

Sieci lokalne

Trochę teorii, nieco praktyki

2000-07-21

Copyright © 2000 Bartosz Kiziukiewicz

Oryginalna wersja tego dokumentu powstała pewien czas temu dla osoby, która w sposób dosyć szybki musiała wejść w świat sieci lokalnych i Internetu. Obserwując jednak pytania, jakie pojawiają się co jakiś czas na grupie *pl.comp.networking* postanowiłem udostępnić go szerszemu gronu ufając, że będzie on służył pomocą początkującym oraz mniej doświadczonym administratorom własnych sieci lokalnych.

Przy tej okazji chciałem złożyć specjalne podziękowania osobom, które na przeczytanie niniejszego opracowania poświęciły swój czas i wysunęły wiele uwag i propozycji dotyczących zawartości opracowania, a które ja skrupulatnie wykorzystałem.

Podziękowania należą się w szczególności:
Ziemkowi Borowskiemu <ziembor@FAQ-bot.ZiemBor.waw.pl>,
Ryszardowi Kulickiemu <ryszardk@unix.sim.com.pl>,
i Romanowi Niewiadomskiemu <newrom@rp.zax.pl>.

Osoby te służyły mi bezinteresowną pomocą wskazując niedociągnięcia i nieścisłości w przygotowanym materiale za co jestem im niezmiernie wdzięczny.

Pewien wkład w powstanie niniejszej pracy miały również grupy *pl.comp.networking* oraz *pl.comp.os.win95* bez których nieświadomego udziału dokument ten prawdopodobnie nigdy by nie powstał a które ukierunkowały moją uwagę na problemy najczęściej nurtujące początkujących adeptów sieci komputerowych.

Jestem oczywiście otwarty na wszelkie uwagi na temat niniejszego opracowania oraz pomysły, które przyczynią się do poszerzenia zawartości merytorycznej tej pracy.

Dokument ten rozpowszechniany jest zgodnie z zasadami licencji GNU GPL.

Z pozdrowieniem
Bartosz Kiziukiewicz
<kiziuk@alpha.net.pl>

WPROWADZENIE TEORETYCZNE	4
MEDIA TRANSMISYJNE	4
<i>Skrętka nieekranowana (UTP – Unshielded Twisted Pair)</i>	<i>4</i>
<i>Skrętka foliowana (FTP – Foiled Twisted Pair).....</i>	<i>4</i>
<i>Skrętka ekranowana (STP – Shielded Twisted Pair)</i>	<i>4</i>
<i>Kategorie kabli miedzianych</i>	<i>4</i>
<i>Kabel współosiowy (koncentryczny).....</i>	<i>4</i>
<i>Kabel światłowodowy.....</i>	<i>5</i>
TOPOLOGIE SIECI LAN.....	5
<i>Sieci LAN typu szyna (Ethernet 10Base-2).....</i>	<i>5</i>
<i>Sieć LAN typu gwiazda (Ethernet - 10Base-T, Fast Ethernet - 100Base-TX)</i>	<i>6</i>
URZĄDZENIA AKTYWNE LAN	6
ŚCIANA OGNI (FIREWALL)	6
ADRESY MAC	7
SPOSOBY TRANSMISJI I ADRESOWANIA W LAN	7
MODEL WARSTWOWY OSI	7
UPROSZCZONY CZTEROWARSTWOWY MODEL SIECI TCP/IP	8
PROTOKOŁY SIECIOWE	8
TCP/IP I INTERNET	8
<i>Adresy IP (IPv4).....</i>	<i>8</i>
<i>Maska sieciowa (IPv4)</i>	<i>9</i>
<i>Adres sieciowy (IPv4).....</i>	<i>10</i>
<i>IPv4 i IPv6.....</i>	<i>10</i>
<i>System nazw domen</i>	<i>10</i>
<i>Adres URL</i>	<i>11</i>
<i>NAT, PAT, IP-Masqarade i serwery Proxy</i>	<i>11</i>
<i>DHCP.....</i>	<i>11</i>
INSTALACJA SIECI LOKALNEJ.....	12
WSTĘP.....	12
ZAKOŃCZENIA KABLI.....	13
KROSOWANIE PRZEWODÓW.....	13
SZAFY DYSTRYBUCYJNA	15
KONFIGURACJA SIECI.....	15
SIEĆ TCP/IP NA WINDOWS 95/98	16
<i>Instalacja karty sieciowej i protokołów.....</i>	<i>16</i>
<i>Konfiguracja TCP/IP.....</i>	<i>17</i>
UDOSTĘPNIANIE POŁĄCZENIA INTERNETOWEGO W SIECI LOKALNEJ.....	17
<i>Konfiguracja SyGate'a.....</i>	<i>18</i>
ŹRÓDŁA.....	19
POZYCJE WYDAWNICZE	19
MIEJSCA W INTERNECIE	19

Wprowadzenie teoretyczne

Media transmisyjne

Skrętka nieekranowana (UTP – Unshielded Twisted Pair)

Kabel typu UTP jest zbudowany ze skręconych ze sobą par przewodów i tworzy linię zrównoważoną (symetryczną). Skręcenie przewodów ze splotem 1 zwój na 6-10 cm chroni transmisję przed interferencją otoczenia. Tego typu kabel jest powszechnie stosowany w sieciach informatycznych i telefonicznych, przy czym istnieją różne technologie splotu, a poszczególne skrętki mogą mieć inny skręt.

Dla przesyłania sygnałów w sieciach komputerowych konieczne są skrętki kategorii 3 (10 Mb/s) i kategorii 5 (100 Mb/s), przy czym powszechnie stosuje się tylko tą ostatnią.

Skrętka foliowana (FTP – Foiled Twisted Pair)

Jest to skrętka ekranowana za pomocą folii z przewodem uziemiającym. Przeznaczona jest głównie do budowy sieci komputerowych umiejscowionych w ośrodkach o dużych zakłóceniach elektromagnetycznych. Stos. jest również w sieciach Gigabit Ethernet (1 Gb/s) przy wykorzystaniu wszystkich czterech par przewodów.

Skrętka ekranowana (STP – Shielded Twisted Pair)

Różni się od skrętki FTP tym, że ekran jest wykonany w postaci opłotu i zewnętrznej koszulki ochronnej. Jej zastosowanie wzrasta w świetle nowych norm europejskich EMC w zakresie emisji EMI (ElectroMagnetic Interference).

Poza wyżej wymienionymi można spotkać także hybrydy tych rozwiązań:

FFTP – każda para przewodów otoczona jest osobnym ekranem z folii, cały kabel jest również pokryty folią.

SFTP – każda para przewodów otoczona jest osobnym ekranem z folii, cały kabel pokryty jest opłotem.

Kategorie kabli miedzianych

Kategorie kabli miedzianych zostały ujęte w specyfikacji EIA/TIA w kilka grup, w których przydatność do transmisji określa się w MHz:

- kategoria 1 – tradycyjna nieekranowana skrętka telefoniczna przeznaczona do przesyłania głosu, nie przystosowana do transmisji danych;
- kategoria 2 – nieekranowana skrętka, szybkość transmisji do 4 MHz. Kabel ma 2 pary skręconych przewodów;
- kategoria 3 – skrętka o szybkości transmisji do 10 MHz, stos. w sieciach Token Ring (4 Mb/s) oraz Ethernet 10Base-T (10 Mb/s). Kabel zawiera 4 pary skręconych przewodów;
- kategoria 4 – skrętka działająca z szybkością do 16 MHz. Kabel zbudowany jest z czterech par przewodów;
- kategoria 5 – skrętka z dopasowaniem rezystancyjnym pozwalająca na transmisję danych z szybkością 100 MHz pod warunkiem poprawnej instalacji kabla (zgodnie z wymaganiami okablowania strukturalnego) na odległość do 100 m.
- kategoria 6 – skrętka umożliwiająca transmisję z częstotliwością do 200 MHz;
- kategoria 7 – kabel o przepływności do 600 MHz. Będzie wymagać już stosowania nowego typu złączy w miejsce RJ-45 oraz kabli każdą parą ekranowaną oddzielnie.

