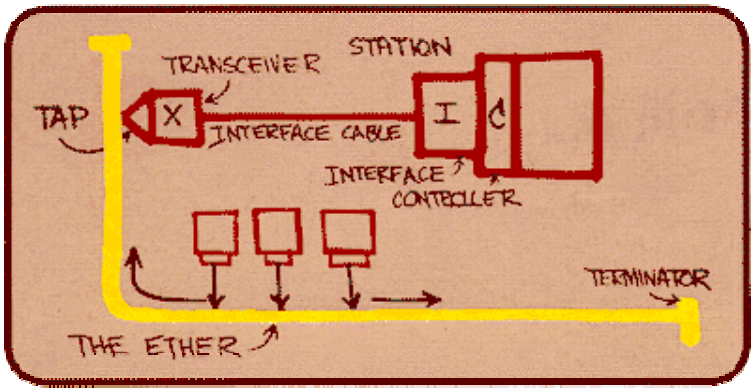


Jeden z pierwszych rysunków przedstawiających ideę działania sieci Ethernet wykonany w 1976 roku przez dr Roberta M. Metcalfe'a.

Sieci lokalne

Trochę teorii, nieco praktyki

Wydanie drugie poprawione i uzupełnione - 2001-02-27

Jest to już drugie oficjalne wydanie tego opracowania. Dołożyłem wszelkich starań, aby było ono lepsze od poprzedniego oraz jak najbardziej kompetentne. Mam nadzieję, że będzie służyć pomocą osobom początkującym oraz mniej doświadczonym administratorom własnych sieci lokalnych.
Niestety, ponieważ informacji, które chciałem w tym dokumencie zawrzeć, ciągle przybywa, więc mam coraz większe problemy z ich usystematyzowaniem. Moim celem było stworzenie kompendium zawierającego jak najwięcej wiedzy zebranej w jednym miejscu tak, aby każdy mógł znaleźć odpowiedzi na nurtujące go pytania. Zawarte tu treści mogą więc sprawiać wrażenie „grochu z kapustą" za co z góry przepraszam.

Chcę również 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 te należą się (kolejność alfabetyczna):
Ziemkowi Borowskiemu <ziembor@FAQ-bot.ZiemBor.waw.pl>,
Ryszardowi Kulickiemu <ryszardk@unix.sim.com.pl>,
Romanowi Niewiarowskiemu <newrom@rp.zax.pl>,
Przemysławowi Sarnowskiemu <sarp@nfosigw.gov.pl>
i Rafałowi Woźniakowi <kanar@infinity.net.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.ms-windows.win9x* 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 cały czas otwarty na wszelkie uwagi na temat niniejszego opracowania oraz pomysły, które przyczynią się do poszerzenia zawartości merytorycznej tej pracy.

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

Wprowadzenie teoretyczne

Sieć lokalna

Z definicji sieć lokalna (LAN – *Local Area Network*) jest siecią przeznaczoną do łączenia ze sobą stanowisk komputerowych znajdujących się na małym obszarze (podział ten uwzględnia jeszcze sieci metropolitarne – MAN – *Metropolitan Area Network*, oraz sieci rozległe – WAN – *Wide Area Network*).
Umożliwia ona wymianę plików oraz komunikatów pomiędzy użytkownikami, współużytkowanie zasobów udostępnionych w sieci np. plików i drukarek, a także korzystanie z innych usług.
Obecne sieci lokalne oparte są na technologii Ethernet (stąd synonim sieci ethernetowych), Token Ring lub FDDI. Jednakże ta pierwsza jest obecnie najczęściej stosowana. Stąd też jedynie jej poświęcimy więcej uwagi.

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. Stosowana 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 oplotu 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 oplotem.

Kategorie skrętek 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 5e – (*enchanced*) – ulepszona wersja kabla kategorii 5. Jest zalecana do stosowana w przypadku nowych instalacji;
- kategoria 6 – skrętka umożliwiająca transmisję z częstotliwością do 200 MHz. Kategoria ta obecnie nie jest jeszcze zatwierdzona jako standard, ale prace w tym kierunku trwają;
- 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. Obecnie nie istnieje.

Warto wspomnieć również, że skrętki wykonywane są w znormalizowanych średnicach, które podawane są w jednostkach AWG oraz mogą zawierać różną liczbę par. Powszechnie w sieciach komputerowych stosuje się skrętki czteroparowe.

Warto też zwrócić uwagę, że ponieważ kategoria 6 nie jest jeszcze potwierdzona normami międzynarodowymi, oraz mając na uwadze zalety, a także ciągle spadający koszt łączy światłowodowych może się okazać, że w niedalekiej przyszłości struktury budowane w oparciu o medium światłowodowe będą tańsze niż te, budowane w oparciu o drogi kabel miedziany kategorii 6.

Kabel współosiowy (koncentryczny)

Składa się z dwóch przewodów koncentrycznie umieszczonych jeden wewnątrz drugiego, co zapewnia większą odporność na zakłócenia a tym samym wyższą jakość transmisji. Jeden z nich wykonany jest w postaci drutu lub linki miedzianej i umieszczony w osi kabla (czasami zwany jest przewodem gorącym), zaś drugi (ekran) stanowi oplot.
Powszechnie stosuje się dwa rodzaje kabli koncentrycznych – o impedancji falowej 50 i 75 Ohm, przy czym te pierwsze stosuje się m.in. w sieciach komputerowych.
Zastosowanie znalazły dwa rodzaje kabli koncentrycznych:
- Cienki Ethernet (*Thin Ethernet*) – (sieć typu 10Base-2) – kabel RG-58 o średnicy ¼" i dopuszczalnej długości segmentu sieci wynoszącej 185 m. Stosowany nadal zwłaszcza tam, gdzie istnieje potrzeba połączenia na odległość większą niż 100 m.
- Gruby Ethernet (*Thick Ethernet*) – (sieć typu 10Base-5) – kable RG-8 i RG-11 o średnicy ½" i dopuszczalnej długości segmentu wynoszącej 500 m. Nie stosowany obecnie, lecz można go spotkać jeszcze w bardzo starych sieciach.

Oba kable mają impedancję falową 50 Ohm. Należy dodać, że impedancja kabla jest ściśle związana z impedancją urządzeń do niego podłączonych. Nie można więc bezkarnie stosować w sieciach komputerowych np. telewizyjnego kabla antenowego (o impedancji falowej 75 Ohm), gdyż wykonana w ten sposób sieć najprawdopodobniej nie będzie po prostu działać.

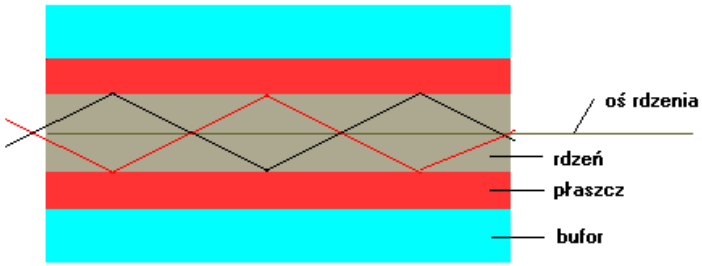
Zalety:
- jest mało wrażliwy na zakłócenia i szumy;
- nadaje się do sieci z przesyłaniem modulowanym (szerokopasmowym)
- jest tańszy niż ekranowany kabel skręcany

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.
Wykorzystywany jest również czasem do łączenia ze sobą skupisk stacji roboczych okablowanych w technologii gwiazdy zwłaszcza tam, gdzie odległość koncentratorów od siebie przekracza 100 m i nie jest wymagane stosowanie prędkości wyższych niż 10 Mb/s.
Rozwiązanie to jest jednak spotykane prawie wyłącznie w sieciach amatorskich. W sieciach profesjonalnych zaś (gdzie liczy się szybkość i niezawodność, a koszt instalacji jest sprawą drugorzędną) praktycznie nie stosuje się już kabla koncentrycznego, a zamiast niego wykorzystuje się światłowody.

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.
Kabel światłowodowy składa się z jednego do kilkudziesięciu włókien światłowodowych.

Medium transmisyjne światłowodu stanowi szklane włókno wykonane najczęściej z domieszkowanego dwutlenku krzemu (o przekroju kołowym) otoczone płaszczem wykonanym z czystego szkła (SiO_2), który pokryty jest osłoną (buforem). Dla promieni świetlnych o częstotliwości w zakresie bliskim podczerwieni współczynnik załamania światła w płaszczu jest mniejszy niż w rdzeniu, co powoduje całkowite wewnętrzne odbicie promienia i prowadzenie go wzdłuż osi włókna.
Zewnętrzną warstwę światłowodu stanowi tzw. bufor wykonany zazwyczaj z akrylonu poprawiający elastyczność światłowodu i zabezpieczający go przed uszkodzeniami. Jest on tylko osłoną i nie ma wpływu na właściwości transmisyjne światłowodu.



Wyróżnia się światłowody jedno- oraz wielomodowe. Światłowody jednomodowe oferują większe pasmo przenoszenia oraz transmisję na większe odległości niż światłowody wielomodowe. Niestety koszt światłowodu jednomodowego jest wyższy.
Zazwyczaj przy transmisji typu *full-duplex* stosuje się dwa włókna światłowodowe do oddzielnej transmisji w każdą stroną, choć spotykane są rozwiązania umożliwiające taką transmisję przy wykorzystaniu tylko jednego włókna.

