Uczniowie i komputery w sieci…

Mariusz Piwiński
Wydział Fizyki, Astronomii i Informatyki Stosowanej UMK, Toruń
Mariusz.Piwinski@fizyka.umk.pl

Wstęp

Wszechobecność komputerów w naszym życiu spowodowała, iż często nie wyobrażamy sobie dnia bez włączenia komputera i sprawdzenia poczty elektronicznej, czy wyszukania informacji w dostępnych serwisach internetowych. Podłączenie naszego komputera do sieci Internet staje się powoli standardem, który niestety w Polsce cały czas stosunkowo za dużo kosztuje. W sytuacji, gdy jednak zdecydujemy się już na podłączenie naszego komputera do sieci pojawiają się pierwsze pytania. Jaka opcja będzie dla mnie najlepsza? Jakie pasmo wybrać? Co to jest numer IP? Większość użytkowników pracowni komputerowych przyzwyczajona jest do istniejącej infrastruktury, która została zaprojektowana i wykonana w ściśle określony sposób i najczęściej nie ulega zmianie, podczas gdy wymagania zarówno ze strony użytkowników jak i używanego oprogramowania ciągle rosną.

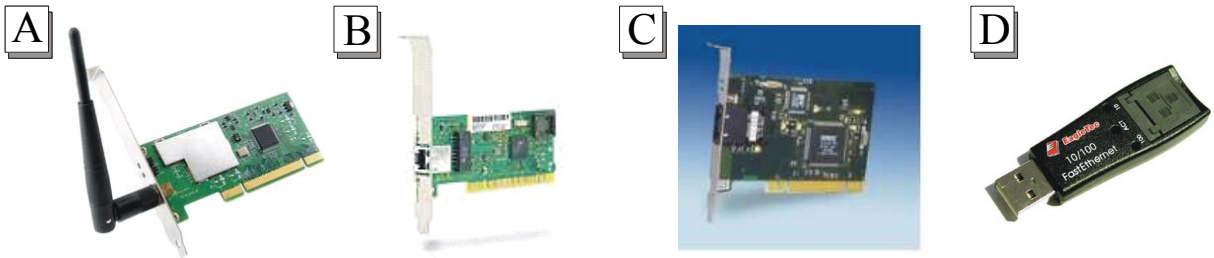
Odwiedzając witryny internetowe, czy obsługując wspomnianą już pocztę elektroniczną nie zastanawiamy się nad sposobem działania wykorzystywanej sieci. Oczywiście problem pojawia się w momencie, gdy coś przestaje prawidłowo funkcjonować, a my do końca nie jesteśmy pewni, czy przyczyna tkwi u dostawcy Internetu, czy w naszym lokalnym systemie. Moim celem nie jest tutaj bynajmniej chęć wyjaśnienia wszystkich aspektów związanych z sieciami komputerowymi, ale tylko przekonanie czytelnika, że jest on w stanie poradzić sobie z prostymi problemami, a nawet samodzielnie połączyć dostępne komputery w prostą sieć. Takie rozwiązanie zapewnia nie tylko wygodny sposób przenoszenia danych, ale również umożliwia udostępnianie zasobów dyskowych, czy drukarek sieciowych. Do łączenia komputerów w proste sieci skłania dodatkowo fakt, iż większość sprzedawanych obecnie płyt głównych wyposażona jest w zintegrowaną kartę sieciową.

Rys.1 Tylne panele obudów komputerów z widocznymi gniazdami kart sieciowych oraz podłączonymi kablami UTP zakończonymi wtyczkami RJ45.

1. Co warto wiedzieć dokonując wyboru karty sieciowej?

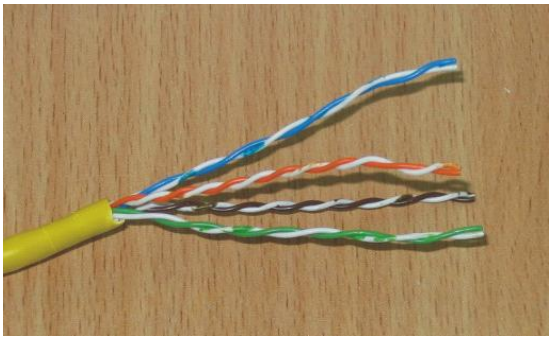
Wielkością charakteryzującą maksymalną szybkość przesyłania informacji przez urządzenie jest pasmo transmisji, którego wielkość określana jest w Mbps, czyli w ilości mega bitów (a nie bajtów) przesyłanych w ciągu jednej sekundy. Jednocześnie należy zdawać sobie sprawę z faktu, iż aby transmisja danych w sposób poprawny odbywała się z określoną prędkością, wszystkie urządzenia biorące w niej udział muszą tą prędkość zapewniać. W większości dostępne urządzenia pracujące w trybie autonegocjacji, są w stanie same określić szybkość komunikacji z drugim interfejsem sieciowym, co w praktyce oznacza, iż maksymalna prędkość zawsze określana jest przez najwolniejsze urządzenie.

W przypadku, gdy komputer nie jest wyposażony w interfejs sieciowy, można wzbogacić go o kartę Ethernetową, która w najprostszej wersji nie kosztuje więcej niż 30 zł. Przed zakupem odpowiedniego urządzenia należy określić typ złącza, który chcemy wykorzystywać w naszym komputerze. Najczęściej będzie to gniazdo PCI, ale dostępne są również karty wykorzystujące starsze rozwiązania oparte na złączu ISA, jak i nowsze wykorzystujące złącze USB. Te ostatnie dedykowane są głównie komputerom przenośnym, jednakże w przypadku korzystania z portu USB 1.0 maksymalna prędkość transmisji danych do komputera ograniczona jest przez szybkość samego portu. Oznacza to, iż podłączenie takiej karty do Fast Ethernetu pozwoli na pracę z maksymalną prędkością nieprzekraczającą 12 Mbps.



Rys. 2 A) Ethernetowa bezprzewodowa karta sieciowa wraz z anteną, pasmo 11 Mbps, B) Ethernetowa karta sieciowa z gniazdem RJ45, pasmo 10/100 Mbps, C) Fast Ethernetowa karta sieciowa ze złączem światłowodowym, pasmo 100 Mbps, D) Karta sieciowa Ethernet (10 Mbps)\FastEthernet (100 Mbps) z gniazdem RJ45 wykorzystująca port USB 1.0.

