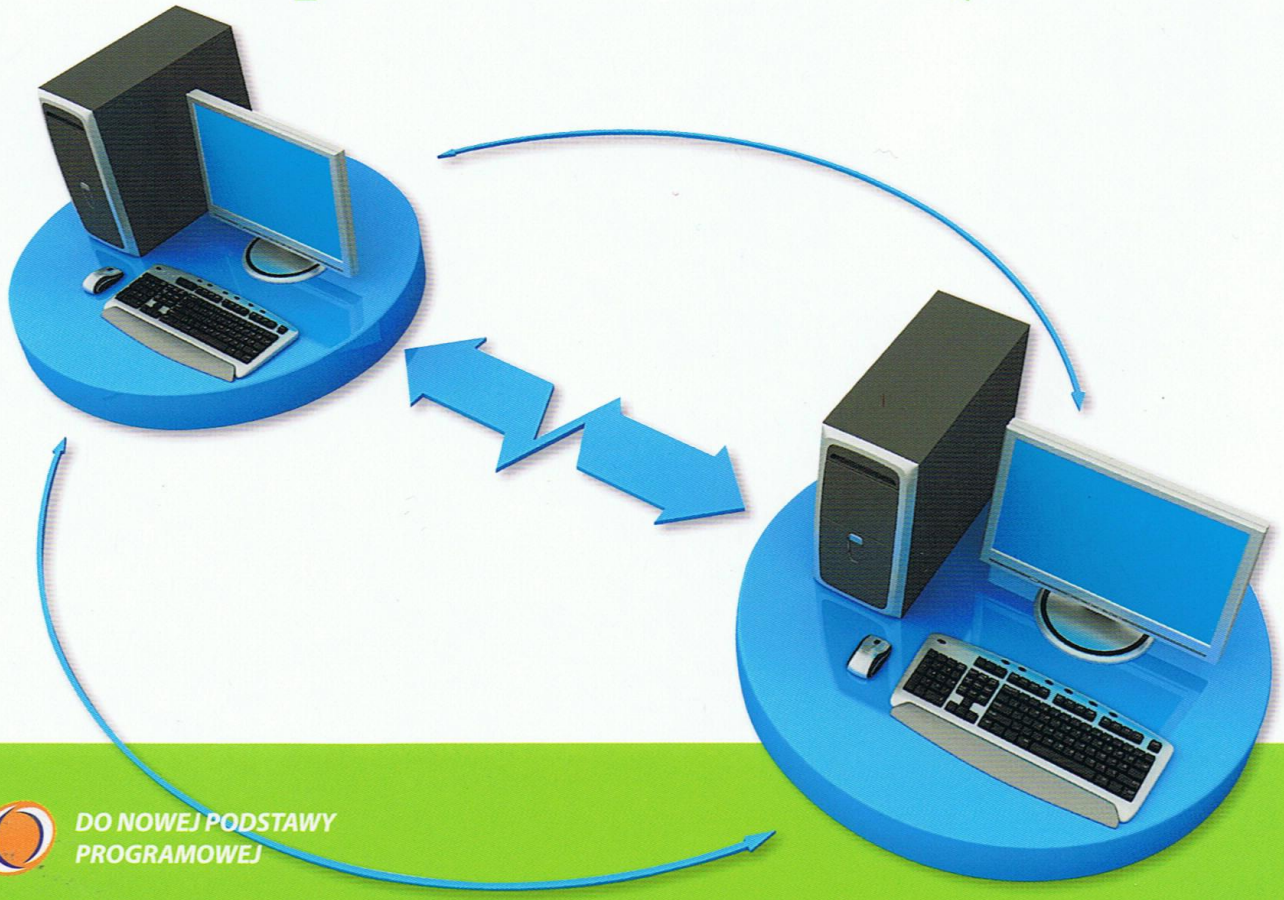
REFORMA 2012

Projektowanie i wykonywanie lokalnej sieci komputerowej



DO NOWEJ PODSTAWY PROGRAMOWEJ

Kwalifikacja E.13.1

Podręcznik do nauki zawodu

- TECHNIK INFORMATYK
- TECHNIK TELEINFORMATYK

WSiP

REFORMA 2012

Projektowanie i wykonywanie lokalnej sieci komputerowej

Krzysztof Pytel, Sylwia Osetek

Kwalifikacja E.13.1

Podręcznik do nauki zawodu

- TECHNIK INFORMATYK
- TECHNIK TELEINFORMATYK

WSiP

Podręcznik dopuszczony do użytku szkolnego przez ministra właściwego do spraw oświaty i wychowania i wpisany do wykazu podręczników przeznaczonych do kształcenia w zawodach na podstawie opinii rzeczoznawców:
dr. Jarosława Pacuły, dr. Kazimierza Mikulskiego, dr. inż. Tomasza Ciszewskiego.
Typ szkoły: **technikum i szkoła policealna.**
Zawód: **technik informatyk, technik teleinformatyk.**
Kwalifikacja: **E13. Projektowanie lokalnych sieci komputerowych i administrowanie sieciami.**
Część kwalifikacji: **1. Projektowanie i wykonywanie lokalnej sieci komputerowej**

Rok dopuszczenia **2013.**

© Copyright by Wydawnictwa Szkolne i Pedagogiczne sp. z o.o.
Warszawa 2013

Wydanie I (rzut I)

ISBN 978-83-02-13411-1

Opracowanie merytoryczne i redakcyjne: **Zbigniew Dziedzic** (redaktor koordynator)
Konsultacja: **dr inż. Mieczysław Rudnicki**
Redakcja językowa: **Aleksandra Wieczorek**
Redakcja techniczna: **Elżbieta Walczak**
Projekt okładki: **Dominik Krajewski**
Skład i łamanie: **Pracownia Książki**

Wydawnictwa Szkolne i Pedagogiczne spółka z ograniczoną odpowiedzialnością
02-807 Warszawa, Aleje Jerozolimskie 96
Tel.: 22 576 25 00
Infolinia: 801 220 555
www.wsip.pl
Druk i oprawa: Drukarnia Trans-Druk Sp. Jawna

Publikacja, którą nabyłeś, jest dziełem twórcy i wydawcy. Prosimy, abyś przestrzegał praw, jakie im przysługują. Jej zawartość możesz udostępnić nieodpłatnie osobom bliskim lub osobiście znanym. Ale nie publikuj jej w internecie. Jeśli cytujesz jej fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A kopiując jej część, rób to jedynie na użytek osobisty.

prawolubni

Szanujmy cudzą własność i prawo.
Więcej na www.legalnakultura.pl
Polska *Izba Książki*

I. Podstawy lokalnych sieci komputerowych

II. Projektowanie lokalnych sieci komputerowych

III. Projektowanie i montaż okablowania

IV. Modernizacja i rekonfiguracja lokalnych sieci komputerowych

I. Podstawy lokalnych sieci komputerowych

- Podstawowe pojęcia dotyczące sieci komputerowych
- Jednostki miar w sieciach komputerowych
- Rodzaje oraz charakterystyka mediów transmisyjnych
- Rodzaje, budowa i funkcje urządzeń sieciowych
- Symbole graficzne urządzeń sieciowych
- Dokumentacja techniczna urządzeń sieciowych
- Topologie sieciowe (logiczna i fizyczna)
- Metody dostępu do nośnika
- Rodzaje środowisk sieciowych (architektura równorzędna i klient-serwer)
- Komunikacja w sieci
- Modele warstwowe sieci
- Protokoły warstwy łącza danych
- Protokoły warstwy sieci
- Adresowanie w sieci komputerowej
- Zasady projektowania adresacji IP
- Adresowanie IPv6
- Protokoły warstwy transportowej
- Protokoły warstwy aplikacji
- Inne zestawy protokołów sieciowych

1 Podstawowe pojęcia dotyczące sieci komputerowych

ZAGADNIENIA

- **Z jakich elementów składa się sieć komputerowa?**
- **Po co buduje się sieci komputerowe?**
- **Jakie są rodzaje adresów sieciowych?**
- **Jak dzieli się sieci ze względu na obszar ich działania?**

We współczesnym świecie komunikacja odgrywa ważną rolę w przekazywaniu informacji. Komunikujemy się z innymi bezpośrednio za pomocą np. głosu, znaków, gestów. Również komunikacja na odległość stała się już codziennością. Wykorzystujemy w tym celu różne urządzenia techniczne, takie jak telefony stacjonarne i komórkowe, usługi pocztowe, stacje radiowe i telewizyjne. Coraz większą rolę w procesach komunikacji odgrywają sieci komputerowe. **Sieć komputerowa** (*computer network*) jest systemem komunikacyjnym służącym do przesyłania danych, łączącym co najmniej dwa komputery i urządzenia peryferyjne.

Sieci komputerowe łączą ze sobą odległe komputery. Ze względu na obszar, jaki obejmują swym zasięgiem, przeznaczenie i przepustowość sieci można podzielić na następujące typy:

Sieci osobiste PAN (*Personal Area Network*) – sieci o zasięgu kilku metrów wykorzystywane np. do bezprzewodowego połączenia telefonu komórkowego ze słuchawką, komputera z myszką lub klawiaturą.

Sieci lokalne LAN (*Local Area Network*) – sieci łączące użytkowników na niewielkim obszarze (pomieszczenie, budynek). W sieciach LAN prędkość przesyłania danych jest duża. Przykładem sieci lokalnej może być sieć szkolna.

Sieci miejskie MAN (*Metropolitan Area Network*) – sieci o zasięgu miasta, najczęściej szybkie. Umożliwiają połączenia między sieciami lokalnymi uczelni, ośrodków naukowych, organów administracji i centrów przemysłowych.

Sieci rozległe WAN (*Wide Area Network*) – sieci, których zasięg przekracza granice miast, państw i kontynentów. Składają się z węzłów i łączących je łączy transmisyjnych, realizowanych za pomocą publicznej sieci komunikacyjnej, np. telefonicznej, kanałów satelitarnych, radiowych. Dostęp do sieci rozległej uzyskuje się przez dołączenie komputerów lub sieci lokalnych do węzłów sieci. Przykładem sieci rozległej jest internet.

Sieci komputerowe umożliwiają:

- współużytkowanie programów i plików,
- współużytkowanie innych zasobów, takich jak: drukarki, plotery, pamięci masowe,
- współużytkowanie baz danych,
- ograniczenie wydatków na zakup stacji roboczych,

- tworzenie grup roboczych, w których ludzie z różnych miejsc mogą uczestniczyć w tym samym projekcie,
- wymianę poczty elektronicznej.

Na sieci komputerowe składają się **elementy sprzętowe** oraz **programowe.**
Do elementów sprzętowych sieci zaliczamy:

- **Urządzenia transmisji** – nośniki używane do transportu sygnałów biegnących przez sieć do ich miejsc docelowych. Najczęściej stosowanymi nośnikami są kable miedziane i światłowodowe. Nośniki mogą być również niematerialne, jak przestrzeń, przez którą są przesyłane światło lub fale radiowe.
- **Urządzenia dostępu** – są odpowiedzialne za formatowanie danych w taki sposób, aby nadawały się one do przesyłania w sieci. Odpowiadają także za umieszczanie danych w sieci oraz ich odbieranie. W sieci lokalnej urządzeniami dostępu są karty sieciowe. W sieciach rozległych urządzeniami dostępu są modemy.
- **Urządzenia wzmacniania przesłanych sygnałów** – urządzenia, które odbierają przesyłane sygnały, wzmacniają je i wysyłają z powrotem do sieci. W sieciach lokalnych tę funkcję pełni koncentrator, który umożliwia ponadto przyłączanie do sieci wielu urządzeń.

Składnikami programowymi sieci są:

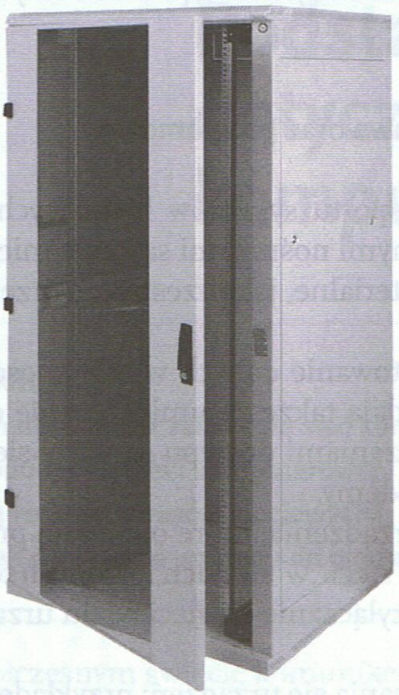
- **Protokoły** (*protocols*) – określają sposoby komunikowania się urządzeń; przykładem protokołu może być IP.
- **Sterowniki urządzeń** (*drivers*) – programy umożliwiające działanie urządzeniom, takim jak karty sieciowe.
- **Oprogramowanie komunikacyjne** (*communication software*) – korzysta ono z protokołów i sterowników do wymiany danych. Są to np. programy do udostępniania zasobów, programy przesyłania plików, programy do obsługi poczty elektronicznej, przeglądarki internetowe itp.

Dane w sieci przesyłane są pomiędzy nadawcą a odbiorcą przez łącza komunikacyjne (*communication links*). Łącze komunikacyjne to zespół środków technicznych służących do przesyłania sygnałów między oddalonymi stacjami sieci teleinformatycznej, np. kanał telefoniczny. Pomiędzy nadawcą a odbiorcą danych może znajdować się wiele **węzłów sieci** (*nodes*). Węzeł sieci to urządzenie sieciowe, w którym zbiega się wiele łączy komunikacyjnych. Węzeł sieci kieruje przesyłaniem informacji do odpowiedniego łącza. Węzłami sieci lokalnych mogą być **przełączniki sieciowe** (*switches*), a w sieciach rozległych stosuje się **routery** (*routers*).

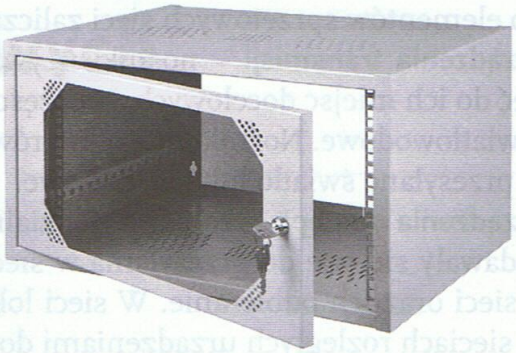
W sieci istnieje wiele komputerów, których zadaniem jest świadczenie pewnych usług innym urządzeniom w sieci, np. udostępnianie plików, drukarek lub innych zasobów. Komputer taki nazywany jest **serwerem** (*server*), a urządzenie korzystające z tych usług – **klientem** (*client*). Serwerem może być zwykły komputer, jednak w celu pełnego wykorzystania możliwości i zapewnienia niezawodności powinna to być maszyna przystosowana do pracy ciągłej, wyposażona w duże i szybkie dyski twarde, dużą ilość pamięci RAM oraz wydajne procesory.

Profesjonalne urządzenia sieciowe, takie jak przełączniki, routery, serwery i inne, przystosowane są do montażu w specjalnych szafach dystrybucyjnych typu RACK. Standardowa szerokość urządzeń wynosi 19" (19 cali, 482 mm). Wysokość urządzeń określana jest w jednostkach U. 1 U oznacza urządzenie o wysokości 1,75" (44,5 mm). Szafy dystrybucyjne stojące mogą mieć wysokość do 47 U (w takiej szafie można zmieścić np. 47 modularnych urządzeń o wysokości 1U). Szafki wiszące są na ogół mniejsze i mają wysokość kilku lub kilkunastu U. Szafy mogą być wyposażone w dodatkowe urządzenia, takie jak zestawy wentylatorów, moduły oświetlenia, zamki i systemy kontroli dostępu.

a)



b)



Rys. 1.1. Przykładowe szafy dystrybucyjne: a) szafa stojąca, b) szafa wisząca

Aby dane mogły niezawodnie przemieszczać się pomiędzy poszczególnymi punktami sieci, każdy z takich punktów musi być jednoznacznie oznaczony. Każde urządzenie pracujące w sieci i każdy komputer ma przypisany identyfikator, który jednoznacznie identyfikuje go w sieci. Identyfikator taki nazywany jest **adresem sieciowym** (*network address*). W sieciach stosowane są różne systemy adresowania, np. w sieci internet obowiązują adresy IP, a w sieciach Ethernet każde urządzenie ma unikatowy adres fizyczny (MAC).

Dane przed przesłaniem ich przez sieć dzielone są na mniejsze części, np. ramki lub pakiety, które łatwiej przesyłać. Każda z tych części zaopatrzona jest w adres miejsca źródłowego i docelowego, dzięki czemu można określić, kto jest nadawcą i adresatem danych, a także mogą one niezależnie od innych przemieszczać się w sieci.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jakie inne, niewymienione w rozdziale, urządzenia wykorzystuje się do komunikacji?
2. Do jakich celów Ty wykorzystujesz sieć komputerową?
3. Ile milimetrów ma 1 cal angielski?

2 Jednostki miar w sieciach komputerowych

ZAGADNIENIA

- **Jakich jednostek używa się do wyrażenia zmian względnych wielkości fizycznych?**
- **W jaki sposób wyraża się wartość szumów w telekomunikacji?**
- **Jakie są jednostki przesyłania danych?**
- **Jak policzyć, ile czasu zajmie przesłanie pliku przez sieć?**

Procesor, układy pamięci i inne układy komputera rozróżniają jedynie dwie wartości, oznaczone symbolami **0** i **1**. Taki sposób interpretowania umownych wartości 0 i 1 został powszechnie przyjęty w informatyce i jest stosowany również do określania parametrów transmisji danych. Ilość pamięci potrzebna do zapisania jednej z tych wartości jest podstawową jednostką i nazywa się **bitem** (*binary digit*). Oznacza się ją symbolem **b**.

Istnieją różne typy transmisji danych. Transmisja może odbywać się między poszczególnymi komponentami wewnątrz komputera lub między różnymi komputerami za pośrednictwem sieci, linii telefonicznych, modemu itp. Podstawową jednostką prędkości przesyłania danych w transmisji szeregowej (czyli takiej, podczas której poszczególne bity informacji są przesyłane kolejno) jest bit na sekundę. Jednostka ta może być zapisywana jako **bps** (*bit per second*) lub b/s.

W celu zwiększenia stopnia wykorzystania pasma transmisyjnego można stosować sposoby kodowania sygnałów, w których każdy symbol może przyjmować więcej niż dwie wartości (reprezentowane za pomocą większej liczby bitów). Liczba symboli przesyłanych w ciągu jednej sekundy mierzona jest w jednostkach nazywanych bodami (baud). Na przykład transmisja z prędkością 100 bodów oznacza, że w ciągu sekundy sygnał może zmienić się 100 razy. Jeżeli każdy symbol niesie informację o 3 bitach, oznacza to, że w ciągu każdej sekundy przesyłanych jest 300 bitów.

Przed wprowadzeniem łączności radiowej w marynarce do komunikacji wykorzystywany był alfabet semaforowy, w którym sygnalista za pomocą pozycji rąk przekazywał informacje. Pojedyncza flaga sygnalizacyjna mogła być umieszczona w jednej z 8 pozycji: podniesiona w górę, pod kątem 45 stopni w lewo w górę, w lewo, w lewo w dół, w dół, w prawo w dół, w prawo i w prawo w górę. W systemie dwójkowym informacja taka byłaby zapisana na 3 bitach (8 różnych wartości). Jeżeli sygnalista zmieniałby położenie ręki 1 raz w ciągu sekundy, to prędkość przesyłania danych wynosiłaby 1 bod (1 symbol na sekundę) lub 3 b/s (3 bity na sekundę). Liczbę przesłanych bitów można byłoby zwiększyć, gdyby użyto obu rąk (każdy symbol reprezentowałby większą ilość bitów) przy niezmienionej liczbie przesłanych symboli.

Zamawiając u dostawcy usług internetowych (*ISP – Internet Service Provider*) łącze, należy określić parametry tego łącza. Jednym z tych parametrów jest oferowana prędkość transmisji danych podawana w kb/s lub Mb/s. Obecnie ISP oferują dwa główne sposoby

dostępu: stacjonarny oraz mobilny. Oba rozwiązania należą do usług szerokopasmowej transmisji danych. Dostęp stacjonarny oznacza na ogół stały dostęp do Internetu, o dużej przepustowości transferu, bez ograniczeń ilości pobieranych danych. Rozwiązania mobilne umożliwiają korzystanie z Internetu w każdym miejscu, które jest w zasięgu działania sieci operatora. Prędkości łączy mobilnych dorównują tym, z którymi spotykamy się w rozwiązaniach stacjonarnych, lecz mogą posiadać ograniczenie ilości odbieranych i wysyłanych danych. Jest to jednak ograniczenie techniczne, wprowadzone przez dostawcę w celu zróżnicowania oferty. W przypadku sieci lokalnych zbudowanych w standardzie Ethernet możemy spotkać różne prędkości przesyłania danych. Pierwsze wersje Ethernetu zbudowanego w oparciu o łącza kablowe oferowały prędkość do 10 Mb/s. Później wprowadzono FastEthernet o prędkości 100 Mb/s. Obecnie najczęściej stosuje się standard Gigabit Ethernet, a do wysoko wydajnych sieci wprowadzana jest prędkość 10Gigabit Ethernet lub 100Gigabit Ethernet.

Ponieważ wielkość plików zwykle jest podawana w bajtach, należy uwzględnić różnice w jednostkach. Aby obliczyć prędkość pobierania plików, których rozmiar jest podany w bajtach, prędkość przesyłania należy podzielić przez 8 (zamienić bajty na bity – 1 bajt to 8 bitów), czyli transfer 256 kb/s jest równoznaczny pobieraniu 32 kB/s.