Zalety:

- większa przepustowość w porównaniu z kablem miedzianym, a więc możliwość sprostania przyszłym wymaganiom co do wydajności transmisji
- małe straty, a więc zdolność przesyłania informacji na znaczne odległości
- niewrażliwość na zakłócenia i przesłuchy elektromagnetyczne
- wyeliminowanie przesłuchów międzykablowych
- mała masa i wymiary
- duża niezawodność poprawnie zainstalowanego łącza i względnie niski koszt, który ciągle spada

Więcej informacji na temat światłowodów można znaleźć pod adresem http://wtm.ite.pwr.wroc.pl/~spatela/dydak/wprowadzenie/, zaś odpowiedzi na najczęściej zadawane na ich temat pytania pod adresem http://wtm.ite.pwr.wroc.pl/~spatela/fo_faq/fiboptfaq_pl.html.

Oznaczenia standardów sieci

Standard sieci Ethernet został zdefiniowany przez IEEE (*Institute of Electrical and Electronic Engineers*) w normie o oznaczeniu 802.3. Oryginalna norma 802.3 definiuje standard sieci oznaczony jako 10Base-5. Kolejne odmiany tej technologii oznaczane są dodatkowymi przyrostkami literowymi. Są to między innymi: 802.3a (10Base-2), 802.3i (10Base-T), 802.3j (10Base-F), 802.3u (100Base-T4, 100Base-TX, 100Base-FX), 802.3z (1000Base-F), 802.3ab (1000Base-T), 802.3ae (10000Base-F).
Spis wszystkich norm z rodziny 802.3 można znaleźć na witrynie internetowej IEEE pod adresem http://standards.ieee.org.
Ogólny schemat oznaczania przepływności oraz rodzaju medium stosowanego w sieciach Ethernet składa się z następujących części:

- przepustowości wyrażonej w Mb/s – 10, 100, 1000
- rodzaj transmisji
  - Base – transmisja w paśmie podstawowym (*Baseband Network*)
  - Broad – transmisja przy wykorzystaniu częstotliwości nośnej (*Broadband Network*)
- rodzaj zastosowanego medium
  - 2 – cienki kabel koncentryczny (*Thin Ethernet*)
  - 5 – gruby kabel koncentryczny (*Thick Ethernet*)
  - T – skrętka (*Twisted Pair*)
  - F – światłowód (*Fiber Optic*)
- dodatkowe oznaczenie
  - X – transmisja po jednej parze w każdą stronę (dla 100Base-T i 100Base-F)

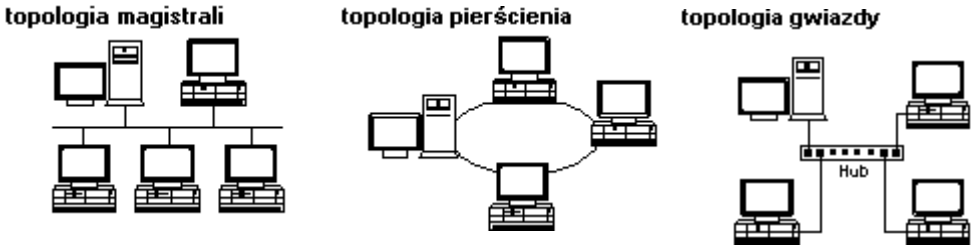
- 4 – transmisja przy wykorzystaniu 4 par na raz oraz kabla miedzianego kat. 3, 4 lub 5 (dla 100Base-T)
- L – zwiększona długość segmentu do 2000 m (dla 10Base-F)

Nie są to oczywiście wszystkie możliwe oznaczenia, a jedynie te najczęściej stosowane.

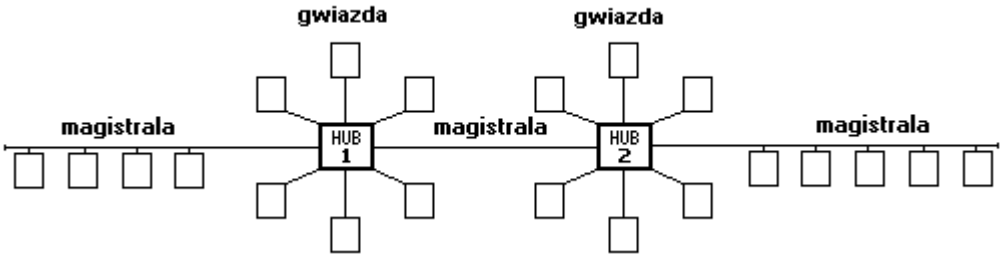
Topologie sieci LAN

Topologia LAN określa sposób wzajemnego połączenia stacji w sieci. Rozróżnia się topologie fizyczne i logiczne. Tpoplogia fizyczna określa sposób fizycznego połączenia stacji i urządzeń sieciowych. Topologia logiczna zaś sposób ich komunikacji między sobą.
Wyróżnia się następujące najczęściej stosowane fizyczne topologie LAN:

- magistrali (*bus*) – wszystkie stacje robocze w sieci dołączone są do jednej wspólnej szyny,
- pierścienia (*ring*) – stacje sieciowe podłączone są do okablowania tworzącego pierścień. Topologię pierścienia stosuje się w technologiach Token Ring/IEEE 802.5 i FDDI,
- gwiazdy (*star*) – kable sieciowe połączone są w jednym wspólnym punkcie, w którym znajduje się koncentrator lub przełącznik,
- drzewiasta (*tree*) – (hierarchiczna gwiazda) – jest strukturą podobną do topologii gwiazdy z tą różnicą, że są tu możliwe gałęzie z wieloma węzłami,
- mieszana – stanowi połączenie sieci o różnych topologiach.



Obecnie stosuje się w lokalnych sieciach komputerowych powszechnie praktycznie tylko topologię gwiazdy (oraz jej rozszerzenie – topologię drzewiastą) i topologię magistrali.
Można również często spotkać topologię mieszaną będącą połączeniem dwóch topologii fizycznych – magistrali i gwiazdy. Polega to na tym, że skupiska stacji roboczych łączone są w gwiazdę, zaś one same dołączane są do wspólnej magistrali, do której mogą być również dołączone pojedyncze stacje robocze:



Sieci LAN typu magistrala (Ethernet 10Base-2)

Zbudowane są z wykorzystaniem kabla koncentrycznego o impedancji 50 Ohm – RG-58 (tzw. cienki koncentryk). Długość jednego segmentu sieci (czyli od jednego końca do drugiego) nie powinna dla cienkiego koncentryka przekraczać 185 m (w pewnych warunkach – zastosowanie dobrych kart sieciowych, dobrej jakości kabla oraz małym poziomie zakłóceń zewnętrznych – możliwe jest osiągnięcie połączenia nawet na odległość do 300 m, lecz nie jest to zalecane, a tym bardziej objęte normami). 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).
Prędkość połączenia jest ograniczona do 10 Mb/s zaś minimalna długość segmentu wynosi 0,5 m.
Jeden segment nie powinien zawierać więcej, niż 30 komputerów ze względu na duży spadek wydajności sieci przy dalszym ich zwiększaniu.
Możliwe jest osiągnięcie rozpiętości sieci do 925 m poprzez połączenie szeregowe 5 segmentów przy wykorzystaniu repeater'ów, przy czym wypełnione komputerami może być co najwyżej 3 z nich (zasada 5-4-3).

Zalety:

- stosunkowo niski koszt instalacji w porównaniu z siecią zbudowaną w oparciu o skrętkę

Wady:

- trudności w lokalizowaniu usterki zwłaszcza przy większej liczbie komputerów
- podłączenie nowego stanowiska wymaga rozpięcia kabla
- awaria lub rozpięcie kabla skutkuje unieruchomieniem całego segmentu sieci
- niezawodność jest niższa, niż sieci opartych na skrętce
- prędkość przesyłu danych ograniczona do 10 Mb/s

Sieci 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 powinna przekraczać 100 m. Praktyka dowodzi jednak, że sieć 10Base-T działa w sprzyjających warunkach do około 150 metrów zaś 100Base-TX do około 120 metrów (przy zastosowaniu dobrej jakości kart sieciowych i dobrego kabla, jego ekranowania oraz niskich zakłóceniach zewnętrznych). Należy jednak pamiętać, że w obu przypadkach przekroczona jest norma długości i nie należy robić takich rzeczy w zastosowaniach profesjonalnych.

Zalety:

- łatwa instalacja (standardowo instalowane 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

Sieć 100Base-TX jest (podobnie, jak 10Base-T) oparta o transmisję przy wykorzystaniu dwóch par skrętki. Pozostałe dwie nie są wykorzystywane aczkolwiek nie zaleca się ich stosowania do innych celów (np. podłączenia jeszcze jednego komputera) ze względu na możliwość powstania zakłóceń pomiędzy liniami.
Można tu jeszcze wspomnieć o sieci 100Base-T4, która nie jest obecnie stosowana. Technologia ta była wykorzystywania do osiągnięcia prędkości transmisji 100 Mb/s przy wykorzystaniu wszystkich czterech par skrętki kategorii 3.

Warto wspomnieć, że w 1999 roku został ostatecznie zdefiniowany przez normę IEEE 802.3ab standard 1000Base-T. Umożliwia on transmisję z szybkością 1000 Mb/s przez skrętkę kategorii 5 na odległość do 100 m.