Kolejny wybór związany jest z medium, które wykorzystamy do przesyłania informacji. Należy pamiętać, iż musi ono spełniać wymogi dotyczące zarówno żądanej szybkości transferu danych oraz odpowiedniej jakości sygnału po przesłaniu go na maksymalną odległość. Różne rozwiązania techniczne sprawiły, iż obecnie mamy do czynienia z licznymi standardami szczegółowo charakteryzującymi warunki pracy poszczególnych typów okablowania. Jednym z najbardziej rozpowszechnionych mediów stosowanych w lokalnych sieciach LAN (*Local Area Network*), a zatem również typowym dla pracowni komputerowych, jest kabel UTP (*Unshielded Twisted Pair*) kategorii 5. Pospolicie jest on nazywany nieekarnowaną skrętką, ze względu na fakt, iż tworzą go cztery pary skręconych ze sobą przewodów, które mogą składać się z pojedynczych drutów lub splecionych żył. W przypadku pierwszego rozwiązania kabel jest stosunkowo sztywny, co znacznie ułatwia jego montaż w korytkach i ścianach budynków. Plecionka zaś, jako znacznie bardziej elastyczna, stosowana jest najczęściej przy łączeniu poszczególnych komputerów z gniazdkami lub bezpośrednio z urządzeniami sieciowymi.



Rys. 3 Kabel UTP kategorii 5.

Jak widać na Rysunku 3 każdy z przewodów oznaczony jest innym kolorem, przy czym przewód niebieski skręcony jest z biało–niebieskim, pomarańczowy z biało–pomarańczowym, brązowy z biało–brązowym i zielony z biało–zielonym. Podczas przesyłania sygnałów ze względu na brak idealnego medium zawsze mamy do czynienia ze zjawiskami powodującymi tłumienie oraz dyspersję sygnału, które wpływają na pogorszenie jakości docierających do odbiorcy impulsów. Kolejnym bardzo istotnym czynnikiem są szumy, których duże natężenie uniemożliwia poprawne odczytanie przesyłanych informacji. Jak się okazuje w większości przewodów sygnałowych, dokonuje się szeregu zabiegów, aby w możliwie największym stopniu wpływ tych zakłóceń zminimalizować. W przypadku kabla UTP podłączane urządzenia zapewniają, iż w każdym ze skręconych ze sobą przewodów, prąd płynie w przeciwną stronę, a zatem wytwarzane przez oba przewodniki pola elektromagnetyczne znoszą się wzajemnie powodując tak zwane samoekranowanie przewodów, tym samym w pewnym stopniu zapewniają ich izolację od zakłóceń zewnętrznych. Ponadto powoduje ono, iż przy poprawnym działaniu połączenia, transmisja danych przez jedną parę przewodów nie powoduje przesłuchów, czyli pojawienia się sygnału w pozostałych. W związku z powyższym, aby zamierzony efekt przynosił poprawne rezultaty, należy zadbać o prawidłowe wykonanie połączeń oraz minimalizowanie odległości, na których występuje rozplecenie par. Opisane rozwiązanie umożliwia łącznie dwóch aktywnych urządzeń kablem UTP o długości nieprzekraczającej 99 m. W przypadku występowania silnych zakłóceń zewnętrznych stosuje się kable ScTP (*Screened Twisted Pair*) posiadające pojedynczy metalowy ekran lub STP (*Shielded Twisted Pair*), w których dodatkowo każda para otoczona jest swoim własnym ekran.

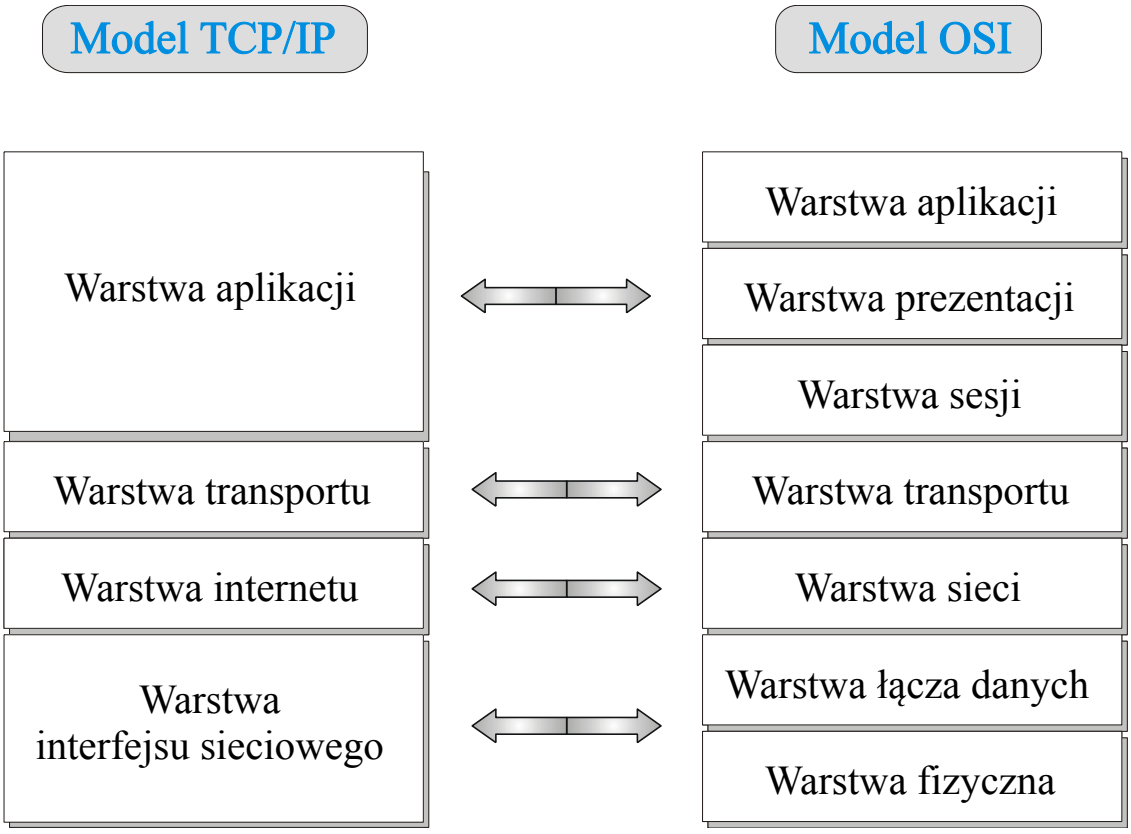
Mówiąc o rodzaju transmisji nie sposób wspomnieć o coraz silniej rozwijającej się sieci bezprzewodowej wykorzystującej łącza radiowe. Jest to doskonałe rozwiązanie zwłaszcza w przypadku komputerów przenośnych, gdy chcemy zapewnić użytkownikom stały dostęp do sieci bez względu na miejsce, w którym się znajdują. Niestety posiada ono również swoje wady, ze względu na możliwe zakłócenia w transmisji, które znacznie mogą ograniczać pasmo. Ponadto przy użyciu standardowych anten maksymalna odległość pomiędzy urządzeniami nadawczo odbiorczymi najczęściej nie może być większa niż kilkaset metrów. Należy pamiętać, iż maksymalny zasięg pracy urządzeń podawany jest najczęściej dla otwartej przestrzeni, a umieszczenie ich w budynku znacznie zwiększa poziom tłumienia sygnału, co wpływa na drastyczne obniżenie wielkość efektywnego pasma transmisji.

