rodzaje 10BASE2 mają różne właściwości elektryczne i dlatego mogą być ze sobą niekompatybilne.

Przewód koncentryczny RG58, linka, impedancja 50Ω, średnica zewnętrzną 5mm. (miedziana linka 1,1mm)



Wi-Fi Fale radiowe

Sieci bezprzewodowe opierają się na standardach IEEE 802 opierają się ona na protokołach kodowania a,b,g i n. Technologia Wi-Fi polega na bezprzewodowej łączności w dwóch częstotliwościach 2,4 GHz lub 5 GHz. Stosowane są urządzenia działające w obu tych pasmach jednocześnie.

Standardy sieci bezprzewodowych

Nazwa standardu	Częstotliwość radiowa	Zasięg sygnału	Maksymalna szybkość transmisji
802.11b	2.4 GHz	30 metrów	11 Mb/s
802.11a	5 GHz	30 metrów	54 Mb/s
802.11g	2.4 GHz	30 metrów	54 Mb/s
802.11n	2.4 GHz	50 metrów	540 Mb/s
802.15.1 Bluetooth	2.4 GHz	10 metrów	2 Mb/s

IEEE 802.11ac przepustowość przy zastosowaniu wielu stacji ma być na poziomie przynajmniej **1 Gbit/s** Urządzenia standardu 802.11ac pracują na częstotliwości 5 GHz. Prace nad specyfikacją zostały ukończone w grudniu 2013 roku a zatwierdzenie standardu nastąpiło w styczniu 2014 roku.

W Polsce używa się 14 kanałów. Dokładna częstotliwość stosowana w określonej sieci zależy od wykorzystywanego kanału transmisyjnego, ustawionego podczas konfiguracji AP.

Kanały transmisyjne

Urządzenia sieciowe.

Karta sieciowa - Jest to urządzenie wymagane we wszystkich stacjach roboczych przyłączonych do sieci. Każda karta jest przystosowana tylko do jednego typu sieci i posiada niepowtarzalny numer, który identyfikuje zawierający ją komputer. Przydziela go międzynarodowa instytucja pod nazwą **IEEE**. Każdemu producentowi przypisuje ona odpowiedni kod i zakres liczbowy. **MAC (Media Access Control)** – Jest to unikalny 48 bitowy adres karty sieciowej zapisany w systemie szesnastkowym Np. **00:0E:90:C4:56:87** Gdzie pierwsze 24 bity oznaczają producenta danej karty czyli w naszym przypadku oznaczenie producenta to **00:0E:90** a kolejne 24 bity czyli **C4:56:87** są unikalnym numerem seryjnym danej karty sieciowej. Oczywiście to tylko przykład wymyślonego adresu na potrzeby tego artykułu. Pełną listę producentów kart sieciowych oraz

przypisanych im identyfikatorów można zobaczyć pod adresem http://standards.ieee.org/regauth/oui/oui.txt – Instytut Inżynierów Elektryków i Elektroników (IEEE).

Istnieją karty sieciowe przystosowane do magistrali **ISA**,**PCI**,**PCI-E** jak i karty zewnętrzne łączone przez porty np. USB. Obecnie karty sieciowe posiadają własny procesor i pamięć RAM. Procesor pozwala przetwarzać dane bez angażowania w to głównego procesora komputera, a pamięć pełni rolę bufora w sytuacji, gdy karta nie jest w stanie przetworzyć napływających z sieci dużych ilości danych. Są one wtedy tymczasowo umieszczane w pamięci. Na karcie sieciowej znajduje sie złącze dla medium transmisyjnego. Obecnie najpopularniejsze są wtyczki **RJ-45** stosowane do gniazd **P8C8**.