Kabel współosiowy (koncentryczny)

Początkowo stosowany był jako zamiennik dla standardu ARCnet. Składa się z dwóch przewodów koncentrycznie umieszczonych jeden wewnątrz drugiego, co zapewnia większą odporność na zakłócenia a tym samym wyższą jakość transmisji. Powszechnie stos. się dwa rodzaje kabli koncentrycznych – o impedancji falowej 50 i 75 Ohm, przy czym te pierwsze stosuje się m.in. w sieciach komputerowych. Obecnie kabel współosiowy jest stosowany tylko w bardzo małych sieciach (do 3-4 komputerów) stawianych możliwie najniższym kosztem. Wadą tego rozwiązania jest dosyć duża (w porównaniu z siecią na skrętce) awaryjność instalacji.

Kabel światłowodowy

Transmisja światłowodowa polega na prowadzeniu przez włókno szklane promieni optycznych generowanych przez laserowe źródło światła. Ze względu na znikome zjawisko tłumienia, a także odporność na zewnętrzne pola elektromagnetyczne, przy braku emisji energii poza tor światłowodowy, światłowód stanowi obecnie najlepsze medium transmisyjne.

Medium transmisyjne światłowodu stanowi czyste szklane włókno kwarcowe wykonane z dwutlenku krzemu (o przekroju kołowym), w którym światło jest zamknięte przez otoczenie nieprzezroczystym płaszczem centralnie położonego rdzenia. Dla promieni świetlnych o częstotliwości w zakresie bliskim podczerwieni współczynnik odbicia światła w płaszczu jest mniejszy niż w rdzeniu, co powoduje całkowite wewnętrzne odbicie promienia i prowadzenie go wzdłuż osi włókna.

Topologie sieci LAN

Topologia LAN określa sposób wzajemnego połączenia stacji w sieci. Wyróżnia się cztery najczęściej stosowane topologie LAN:

- szynowa (bus) – pakiet wysyłany przez dowolną stację sieciową dociera, za pośrednictwem medium, do wszystkich stacji sieciowych,
- pierścieniowa (ring) – stacje sieciowe podłączone są do okablowania tworzącego pierścień. Topologię pierścienia stosuje się w technologiach Token Ring/IEEE 802.5 i FDDI,
- gwiazdzista (star) – kable sieciowe połączone są w jednym wspólnym punkcie, w którym znajduje się koncentrator lub przełącznik,
- drzewiasta (tree) – jest strukturą podobną do topologii szynowej, z tą różnicą, że są tu możliwe gałęzie z wieloma węzłami.

Wymienione topologie są strukturami logicznymi i technicznie nie muszą być w taki sposób zorganizowane. Na przykład logicznie rozumiane topologia szynowa i pierścieniowa są zorganizowane jako gwiazda fizyczna.

Obecnie stosuje się w lokalnych sieciach komputerowych powszechnie praktycznie tylko topologię pierścieniową i topologię szynową.

Sieci LAN typu szyna (Ethernet 10Base-2)

Zbudowane są z wykorzystaniem kabla koncentrycznego 50 Ohm RG-58 (tzw. cienki koncentryk). Długość jednego segmentu sieci (czyli od jednego końca do drugiego) nie może dla cienkiego koncentryka przekraczać 185 m. Komputery są dołączone do kabla za pomocą trójników. Każdy segment sieci musi być ponadto na końcach wyposażony w terminatory o oporności przystosowanej do impedancji falowej kabla (powszechnie jest to 50 Ohm).

Zalety:

- jest mało wrażliwy na zakłócenia i szumy;
- nadaje się do sieci z przesyłaniem modulowanym (szerokopasmowym)
- jest tańszy niż ekranowany kabel skręcany

Wady:

- łatwo ulega uszkodzeniom
- trudności przy lokalizowaniu usterki
- jakakolwiek usterka kabla bądź połączeń powoduje awarię całej sieci
- podłączenie nowego komputera wymaga rozpięcia kabla co skutkuje unieruchomieniem całej sieci

Sieć LAN typu gwiazda (Ethernet - 10Base-T, Fast Ethernet - 100Base-TX)

Jest powszechnie stosowana ze względu na dużo mniejszą awaryjność, niż sieć zbudowana w oparciu o kabel koncentryczny. Długość kabla od koncentratora do komputera nie może przekraczać 100 m.

Zalety:

- jest akceptowany przez wiele rodzajów sieci
- łatwa instalacja (standardowo instalowany w nowych budynkach)
- duża niezawodność
- awaria bądź rozpięcie kabla powoduje tylko odcięcie jednego stanowiska
- stosunkowa łatwość lokalizacji usterki

Wady:

- ograniczona długość odcinków kabla z uwagi na małą odporność na zakłócenia
- większy koszt instalacji niż w przypadku kabla koncentrycznego

Pozostałe dwie topologie ze względu na znikome obecnie zastosowanie nie będą omówione.

Urządzenia aktywne LAN

Sieci LAN buduje się z biernych i aktywnych urządzeń sieciowych. Bierne urządzenia sieciowe to komponenty systemów okablowania strukturalnego.

Do aktywnych urządzeń sieci LAN należą:

- regenerator (repeater) – jest urządzeniem pracującym w warstwie fizycznej modelu OSI, stosowanym do łączenia segmentów kabla sieciowego. Regenerator odbierając sygnały z jednego segmentu sieci wzmacnia je, poprawia ich parametry czasowe i przesyła do innego segmentu.
- koncentrator (hub) – jest czasami określany jako wieloportowy regenerator. Służy do tworzenia fizycznej gwiazdy przy istnieniu logicznej struktury szyny lub pierścienia. Pakiety wchodzące przez jeden port są transmitowane na wszystkie inne porty. Wynikiem tego jest fakt, że koncentratory pracują w trybie half-duplex (transmisja tylko w jedną stronę w tym samym czasie).
- przełącznik (switch) – są urządzeniami warstwy łącza danych (warstwy 2) i łączą wiele fizycznych segmentów LAN w jedną większą sieć. Przełączniki działają podobnie do koncentratorów z tą różnicą, że transmisja pakietów nie odbywa się z jednego wejścia na wszystkie wyjścia przełącznika, ale na podstawie adresów MAC kart sieciowych przełącznik uczy się, a następnie kieruje pakiety tylko do konkretnego odbiorcy co powoduje wydajne zmniejszenie ruchu w sieci. W przeciwieństwie do koncentratorów, przełączniki działają w trybie full-duplex (jednoczesna transmisja w obu kierunkach).
- most (bridge) – służy do przesyłania i ew. filtrowania ramek między dwoma sieciami. Śledzi adresy MAC umieszczane w przesyłanych do nich pakietach. Mosty nie mają dostępu do adresów warstwy sieciowej, dlatego nie można ich użyć do dzielenia sieci opartej na protokole TCP/IP na dwie podsieci IP. To zadanie mogą wykonywać wyłącznie routery. Analizując adresy MAC, urządzenie wie, czy dany pakiet należy wyekspediować na drugą stronę mostu, czy pozostawić bez odpowiedzi. Mosty podobnie jak przełączniki przyczyniają się w znacznym stopniu do zmniejszenia ruchu w sieci.
- router – urządzenie wyposażone najczęściej w kilka interfejsów sieciowych LAN, porty obsługujące sieć WAN, pracujący wydajnie procesor i oprogramowanie zawiadujące ruchem pakietów przepływających przez router. W sieciach lokalnych stos. są gdy sieć chcemy podzielić na dwie lub więcej podsieci. Segmentacja sieci powoduje, że poszczególne podsieci są od siebie odseparowane i pakiety nie przenikają z jednej podsieci do drugiej. W ten sposób zwiększamy przepustowość każdej podsieci.