W przypadku typowych zastosowań stworzenie prostej sieci w oparciu o karty Ethernetowe wyposażone w gniazda RJ45 oraz kabel UTP kategorii 5, jest w zupełności wystarczające zwłaszcza, iż w ten sposób jesteśmy w stanie zapewnić standardowe pasmo wynoszące 100 Mbps, przy stosunkowo niewielkich kosztach w stosunku do innych rozwiązań.

2. Zacznijmy do podstaw

Przed przystąpieniem do tworzenia sieci komputerowej niezbędne jest zrozumienie ogólnych reguł i zasad rządzących sposobem przesyłania informacji. Potrzeba łączenia komputerów w sieci spowodowała, iż na przestrzeni lat producenci proponowali swoje indywidualne rozwiązania, które jednak ze względu na brak jednoznacznego standardu nie były ze sobą w pełni kompatybilne. W związku z powyższym na zamówienie Departamentu Obrony USA został opracowany model TCP/IP (*Transmission Control Protocol/Internet Protocol*), opisujący i pozwalający na praktyczną realizację połączeń pomiędzy dowolnymi komputerami na świecie. Rozwiązywał on między innymi problem, dotyczący możliwości automatycznego znajdowania nowych dróg i przesłania za ich pomocą danych, w przypadku awarii dotychczasowych łączy pomiędzy urządzeniami sieciowymi.

Ostatecznie w 1984 roku organizacja ISO (*International Organization for Standardization*) zaproponowała warstwowy model odniesienia OSI (*Open System Interconnection*), który z powodzeniem stosowany jest do dnia dzisiejszego.



Rys. 4 Zestawienie modelu TCP/IP z modelem OSI.

Składa się on z siedmiu ustawionych hierarchicznie warstw, z którymi można utożsamiać poszczególne procesy oraz realizujące je urządzenia. Takie podejście pozwala na podzielenie złożonych zagadnień na mniej skomplikowane elementy, którymi w praktyce jest znacznie łatwiej kierować. Ponadto dokładny opis zależności występujących pomiędzy poszczególnymi warstwami pozwala na modyfikację zarówno sposobu realizacji samych procesów, jak również urządzeń je realizujących. Jednocześnie zachowanie zgodności odpowiednich standardów powoduje, iż zmiany w jednej warstwie nie wymagają dokonywania zmian w pozostałych. Takie rozwiązanie sprzyja szybkiemu wdrażaniu nowych rozwiązań zarówno w sferze programowej jak i sprzętowej.

3. Model OSI

W celu przybliżenia czytelnikowi modelu OSI, warto zająć się krótką charakterystyką każdej z warstw.

3.1 Warstwa 7, Warstwa aplikacji

Jak sama nazwa wskazuje jest ona związana z wykorzystywanymi aplikacjami, którym ma zapewnić dostęp do odpowiednich usług sieciowych. Odpowiada za weryfikację dostępności partnerów podczas próby ich wzajemnej komunikacji, a po jej nawiązaniu za synchronizację pomiędzy współpracującymi aplikacjami, a także kontrolę integralności danych w tym również rozpoznawanie błędów.
Przeciętnemu użytkownikowi kojarzy się między innymi z programami obsługującymi pocztę elektroniczną, przeglądarkami internetowymi, sesjami telnet i ftp.

3.2 Warstwa 6, Warstwa prezentacji

Odpowiedzialna jest za prezentację danych, czyli za fakt, iż dane wysłane przez program pracujący w warstwie aplikacji jednego komputera, zostaną poprawnie odczytane przez aplikację pracującą w tej samej warstwie u odbiorcy. Jednocześnie w przypadku różnych formatów danych są one tłumaczone na zrozumiały format. To właśnie dzięki niej pliki o formacie TIFF, GIF, czy JPEG obserwujemy w postaci wyświetlanego obrazu na ekranie oraz jesteśmy wstanie wykonać poprawną kompresję lub dekompresję danych.

3.3 Warstwa 5, Warstwa sesji

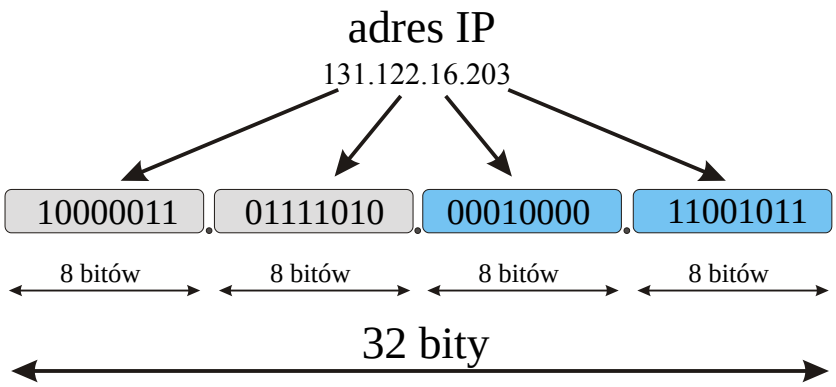
W bezpośredni sposób nadzoruje połączenia pomiędzy aplikacjami z różnych komputerów (zwanych sesjami), ustanawiając je, zarządzając nimi i kończąc w odpowiednim momencie.

