Kierunek: technik informatyk 312[01]

Semestr: II
Przedmiot: Urządzenia techniki komputerowej
Nauczyciel: Mirosław Ruciński

Temat 2. <u>Sieci komputerowe.</u>

Cele kształcenia: Rodzaje sieci komputerowych. Metody transmisji w sieciach. Topologie sieci komputerowych. Karty sieciowe: budowa, zasada działania, rodzaje. Urządzenia sieciowe, przeznaczenie i ich parametry. Podstawowe standardy sieci komputerowych. Budowa i zasada działania modemu, przełącznika i routera, protokoły, standardy.

- scharakteryzować działanie modemów, hubów, przełączników i routera,
- scharakteryzować budowę karty sieciowej oraz jej zadania,
- scharakteryzować topologie i zaprojektować sieć komputerową,
- scharakteryzować dodatkowe urządzenia wykorzystywane przy rozbudowie sieci komputerowych.

Sieci komputerowe są nieodzownym składnikiem każdej niemalże instytucji, organizacji czy firmy. Korzyści wielokrotnie przewyższają koszty ich realizacji. Do najważniejszych można tu zaliczyć:

- możliwość wykorzystywania tych samych zasobów sprzętowych przez grupę użytkowników (np. napędu CD),
- udostępnienie wielu różnych usług sieciowych jak np. przesyłanie danych (od plików po dźwięk i obraz w czasie rzeczywistym), poczta elektroniczna, Internet,
- heterogeniczność czyli zdolność łączenia różnorodnych zasobów sprzętowych, często niekompatybilnych,
- integralność danych - te same informacje mogą być wykorzystywane przez wielu użytkowników jednocześnie.

Szybkość sieci komputerowych jest stale zwiększana, dzięki coraz to doskonalszym urządzeniom i mediom transmisyjnym. Dominujący do niedawna standard Ethernet, o przepustowości 10 Mb/s, jest stopniowo wypierany przez Fast Ethernet. (100Mb/s), Przyszłość stanowi zapewne, opracowywany właśnie standard Gigabitowego Ethernetu. Z innych typów sieci do najbardziej znanych należą: ARCnet, Token Ring i ATM.

Rodzaje sieci komputerowych

Jednym z kryteriów podziału sieci komputerowych jest wielkość obszaru, na którym się znajdują:

LAN, MAN,WAN, (PAN, Campus Network)

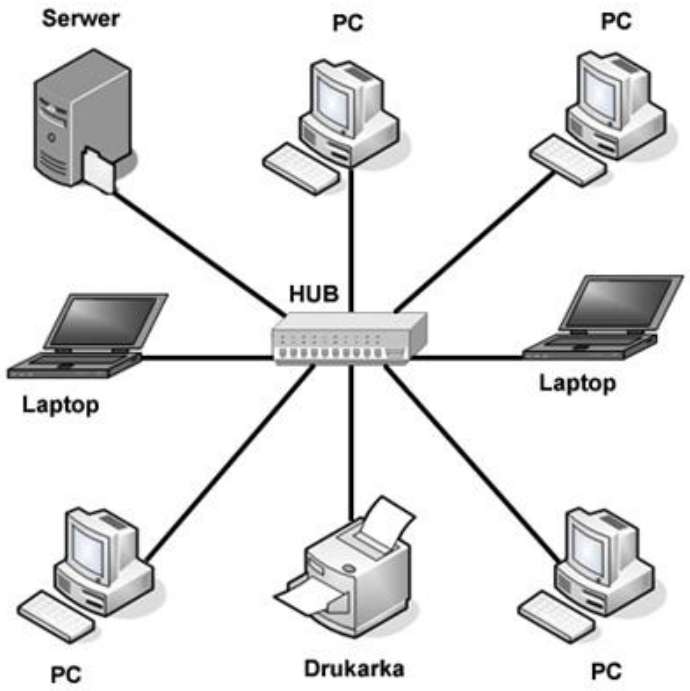
LAN (ang. *Local Area Network*). Sieci LAN składają się z kilku do kilkudziesięciu komputerów połączonych ze sobą w miarę możliwości tym samym nośnikiem danych, występuje przeważnie w prywatnych firmach, budynkach mieszkaniowych lub w innych niewielkich instytucjach. Lokalna sieć komputerowa najczęściej występuje w dwóch technologiach – przewodowych oraz bezprzewodowych.

MAN (ng. Metropolitan Area Network). Sieć miejska, sieć występująca najczęściej na obszarze jednego miasta lub całego regionu.

WAN (ang. *Wide Area Network*). Sieć rozległa, sieć komputerowa znajdująca się na obszarze wykraczającym poza jedno miasto (bądź kompleks miejski).

Fizyczne topologie sieci komputerowych

Topologia gwiazdy (ang. star network) – sposób połączenia komputerów w sieci komputerowej, charakteryzujący się tym, że kable sieciowe połączone są w jednym wspólnym punkcie, w którym znajduje się koncentrator lub przełącznik. Sieć o topologii gwiazdy zawiera przełącznik (switch) i hub (koncentrator) łączący do niego pozostałe elementy sieci.



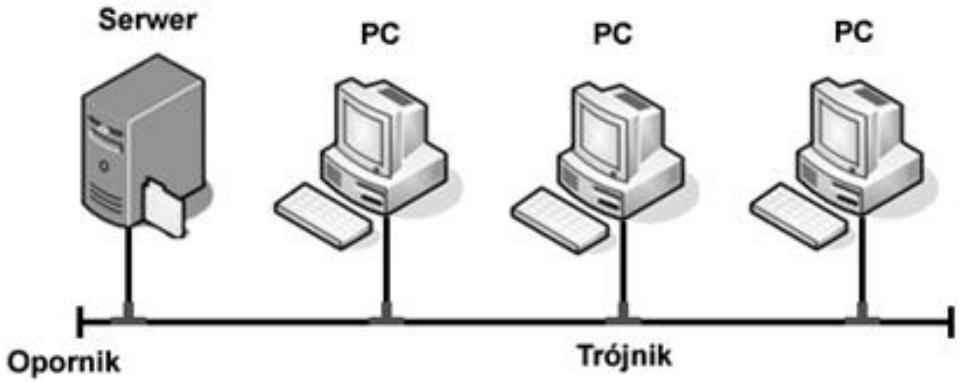
Zalety:

Większa przepustowość.
Łatwa lokalizacja uszkodzeń ze względu na centralne sterowanie.
Wydajność.
Łatwa rozbudowa.
Awaria komputera peryferyjnego nie blokuje sieci.

Wady:

Duża liczba połączeń (duże zużycie kabli).
Gdy awarii ulegnie centralny punkt (koncentrator lub przełącznik), to nie działa cała sieć.

Topologia magistrali (ang. Bus Network) szynowa - charakteryzująca się tym, że wszystkie elementy sieci są podłączone do jednej magistrali. Sieć składa się z jednego kabla koncentrycznego (10Base-2, 10Base-5). Poszczególne części sieci (takie jak hosty, serwery) są podłączane do kabla koncentrycznego za pomocą specjalnych trójników (zwanych także łącznikami T) oraz łączy BNC. Na obu końcach kabla powinien znaleźć się opornik (tzw. terminator) o rezystancji równej impedancji falowej wybranego kabla, aby zapobiec odbiciu się impulsu i tym samym zajęciu całego dostępnego łącza. Maksymalna długość segmentu sieci to w przypadku: 10Base-2 – 185 m, 10Base-5 – 500 m.