Pozostałe 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. Może łączyć segmenty sieci o różnych mediach transmisyjnych.
- koncentrator (*hub*) – jest czasami określany jako wieloportowy regenerator. Służy do tworzenia fizycznej gwiazdy przy istnieniu logicznej struktury szyny lub pierścienia. Pracuje w warstwie 1 (fizycznej) modelu OSI. 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 wydatne zmniejszenie ruchu w sieci. W przeciwieństwie do koncentratorów, przełączniki działają w trybie *full-duplex* (jednoczesna transmisja w obu kierunkach).
Przełączniki działają w oparciu o jeden z dwóch trybów pracy: *cut through* (przełączanie bezzwłoczne) oraz *store&forward* (zapamiętaj i wyślij). Pierwsza technologia jest wydajniejsza ponieważ pakiet jest natychmiast kierowany do portu przeznaczenia (na podstawie MAC adresu) bez oczekiwania na koniec ramki, lecz pakiety przesyłane w taki sposób nie są sprawdzane pod względem poprawności. Druga technologia pracy charakteryzuje się tym, że przełącznik odczytuje najpierw całą ramkę, sprawdza, czy została odczytana bez błędów i dopiero potem kieruje ją do portu docelowego. Przełącznik taki pracuje wolniej, ale za to prawie niezawodnie.

- przełącznik VLAN – jest odmianą przełącznika umożliwiającą tworzenie wirtualnych sieci LAN, których stanowiska są zlokalizowane w różnych punktach (sieciach, podsieciach, segmentach), zaś w sieć wirtualną łączy je jedynie pewien klucz logiczny. Sieć taka pozwala optymalizować natężenie ruchu pakietów w poszczególnych częściach sieci. Możliwa jest również łatwa zmiana konfiguracji oraz struktury logicznej takiej sieci.
- most (*bridge*) – służy do przesyłania i ew. filtrowania ramek między dwoma sieciami przy czym sieci te niekoniecznie muszą być zbudowane w oparciu o takie samo medium transmisyjne. Śledzi on 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 sprzętowe 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 stosowane 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.
- transceiver – urządzenie nadawczo-odbiorcze łączące port AUI (*Attachment Unit Interface*) urządzenia sieciowego z wykorzystywanym do transmisji typem okablowania. Poza wysyłaniem i odbieraniem danych realizuje on funkcje wykrywania kolizji (przy jednoczesnym pojawieniu się pakietów danych), nie dopuszcza do przesyłania zbyt długich (>20 ms) pakietów danych (*Jabber function*) oraz wykrywa przerwy w linii światłowodowej.

Zapora sieciowa (firewall)

Kiedy sieć lokalna podłączona jest do Internetu, odbywa się to poprzez router, samodzielny komputer filtrujący pakiety lub wykorzystujący oprogramowanie proxy albo inne, gotowe urządzenie przeznaczone do tego celu (tzw. *„firewall in a box”*). Kluczowym problemem jest zapewnienie bezpieczeństwa sieci lokalnej przed dostępem z zewnątrz. Funkcję taką pełni właśnie firewall. Pozwala ograniczyć lub zablokować całkowicie dostęp z zewnątrz pozostawiając możliwość ruchu w kierunku odwrotnym.
Zapora wyposażona może być w następujące rodzaje filtrów:

- bramki aplikacji/zapory proxy – działające tak, że pakiety nie są przekazywane pomiędzy siecią wewnętrzną i zewnętrzną, ale następuje swego rodzaju tłumaczenie dokonywane przez bramkę. Dzięki temu można uzyskać większą kontrolę nad poszczególnymi usługami. Wadą takiego rozwiązania jest konieczność dużego zaangażowania administratora systemu, który musi skonfigurować aplikację proxy dla każdej usługi sieciowej na każdym komputerze kliencie osobno. Użytkownicy wewnętrzni muszą więc korzystać z oprogramowania obsługującego proxy, które w dodatku będzie odpowiednio skonfigurowane.
- filtry pakietów – są to zapory na poziomie sieci dzięki którym możemy udzielać lub blokować dostęp na podstawie adresu pochodzenia, adresu docelowego pakietu, protokołu, numeru portu, czy nawet zawartości. Rozwiązanie to ma poważną zaletę w stosunku do zapory proxy. Nie trzeba bowiem stosować różnych zabiegów konfiguracyjnych dla każdej stacji roboczej w sieci gdyż filtr pakietów jest niezależny od systemu i aplikacji klienckich.

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.
Adres MAC służy do jednoznacznej identyfikacji konkretnej karty sieciowej w sieci lokalnej i może być wykorzystany np. do ograniczenia dostępu konkretnych maszyn z tejże sieci do Internetu udostępnianego za pomocą maskarady pracującej pod systemem uniksowym.
Pod adresem http://standards.ieee.org/regauth/oui/oui.txt można znaleźć spis wszystkich MAC-adresów przyporządkowanych poszczególnym producentom.

Metody dostępu do medium transmisyjnego

Ponieważ dowolna stacja w sieci lokalnej może rozpocząć transmisję w sieci tylko wtedy, gdy medium transmisyjne nie jest zajęte (czyli, gdy nie nadaje w tym samym momencie żadna inna stacja), więc potrzebna jest metoda umożliwiająca współpracę wielu komputerów w sieci lokalnej. Protokoły LAN używają jednej z następujących metod dostępu do medium:

- CSMA/CD (*Carrier Sense Multiple Access with Collision Detection* – wielodostęp z rozpoznawaniem stanu kanału oraz wykrywaniem kolizji) – stacje chcące nadawać konkurują między sobą o dostęp do medium. Stacja może zacząć nadawanie jeśli stwierdzi, że medium transmisyjne nie jest w danym momencie zajęte. Jeżeli jednak zdarzy się tak, że po stwierdzeniu braku zajętości medium dwie stacje zaczną nadawać jednocześnie (czyli nastąpi kolizja), sytuacja taka jest wykrywana, zaś transmisja jest ponawiana po losowym odstępie czasu. Metoda ta wykorzystywana jest w sieciach Ethernet.
- Token Passing – (przekazywanie znacznika) – stacje sieciowe uzyskują dostęp do medium w zależności od tego, gdzie w aktualnej chwili znajduje się tzw. token (przekazywana pomiędzy komputerami specjalna ramka sterująca). Tą metodę dostępu stosuje się w sieciach Token Ring i FDDI.

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 medium transmisyjnego. 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 – Łącza 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 przysłania poczty (SMTP), usługi nazewnicze 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”) zaprojektowane przez firmę IBM, wykorzystywany m.in. przez system operacyjny Microsoftu. Ponadto NetBIOS może być tunelowany dowolnym innym protokołem np. IPX lub TCP/IP
- zestaw protokołów TCP/IP („protokół kontroli transmisji”/„protokół internetowy”) używany powszechnie w Internecie oraz sieciach lokalnych mających do niego dostęp

TCP/IP i Internet

Szczegóły każdego protokołu TCP/IP są przedstawione w dokumentacji RFC (*Request for Comments*) – poddanie pod dyskusję.

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>
Można jednak niekiedy spotkać inny zapis będący dziesiętnym wyrażeniem 32 bitowej liczby binarnej. Na przykład adres 148.81.78.1 w notacji kropkowo dziesiętnej, będzie w postaci binarnej wyglądał następująco: 10010100010100010100111000000001 zaś dziesiętnie będzie to liczba 2488356353.

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 routing) - ponieważ powodowało to duże marnotrawstwo IP.

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 różnorakich problemów mających swe źródło w dublowaniu się adresów IP w sieci lokalnej oraz w Internecie.

Maska sieciowa (IPv4)

Jest to adres IP, który ma jedynki 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 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. 11111111111111111111111111100000 (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
6	11111111111111111111111111111000	255.255.255.248
14	11111111111111111111111111110000	255.255.255.240
30	11111111111111111111111111100000	255.255.255.224
62	11111111111111111111111111000000	255.255.255.192
126	11111111111111111111111110000000	255.255.255.128
254	11111111111111111111111100000000	255.255.255.0

Adres sieciowy (IPv4)

Adres sieciowy jest bitowym iloczynem maski sieciowej z którymkolwiek z adresów IP sieci. Jeśli 206.197.168.200 jest adresem IP systemu, a 255.255.0.0 jest maską, to 206.197.0.0 jest adresem sieciowym. Jeśli zaś 206.197.168.200 jest adresem IP (bitowo 11001110110001011010100011001000) zaś 255.255.192.0 jest maską (bitowo 11111111111111111100000000000000), to iloczyn bitowy daje 206.197.128.0 (bitowo 11001110110001011000000000000000).
Czasami można spotkać skrótowo zapisany adres sieciowy w postaci: 168.100.189.0/24 gdzie część stojąca przed znakiem „/” jest adresem IP zaś liczba 24 jest skrótowo zapisaną maską sieciową. Jest to liczba bitów ustawionych w masce sieciowej na 1, czyli przy standardowej 32 bitowej masce jest to 11111111111111111111111100000000 (255.255.255.0).