3.4 Warstwa 4, Warstwa transportu

Warstwa ta jest granicą pomiędzy warstwami związanymi bezpośrednio z działaniem aplikacji, a warstwami odpowiedzialnymi za przenoszenie danych. Dokonywany jest tutaj ich podział na segmenty, co stanowi wstępne przygotowanie do procesu przesłania. Odpowiada ona również za kontrolę przepływu ustanawiając, zarządzając oraz kończąc związane z nim wirtualne połączenia.

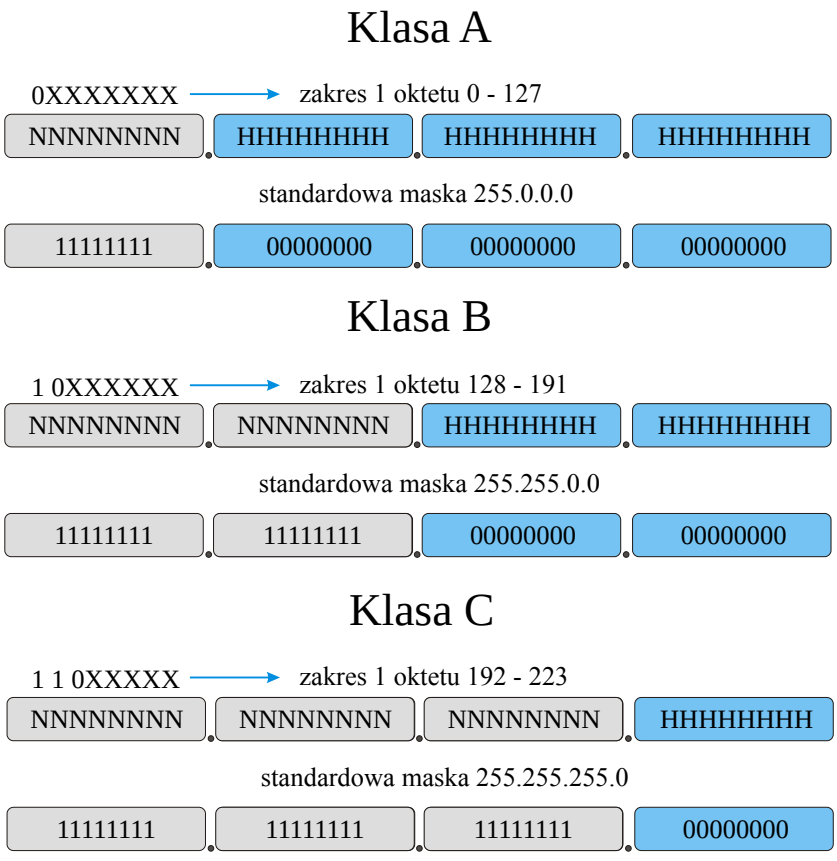
3.5 Warstwa 3, Warstwa sieci

W warstwie tej pracują urządzenia (routery), których głównym zadaniem jest określanie najlepszej drogi dla przesyłanych pakietów, a w związku z tym wysyłanie ich przez swoje interfejsy w odpowiednich kierunkach. Wybór ten dokonywany jest w oparciu o adres sieciowy IP, który analizowany jest na poziomie tej warstwy. Składa się on z 32 bitów zgrupowanych w cztery oktety i zapisywanych najczęściej w postaci czterech liczb dziesiętnych oddzielonych kropkami.



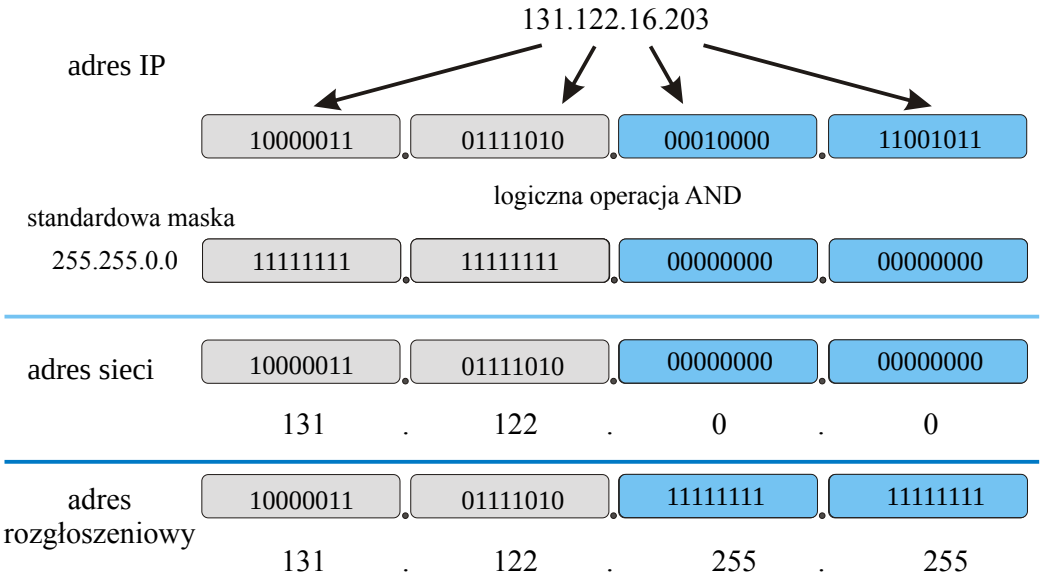
Rys. 5 Format adresu logicznego IP.

Pozwala on na jednoznaczne określenie komputera w całej sieci Internet, zatem jest to pierwszy krok do przekonania się, iż pojęcie „anonimowego użytkownika sieci" w praktyce prawie nie ma racji bytu. Adres ten składa się z dwóch części, z których pierwsza jest numerem sieci, w której komputer się znajduje. To właśnie w oparciu o ten fragment podejmowana jest decyzja o drodze, którą pakiet zostanie wysłany do urządzenia docelowego. Pozostałe bity nazywane są polem hosta, gdyż określają już numer konkretnego komputera. Jak łatwo zauważyć, administrator otrzymując numer IP dla swojej sieci, ma ściśle określoną liczbę bitów, które może użyć do numerowania kolejnych hostów, zatem istnieją klasy adresów, które przydzielane są w zależności od przewidywanej liczby użytkowników. Aby nie komplikować całego obrazu skupmy się na trzech podstawowych klasach adresowych IP.