Ściana ognia (firewall)

Kiedy sieć lokalna podłączona jest do Internetu, odbywa się to poprzez router lub inne urządzenie pełniące funkcję bramy do Internetu. Kluczowym problemem jest zapewnienie bezpieczeństwa sieci lokalnej przed dostępem z zewnątrz. Funkcją taką pełni właśnie firewall. Pozwala ograniczyć dostęp z zewnątrz pozostawiając możliwość ruchu w kierunku odwrotnym.

Ściana ognia wyposażona jest w dwa rodzaje filtrów – proxy aplikacyjne pozwalające na filtrowanie wybranych usług sieciowych takich, jak ftp, telnet, finger bez konieczności ręcznego definiowania filtrów, oraz tzw. filtry pakietów – proste, pozwalające na filtrowanie informacji w zależności od zawartości nagłówek, lub bardziej skomplikowane.

Adresy MAC

Adresy MAC (Media Access Control) są podzbiorem adresów warstwy 2 modelu OSI. Adres MAC ma 48 bitów. Składa się z dwóch podstawowych części: w pierwszej zapisany jest kod producenta karty sieciowej, przydzielany przez IEEE (Institute of Electrical and Electronic Engineers), a w drugiej – unikatowy adres karty sieciowej tego producenta.

Pod adresem <http://standards.ieee.org/regauth/oui/oui.txt> można znaleźć spis wszystkich MAC-adresów przyporządkowanych poszczególnym producentom.

Sposoby transmisji i adresowania w LAN

Wyróżnia się trzy sposoby transmisji i adresowania w LAN:

- Transmisja pojedyncza Unicast – stacja nadawcza adresuje pakiet używając adresu stacji odbiorczej. Pojedynczy pakiet jest wysyłany przez stację nadawczą do stacji odbiorczej.
- Transmisja grupowa Multicast – stacja nadawcza adresuje pakiet używając adresu multicast. Pojedynczy pakiet danych jest wysyłany do grupy stacji sieciowych (określonej przez adres multicast).
- Transmisja rozgłoszeniowa Broadcast – stacja nadawcza adresuje pakiet używając adresu broadcast. W tym typie transmisji pakiet jest wysyłany do wszystkich stacji sieciowych.

Model warstwowy OSI

Model OSI (Open Systems Interconnection) opisuje sposób przepływu informacji między aplikacjami software'owymi w jednej stacji sieciowej a software'owymi aplikacjami w innej stacji sieciowej przy użyciu kabla sieciowego. Model OSI jest ogólnym modelem koncepcyjnym, skomponowanym z siedmiu warstw, z których każda opisuje określone funkcje sieciowe. Nie określa szczegółowych metod komunikacji. Mechanizmy rzeczywistej komunikacji są określone w formie protokołów komunikacyjnych. Dzieli on zadanie przesyłania informacji między stacjami sieciowymi na siedem mniejszych zadań składających się na poszczególne warstwy. Zadanie przypisane każdej warstwie ma charakter autonomiczny i może być interpretowane niezależnie.

Warstwy OSI:

- warstwa 7 – Aplikacji. Jest bramą, przez którą procesy aplikacji dostają się do usług sieciowych. Ta warstwa prezentuje usługi, które są realizowane przez aplikacje (przesyłanie plików, dostęp do baz danych, poczta elektroniczna itp.)
- warstwa 6 - Prezentacji danych. Odpowiada za format używany do wymiany danych pomiędzy komputerami w sieci. Na przykład kodowanie i dekodowanie danych odbywa się w tej warstwie. Większość protokołów sieciowych nie zawiera tej warstwy.
- warstwa 5 – Sesji. Pozwala aplikacjom z różnych komputerów nawiązywać, wykorzystywać i kończyć połączenie (zwane sesją). Warstwa ta tłumaczy nazwy systemów na właściwe adresy (na przykład na adresy IP w sieci TCP/IP).
- warstwa 4 – Transportu. Jest odpowiedzialna za dostawę wiadomości, które pochodzą z warstwy aplikacyjnej. U nadawcy warstwa transportu dzieli długie wiadomości na kilka pakietów, natomiast u odbiorcy odtwarza je i wysyła potwierdzenie odbioru. Sprawdza także, czy dane zostały przekazane we właściwej kolejności i na czas. W przypadku pojawienia się błędów warstwa żąda powtórzenia transmisji danych.
- warstwa 3 – Sieciowa. Kojarzy logiczne adresy sieciowe i ma możliwość zamiany adresów logicznych na fizyczne. U nadawcy warstwa sieciowa zamienia duże pakiety logiczne w małe fizyczne ramki danych, zaś u odbiorcy składa ramki danych w pierwotną logiczną strukturę danych.
- warstwa 2 - Łączy transmisyjnego (danych). Zajmuje się pakietami logicznymi (lub ramkami) danych. Pakuje nieprzetworzone bity danych z warstwy fizycznej w ramki, których format zależy od typu sieci: Ethernet lub Token Ring. Ramki używane przez tą warstwę zawierają fizyczne adresy nadawcy i odbiorcy danych.

- warstwa 1 – Fizyczna. Przesyła nieprzetworzone bity danych przez fizyczny nośnik (kabel sieciowy lub fale elektromagnetyczne w przypadku sieci radiowych). Ta warstwa przenosi dane generowane przez wszystkie wyższe poziomy.

przy czym warstwy 1 do 4 są to tzw. warstwy niższe (transport danych) zaś warstwy 5 do 7 to warstwy wyższe (aplikacje).

Model OSI nie odnosi się do jakiegokolwiek sprzętu lub oprogramowania. Zapewnia po prostu strukturę i terminologię potrzebną do omawiania różnych właściwości sieci.

Uproszczony czterowarstwowy model sieci TCP/IP

Siedmiowarstwowy model OSI nie jest dokładnym wykazem – daje jedynie wskazówki, jak organizować wszystkie usługi sieciowe. W większości zastosowań przyjmuje się model warstwowy usług sieciowych, który może być odwzorowany w modelu odniesienia OSI. Na przykład model sieciowy TCP/IP można adekwatnie wyrazić przez uproszczony model odniesienia.

Aplikacje sieciowe zazwyczaj zajmują się trzema najwyższymi warstwami (sesji, prezentacji i aplikacji) siedmiowarstwowego modelu odniesienia OSI. Stąd te trzy warstwy mogą być połączone w jedną zwaną warstwą aplikacyjną.

Dwie najniższe warstwy modelu OSI (fizyczną i łącza transmisyjnego) także można połączyć w jedną warstwę. W efekcie otrzymujemy uproszczony czterowarstwowy model:

- warstwa 4 – Aplikacyjna – poczta, transmisja plików, telnet
- warstwa 3 – Transportu – TCP (Transmission Control Protocol) – protokół sterujący transmisją
- warstwa 2 – Sieciowa – IP (Internet Protocol) – protokół internetowy
- warstwa 1 – Fizyczna – Ethernet (karta sieciowa i połączenia sieciowe)

W każdej z tych warstw informacje są wymieniane przez jeden z wielu protokołów sieciowych.