Głównym zadaniem karty sieciowej jest **transmisja** i **rozszyfrowywanie informacji** biegnących łączami komunikacyjnymi. Przesyłanie danych rozpoczyna się od uzgodnienia parametrów transmisji pomiędzy stacjami (np. prędkość, rozmiar pakietów). Następnie dane są przekształcane na sygnały elektryczne, kodowane, kompresowane i wysyłane do odbiorcy. Jego karta dokonuje ich **deszyfracji** i **dekompresji**. Tak więc karta odbiera i zamienia pakiety na bajty zrozumiałe dla procesora stacji roboczej. Współczesne karty posiadają programowalną pamięć **Remote Boot PROM** służącą do startu systemu z serwera sieci, a nie jak dawniej z dyskietki. Jest to rozwiązanie o wiele szybsze i bezpieczniejsze. Przesyłanie informacji z karty do systemu może się odbywać na cztery różne sposoby:

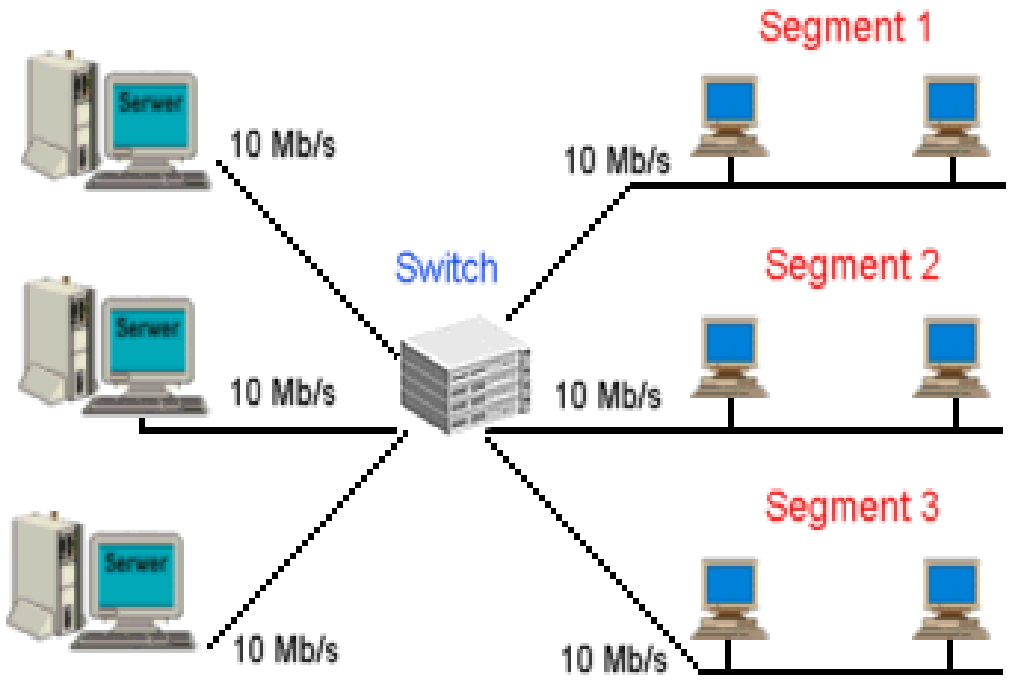
1. Bezpośredni dostąp do pamięci (DMA). Dane przesyłane są dzięki kontrolerowi DMA do pamięci, nie obciążając procesora.
2. Współdzielona pamięć karty (SAM). Dane umieszczane są we własnej pamięci karty. Procesor uznaje ją za część pamięci operacyjnej komputera.
3. Współdzielona pamięć komputera (SSM) Dane umieszczane są w wydzielonej części pamięci operacyjnej komputera, do której ma dostęp także procesor karty sieciowej.
4. Bus mastering. Najszybszy sposób przesyłania danych, ulepszona forma DMA. Karta przejmuje kontrolę nad szyną danych komputera i wpisuje dane bezpośrednio do pamięci nie obciążając procesora.

Karta sieciowa złącza PCI- E złącze Ethernet RJ45 P8C8

Switch - Nazywany jest również **przełącznikiem** lub **hubem przełączającym**.
Switche stosuje się zwykle w sieciach opartych na **skrętce**. Są urządzeniem służącym do przyłączania stacji przede wszystkim w **topologii gwiazdy**, a także do rozładowania ruchu w sieci i wyeliminowania **kolizji**.
Posiadają kilka **portów** do podłączenia stacji końcowych, innych przełączników, bądź hubów.