Rys. 6 Klasy adresowe IP.

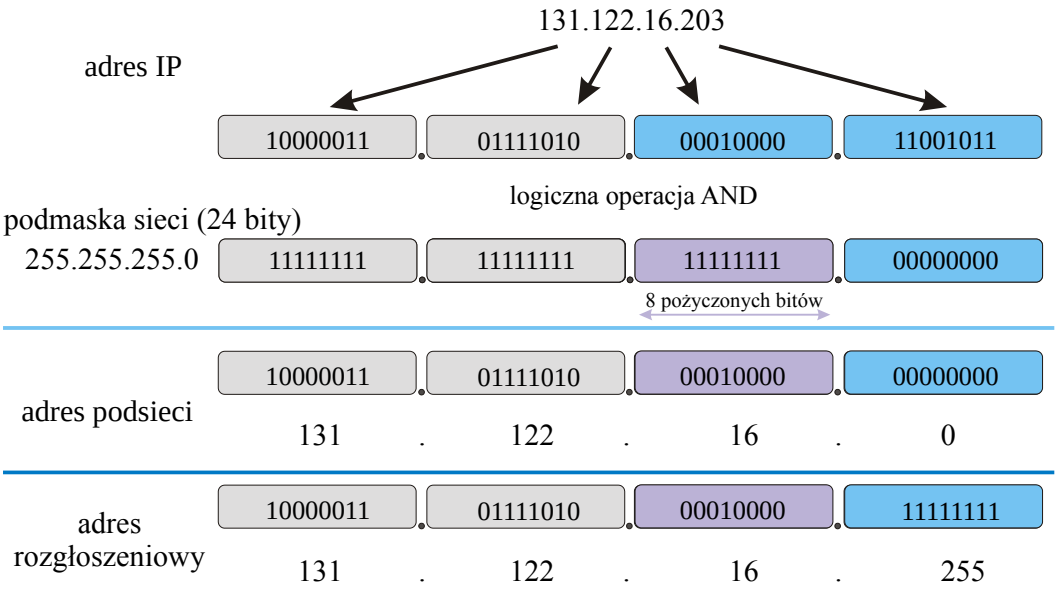
Klasa A zawiera adresy sieciowe, które w pierwszym oktecie posiadają liczbę pomiędzy 0 a 127. Wynika to z faktu, iż dla takich adresów pierwszy bit w pierwszym oktecie ma zawsze wartość 0. Pozostałe trzy oktety przeznaczone są na adresowanie hostów. W przypadku klasy B adres sieciowy określony jest za pomocą dwóch pierwszych oktetów, z czego pierwszy oktet przedstawia liczbę z zakresu od 128 do 191. W każdej z takich sieci można numerować użytkowników używając pozostałych 16 bitów. Adresy sieciowe klasy C określane są przy użyciu trzech pierwszych oktetów, a pierwszy oktet przedstawia liczbę z zakresu 192-223. W sieciach takich do zaadresowania hostów pozostaje tylko 8 bitów.
Efektywnie licząc maksymalną liczbę urządzeń, którą można zaadresować w danej sieci, należy zawsze odjąć dwa zarezerwowane adresy. Pierwszy z nich jest adresem sieciowym posiadającym w polu hosta same zera, drugi zaś adresem rozgłoszeniowym, posiadającym w polu hosta same jedynki. Zatem routery odczytując z pakietu adres IP docelowego urządzenia, mogą bardzo łatwo zakwalifikować go do odpowiedniej klasy adresowej. Następnie znając postać standardowej maski sieci, poprzez wykonanie logicznej operacji AND otrzymują adres sieci pozwalający na podjęcie odpowiedniej decyzji dotyczącej kierunku dalszego przesyłania informacji.



Rys. 7 Sposób odczytania adresu sieci z adresu IP z wykorzystaniem standardowej maski.

Ostatecznie pakiet trafiając do odbiorcy weryfikowany jest w warstwie sieci pod kątem poprawności adresu IP. Jeżeli zgodność została potwierdzona, informacje przesyłane są do wyższych warstw modelu OSI, w przeciwnym przypadku są one niszczone. Ze względu na fakt, iż istnieją informacje, które powinny trafić do każdego odbiorcy w danej sieci, istnieje adres rozgłoszeniowy, który zawsze przechodzi poprawną weryfikację w warstwie sieci u wszystkich użytkowników danej sieci.

Analizując informacje dotyczące adresu IP komputera oraz jego maski, możemy czasami zauważyć, iż ma ona znacznie więcej bitów o wartości 1, niż wynikałoby to z klasy adresowej IP. Taka sytuacja oznacza, iż administrator w obrębie przydzielonego adresu IP, „pożyczając bity" z pola hosta, zastosował podział na dodatkowe podsieci, pozwalający na wyodrębnienie kilku sieci lokalnych, które można traktować z zupełnie różnymi priorytetami. Z punktu widzenia użytkownika nie ma to większego znaczenia, poza faktem, iż ze względu na zmianę maski zmienia się również adres sieci na adres podsieci oraz adres rozgłoszeniowy.

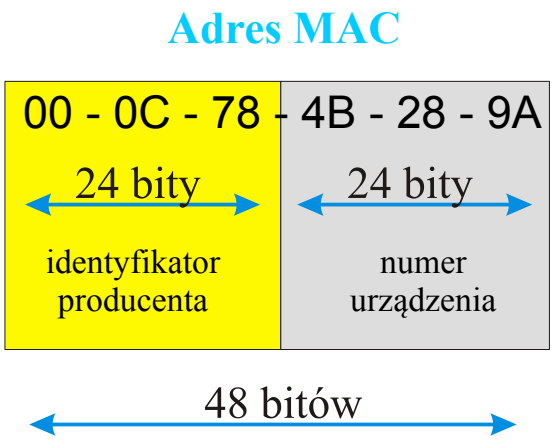


Rys. 8 Sposób odczytania adresu podsieci z adresu IP z wykorzystaniem podmaski.

Najczęściej pakiety wysyłane do odbiorcy mają na celu uzyskanie jakichś zwrotnych informacji, zatem aby mogły być one z powodzeniem dostarczone, w pakiecie zawarty jest zarówno adres IP odbiorcy jak i nadawcy.