IPv4 i IPv6

Ciągły rozwój Internetu spowodował, że dotychczasowa wersja zestawu protokołów używanych w nim do transmisji, mimo swej olbrzymiej elastyczności, przestaje wystarczać. Jest to spowodowane głównie wyczerpującym się obszarem adresowym (ograniczenie 32 bitowego adresu), ale wpływają na to także i inne czynniki, jak nowe techniki komunikacyjne, nowe programy wymagające sposobów komunikacji, której dotychczasowe protokoły nie są w stanie zapewnić (np. efektywne przesyłanie obrazu i dźwięku).
Dotychczasowa wersja protokołów TCP/IP (oznaczona numerem 4) jest oznaczana potocznie IPv4 i pod takim oznaczeniem (bądź częściej po prostu IP) figuruje w opracowaniach. Nową wersję oznaczono numerem 6 (stąd oznaczenie IPv6) i dla odróżnienia od wersji poprzedniej nazwano IPng (Next Generation).
Głównymi zmianami, jakie zostały wprowadzone i które na pierwszy rzut oka są widoczne, to rozszerzenie przestrzeni adresowej z 32 do 128 bitów (z 4 do 16 oktetów) co daje liczbę adresów niewyobrażalną do wyczerpania w dającej się przewidzieć przyszłości.
Choć długie adresy rozwiązują problem niewystarczającej przestrzeni, to pojawia się inny, równie interesujący. Ludzie zajmujący się administracją sieciami muszą tymi adresami operować. Notacja kropkowo-dziesiętna używana w IPv4 nie nadaje się, gdyż adresy są za długie. Jako rozwiązanie zaproponowano używanie notacji szesnastkowej z dwukropkami co umożliwia dodatkowo także kompresję zer.
Adres kropkowo-dziesiętny dla IPv6 wyglądałby przykładowo tak: 104.230.140.100.255.255.255.255.0.0.17.128.150.10.255.255. Adres taki można przedstawić w formie krótszej stosując zapis szesnastkowy: 68E6:8C64:FFFF:FFFF:0:1180:96A:FFFF.
Poza tym, jak wspomniano wyżej, możliwa jest tzw. kompresja zer – ciąg powtarzających się zer jest zastępowany przez parę dwukropków. Adres FF05:0:0:0:0:0:0:B3 może zostać zapisany jako FF05::B3. Aby zapewnić, że kompresja zer nie powoduje niejednoznaczności w zapisie, może być ona zastosowana tylko raz.
Poza tym notacja szesnastkowa z dwukropkami pozwala na pisanie końcówek w notacji kropkowo-dziesiętnej co planuje się wykorzystać przy przejściu z IPv4 na IPv6. Następujący adres jest więc poprawny: 0:0:0:0:0:0:128.10.2.1. I tutaj możliwe jest oczywiście zastosowanie kompresji zer: ::128.10.2.1.

System nazw domen

Każdy hostowy komputer w sieci TCP/IP ma swój adres IP. Jednak, ponieważ trudno jest zapamiętać adresy IP nawet kilku hostów, więc powstały specjalne serwery tłumaczące adresy domenowe (postaci: it.pw.edu.pl) na adresy kropkowo-dziesiętne (148.81.78.1). Serwery te nazywane są serwerami DNS (Domain Name Server). Serwery dokonujące translacji w drugą stronę, to serwery Rev-DNS. System ten nosi nazwę systemu nazw domenowych (Domain Name System).
Nazwa domenowa tworzona jest od strony prawej do lewej. Na początku występują nazwy domen najwyższego poziomu (Top-Level Domains), następnie domeny niższych poziomów, a na końcu znajduje się nazwa hosta. Nazwy te są oddzielone od siebie kropkami.
Domeny najwyższego poziomu podzielone są na domeny geograficzne (Country Code Domains – dwuliterowe identyfikatory przyznane poszczególnym krajom np. .uk, .de, .jp, .us, itp.) oraz organizacyjne (Generic Domains – przyznawane w zależności od prowadzonej działalności np. .com, .org, .net, .edu, .gov, .mil, .int).
Więcej informacji oraz listę domen najwyższego poziomu można znaleźć pod adresem http://www.iana.org/domain-names.htm.

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://
  - news://
- 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 umożliwiająca 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, wspomnianymi wcześniej normami i zwane adresami prywatnymi lub czasem 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 (czyli praktycznie przy każdym uruchomieniu komputera). 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).

Najważniejsze usługi internetowe

- Finger – usługa umożliwiająca zdobywanie informacji o użytkowniku mającym konto na zdalnym serwerze. Ze względu jednak na to, że zdobyte w ten sposób dane mogą zostać wykorzystane przez hackerów, obecnie większość maszyn w Internecie ma wyłączoną tą usługę
- FTP (*File Transfer Protocol*) – protokół transmisji plików umożliwiający obustronną ich transmisję pomiędzy systemem lokalnym i zdalnym
- Gopher – po polsku „świstak”. Obecnie odchodzący w zapomnienie i zastępowany przez WWW, wykorzystywany do wyszukiwania i udostępniania informacji w Internecie dzięki stosowaniu hierarchii menu i plików
- HTTP (*Hypertext Transfer Protocol*) – protokół przesyłania hipertekstu odpowiedzialny za transmisję stron WWW
- IRC (*Internet Relay Chat*) – protokół służący do prowadzenia rozmów za pomocą terminala tekstowego
- NNTP (*Usenet News Transfer Protocol*) – protokół transmisji używany do wymiany wiadomości z serwerami grup dyskusyjnych
- POP (*Post Office Protocol*) – protokół pocztowy służący do odbioru poczty z serwera i transmisję jej do maszyny lokalnej
- SMTP (*Simple Mail Transfer Protocol*) – podstawowy protokół transmisji poczty stosowany do wysyłania poczty z maszyny lokalnej na serwer
- SNMP (*Simple Network Managament Protocol*) – protokół zarządzania siecią. Służy do zdalnej administracji urządzeniami sieciowymi, które udostępniają tą usługę
- SSH (*Secure Shell*) – bezpieczny protokół terminala sieciowego udostępniający funkcję szyfrowania przesyłanych danych. Jest zalecany do wykorzystania zamiast Telnetu.
- Telnet – protokół terminala sieciowego umożliwiający logowanie się oraz zdalną pracę na odległym komputerze przy wykorzystaniu terminala tekstowego. Cechą charakterystyczną jest transmisja otwartym tekstem, a więc możliwość łatwego podsłuchania tejże transmisji.

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 czasem, zwłaszcza w sieciach o dużej rozpiętości, topologie mieszane polegające na łączeniu małych skupisk stacji z zastosowaniem topologii gwiazdowej, zaś skupiska te dołącza się do jednej szyny typu *bus*. Lecz takie rozwiązanie (w oparciu o kabel koncentryczny) spotyka się praktycznie tylko w sieciach amatorskich. W profesjonalnych instalacjach zamiast kabla koncentrycznego stosuje się światłowody.
- 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.), w tym dokonanie wstępnych pomiarów dla określenia liczby metrów rynienek i kabla.
- 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 powinna przekraczać 185 m. Oczywiście nie jest powiedziane, że kabel o długości niewiele większej nie będzie działać, ale takie rozwiązanie wiąże się z przekroczeniem założeń odpowiedniej normy i powinno być stosowane z rozwagą
- końce każdego segmentu sieci 10Base-2 muszą być zakończone trójnikami z zapiętymi na nich terminatorami 50 Ohm
- dla sieci 10Base-2 oraz 10Base-T obowiązuje zasada 5-4-3 co oznacza, że w sygnał podróżujący w sieci może być transmitowany przez maksymalnie przez 5 segmentów i 4 repeatery (huby) przy czym tylko 3 segmenty wypełnione mogą być komputerami
- dla sieci 10Base-T można połączyć kaskadowo maksymalnie 4 koncentratory (przy pomocy łącza UpLink), zaś dla sieci 100Base-TX można połączyć kaskadowo tylko 2. Dla uściślenia oznacza to, że między dwoma dowolnymi komputerami podłączonymi do sieci nie powinno być więcej niż odpowiednio cztery lub dwa koncentratory. Przy większej planowanej ilości takich urządzeń należy już stosować w miejsce niektórych przełączniki tak, aby ilości te nie były przekroczone. Przekroczenie podanych wartości nie spowoduje oczywiście, że nic z zasady nie będzie działać, ale może spowodować znaczne zmniejszenie szybkości transmisji ze względu na wzrost liczby kolizji i należy raczej podchodzić do tego ostrożnie. Jednak warto zaznaczyć, że liczba podłączonych kaskadowo urządzeń może być większa o ile pozwala na to producent tych urządzeń
- teoretycznie rzecz biorąc w sieci lokalnej można podłączyć kaskadowo nieograniczoną liczbę switch'y, ale praktycznie nie warto przesadzać z ich liczbą
- długość kabla wraz z przyłączami w sieciach 10Base-T i 100Base-TX nie powinna przekraczać 100 m. W praktyce przyjmuje się, że długość kabla wynosi 90 m zaś 10 m rezerwuje się na patchcordy (szafa+podłączenie stacji roboczej do gniazdka). Tutaj również stosuje się uwagę jak w punkcie pierwszym