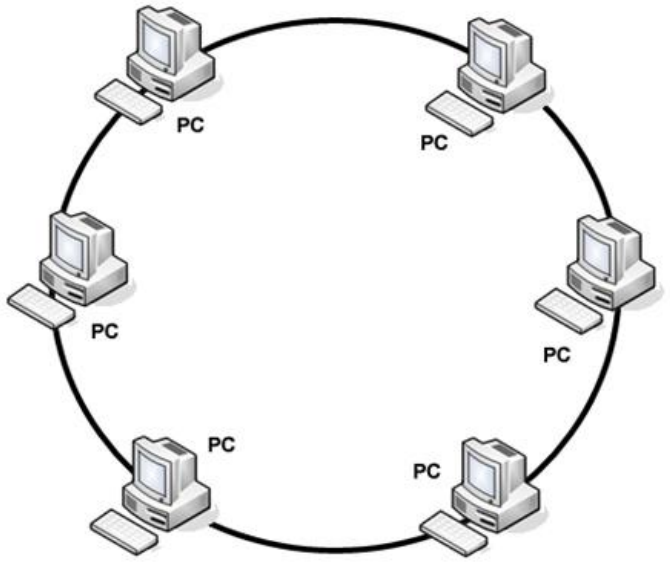
Zalety:

Małe użycie kabla.
Brak dodatkowych urządzeń (koncentratorów, switchów), niska cena sieci.
Łatwość instalacji.
Awaria pojedynczego komputera nie powoduje, unieruchomienia całej sieci.

Wady:

Trudna lokalizacja usterek.
Tylko jedna możliwa transmisja w danym momencie.
Potencjalnie duża ilość kolizji.
Awaria głównego kabla powoduje unieruchomienie całej domeny kolizji.
Słaba skalowalność.
Niskie bezpieczeństwo.

Topologia pierścienia (ang. Ring) -Komputery połączone są za pomocą jednego nośnika informacji w układzie zamkniętym. Metoda transmisji danych w pętli nazywana jest przekazywaniem żetonu dostępu. Żeton dostępu jest określoną sekwencją bitów zawierających informację kontrolną. Przejęcie żetonu zezwala urządzeniu w sieci na transmisję danych w sieci. Komputer wysyłający, usuwa żeton z pierścienia i wysyła dane przez sieć. Każdy komputer przekazuje dane dalej, dopóki nie zostanie znaleziony komputer, do którego pakiet jest adresowany. Następnie komputer odbierający wysyła komunikat do komputera wysyłającego o odebraniu danych. Po weryfikacji, komputer wysyłający tworzy nowy żeton dostępu i wysyła go do sieci.



Topologia pierścienia

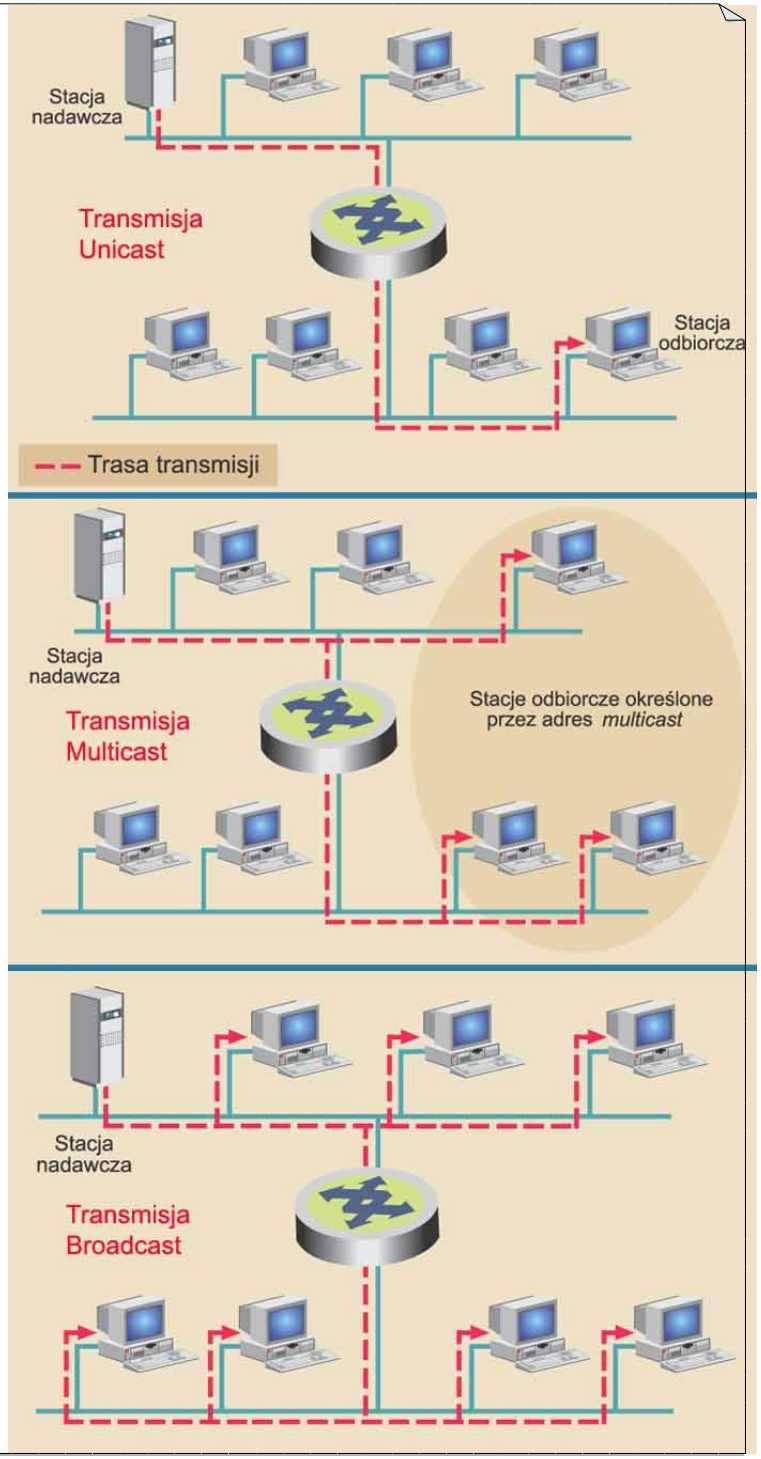
Sposoby transmisji i adresowania w LAN

Transmisje: Unicast, Multicast i Broadcast

Wyróżnia się trzy sposoby transmisji i adresowania w LAN:

Transmisja pojedyncza **Unicast**,
Transmisja grupowa **Multicast**,
Transmisja rozgłoszeniowa **Broadcast**.

W transmisji **Unicast** pojedynczy pakiet jest wysyłany przez stację nadawczą do stacji odbiorczej. Przedtem jednak stacja nadawcza adresuje pakiet używając adresu stacji odbiorczej. Po zaadresowaniu pakiet jest wysyłany do sieci, w której "przepływa" do stacji odbiorczej.
W transmisji **Multicast** pojedynczy pakiet danych jest kopiowany i wysyłany do grupy stacji sieciowych (określonej przez adres multicast). Przedtem jednak stacja nadawcza adresuje pakiet używając adresu multicast. Po zaadresowaniu pakiet jest wysyłany do sieci, gdzie jest kopiowany; każda kopia pakietu jest wysyłana do wszystkich stacji należących do grupy adresów multicast.
W transmisji **Broadcast** pojedynczy pakiet jest kopiowany i wysyłany do wszystkich stacji sieciowych. W tym typie transmisji stacja nadawcza adresuje pakiet używając adresu broadcast. Następnie pakiet jest wysyłany do sieci, gdzie jest kopiowany; kopie są wysyłane do wszystkich stacji sieciowych .