3.6 Warstwa 2, Warstwa łącza danych

Odpowiada za niezawodne przenoszenie danych w stosowanym fizycznym medium, którym może być światłowód, przewód UTP, czy przewód telewizji kablowej. W związku z powyższym określa ona również związane z nimi zasady dotyczące kolejności dostępu oraz sterowaniem przepływem. Na tym etapie dodawany lub weryfikowany jest adres fizyczny MAC, który jednoznacznie określa stosowany interfejs sieciowy. Składa się on z 48 bitów, z których pierwsza połowa określa producenta, a druga numer urządzenia. Jest on nadawany każdemu interfejsowi sieciowemu w fazie produkcji i zapisywany w pamięci ROM karty.



Rys. 9 Format adresu fizycznego MAC.

W związku z powyższym możliwa jest jednoznaczna identyfikacja urządzenia w oparciu o jego adres fizyczny MAC, a zatem również filtrowanie i przełączanie ramek w taki sposób, aby trafiały one tylko do właściwego odbiorcy. Urządzeniami realizującymi te zadania w

warstwie drugiej modelu OSI są przełączniki Ethernetowe (Rys.10), które podejmują swoje decyzje w oparciu o tablicę wiążącą adresy MAC z odpowiednimi portami. Wpisy do tablicy dokonywane są automatycznie po zarejestrowaniu ramki, a w przypadku braku transmisji z danym urządzeniem są z niej automatycznie usuwane.

Rys. 10 Przełącznik Ethernetowy (*switch*) Cisco Catalyst 1900.

Z tego wynika, że ramka musi posiadać zarówno adres MAC interfejsu źródłowego, jak i interfejsu urządzenia, do którego informacja jest kierowana. W przypadku poprawnej weryfikacji w warstwie drugiej informacja jest przesyłana do warstwy wyższej, w przeciwnym razie następuje jej zniszczenie. Również z tych samych przyczyn, co w warstwie trzeciej istnieje adres rozgłoszeniowy, który ma postać FF-FF-FF-FF-FF-FF.

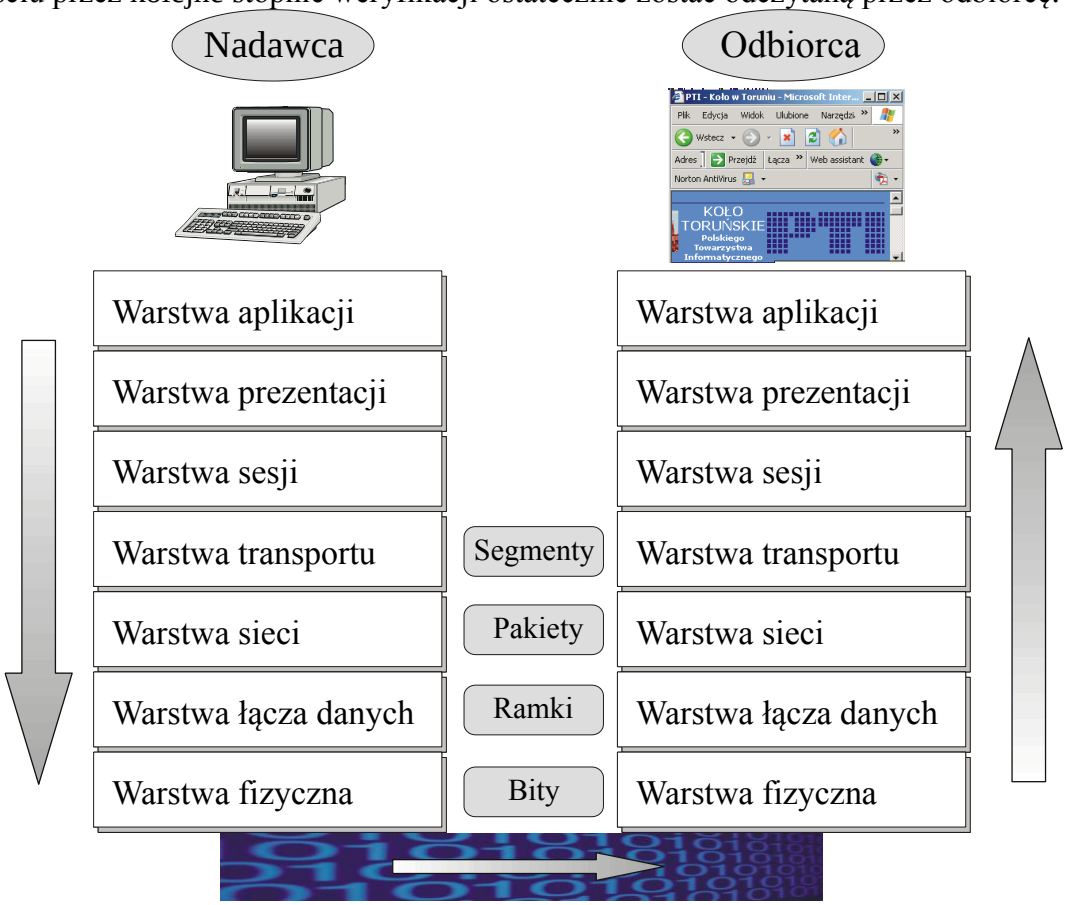
3.7 Warstwa 1, Warstwa fizyczna

Jest warstwą sprzętową, a zatem odpowiada bezpośrednio za media oraz binarną transmisję danych. Określane są tutaj poziomy sygnałów, częstotliwość pracy, czy wręcz jakość wykonywanych połączeń. Do urządzeń pracujących w tej warstwie można zaliczyć koncentrator wieloportowy (Rys. 11), którego zadaniem jest rozsyłanie informacji przez wszystkie swoje porty oraz w przypadku, gdy jest on urządzeniem aktywnym również regeneracja sygnału.

Rys. 11 Aktywny koncentrator wieloportowy (*hub*) firmy D-Link.

4. Enkapsulacja danych

Powyższy opis wskazuje, iż informacja wysyłana z komputera nadawcy musi przejść przez kolejne warstwy modelu OSI, aby po przesłaniu przez medium trafić do interfejsu sieciowego odbiorcy. Tam też rozpoczyna ona swoją drogę poprzez kolejne warstwy, aby po przejściu przez kolejne stopnie weryfikacji ostatecznie zostać odczytaną przez odbiorcę.