Wyniki testowania sieci, np. światłowodowych lub bezprzewodowych mogą być podawane w decybelach. Decybeli (dB) używamy do porównania wielkości zmieniających się w bardzo szerokim zakresie, jeżeli interesują nas zmiany względne (np. procentowe). Wartości wyrażane w decybelach odnoszą się do stosunku dwóch wielkości, np. mocy sygnału P_k dostarczonej do odbiornika do mocy P_p przekazanej przez nadajnik. Do obliczania decybeli stosuje się wzór:

$$\mathrm{dB} = 10 \log_{10}\left(\frac{P_k}{P_p}\right).$$

Wartość wyrażona w decybelach wyraża wzrost (wartość dodatnia) lub spadek mocy (wartość ujemna). Liczba decybeli pozwala stwierdzić ile energii pozostało w fali, np. radiowej po pokonaniu określonej odległości. Przykładowo, jeżeli nadajnik wyemitował sygnał o mocy 100 [W], tłumienie w kanale komunikacyjnym wynosi 10 dB, to odbiornik odbierze sygnał o mocy 10 [W].

Innym ważnym parametrem jest wartość stosunku **sygnału do szumu** (*SNR, signal-to-noise ratio*). **Szum** jest to niepożądany sygnał pochodzący ze źródeł naturalnych, np. wyładowania elektryczne w czasie burzy, lub sztucznych, np. przewody energetyczne, urządzenia elektryczne itp. SNR określa wartość (wyrażoną najczęściej w dB) mocy sygnału użytecznego w zadanym paśmie częstotliwościowym do mocy szumów w tym samym paśmie częstotliwościowym. Im wyższa jest wartość SNR, tym odbiornik może łatwiej oddzielić sygnał użyteczny od zakłóceń.

Tabela 2.1. Jednostki szybkości transmisji danych

Jednostka	Nazwa
b/s (bps)	bity na sekundę
kb/s (kbps)	kilobity na sekundę
Mb/s (Mbps)	megabity na sekundę
Gb/s (Gbps)	gigabity na sekundę

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Oblicz minimalny czas potrzebny do transferu pliku o rozmiarze 5 MB przez łącze o przepustowości 56 kb/s, przy założeniu, że cała przepustowość jest wykorzystana do transmisji pliku (bez dodatkowego narzutu związanego z transmisją).
2. Co będzie przesłane szybciej: zawartość płyty CD (rozmiar 700 MB) przez sieć FastEthernet czy zawartość płyty DVD (4,7GB) przez sieć GigabitEthernet? Wykonaj obliczenia, aby uzasadnić odpowiedź. Przyjmij, że cała przepustowość jest wykorzystana do transmisji danych (bez dodatkowego narzutu związanego z transmisją). Wyniki i wnioski z obliczeń przedstaw do sprawdzenia nauczycielowi.

3 Rodzaje oraz charakterystyka mediów transmisyjnych

ZAGADNIENIA

- **Do czego służą media transmisyjne?**
- **Jakie media wykorzystywane są do budowy sieci komputerowych?**
- **Jak dobrać medium transmisyjne w sieci?**

Urządzenia sieciowe, aby wymieniać informacje, muszą być ze sobą połączone. Łącza wykorzystane w budowie sieci mogą korzystać z różnych nośników. Nośniki transmisji w sieciach, zwane również mediami transmisyjnymi, mogą być przewodowe, np. kable miedziane i światłowodowe, lub bezprzewodowe, np. fale radiowe, podczerwień, światło laserowe.

Najpopularniejszym medium transmisyjnym używanym obecnie do budowy sieci lokalnych jest **skrętka.** Składa się ona z czterech par przewodów umieszczonych we wspólnej osłonie. Aby zmniejszyć oddziaływanie elektromagnetyczne przewodów na siebie, są one wspólnie skręcone. Najpopularniejsze typy skrętki to:

- **nieekranowana** UTP (*Unshielded Twisted Pair*) – stosowana w większości sieci,
- **ekranowana** STP (*Shielded Twisted Pair*) – wyposażona w specjalną warstwę (ekran) chroniącą przed wpływem zakłóceń elektromagnetycznych. Odmiany skrętki ekranowanej różnią się między sobą sposobem wykonania ekranu.

Skrętka jest stosowana w telekomunikacji do przesyłania danych zarówno w postaci analogowej, jak i cyfrowej. Przydatność skrętki do transmisji danych jest określana za pomocą kategorii. Do budowy sieci jest używana:

- kategoria 3 (CAT 3) – stosowana w starszych sieciach o przepustowości do 10 Mb/s,
- kategoria 5 (CAT 5) – stosowana w sieciach o przepustowości do 100 Mb/s,
- kategoria 5e (CAT 5e) – skrętka kategorii 5, w której poprawiono parametry transmisji, stosowana w szybkich sieciach o przepustowości do 100 Mb/s lub 1 Gb/s,
- kategoria 6 (CAT 6) – stosowana do przenoszenia danych w sieciach o przepustowości do 10 Gb/s
- kategoria 7 (CAT 7) – ekranowana skrętka stosowana do przenoszenia danych w sieciach o przepustowości powyżej 1 Gb/s.

Większość nowych sieci komputerowych jest wykonywana przy wykorzystaniu skrętki kategorii 5e lub wyższych. Maksymalna długość połączeń wykonanych za pomocą skrętki, zapewniających standardowe parametry transmisji, wynosi 100 metrów. Skrętkę przyłącza się do karty sieciowej za pomocą złącza RJ-45. W starszych sieciach jako medium transmisyjne wykorzystywano **kabel koncentryczny** (*coaxial cable*), zbudowany z miedzianego rdzenia umieszczonego w osi kabla, otoczonego izolatorem oraz ekranem. Maksymalna prędkość transmisji przesyłanych nim danych wynosiła 10 Mb/s. Istnieją dwa rodzaje kabla koncentrycznego:

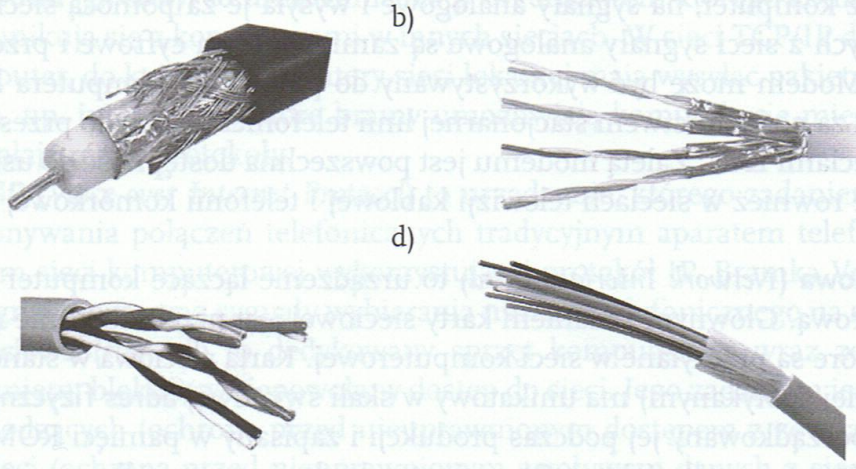
- gruby Ethernet – o średnicy około 1 cm, pozwalający transmitować dane na maksymalną odległość 500 m,
- cienki Ethernet – o średnicy około 0,5 cm, pozwalający transmitować dane na maksymalną odległość 185 m.

Najnowocześniejszym z obecnie stosowanych nośników transmisji przewodowej jest **światłowód** (*fiber optic cable*). Rdzeń światłowodu, wykonany ze szkła kwarcowego lub specjalnego tworzywa sztucznego, jest okryty płaszczem oraz warstwą ochronną. Transmisja polega na przesyłaniu przez rdzeń światłowodu wiązki światła, generowanej przez diodę lub laser. Dane są zakodowane w postaci impulsów światła. Do transmisji danych używa się zawsze pary przewodów, z których jeden służy do wysyłania danych, a drugi do ich odbierania. Ze względu na wysoką cenę oraz duże prędkości przesyłania danych i zasięg, światłowody najczęściej są stosowane do budowy szkieletu sieci, np. połączeń między przełącznikami. Światłowód jest całkowicie odporny na zakłócenia elektromagnetyczne, a ponadto uniemożliwia podsłuch transmisji.

Coraz większą popularność w sieciach komputerowych zdobywa **łączność bezprzewodowa**. Do transmisji danych są wykorzystywane fale elektromagnetyczne.

Najczęściej używane są:

- **Fale elektromagnetyczne w zakresie podczerwieni IR** (*InfraRed*) – jako źródła promieniowania wykorzystuje się diody LED lub diody laserowe. Zasięg i prędkość transmisji są niewielkie, stosowane do przyłączania, np. klawiatury lub myszy.
- **Fale radiowe** – najpopularniejsze sieci korzystają z częstotliwości 2,4 GHz lub 5 GHz, które nie podlegają koncesjonowaniu (w Polsce organem regulacyjnym w zakresie działalności pocztowej, telekomunikacyjnej i gospodarki częstotliwościowej oraz kontroli spełniania wymagań dotyczących kompatybilności elektromagnetycznej urządzeń jest Urząd Komunikacji Elektronicznej http://www.uke.gov.pl). Istnieją cztery standardy oznaczone 802.11a, 802.11b, 802.11g i 802.11n, zapewniające różne prędkości transmisji. Obecnie najbardziej popularnym standardem jest 802.11n zapewniający prędkość transmisji do 300 Mb/s. Fale radiowe wykorzystywane są również w innych typach łączności bezprzewodowej, np. w technologii Bluetooth, sieci 802.16 WiMAX lub w telefonii komórkowej 3G-UMTS/4G-LTE.



Rys. 3.1. Przykłady mediów transmisyjnych: a) kabel koncentryczny, b) skrętka ekranowana, c) skrętka nieekranowana, d) kabel światłowodowy

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jakie medium lub media transmisyjne są używane w Twojej szkole?
2. Jakie medium zapewnia najwyższe bezpieczeństwo przesyłanych danych i dlaczego?

4 Rodzaje, budowa i funkcje urządzeń sieciowych

ZAGADNIENIA

- **Jakie urządzenia są stosowane do budowy sieci komputerowych?**
- **Jaką rolę pełnią urządzenia sieciowe w przesyłaniu danych?**

Sieci komputerowe zbudowano, aby wymieniać dane między komputerami. Wymianę tę zapewnia zastosowanie odpowiedniego sprzętu oraz oprogramowania. Podstawowymi urządzeniami stosowanymi do budowy sieci komputerowych są:

- modemy,
- karty sieciowe,
- urządzenia wzmacniające,
- koncentratory,
- mosty,
- przełączniki,
- punkty dostępowe,
- routery,
- bramy sieciowe,
- bramki VoIP,
- zapory sieciowe.

Modem (*MOdulator DEModulator*) to urządzenie, które zamienia cyfrowe dane, generowane przez komputer, na sygnały analogowe i wysyła je za pomocą sieci. Podczas odbierania danych z sieci sygnały analogowe są zamieniane na cyfrowe i przekazywane do komputera. Modem może być wykorzystywany do połączenia komputera lub sieci LAN z Internetem za pośrednictwem stacjonarnej linii telefonicznej lub do przesyłania danych pomiędzy sieciami LAN. Zaletą modemu jest powszechna dostępność do usługi. Modemy są stosowane również w sieciach telewizji kablowej i telefonii komórkowej (np. modemy 3G/4G).

Karta sieciowa (*Network Interface Card*) to urządzenie łączące komputer z lokalną siecią komputerową. Głównym zadaniem karty sieciowej jest przekształcanie ramek danych w sygnały, które są przesyłane w sieci komputerowej. Karta sieciowa w standardzie **Ethernet** (najczęściej spotykanym) ma unikatowy w skali światowej **adres fizyczny** MAC (*MAC adress*), przyporządkowany jej podczas produkcji i zapisany w pamięci ROM. Karty mogą pracować z różnymi prędkościami. Obecnie standardem w przypadku sieci przewodowych są karty sieciowe pracujące z prędkością 100 Mb/s lub 1 Gb/s. W bezprzewodowych kartach sieciowych do przesyłania danych wykorzystywane są fale radiowe. Karta sieciowa może być wlutowana w płytę główną komputera lub innego urządzenia, albo montowana w różnych odmianach złączy PCI, PCMCIA, ExpressCard, USB, PCIExpress.

Wzmacniak (*repeater*), zwany również regeneratorem, wykorzystuje się w miejscach, w których jest wymagane wzmocnienie lub regeneracja sygnału, niezbędne do zwiększenia

zasięgu sieci. Rzadko jest to samodzielne urządzenie. Najczęściej funkcję wzmacniaka pełni urządzenie sieciowe posiadające własne zasilanie w energię elektryczną, np. koncentrator.

Koncentrator (*hub*) to urządzenie posiadające wiele portów służących do przyłączania stacji roboczych lub innych urządzeń. Koncentratory mogą być pasywne i aktywne. Pasywny pełni tylko funkcję skrzynki łączeniowej, rozsyłającej sygnał otrzymany na jednym porcie do wszystkich pozostałych. Aktywny dodatkowo wzmacnia sygnały.

Most (*bridge*) to urządzenie posiadające dwa porty, służące do łączenia segmentów sieci. W swojej pamięci zapamiętuje adresy MAC urządzeń przyłączonych do poszczególnych portów. Po otrzymaniu ramki danych sprawdza adres miejsca docelowego i określa, do jakiego segmentu należy przesłać daną ramkę. Gdy komputer z jednego segmentu wysyła wiadomość, most analizuje zawarte w niej adresy MAC i na tej podstawie podejmuje decyzję, czy sygnał przesłać do drugiego segmentu, czy go zablokować. W sieci nie są wtedy przesyłane zbędne ramki, dzięki czemu zwiększa się jej wydajność.

Przełącznik (*switch*) oferuje te same funkcje, co koncentrator, a dodatkowo pozwala, podobnie jak most, podzielić sieć na segmenty. Urządzenie posiada wiele portów przyłączeniowych, pozwalających na podłączenie komputerów, innych przełączników lub koncentratorów. Porty w przełączniku mogą pracować z jednakowymi prędkościami (przełączniki symetryczne) lub z różnymi prędkościami (przełączniki asymetryczne). Przełączniki mogą być wyposażone w funkcje zarządzania i monitoringu sieci.

Punkt dostępowy (*Access Point*) to urządzenie zapewniające stacjom bezprzewodowym dostęp do zasobów sieci za pomocą bezprzewodowego medium transmisyjnego. Pełni funkcję mostu łączącego sieć bezprzewodową z siecią przewodową. Do sieci bezprzewodowych są przyłączane laptopy, palmtopy, smartfony oraz komputery stacjonarne wyposażone w karty bezprzewodowe. Punkt dostępowy może być połączony w jedno urządzenie z routerem.

Router to urządzenie stosowane do łączenia sieci, np. do przyłączania sieci LAN do Internetu. Jest urządzeniem konfigurowalnym, pozwala sterować przepustowością sieci i podnosi jej bezpieczeństwo.

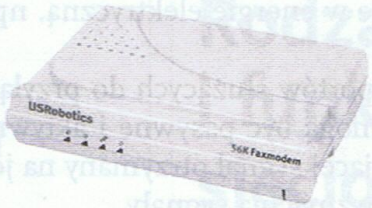
Brama sieciowa (*gateway*) to urządzenie, za pośrednictwem którego komputery z sieci lokalnej komunikują się z komputerami w innych sieciach. W sieci TCP/IP domyślna brama oznacza router, do którego komputery sieci lokalnej mają wysyłać pakiety adresowane do innej sieci, np. internet. Niektóre bramy umożliwiają komunikację między sieciami, w których działają różne protokoły.

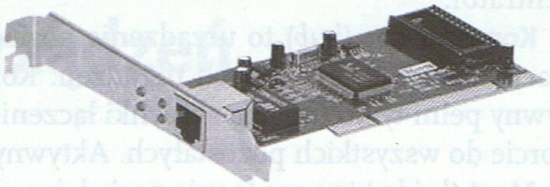
Bramka VoIP (*Voice over Internet Protocol*) to urządzenie, którego zadaniem jest umożliwienie wykonywania połączeń telefonicznych tradycyjnym aparatem telefonicznym za pośrednictwem sieci komputerowej wykorzystującej protokół IP. Bramka VoIP zamienia analogowy sygnał mowy oraz sygnały wybierania numeru telefonicznego na sygnały VoIP.

Zapora sieciowa (*firewall*) to dedykowany sprzęt komputerowy wraz ze specjalnym oprogramowaniem, blokujący niepowołany dostęp do sieci. Jego zadaniem jest filtrowanie połączeń wchodzących (ochrona przed nieuprawnionym dostępem z zewnątrz) i wychodzących do sieci (ochrona przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz). Rolę zapory może pełnić również komputer wyposażony w system operacyjny, np. Linux z odpowiednim oprogramowaniem.

Urządzenia sieciowe mogą być ze sobą łączone, np. router z przełącznikiem i punktem dostępowym, zintegrowana brama sieciowa zawierająca router, przełącznik, firewall, bramkę VoIP i punkt dostępowy. Przykłady urządzeń sieciowych pokazano na rys. 4.1.

a) b)





c) d)

Rys. 4.1. Przykłady urządzeń sieciowych: a) modem, b) karta sieciowa, c) router z punktem dostępowym, d) bramka VoIP

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jakie urządzenia sieciowe wykorzystywane są w Twojej szkole?
2. Gdzie w Twojej szkole zlokalizowane są poszczególne urządzenia sieciowe?
3. Jakie urządzenia sieciowe wykorzystujesz w domu?

5 Symbole graficzne urządzeń sieciowych

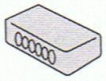
ZAGADNIENIA

- **Jakie symbole urządzeń i łączy stosowane są w schematach sieci?**
- **Jakie programy można wykorzystać do rysowania schematów sieci?**

Sieć komputerowa może składać się z dwóch komputerów połączonych kablem. Z drugiej strony sieć internet składa się z kilku miliardów urządzeń. Aby zilustrować budowę sieci komputerowej, przedstawia się ją w postaci schematów. Pozwala to na ominięcie wielu nieistotnych szczegółów i skupienie się na jej istocie. W naszym przypadku schematy będą najczęściej dotyczyć budowy sieci lokalnej, np. w szkole lub w pracowni.

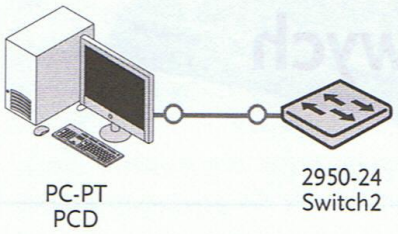
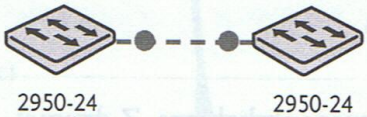
Do sporządzania schematów sieci można wykorzystać wiele programów, np. Microsoft Visio (program komercyjny) lub bezpłatny program Dia (dostępny na stronie http://projects.gnome.org/dia/ w wersji dla systemu Linux i Windows). We wcześniejszym rozdziale omówiono wybrane urządzenia stosowane do budowy sieci. Każdemu z tych urządzeń przypisano symbol graficzny, za pomocą którego jest on reprezentowany w schematach. Wybrane symbole urządzeń używane w schematach zebrano w tabeli 5.1.

Tabela 5.1. Symbole graficzne wybranych urządzeń używane w schematach

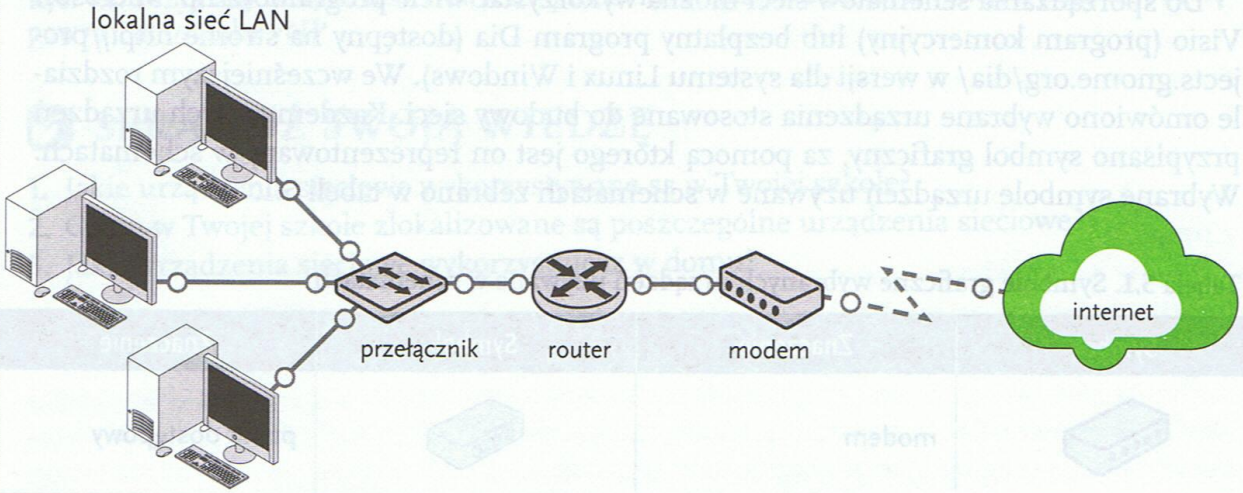
Symbol	Znaczenie	Symbol	Znaczenie
	modem		punkt dostępowy
	koncentrator		router
	most		stacja robocza
	przełącznik		zapora sieciowa

Połączenia pomiędzy urządzeniami mogą być wykonane za pomocą różnych typów łączy. Wybrane symbole łączy używane w schematach zebrano w tabeli 5.2.

Tabela 5.2. Symbole graficzne łączy używane w schematach

Symbol	Znaczenie	Symbol	Znaczenie
	kabel Ethernetowy prosty		kabel szeregowy
	kabel Ethernetowy krosowany		kabel światłowodowy

Przykładowy schemat prostej sieci pokazany jest na rysunku 5.1.