Protokoły sieciowe

Protokół sieciowy wyjaśnia cały uprzednio uzgodniony przez nadawcę i odbiorcę proces wymiany danych na określonej warstwie modelu sieciowego. W uproszczonym czterowarstwowym modelu sieciowym można wyróżnić następujące protokoły:

- Protokoły warstwy fizycznej: Ethernet, Token Ring
- Protokoły warstwy sieciowej: protokół internetowy (IP) będący częścią zestawu protokołów TCP/IP
- Protokoły warstwy transportu: protokół sterowania transmisją w sieci (TCP/IP) i protokół datagramów użytkownika (UDP), które są częścią zestawu protokołów TCP/IP
- Protokoły warstwy aplikacyjnej: protokół przesyłania plików (FTP), prosty protokół przysyłania poczty (SMTP), usługi nazewnictwa domen (DNS), telnet, protokół przesyłania hipertekstu (HTTP), prosty protokół zarządzania siecią (SNMP), które także są częścią zestawu protokołów TCP/IP

Określenie „zestaw protokołów” oznacza dwa lub więcej protokołów z tych warstw, które stanowią podstawę sieci.

Kilka najlepiej znanych zestawów protokołów to:

- zestaw protokołów IPX/SPX (międzysieciowa wymiana pakietów/sekwencyjna wymiana pakietów) używany przez system Novell Netware
- NetBIOS i NetBEUI (rozszerzony interfejs użytkownika podstawowego sieciowego systemu wejścia/wyjścia) wykorzystywany przez system operacyjny Microsoftu
- zestaw protokołów TCP/IP

TCP/IP i Internet

Szczegóły każdego protokołu TCP/IP są przedstawione w dokumentacji RFC (Request for Comments) – żądanie odpowiedzi.

Adresy IP (IPv4)

W sieciach TCP/IP adres komputera zwany jest adresem IP. Oryginalny adres IP jest czterobajtową (32 bitową) liczbą. Przyjęła się konwencja zapisu każdego bajtu w postaci dziesiętnej i oddzielania ich kropkami. Ten sposób zapisu zwany jest notacją kropkowo-dziesiętną.

Bity w adresie IP są interpretowane jako: <adres sieciowy, adres hosta>

Określona liczba bitów 32-bitowego adresu IP jest adresem sieciowym, a reszta adresem hostowym. Adres sieciowy określa sieć LAN, zaś adres hosta konkretną stację roboczą w tej sieci.

By dopasować sieci o różnych rozmiarach (różnej liczbie komputerów), adresy IP podzielono na kilka klas. Istnieje pięć klas adresów IP: A, B, C, D oraz E, z czego tylko A, B i C są wykorzystywane do adresowania sieci i hostów, a D i E są zarezerwowane do zastosowań specjalnych.

Klasa A obsługuje 126 sieci, z których każda ma ponad 16 milionów hostów (ponieważ pomimo tego, że jest to adres 7-bitowy, to wartości 0 i 127 mają specjalne znaczenie).

Adresy klasy B są przeznaczone dla sieci o rozmiarach do 65534 hostów. Może być co najwyżej 16384 sieci w klasie B.

Adresy klasy C przeznaczone są dla małych organizacji. Każda klasa C może mieć do 254 hostów, a klas może być ponad 2 miliony.

Klasę sieci można określić na podstawie pierwszej liczby w notacji kropkowo-dziesiętnej:

- klasa A: 1.xxx.xxx.xxx do 126.xxx.xxx.xxx
- klasa B: 128.zzz.xxx.xxx do 191.zzz.xxx.xxx
- klasa C: 192.zzz.zzz.xxx do 223.zzz.zzz.xxx

Adres z samymi zerami wskazuje na lokalną sieć. Adres 0.0.0.150 wskazuje na host z numerem 150 w tej sieci klasy C.

Adres 127.xxx.xxx.xxx klasy A jest używany do testu zwrotnego (loopback) – komunikacji hosta z samym sobą. Zazwyczaj jest to adres 127.0.0.1. Proces próbujący połączyć się z innym procesem na tym samym hoście, używa adresu zwrotnego aby uniknąć wysyłania pakietów przez sieć.

Włączenie wszystkich bitów w jakiejś części adresu oznacza komunikat sieciowy (broadcast). Na przykład adres 128.18.255.255 oznacza wszystkie hosty w sieci 128.18 klasy B. Adres 255.255.255.255 oznacza, że wszystkie węzły danej sieci otrzymają ten pakiet.

Należy jednak podkreślić, że mniej więcej od roku 1997 podział na klasy sieci jest już nie aktualny. Obecnie adresy IPv4 są przydzielane bez specjalnego zwracania uwagi na klasy sieci - wg założeń CSDIR (classless routinig).

Dokument RFC 1918 („Address Allocation for Private Internets”) określa, jakie adresy IP mogą być użyte wewnątrz prywatnej sieci. Zarezerwowane są dla nich trzy grupy adresów IP:

- od 10.0.0.0 do 10.255.255.255
- od 172.16.0.0 do 172.16.255.255
- od 192.168.0.0 do 192.168.255.255

Nie należy w sieciach lokalnych stosować dowolnych adresów IP, gdyż może przyczynić się to do różnorodnych problemów mających swe źródło w dublowaniu się adresów IP w sieci lokalnej oraz w Internecie.

Maska sieciowa (IPv4)

Jest to adres IP, który ma jedyne na pozycjach bitów odpowiadających adresom sieciowym i zera na pozostałych (odpowiadających adresom hosta). Klasa adresów sieciowych wyznacza maskę sieciową.

Adresy klasy A mają maskę 11111111000000000000000000000000 czemu w zapisie kropkowo-dziesiętnym odpowiada 255.0.0.0, klasy B: 11111111111111110000000000000000 (255.255.0.0) klasy C zaś: 11111111111111111111111100000000 (255.255.255.0). Dla wygody używany jest najczęściej zapis kropkowo-dziesiętny. Należy jednak pamiętać, że maska (jak również adres IP) zapisana jest stricte w postaci binarnej.

Należy również zauważyć, że zwłaszcza ostatnio zaczęto nadawać maski nie będące czysto maskami wg klas adresów IP (czyli takich, w których liczba jedynek jest wielokrotnością oktetów – liczby 8), lecz zwiększając liczbę jedynek przy takiej samej liczbie bitów (32). Umożliwiło to uzyskanie maski np. 11111111111111111111111111000000 (255.255.255.224) co pozwala na objęcie podsiecią 30 hostów.

Poniższa tabela przedstawia wszystkie możliwe podsieci dla zakresu od 2 do 254 hostów:

Liczba hostów	Maska podsieci	
	w postaci binarnej	w postaci dziesiętnej
2	11111111111111111111111111111100	255.255.255.252

Adres URL

URL jest adresem lokalizującym zasób w Internecie. Składa się z trzech głównych części:

- identyfikatora usługi
określa m.in. następujące typy usług:
 - http://
 - ftp://
 - gopher://
 - telnet://
- nazwy domeny
może składać się z adresu domenowego lub adresu kropkowo-dziesiętnego np. www.firma.com lub 148.81.78.1. Określa nazwę nadaną serwerowi lub jego adres IP
- ścieżki dostępu
np. /tracking/ - określa ścieżkę katalogową na serwerze prowadzącą do pliku, który ma być sprowadzony.

Wadą adresu URL jest jego nietrwałość. Zmiana położenia dokumentu w systemie katalogów plików powoduje utratę ważności wszystkich istniejących do niego odniesień.

NAT, PAT, IP-Masqarade i serwery Proxy

Są to technologie umożliwiające współdzielenie jednego publicznego adresu IP w celu umożliwienia dostępu do Internetu przez wiele komputerów w sieci lokalnej. Stosowane są dlatego, że liczba publicznych adresów IP (mowa tu cały czas o IPv4) jest dużo mniejsza, niż liczba komputerów podłączonych do Internetu.