- długość miedzi pomiędzy połączonymi ze sobą koncentratorami 100 Mb nie powinna być większa niż 2 m
- 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.). Producent okablowania Mod-Tap zaleca odległości przynajmniej 30 cm od wysokonapięciowego oświetlenia (świetlówki), 90 cm od przewodów elektrycznych o przesyłanej mocy od 5 kVA w górę oraz 100 cm od transformatorów i silników
- kable powinny być prowadzone równolegle oraz prostopadle do korytarzy jak również powinny być wyprowadzane z głównych kanałów kablowych pod kątem 90 stopni gdyż ułatwia to konserwację sieci kablowej oraz umożliwia szybsze zlokalizowanie ich przebiegu w budynku
- jeśli istnieje konieczność krzyżowania się kabli sieciowych z instalacją elektryczną, to powinno być one wykonane pod kątem 90 stopni
- kable biegnące w otwartej przestrzeni (np. podwieszane) powinny być mocowane co 1,25-1,5 m co eliminuje dodatkowe niekorzystne obciążenia kabli ich własnym ciężarem.
- jeżeli instalacja sieciowa jest prowadzona jedną listwą kablową wraz z dedykowaną instalacją zasilającą, to powinny być one od siebie separowane przegrodami z PCV oraz suma prądów płynących w kablach zasilających nie powinna przekraczać 20A (wg zaleceń Mod-Tap)
- 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 przesuwać
- nie należy rozciągać kabli. Nie może być on naprężony na całym przebiegu ani na końcach
- dodatkowe połączenia w kablu typu lutowanie nie powinny mieć miejsca
- nie powinno się 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 zatwierdzonego jeszcze standardu kategorii 6. Prace nad jego wprowadzeniem są jednak prowadzone. Istnieje również, jak dotąd nieformalnie, ulepszona kategoria 5 oznaczana 5e, która zalecana jest do stosowania w nowych instalacjach.
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. Jeśli jednak planujemy zaciskać wtyczki RJ-45 na drucie, to należy zaopatrzyć się w ich odmianę przystosowaną do zaciskania na nim (różnią się one kształtem nożna przecinającego izolację żyły).
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 co jest niezbędne do skutecznego odprowadzania zakłóceń w nim indukowanych. Wiąże się to oczywiście z większymi kosztami takiej instalacji.

Zakończenia kabli

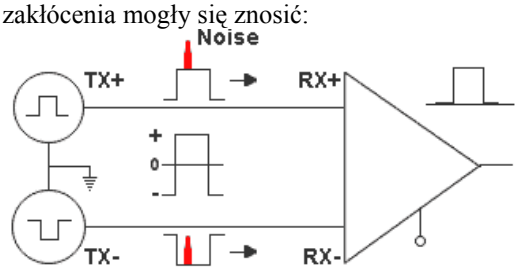
Kable skrętkowe w instalacji naściennej powinny być zakończone gniazdami standardu RJ-45 przy czym w punkcie przyłączeniowym powinna być zainstalowana puszka z tymże rodzajem gniazda, zaś od strony szafy dystrybucyjnej kable powinny być dołączone do patchpanela o odpowiedniej liczbie gniazd.
Do wciskania przewodów w gniazda powinna być wykorzystywana specjalna wciskarka (zwana czasami, z racji swojego działania, narzędziem uderzeniowym) np. Mod-Tap lub Krone. Przewody powinny być podłączone w gnieździe w odpowiedniej kolejności (o czym dalej). Gniazda oraz patchpanele oznaczone są kodami barwnymi odpowiadającymi kolorom przewodów w kablu.

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

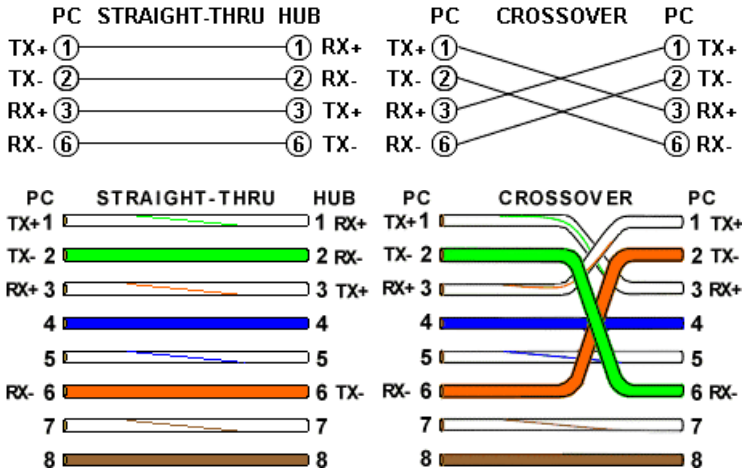
Każdy odcinek kabla koncentrycznego powinien być zakończony wtykiem BNC i dołączony do trójnika połączonego z urządzeniem sieciowym (komputerem lub koncentratorem). Na trójnikach umieszczonych na końcach segmentu powinny być założone terminatory 50 Ohm. Zalecane jest również, aby przewód masowy kabla był na jednym z końców każdego segmentu uziemiony.

Krosowanie przewodów

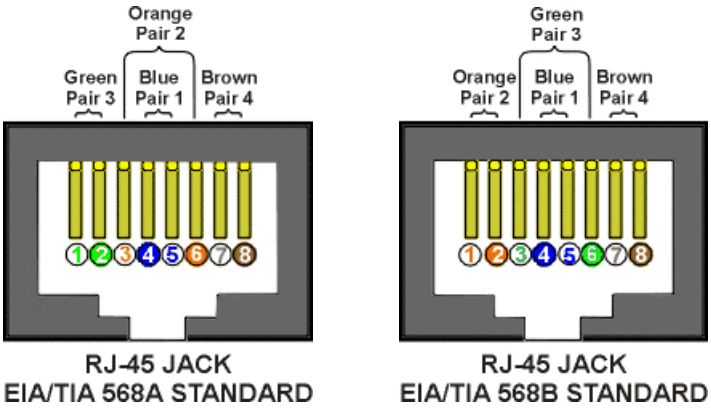
Do prawidłowego działania kabla skrętkowego konieczne jest, aby pary przewodów były we właściwy sposób podłączone tak, aby powstające zakłócenia mogły się znosić:



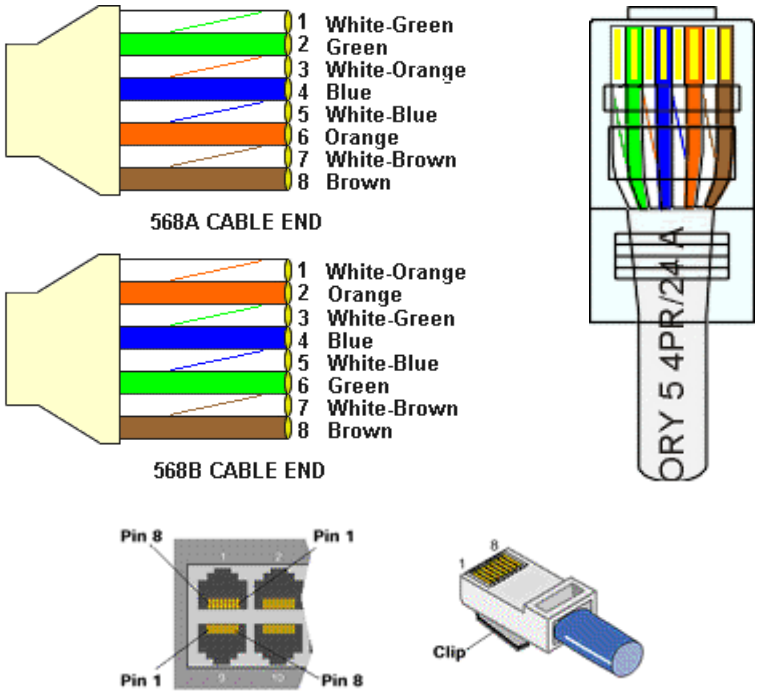
Kolejność podłączenia przewodów skrętki jest opisana dwoma normami EIA/TIA 568A oraz 568B.
Dla połączenia komputera z koncentratorem lub przełącznikiem stosuje się tzw. kabel prosty (straight-thru cable), który z obu stron podłączony jest tak samo wg standardu 568A lub 568B. Dla połączenia bezpośrednio 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 krzyżowego (cross-over cable) i charakteryzuje się tym, że jeden koniec podłączony jest wg standardu 568A zaś drugi 568B.
Odpowiednikim kabla krzyżowego 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 krzyżowym dwóch hubów, oba końce kabla muszą być dołączone do portów zwykłych lub do portów UpLink. Port UpLink został wprowadzony po to, aby w połączeniach pomiędzy hubami uniknąć konieczności stosowania innego kabla niż we wszystkich innych połączeniach. Ze względu na swą funkcję, port ten określany jest czasami terminem portu z wewnętrznym krzyżowaniem.
Zarówno kable, gniazda, jak i przełączniki realizujące funkcję krzyżowania powinny być dla odróżnienia oznaczone symbolem X.



Jeżeli połączenie wykonywane jest kablem prostym to zaleca się stosowanie sekwencji 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 tych standardach. Oczywiście dopuszczalne jest również stosowanie alternatywnej sekwencji 568B.



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

Pary oznaczane są następująco:

1. para niebieska
2. para pomarańczowa
3. para zielona
4. para brązowa

Przed włożeniem przewodów we wtyczkę, zewnętrzna izolacja kabla UTP powinna zostać ściągnięta na odcinku około 12 mm, a następnie przewody powinny zostać wsunięte do oporu 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.

Testowanie połączeń

Po podłączeniu wszystkich przewodów należy sprawdzić ciągłość połączeń. Do tego celu w najprostszym przypadku nadaje się multimetr z próbnikiem przejścia, lecz jest to uciążliwy proces wymagający uwagi i systematyki zwłaszcza, jeśli mamy do sprawdzenia więcej niż jedno połączenie.
Najlepiej nadaje się do tego tester przejścia do sieci (skrętkowych lub BNC, dzięki któremu można szybko się zorientować, czy kabel jest uszkodzony), lub urządzenie do wykonywania pomiarów sieci, które ponadto stwierdzi jakość okablowania.