Rys. 5.1. Schemat prostej sieci

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Przy pomocy dowolnego programu narysuj schemat sieci komputerowej w Twojej szkole.

6 Dokumentacja techniczna urządzeń sieciowych

ZAGADNIENIA

- **Jakie informacje powinny być umieszczane w dokumentacji technicznej?**
- **W jakim języku powinna być sporządzona dokumentacja techniczna i kto jest za nią odpowiedzialny?**
- **Jak korzystać z dokumentacji technicznej urządzeń?**

Celem **dokumentacji technicznej** jest dostarczanie informacji dotyczących urządzenia, jego instalowania oraz działania. Dokumentacja techniczna powinna zawierać wszystkie informacje wykazujące zgodność wyrobu z wymaganiami dotyczącymi danego urządzenia. Dokumentacja powinna być sporządzona w jednym z oficjalnych języków Unii Europejskiej, z wyjątkiem instrukcji użytkowania oraz Deklaracji Zgodności, które muszą być dostępne także w języku rynku docelowego.

Odpowiedzialność za wprowadzenie zgodnego z dokumentacją wyrobu do obrotu oraz za dysponowanie dokumentacją techniczną spoczywa na wytwórcy lub importerze danego urządzenia. Dokumentacja techniczna urządzenia jest opracowywana dla każdego urządzenia osobno i powinna zawierać:

- charakterystykę (parametry techniczne),
- rysunek zewnętrzny,
- wykaz wyposażenia normalnego i specjalnego,
- schemat elektryczny,
- schematy funkcjonowania,
- instrukcję obsługi i konserwacji,
- instrukcję BHP,
- wykaz części zamiennych i zapasowych,
- wykaz faktycznie posiadanego wyposażenia,
- wykaz załączonych rysunków.

Odpowiednio opracowana dokumentacja techniczna ułatwia taką konfigurację urządzenia, przy której pracuje ono efektywnie i przy zachowaniu wyższego poziomu bezpieczeństwa podczas jego użytkowania. Producenci urządzeń sieciowych udostępniają na swoich stronach internetowych dodatkowe informacje dotyczące problemów pojawiających się podczas eksploatacji urządzeń, aktualizacje oprogramowania firmowego oraz świadczą pomoc techniczną związaną z eksploatacją urządzeń.

Dokumentację techniczną dostarczoną z urządzeniem należy przechowywać w łatwo dostępnym i bezpiecznym miejscu. W przypadku pojawiających się problemów będzie służyła jako pierwsze źródło informacji o urządzeniu oraz dostarczy informacji o możliwości uzyskania pomocy od producenta lub dostawcy. Przed zainstalowaniem nowego urządzenia w sieci należy sprawdzić w dokumentacji (specyfikacji technicznej):

7 Topologie sieciowe (logiczna i fizyczna)

ZAGADNIENIA

- **Do czego służy topologia sieci?**
- **Jakie są rodzaje topologii?**
- **Jakie są wady i zalety różnych topologii?**

Topologia sieci określa sposób jej wykonania, czyli połączenia urządzeń komputerowych za pomocą medium transmisyjnego. Topologie sieci LAN mogą być opisane zarówno na płaszczyźnie fizycznej, jak i logicznej. **Topologia fizyczna** określa geometryczną organizację sieci lokalnej, graficznie przedstawiając jej kształt i strukturę. **Topologia logiczna** opisuje reguły komunikacji, z których korzystają urządzenia komunikujące się w sieci. Za jej pomocą można opisać, które urządzenia mogą się ze sobą komunikować lub mają wzajemne, bezpośrednie połączenie fizyczne. W lokalnych sieciach komputerowych stosuje się topologie logiczne:

Topologia rozgłaszania – polega na tym, że host wysyła dane do wszystkich hostów podłączonych do medium. Kolejność korzystania z medium określa reguła „kto pierwszy wyśle, ten pierwszy zostanie obsłużony" (*first come, first serve*). Przykładem takiej topologii jest sieć Ethernet.

Topologia przekazywania tokenu (żetonu) – polega na kontrolowaniu dostępu do sieci poprzez przekazywanie elektronicznego tokenu (specjalnej ramki danych). Host, który w danym momencie posiada token, może skorzystać z medium. W przypadku, gdy host nie potrzebuje dostępu do medium, przekazuje token kolejnemu hostowi i cykl się powtarza. Z tej topologii korzystają sieci Token Ring i FDDI.

Podstawowymi topologiami fizycznymi, stosowanymi w budowie lokalnych sieci przewodowych, są:

- magistrala (*bus*),
- pierścień (*ring*),
- gwiazda (*star*).

W rzeczywistych rozwiązaniach sieć komputerowa może być bardziej skomplikowana i tworzyć topologię:

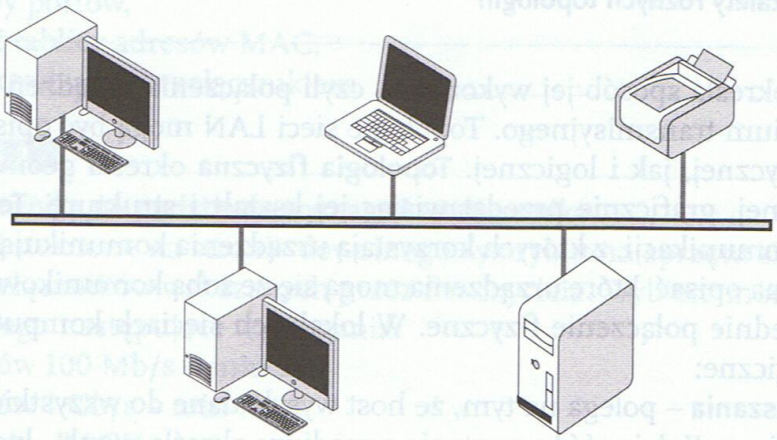
- rozszerzonej gwiazdy,
- siatki pełnej lub niepełnej.

W topologii **magistrali** (rys. 7.1) wszystkie węzły sieci (np. komputery, drukarki sieciowe) są połączone ze sobą za pomocą pojedynczego kabla koncentrycznego, który obsługuje tylko jeden kanał i nosi nazwę magistrali. Węzły są dołączane do wspólnej magistrali za pomocą „trójników", w sposób charakterystyczny dla sieci równorzędnej. Oba końce magistrali muszą być zakończone elementami ograniczającymi, zwanymi **terminatorami**, które chronią przed odbiciami sygnału. Magistrala nie jest obsługiwana przez żadne urządzenia

zewnętrzne, a więc wszystkie urządzenia przyłączone do sieci słuchają transmisji przesyłanych magistralą i odbierają pakiety do nich zaadresowane. Topologia ta była stosowana w małych sieciach.

Zaletami magistrali są: krótkie odcinki kabla użyte do budowy sieci, brak konieczności stosowania dodatkowych urządzeń (koncentratorów, przełączników) i łatwość przyłączenia nowego urządzenia. Wadą magistrali jest trudna lokalizacja uszkodzenia kabla. Możliwa jest tylko jedna transmisja w danym momencie, a awaria kabla może spowodować podział sieci na 2 segmenty lub unieruchomienie całej sieci.

W topologii **pierścienia** (rys. 7.2) każda przyłączona do sieci stacja robocza ma dwa połączenia – po jednym do każdego ze swoich najbliższych sąsiadów. Połączenie takie tworzy fizyczną pętlę, czyli pierścień. Dane są przesyłane wokół pierścienia w jednym kierunku. Każda stacja robocza działa podobnie jak wzmacniak, pobierając



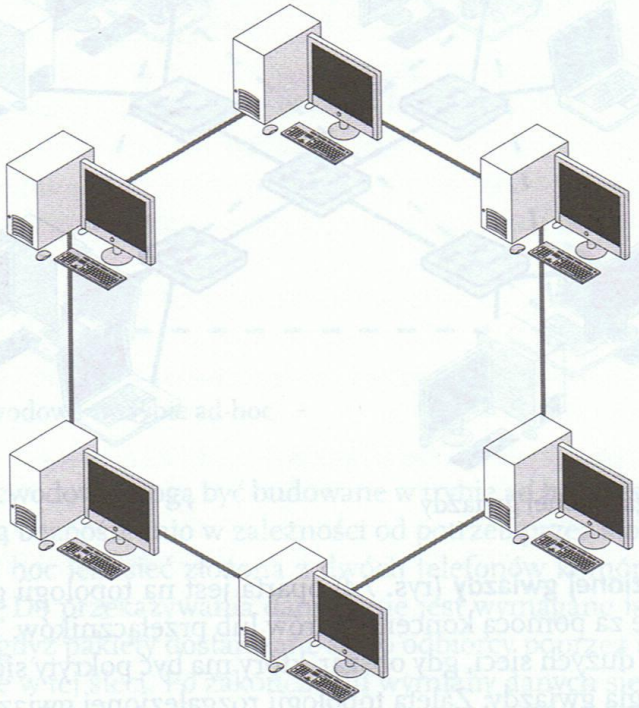
Rys. 7.1. Topologia magistrali

i odpowiadając na pakiety do niej zaadresowane, a także przesyłając pozostałe pakiety do następnej stacji roboczej. Im więcej urządzeń jest przyłączonych do pierścienia, tym czas odpowiedzi jest dłuższy. Czas ten można jednak określić, co nie jest możliwe w przypadku innych topologii.

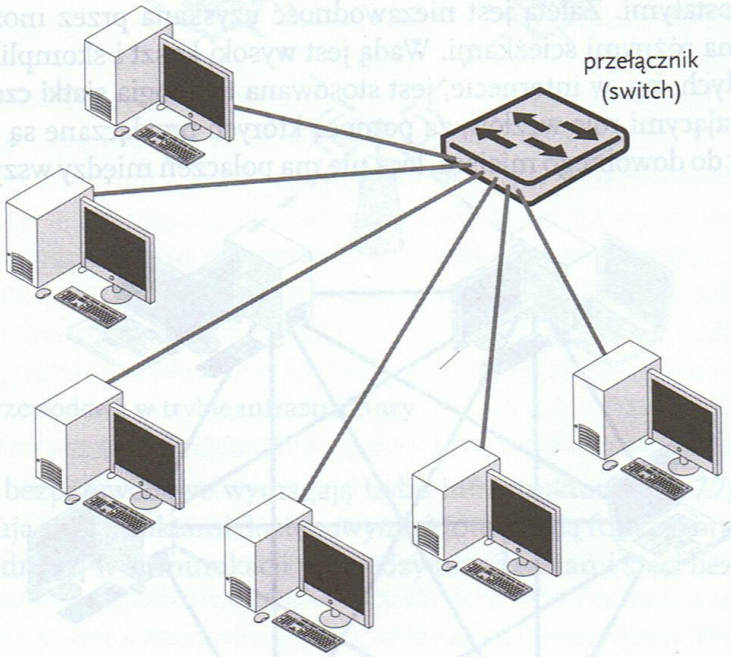
Wadą pierścienia jest to, że awaria pojedynczego przewodu lub komputera powoduje problemy z działaniem sieci. Problemy te można jednak rozwiązać stosując podwójny pierścień lub układy obejściowe.

W topologii **gwiazdy** (rys. 7.3) połączenia sieci rozchodzą się z centralnego punktu, którym może być koncentrator lub przełącznik. Każde urządzenie przyłączone do sieci może uzyskiwać dostęp do współdzielonego nośnika. Zaletami topologii gwiazdy jest duża przepustowość i łatwa lokalizacja uszkodzeń. W przypadku awarii łącza lub komputera pozostała część sieci pracuje bez zakłóceń. Wadą jest większe zapotrzebowanie na kable oraz konieczność stosowania koncentratorów lub przełączników, których awaria może unieruchomić całą sieć. Topologia gwiazdy dominuje we współczesnych sieciach LAN. Są one elastyczne, skalowalne[1] i stosunkowo tanie.

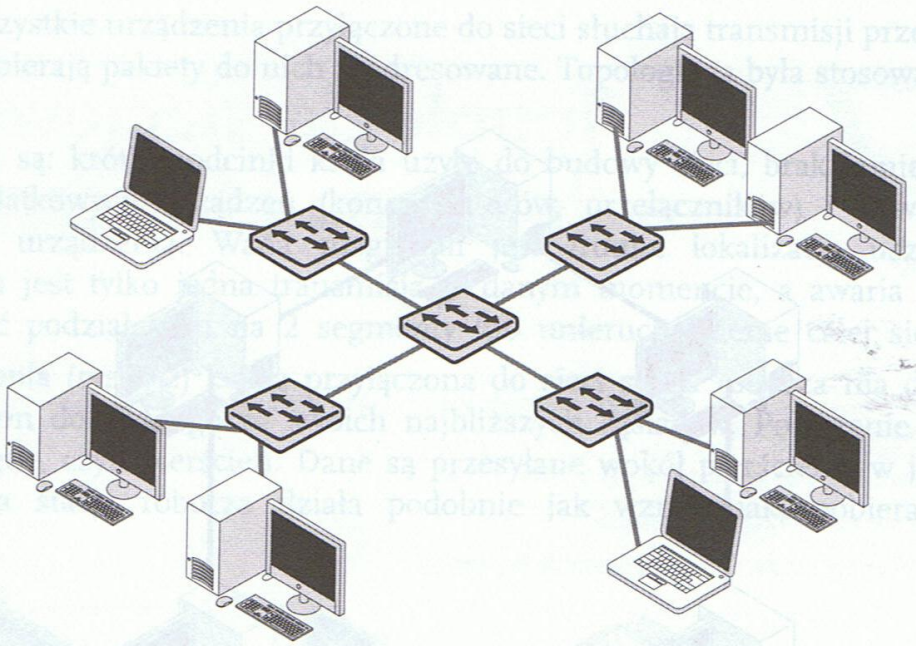
[1] Skalowalność (scalability) jest cechą określającą zdolność do dalszej rozbudowy sieci. Oznacza zapewnienie wydajnej pracy sieci komputerowej przy zwiększaniu liczby jej elementów składowych.



Rys. 7.2. Topologia pierścienia



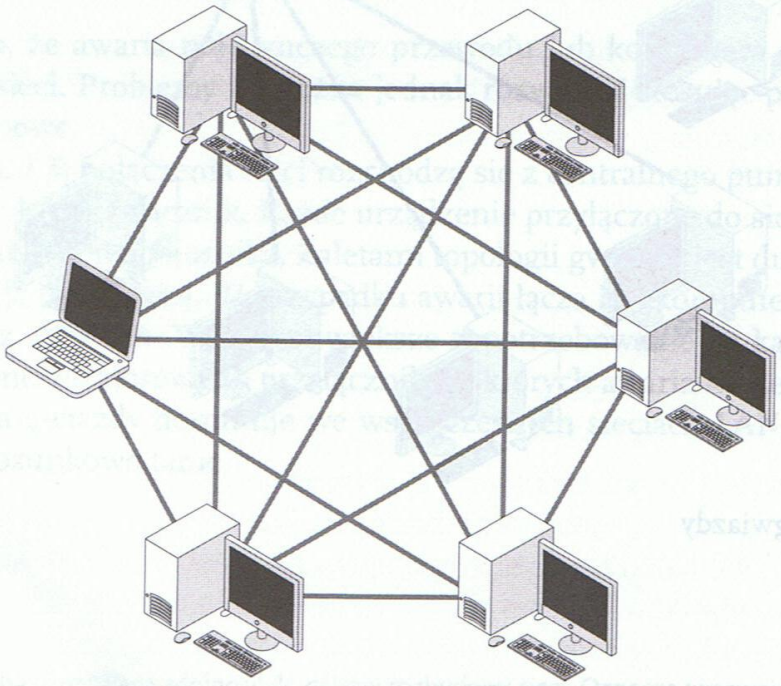
Rys. 7.3. Topologia gwiazdy



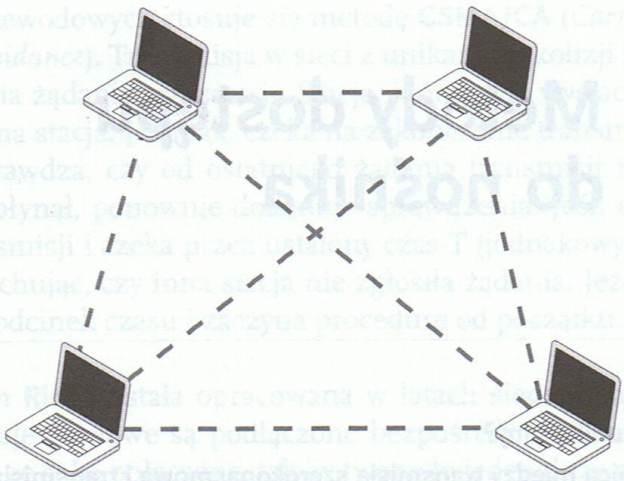
Rys. 7.4. Topologia rozgałęzionej gwiazdy

Topologia **rozgałęzionej gwiazdy** (rys. 7.4) oparta jest na topologii gwiazdy. Pojedyncze gwiazdy są połączone za pomocą koncentratorów lub przełączników. Topologia ta jest stosowana w przypadku dużych sieci, gdy obszar, który ma być pokryty siecią, jest większy niż pozwala na to topologia gwiazdy. Zaletą topologii rozgałęzionej gwiazdy jest ograniczenie liczby urządzeń, które muszą być połączone z centralnym węzłem oraz możliwość ograniczenia ruchu lokalnego do pojedynczej gwiazdy.

Topologia **siatki** (rys. 7.5) jest używana wtedy, gdy każdy węzeł ma własne połączenia z wszystkimi pozostałymi. Zaletą jest niezawodność uzyskana przez możliwość przesyłania danych wieloma różnymi ścieżkami. Wadą jest wysoki koszt i skomplikowana budowa. W sieciach rozległych, np. w internecie, jest stosowana topologia **siatki częściowej.** Między routerami odgrywającymi rolę węzłów, za pomocą których przyłączane są sieci lokalne, istnieje wiele ścieżek do dowolnego miejsca, lecz nie ma połączeń między wszystkimi węzłami.

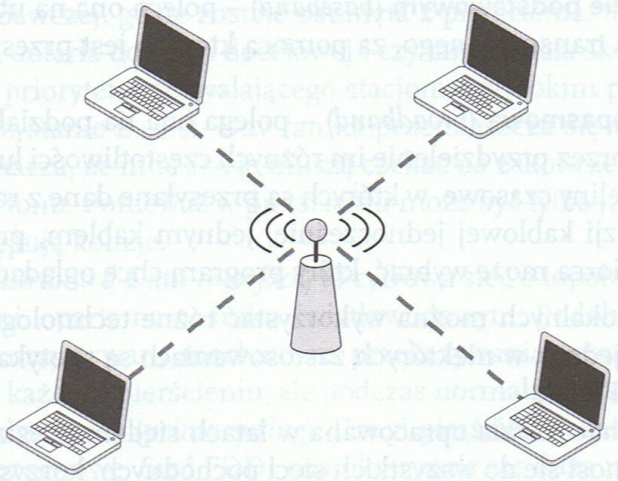


Rys. 7.5. Topologia siatki



Rys. 7.6. Sieć bezprzewodowa w trybie ad-hoc

Małe sieci bezprzewodowe mogą być budowane w trybie **ad hoc** (rys. 7.6). Urządzenia komunikują się ze sobą bezpośrednio w zależności od potrzeb przez stosunkowo krótki czas. Przykładem sieci ad hoc jest sieć złożona z dwóch telefonów komórkowych połączonych dla przesłania pliku. Do przekazywania danych nie jest wymagane istnienie żadnej infrastruktury sieciowej, gdyż pakiety dostarczane są do odbiorcy poprzez inne, dowolnie zlokalizowane, urządzenie w tej sieci. Po zakończeniu wymiany danych sieć jest demontowana.



Rys. 7.7. Sieć bezprzewodowa w trybie infrastruktury

Większe sieci bezprzewodowe wymagają trybu **infrastruktury** (rys. 7.7). Wszystkie urządzenia komunikują się z punktami dostępowymi, które pełnią funkcję bramy (do sieci przewodowej) i pośredniczą w komunikacji pomiędzy urządzeniami sieci bezprzewodowej.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jaka topologia fizyczna jest stosowana w Twojej szkole?
2. Którą ze strategii znanych z algorytmiki zastosowałbyś do lokalizacji miejsca awarii w topologii magistrali? Opisz, jak ta zasada będzie realizowana w lokalizowaniu awarii.

8 Metody dostępu do nośnika

ZAGADNIENIA

- **Czym jest kanał komunikacyjny?**
- **Na czym polega różnica między transmisją szerokopasmową i transmisją w paśmie podstawowym?**
- **W jaki sposób kontrolowany jest dostęp urządzeń do nośnika danych?**

Urządzenia w sieci są połączone za pomocą łączy. Dane między urządzeniami są przesyłane za pomocą kanałów. **Kanał** może być rozumiany jako pojedyncze połączenie między dwoma urządzeniami. W łączu może być wydzielony jeden kanał transmisyjny lub wiele kanałów, z których każdy wykorzystuje część tego łącza. W zależności od sposobu wykorzystania łączy możemy wyróżnić:

- **transmisję w paśmie podstawowym** (*baseband*) – polega ona na utworzeniu w łączu tylko jednego kanału transmisyjnego, za pomocą którego jest przesyłany tylko jeden ciąg sygnałów,
- **transmisję szerokopasmową** (*broadband*) – polega ona na podziale pojedynczego łącza na wiele kanałów przez przydzielenie im różnych częstotliwości lub przez podział czasu transmisji na szczeliny czasowe, w których są przesyłane dane z różnych kanałów. Przykładowo, w telewizji kablowej jednocześnie, jednym kablem, przesyłanych jest wiele programów, a odbiorca może wybrać, który program chce oglądać.

Do budowy sieci lokalnych można wykorzystać różne technologie. Najpopularniejszą z nich jest Ethernet, jednak w niektórych zastosowaniach są spotykane również technologie Token Ring oraz FDDI.