Chcąc umożliwić dostęp wielu komputerom w sieci lokalnej do Internetu przy pomocy tylko jednego adresu IP należy zastosować urządzenie (najczęściej jest to po prostu komputer) podłączone z Internetem pełniące funkcję tzw. bramy z przydzielonym publicznym adresem IP i połączonym z siecią lokalną. Komputerom w sieci lokalnej przydziela się adresy z prywatnej puli adresów IP (takie, które nie występują już w Internecie-określone odpowiednimi normami i zwane adresami nieroutowalnymi). Dzięki takiemu rozwiązaniu każdy komputer w danej sieci lokalnej ma możliwość dostępu do Internetu, zaś z zewnątrz cała sieć lokalna jest widziana jako jeden host.

Technologia NAT (Network Address Translation) polega na mapowaniu adresów zewnętrznych IP do jednego lub więcej adresów IP hostów wewnętrznych.

Technologie PAT (Port Address Translation) oraz IP-Masqarade polegają na tym, że komputer pełniący funkcję bramy zajmuje się takim modyfikowaniem ramek pakietów wchodzących i wychodzących z sieci lokalnej, aby możliwy był dostęp poprzez pojedynczy publiczny adres IP, a pakiety przychodzące docierały do właściwych komputerów w sieci lokalnej.

Nieco inna jest filozofia działania proxy serwerów. Są to dodatkowe serwery pośredniczące pomiędzy klientem (np. przeglądarką WWW) a serwerem docelowym. Serwer taki posiada własny cache w którym przechowuje pliki pobrane wcześniej przez użytkowników co pozwala na szybszy dostęp do odwiedzonych wcześniej stron.

DHCP

DHCP jest usługą umożliwiającą dynamiczne przydzielanie adresów IP (z zadanej puli) komputerom w sieci LAN podczas konfiguracji w tych komputerach stosu TCP/IP przez jądro systemu lub skrypty startowe. Zajmuje się tym komputer noszący nazwę serwera DHCP. Umożliwia to zwolnienie administratora sieci od przydzielania ręcznie adresów statycznych IP każdemu z komputerów z osobna.

Takie działanie nie wyklucza jednak przydzielania adresów statycznych (również tych rozdzielanych przez serwer - co oznacza, że komputerowi przydzielany jest zawsze taki sam, z góry określony adres IP).

Instalacja sieci lokalnej

Wstęp

Proces instalacji sieci lokalnej należy rozpocząć od poczynienia pewnych wstępnych założeń, które są niezbędne do jej zbudowania. Są to:

- wybór fizycznej topologii sieci
obecnie do wyboru są praktycznie tylko dwie topologie: topologia typu szyna oraz typu gwiazda. Współcześnie stosuje się powszechnie tylko drugie rozwiązanie ze względów omówionych w części teoretycznej. Należy wspomnieć, że stosuje się często, zwłaszcza w dużych sieciach topologie mieszane polegające na łączeniu małych skupisk stacji z zastosowaniem topologii gwiazdowej, zaś skupiska te dołącza się do jednej szyny typu bus.
- wybór przepustowości sieci
przepustowość sieci lokalnej w głównej mierze zależy od tego, do czego dana sieć ma być wykorzystywana. Do wyboru są praktycznie dwie technologie: sieć 10Base-T (zbudowana na skrętce, o przepustowości 10 Mb/s) oraz sieć 100Base-TX (skrętka, o przepustowości 100 Mb/s). W przypadku kabla koncentrycznego RG-58 przepustowość łącza wynosi 10 Mb/s. Rozwiązania typu Gigabit Ethernet (1000Base-T) są jak dotąd, ze względu na koszty, nieopłacalne w małych sieciach.
- określenie miejsca lokalizacji gniazd przyłączeniowych oraz miejsca umieszczenia szafy dystrybucyjnej z aktywnym osprzętem sieciowym (koncentratory, przełączniki itp.).
- zaprojektowanie logicznej struktury sieci
w tym punkcie należy określić, czy sieć będzie mała, czy będzie na tyle duża, że opłacalne będzie (ze względów funkcjonalnych i wydajnościowych) podzielenie jej na podsieci z wykorzystaniem przełączników, mostów itp.
- sporządzenie wstępnego kosztorysu inwestycji przy uwzględnieniu liczby koniecznych urządzeń, długości zastosowanego kabla, liczby gniazd przyłączeniowych, długości listew kablowych, liczby kołków rozporowych, itd.

Wymienione powyżej czynności można określić wspólnym mianem zaprojektowania sieci.

Należy przy tym pamiętać o kilku zasadach:

- długość jednego segmentu sieci 10Base-2 nie może przekraczać 185 m
- końce każdego segmentu sieci 10Base-2 muszą być zakończone trójnikami z zapiętymi na nich terminatorami 50 Ohm
- długość kabla wraz z przyłączami w sieciach 10Base-T i 100Base-TX nie może przekraczać 100 m. W praktyce przyjmuje się, że długość kabla wynosi 90 m zaś 10 m rezerwuje się na patchcordy (szafa+podłączenie do gniazdk)
- dla sieci 10Base-T można połączyć kaskadowo maksymalnie 4 koncentratory (przy pomocy łącza UpLink), zaś dla sieci 100Base-TX można połączyć kaskadowo tylko 2. Przy większej ilości należy już stosować przełączniki
- kable sieciowe nie mogą być prowadzone wzdłuż kabli energetycznych w odległości mniejszej niż 20 cm, oraz w bezpośredniej bliskości innych źródeł zakłóceń elektromagnetycznych (silniki, transformatory, inne urządzenia elektryczne dużej mocy itp.)
- jeśli istnieje konieczność krzyżowania się kabli sieciowych z instalacją elektryczną, to powinno być one wykonane pod kątem 90 stopni
- jeżeli instalacja sieciowa jest prowadzona jedną listwą kablową wraz z dedykowaną instalacją zasilającą, to powinny być one od siebie separowane przegrodami z PCV
- promień skrętu kabla UTP nie powinien być mniejszy, niż ośmiokrotna jego średnica. Taką wartość przyjmuje większość producentów Systemów Okablowania
- przy spinaniu kilku kabli ze sobą nie należy ściągać spinki do stopnia powodującego deformację wiązki. Kable po ich spięciu powinny się móc przesuwac
- nie należy rozciągać kabli
- nie należy prowadzić kabli UTP na zewnątrz budynku. Może to spowodować niebezpieczne w skutkach przepięcia wynikłe na przykład z uderzenia pioruna

Należy pamiętać też o tym, że w zależności od szybkości transmisji, jaka ma odbywać się w sieci, stosowany powinien być różny kabel, tzn. dla sieci 10Base-T należy stosować skrętkę przynajmniej 3 kategorii (powszechnie stos. się okablowanie kategorii 5), zaś dla sieci 100Base-TX stosowanie skrętki co najmniej 5 kategorii jest działaniem obligatoryjnym. Należy jednak zauważyć, że w chwili obecnej nie ma zatwierzonego jeszcze standardu kategorii 6. Prace nad jego wprowadzeniem są jednak prowadzone.

Ponadto krótkie odcinki takie jak przewody przyłączeniowe (tzw. patchcordy) powinny być wykonane z linki, natomiast dłuższe odcinki powinny być prowadzone drutem ze względu na jego lepsze parametry transmisyjne. Nie ma to co prawda dużego znaczenia w sieciach 10 Mb/s, ale przy prędkości 100 Mb/s (Fast Ethernet) odcinki prowadzone linką UTP nie powinny być dłuższe niż około 15 m.

Generalnie nie prowadzi się kanałów przesyłowych linką tylko drutem z co najmniej dwóch powodów. Po pierwsze drut jest blisko dwukrotnie tańszy od linki. Po drugie instalacja jest przedsięwzięciem na wiele lat, a jak wiadomo, wymagania szybko idą naprzód. Dziś chcemy 10 Mb/s, jutro 100 Mb/s.

Patchcordy powinny być natomiast wykonane linką ze względu na jej większą elastyczność (wielokrotne przeginanie wiszącego kabla), oraz fakt, że wtyczki RJ-45 dużo lepiej zaciskają się na lince, niż drucie.