Tester ciągłości połączeń

Jest to proste urządzenie (nieco nowocześniejsza oraz ulepszona wersja bateryjki i żarówki) pozwalające wykryć:

- brak przewodzenia którejś z par skrętki
- kolejność podłączenia par skrętki
- prawidłowość polaryzacji każdej pary
- fakt zwarcia w kablu

Tester do pomiarów sieci

Urządzenia do pomiarów sieci wykonują szereg testów (zazwyczaj automatycznie, po wciśnięciu jednego przycisku) i określają, czy dany parametr spełnia założenia danej normy (*pass*) lub nie (*fail*). Ocenie podlegają tu:

- Line Map – mapa połączeń;
- NEXT (Near End Crosstalk) – przesłuch pomiędzy parami;
- Return Loss – wartość sygnału odbitego będącego wynikiem niedopasowania impedancji elementów;
- Attenuation – tłumienie;
- Link Length – długość połączenia;

Niestety obecnie koszt testerów do wykonywania pomiarów w zależności od ich nowoczesności i uniwersalności sięga kilkuset do kilku tysięcy dolarów amerykańskich więc jest to inwestycja, na którą mogą sobie pozwolić jedynie duże firmy.

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.
Ponadto u wielu producentów (np. Krone, ZPAS) zaczęły pojawiać się rozwiązania szaf o szerokości 10 cali, które przeznaczone są dla małych instalacji sieciowych.

Konfiguracja sieci

W przypadku systemu Windows 95/98, bo taki system najczęściej jest na stacjach klienckich 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:

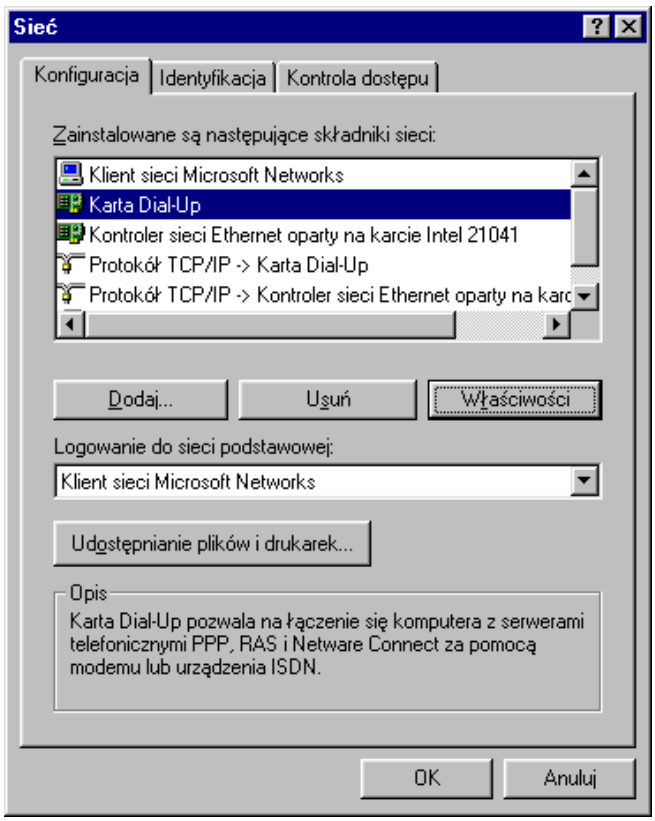
- NetBEUI – protokół używany w aplikacjach Microsoftu, który jednak nie zdobył większego uznania, choć może być z powodzeniem wykorzystywany do dzielenia plików i drukarek w małych sieciach MS Networking;
- IPX/SPX – wykorzystywany do łączenia z serwerami pracującymi w oparciu o system Novell Netware;
- 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.

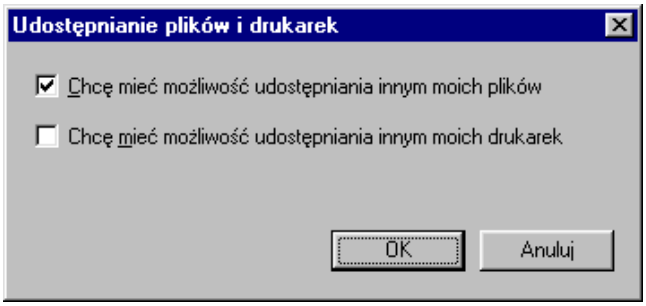
Sieć TCP/IP na Windows 95/98/Me

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 dalej wyświetlić właściwości zainstalowanej karty i sprawdzić, czy „Urządzenie działa poprawnie” oraz czy nie występują konflikty sprzętowe.
Następnie należy otworzyć z Panelu Sterowania ikonę „Sieć”. Pousuwać 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:

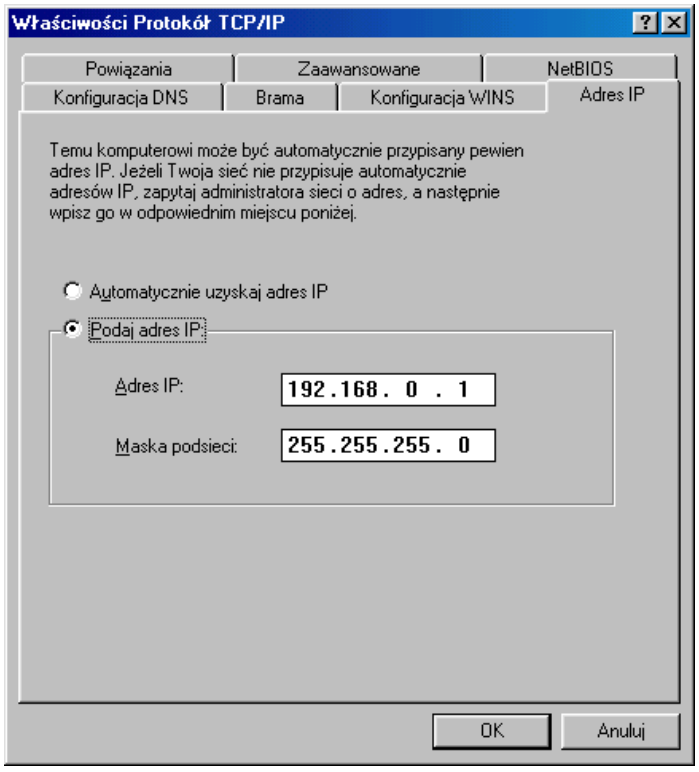


Jeżeli komputer w sieci MS Networking (czyli dla innych komputerów z Windows 95/98) ma udostępniać swoje pliki bądź podłączone lokalnie drukarki, należy kliknąć przycisk „Udostępnianie plików i drukarek” i wybrać odpowiednie opcje:



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. Oczywiście nic nie stoi na przeszkodzie, aby zastosować adresy IP np. z przedziału 10.1.1.1-10.1.1.254 lub inne z puli adresów prywatnych.
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.

Podłączenie sieci lokalnej do Internetu

Łącze z Internetem

Aby połączyć sieć lokalną z Internetem, w pierwszej kolejności wybrać należy rodzaj tego połączenia adekwatnie do potrzeb, możliwości technicznych oraz zasobów finansowych.

Modem analogowy

Analogowe łącze komutowane jest to najprostszy i na krótką metę obecnie chyba najtańszy sposób na połączenie z Internetem. Jego podstawową wadą jest mała szybkość transmisji, niska niezawodność oraz fakt zajęcia linii telefonicznej podczas połączenia modemowego. Opłata za połączenie jest zależna od czasu jego trwania i wynosi zazwyczaj tyle samo, ile lokalna rozmowa telefoniczna. Największą prędkością, jaką można przy wykorzystaniu tego rodzaju połączenia uzyskać, jest teoretycznie 56 kb/s, ale praktycznie prędkość transmisji rzadko przekracza 40 kb/s. Oczywiście, aby uzyskać połączenie z prędkością 56 kb/s potrzebny jest do tego modem, który taki transfer danych zapewnia. Aktualnie można spotkać modemy o prędkościach 14.4, 28.8, 33.6 i 56 kb/s przy czym ostatnie dwa są obecnie z powodzeniem stosowane.
Pomimo swych wad rozwiązanie takie może być z powodzeniem stosowane do połączenia z Internetem małych sieci (do 3 lub 4 komputerów) przy założeniu, że nie wszystkie komputery będą jednocześnie z połączenia tego korzystać (gdyż znacznie spadnie jego wydajność w przeliczeniu na jeden komputer).

Modem ISDN

ISDN (*Integrated System Digital Network*)jest łączem cyfrowym złożonym z dwóch kanałów o prędkości 64 kb/s każdy. Można więc przy jego wykorzystaniu uzyskać połączenie z prędkością 128 kb/s lub 64 kb/s przy jednoczesnym korzystaniu z telefonu. Wadą tego rozwiązania są wyższe koszty eksploatacji (droższe są połączenia telefoniczne) w porównaniu z linią analogową.