Cisco switch

Switche umożliwiają zmniejszenie obciążenia w sieci, poprzez jej podział na **mikrosegmenty** i tzw. **przełączanie (komutowanie)**. Polega to na tym, iż do jednego segmentu można przydzielić zaledwie jedną stacje roboczą, co znacznie redukuje rywalizację o dostęp do medium. Użytkownik otrzymuje całą szerokość pasma dla siebie. Każdy port switcha stanowi wejście do jednego segmentu sieci. W efekcie pracy, przykładowo przełącznika posiadającego 10 portów, jest uzyskanie 10 niezależnych segmentów z całą szerokością pasma (np. pełnych 10 Mbps w przypadku 10Base-T).



Sieć jest podzielona na 3 segmenty i każdy serwer ma dostępne pełne pasmo transmisji

Nowoczesne, inteligentne switche posiadają dwa tryby przełączania: **fast forward** (zwany też cut-through) i **store and foreward**. W fast forward odebrana **ramka** jest wysyłana natychmiast po otrzymaniu adresu docelowego. Powoduje to, iż mogą zostać wysłane ramki z błędami lub biorące udział w kolizji.
W store-and-foreward ramka jest sprawdzana pod kątem sumy kontrolnej. Eliminowane są ramki błędne i biorące udział w kolizjach. Wadą tego trybu są jednak dość duże opóźnienia w transmisji.
Inteligentne przełączanie polega na tym, że standardowo przełącznik pracuje w trybie fast forward, a gdy liczba błędów przekracza kilkanaście na sekundę, zaczyna automatycznie stosować metodę store-and-foreward. Gdy liczba błędów spada poniżej tego poziomu, przełącznik powraca do trybu fast forward. Dodatkową i coraz ważniejszą cechą przełączników wyższej klasy jest możliwość budowania **sieci wirtualnych VLAN**. Oznacza to możliwość definiowania logicznych grup stacji

roboczych, które mogą komunikować się ze sobą tak, jakby znajdowały się w jednej sieci lokalnej, niezależnie od ich fizycznej lokalizacji i od fizycznej struktury połączeń. Sieci wirtualne pozwalają na tworzenie bezpiecznych grup roboczych, zwiększenie efektywnej przepustowości sieci i rozdzielanie ruchu broadcastowego.

Switch IBM 8285 Nways ATM

Nowy model z serii bardzo wydajnych switchów firmy IBM przeznaczonych dla standardu szybkich sieci ATM. Oferuje 12 portów ATM (rozszerzalnych do 48) o przepustowości 25 Mb/s i jeden 155 Mb/s , pełni rolę routera, potrafi emulować standardy Token Ring i Ethernet, umożliwia kompleksową obsługę dużych sieci. Jest zalecany przy prowadzeniu wideokonferencji.

Router - To najbardziej zaawansowane urządzenie stosowane do łączenia **segmentów sieci** i zwiększania jej fizycznych rozmiarów. Router jest urządzeniem **konfigurowalnym**, pozwala sterować **przepustowością** sieci i zapewnia pełną **izolację** pomiędzy segmentami.

Funkcje routera są podobne do **mostu**. Różnica polega na tym, iż routery są używane do przekazywania danych pomiędzy sieciami opartymi na różnych technologiach oraz na większym zaawansowaniu technicznym. Routery są integralną częścią Internetu, gdyż składa się on z wielu sieci opartych na różnych technologiach sieciowych.

W sieciach rozległych dane przesyłane są z jednego **węzła** do konkretnego drugiego, a nie do wszystkich. Po drodze napotykają na wiele węzłów pośredniczących, mogą też być transmitowane wieloma różnymi trasami. Router jest jednym z tych węzłów, który ma za zadanie przesłać dane najlepszą (najszybszą) trasą.