Przy sieci Fast Ethernet zalecane jest również stosowanie skrętki FTP lub STP. Jednakże nie stosuje się skrętki FTP lub STP bez ekranowania pozostałych elementów systemu, gdyż daje to odwrotny efekt. Ekran ma sens tylko wtedy, gdy zarówno kabel, jak i pozostałe elementy są ekranowane. Tylko wówczas istnieje możliwość prawidłowego uziemienia tego ekranu. Wiąże się to oczywiście z większymi kosztami takiej instalacji.

Zakończenia kabli

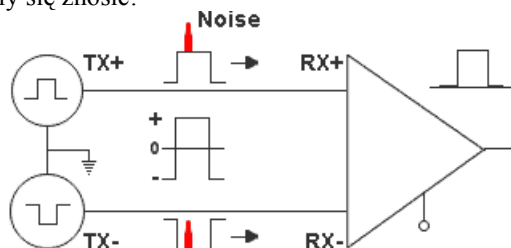
Kable skrętkowe w instalacji naściennej powinny być zakończone gniazdami standardu RJ-45 przy czym w punkcie przyłączeniowym powinna być zainstalowana puszka z tymże rodzajem gniazda, zaś od strony szafy dystrybucyjnej kable powinny być dołączone do patchpanela o odpowiedniej liczbie gniazd.

Do wciskania przewodów w gniazda powinna być wykorzystywana specjalna wciskarka produkcji np. Krone.

Tzw. patchcordy czyli odcinki kabla połączeniowego powinny być zakończone wtyczkami RJ-45 zaciśniętymi przy pomocy odpowiedniej zaciskarki.

Krosowanie przewodów

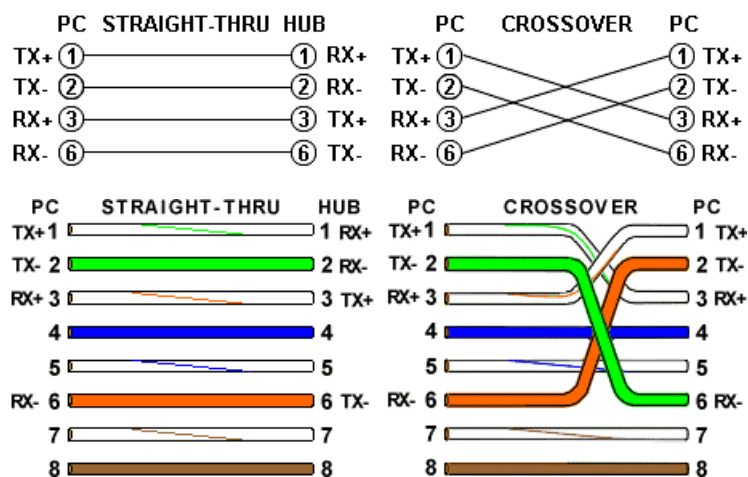
Do prawidłowego działania kabla konieczne jest, aby pary przewodów były we właściwy sposób podłączone tak, aby powstające zakłócenia mogły się znosić:



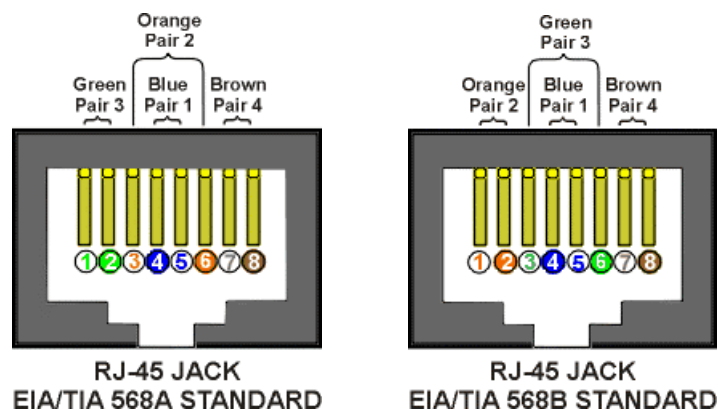
Kolejność podłączenia przewodów skrętki jest opisana dwoma normami EIA/TIA 568A oraz 568B.

Dla połączenia komputera z koncentratorem lub przełącznikiem stosuje się tzw. kabel prosty (straight-thru cable), który z obu stron podłączony jest tak samo wg standardu 568A lub 568B. Dla połączenia bezpośrednio dwóch komputerów bez pośrednictwa huba konieczna jest taka zamiana par przewodów, aby sygnał nadawany z jednej strony mógł być odbierany z drugiej. Ten kabel nosi nazwę kabla krosowego (cross-over cable) i charakteryzuje się tym, że jeden koniec podłączony jest wg standardu 568A zaś drugi 568B.

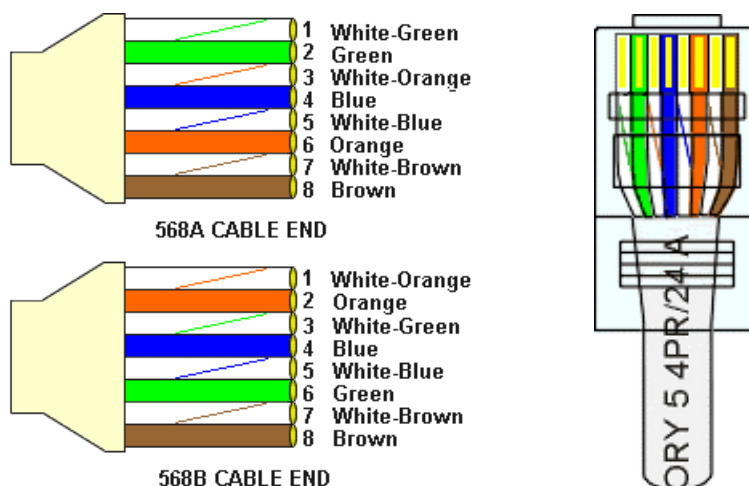
Odpowiednikiem kabla krosowego w połączeniu dwóch hubów jest gniazdo UpLink. Przy połączeniu kaskadowo dwóch hubów kablem prostym jeden koniec kabla podłączamy do jednego z portów huba pierwszego, zaś drugi koniec podłączony musi być do huba drugiego do portu UpLink. Przy podłączeniu kablem krosowym dwóch hubów, oba końce kabla muszą być dołączone do portów zwykłych lub do portów UpLink.



Jeżeli połączenie wykonywane jest kablem prostym to zaleca się stosowanie standardu 568A ze względu na to, że elementy sieciowe typu patchpanel lub gniazdo przyłączeniowe mają naniesione kody barwne przewodów tylko w standardzie 568A lub w obu standardach.



Są więc tylko dwa rodzaje końców kabla, które odpowiadają normom EIA/TIA 568A oraz EIA/TIA 568B. W skrętce 5 kategorii są cztery pary przewodów. Każda para składa się z przewodu o danym kolorze, oraz przewodu białego oznaczonego kolorowym paskiem o kolorze tym samym, co skręcony z nim przewód przy czym przewód z paskiem jest przed przewodem w kolorze jednolitym. Wyjątek stanowi para niebieska, która ma kolejność odwrotną:



Kolejność przewodów wg standardu EIA/TIA 568A jest następująca:

1. biało-zielony
2. zielony
3. biało-pomarańczowy

4. niebieski
5. biało-niebieski
6. pomarańczowy
7. biało-brązowy
8. brązowy

Kolejność przewodów wg standardu EIA/TIA 568B jest następująca:

1. biało-pomarańczowy
2. pomarańczowy
3. biało-zielony
4. niebieski
5. biało-niebieski
6. zielony
7. biało-brązowy
8. brązowy

Przed włożeniem przewodów we wtyczkę, zewnętrzna izolacja kabla UTP powinna zostać ściągnięta na odcinku około 12 mm i wsunięta we wtyczkę w podanej powyżej kolejności.