HIS czyli SDI

Usługą, którą Telekomunikacja Polska S.A. zaczęła oferować polskim internautom, jest tania oferta połączenia stałego z Internetem opartego na rozwiązaniu firmy Ericsson – HIS (*Home Internet Solution*) i zwane w TPSA – SDI (Szybki Dostęp do Internetu). Usługa ta zapewnia dostęp z prędkością 115.2 kb/s. Taka szybkość wystarcza do połączenia z Internetem sieci złożonej już z kilku komputerów. Oczywiście wydajność takiego połączenia w przeliczeniu na jeden komputer będzie tym mniejsza, im więcej komputerów będzie z niego jednocześnie korzystać.
Technologia przesyłu danych jest podobna do linii ISDN. SDI umożliwia jednoczesne korzystanie z podłączonego telefonu, lecz w takim wypadku prędkość połączenia spada do 70 kb/s.
Jest to obecnie najtańsza na rynku oferta połączenia stałego, której dodatkową zaletą jest stały, widziany z zewnątrz adres IP co oznacza, że możliwe jest postawienie własnego prostego serwera internetowego.
Więcej informacji można znaleźć na stronach Telekomunikacji Polskiej S.A. pod adresem http://www.tpsa.pl oraz witrynie firmy Ericsson (http://his.ericsson.pl).

Modem kablowy

Ofertą przedstawianą coraz częściej przez telewizje kablowe jest dołączenie do Internetu przez łącze stałe. Połączenie to jest wykonywane przy pomocy tzw. modemu kablowego umożliwiającego transmisję danych po kablu telewizyjnym. Rozwiązanie to jednak jest jak dotąd mało rozpowszechnione prawdopodobnie ze względu na wysokie koszty takiego rozwiązania. Należy jednak przypuszczać, że w najbliższych latach technologia ta się rozwinie.

xDSL

Jest to technologia dzierżawionych łącz stałych umożliwiająca, przy pomocy modemów z rodziny DSL (*Digital Subscriber Line*), uzyskanie transmisji danych po parze miedzianej wydzielonej specjalnie do tego celu.
ADSL (*Asymmetric* DSL) – polega na podziale pasma wykorzystywanego do transmisji na tzw. UpLink i DownLink. Wykorzystuje się tu fakt, że przeciętny użytkownik Internetu pobiera z Sieci znacznie więcej danych, niż do niej wysyła. Umożliwia to przydzielenie większej szerokości pasma dla transmisji do internauty oraz mniejszej dla transmisji od niego, co skutkuje różną przepustowością łącza w każdym kierunku. Szybkość transmisji zależy również oczywiście od długości pary miedzianej oraz jakości kabla i zakłóceń zewnętrznych.
W chwili gdy piszę te słowa, TPSA wprowadza nową usługę pod nazwą „neostrada" będącą ofertą stałego dostępu do Internetu przy wykorzystaniu technologii ADSL. Przepustowość UpLink'a ma w założeniu wynosić 64 kb/s zaś DownLink'a do 256 kb/s.
RADSL (*Rate Adaptive* DSL) – opiera się na technologii ADSL. Jej cechą charakterystyczną jest możliwość negocjacji przez modemy prędkości połączenia w zależności do jakości linii.
SDSL (*Single line* DSL) – zapewnia symetryczną transmisję dwukierunkową po jednej parze przewodów miedzianych z prędkością 2 Mb/s.
HDSL (*High data rate* DSL) – umożliwia transmisję z prędkością 2 Mb/s po dwóch parach miedzianych. Jest to starsza wersja SDSL.

Udostępnianie połączenia internetowego w sieci lokalnej

Gdy już mamy zapewnione połączenie z Internetem na jednej maszynie, należy zastanowić się, jak udostępnić to połączenie innym komputerom. 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.
Komputer udostępniający połączenie może być zwykłą stacją roboczą przeznaczoną dodatkowo do tego celu. Do bardziej znanych proxy serwerów pod Windows 95/98 należą: WinGate, WinProxy, NetProxy, CProxy.

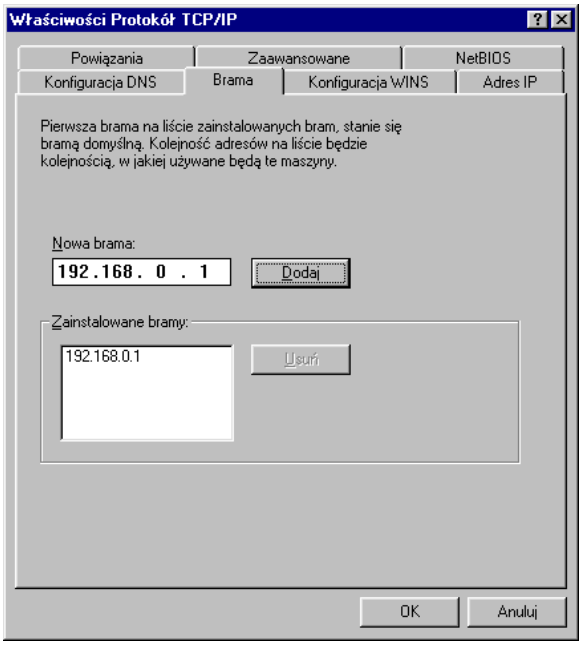
Technologię NAT wykorzystuje zaś m.in. program SyGate i WinRoute (który dodatkowo wbudowane ma pewnego typu proxy i filtr pakietów).

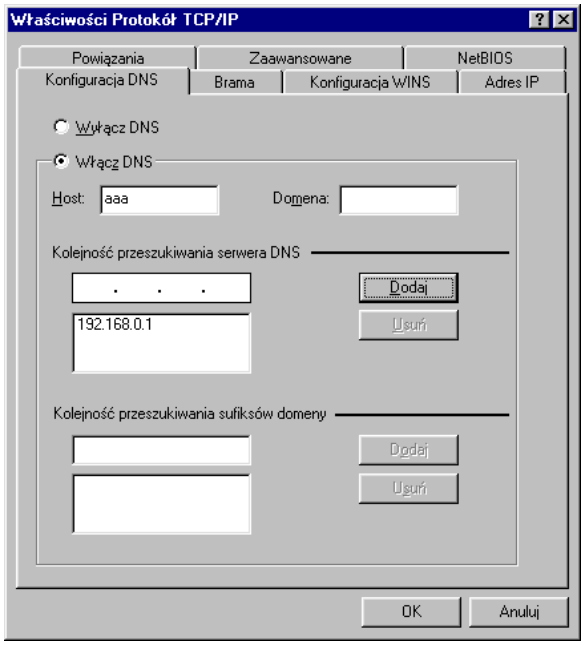
Można również wykorzystać mechanizm dzielenia połączenia modemowego wbudowany w drugą edycję systemu MS Windows 98 (tzw. SE – *Second Edition*).

Dużo lepszym jednak rozwiązaniem (dającym dużo większe możliwości zwłaszcza, jeśli dysponujemy stałym łączem do Internetu) jest uruchomienie osobnej maszyny zajmującej się tylko umożliwieniem dostępu do Sieci (ew. udostępniającymi również inne usługi sieciowe) pracującej pod którymś z systemów uniksowych np. pod systemem Linux. Jej uruchomienie będzie na pewno dużo trudniejsze, niż uruchomienie udostępniania połączenia pod Windows, lecz w wielu wypadkach będzie się to bardziej opłacać, gdyż będziemy mieć większą (praktycznie prawie całkowitą) kontrolę nad tym, jakiego rodzaju aplikacjom klienckim umożliwiamy dostęp do Internetu. Rozwiązanie to jest również o wiele wydajniejsze, dużo bardziej niezawodne i bezpieczniejsze z punktu widzenia bezpieczeństwa samej sieci wewnętrznej przed atakami z zewnątrz. Pamiętać jednak należy, że skonfigurowanie zapory sieciowej w sposób zapewniający maksymalne bezpieczeństwo przy równie wysokiej funkcjonalności wymaga już doświadczenia i wykracza daleko poza ramy tego opracowania.

Konfiguracja SyGate'a

Po zainstalowaniu programu SyGate w systemie Windows (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 tak, aby wskazywały 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:





Uruchomienie maskarady na maszynie linuksowej

Rozdział ten zawiera krótki przewodnik, jak postawić szybko maskaradę w oparciu o system Linux (na przykładzie dystrybucji Debian), przygotowany przez Rafała Woźniaka <kanar@infinity.net.pl>.
Aby postawić maszynę linuksową pełniącą rolę maskarady, należy w pierwszej kolejności zaopatrzyć się w komputer, który rolę tę będzie pełnił. Zalecane jest przynajmniej Pentium 60 z dyskiem 512 MB i 16 MB pamięci RAM. Oczywiście bardzo pomocny będzie również napęd CD-ROM przy instalacji. Później staje się zbędnym gadżetem.

Niestety, ponieważ Linux jako system operacyjny różni się w dość dużym stopniu od systemu Windows, więc aby w ogóle go uruchomić, a następnie nim administrować, należy posiąść pewną wiedzę. Najlepszym jej źródłem są, moim zdaniem, dokumenty HOW-TO oraz pozycje książkowe. Dużą pomocą będą również podane na końcu tego opracowania linki jak również lektura archiwów grup *pl.comp.os.linux* oraz *pl.comp.os.linux.sieci*.

Po pierwsze, aby działało współdzielenie łącza na maszynie linuksowej, *kernel* musi być skompilowany z odpowiednimi opcjami. Dla *kernela* 2.2.17 (opis kompilacji *kernela*, znajdziesz np. pod adresem http://www.linuxfan.com.pl/artykuly/kompilacja.html) wchodzimy do menu *„Networking options”* i zaznaczamy opcję (o ile jeszcze nie jest) *„TCP/IP networking”*. Wówczas pokażą nam się opcje typu *„IP: [coś]”*. Aby działało współdzielenie łącza musimy wybierać *„IP: masquerading”*. Ogólnie warto zaznaczyć większość opcji *„IP: [coś]”*.
Jeśli nie czujesz się na siłach, aby na początek kompilować *kernel*, to można zostawić domyślny *kernel* wgrywany przez program instalacyjny. Powinien zawierać wszystkie składniki potrzebne do współdzielenia łącza.