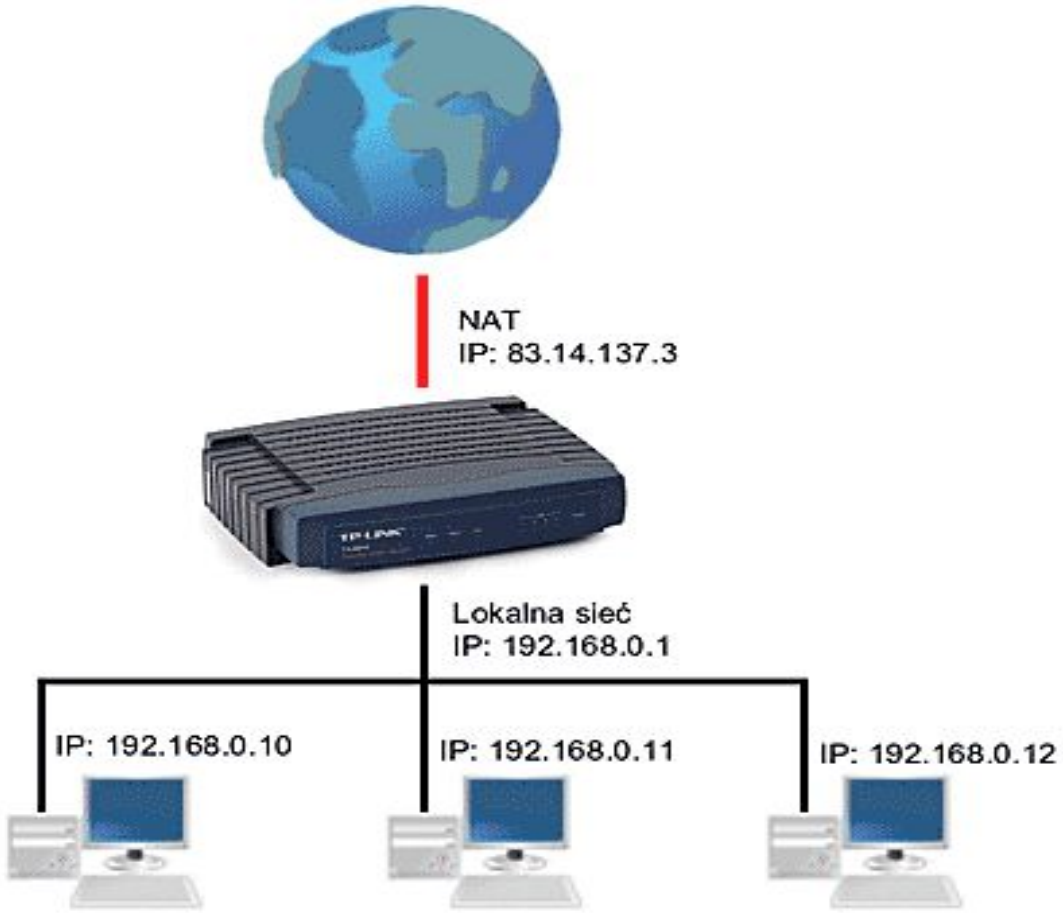
Do kierowania danych routery używają tzw. **tablicę routingu,** zawierającą informacje o sąsiadujących routerach i sieciach lokalnych. Służy ona do wyszukania optymalnej drogi od obecnego położenia **pakietu** do innego miejsca sieci. Tablica routingu może być **statyczna** lub **dynamiczna,** zależy to od postawionych wymagań. Statyczna musi być aktualizowana ręcznie przez administratora sieci, dynamiczna natomiast jest aktualizowana automatycznie przez oprogramowanie sieciowe. Zaletą dynamicznej tablicy routingu jest to, że w wypadku zablokowania sieci z powodu ruchu o dużym natężeniu oprogramowanie sieciowe może zaktualizować tablicę, tak aby poprowadzić pakiety drogą omijającą zator.

Komunikacja w sieci z routerem oparta jest na **adresacji logicznej**, co pozwala np. na fizyczne umiejscowienie adresata. Każdy segment sieci musi mieć wlasny **adres sieciowy**, podobnie jak i każdy komputer. Informacje o nich umieszczane są w pakietach.
Routery funkcjonują na poziomie **warstwy sieciowej**, maję więc szerokie możliwości.

Do ich głównych zalet zaliczyć można:

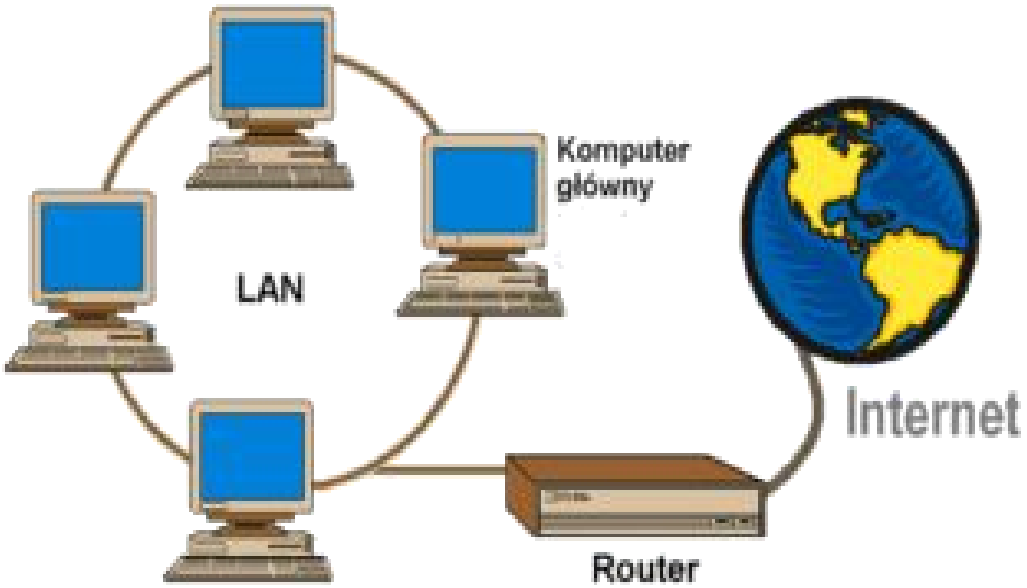
- wybór optymalnej trasy między nadawcą a odbiorcą,

- ochrona (zapory, kodowanie),
- transakcja protokołów (łączenie różnych segmentów o różnych protokołach),
- filtrowanie pakietów (sortowanie i selekcja transmitowanych pakietów),
- usuwanie pakietów bez adresu.



Router

Routery pełnia także funkcje tzw. **firewalli**.



Router, jako firewall

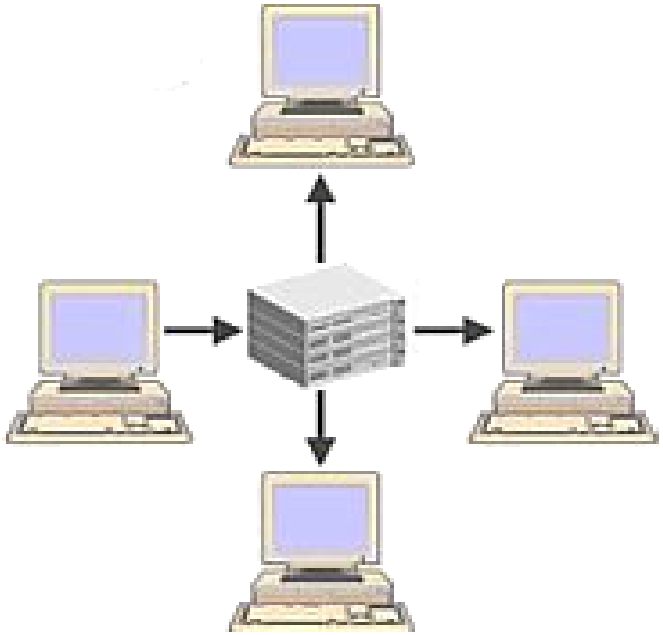
Na rysunku router łączy sieć lokalną z Internetem i filtruje określone typy pakietów. Należy go tak skonfigurować, aby widoczny dla niego był tylko jeden komputer główny. Wszyscy użytkownicy **LAN** przy dostępie do Internetu korzystają z pośrednictwa tego komputera, a użytkownicy Internetu mają dzięki niemu ograniczony dostęp do sieci lokalnej.

Rozmiar sieci opartej na routerze nie jest limitowany jak np. w przypadku bridge'a. Jest też szybszy, z reguły potrafi przesłać kilkanaście tysięcy pakietów na sekundę (bridge maksymalnie 10 tys.) i sieć na jego bazie jest prostsza w utrzymaniu od sieci na bazie bridge'ów.

Hub - Nazywany jest również **koncentratorem, multiportem** lub **multiplekserem**.
Jest to urządzenie posiadające wiele **portów** służących do przyłącznia stacji roboczych zestawionych przede wszystkim w **topologii gwiazdy.**

Hub 8-portowy

W zależności od liczby komputerów przyłączonych do sieci może się okazać konieczne użycie wielu hubów. W sieci takiej nie ma bezpośrednich połączeń pomiędzy stacjami . Komputery podłączone są przy pomocy jednego kabla do centralnego huba, który po nadejściu sygnału rozprowadza go do wszystkich linii wyjściowych.