Należy pamiętać, aby podczas montowania kabla w przyłączach gniazd nie dopuścić do rozkręcenia par przewodu na odcinku większym niż 13 mm gdyż może spowodować to zmniejszenie odporności na zakłócenia.

Po podłączeniu wszystkich przewodów należy sprawdzić ciągłość połączeń. Do tego celu najlepiej użyć testera do sieci skrętkowych, dzięki któremu można szybko się zorientować, czy któraś para w kablu nie przewodzi lub urządzenie do wykonywania pomiarów sieci, które ponadto stwierdzi jakość okablowania.

Szafa dystrybucyjna

Wszystkie przewody sieciowe powinny schodzić się w jednym miejscu, w którym powinna być umieszczona szafa dystrybucyjna. W zależności od liczby urządzeń w szafce stosuje się różne jej wielkości. Standardowa szafka dystrybucyjna ma szerokość 19 cali i wysokość będącą wielokrotnością standardowej wysokości urządzeń przeznaczonych do montażu w tejże szafce. Wysokość podaje się w jednostkach U gdzie jedno U to jedno urządzenie - około 4,45 cm. Szafy mogą być budowane jako dzielone, bądź niedzielone.

W praktyce stosuje się szafy wiszące, trójdzielne bądź szafy stojące z możliwością otwierania wszystkich boków. Chodzi o to aby można było zaglądać i kontrolować pracę szafy bez przerywania pracy Systemu. Warto dodać, że zarówno w gnieździe jak i przy szafie należy pozostawić taki nadmiar przewodu aby zapewnić możliwość zerwania i ponownego zarobienia przewodu albo np. zdjęcia lub odsunięcia szafy do malowania.

Typowe oznaczenia szaf to np. 6U1S czyli szafa niedzielona na 6 urządzeń.

Konfiguracja sieci

W przypadku systemu Windows 95/98, bo taki system najczęściej jest używany (co oczywiście nie oznacza, że jest systemem ze wszech miar najlepszym ;-), konfiguracja sieci jest zadaniem względnie prostym ze względu na wbudowanie mechanizmów obsługi sieci w sam system. Biorąc pod uwagę to, do jakich zadań komputer ma być wykorzystywany, możliwe są do instalacji trzy protokoły sieciowe:

- NetBEUI – protokół używany w aplikacjach Microsoftu, który jednak nie zdobył większego uznania, choć może być z powodzeniem wykorzystywany do dzielenia plików i drukarek w małych sieciach MS Networking;
- IPX/SPX – wykorzystywany do łączenia z serwerami pracującymi w oparciu o system Novell Netware;
- TCP/IP – wykorzystywany w systemie Novell Netware 5 oraz przede wszystkim przy łączeniu sieci rozległych, czyli w Internecie.

Ponieważ obecnie sieci lokalne są wykorzystywane najczęściej do pracy w sieciowych systemach operacyjnych (Novell, Linux, Windows NT) oraz do dostępu do Internetu, praktycznie stosuje się tylko dwa ostatnie protokoły sieciowe.

Nic nie stoi na przeszkodzie, aby instalować wszystkie protokoły, ale przyczynia się to zazwyczaj do spadku wydajności sieci. Dlatego też instaluje się jeden, lub tam gdzie jest to konieczne, co najwyżej dwa (na przykład

IPX/SPX do łączenia się z serwerem Netware oraz TCP/IP do łączenia się z Internetem). Jeśli sieć lokalna wykorzystywana jest tylko do dostępu do Internetu, wtedy konieczne jest zainstalowanie tylko tego ostatniego.

Sieć TCP/IP na Windows 95/98

Instalacja karty sieciowej i protokołów

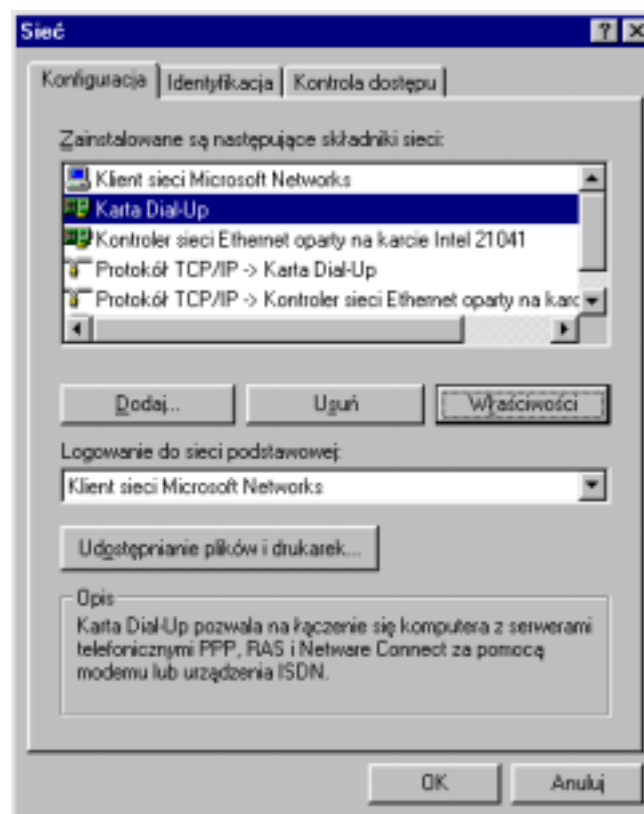
Przed rozpoczęciem instalacji należy zaopatrzyć się w drivery do karty sieciowej oraz płytę z systemem Windows w wersji adekwatnej do używanej.

Po włożeniu karty sieciowej do komputera powinna ona zostać automatycznie wykryta przez system (jeśli jest to karta Plug&Play) i rozpocząć się powinna procedura jej instalacji przy czym należy postępować zgodnie z informacjami pojawiającymi się na ekranie. Jeżeli karta nie zostanie automatycznie wykryta, należy skorzystać z opcji „Dodaj nowy sprzęt” w Panelu Sterowania.

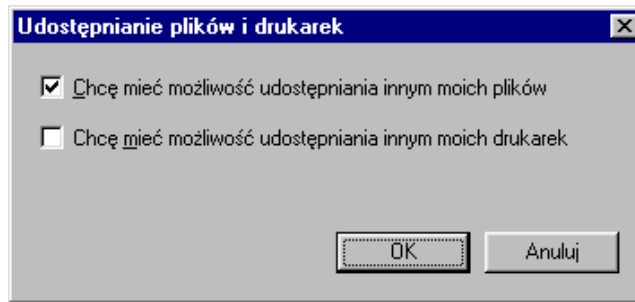
Po zainstalowaniu karty sieciowej należy upewnić się, czy karta została zainstalowana poprawnie. W tym celu należy otworzyć Panel Sterowania i kliknąć dwukrotnie na ikonie System. Następnie należy kliknąć zakładkę „Menedżer urządzeń” i rozwinąć gałąź „Karty sieciowe” a następnie wyświetlić właściwości zainstalowanej karty i sprawdzić, czy „Urządzenie działa poprawnie” oraz czy nie występują konflikty sprzętowe.

Następnie należy otworzyć z Panelu Sterowania ikonę „Sieć”. Pusuwać ewentualnie istniejące protokoły NetBEUI i IPS/SPX, a następnie zainstalować protokół TCP/IP (jeśli go nie ma). Klikamy Dodaj --> Protokół --> Microsoft --> TCP/IP i klikamy OK.