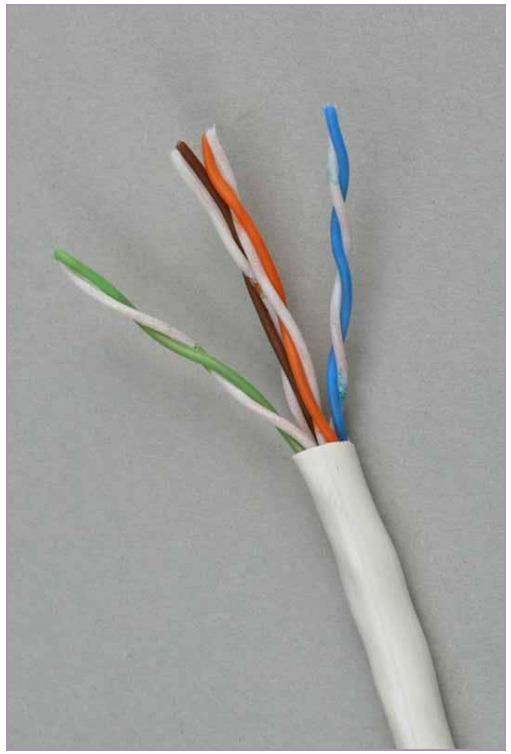


Temat 3. <u>Media transmisyjne.</u>

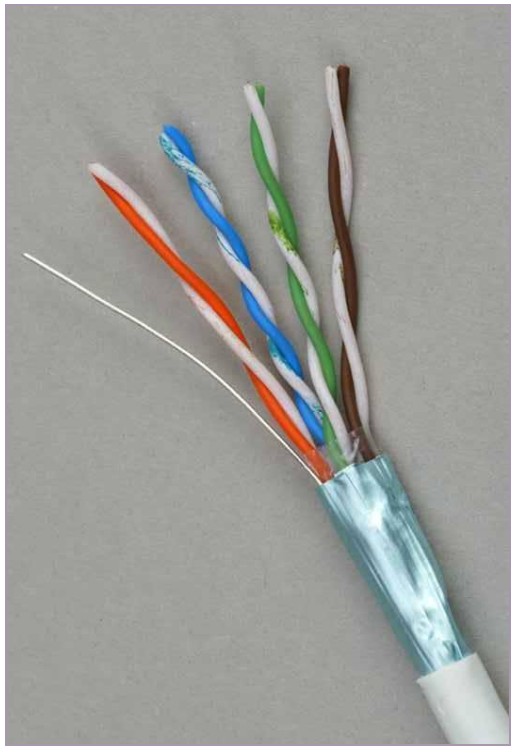
Skrętka nieekranowana (UTP – Unshielded Twisted Pair)
Skrętka foliowana (FTP – Foiled Twisted Pair)
Skrętka ekranowana (STP – Shielded Twisted Pair)
Kategorie skrętek miedzianych
Kabel światłowodowy
Kabel współosiowy (koncentryczny)

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.

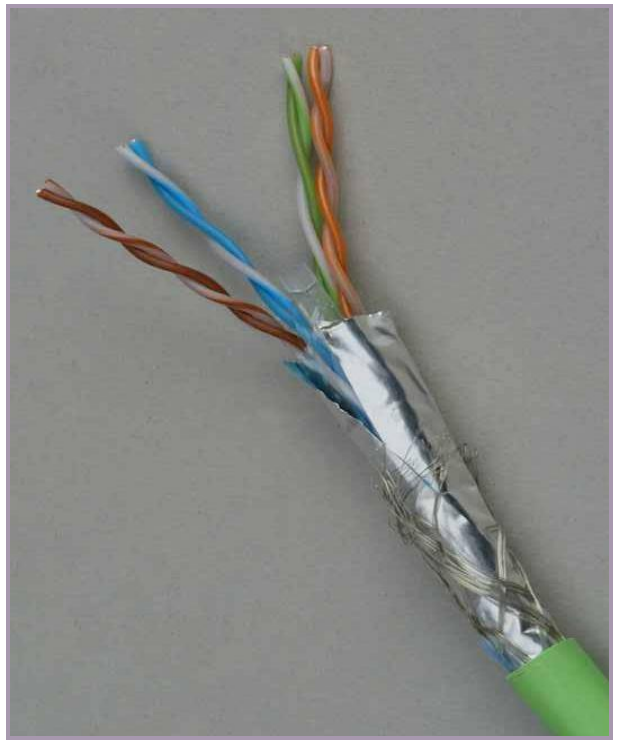
Przepustowość skrętki zależna jest od tzw. **kategorii**. Skrętka kategorii 1 to kabel telefoniczny, kategorii 2 przeznaczona jest do transmisji danych z szybkością 4 Mb/s, kategorii 3 do transmisji o przepustowości do 10 Mb/s, kategorii 4 do 16 Mb/s, kategorii 5 do ponad 100 Mb/s - ten typ ma zastosowanie 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



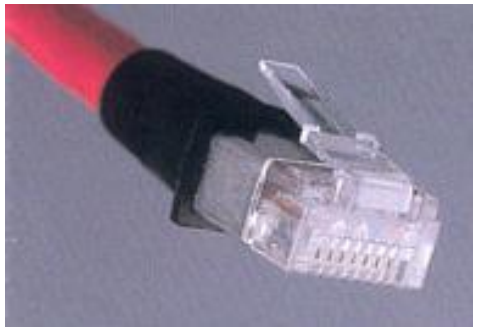
"SFTP"
Shielded Foiled Twisted Pairs
Ekranowana i foliowana skrętka

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.

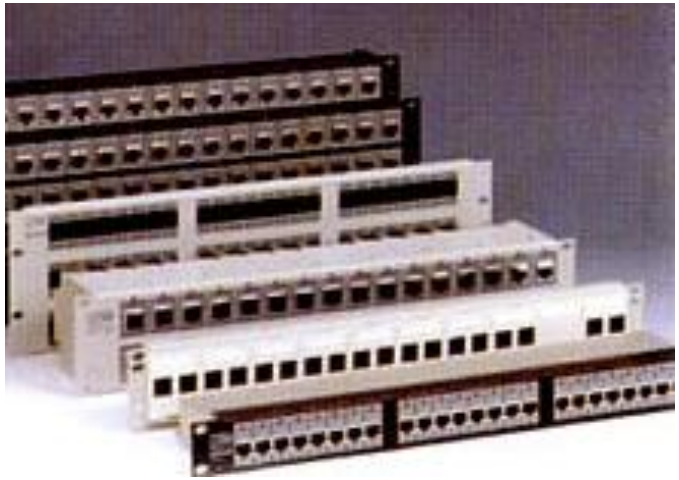
W sieciach opartych na skrętce podobnie jak w pozostałych okablowaniach standardu **Ethernet** obowiązuje zasada, iż sygnał może przejść tylko przez 4 repeatery.

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 skrętkowego jest bardzo prosta dzięki zastosowaniu połączeń zaciskowych. W celu zmniejszenia awaryjności sieci, zaleca sie stosowanie tzw. **paneli przyłączeniowych** (krosownic).