Hub w sieci. Informacja z jednej stacji jest rozsyłana do pozostałych.

Dużą zaletą takiego rozwiązania jest fakt, iż przerwanie komunikacji między jednym komputerem a hubem nie powoduje awarii całej sieci, ponieważ każda stacja posiada z nim oddzielne połączenie. Ponadto każdy **pakiet** musi przejść przez hub, więc możliwa jest kontrola stanu poszczególnych odcinków sieci. Jednak uszkodzenia huba unieruchomi całą sieć.

Można wyróżnić huby **pasywne** i **aktywne**.
Hub pasywny jest tanim urządzeniem pełniącym funkcję skrzynki łączeniowej, nie wymaga zasilania.

Hub aktywny dodatkowo wzmacnia sygnały ze stacji roboczej i pozwala na wydłużenie połączenia z nią. Zasilanie jest wymagane.

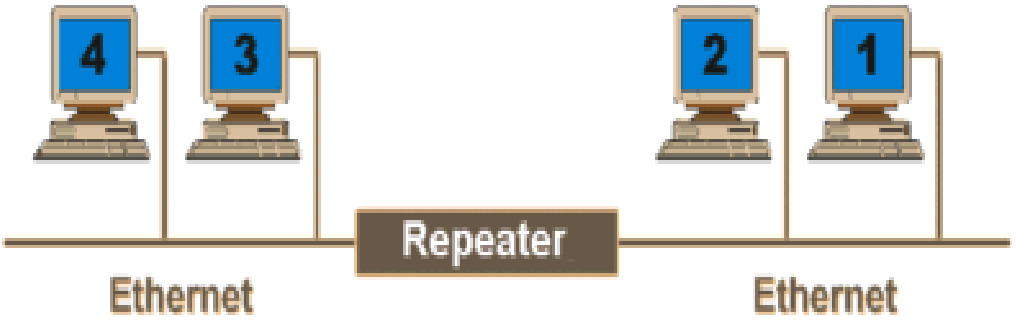
Najczęstszym rodzajem kabla łączącego komputer i hub jest **skrętka** . Huby potrafią jednak dokonać konwersji sygnału pochodzącego z różnych mediów transmisyjnych. Dostosowują się też do różnych standardów sieciowych jak np. **Ethernet**, **Token Ring**, **ATM**.

Repeator - Nazywany jest również **wzmacniakiem lub regeneratorem**.
Informacja przesyłana kablem ulega zniekształceniom proporcjonalnie do jego długości. Jednym z urządzeń, które wzmacnia i regeneruje sygnały przesyłane kablem jest repeater. Tak więc repeater służy do fizycznego zwiększania rozmiarów sieci . Zwykle zawierają one kilka wzmacniaków.

Repeater 4-portowy

Repeater powtarza (kopiuje) odbierane sygnały i wzmacnia sygnał . Polega to na zwiększeniu poziomu odbieranego przebiegu falowego bez zmiany jego częstotliwości. Jest to najprostsze urządzenie tego typu. Może łączyć tylko sieci a takiej

samej architekturze, używające tych samych **protokołów** i technik transmisyjnych. Potrafi jednak łączyć **segmenty sieci** o różnych mediach transmisyjnych.