Technologia **Ethernet** została opracowana w latach siedemdziesiątych w firmie Xerox. Obecnie nazwa ta odnosi się do wszystkich sieci pochodnych, korzystających z dostępu do nośnika metodą **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*). W metodzie tej urządzenia **rywalizują** ze sobą o dostęp do nośnika. Stacja zamierzająca transmitować dane może uzyskać dostęp do niego w dowolnej chwili. Przed wysłaniem danych stacja nasłuchuje, czy w sieci odbywa się ruch. Jeżeli go wykryje, to czeka do momentu, kiedy nośnik będzie wolny. Jeżeli dwie stacje nadają w tym samym czasie, następuje kolizja i obie transmisje muszą zostać powtórzone. Zjawisko kolizji jest niekorzystne, ponieważ powoduje zmniejszenie wydajności sieci, ale jego występowanie w sieci jest naturalne i niewielka liczba kolizji nie powinna być powodem do niepokoju. Po wykryciu kolizji stacja nadaje jeszcze przez określony czas specjalny sygnał wymuszania kolizji, aby poinformować wszystkie inne urządzenia o jej wystąpieniu. Następnie przed ponowieniem próby transmisji odczekuje losowo wybrany czas, co zabezpiecza sieć przed sytuacją, gdy stacje ponawiałyby swe próby w takich samych odstępach czasu, powodując powstawanie kolejnych kolizji.

W sieciach bezprzewodowych stosuje się metodę **CSMA/CA** (*Carrier Sense Multiple Access with Collision Avoidance*). Transmisja w sieci z unikaniem kolizji może być zrealizowana poprzez zgłoszenia żądania transmisji. Stacja, która chce wysłać dane, sprawdza, czy w sieci nadaje już inna stacja. Jeśli tak, czeka na zakończenie transmisji. Jeśli nie wykryła innej transmisji, sprawdza, czy od ostatniego żądania transmisji minął określony czas T. Jeśli czas T nie upłynął, ponownie dokonuje sprawdzenia. Jeśli upłynął czas T, stacja zgłasza żądanie transmisji i czeka przez ustalony czas T (jednakowy dla wszystkich stacji w danej sieci), nasłuchując, czy inna stacja nie zgłosiła żądania. Jeżeli stwierdzi inne żądanie, czeka losowy odcinek czasu i zaczyna procedurę od początku. W innym przypadku zaczyna nadawać.

Technologia **Token Ring** została opracowana w latach siedemdziesiątych przez firmę IBM. W sieci tej stacje sieciowe są podłączone bezpośrednio do urządzeń MAU (*Multi Access Unit*), które są ze sobą połączone, tak by tworzyły jeden duży pierścień. Token Ring stosuje metodę dostępu do nośnika, nazywaną **przekazywaniem żetonu** (*Token-Passing*). W pierścieniu krąży specjalna ramka – **żeton** *(token)*. Stacja sieciowa uzyskuje prawo do transmisji danych tylko wtedy, gdy posiada żeton. Jeżeli stacja sieciowa posiada żeton, ale nie jest gotowa do wysyłania danych, to przesyła żeton do następnej w kolejności stacji sieciowej. Stacja może przetrzymać żeton tylko przez określony czas, po którym musi przekazać go stacji następnej w pierścieniu. Stacja posiadająca żeton przekształca go w ramkę, dodając dane przeznaczone do przesłania, i wysyła ją do następnej stacji w pierścieniu. Ramka informacyjna, po osiągnięciu stacji docelowej, jest przez nią kopiowana w celu dalszego wykorzystania. Ramka kontynuuje wędrówkę w pierścieniu aż do momentu osiągnięcia ramki nadawczej, gdzie zostaje usunięta z pierścienia. Stacja nadawcza może sprawdzić, czy ramka dotarła do stacji docelowej i czy tam została skopiowana. Sieć Token Ring używa systemu priorytetu, zezwalającego stacjom o wysokim priorytecie, np. serwerom, na częstsze korzystanie z sieci. Gdy ramka przemieszcza się w pierścieniu, w sieci nie ma żetonu, co oznacza, że inne stacje muszą czekać na zakończenie transmisji i wygenerowanie nowego żetonu. Ponieważ w pierścieniu może być tylko jeden żeton, w sieciach Token Ring nie występują kolizje.

Sieć **FDDI** (*Fiber Distributed Data Interface*) to cyfrowa sieć o topologii podwójnych przeciwbieżnych pierścieni, oparta na nośniku światłowodowym. Podobnie jak w sieci Token Ring, jest w niej wykorzystywany mechanizm przekazywania żetonu. Informacje mogą być transmitowane w każdym pierścieniu, ale podczas normalnej pracy jest wykorzystywany tylko pierścień podstawowy (*primary ring*). Drugi pierścień dodatkowy (*secondary ring*) stanowi połączenie rezerwowe. Sieć FDDI charakteryzuje się dużą niezawodnością pracy. W razie awarii stacji lub uszkodzenia światłowodu pierścień jest automatycznie zamykany przy wykorzystaniu pierścienia dodatkowego, tak aby sygnał ze stacji poprzedniej przechodził bezpośrednio do stacji następnej.

Metoda dostępu na zasadzie **priorytetu żądań** wykorzystywana jest w sieciach opartych na specyfikacji IEEE 802.12, np. w sieci VG-AnyLAN opracowanej przez Hewlett-Packard. W metodzie tej centralny koncentrator (wzmacniak) kolejno sprawdza stan portów do niego przyłączonych w celu określenia, które z nich zgłaszają żądania transmisji. Po otrzymaniu zgłoszenia koncentrator określa jego priorytet. Procesy, które muszą być obsłużone w określonym czasie otrzymują priorytet wysoki i są uprzywilejowane w stosunku do zwykłych procesów (z priorytetem normalnym). Każdy port, który nie przeprowadza transmisji, przesyła sygnał nośny (informację, że jest wolny). Koncentrator identyfikuje stację następną w kolejce do przeprowadzenia transmisji i nakazuje jej zaprzestanie wysyłania sygnału nośnego, po czym port może rozpocząć transmisję. Koncentrator informuje

pozostałe stacje, że mogą otrzymać wiadomość przychodzącą. Stacja nie może wykonywać dwóch kolejnych transmisji, jeśli żądania transmisji innych stacji mają taki sam priorytet. Aby zapewnić, że żadne z żądań nie będzie zawsze ignorowane, żądania o priorytecie normalnym, które oczekują dłużej niż 250 ms, otrzymują priorytet wysoki.

W sieciach **przełączanych** dostęp do sieci realizowany jest za pomocą przełączników. Przełącznik jest wieloportowym urządzeniem, które uczy się adresów urządzeń i zapamiętuje je w wewnętrznej tabeli. Następnie tworzy między nadawcą i odbiorcą tymczasowe ścieżki przełączane, którymi przesyłane są dane. W protokołach wykorzystujących mechanizm rywalizacji przełączanie portu zmniejsza rozmiar domeny kolizji do dwóch urządzeń - przełączanego portu oraz urządzenia przyłączonego do tego portu. Pozwala to na zwiększenie wydajności sieci.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Podaj przykłady wykorzystania transmisji szerokopasmowej.
2. Opisz, co zrobić, aby zmniejszyć liczbę kolizji w sieci.

9 Rodzaje środowisk sieciowych (architektura równorzędna i klient-serwer)

ZAGADNIENIA

- **Jaka jest różnica między architekturą równorzędną i klient-serwer?**
- **Czym charakteryzuje się architektura równorzędna i klient-serwer?**

Jednym z podstawowych celów tworzenia sieci komputerowych jest współdzielenie zasobów, takich jak pliki lub drukarki. Każdy z takich zasobów musi być **udostępniony**, to znaczy jego właściciel musi wyrazić zgodę na korzystanie z niego przez innych użytkowników. Komputer, który udostępnia zasoby lub usługi w sieci nazywany jest **serwerem**.

Komputer – lub inne urządzenie korzystające z zasobów udostępnianych przez serwer – będzie nazywany **klientem**. W zależności od tego, jak będzie zorganizowane udostępnianie i korzystanie z udostępnionych zasobów w sieci, możemy mówić o architekturze sieci równorzędnej lub opartej na serwerach. W architekturze **równorzędnej** (*peer-to-peer*) każdy użytkownik może jednocześnie udostępniać zasoby swojego komputera oraz korzystać z zasobów innych komputerów. Wszystkie urządzenia w sieci mają taki sam status – żadne z nich nie jest podporządkowane innemu. Użytkownik sam zarządza swoim komputerem i dba o dostęp innych użytkowników do swoich zasobów. Rozwiązanie to jest stosowane w małych sieciach (do dziesięciu komputerów). Wszystkie informacje o udostępnionych zasobach i użytkownikach uprawnionych do ich wykorzystania są zapisane na komputerze udostępniającym dany zasób. Jeżeli korzystamy z wielu serwerów, na których jest zapisana lokalnie informacja o zasobach, to na każdym z nich musimy uzyskać prawo do korzystania z zasobów, co oznacza wpisywanie hasła na każdym serwerze. Sieć taka jest tania w budowie, lecz trudna w utrzymaniu i zarządzaniu. Może być zbudowana na podstawie systemów Windows i innych, np. Linux. W architekturze **klient-serwer** (*client-server*) istnieje jeden lub więcej komputerów spełniających tylko funkcję serwera. Na serwerze jest zainstalowany sieciowy system operacyjny, umożliwiający realizację zadań serwera.

Serwer przechowuje i udostępnia zasoby, np. w postaci plików, zarządza współdzieleniem drukarek oraz przechowuje wspólnie wykorzystywaną bazę danych o zasobach sieci, jej użytkownikach oraz uprawnieniach użytkowników do zasobów. Stacja robocza, pełniąca funkcję klienta, komunikuje się z serwerem, korzystając z oprogramowania klienta sieci. Przykładem sieci klient-serwer jest sieć Novell NetWare lub sieć zbudowana na podstawie systemów Windows Server.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Podaj przykłady systemów operacyjnych, które instalowane są na serwerach i klientach.
2. Jaki typ sieci zainstalowałbyś w swojej szkole? Uzasadnij wybór.
3. Gdzie i dlaczego używane są sieci równorzędne?

10 Komunikacja w sieci

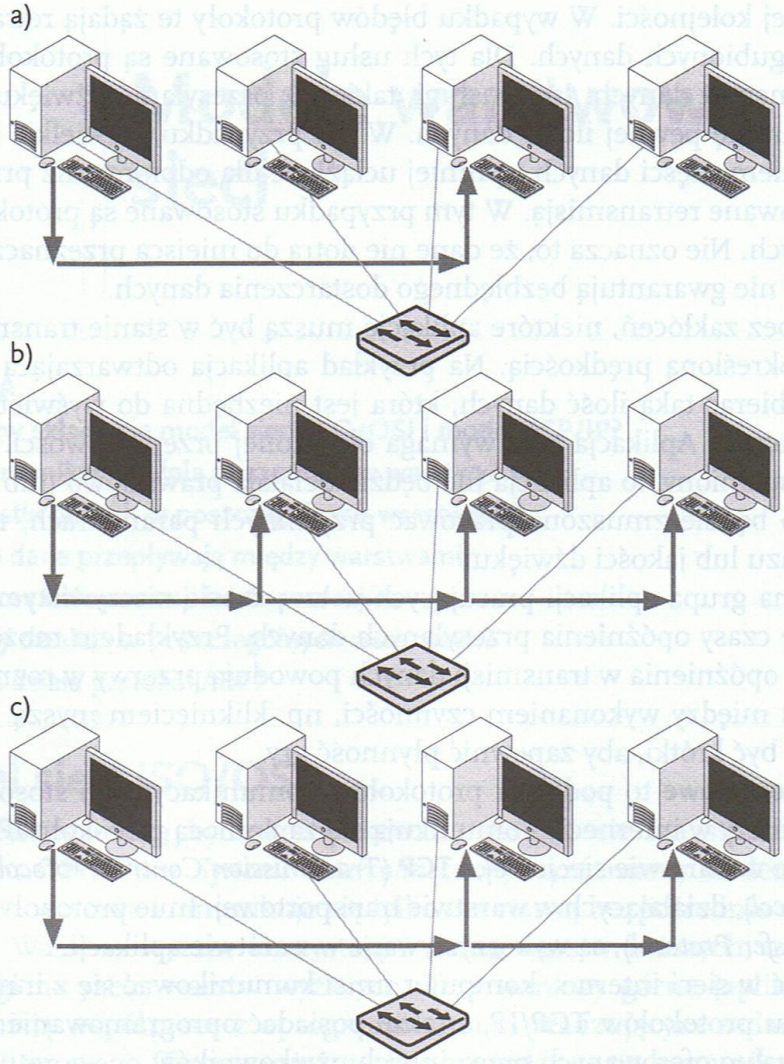
ZAGADNIENIA

- **Czym jest protokół komunikacyjny?**
- **Na czym polega transmisja danych w trybie połączeniowym i bezpołączeniowym?**
- **Jakie są rodzaje transmisji?**
- **Na czym polega transmisja jednokierunkowa, w trybie półdupleksu i pełnego dupleksu?**
- **Na czym polegają wymagania aplikacji dotyczące przepustowości łącza?**

Użytkownicy i urządzenia w sieci komputerowej komunikują się ze sobą i wymieniają informacje. Wymiana informacji musi przebiegać w ściśle określony sposób, umożliwiający przesyłanie danych. Każde z komunikujących się urządzeń musi przestrzegać pewnych ustalonych zasad i reguł postępowania. Zbiór zasad i norm, których muszą przestrzegać komunikujące się ze sobą urządzenia, jest nazywany **protokołem komunikacyjnym**. Komunikacja między urządzeniami może przebiegać w trybie połączeniowym (*connection oriented*) lub **bezpołączeniowym** (*connectionless oriented*).

Tryb połączeniowy polega na ustanowieniu logicznego połączenia pomiędzy dwoma komunikującymi się ze sobą urządzeniami. Aby rozpocząć komunikację, należy najpierw nawiązać połączenie. Z trybu połączeniowego korzysta się wtedy, gdy powstaje potrzeba przesyłania wielu komunikatów w obu kierunkach, np. podczas korzystania z usługi telnet. W **trybie bezpołączeniowym** komunikaty przekazywane są niezależnie, np. przy przekazywaniu wiadomości za pomocą poczty elektronicznej. W komunikacji biorą udział przynajmniej dwa urządzenia. Jeżeli jedno urządzenie wysyła dane do dokładnie jednego urządzenia, to taki tryb transmisji nazywamy **jednostkowym** (*unicast*). W sieciach rozwiązane to jest w ten sposób, że każde urządzenie posiada swój unikatowy adres. Dane wysyłane przez nadawcę docierają do wielu urządzeń, ale odbierane są tylko przez to urządzenie, którego adres jest adresem docelowym (pozostałe urządzenia ignorują dane, które nie są przeznaczone dla nich). Urządzenie nadawcze może wysłać informację do wszystkich dostępnych urządzeń. W takim przypadku adresem docelowym jest specjalny adres, nazywany **rozgłoszeniowym** (*broadcast*). Urządzenia traktują transmisje na adres rozgłoszeniowy tak, jakby były adresowane na ich adres jednostkowy. W rozgłaszaniu **grupowym** (*multicast*) dane przeznaczone są tylko dla wybranej grupy urządzeń. Adres docelowy jest specjalnym adresem, określającym wybrane urządzenia z danej sieci. W transmisji grupowej unika się wielokrotnego wysyłania tego samego komunikatu do wielu nadawców, po każdym łączu sieciowym informacja jest przekazywana jednokrotnie.

Transmisja **jednokierunkowa** (*simplex*) to transmisja, w której odbiornik nie może przesłać odpowiedzi ani innych danych. Przykładem tego typu transmisji jest emisja audycji radiowych, gdzie słuchacz przy odbiorniku radiowym może tylko odbierać informacje pochodzące z nadajnika. Tego typu transmisje nie są stosowane w sieciach komputerowych.



Rys. 10.1. Typy transmisji: a) jednostkowa, b) rozgłoszeniowa, c) grupowa

Półdupleks (*half-duplex*) to transmisja dwukierunkowa, naprzemienna. W danym momencie jest ustalony tylko jeden kierunek transmisji, a urządzenie może albo nadawać, albo odbierać informacje. Do odwrócenia kierunku transmisji jest potrzebny system sygnalizacji, wskazujący, że urządzenie ukończyło nadawanie i może odbierać informacje. Przykładem podobnych transmisji spoza obszaru sieci komputerowych jest amatorska stacja krótkofalowa lub radio CB.

Dupleks (*full-duplex*) to transmisja jednoczesna i dwukierunkowa. Wymaga zazwyczaj dwóch par przewodów dla sieci cyfrowych. Dla połączeń analogowych dla jednej pary przewodów szerokość pasma jest dzielona na dwie części. Przykładem podobnych transmisji spoza obszaru sieci komputerowych jest rozmowa telefoniczna.

Aby usługi i aplikacje sieciowe mogły prawidłowo działać, muszą mieć zapewnione odpowiednie warunki. Najważniejszymi warunkami są:

- niezawodność przesyłania danych,
- przepustowość łączy,
- czas odpowiedzi.

Niektóre usługi sieciowe, takie jak poczta elektroniczna, transfer plików, pobieranie stron internetowych itp., wymagają niezawodnego przesyłania danych. Nadawca i odbiorca komunikują się między sobą, aby się upewnić, że wszystkie dane dotarły bez błędów

i w odpowiedniej kolejności. W wypadku błędów protokoły te żądają retransmisji uszkodzonych lub zagubionych danych. Dla tych usług stosowane są protokoły zapewniające niezawodny transport danych. Inne usługi, takie jak przesyłanie dźwięku lub obrazu na żywo, tolerują utratę pewnej ilości danych. W ich przypadku niewielkie zakłócenia spowodowane brakiem części danych są mniej uciążliwe dla odbiorcy niż przerwy w odtwarzaniu spowodowane retransmisją. W tym przypadku stosowane są protokoły zawodnego transportu danych. Nie oznacza to, że dane nie dotrą do miejsca przeznaczenia, lecz tylko to, że protokoły nie gwarantują bezbłędnego dostarczenia danych.

Aby działać bez zakłóceń, niektóre aplikacje muszą być w stanie transmitować lub odbierać dane z określoną prędkością. Na przykład aplikacja odtwarzająca pliki multimedialne musi odbierać taką ilość danych, która jest niezbędna do wyświetlania filmu lub odtwarzania muzyki. Aplikacja taka wymaga określonej przepustowości. Jeżeli warunek ten nie będzie spełniony, to aplikacja nie będzie działała prawidłowo (lub w ogóle się nie uruchomi) albo będzie zmuszona pracować przy innych parametrach, np. niższej rozdzielczości obrazu lub jakości dźwięku.

Istnieje pewna grupa aplikacji pracujących w tzw. **czasie rzeczywistym,** które dopuszczają niewielkie czasy opóźnienia przesyłanych danych. Przykładem może być telekonferencja, w której opóźnienia w transmisji danych powodują przerwy w rozmowie. W grach sieciowych czas między wykonaniem czynności, np. kliknięciem myszą, a reakcją na to zdarzenie musi być krótki, aby zapewnić płynność gry.

Protokoły internetowe to podzbiór protokołów komunikacyjnych stosowanych w sieci internet. Komputery w internecie komunikują się za pomocą protokołu **IP** (*Internet Protocol*), działającego w warstwie sieciowej, i **TCP** (*Transmission Control Protocol*) lub **UDP** (*User Datagram Protocol*), działających w warstwie transportowej. Inne protokoły, takie jak **HTTP** (*Hypertext Transfer Protocol*), są wykorzystywane w warstwie aplikacji.

Aby pracować w sieci internet, komputer musi komunikować się z innymi systemami za pomocą stosu protokołów TCP/IP, a także posiadać oprogramowanie pozwalające na wykorzystanie usług oferowanych przez innych użytkowników.

Dane przesyłane w sieci internet są dzielone na pakiety. Każdy pakiet jest opatrzony nagłówkiem IP, zawierającym między innymi adresy nadawcy i odbiorcy. Na podstawie tych informacji routery podejmują decyzję, jaką drogą dany pakiet powinien być dostarczony do miejsca przeznaczenia. Protokół IP nie posiada możliwości sprawdzenia, czy pakiet dotarł do miejsca przeznaczenia. W tym celu jest używany protokół TCP. Do każdego pakietu dołącza on swój nagłówek, w którym między innymi numeruje wszystkie wychodzące pakiety. Jeżeli nie otrzyma od adresata potwierdzenia otrzymania pakietu, wysyła go ponownie. W nagłówku TCP znajduje się również numer portu, który identyfikuje usługę w sieci, dla której jest przeznaczony pakiet, np. port 80 jest zarezerwowany dla WWW.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Podaj nazwy znanych Ci protokołów komunikacyjnych.
2. Podaj przykłady aplikacji, które wymagają zapewnienia minimalnej przepustowości łącza.

Zadaniem czterech najniższych warstw jest transmisja danych. Zajmują się odnajdywaniem odpowiedniej drogi do miejsca przekazania konkretnej informacji. Dzielą dane na odpowiednie dla danej warstwy **jednostki danych** PDU (*Protocol Data Unit*). Dodatkowo mogą zapewniać weryfikację bezbłędności przesyłanych danych. Warstwy dolne to warstwa transportowa, sieciowa, łącza danych oraz fizyczna. Warstwa **transportowa** przesyła wiadomość kanałem stworzonym przez warstwę sieciową. W tym celu dzieli dane otrzymane z warstwy sesji na **segmenty**, które są kolejno wysyłane do stacji docelowej. Zapewnia właściwą kolejność otrzymanych segmentów, a w razie zaginięcia lub uszkodzenia segmentu może zażądać jego retransmisji. Stacja docelowa może również wysyłać potwierdzenie odebrania segmentu.