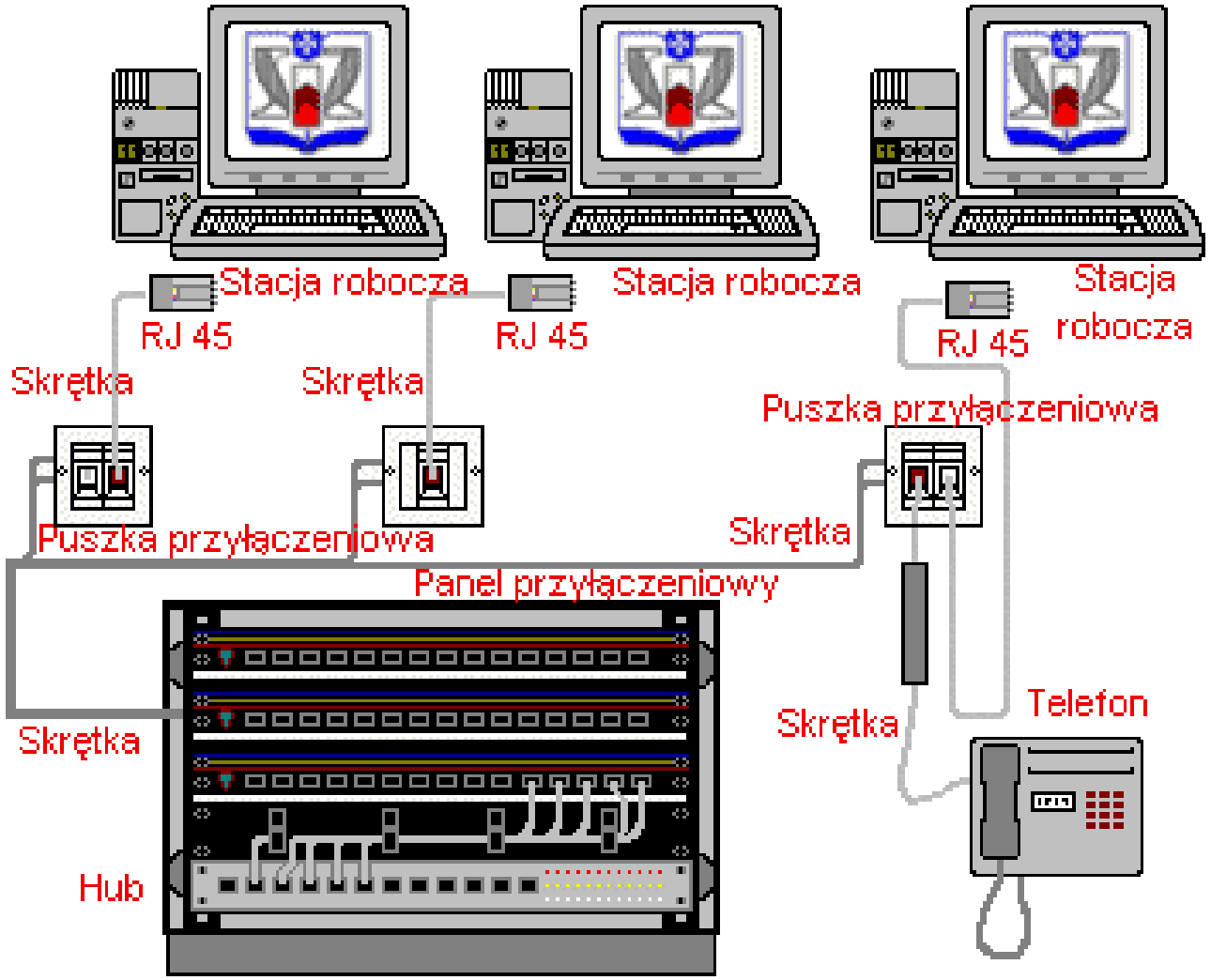


Krosownice.

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.

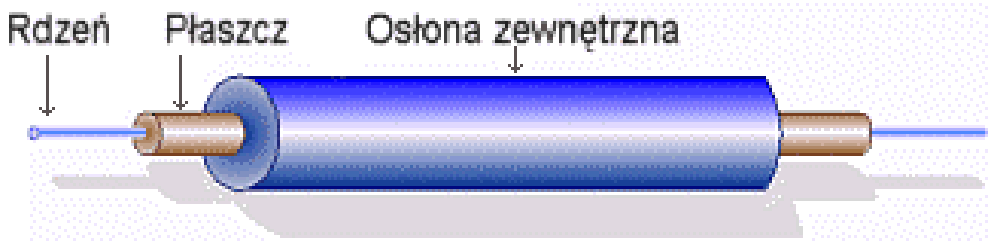
Ogromną zaletą skrętki jest też uniwersalność, można ją stosować dla różnych typów sygnałów, np. informatycznych i telefonicznych. Skrętkę stosuje sie także w nowych sieciach Fast Ethernet (100BASE-T) i **Gigabit Ethernet** (1000BASE-T). W przypadku przejścia z technologii Ethernet na Fast Ethernet okablowanie 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.

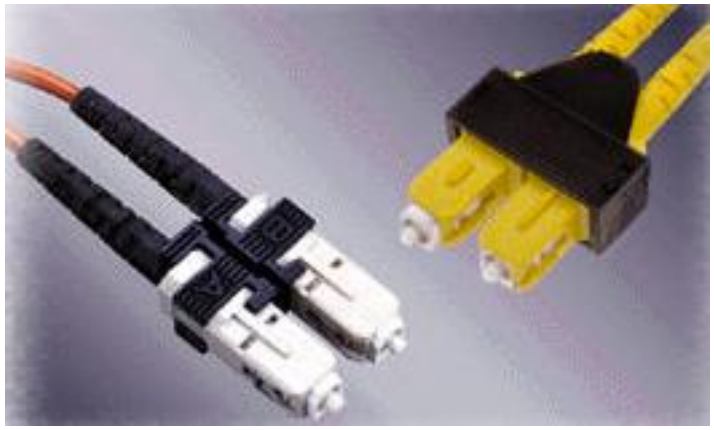
Światłowód - W światłowodach do transmisji informacji wykorzystywana jest **wiązka światła**, która jest odpowiednikiem prądu w kablach miedzianych. Wiązka ta jest modulowana zgodnie z treścią przekazywanych informacji. Właściwie dobrany kabel może przebiegać w każdym środowisku. Szybkość transmisji 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