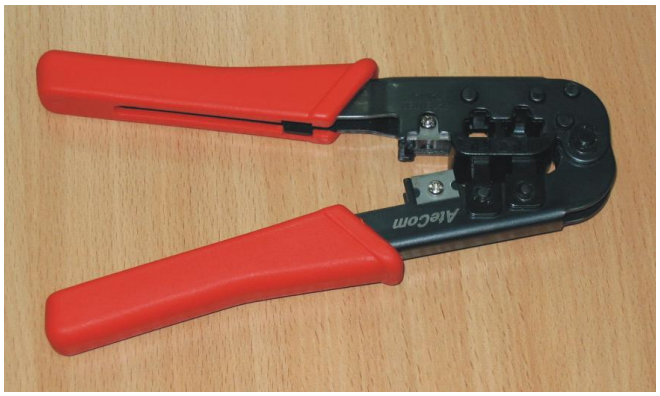


Rys. 12 Przesyłanie informacji na tle modelu OSI.

Analizując ten proces dokładniej można powiedzieć, iż w pierwszej fazie na poziomie warstwy transportu informacja dzielona jest na segmenty. Każdy z nich po przejściu przez warstwę sieci między innymi otrzymuje adres IP odbiorcy oraz nadawcy, tworząc tym samym pakiet. W warstwie łącza danych w wyniku kolejnego etapu pojawiają się adresy MAC źródła oraz kolejnego urządzenia, do którego ma trafić przesyłana informacja. W przypadku, gdy odbiorca znajduje się w tej samej sieci, jest to adres fizyczny interfejsu sieciowego odbiorcy, w innym przypadku jest to adres fizyczny interfejsu sieciowego bramy. Tak utworzone ramki zamieniane są w warstwie fizycznej na bity, a następnie sygnały, które zostają wysłane poprzez medium. Po poprawnym odebraniu sygnałów przez odbiorcę, odtwarzana jest z nich ramka, która w przypadku poprawnej weryfikacji adresów zostaje rozpakowana, tym samym tworząc pakiet. Ten z kolei po weryfikacji adresu IP zostaje rozpakowany do postaci segmentu. Ostatecznie zebrane w odpowiedniej kolejności, połączone ze sobą segmenty pozwalają na odczytanie przesłanej informacji.

5. Jak połączyć ze sobą dwa komputery?

Spróbujmy teraz połączyć dwa komputery w prostą sieć. W tym celu musimy posiadać odpowiedniej długości kabel UTP kategorii 5 oraz wtyczki RJ45. Ich montaż jest szybki, ale wymaga odpowiedniej zaciskarki. Najprostsze urządzenie tego typu można kupić już za około 40 zł, jednakże w przypadku, gdy zdecydujemy się wydać około 80 zł, nasza zaciskarka będzie z pewnością lepiej wykonana, a dodatkowo umożliwi również montaż końcówek telefonicznych RJ11.

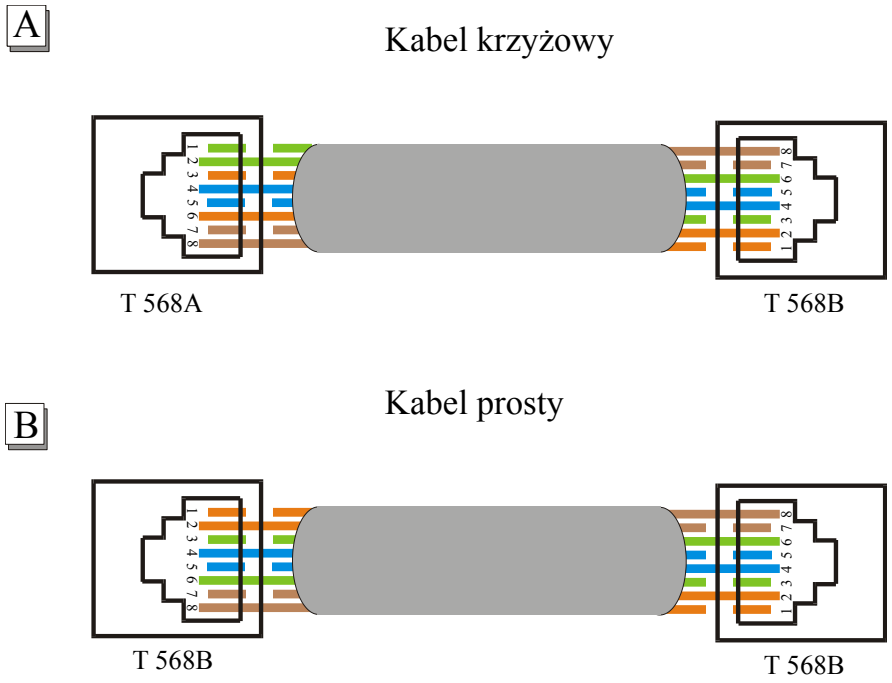


Rys. 13 Zaciskarka do wtyczek RJ45 oraz RJ11.

W przypadku bezpośredniego połączenia dwóch komputerów ze sobą należy zadbać, aby para przewodów pełniąca funkcję obwodu nadawczego w jednym komputerze, trafiała do drugiego jako para odbiorcza i na odwrót. W związku z powyższym przy tworzeniu tego typu kabla należy dokonać zamiany funkcji odpowiednich przewodów ─ stąd też tego typu kabel nazywa się krzyżowym. W praktyce realizuje się to poprzez wykonanie po jednej stronie kabla wtyczki w standardzie T568-A, a po drugiej stronie w standardzie T568-B. W przypadku łączenia ze sobą większej ilości komputerów, niezbędnym staje się zastosowanie odpowiedniego koncentratora lub przełącznika Ethernetowego. Wymienione urządzenia sieciowe łączymy z komputerami za pomocą kabli prostych, czyli takich, w których wtyczki na obu końcach zostały wykonane w jednym standardzie. Warto przy tym zaznaczyć, iż standard T568-A stosowany jest w przypadku okablowania pionowego, T568-B w przypadku okablowania poziomego, czyli biegnącego pomiędzy komputerem, a węzłem dystrybucyjnym.

Tabela 1 Schematy dotyczące realizacji połączeń wtyczek RJ45 w standardzie T568-A i T568-B.