Warstwa **sieciowa**, jako jedyna, dysponuje wiedzą dotyczącą fizycznej topologii sieci. Rozpoznaje, jakie trasy łączą poszczególne komputery oraz sieci i na tej podstawie decyduje, którą z nich wybrać. Jednostką danych w tej warstwie jest **pakiet.** Warstwa ta odpowiada za adresowanie logiczne węzłów sieci (np. adresy IP).

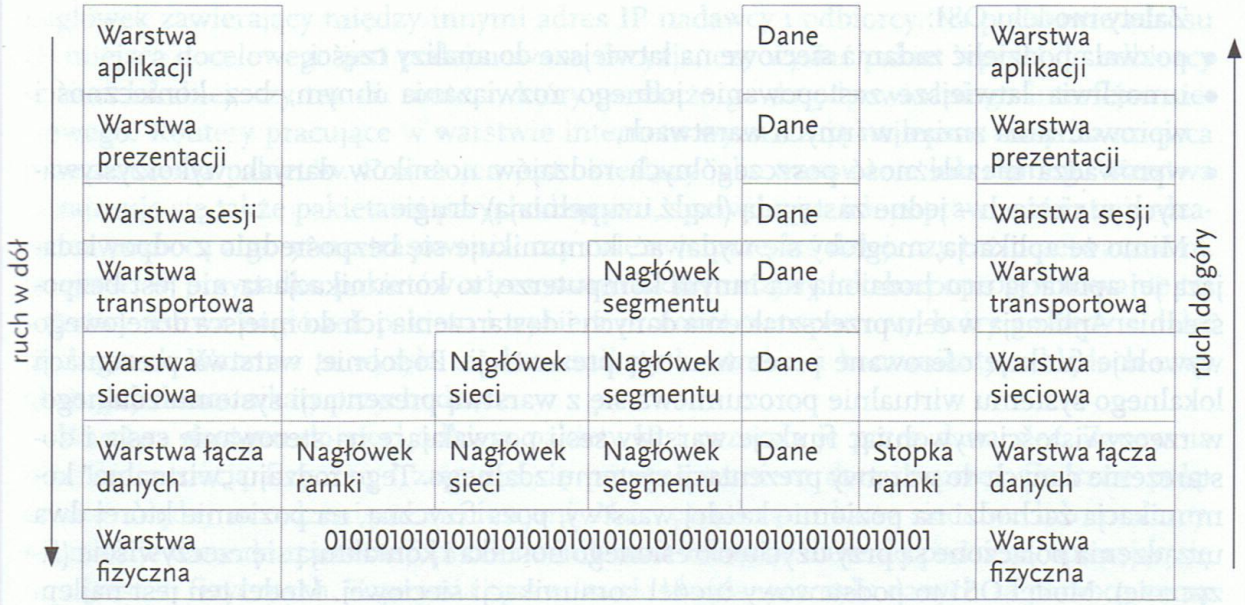
Warstwa **łącza danych** nadzoruje warstwę fizyczną i steruje fizyczną wymianą bitów. Ma możliwość zmiany parametrów pracy warstwy fizycznej tak, aby obniżyć liczbę pojawiających się podczas przekazu błędów. Definiuje mechanizmy **kontroli błędów** CRC (*Cycling Redundancy Check*) i zapewnia dostarczanie ramek informacji do odpowiednich węzłów sieci na podstawie fizycznego adresu MAC karty sieciowej. Jednostką danych w tej warstwie jest **ramka**. Warstwa łącza danych dzieli się na dwie podwarstwy:

- LLC (*Logical Link Control*) – podwarstwa sterowania łączem danych – kontroluje poprawność transmisji i obsługuje tworzenie ramek. Współpracuje przede wszystkim z warstwą sieciową.
- MAC (*Media Access Control*) – podwarstwa sterowania dostępem do nośnika – zapewnia dostęp do nośnika sieci lokalnej i współpracuje przede wszystkim z warstwą fizyczną.

Warstwa **fizyczna** jest odpowiedzialna za przesyłanie strumieni bitów bez kontroli ruchu i bez uwzględnienia rodzaju informacji. Określa ona wszystkie składniki sieci niezbędne do obsługi elektrycznego, optycznego oraz radiowego wysyłania i odbierania sygnałów. Ustala sposób przesyłania bitów i odległości przerw między nimi.

11.2. Przepływ danych między warstwami

Aplikacje użytkownika działają w warstwie aplikacji, generując strumień danych, który jest przesyłany do niższych warstw modelu OSI. W warstwie transportowej zostaje on podzielony na segmenty, każdy z segmentów posiada **nagłówek** warstwy czwartej, który zostaje nadany przez tę właśnie warstwę. W nagłówku jest umieszczany między innymi numer sekwencyjny, potrzebny do ustalenia kolejności przesyłania danych. Warstwa sieciowa odpowiedzialna jest za podzielenie danych na pakiety i opatrzenie każdego pakietu nagłówkiem. W nagłówku pakietu jest umieszczany między innymi adres IP nadawcy i odbiorcy. Adres IP odbiorcy jest wykorzystywany przez router do ustalenia optymalnej trasy, po której pakiet będzie przesłany. Pakiet przesyłany jest do warstwy łącza danych i dzielony na ramki. Każda z ramek posiada nagłówek zawierający między innymi adresy MAC nadawcy i odbiorcy oraz stopkę zawierającą pole kontroli parzystości CRC. Warstwa fizyczna zamienia dane na ciąg bitów i przesyła je za pośrednictwem medium transmisyjnego. Proces podziału strumienia danych na jednostki danych i opatrywania ich nagłówkami nazywamy **enkapsulacją** (*encapsulation*). Proces odwrotny, realizowany podczas odbierania informacji i przesyłania danych do górnych warstw, nazywamy **dekapsulacją** (*decapsulation*). Przepływ danych między warstwami modelu OSI jest pokazany na rysunku 11.1.



Rys. 11.1. Przepływ danych między warstwami modelu OSI

Warstwa aplikacji			
Warstwa prezentacji			
Warstwa sesji			
Warstwa transportowa			
Warstwa sieciowa	Warstwa sieciowa		
Warstwa łącza danych	Warstwa łącza danych	Warstwa łącza danych	
Warstwa fizyczna	Warstwa fizyczna	Warstwa fizyczna	Warstwa fizyczna
Brama	Router	Przełącznik, most, karta sieciowa	Koncentrator, regenerator

Rys. 11.2. Zasięg danych w urządzeniach

Dane, przechodząc przez różne urządzenia sieciowe, dochodzą do różnych warstw modelu OSI. Zasięg danych w urządzeniu przedstawiono na rysunku 11.2.

W zależności od zasięgu danych analizowanych przez urządzenia możemy zaklasyfikować je do poszczególnych warstw, np. router będzie urządzeniem warstwy 3, przełącznik, most i karta sieciowa są urządzeniami warstwy 2.

Uwaga:

W ofercie różnych producentów można spotkać również **przełączniki warstwy trzeciej** – przełączniki rutujące (*switch layer 3, routing switch*). Są to urządzenia, które podobnie jak router, przekazują pakiety, ale przy użyciu dedykowanych układów scalonych **ASIC** (*Application Specific Integrated Circuit*). W routerach przełączanie pakietów odbywa się programowo, z wykorzystaniem mikroprocesora. Przełącznik warstwy trzeciej jest zazwyczaj szybszy w działaniu niż router, ale nie posiada wszystkich funkcji routera i ma mniejsze możliwości konfiguracji.

Zalety modelu OSI:

- pozwala podzielić zadania sieciowe na łatwiejsze do analizy części,
- umożliwia łatwiejsze zastępowanie jednego rozwiązania innym, bez konieczności wprowadzania zmian w innych warstwach,
- wprowadza niezależność poszczególnych rodzajów nośników danych wykorzystywanych w sieciach – jedne zastępują (bądź uzupełniają) drugie.

Mimo że aplikacja, mogłoby się wydawać, komunikuje się bezpośrednio z odpowiadającą jej aplikacją uruchomioną na innym komputerze, to komunikacja ta nie jest bezpośrednia. Aplikacja w celu przekształcenia danych i dostarczenia ich do miejsca docelowego wywołuje funkcje oferowane przez warstwę prezentacji. Podobnie, warstwa prezentacji lokalnego systemu wirtualnie porozumiewa się z warstwą prezentacji systemu zdalnego, w rzeczywistości wywołując funkcje warstwy sesji pozwalające na sterowanie sesją i dostarczenie danych do warstwy prezentacji systemu zdalnego. Tego rodzaju „wirtualna" komunikacja zachodzi na poziomie każdej warstwy, poza fizyczną, na poziomie której dwa urządzenia połączone są przy użyciu określonego nośnika i kontaktują się rzeczywiście (fizycznie). Model OSI to podstawowy model komunikacji sieciowej. Model ten jest najlepszym narzędziem służącym do nauki wysyłania i odbierania danych w sieci. Pozwala on obserwować funkcje poszczególnych warstw sieci. Model OSI jest traktowany jako model odniesienia (wzorzec) dla większości rodzin protokołów komunikacyjnych. Model ten jest otwarty, co oznacza, że każdy może z niego korzystać bez wnoszenia opłat licencyjnych.

11.3. Stos protokołów TCP/IP

Oprócz modelu OSI istnieją także inne modele sieci, z których najpopularniejszy, stos protokołów **TCP/IP**, powstał na zamówienie Departamentu Obrony USA (stąd druga nazwa to „stos DOD"). Stos protokołów TCP/IP jest powszechnie stosowany, między innymi w sieci internet. Podobnie jak w modelu OSI, możemy w nim wyróżnić warstwy, jednak funkcje są różne, mimo że niektóre z nich posiadają nazwy takie same jak w modelu OSI. Stos protokołów TCP/IP składa się z czterech warstw.

Warstwa aplikacji obejmuje funkcje trzech najwyższych warstw modelu OSI (aplikacji, prezentacji i sesji). Użytkownicy uruchamiają programy, które uzyskują dostęp do usług za pośrednictwem protokołu na poziomie warstwy transportu i wysyłają lub odbierają dane w postaci pojedynczych komunikatów lub strumienia bajtów. Programy użytkowe przekazują do warstwy transportowej dane w wymaganym formacie, aby mogły one zostać dostarczone w odpowiednie miejsce. W warstwie tej działa wiele protokołów aplikacji, między innymi: http, ftp, telnet, ssh, smtp, pop3.

Podstawowym zadaniem **warstwy transportowej** jest zapewnienie komunikacji między programami użytkownika. Warstwa ta może zarządzać przepływem informacji oraz zapewniać niezawodność przesyłania przez porządkowanie segmentów danych i retransmisję uszkodzonych lub zagubionych segmentów. W komputerze może działać wiele aplikacji wymieniających dane w sieci przy wykorzystaniu portów określonych dla każdego połączenia i nie nastąpi wymieszanie się przesyłanych przez nie danych. Warstwa transportowa dzieli strumień danych na segmenty, a w nagłówku umieszcza numer portu identyfikujący aplikację wysyłającą lub odbierającą dane. W warstwie tej działa **protokół połączeniowy TCP** oraz **bezpołączeniowy UDP**.

Warstwa internetowa przyjmuje segmenty z warstwy transportowej razem z informacjami identyfikującymi odbiorcę. Zadaniem jej jest wysyłanie pakietów i dostarczenie ich do miejsca przeznaczenia, niezależnie od trasy, po której będą przesyłane. Protokołem zarządzającym tą warstwą jest **protokół IP**. Warstwa dzieli dane na pakiety, dodając

nagłówek zawierający między innymi adres IP nadawcy i odbiorcy. Na podstawie adresu IP miejsca docelowego jest podejmowana decyzja, czy wysłać pakiet wprost do odbiorcy w sieci lokalnej, czy też do routera, który przekaże go do odpowiedniego interfejsu sieciowego. Routery pracujące w warstwie internetu wyznaczają najlepsze trasy do miejsca przeznaczenia pakietów. Proces ten jest określany jako **trasowanie** lub **routing**. Warstwa ta zajmuje się także pakietami przychodzącymi, sprawdzając ich poprawność i stwierdzając za pomocą algorytmu trasowania, czy należy je przesłać dalej, czy też przetwarzać na miejscu. W przypadku pakietów adresowanych do maszyny lokalnej oprogramowanie tej warstwy usuwa nagłówek pakietu i wybiera protokół transportowy, który go będzie dalej obsługiwał. Warstwa ta wysyła też komunikaty kontrolne i komunikaty o błędach oraz obsługuje komunikaty przychodzące.

Warstwa dostępu do sieci odbiera pakiety IP i przesyła je przez daną sieć. Zapewnia interfejs z siecią fizyczną i zajmuje się przekazywaniem danych przez fizyczne połączenia między urządzeniami sieciowymi. Najczęściej są to karty sieciowe lub modemy. Formatuje dane do transmisji przez nośnik oraz adresuje dane do podsieci, opierając się na adresach fizycznych. Zapewnia sprawdzanie błędów przesyłu danych za pomocą sumy kontrolnej ramki.

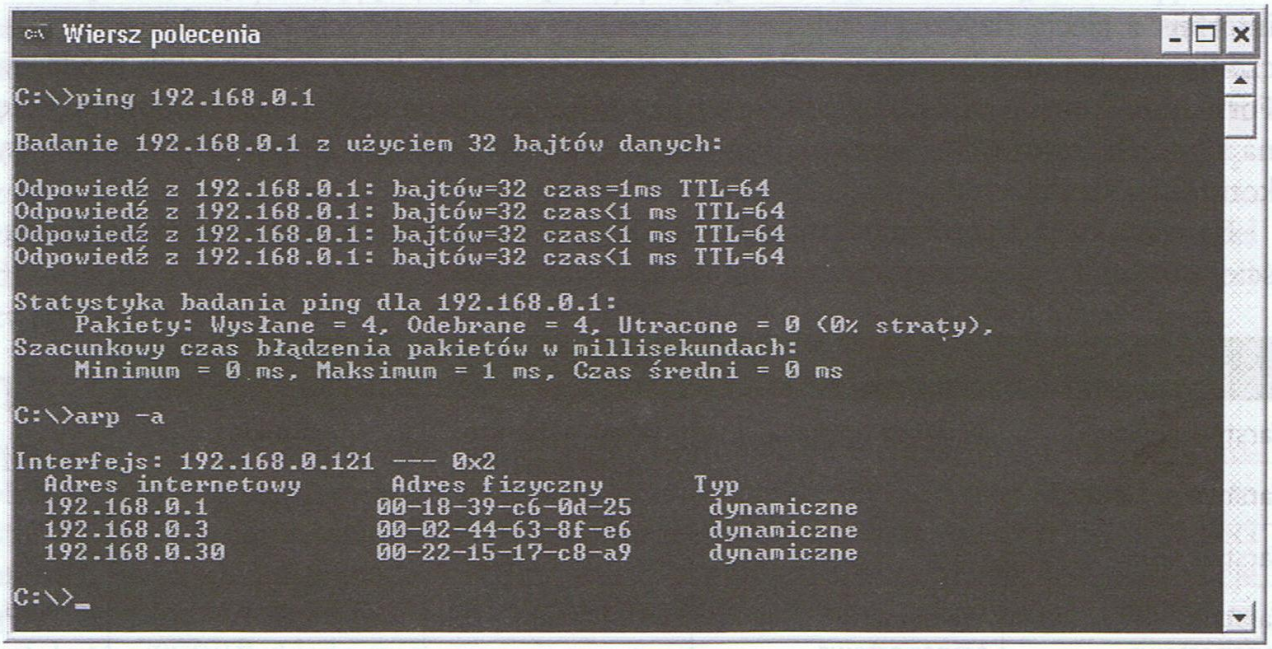
Na rysunku 11.3 porównano model OSI i TCP/IP oraz przedstawiono protokoły najczęściej używane w poszczególnych warstwach.

<table>
<tr><th>Model OSI</th><th>Model TCP/IP</th><th colspan="3">Protokoły</th></tr>
<tr><td>Warstwa aplikacji</td><td rowspan="3">Warstwa aplikacji</td><td rowspan="3">telnet, ssh, http, smtp, pop3, ftp</td><td rowspan="3">tftp, dns</td><td rowspan="3"></td></tr>
<tr><td>Warstwa prezentacji</td></tr>
<tr><td>Warstwa sesji</td></tr>
<tr><td>Warstwa transportowa</td><td>Warstwa transportowa</td><td>TCP</td><td>UDP</td><td>ARP</td></tr>
<tr><td>Warstwa sieciowa</td><td>Warstwa internetowa</td><td colspan="2">IP, ICMP, IGMP, RIP, OSPF, BGP</td><td rowspan="3"></td></tr>
<tr><td>Warstwa łącza danych</td><td rowspan="2">Warstwa dostępu do sieci</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>Warstwa fizyczna</td></tr>
</table>

Rys. 11.3. Porównanie modelu OSI i TCP/IP

W modelu TCP/IP sieci lokalne w warstwie dostępu do sieci są budowane na podstawie standardu Ethernet. W sieciach rozległych WAN w tej warstwie stosowane są różne technologie, np. połączenia modemowe, DSL, Frame Relay, ATM. Na styku między warstwą internetową i warstwą dostępu do sieci działa protokół **ARP** (*Address Resolution Protocol*), który pozwala na ustalenie adresu sprzętowego MAC hosta, gdy dany jest adres warstwy sieciowej IP. Z protokołu tego korzystamy podczas wysyłania danych. Podczas komunikacji urządzeń w sieci dane muszą przejść wszystkie etapy enkapsulacji. W nagłówku pakietu urządzenie nadawcze umieszcza adres IP nadawcy oraz odbiorcy. Adres nadawcy jest przydzielony każdemu urządzeniu, adres odbiorcy jest wprowadzany przez użytkownika w postaci adresu IP lub nazwy domenowej komputera. Adresy te są więc znane i urządzenie może utworzyć pakiet. W nagłówku ramki jest potrzebny adres MAC nadawcy i odbiorcy. Każda karta sieciowa posiada unikatowy adres MAC, więc urządzenie „zna" swój adres, brakuje jeszcze adresu MAC urządzenia odbiorcy. Do ustalenia tego właśnie adresu

jest wykorzystywany protokół ARP. Gdy komputer chce skorzystać z protokołu ARP, przygotowuje specjalny pakiet zapytania ARP, który jest wysyłany na adres rozgłoszeniowy, dzięki czemu dociera do wszystkich urządzeń w sieci lokalnej. Urządzenie o szukanym adresie sieciowym odpowiada, przesyłając pakiet z odpowiedzią zawierającą adres sprzętowy MAC. Komputer dysponuje już wszystkimi adresami i może przygotować ramkę. Aby uniknąć konieczności wysyłania kolejnego zapytania ARP, komputer zapisuje sobie w specjalnej tablicy informacje o adresach urządzeń, z którymi się komunikował. Przed następnym wysłaniem zapytania ARP sprawdzi w tablicy, czy nie ma zapisanego poszukiwanego adresu. Komputery mogą się ze sobą komunikować za pośrednictwem adresu fizycznego tylko w obrębie danej sieci (w warstwie drugiej modelu OSI). Jeśli jakieś informacje mają być przesłane do innej sieci, to protokół ARP jest wykorzystywany do uzyskania informacji



Rys. 11.4. Tablica ARP

o adresie bramy sieciowej. Na rysunku 11.4 pokazano zawartość tablicy ARP komputera, który komunikował się z innymi urządzeniami. Protokół odwrotny **RARP** (*Reverse Address Resolution Protocol*) pozwala na ustalenie adresu IP na podstawie adresu fizycznego MAC.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Korzystając z metody opisanej powyżej, sprawdź, jaki jest adres MAC bramy w sieci w Twojej szkole.
2. Wyszukaj w internecie, np. na stronie http://pl.wikipedia.org/wiki pod hasłem „Ethernet" i „IPv4" informacje o maksymalnym całkowitym rozmiarze pakietu i ramki Ethernet.

12 Protokoły warstwy łącza danych

ZAGADNIENIA

- **Jakie są wersje Ethernetu?**
- **Jak zbudowana jest ramka w sieci Ethernet?**
- **Jakie są zasady oznaczania nośników w sieci Ethernet?**
- **Według jakich standardów ustala się kolejność kabli w złączu RJ-45?**
- **Jakie typy kabli wykorzystywane są do łączenia urządzeń?**
- **Czym są kolizje i domeny kolizyjne?**
- **Jak ograniczyć liczbę kolizji?**
- **Jak zmniejszyć rozmiar domeny rozgłoszeniowej?**

12.1. Standard Ethernet

Podstawowym standardem wykorzystywanym w budowie sieci lokalnych jest Ethernet. Standard ten opisany został w dokumencie IEEE 802.3. Ethernet odnosi się do wielu technologii sieci lokalnych LAN, z których należy wyróżnić trzy podstawowe kategorie:

- Ethernet 10 Mb/s (*Standard Ethernet*),
- Ethernet 100 Mb/s (*Fast Ethernet*),
- Ethernet 1 Gb/s (*Gigabit Ethernet*).

Dane przesyłane w sieci Ethernet są podzielone na fragmenty, nazywane ramkami. Budowę ramki Ethernet przedstawiono na rys. 12.1.

7	1	6	6	2	46-155	4
Preambuła	SFD	MAC odbiorcy	MAC nadawcy	Typ ramki	Dane	CRC

Rys. 12.1. Budowa ramki Ethernet

- Preambuła – 7 bajtów złożonych z naprzemiennych jedynek i zer pozwalających na szybką synchronizację odbiorników,
- SFD (*Start Frame Delimiter*) – znacznik początkowy ramki (1 bajt),
- adres MAC odbiorcy (6 bajtów),
- adres MAC nadawcy (6 bajtów),
- typ ramki/długość (2 bajty) – jeżeli jego wartość jest mniejsza niż 1500, to oznacza długość ramki, jeżeli większa – typ pakietu,
- przesyłane dane (46–1500 bajtów) – jeżeli dane są mniejsze od 46 bajtów, to są uzupełniane zerami,
- suma kontrolna FCS (*Frame Check Sequence*) – pozwala na wykrycie błędów transmisji (4 bajty).