Po wszystkim okienko powinno wyglądać w podobny sposób:



Jeżeli komputer w sieci MS Networking (czyli dla innych komputerów z Windows 95/98) ma udostępniać swoje pliki bądź podłączone lokalnie drukarki, należy kliknąć przycisk „Udostępnianie plików i drukarek” i wybrać odpowiednie opcje:

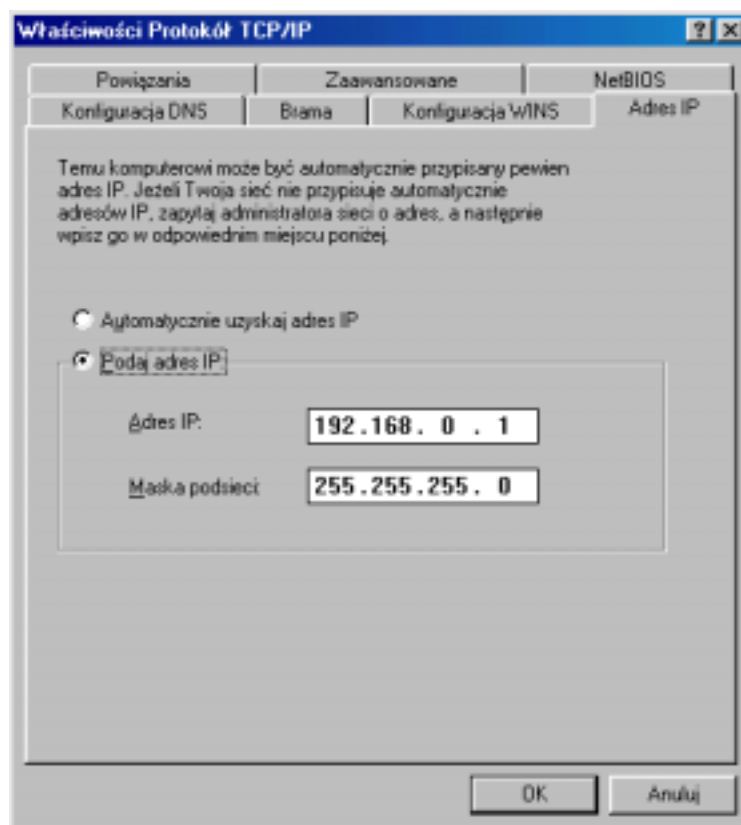


Konfiguracja TCP/IP

Następnie wyświetlamy właściwości protokołu TCP/IP i ustawiamy:

Adres IP – jeżeli ma być przydzielony adres statyczny, to klikamy „Podaj adres IP” i wpisujemy adres oraz maskę podsieci. Dla małych sieci zalecane jest używanie puli adresów 192.168.0.1-192.168.0.254 oraz maski 255.255.255.0.

Jeżeli adres IP będzie przydzielany automatycznie z serwera DHCP to pozostawiamy „Automatycznie uzyskaj adres IP”.



Na wszystkich komputerach powinna być taka sama maska podsieci, zaś adres IP musi być wszędzie inny, ale z zadanej puli adresowej. Ponadto przy zmianie właściwości protokołu TCP/IP należy pamiętać aby zmienić właściwości tylko tej pozycji, która przypisana jest do karty sieciowej (w przypadku, gdy zainstalowana jest więcej niż jedna karta sieciowa lub jeszcze karta Dial-Up).

Po instalacji i konfiguracji TCP/IP możemy zainstalować usługi takie jak www, ftp, poczta i korzystać z nich podobnie jak w Internecie lub udostępnić połączenie internetowe do sieci lokalnej.

Udostępnianie połączenia internetowego w sieci lokalnej

Do udostępniania połączenia internetowego w sieci lokalnej można wykorzystać komputer podpięty do sieci lokalnej z jednej strony, oraz posiadający kartę Dial-Up (czyli modem) lub drugą kartę sieciową połączoną z Internetem. Aby Internet był widziany z sieci lokalnej należy zastosować oprogramowanie wykorzystujące technologię NAT lub tzw. proxy serwer.

Do bardziej znanych proxy serwerów pod Windows 95/98 należą: WinGate, WinProxy, NetProxy, CProxy. Technologię NAT wykorzystuje zaś m.in. program SyGate i WinRoute (który dodatkowo wbudowane ma pewnego typu proxy i filtr pakietów).

Można również wykorzystać mechanizm dzielenia połączenia modemowego wbudowany w drugą edycję systemu MS Windows 98 (tzw. SE – Second Edition).

Konfiguracja SyGate'a

Po zainstalowaniu programu SyGate (jego konfiguracja jest w zasadzie prosta i ogranicza się do wyboru odpowiednich opcji podczas instalacji) na komputerze pełniącym funkcję bramy do Internetu (załóżmy, że ma on adres IP 192.168.0.1) należy ustawić adres bramy oraz adres serwera DNS na wszystkich innych komputerach na komputer pełniący funkcję bramy. W tym celu na wszystkich innych komputerach wybieramy właściwości TCP/IP, klikamy zakładkę „Brama”, a następnie w okienku „Nowa brama” wpisujemy adres IP bramy (w naszym przypadku 192.168.0.1) i klikamy przycisk Dodaj. Następnie klikamy na zakładkę „Konfiguracja DNS”, wybieramy „Włącz DNS”, wpisujemy jakąś nazwę (nie jest ważne jaką, ale komputer wymaga, aby coś było wpisane) w pole „Host”, wpisujemy adres bramy w pole „Kolejność przeszukiwania serwerów DNS” (w naszym przypadku 192.168.0.1), klikamy Dodaj, a następnie OK:



Źródła

Pozycje wydawnicze

- „Vademecum Teleinformatyka” - IDG Poland S.A., Wydanie I, Warszawa 1999 r. – przewodnik po telekomunikacji, sieciach komputerowych i zagadnieniach instalatorstwa sieciowego.
- „Internet, od podstaw do mistrzostwa” – Komputerowa Oficyna Wydawnicza HELP, Wydanie II, Warszawa 1996 r. – pozycja pod względem zawartości już dosyć stara, przeznaczona dla początkujących. Nie mniej można znaleźć w niej dosyć wiele informacji na temat „działania” Internetu i większości jego usług.

Miejsca w Internecie

- http://gadula.nfosigw.gov.pl/network_FAQ/network_FAQ.html – FAQ grupy *pl.comp.networking*.
- <http://lanzone.koti.com.pl> – „Wszystko o sieciach lokalnych” jak głosi slogan na stronie powitalnej. Można tu znaleźć wciąż uaktualniane opisy technologii sieciowych, wiele programów użytkowych i narzędzi sieciowych.
- <http://www.trzepak.pl> – strona prowadzona przez ludzi zajmujących się sieciami komputerowymi (na małą i większą skalę). Można znaleźć tu m.in. listę osiedlowych sieci komputerowych.
- <http://www.kki.net.pl/~alchemialan/> – można tu znaleźć informacje o standardach i konfiguracji sieci komputerowych, konfiguracji serwerów unixowych.
- <http://www.jtz.org.pl> – zbiór dokumentów HOW-TO Linuxa tłumaczony na język polski. Ciekawa lektura nie tylko dla Linuxowców.
- http://www.immt.pwr.wroc.pl/export_hp/tool/ – „Narzędzia sieciowe” – bardzo dobry elektroniczny podręcznik na temat sieci.
- <http://www.reporter.pl/encyklopedia> – „Encyklopedia Internetu” – zbiór wielu terminów i pojęć związanych z Internetem.
- <http://leksykon.koti.com.pl> – onlinowa wersja książki opublikowanej przez wydawnictwo Mikom. Prezentuje ponad 1000 haseł opatrzonych ilustracjami oraz odnośnikami do miejsc w Sieci.
- <http://free.polbox.pl/c/cyfraa/> – inna strona poświęcona sieciami lokalnym.
- <http://www.ots.utexas.edu/ethernet/> – strona zawierająca opisy technologii ethernetowych 10 Mb/s, 100 Mb/s, 1000 Mb/s, 10 Gbit/s.