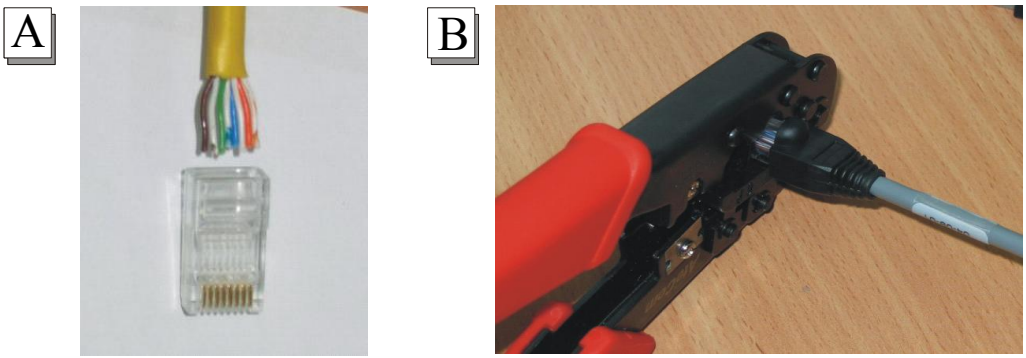
Standard okablowania T568-A			Standard okablowania T568-B		
Pin	**Funkcja**	**Kolor przewodu**	**Pin**	**Funkcja**	**Kolor przewodu**
1	Transmisja	biało - zielony	1	Transmisja	biało – pomarańczowy
2	Transmisja	Zielony	2	Transmisja	pomarańczowy
3	Odbiór	biało – pomarańczowy	3	Odbiór	biało – zielony
4	Brak	niebieski	4	Brak	niebieski
5	Brak	biało – niebieski	5	Brak	biało – niebieski
6	Odbiór	pomarańczowy	6	Odbiór	zielony
7	Brak	biało – brązowy	7	Brak	biało – brązowy
8	Brak	brązowy	8	Brak	brązowy



Rys. 14 Schematy połączeń dotyczące: A) kabla krzyżowego, B) kabla prostego wykonanego w standardzie T568B.

5.1 Wykonujemy kabel prosty

Po ucięciu określonej ilości kabla UTP, należy usunąć izolację zewnętrzną przewodu. Po rozpleceniu par przewodów, układa się je w ręce w kolejności opisanej przez wybrany standard (Rys.15). Kolejny krok polega na równym przycięciu przewodów tak, aby nie były dłuższe niż 1,3 cm. Po wsunięciu przewodów do wtyczki umieszczamy ją w gnieździe zaciskarki i mocno zaciskamy.



Rys.15 A) Przewody ułożone zgodnie ze standardem T568-B gotowe do ostatecznego przycięcia na długość. B) Zaciskanie wtyczki RJ45 przy użyciu zaciskarki.

W analogiczny sposób należy wykonać wtyczkę po drugiej stronie kabla. Pozostaje jeszcze sprawdzić poprawność wykonanego przewodu. Możemy to zrobić używając odpowiedniego testera, który najczęściej składa się z generatora i nadajnika (Rys. 16).

Rys. 16 Testery pozwalające na sprawdzenie poprawności połączeń w kablu UTP.

W przypadku braku tego typu urządzeń, test może polegać na połączeniu dwóch komputerów z wykorzystaniem nowego kabla. Po wpięciu przewodu do interfejsów sieciowych, należy skonfigurować karty sieciowe poprzez wpisanie adresów IP należących do tej samej sieci oraz odpowiadającą jej maskę. Najczęściej wykonywany test, przeprowadzany w celu weryfikacji połączenia polega na wywołaniu funkcji ping (protokół ICMP) z parametrem, który określa adres IP odbiorcy. Polecenie to umożliwia przetestowanie połączenia pomiędzy hostami do warstwy trzeciej, w której działa właśnie ten protokół. W przypadku poprawnego połączenia nadawca otrzymuje potwierdzenie odbioru każdego z wysłanych pakietów, co widoczne jest w postaci wyświetlanej informacji dotyczącej czasu, po którym nastąpiła odpowiedź oraz statystyki wszystkich pakietów.

```
C:\>ping 158.75.5.190

Badanie 158.75.5.190 z użyciem 32 bajtów danych:

Odpowiedź z 158.75.5.190: bajtów=32 czas=9ms TTL=252
Odpowiedź z 158.75.5.190: bajtów=32 czas=7ms TTL=252
Odpowiedź z 158.75.5.190: bajtów=32 czas=11ms TTL=252
Odpowiedź z 158.75.5.190: bajtów=32 czas=7ms TTL=252

Statystyka badania ping dla 158.75.5.190:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 7 ms, Maksimum = 11 ms, Czas średni = 8 ms
```

Rys. 17 Badanie połączenia z hostem o adresie IP 158.75.5.190 za pomocą funkcji ping.

W przypadku braku połączenia z innym komputerem, szukanie przyczyny warto rozpocząć od sprawdzenia poprawności działania lokalnej karty sieciowej, poprzez wywołanie funkcji ping 127.0.0.1.

```
C:\>ping 127.0.0.1

Badanie 127.0.0.1 z użyciem 32 bajtów danych:

Odpowiedź z 127.0.0.1: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 127.0.0.1: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 127.0.0.1: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 127.0.0.1: bajtów=32 czas<1 ms TTL=128

Statystyka badania ping dla 127.0.0.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 0 ms, Maksimum = 0 ms, Czas średni = 0 ms
```

Rys. 18 Badanie lokalnej karty sieciowej za pomocą funkcji ping.

Podsumowując warto zauważyć, iż posiadając kilka własnoręcznie zrobionych kabli oraz proste urządzenia sieciowe jak koncentrator i przełącznik Ethernetowy, można tworzyć proste sieci w rozmaitych konfiguracjach, jednocześnie badając ich zachowanie zarówno w normalnych warunkach pracy jak i w przypadku sztucznie wywoływanych awarii. Wykonywanie szeregu testów, zadań oraz praktyczne rozwiązywanie stawianych problemów jest najlepszym sposobem na zaznajomienie uczniów ze światem sieci komputerowych.

Literatura:

1. Vito Amato, Wayne Lewis, „Akademia Sieci Cisco”, Mikom, Warszawa 2001,
2. http://www.dlink.com/
3. http://www.meditronik.com.pl/doc/komp/wireless=karta=pci=3n.htm
4. http://sklep.age.pl/opis.php?m_kod=KSUS_BILL_THUMB.LAN
5. http://www.korins.com/m/cox/p-2-05.htm
6. http://www.assmann.com.pl/text9.htm