W sieci Ethernet każda stacja widzi wszystkie przepływające ramki danych i sprawdza, czy przepływająca ramka nie jest adresowana do niej. Sprawdzenie ramki polega na porównaniu adresu MAC karty sieciowej i adresu zapisanego w polu „adres MAC odbiorcy". Jeżeli adresy są identyczne, to ramka jest odbierana, w innym przypadku ramka jest odrzucana.

W sieciach Ethernet mogą być stosowane różne rodzaje nośników, charakteryzujących się różnymi prędkościami przesyłania danych. Ogólny schemat oznaczania prędkości przesyłania danych oraz rodzaju medium stosowanego w sieciach Ethernet składa się z następujących części:

- prędkość przesyłania danych wyrażona w Mb/s, np. 10, 100, 1000,
- rodzaj transmisji:
  - Base – transmisja w paśmie podstawowym (*baseband*),
  - Broad – transmisja przy wykorzystaniu częstotliwości nośnej (*broadband*),
- 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.

Najczęściej stosowane nośniki danych dla sieci Ethernet:

- 10Base2 – cienki kabel koncentryczny o prędkości przesyłania sygnału 10 Mb/s, transmisja pasmem podstawowym, 2 to maksymalna długość kabla w metrach, zaokrąglona do setek, a następnie podzielona przez 100,
- 10Base5 – gruby kabel koncentryczny o maksymalnej długości 500 metrów,
- 10BaseT – długość kabla ograniczona do 100 metrów, litera T symbolizuje skrętkę jako nośnik fizyczny.

Najczęściej stosowane nośniki danych dla sieci FastEthernet:

- 100BaseTX – nieekranowana skrętka (UTP) Kategorii 5,
- 100BaseFX – światłowód obsługujący transmisję danych z szybkością 100 Mb/s na odległość do 400 metrów.

Najczęściej stosowane nośniki danych dla sieci Gigabit Ethernet:

- 1000BASE-T – skrętka kategorii 5 lub wyższej za pomocą czterech par przewodów,
- 1000BASE-SX – 1 Gb/s na światłowodzie wielomodowym (do 550 m),
- 1000BASE-LX – 1 Gb/s na światłowodzie jednomodowym (do 10 km).

Najpopularniejszym medium transmisyjnym stosowanym w budowie sieci komputerowych jest skrętka. Kabel ten składa się z czterech par przewodów, skręconych ze sobą i oznakowanych za pomocą kolorów izolacji. Każdy tego typu kabel jest zakończony wtyczką typu RJ-45[1]. Kolejność przewodów we wtyku jest określona za pomocą standardów TIA/EIA 568A i TIA/EIA 568B (tab. 12.1).

Do łączenia urządzeń są stosowane dwa rodzaje kabli:

- **prosty** (*straight-through*) – wtyki na obu końcach są wykonane według jednego standardu. Kabel prosty jest stosowany do łączenia komputera z przełącznikiem lub koncentratorem oraz routera z przełącznikiem lub koncentratorem;
- **skrosowany** (*crossover*) – wtyk na jednym końcu jest wykonany według standardu 568A, a na drugim według standardu 568B. Kabel skrosowany jest stosowany do łączenia komputera z komputerem, przełącznika lub koncentratora z przełącznikiem lub koncentratorem, komputera z routerem.

[1] Z technicznego punktu widzenia prawidłowe oznaczenie to 8P8C, ale powszechnie używa się nazwy RJ-45.

Większość nowoczesnych urządzeń sieciowych wyposażona jest w funkcję Auto MDI/MDIX (*Automatic MDI/MDIX crossover*). Funkcja ta polega na automatycznym rozpoznaniu przez to urządzenie, czy podłączony kabel sieciowy jest prosty czy skrosowany. Dzięki niej do portu takiego urządzenia można podłączyć zarówno kabel prosty jak i skrosowany. W starszych urządzeniach stosowane były specjalne porty typu uplink (zazwyczaj współdzielone z portem pierwszym) lub ręczne przełączniki normal/uplink, umożliwiające wewnętrzne „skrosowanie" portu.

Wtyczkę RJ45 pokazano na rysunku 12.2.

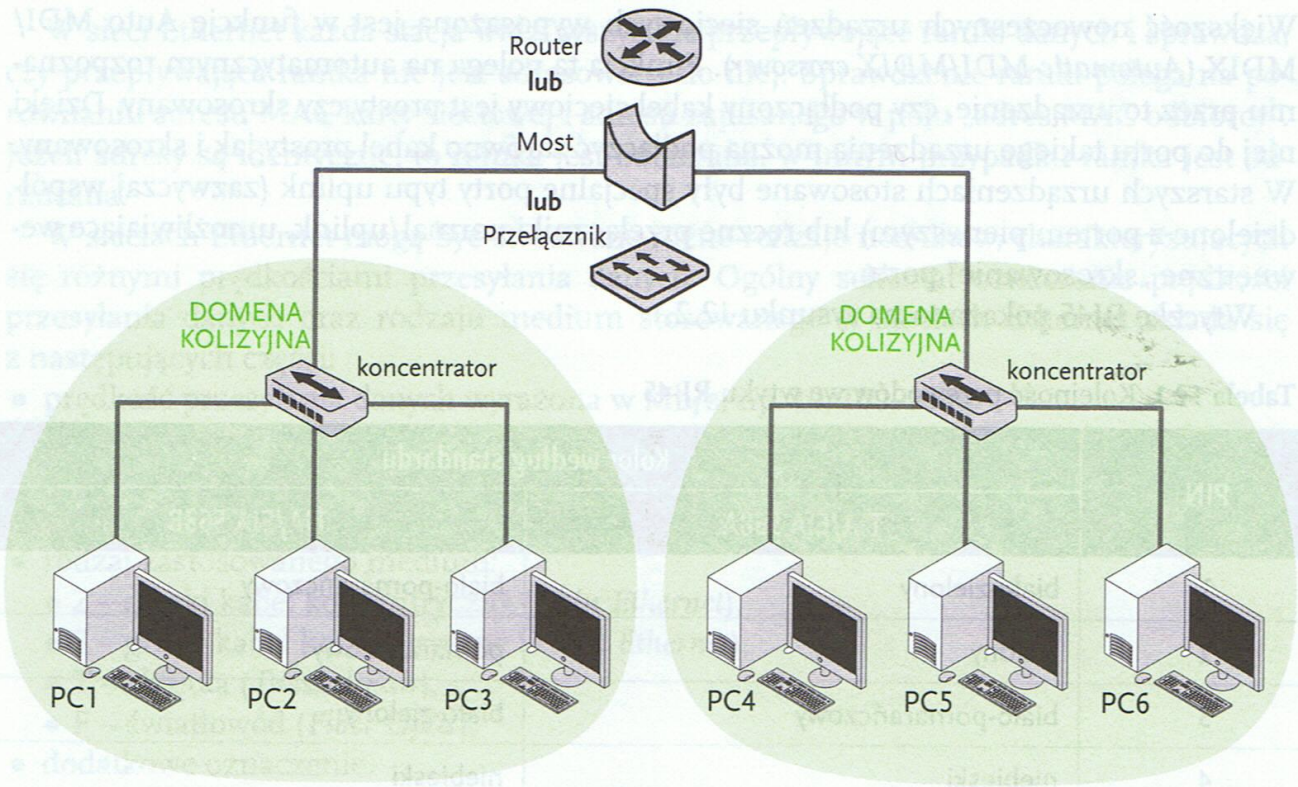
Tabela 12.1. Kolejność przewodów we wtyku RJ-45

PIN	Kolor według standardu	
	TIA/EIA 568A	TIA/EIA 568B
1	biało-zielony	biało-pomarańczowy
2	zielony	pomarańczowy
3	biało-pomarańczowy	biało-zielony
4	niebieski	niebieski
5	biało-niebieski	biało-niebieski
6	pomarańczowy	zielony
7	biało-brązowy	biało-brązowy
8	brązowy	brązowy

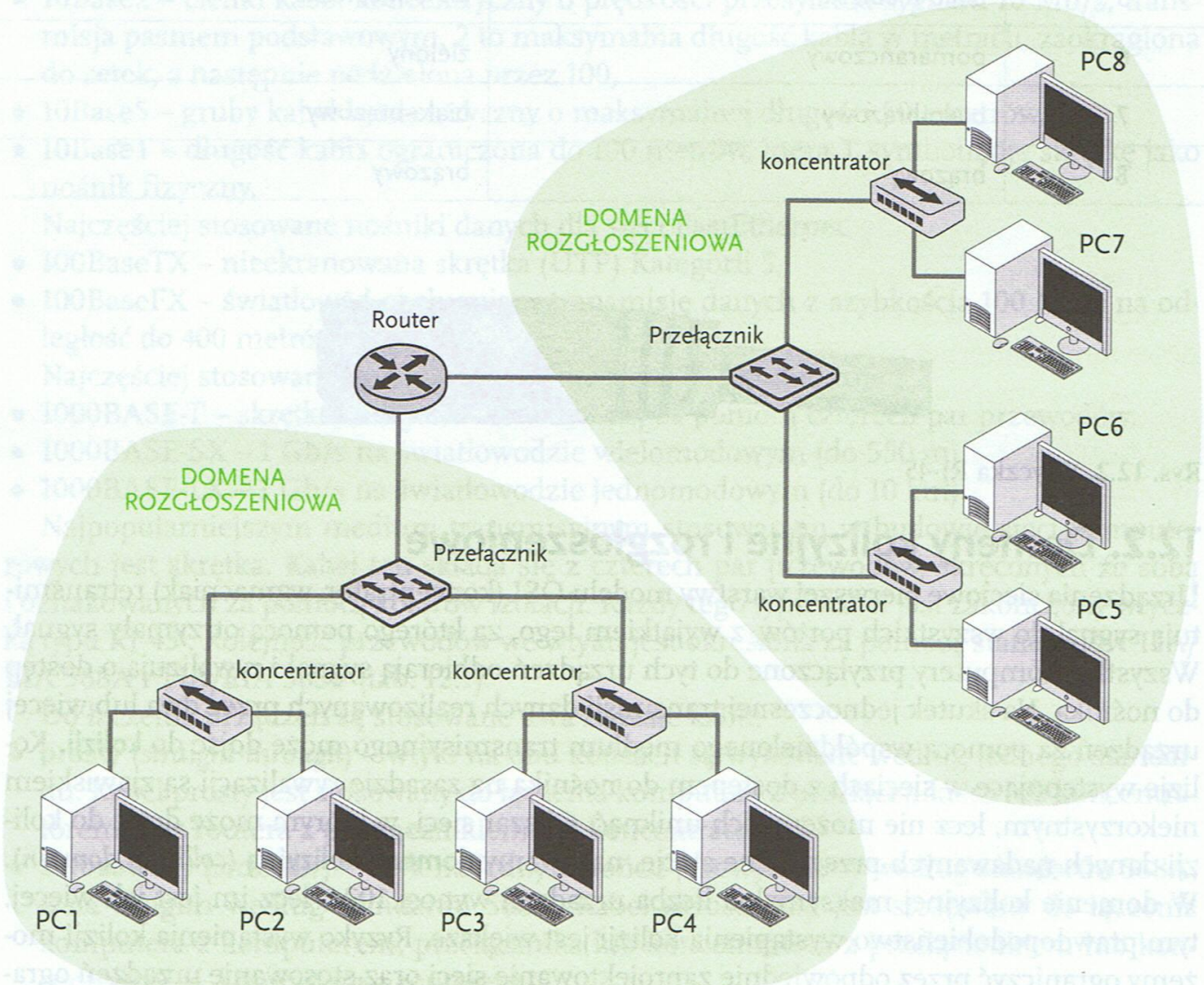
Rys. 12.2. Wtyczka RJ-45

12.2. Domeny kolizyjne i rozgłoszeniowe

Urządzenia sieciowe pierwszej warstwy modelu OSI (koncentrator, wzmacniak) retransmitują sygnał do wszystkich portów, z wyjątkiem tego, za którego pomocą otrzymały sygnał. Wszystkie komputery przyłączone do tych urządzeń odbierają sygnał i rywalizują o dostęp do nośnika. Na skutek jednoczesnej transmisji danych realizowanych przez dwa lub więcej urządzeń za pomocą współdzielonego medium transmisyjnego może dojść do **kolizji.** Kolizje występujące w sieciach z dostępem do nośnika na zasadzie rywalizacji są zjawiskiem niekorzystnym, lecz nie możemy ich uniknąć. Obszar sieci, w którym może dojść do kolizji danych nadawanych przez różne stacje, nazywamy **domeną kolizyjną** (*collision domain*). W domenie kolizyjnej maksymalna liczba urządzeń wynosi 1024, lecz im jest ich więcej, tym prawdopodobieństwo wystąpienia kolizji jest większe. Ryzyko wystąpienia kolizji możemy ograniczyć przez odpowiednie zaprojektowanie sieci oraz stosowanie urządzeń ograniczających wielkość domen kolizyjnych, takich jak mosty, przełączniki lub routery.



Rys. 12.3. Podział sieci na domeny kolizyjne



Rys. 12.4. Podział sieci na domeny rozgłoszeniowe

Efektywne projektowanie sieci prowadzi do organizacji struktury sieci w taki sposób, aby domeny kolizyjne były jak najmniejsze. Urządzenia, takie jak: przełącznik, most lub router, pozwalają na zmniejszenie obszaru domeny kolizyjnej. Transmisje realizowane między urządzeniami w obrębie domeny kolizyjnej nie są przesyłane przez mosty, przełączniki i routery do innych domen. Jeżeli komputer PC1 (rys. 12.3) będzie przesyłał dane do komputera PC2, to most, przełącznik lub router stwierdzi, że oba komputery są przyłączone do tego samego portu (domeny kolizyjnej) i nie prześle ramki do drugiego portu. W tym samym czasie po drugiej stronie urządzenia może odbywać się inna transmisja, np. z komputera PC4 do PC5, co zwiększa wydajność sieci. Jeżeli transmisja będzie się odbywać między komputerami znajdującymi się w różnych domenach kolizyjnych, np. PC1 i PC4, to ramka dotrze do wszystkich komputerów w obu domenach. Jakakolwiek inna transmisja w tym samym czasie w tych domenach spowoduje kolizję.

W sieci przesyłane mogą być również komunikaty rozgłoszeniowe. Obszar sieci, w którym następuje emisja komunikatu rozgłoszeniowego wysyłanego przez jedną stację do wszystkich innych, nazywamy **domeną rozgłoszeniową** (*Broadcast domain*). Urządzenia warstwy pierwszej (koncentrator i wzmacniak) oraz drugiej (most i przełącznik) przekazują ruch rozgłoszeniowy. Urządzenia te rozszerzają domenę rozgłoszeniową, natomiast urządzenia warstwy trzeciej (router) ograniczają jej rozmiar. Rozmiar domeny rozgłoszeniowej można ograniczyć również przez zdefiniowanie **sieci wirtualnych** VLAN (*Virtual Local Area Network*). Komunikacja między sieciami wirtualnymi musi się odbywać za pośrednictwem routera. Komunikaty rozgłoszeniowe wysyłane przez komputer, np. PC1, będą docierać tylko do komputerów PC2, PC3 i PC4, przesyłanie ich do pozostałych komputerów w sieci zostanie zablokowane przez router (rys. 12.4).

SPRAWDŹ SWOJĄ WIEDZĘ

1. Sprawdź, według którego standardu wykonany jest kabel, którym Twój komputer podłączony jest do sieci.
2. Narysuj schemat sieci w Twojej szkole. Oblicz liczbę domen kolizyjnych i rozgłoszeniowych.

13 Protokoły warstwy sieci

ZAGADNIENIA

- **Jakie funkcje pełni protokół IP?**
- **Jak zbudowany jest nagłówek pakietu IP?**
- **Do czego służy tablica routingu?**
- **Do czego służą protokoły routingu?**
- **Jakie są przykładowe protokoły routingu i jak działają?**
- **Jak działa rozsyłanie grupowe informacji?**

13.1. Protokół IP

Protokół IP (*Internet Protocol*) jest odpowiedzialny za przesyłanie pakietów między użytkownikami sieci. Jest protokołem bezpołączeniowym, co oznacza, że w trakcie transmisji nie sprawdza się poprawności pakietów przesyłanych przez sieć. Nie ma zatem gwarancji ich dostarczenia, ponieważ mogą one zostać po drodze zagubione lub uszkodzone.

Podstawowymi funkcjami protokołu IP są:

- określanie i tworzenie struktury pakietu,
- określanie schematu adresowania logicznego IP,
- kierowanie ruchem pakietów w sieci.

IP jest protokołem zawodnym. Jedynym kryterium pozwalającym sprawdzić poprawność przesyłania jest suma kontrolna nagłówka zawarta w polu „Suma kontrolna". Jeżeli w trakcie transmisji został odkryty błąd, to pakiet jest niszczony przez stację, która wykryła niezgodność. W takim przypadku nie ma żadnych powtórek transmisji i kontroli przepływu danych. Nagłówek protokołu IP jest wykorzystywany do transportu danych między urządzeniem źródłowym i docelowym. Budowa nagłówka jest pokazana na rysunku 13.1.

<table>
<tr><td colspan="2">1 bajt</td><td>2 bajt</td><td colspan="2">3 bajt</td><td>4 bajt</td></tr>
<tr><td>Wersja</td><td>Dł. Nag.</td><td>Typ usług</td><td colspan="3">Całkowita długość pakietu</td></tr>
<tr><td colspan="3">Identyfikacja</td><td>Flagi</td><td colspan="2">Przesunięcie fragmentu</td></tr>
<tr><td colspan="2">Czas życia</td><td>Protokół</td><td colspan="3">Suma kontrolna</td></tr>
<tr><td colspan="6">Adres źródłowy</td></tr>
<tr><td colspan="6">Adres docelowy</td></tr>
<tr><td colspan="5">Opcje</td><td></td></tr>
<tr><td colspan="6">Dane</td></tr>
</table>

Rys. 13.1. Budowa nagłówka protokołu IP

Znaczenie wybranych pól nagłówka:

- **Czas życia TTL** (*Time To Live*) – określa maksymalny czas przebywania pakietu w sieci. Każdy router, przez który przechodzi pakiet, zmniejsza wartość o 1. Gdy wartość w polu osiągnie zero, pakiet jest kasowany. Zabezpiecza to sieć przed przesyłaniem pakietów krążących w pętli. Maksymalna wartość tego pola wynosi 255, co oznacza, że na trasie pakietu nie może być więcej niż 255 routerów.
- **Adres źródłowy** – adres IP nadawcy pakietu.
- **Adres docelowy** – adres IP odbiorcy pakietu.

Warstwa sieciowa odpowiada za wybranie optymalnej trasy, po jakiej będzie przesyłany każdy pakiet. Jeżeli odbiorca znajduje się w tej samej sieci, pakiet będzie wysłany bezpośrednio do niego. W przeciwnym razie musi być przekazany do bramy łączącej sieci. Decyzję o wyborze trasy podejmuje router na podstawie adresu IP urządzenia docelowego, umieszczonego w nagłówku pakietu, oraz na podstawie informacji posiadanych w tablicy routingu. W tablicy tej router przechowuje informacje o wszystkich sieciach, do których jest w stanie wysyłać pakiety. Jeżeli w tablicy routingu nie ma adresu docelowego, umieszczonego w nagłówku pakietu, router może wysłać pakiet, korzystając z trasy domyślnej (jeżeli została zdefiniowana) lub pakiet jest kasowany. Przykładowa tablica routingu pokazana jest na rysunku 13.2.

```
R4# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX -
EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i
- IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default U - per-user static route, o
- ODR
Gateway of last resort is not set
[1] C   10.77.0.0/16 is directly connected, Ethernet0
[2] C   10.80.0.0/16 is directly connected, Ethernet0
[3] C   10.5.0.0/16 is directly connected, Ethernet0
[4] C   10.125.0.0/16 is directly connected, Ethernet0
[5] C   10.1.0.0/16 is directly connected, Ethernet0
[6] R   192.168.5.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
[7] R   192.168.1.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
[8] R   192.168.2.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
[9] R   192.168.3.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
[10] R 192.168.4.0/24 [120/3] via 192.168.6.1, 00:00:13, Serial0
R4#
```

Rys. 13.2. Przykładowa tablica routingu

Z tablicy tej wynika, że pakiet adresowany do sieci 10.77.0.0/16 zostanie wysłany za pomocą interfejsu Ethernet0, a pakiety adresowane do sieci 192.168.1.0/24 wysyłane będą interfejsem Serial0.

13.2. Protokoły routingu

Informacje o trasach w tablicach routingu mogą być wprowadzane **statycznie** przez administratora, lecz wymaga to dużo czasu i rekonfiguracji wszystkich routerów w przypadku zmian w sieci. Routery mogą również uczyć się tras w sposób **dynamiczny.** W tym celu korzystają z **protokołów routingu** do wymiany między sobą informacji o trasach lub to-

pologii sieci. Na podstawie tych informacji ustalane są optymalne trasy prowadzące do poszczególnych sieci i umieszczane w tablicy routingu. Przykładami protokołów routingu są RIP, OSPF, IGRP, EIGRP.