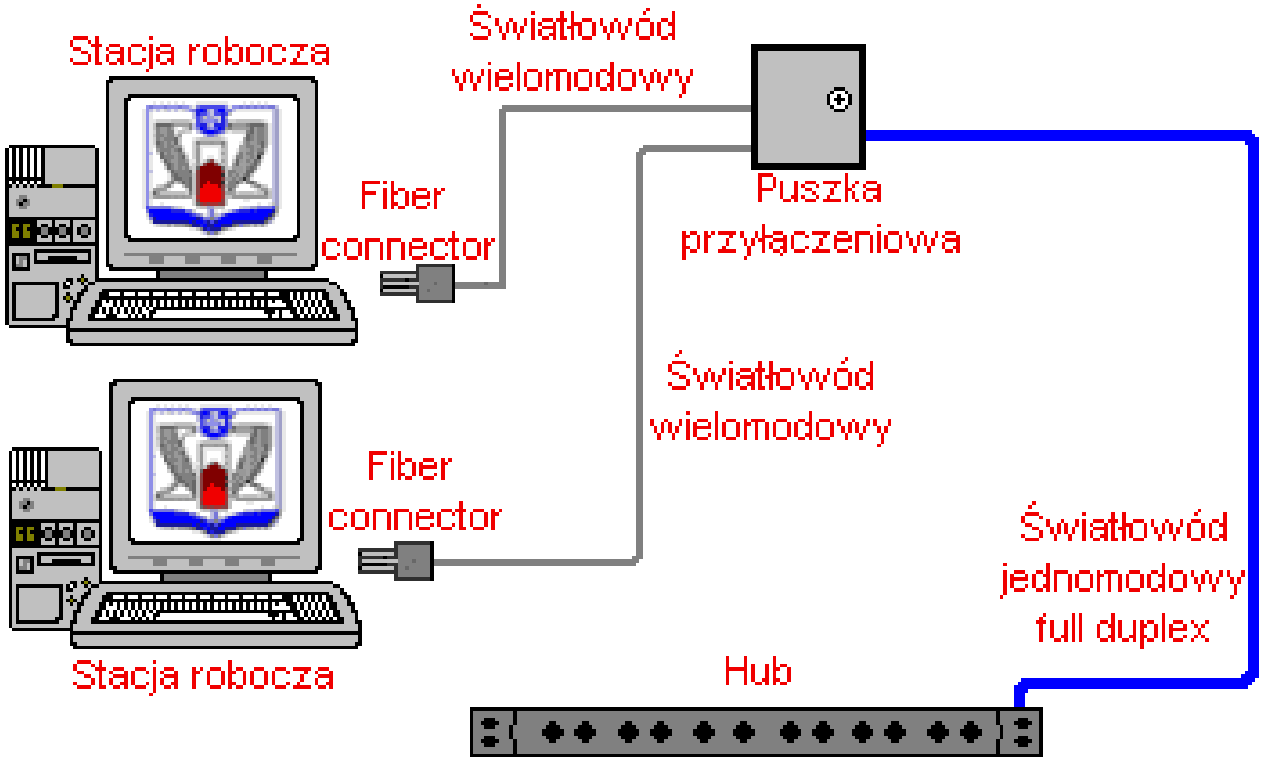
Do karty sieciowej światłowód przyłącza się za pomocą złącza ***fiber connector***. Może ono wyglądać różnie, w zależności od rodzaju.



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 tłumieniościowych 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.

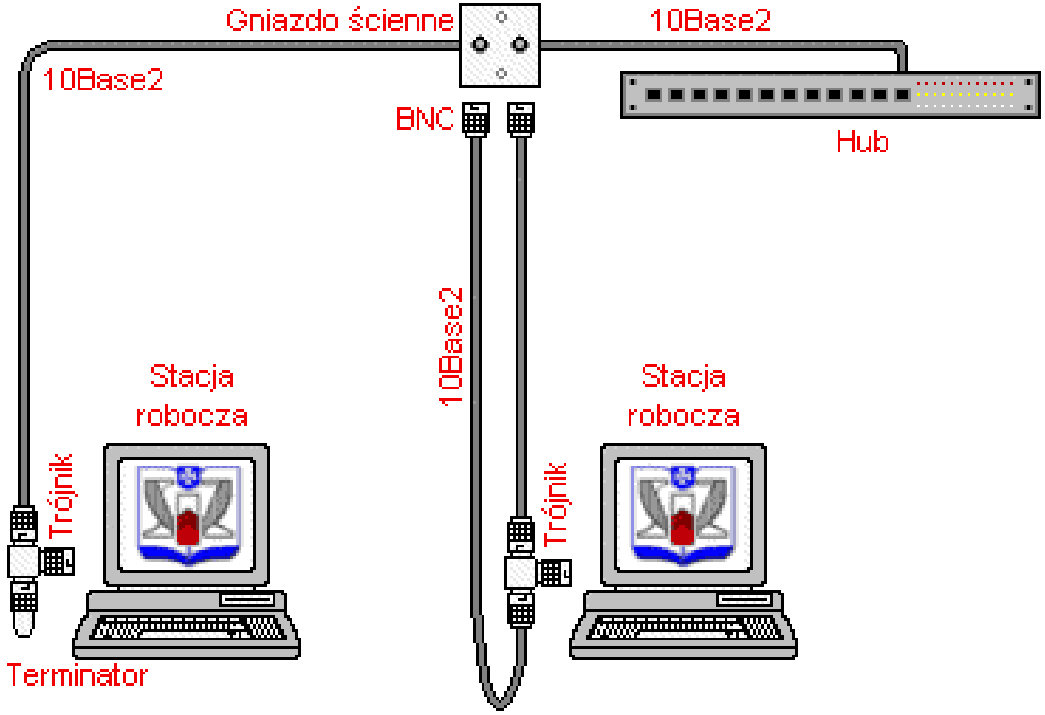


Przykład zastosowania kabla światłowodowego.

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)



Przykład zastosowania kabla 10BASE2.

Temat 4. <u>Protokoły sieciowe.</u>

Protokół jest to zbiór procedur oraz reguł rządzących komunikacją, między co najmniej dwoma urządzeniami sieciowymi. Istnieją różne protokoły, lecz nawiązujące w danym momencie połączenie urządzenia muszą używać tego samego protokołu, aby wymiana danych pomiędzy nimi była możliwa.

W celu komunikacji między różnymi protokołami wykorzystuje łącza *(ang. gateway)* - czyli urządzenia, które tłumaczącą rozkazy jednego protokołu na drugi. Kolejnym rozwiązaniem może być skonfigurowanie komputerów w taki sposób, by wykorzystywały kilka protokołów równocześnie, jednak i to rozwiązanie może prowadzić do dodatkowego obciążania sieci.

Do najważniejszych protokołów należą:

- TCP/IP
- IP
- SLIP
- PPP

TCP/IP (ang. Transmission Control Protocol / Internet Protocol) - to zespół protokołów sieciowych używany w sieci Internet. Najczęściej wykorzystują go systemy Unixowe oraz systemy Windows, choć można stosować go również w systemach Novell NetWare. Zadanie protokołu TCP/IP polega na dzieleniu danych na pakiety odpowiedniej wielkości, ponumerowaniu ich w taki sposób, aby odbiorca mógł sprawdzić, czy dotarły wszystkie pakiety oraz ustawieniu ich we właściwej kolejności. Kolejne partie informacji wkładane są do kopert TCP, a te z kolei umieszczane są w kopertach IP. Oprogramowanie TCP po stronie odbiorcy zbiera wszystkie nadesłane koperty, odczytując przesłane dane. Jeśli brakuje którejś koperty, wysyła żądanie ponownego jej dostarczenia. Pakiety wysyłane są przez komputery bez uprzedniego sprawdzenia, czy możliwa jest ich transmisja. Może się zdarzyć taka sytuacja, że do danego węzła sieci, gdzie znajduje się router, napływa więcej pakietów, aniżeli urządzenie może przyjąć, posegregować i przesłać dalej. Każdy router posiada bufor, który gromadzi pakiety czekające na wysłanie. Gdy bufor ulegnie całkowitemu zapełnieniu, nowo nadchodzące

pakiety zostaną odrzucone i bezpowrotnie przepadną. Protokół, który obsługuje kompletowanie pakietów zażąda, więc wtedy ponownego ich wysłania.