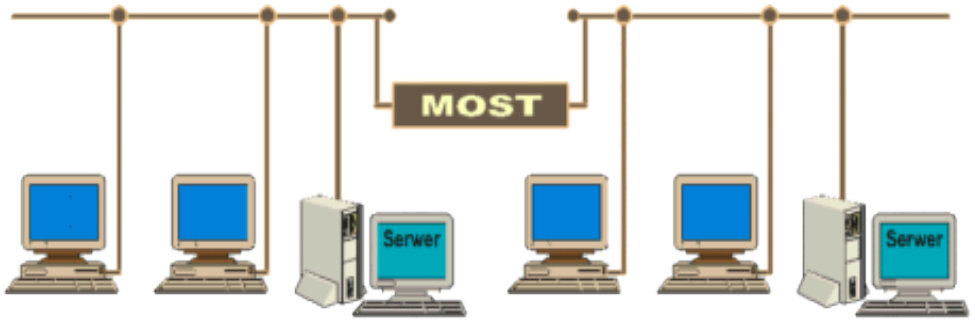
Sieć z repeaterem

Instalacja repeatera jest bardzo prosta, nie wymaga on żadnej konfiguracji i jest przeźroczysty dla innych urządzeń sieciowych. Traktowany jest jako węzeł w każdym z przyłączonych do niego segmentów. Repeater dostosowuje się do do prędkości transmisji w sieci i przekazuje pakiety z taką samą szybkością, co powoduje, że jest wolniejszy od np. **bridge'a**.

Bridge - czyli **mostek** to urządzenie posiadające 2 lub więcej **portów**, służące do łączenia **segmentów sieci**. Na bieżąco identyfikuje swoje porty i kojarzy konkretne komputery. Pozwala na podniesienie wydajności i zwiększenie maksymalnych długości sieci.

Bridge ze złączem AUI

Bridge sa proste w instalacji, nie wymagają konfiguracji. Są urządzeniami wysoce elastycznymi i adaptowalnymi - przy dodawaniu nowego **protokołu** potrafią automatycznie dostosować się.
Zapewniają proste **filtrowanie**, odczytują adres zapisany w **ramce** np. **sieci Ethernet** i określają do jakiego segmentu należy przesłać dany **pakiet**. 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.



Sieć z bridgem.

Bridge nie potrafią jednak zablokować pakietów uszkodzonych, ani przeciwdziałać **zatorom**, powstałym gdy wiele stacji

roboczych usiłuje naraz rozsyłać dane w trybie broadcastowym. Bridge mogą przesyłać pakiety wieloma alernatywnymi drogami i może zdarzyć się, że na dwóch różnych interfejsach pojawi się ta sama informacja i pakiety będą krążyć po sieci w nieskończoność. Może to spowodować powstanie **sztormów broadcastowych** i zakłócenie pracy sieci.

Mosty posiadają technikę uczenia się. Zaraz po dołączeniu do sieci wysyłają sygnał do wszystkich **węzłów** z żądaniem odpowiedzi. Na tej podstawie oraz na analizie przepływu pakietów, tworzą **tablicę adresów fizycznych** komputerów w sieci. Przy przesyłaniu danych bridge odczytuje z tablicy położenie komputera odbiorcy i zapobiega rozsyłaniu pakietów po wszystkich segmentach sieci.

Urządzenia te wykorzystuje sie również do poprawienia niezawodności sieci, co polega na podziale dużych sieci na mniejsze segmenty. Uszkodzony kabel czy węzęł może doprowadzić do unieruchomienia całej sieci, tak więc podział pojedynczej sieci lokalnej na kilka mniejszych sieci połączanych ze sobą za pośrednictwem mostu zmniejsza wpływ uszkodzonego kabla lub węzła na funkcjonowanie całej sieci.

W sieci może pracować wiele mostów, ale każdy musi pamiętać adresy wszystkich węzłów, nie tylko tych, które są do niego przyłączone. Jeśli więc stacja A z sieci LAN 1 chce wysłać komunikat do stacji C z sieci LAN 3, to most 1 musi wiedzieć jak przesłać dane zarówno do sieci LAN 2 jak i LAN 3. Most 2 pośredniczy w przekazaniu danych do LAN 3.

Literatura:

Urządzenia techniki komputerowej – Tomasz Kowalski
Sam składam komputer – Bartosz Danowski, Andrzej Pytchla
Wikipedia- wolna encyklopedia internetowa

Strona internetowa:

http://standards.ieee.org/regauth/oui/oui.txt
http://itpedia.pl/index.php/LAN#Sposoby_transmisji_i_adresowania_w_LAN
http://www.bryk.pl/teksty/liceum/pozosta%C5%82e/informatyka/15947-protoko%C5%82y_sieciowe.html
http://sieci.res.pl/%21start.htm

http://informatykaplus.edu.pl/upload/list/czytelnia/Komunikacja_w_sieciach_komputerowych.pdf

Opracował Mirosław Ruciński
e-mail: nauczyciel.zsen@gmail.com