Protokół RIP (*Routing Information Protocol*) jest protokołem wykorzystującym algorytm **wektora odległości** (*distance-vector*). Ze względu na niskie wymagania sprzętowe może być używany przez wszystkie routery. Router, na którym jest uruchomiony protokół RIP, wysyła do swoich bezpośrednich sąsiadów zawartość swojej tablicy routingu w określonych, stałych przedziałach czasu, standardowo co trzydzieści sekund. Router po przyjęciu aktualizacji od sąsiada porównuje ją z własną tablicą routingu i w razie konieczności uaktualnia ją. W tablicy routingu znajdują się najlepsze trasy do wszystkich sieci. Jako miarę jakości trasy (metrykę) w protokole RIP przyjęto liczbę przeskoków (*hops*) między routerami, jakie pakiet musi wykonać, aby dotrzeć do celu. Gdy router przyjmie uaktualnienie tablicy routingu, które zawiera nowe lub zmienione informacje o trasach, to dodaje jedynkę do wartości metryki wskazanej w uaktualnieniu i wpisuje zmianę do tablicy routingu. Adresem następnego przeskoku jest adres IP nadawcy. Liczba przeskoków jest ograniczona do 15. Dlatego RIP nie może być stosowany w bardzo dużych sieciach. RIP dobrze spełnia swoje zadanie w sieciach jednorodnych, to znaczy takich, w których wszystkie łącza mają jednakową przepustowość.

Protokół OSPF (*Open Shortest Path First*) jest, podobnie jak RIP, protokołem otwartym, co oznacza, że jego specyfikacja jest ogólnie dostępna. Protokół OSPF jest protokołem routingu **stanu łącza** (*link-state*), wykorzystującym **algorytm SPF** (algorytm Dijkstry) do obliczania najkrótszych ścieżek. Metryką w protokole OSPF jest koszt, który jest powiązany z przepustowością łączy (im większa przepustowość, tym niższy koszt). Protokół OSPF jest przeznaczony do dużych sieci. Sieć taka może być podzielona na obszary. Routery w danym obszarze, na których uruchomiono protokół OSPF, wymieniają się wzajemnie krótkimi komunikatami LSA (*Link State Advertisement*). Na podstawie tych komunikatów każdy router zbiera informacje o całej topologii obszaru, a następnie za pomocą algorytmu SPF oblicza najlepsze trasy do wszystkich sieci. Każdy obszar musi być dołączony do obszaru 0 (szkieletowego), co pozwala na połączenie sieci w jedną całość. Zmiany dokonane w jednym z obszarów nie powodują konieczności uruchomienia algorytmu SPF w pozostałych obszarach. Obliczanie ścieżek w poszczególnych obszarach jest łatwiejsze i wymaga mniejszego nakładu obliczeniowego. Ze względu na konieczność dokonywania skomplikowanych obliczeń protokół OSPF ma większe wymagania sprzętowe niż RIP.

Protokół IGRP (*Interior-Gateway Routing Protocol*) i jego następca **EIGRP** (*Extended IGRP*) zostały opracowane przez firmę CISCO. IGRP, podobnie jak RIP, jest protokołem typu dystans-wektor, ale wykorzystuje jako metrykę różne kombinacje czterech miar: opóźnienia, szerokości pasma (przepustowości), obciążenia i niezawodności. Protokół jest zastępowany przez EIGRP. EIGRP posiada cechy algorytmów routingu z wykorzystaniem wektora odległości i według stanu łącza. Protokół EIGRP do wyznaczania tras stosuje **algorytm DUAL** (*Diffusing-Update ALgorithm*). Jest on zalecany do stosowania przez CISCO.

Współcześnie liczba routerów w sieci internet jest tak duża, że żaden z nich nie byłby w stanie przechowywać tras do wszystkich sieci. Aby temu zapobiec i ułatwić zarządzanie w internecie, wprowadzono hierarchię routingu. Największą jednostką w hierarchii jest **system autonomiczny** AS (*Autonomous System*), który jest zbiorem sieci pod wspólną administracją, z ustaloną wspólną strategią routingu. System AS można podzielić na pewną liczbę **obszarów** (*areas*), które są grupami sąsiednich sieci i przyłączonych hostów. Poszczególne obszary sprzęgają routery graniczne obszaru (*area border routers*). Router graniczny utrzymuje oddzielną dla każdego obszaru bazę danych o topologii. Protokoły RIP, OSPF, IGRP i EIGRP są protokołami **routingu wewnętrznego** IGP (*Interior Gateway*

Protocol) i mogą działać wewnątrz systemu autonomicznego. Do ustalania tras między systemami autonomicznymi wykorzystywane są **zewnętrzne protokoły routingu** EGP (*Exterior Gateway Protocol*), np. protokół BGP.

13.3. Rozsyłanie grupowe informacji

Normalna komunikacja z wykorzystaniem protokołu IP odbywa się między jednym nadawcą i jednym odbiorcą (nie licząc pakietów rozgłoszeniowych). Dla niektórych aplikacji jest użyteczne wysyłanie informacji jednocześnie do wielu odbiorców, takie aplikacje to np. giełdowe informacje dla brokerów, połączenia konferencyjne, odbieranie audycji radiowych i telewizyjnych za pośrednictwem internetu. **Rozgłaszanie grupowe** (*multicasting*) jest technologią opierającą się na następujących zasadach:

- Routery obsługujące transmisję przekazują pakiety multicastowe do danej sieci tylko wtedy, gdy w tej sieci znajduje się przynajmniej jeden członek konkretnej grupy multicastowej. Pojedynczy host może być członkiem jednej grupy lub większej ich liczby.
- Komputery do powiadomienia routera o członkostwie w danej grupie lub o jego rezygnacji wykorzystują protokół **IGMP** (*Internet Group Management Protocol*). Hosty zgłaszają za pomocą IGMP swoje członkostwo w grupie multicastowej do dowolnego sąsiadującego routera multicastowego.
- Komputery mogą być odbiorcami, nadawcami lub pełnić obie te funkcje jednocześnie w danej grupie multicastingowej.

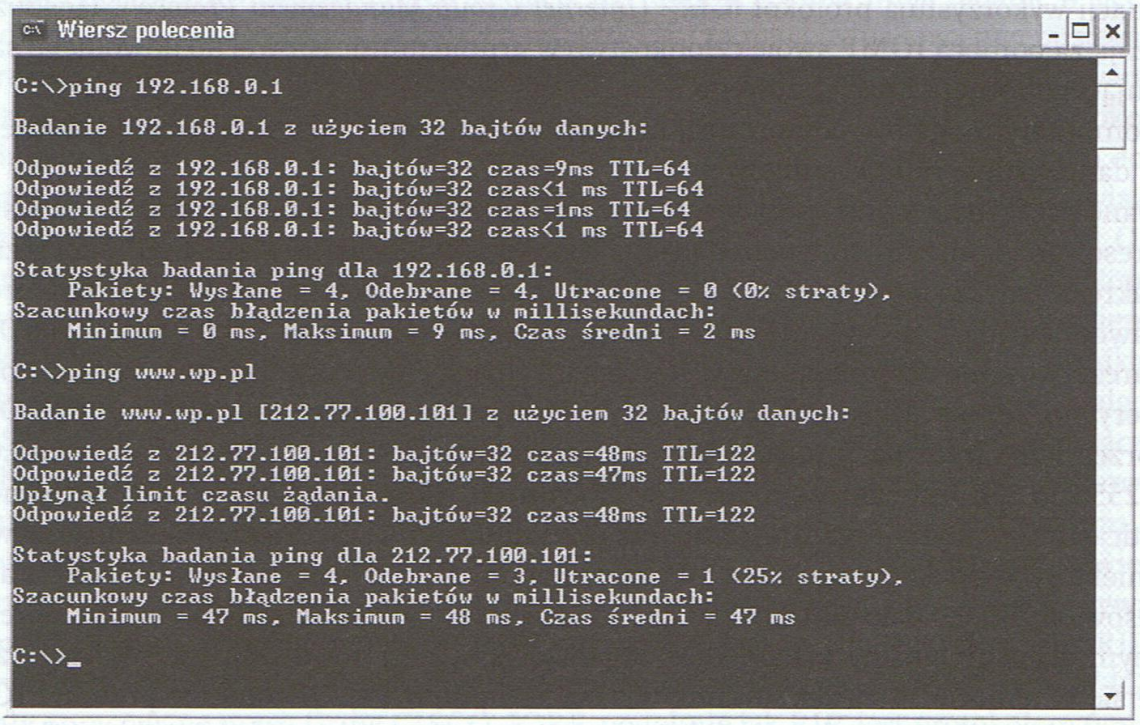
Dane przesyłane są na specjalne adresy multicastowe określające grupę, która jest zainteresowana konkretnym typem danych. Wszystkie multicastowe adresy IP mieszczą się w zakresie od 224.0.0.0 do 239.255.255.255. Zakres ten określa tylko grupę odbiorców, nadawcy posiadają zawsze adres unicastowy. Adresy w zakresie od 224.0.0.0 do 224.0.0.255 są zarezerwowane dla protokołów w sieciach lokalnych i nie mogą być przekazywane przez routery, np. adresy 224.0.0.5 i 224.0.0.6 wykorzystywane są przez protokół routingu OSPF do przesyłania informacji między wszystkimi routerami. Zakres adresów od 224.0.1.0 do 238.255.255.255 jest zakresem adresów globalnych, które mogą być wykorzystywane do multicastingu między organizacjami oraz przez internet. Część z nich jest zarezerwowana dla niektórych aplikacji, np. 224.0.1.1 dla protokołu NTP (*Network Time Protocol*). Zakres adresów od 239.0.0.0 do 239.255.255.255 jest zakresem o ograniczonym zasięgu, przeznaczonym dla grup lokalnych lub jednej organizacji. Więcej informacji o adresach IP znajduje się w temacie 14 – Adresowanie w sieci komputerowej. W routerze protokół IGMP śledzi, do których sieci należy wysyłać transmisje grupowe, na podstawie przynależności hostów do grup. Każdy router okresowo odpytuje swoje sieci, aby sprawdzić, czy dostarczanie danych grupowych nadal jest wymagane. Kontrola ta odbywa się za pomocą zapytań o członkostwo hosta, które kierowane są pod zarezerwowany adres IP 224.0.0.1. Hosty przynależące do grup odpowiadają na ten komunikat raportem, którego adres docelowy odpowiada wymaganemu adresowi grupowemu. Przyłączenie do grupy odbywa się przez transmisje pakietu IGMP – *Host Membership Report*. Pakiet ten zawiera adres IP pożądanej grupy. Przyłączenie hosta do grupy obejmuje dwa procesy u klienta:

- host powiadamia router, że chce przyłączyć się do odpowiedniej grupy,
- host wiąże dynamicznie IP z adresem grupowym zarezerwowanym dla danej aplikacji oraz z zarezerwowanym adresem Ethernet.

Host, który podłączy się do nowej grupy multicastowej, ma obowiązek wysłać natychmiastowy raport do tej grupy, bez czekania na zapytanie od routera. Aby korzystać z transmisji multicastowych, należy dysponować odpowiednią aplikacją obsługującą ten rodzaj transmisji.

13.4. Protokół ICMP

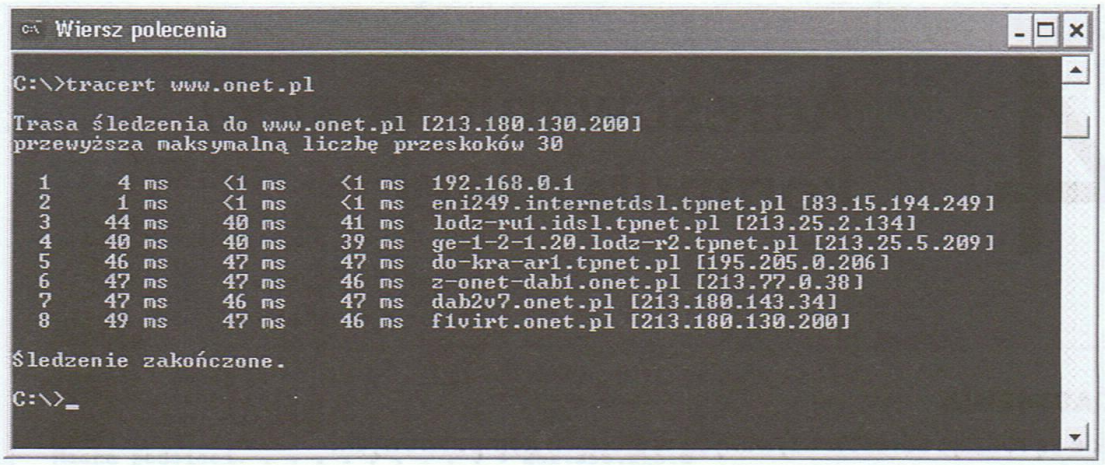
Ściśle związany z protokołem IP jest protokół **ICMP** (*Internet Control Message Protocol*). Protokół IP, jako bezpołączeniowy, nie posiada mechanizmów informowania o błędach w funkcjonowaniu sieci IP oraz diagnostyki sieci. Do tego celu jest przeznaczony protokół ICMP. Umożliwia on przesyłanie między komputerami lub routerami informacji o błędach występujących w funkcjonowaniu sieci IP. Najczęściej używanymi poleceniami korzystającymi w protokołu ICMP są **ping** i **tracert**. Ping jest to program używany w sieciach komputerowych działających na podstawie protokołu TCP/IP, służący do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie, czy istnieje połączenie między hostem testującym i testowanym, oraz na określenie jakości połączenia przez pomiar liczby zgubionych pakietów oraz czasu potrzebnego na ich transmisję. Ping wysyła pakiety **żądania echa** ICMP (*Echo Request*) i odbiera **odpowiedzi na żądanie echa** ICMP (*Echo Reply*). Jako argument dla polecenia ping można podać adres IP lub nazwę domenową komputera testowanego (rys. 13.3).



Rys. 13.3. Działanie programu ping

Komputery powinny odpowiadać na żądanie echa, lecz większość współczesnych programów typu firewall blokuje ten proces, w konsekwencji czego możemy nie otrzymać odpowiedzi, mimo że istnieje połączenie między hostami.

Program tracert (w systemach Linux program nazywa się traceroute) jest przeznaczony do śledzenia trasy, po jakiej są przesyłane pakiety w sieci. Program ten wysyła pakiet żądania echa z polem TTL (*Time To Live*) ustawionym na kolejne wartości, od 1 do 30. Wartość TTL jest zmniejszana przy przechodzeniu przez kolejne routery na trasie. Jeżeli pole TTL osiągnie wartość 0, pakiet jest kasowany przez router. Router dodatkowo wysyła za pomocą protokołu ICMP informację zwrotną o błędzie. Komputer źródłowy uzyskuje, bezpośrednio po wysłaniu żądania o wartości 1, adres IP pierwszego routera na trasie. W następnym pakiecie pole TTL ma wartość 2, co powoduje, że pierwszy router zmniejszy tę wartość do 1, a drugi router zmniejszy TTL do 0 i skasuje pakiet, wysyłając komunikat



Rys. 13.4. Działanie polecenia tracert

o błędzie. W ten sposób program tracert może prześledzić trasę w sieci zawierającej nie więcej niż 30 routerów. Brak odpowiedzi na zadany pakiet jest sygnalizowany znakiem gwiazdki „*" i może wynikać z konfiguracji firewalla lub przeciążenia sieci. Przykład działania polecenia tracert pokazano na rysunku 13.4.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sprawdź, jakiego adresu IP używa Twój komputer w szkole i w domu.
2. Za pomocą polecenia ping sprawdź czas odpowiedzi serwera WWW Twojej szkoły lub innego wskazanego przez nauczyciela.
3. Sprawdź liczbę routerów na trasie do serwera WWW Twojej szkoły lub innego wskazanego przez nauczyciela.

14 Adresowanie w sieci komputerowej

ZAGADNIENIA

- **Jakie są rodzaje adresów używanych w sieciach komputerowych?**
- **Jak zbudowany i reprezentowany jest adres MAC i IP?**
- **Jak szybko przeliczać liczby dwójkowe na dziesiątkowe i dziesiątkowe na dwójkowe?**
- **Jakie są klasy adresów IP i adresy specjalne?**
- **Kto odpowiada za przydzielanie adresów IP?**
- **Co to są adresy prywatne i do czego są używane?**
- **Do czego służy NAT i adresy APIPA?**
- **Jakie metody zapobiegają wyczerpywaniu się dostępnej puli adresów?**
- **Co to jest adresowanie bezklasowe i jak je stosować?**
- **Jak na podstawie adresu IP i maski podsieci wyznaczać adres sieci, adres rozgłoszeniowy, liczbę podsieci i liczbę hostów?**
- **Jak obliczyć, czy komputery będą mogły się komunikować w sieci?**

Do sieci komputerowej mogą być podłączone różne urządzenia, np. serwery, komputery, drukarki. Każde z nich musi mieć możliwość wymiany danych z innymi. Aby to było możliwe, potrzebny jest mechanizm pozwalający na zidentyfikowanie każdego urządzenia podłączonego do sieci. Identyfikacja odbywa się za pomocą unikatowych ciągów znaków, nazywanych adresami. Adresy takie przypominają sposób zapisu miejsca zamieszkania. Znając miejsce zamieszkania, np. kolegi, możemy wysłać do niego list, a poczta, posługując się adresem, dostarczy przesyłkę do miejsca przeznaczenia. W najpopularniejszych obecnie sieciach lokalnych spotyka się dwa rodzaje adresów:

- **fizyczne** – nazywane również adresami MAC (*Media Access Control*),
- **logiczne** – adresy IP (*Internet Protocol*).

14.1. Adresy fizyczne

Adres **fizyczny** jest nadawany przez producenta w każdej karcie sieciowej NIC (*Network Interface Card*) podczas jej wytwarzania. Adres ten jest niepowtarzalny i umieszczony w pamięci ROM karty. Długość adresu fizycznego wynosi 48 bitów, lecz jest przedstawiany w zapisie heksadecymalnym (szesnastkowym), np. 00:03:FF:14:C8:A0. Na rysunku 14.1 zaznaczono adres fizyczny.

Pierwsze 24 bity oznaczają producenta karty sieciowej, pozostałe 24 bity są unikatowym identyfikatorem danego egzemplarza karty. Aby sprawdzić adres fizyczny karty, można w wierszu poleceń systemu Windows 200x i nowszych wersji wpisać polecenie ipconfig/all. W systemach z rodziny Windows 9x można użyć polecenie winipcfg.

dziesiętną z zakresu od 0 do 255. Na zajęciach z matematyki podawane były algorytmy przeliczania liczb dwójkowych na dziesiętne. W tym miejscu zostanie przedstawiona inna prosta metoda wykonywania tych obliczeń. Każdemu bitowi należy przypisać jego wartość wynikającą z pozycji w liczbie dwójkowej (rys. 14.3). Następnie sumuje się te wartości, dla których bit adresu przybiera wartość 1.

Wartość w postaci wykładniczej	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Wartość bitu	128	64	32	16	8	4	2	1	
Adres dwójkowy	1	0	1	0	1	0	1	0	
Wynik	128	+	32	+	8	+	2	=	170

Rys. 14.3. Przeliczanie liczby dwójkowej na dziesiętną

PRZYKŁAD 14.2.

Zamiana adresów z postaci dziesiętnej na dwójkową

Adres podany w postaci dziesiętnej należy zamieniać na postać dwójkową. Spośród wartości dziesiętnych poszczególnych bitów należy wybrać te, których suma jest równa zamienianej liczbie. Zadanie to jest dość trudne, dlatego zostanie wyjaśnione na przykładzie – liczbę 123 należy zapisać w systemie dwójkowym. Poniżej przedstawiono wartości kolejnych bitów, zaczynając od lewej strony:

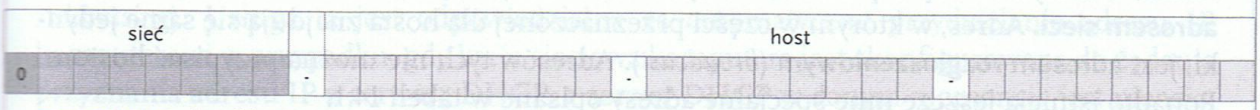
- wartość pierwszego bitu wynosi 128 i jest większa niż liczba 123 – ten bit ma wartość 0,
- wartość drugiego bitu wynosi 64 i jest mniejsza niż liczba 123 – ten bit ma wartość 1 (reszta 123 – 64 = 59),
- wartość trzeciego bitu wynosi 32 i jest mniejsza niż liczba 59 – ten bit ma wartość 1 (reszta 59 – 32 = 27),
- wartość czwartego bitu wynosi 16 i jest mniejsza niż liczba 27 – ten bit ma wartość 1 (reszta 27 – 16 = 11),
- wartość piątego bitu wynosi 8 i jest mniejsza niż liczba 11 – ten bit ma wartość 1 (reszta 11 – 8 = 3),
- wartość szóstego bitu wynosi 4 i jest większa niż liczba 3 – ten bit ma wartość 0 (reszta wynosi ciągle 3),
- wartość siódmego bitu wynosi 2 i jest mniejsza niż liczba 3 – ten bit ma wartość 1 (reszta 3 – 2 = 1),
- wartość ósmego bitu wynosi 1 i jest równa liczbie 1 – ten bit ma wartość 1 (reszta wynosi 0, co oznacza koniec obliczeń).

Liczba 123 w postaci dwójkowej jest reprezentowana przez 01111011.

14.4. Klasy adresów IP

Teoretycznie, mając do dyspozycji 32 bity, można wygenerować 2^{32} (= 4 294 967 296) adresów IP. Adresy IP zostały jednak tak zaprojektowane, aby określić, która część jest związana z adresem całej **sieci**, a która z adresem poszczególnych stacji, nazywanych **hostami.** Adresy IP zostały podzielone na klasy A, B, C, D i E.

Adresy **klasy A** przeznaczono do obsługi bardzo dużych sieci. Adres sieci zajmuje pierwszy oktet, natomiast adres hosta pozostałe trzy. Pierwszy bit adresu klasy A jest zawsze równy 0. Ostatnie 24 bity (3 oktety) adresu klasy A są adresem hosta. Podział bitów w adresie klasy A pokazano na rys. 14.4.