Zanim zaczniemy tworzyć skrypty musimy przyjąć pewne założenia oraz wyjaśnić jak zapisuje się skrótowo *maskę podsieci*. Załóżmy iż w swojej sieci będziesz korzystać z adresów 10.1.1.0-10.1.1.255 (tzw. pula adresów prywatnych, które w zasadzie obejmują adresy od 10.0.0.0 do 10.255.255.255, gdzie maska podsieci jest 255.0.0.0 lub skrótowo 8). Teraz zajmijmy się skrótowym zapisem *maski podsieci*. Otóż np. zapis 10.1.1.0/24 oznacza adresy od 10.1.1.0 do 10.1.1.255. Dla tych adresów maska jest 255.255.255.0, czyli:
24 oznacza maskę 255.255.255.0
16 oznacza maskę 255.255.0.0
8 oznacza maskę 255.0.0.0

Powróćmy do tworzenia skryptu. Nazwijmy ten skrypt **maskarada**.

Każdy skrypt musi zaczynać się od takiej linijki tekstu:

```
#!/bin/sh
```

Aby w ogóle działała maskarada musimy dopisać:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Kolejnym krokiem jest wykasowanie wszystkich regułek:

```
/sbin/ipchains -F
```

Kolejna linijka skryptu oznacza aby nasz serwer nie używał maskarady gdy bezpośrednio odwołujemy się do adresów prywatnych, tzn. gdy ktoś z komputera z adresem prywatnym łączy się z komputerem w naszej sieci, który również ma adres prywatny.

```
/sbin/ipchains -A forward -j ACCEPT -s 10.0.0.0/8 -d 10.0.0.0/8
```

Teraz zajmiemy się uruchomieniem maskarada dla wybranego komputera. Powtarzamy to dla każdego użytkownika jeśli mamy takich, którzy płacą i nie płacą za Internet. Na przykład dla komputera z prywatnym adresem IP 10.1.1.1:

```
/sbin/ipchains -A forward -j MASQ -s 10.1.1.1 -d 0.0.0.0/0
```

Jeśli wszyscy płacą za Internet to prościej to zrobić w następujący sposób (tutaj dla klasy 256 IP od 10.1.1.0 do 10.1.1.255):

```
/sbin/ipchains -A forward -j MASQ -s 10.1.1.0/24 -d 0.0.0.0/0
```

Teraz podam parę innych przykładów, które warto zastosować.
Zacznijmy od zablokowania wysyłania poczty poprzez inne serwery niż nasz. Zapobiega to spamowaniu przez użytkownika sieci w taki sposób, aby nie został wykryty. Zasada jest prosta. Nie może wysyłać przez inny serwer poczty niż nasz. W takim razie musi korzystać z naszego, a gdy z niego skorzysta to zostanie na nim informacja kto wysyłał, skąd, kiedy, etc. Aby ta metoda była skuteczniejsza polecam zainteresowaniem się *staticarp*, czyli przypisaniem adresu MAC karty sieciowej do adresu IP. To znowu w celu zapobieżeniu podszywania się pod czyjeś IP (o tym jak to się robi napiszę w dalszej części). Wówczas to co w logach zostaje oznacza, ze nikt nie mógł się pod kogoś innego podszyć i wiemy, ze to z tego konkretnego komputera wysłano niechcianą pocztę, czyli spam.

```
/sbin/ipchains -A forward -j REJECT -s 10.0.0.0/8 -d 0.0.0.0/0 25 -p TCP
```

Kolejny praktyczny przykład pokazuje jak stworzyć *transparent proxy*, czyli przekierowanie bezpośrednie wywołanie strony www na proxy. Wówczas w przeglądarkach Internet Explorer czy Netscape Navigator nie

trzeba ustawiać proxy. Aby to działało w konfiguracji *kernela* musi być zaznaczona opcja *„IP: transparent proxy support”*, a dodatkowo w konfiguracji SQUIDa (zakładam iż z takiego serwera proxy skorzystasz) w pliku /etc/squid.conf trzeba dopisać:

```
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

Zakładam, że SQUID działa na porcie 8080.

```
ipchains -A input -p tcp -s 10.0.0.0/8 -d 0/0 80 -j REDIRECT 8080
```

Powróćmy na chwilę do zapobiegania spamowaniu przez użytkowników. Otóż powinniśmy teraz przypisać adres MAC do konkretnego adresu IP. Otóż tworzymy plik /etc/ethers. Jego zawartość jest następująca:

```
#MAC adres                      adres IP
#MAC adres serwera              10.1.1.1
MAC adres użytkownika nr 1      10.1.1.2
MAC adres użytkownika nr 2      10.1.1.3
.........
MAC adres użytkownika nr 253    10.1.1.254
```

Proszę zwrócić uwagę na dwie rzeczy. Pierwsza to taka, iż adres serwera (przyjęty jako 10.1.1.1) jest zahaszowany. Po prostu przy wpisywaniu tego adresu do tablicy wystąpi błąd. Nic groźnego. Druga uwaga iż trzeba dla wszystkich 254 adresów IP zrobić przypisanie (adresy 10.1.1.0 oraz 10.1.1.255 to odpowiednio adres sieci i broadcast – do tych adresów nie można przypisać MAC adresów, jak również nie można ich wykorzystać). Jeśli dany adres IP nie jest używany w sieci to po prostu przypisujemy mu jakiś wymyślony (fikcyjny) adres MAC. Gdybyśmy tego nie zrobili to ktoś może ustawić sobie ten adres IP u siebie i wówczas nie będziemy mogli określić kto to zrobił.
Teraz mając tak przygotowany plik *staticarp* uruchamiamy polecenie:

```
arp –f
```

Spowoduje to już w Linuksie przypisanie adresu MAC z adresem IP.

Obydwa skrypty: *maskarada* oraz *arp –f* trzeba dopisać do skryptów startowych. W Debianie w najprostszy i najszybszy sposób to dopisać do pliku /etc/init.d/rmlogin wywołania obydwu skryptów.

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.

„Linux – Sekrety instalacji i konfiguracji” Tom I i II – Wydawnictwo RM sp. z o.o., Wydanie I, Warszawa 1999 r. – książka zawierająca opis systemu Linux na przykładzie dystrybucji RedHat. Nie jest ona wyczerpująca, lecz zawiera wiele interesujących informacji o samym systemie i jego konfiguracji, przydatna zwłaszcza dla początkujących linuksowców.

„Linux – Agresja i Ochrona” – Wydawnictwo Robomatic, 2000 r. – dzieło anonimowego autora opisujące metody ochrony maszyn linuksowych przed atakami zarówno zdalnymi, jak i bezpośrednimi (przy fizycznym dostępie do konsoli systemu).

Miejsca w Internecie

http://gadula.nfosigw.gov.pl/network_FAQ/network_FAQ.html – FAQ grupy *pl.comp.networking*.

http://www.newsgate.pl – system służący do prowadzenia dyskusji przez www, grupy dyskusyjne i pocztę elektroniczną. Zawiera między innymi archiwum grup *pl.comp.networking*, *pl.comp.os.win95*, *pl.comp.os.linux*, *pl.comp.os.linux.sieci* oraz wielu innych.

http://lanzone.koti.com.pl – 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.man.rzeszow.pl/docs/ip/ – opis podstaw protokołu TCP/IP.

http://www.kki.net.pl/~alchemialan/ – tutaj można znaleźć informacje o standardach i konfiguracji sieci komputerowych, konfiguracji serwerów uniksowych.

http://www.jtz.org.pl – witryna projektu „Jak To Zrobić” gdzie znajdziemy zbiór dokumentów HOW-TO Linuksa tłumaczony na język polski. Ciekawa lektura nie tylko dla Linuksowców.

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 – online’owa wersja książki opublikowanej przez wydawnictwo Mikom. Prezentuje ponad 1000 haseł opatrzonych ilustracjami oraz odnośnikami do miejsc w Sieci.

http://dreamnet.help.pl – serwis amatorskich sieci komputerowych. Wiele artykułów opisujących podstawy działania sieci.

http://siecilokalne.republika.pl – jeszcze jedna witryna poświęcona lokalnym sieciom komputerowym

http://www.iksyon.prv.pl – różne informacje na temat sieci lokalnych i rozległych oraz o różnych systemach operacyjnych

http://republika.pl/teoria/ – witryna poświęcona podejściu do działania sieci lokalnych od strony teoretycznej

http://free.polbox.pl/c/cyfraa/ – inna strona poświęcona sieciom lokalnym.

http://www.ots.utexas.edu/ethernet/ – strona zawierająca opisy technologii ethernetowych 10 Mb/s, 100 Mb/s, 1000 Mb/s, 10 Gb/s.

http://www.6bone.pl – informacje o testowej sieci IPv6 w Polsce.

http://zlobek.tcz.wroclaw.pl – żłobek dla początkujących użytkowników Linuksa. Znajdują się tam przystępne opisy krok po kroku, jak zainstalować Linuksa i uruchomić wiele z jego usług.

http://linuxfan.com.pl/artykuly/ – zbiór krótkich artykułów przeznaczonych dla początkujących użytkowników.

http://www.klubhis.hrleon.com – strona klubu użytkowników HIS’a