IP (Internet Protocol) - to protokół do komunikacji sieciowej, gdzie komputer klienta wysyła żądanie, podczas gdy komputer serwera je wypełnia. Protokół ten wykorzystuje adresy sieciowe komputerów zwane adresami IP. Są to 32-bitowa liczby zapisywana, jako sekwencje czterech ośmiobitowych liczb dziesiętnych (mogących przybierać wartość od 0 do 255), oddzielonych od siebie kropkami. Adres IP dzieli się na dwie części: identyfikator sieciowy (network id) i identyfikator komputera (host id). Istnieje kilka klasy adresowych, o różnych długościach obydwu składników.

W celu ułatwienia zapamiętania adresów wprowadzono nazwy symboliczne, które tłumaczone są na adresy liczbowe przez specjalne komputery w sieci, zwane ***serwerami DNS***.

SLIP (ang. Serial Line Interface Protocol) - to protokół transmisji przez łącze szeregowe. Uzupełnia on działanie protokołów TCP/IP tak, by możliwe było przesyłanie danych przez łącza szeregowe.

PPP (ang. Point to Point Protocol) - to protokół transferu, który służy do tworzenia połączeń z siecią Internet przy użyciu sieci telefonicznej i modemu, umożliwiający przesyłanie danych posiadających różne formaty dzięki pakowaniu ich do postaci PPP. Steruje on połączeniem pomiędzy komputerem użytkownika a serwerem dostawcy internetowego. PPP działa również przez łącze szeregowe. Protokół PPP określa parametry konfiguracyjne dla wielu warstw z modelu OSI *(ang. Open Systems Interconnection)*. PPP stanowiąc standard internetowy dla komunikacji szeregowej, określa metody, za pośrednictwem, których pakiety danych wymieniane są pomiędzy innymi systemami, które używają połączeń modemowych.

Do innych popularnych protokołów sieciowych należą:

- IPX/SPX
- NetBEUI

- FTP
- SNMP
- SMTP
- CSMA/CD
- DNS
- DHCP
- AARP
- ARP
- HTTP
- ICMP

IPX/SPX (ang. Internetwork Packet Exchange/Sequenced Packet Exchange) - to zespół protokołów sieciowych opracowanych przez firmę Novell.

NetBEUI (ang. Network BIOS Extended USER Interface) - to protokół transportu sieci LAN, wykorzystywany przez systemu operacyjne firmy Microsoft. NetBEUI jest w pełni samodostrajającym się protokołem i najlepiej działa w małych segmentach LAN. Protokół ten, ma minimalne wymagania, jeśli chodzi o użycie pamięci. Zapewnia bardzo dobrą ochronę przed błędami występującymi w transmisji, oraz powrót do normalnego stanu w przypadku ich wystąpienia. Wadą NetBEUI jest to, że nie może on być trasowany i nie najlepiej działa w sieciach typu WAN.

FTP (ang. File Transfer Protocol) - to protokół służący do transmisji plików. Przeważnie usługę ftp stosuje do przesyłania danych z odległej maszyny do lokalnej lub na odwrót. Protokół ten działa w oparciu o zasadę klient-serwer i korzystanie z usługi polega na użyciu interaktywnej aplikacji. Technologia FTP zapewnia ochronę stosując hasła dostępu.

SNMP (ang. Simple Network Managment Protocol) - to podstawowy protokół służący do zarządzania siecią. SNMP stanowi standard internetowy, jeżeli chodzi o zdalne monitorowanie i zarządzanie routerami, hostami oraz innymi urządzeniami sieciowymi.

SMTP (ang. Simple Mail Transfer Protocol) - jest podstawowym protokołem realizującym transfer poczty elektronicznej, SMTP należy do rodziny protokołów TCP/IP i służy do wysyłania poczty elektronicznej.

CSMA/CD (ang. Carrier Sense Multiple Access with Collision Detection) - to metoda wielodostępu do łącza sieci z wykrywaniem kolizji oraz badaniem stanu kanałów, stosowana w sieciach Ethernet w celu przydziału nośnika dla poszczególnych węzłów. Węzeł zaczyna nadawanie, kiedy nie wykryje w sieci transmisji z innego węzła, sprawdzając przez cały czas, czy nie doszło do kolizji. W przypadku zaistnienia kolizji próba transmisji zostaje ponowiona po przerwie o losowej długości.

DNS (ang. Domain Name Service) - protokół używany w sieci Internet obsługujący system nazywania domen. Umożliwia on nadawanie nazw komputerom, które są zrozumiałe i łatwe do zapamiętania dla człowieka, tłumacząc je na adresy IP. Nazywany czasem usługą BIND (BSD UNIX), DNS oferuje hierarchiczną, statyczną usługę rozróżniania nazw hostów. Administratorzy sieci konfigurują DNS używając listę nazw hostów oraz adresów IP. DNS nie posiada centralnego repozytorium przechowującego adresy IP maszyn w sieci. Dane dotyczące tych adresów dzielone są między wiele komputerów, zwanych serwerami DNS (nazw domenowych), które są zorganizowane hierarchicznie w formie drzewa. Początek drzewa nazywany jest korzeniem. Nazwy najwyższego poziomu składają się z dwuliterowych domen narodowych opartych na zaleceniach ISO 3166 (wyjątek stanowi brytyjska domen uk). Nadrzędna domena narodowa w Polsce oznaczona jest przez pl.

DHCP (ang. Dynamic Host Configuration Protocol) - to standardowy protokół przydzielający adresy IP poszczególnym komputerom. Serwer DHCP przypisuje adresy IP poszczególnym końcówkom.

AARP (ang. AppleTalk Address Resolution Protocol) - protokół służący przyporządkowaniu adresów w sieci AppleTalk. AARP tłumaczy adresy z sieci AppleTalk do formatu sieci Ethernet albo Token ring.

ARP (ang. Address Resolution Protocol) - to protokół sieciowy należący do rodziny TCP/IP (lecz niezwiązany wprost z transportowaniem danych). Jest on stosowany w celu dynamicznego określania fizycznych adresów niskiego poziomu, które odpowiadają adresom IP poziomu wyższego dla określonego komputera Protokół ten ogranicza się do fizycznych systemów sieciowych, które obsługują emisję pakietów.

HTTP (ang. HyperText Transfer Protocol) - to protokół internetowy, używany do obsługi stron WWW. HTTP stanowi podstawowy protokół, przy pomocy którego przebiega komunikacja między klientami i serwerami sieci Web. Jest to protokół poziomu aplikacji dla współpracujących ze sobą, hipermedialnych, rozproszonych systemów informacyjnych.

HTTP jest bezstanowym i generycznym protokołem zorientowanym obiektowo. Cechą charakterystyczną tego protokołu możliwość wpisywania oraz negocjowania reprezentacji danych, co umożliwia budowę systemów niezależnie od typu transferowanych danych.

ICMP (ang. Internet Control Message Protocol) - jest to rozszerzenie protokołu IP (Internet Protocol). Protokół ICMP służy generowaniu komunikatów o występujących błędach, wysyłaniu pakietów testowych oraz komunikatów diagnostycznych związanych z protokołem IP.

Temat 5. <u>Urządzenia sieciowe.</u>

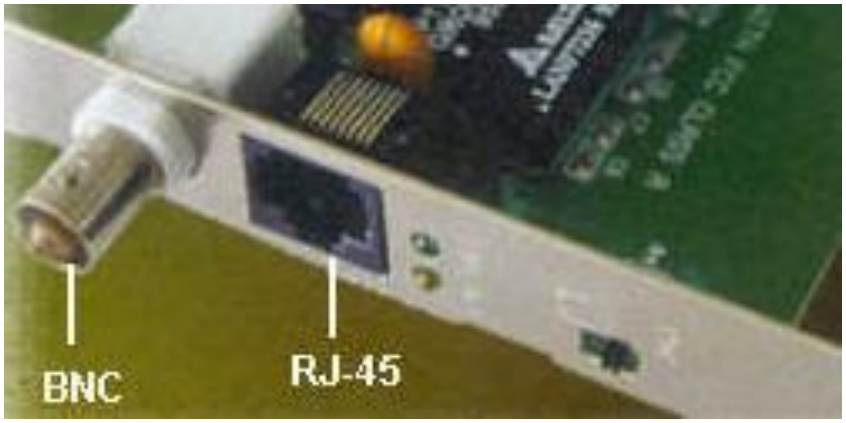
Karta sieciowa - Jest to urządzenie wymagane we wszystkich stacjach roboczych przyłączonych do sieci. Każda karta jest przystosowana tylko do jednego typu sieci i posiada niepowtarzalny numer, który identyfikuje zawierający ją komputer. Przydziela go międzynarodowa instytucja pod nazwą **IEEE**. Każdemu 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.

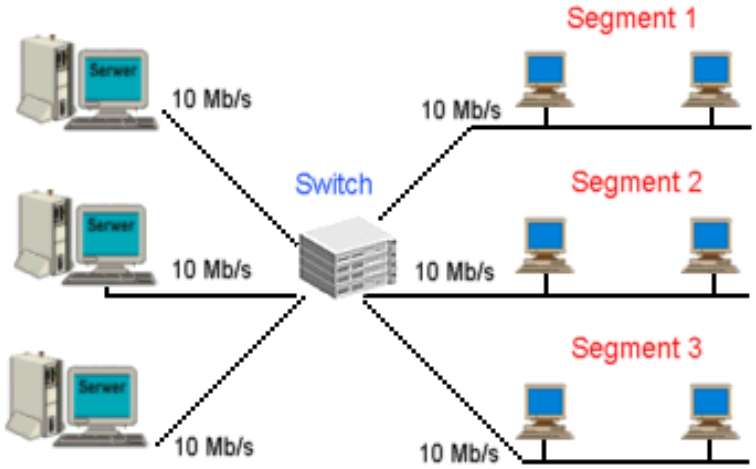


Karta sieciowa złącza BNC i P8C8 na wtyk RJ45

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.

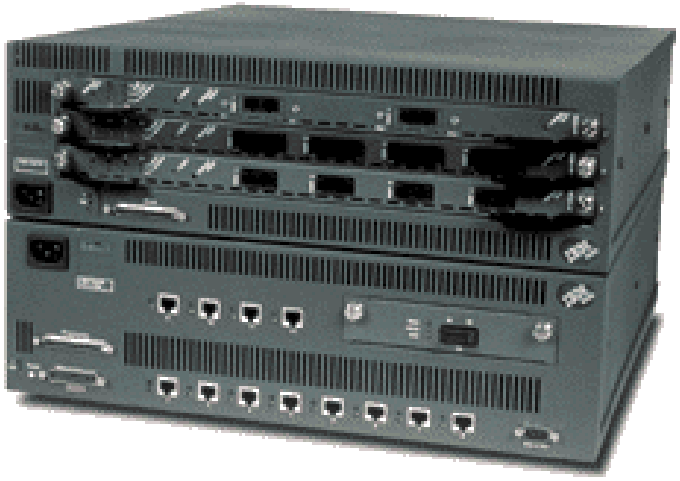
Cisco switch

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.

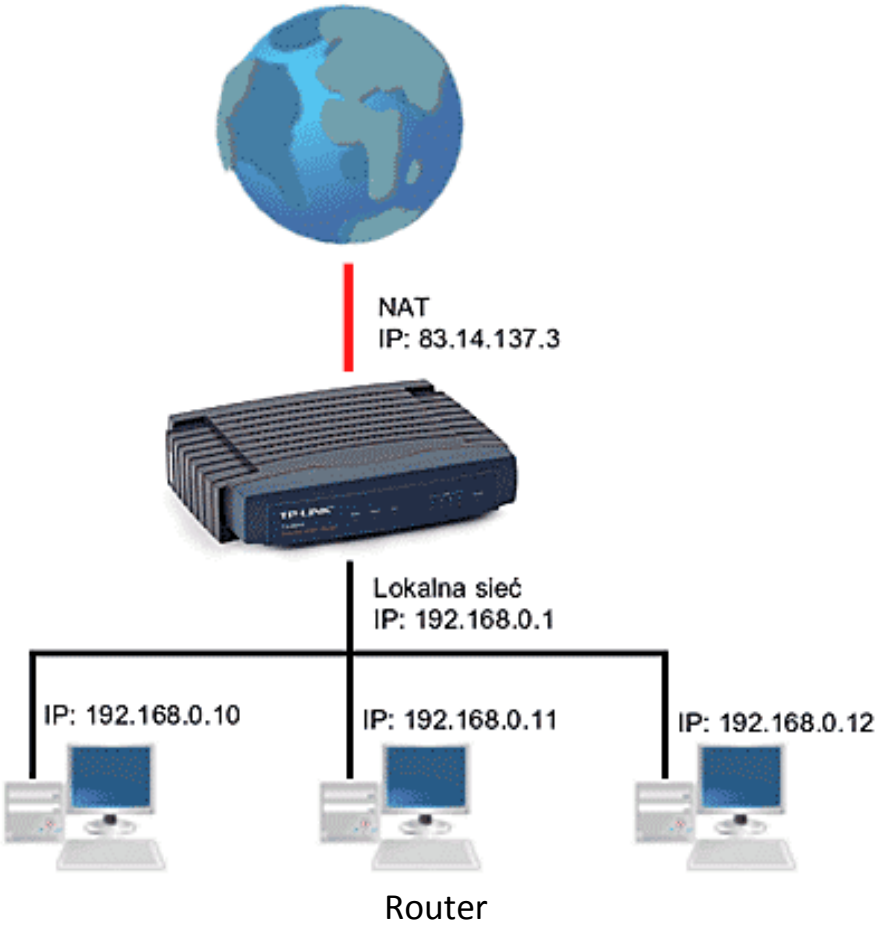


Switch IBM 8285 Nways ATM

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.



Router

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.

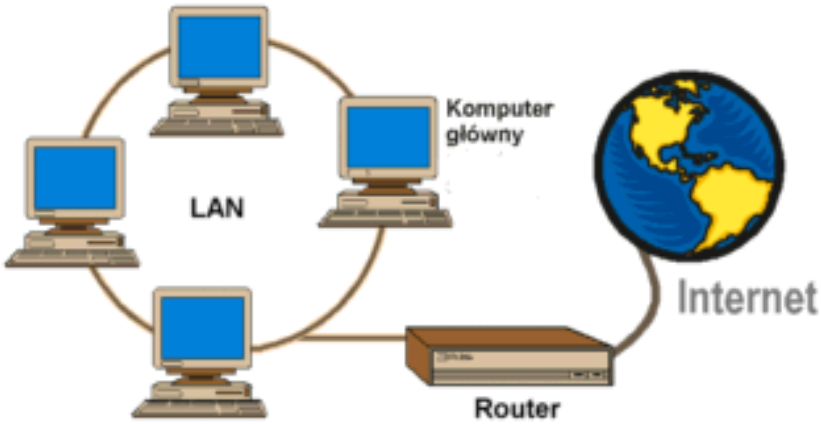
Do kierowania danych routery używają tzw. **tablicę routingu,** zawierającą informacje o sąsiadujących routerach i sieciach lokalnych. Służy ona do wyszukania optymalnej drogi od obecnego położenia **pakietu** do innego miejsca sieci. Tablica routingu może być **statyczna** lub **dynamiczna,** zależy 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.

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



Router, jako firewall

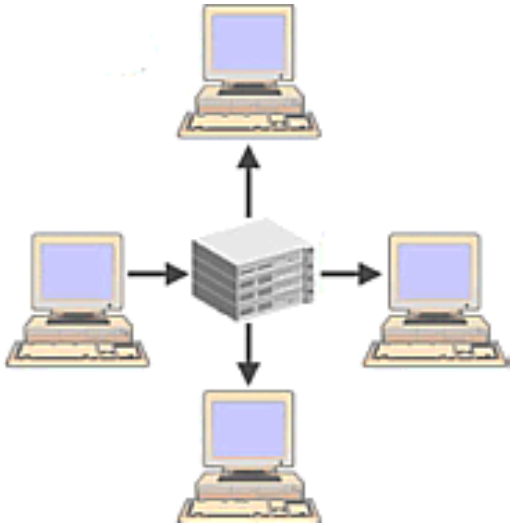
Na rysunku router łączy sieć lokalną z Internetem i filtruje określone typy pakietów. Należy go tak skonfigurować, aby widoczny dla niego był tylko jeden komputer główny. Wszyscy użytkownicy **LAN** przy dostępie do Internetu korzystają z pośrednictwa tego komputera, a użytkownicy Internetu mają dzięki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

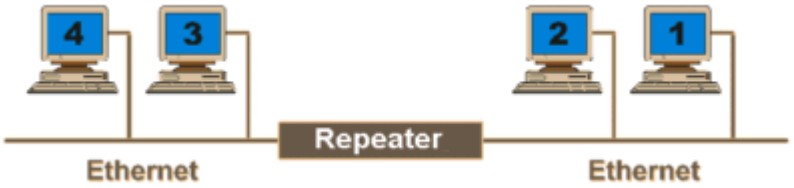
Można wyróżnić huby **pasywne** i **aktywne**.
Hub pasywny jest tanim urządzeniem pełniącym funkcję skrzynki łączeniowej, nie wymaga zasilania.
Hub aktywny dodatkowo wzmacnia sygnały ze stacji roboczej i pozwala na wydłużenie połączenia z nią. Zasilanie jest wymagane.

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.

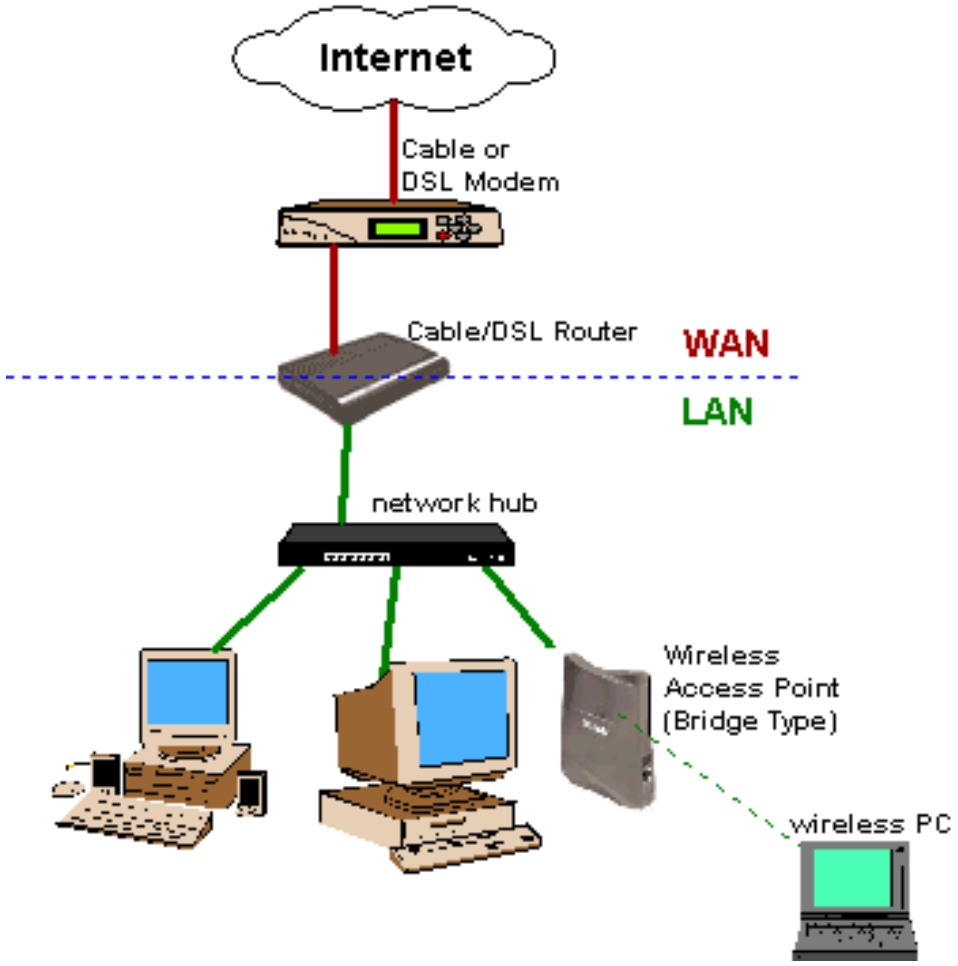
W sieci może pracować wiele mostów, ale każdy musi pamiętać adresy wszystkich węzłów, nie tylko tych, które są do niego przyłączone. Jeśli więc stacja A z sieci LAN 1 chce wysłać komunikat do stacji C z sieci LAN 3, to most 1 musi wiedzieć jak przesłać dane zarówno do sieci LAN 2 jak i LAN 3. Most 2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

Połączenia szerokopasmowe

Połączenia szerokopasmowe (ang. Broadband Connection) wykorzystują dużą część zakresu częstotliwości pasma przenoszenia przewodu miedzianego (od 25 kHz do ponad 1 MHz) Dla porównania: modemy analogowe wykorzystują wąskie pasmo 30 Hz – 4 kHz. Za połączenie szerokopasmowe uważa się technologii kablowe i bezprzewodowe umożliwiające pobieranie i wysyłanie danych z i do Internetu w postaci cyfrowej z prędkością od 128 Kb/s wzwyż.

Do najpopularniejszych technologii szerokopasmowych mżna zaliczyć:

- DSL,
- Połączenia realizowania za pomocą cyfrowych telewizji kablowych,
- Połączenia telefonii komórkowej,
- Połącznie satelitarne.



Technologia DSL – (ang. Digital Subscriber Line- cyfrowa linia abonencka, wykorzystuje istniejącą infrastrukturę telekomunikacyjną. Umożliwia jednoczesne prowadzenie rozmowy i transmisję danych cyfrowych, dzięki wykorzystywaniu różnych częstotliwości okablowania miedzianego.

ADSL (ang. Asimmetric Digital Subscriber Line) – Asymetryczna cyfrowa linia abonencka – Najpopularniejsza odmian DSL, odbierająca i wysyłająca dane z różnymi prędkościami. Zazwyczaj dane pobierane są znacznie szybciej niż wysyłana (na przykład 1024, 128 kb/s).
ADSL2+ umożliwia odbieranie danych z prędkością do 24 Mb/s na odcinku do 2 km, udostępnia przy tym telewizję cyfrową i usługi multimedialne.

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

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