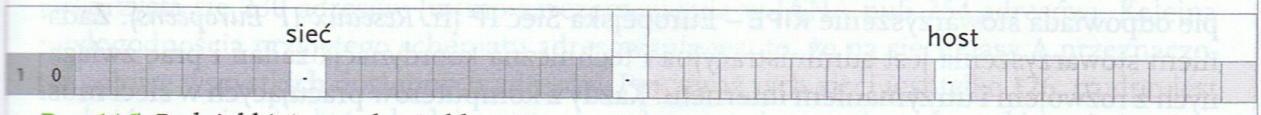


Rys. 14.4. Podział bitów w adresie klasy A

Adresy klasy A obejmują zakres od 1.0.0.0 do 127.255.255.255. Wartość pierwszego oktetu adresu klasy A mieści się w zakresie od 1 do 127. Maksymalna liczba sieci klasy A to 127. Adres 127.0.0.0 również powinien być adresem sieci klasy A, jest jednak zarezerwowany jako adres pętli zwrotnej do testowania hosta i nie można go przypisać żadnej sieci.

Każda sieć klasy A może obsługiwać 16 777 214 stacji. Na 24 bitach można zapisać 2^{24} (= 16 777 216) różnych wartości, jednak 2 spośród tych adresów (adresy specjalne) przeznaczone zostały do innych celów i nie mogą być przypisane hostom.

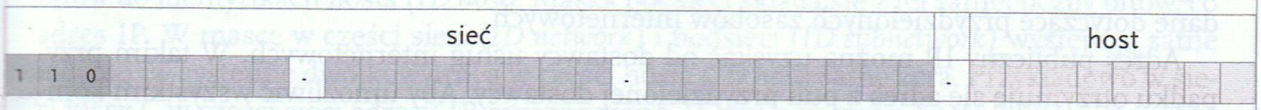
Adresy **klasy B** przeznaczono do obsługi sieci dużych i średnich. Pierwsze dwa oktety adresu IP klasy B oznaczają numer sieci, a pozostałe dwa – numer hosta. Podział bitów w adresie klasy B pokazano na rys. 14.5.



Rys. 14.5. Podział bitów w adresie klasy B

Pierwsze dwa bity pierwszego oktetu adresu klasy B wynoszą 10 (dwójkowo), natomiast pozostałe są dowolne. Adresy klasy B obejmują zakres od 128.0.0.0 do 191.255.255.255. Wartość pierwszego oktetu adresu klasy B mieści się w zakresie od 128 do 191. Ostatnie 16 bitów (2 oktety) określa dopuszczalne adresy hostów. Każda sieć klasy B może obsługiwać 65 534 hosty (wyłączone są adresy specjalne).

Adresy **klasy C** przeznaczono do obsługi dużej liczby małych sieci. W adresie klasy C pierwsze trzy oktety określają sieć, a ostatni – hosta. Podział bitów w adresie klasy C pokazano na rysunku 14.6.



Rys. 14.6. Podział bitów w adresie klasy C

Pierwsze trzy bity pierwszego oktetu adresu klasy C wynoszą 110 (dwójkowo). Adresy klasy C obejmują zakres od 192.0.0.0 do 223.255.255.255. Każda sieć klasy C może obsługiwać 254 stacje (wyłączone są adresy specjalne). Maksymalnie może istnieć 2 097 150 sieci klasy C (2^{21} = 2 097 152).

Adresy **klasy D** służą do multiemisji (*multicast*) w sieciach IP. Adres multiemisji jest niepowtarzalnym adresem sieciowym, kierującym pakiety do zdefiniowanych z góry grup adresów IP. Jedna stacja może przesyłać strumień kierowany do wielu odbiorców jednocześnie. Przestrzeń adresowa klasy D obejmuje zakres od 224.0.0.0 do 239.255.255.255.

Adresy **klasy E** zespół IANA (*Internet Assigned Numbers Authority*) zarezerwował do własnych badań. Nie można korzystać z nich w Internecie (zakres prawidłowych adresów klasy E to 240.0.0.0 - 255.255.255.255).

W każdej z klas adresów dwa spośród nich były zarezerwowane do celów specjalnych. Adres, w którym w części przeznaczonej dla hosta znajdują się same zera (dwójkowo), jest **adresem sieci.** Adres, w którym w części przeznaczonej dla hosta znajdują się same jedynki, jest **adresem rozgłoszeniowym** (*broadcast*). Adresów tych nie można przypisać hostom. Ponadto istnieją jeszcze inne specjalne adresy opisane w tabeli 14.1.

Tabela 14.1. Adresy specjalne

Adres	Funkcja	Zastosowanie
0.0.0.0	Adres domyślnej trasy	Użycie w tablicach routingu
127.0.0.1	Adres pierwszej pętli zwrotnej	Komunikacja sieciowa hosta z samym sobą
255.255.255.255	Adres rozgłoszeniowy w sieci lokalnej	Komunikacja hosta ze wszystkimi hostami w ramach jednej sieci fizycznej

14.5. Translacja i przydzielanie adresów

Liczba komputerów przyłączonych do internetu ciągle rośnie. Za rozwój internetu w Europie odpowiada stowarzyszenie **RIPE** – Europejska Sieć IP (fr. *Reseaux IP Europeens*). Zadaniem stowarzyszenia jest administracyjna i techniczna koordynacja zadań i prac związanych z rozwojem i utrzymaniem internetu. Każdy z komputerów pracujących w sieci musi mieć unikatowy adres IP, przydzielony przez odpowiedni urząd – *Internet Assigned Numbers Authority* (IANA). Adresy takie są nazywane publicznymi; można je uzyskać w urzędzie IANA lub od naszego dostawcy usług internetowych. W takim wypadku otrzymujemy adres z puli przydzielonej naszemu dostawcy.

W Polsce NASK (Naukowa i Akademicka Sieć Komputerowa) prowadzi tzw. **Local Internet Registry** i przydziela adresy IP swoim klientom (również tym, którzy łączą się za pośrednictwem firm nieposiadających własnego rejestru, a dołączonych do NASK). Wszystkie informacje są rejestrowane w **RIPE NCC** (*RIPE Network Coordination Centre*), która jest osobną organizacją zajmującą się zarządzaniem zasobami internetowymi, takimi jak adresy IPv4 i IPv6. RIPE NCC przydziela adresy IP firmom i organizacjom ze swojego regionu, czyli także z Polski. Prowadzi również **bazę danych** (*RIPE Database*) zawierającą dane dotyczące przydzielonych zasobów internetowych.

Adres publiczny IP można uzyskać od dostawcy usług internetowych. W takim przypadku otrzymuje się adres z puli przydzielonej dostawcy. Aby umożliwić wszystkim komputerom w danej instytucji, np. w szkole, korzystanie z internetu, należałoby przydzielić każdemu z nich indywidualny adres publiczny. Sytuacja taka byłaby niekorzystna z powodu szybkiego wyczerpania dostępnej puli adresów. Aby rozwiązać ten problem, zarezerwowano pule **adresów prywatnych**. Adresy te można dowolnie stosować w sieciach lokalnych, nie są natomiast widoczne w Internecie. Adresy prywatne mogą się powtarzać w różnych sieciach lokalnych, nie powodując konfliktu.

Istnienie adresów prywatnych przewidziano dla każdej klasy adresów i zarezerwowano:

- dla klasy A adresy od 10.0.0.0 do 10.255.255.255 (jedna sieć z 16 777 214 hostów),
- dla klasy B adresy od 172.16.0.0 do 172.31.255.255 (16 sieci po 65 534 hosty),
- dla klasy C adresy od 192.168.0.0 do 192.168.255.255 (256 sieci po 254 hosty).

Komputery z adresami prywatnymi nie mogą bezpośrednio wymieniać danych w internecie. Jest to możliwe dopiero po przetłumaczeniu adresów prywatnych na adres publiczny za pomocą usługi **NAT** (*Network Address Translation*). Tłumaczenie adresów odbywa się w bramie internetowej umieszczonej między siecią prywatną a internetem.

W systemach Windows jest wykorzystywana usługa APIPA (*Automatic Private IP Addressing*). Usługa ta jest odpowiedzialna za automatyczne przydzielanie adresu IP komputerowi w przypadku, gdy karta sieciowa komputera jest skonfigurowana do żądania przyznania adresu IP z serwera DHCP, a serwer DHCP w danym momencie jest nieosiągalny. Adres IP jest przydzielany z puli 169.254.0.1 – 169.254.255.254 z domyślną maską 255.255.0.0. Gdy serwer DHCP stanie się osiągalny, komputer automatycznie uzyska adres IP z puli przyznawanej przez serwer.

14.6. Zapobieganie wyczerpywaniu się puli adresów

Początkowo sieć komputerowa zbudowana była z kilku komputerów. Dostępna liczba adresów (ponad 4 miliardy) wydawała się twórcom standardu IPv4 wystarczająca do zaspokojenia potrzeb użytkowników. Szybki rozwój sieci i przyłączanie nowych komputerów doprowadziły do sytuacji, w której zaczęło brakować dostępnych adresów. Inną przyczyną tego stanu było adresowanie klasowe. Jeżeli, na przykład, występuje konieczność przyłączenia do internetu sieci złożonej z 15 komputerów, to należy zarezerwować całą najmniejszą sieć klasy C. Sieć klasy C pozwala na zaadresowanie 254 hostów, co oznacza, że nie wykorzysta się 239 adresów (mimo zarezerwowania w IANA puli 254 adresów). Kolejną niedogodnością przyjętego schematu adresowania jest to, że na sieci klasy A przeznaczono połowę wszystkich dostępnych adresów. Ponieważ tych sieci jest tylko 126, trudno jest znaleźć organizację, która będzie w stanie wykorzystać wszystkie adresy klasy A. Istnieje wiele metod zapobiegania wyczerpywaniu się adresów. Należą do nich m.in.:

- wykorzystanie adresów prywatnych,
- adresowanie bezklasowe,
- adresowanie IPv6.

14.7. Adresowanie bezklasowe

W celu zapewnienia większej elastyczności w przydzielaniu adresów IP wprowadzono pojęcie **maski podsieci** (*Subnetwork Mask*), oznaczonej skrótem SM. Maska podsieci określa, ile bitów w adresie jest przeznaczonych do identyfikacji sieci i podsieci (*ID network*), a ile bitów do identyfikacji hosta (*ID host*). Maska podsieci składa się z tej samej liczby bitów, co adres IP. W masce w części sieci (*ID network*) i podsieci (*ID subnetwork*) występują same jedynki (w systemie dwójkowym), a w części hosta (*ID host*) same zera. Przykładowo w sieci klasy C w części sieci adresu IP przeznaczono 24 bity, a w części hosta 8 bitów. Przykład reprezentacji maski dla tej sieci przedstawiono w tabeli 14.2.

Tabela 14.2. Reprezentacja maski podsieci

Reprezentacja dwójkowa	11111111	–	11111111	–	11111111	–	00000000
Reprezentacja dziesiętna	255	–	255	–	255	–	0
Reprezentacja krótka	/24	–		–		–	

Reprezentacja krótka maski podsieci, zwana również notacją CIDR (*Classless Inter-Domain Routing*), informuje o ilości jedynek występujących w zapisie dwójkowym maski. Dzięki masce podsieci można wydzielić podsieci z mniejszą liczbą komputerów, niż wynikałoby to z użycia pełnej klasy adresów. Aby utworzyć podsieć, należy wykorzystać bity z części przeznaczonej na hosta. Jeśli zostaną wykorzystane trzy bity z części przeznaczonej na hosta, to otrzyma się podział bitów na poszczególne części i wartości maski podsieci taki, jak na rysunku 14.7.

	sieć																								podsieć			host					
IP	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1				
SM	255								-	255								-	255								-	224						
	/27																																	

Rys. 14.7. Podział bitów w adresie sieci bezklasowej

Wyodrębnić podsieci można również w sieciach klasy A i B. Należy jednak pamiętać, że do tworzenia podsieci zawsze wykorzystuje się bity z części przeznaczonej na hosta.

PRZYKŁAD 14.3.

Wyznaczanie adresu sieci

Każdy z komputerów, któremu przydzielono adres IP, musi należeć do jakiejś sieci. Aby ustalić, do jakiej sieci należy komputer, konieczne jest wykonanie obliczeń w systemie dwójkowym. W tym celu należy najpierw przedstawić adres komputera i jego maski podsieci w systemie dwójkowym. Omówiony zostanie przykład komputera o adresie 192.168.0.123 i masce podsieci 255.255.255.224. Adres komputera w postaci dwójkowej pokazano na rysunku 14.8, a maski podsieci na rysunku 14.9.

	192								168								0								123							
IP	1	1	0	0	0	0	0	0	-	1	0	1	0	1	0	0	0	-	0	0	0	0	0	0	0	0	-	0	1	1	1	1	0	1	1

Rys. 14.8. Adres komputera w postaci dwójkowej

	255								255								255								224							
SM	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	0	0	0	0	0

Rys. 14.9. Maska podsieci w postaci dwójkowej

Do jakiej podsieci należy ten komputer?
Aby odpowiedzieć na to pytanie, należy wykonać operację obliczania iloczynu logicznego na poszczególnych bitach adresu IP i maski podsieci.

Porada

Jeżeli nie wiesz, co to iloczyn logiczny bitów, postępuj według zasady zilustrowanej na rysunku 14.10:

- Przepisz z adresu IP (rys. 14.10, wiersz 2 – IP) wszystkie bity na pozycjach, w których w masce sieci i podsieci (wiersz 3 – SM) jest wartość 1.
- W pozostałych miejscach adresu sieci (wiersz 4.) wpisz 0.

	Te bity należy przekopiować																										W tych pozycjach wpisz 0							
IP	1	1	0	0	0	0	0	0	-	1	0	1	0	1	0	0	0	-	0	0	0	0	0	0	0	0	-	0	1	1	1	1	0	1	1
SM	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	0	0	0	0	0
	1	1	0	0	0	0	0	0	-	1	0	1	0	1	0	0	0	-	0	0	0	0	0	0	0	0	-	0	1	1	1	1	0	1	1
	192									168									0									96							

Rys. 14.10. Wyznaczanie adresu sieci

Komputer należy do podsieci 192.168.0.96.

PRZYKŁAD 14.4.

Wyznaczanie adresu rozgłoszeniowego

Adres rozgłoszeniowy (*broadcast*) to adres, dzięki któremu komputer może wysłać wiadomość do wszystkich urządzeń w danej sieci lub podsieci (domenie rozgłoszeniowej). Aby ustalić adres rozgłoszeniowy w danej sieci, należy także wykonać obliczenia w systemie dwójkowym. W tym celu zostanie przedstawiony adres komputera i jego maski podsieci w systemie dwójkowym. Omówiony zostanie ten sam przykład: komputer o adresie 192.168.0.123 i masce podsieci 255.255.255.224. Adres komputera w postaci dwójkowej pokazano na rysunku 14.8, a maski podsieci na rysunku 14.9.

Jaki jest adres rozgłoszeniowy w tej podsieci?

Porada

Aby odpowiedzieć na to pytanie, postępuj, jak pokazano na rys. 14.11:

- Przepisz z adresu IP wszystkie bity na pozycjach, w których w masce podsieci jest wartość „1".
- W pozostałych miejscach wpisz 1.

	Te bity należy przekopiować																										W tych pozycjach wpisz 1							
IP	1	1	0	0	0	0	0	0	-	1	0	1	0	1	0	0	0	-	0	0	0	0	0	0	0	0	-	0	1	1	1	1	0	1	1
SM	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	0	0	0	0	0
	1	1	0	0	0	0	0	0	-	1	0	1	0	1	0	0	0	-	0	0	0	0	0	0	0	0	-	0	1	1	1	1	1	1	1
	192									168									0									127							

Rys. 14.11. Wyznaczanie adresu rozgłoszeniowego

Adres rozgłoszeniowy w tej podsieci to 192.168.0.127.

PRZYKŁAD 14.5.

Obliczanie ilości podsieci

Liczba możliwych do utworzenia podsieci zależy od liczby bitów z części hosta przeznaczonych do utworzenia podsieci. W powyższym przykładzie na podsieci zostały przeznaczone 3 bity. Na 3 bitach można reprezentować 2^3 (= 8) różnych wartości i tyle podsieci możemy utworzyć. Jednak pierwsza i ostatnia z tych podsieci nie będzie mogła być wykorzystana, chyba że wszystkie urządzenia w sieci spełnią dodatkowe warunki dotyczące wymagań sprzętowych i programowych. Pierwsza podsieć ma taki sam adres sieci, jak cała klasa C, natomiast ostatnia ma taki sam adres rozgłoszeniowy jak klasa C. Efektywnie spośród 8 podsieci możemy wykorzystać tylko 6.

Oblicz liczbę podsieci, które można wydzielić z podsieci 172.16.0.0, przy zastosowaniu maski 255.255.192.0.

PRZYKŁAD 14.6.

Obliczanie liczby hostów w danej podsieci

Liczba możliwych hostów w podsieci zależy od liczby bitów w części hosta. W powyższym przykładzie na część hosta pozostało 5 bitów. Na 5 bitach można reprezentować 2^5 (= 32) wartości. Jednak adres zawierający w części hosta same zera jest adresem podsieci, natomiast adres zawierający w części hosta same jedynki jest adresem rozgłoszeniowym podsieci. Adresy te są zarezerwowane i nie wolno ich przypisać do żadnego urządzenia w sieci. Oznacza to, że w omawianej podsieci może być maksymalnie 30 hostów.

Oblicz liczbę adresów, które można przypisać hostom w podsieci 172.16.0.0, przy zastosowaniu maski 255.255.252.0.

Uwaga

Minimalna liczba bitów przeznaczona na część podsieci adresu IP wynosi 2. Jeżeli na część podsieci zostanie przeznaczony 1 bit, to liczba podsieci wyniesie 2, a liczba podsieci efektywnych 0 – tzn. nie moglibyśmy utworzyć podsieci. Liczba bitów przeznaczona na część hosta adresu IP nie może być mniejsza niż 2 – liczba hostów w takiej podsieci wynosi 2.

PRZYKŁAD 14.7.

Przydzielanie adresów IP

W tabeli 14.3 zebrano wszystkie informacje o adresach w sieci analizowanej we wcześniejszym przykładzie.

Tabela 14.3. Adresy w podsieci

Numer podsieci	Adres sieci	Adresy hostów	Adres rozgłoszeniowy	Uwagi
0	192.168.0.0	192.168.0.1 do 192.168.0.30	192.168.0.31	Adres całej sieci (podsieć możliwa do wykorzystania tylko w sieciach spełniających dodatkowe wymagania).
1	192.168.0.32	192.168.0.33 do 192.168.0.62	192.168.0.63	
2	192.168.0.64	192.168.0.65 do 192.168.0.94	192.168.0.95	
3	192.168.0.96	192.168.0.97 do 192.168.0.126	192.168.0.127	
4	192.168.0.128	192.168.0.129 do 192.168.0.158	192.168.0.159	
5	192.168.0.160	192.168.0.161 do 192.168.0.190	192.168.0.191	
6	192.168.0.192	192.168.0.193 do 192.168.0.222	192.168.0.223	
7	192.168.0.224	192.168.0.225 do 192.168.0.254	192.168.0.255	Adres rozgłoszeniowy całej sieci (podsieć możliwa do wykorzystania tylko w sieciach spełniających dodatkowe wymagania).

Postępując analogicznie jak w omówionym przykładzie, wypisz w tabeli wszystkie informacje o adresach w sieci 192.168.16.0 z maską 255.255.255.240.

PRZYKŁAD 14.8.

Sprawdzanie komunikacji między komputerami

Komputery będą mogły bezpośrednio komunikować się ze sobą, jeżeli będą w tej samej sieci, to znaczy będą miały taki sam adres sieci. Jeżeli adresy będą różne, to bezpośrednia komunikacja między nimi nie będzie możliwa. Aby sprawdzić, czy komputery będą mogły komunikować się w sieci, należy, jak w ćwiczeniu 14.3, wyznaczyć adresy sieci obu komputerów i je porównać. Na przykład weźmy dwa komputery, którym przydzielono adresy odpowiednio 10.20.30.40 i 10.20.30.140 oraz maskę podsieci 255.255.255.240. Na rysunku 14.12. pokazano sposób obliczania adresu sieci komputera o adresie 10.20.30.40.

	0	0	0	0	1	0	1	0	-	0	0	0	1	0	1	0	0	-	0	0	0	1	1	1	1	0	-	0	0	1	0	1	0	0	0
IP	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	1	0	0	0	0
SM	0	0	0	0	1	0	1	0	-	0	0	0	1	0	1	0	0	-	0	0	0	1	1	1	1	0	-	0	0	1	0	0	0	0	0
	10									20									30									32							

Rys. 14.12. Wyznaczanie adresu sieci komputera o adresie IP 10.20.30.40

Na rys. 14.13 przedstawiono sposób obliczania adresu sieci komputera o adresie 10.20.30.140.

	0	0	0	0	1	0	1	0	-	0	0	0	1	0	1	0	0	-	0	0	0	1	1	1	1	0	-	1	0	0	0	1	1	0	0
IP	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	1	0	0	0	0
SM	0	0	0	0	1	0	1	0	-	0	0	0	1	0	1	0	0	-	0	0	0	1	1	1	1	0	-	1	0	0	0	0	0	0	0
	10									20									30									32							

Rys. 14.13. Wyznaczanie adresu sieci komputera o adresie IP 10.20.30.140

Komputer o adresie 10.20.30.40 należy do sieci 10.20.30.32. Komputer o adresie 10.20.30.140 należy do sieci 10.20.30.128. Ponieważ adresy sieci są różne, komputery nie będą mogły bezpośrednio się komunikować.

Sprawdź, czy komputery o adresach 10.1.12.123 i 10.1.12.234, pracujące w sieci z maską 255.255.255.224, będą mogły się komunikować.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Jesteś administratorem szkolnej sieci komputerowej, która składa się z 6 pracowni komputerowych, a w każdej z nich jest po 13 komputerów, pracujących w różnych podsieciach. Twoim zadaniem jest przydzielenie komputerom adresów prywatnych z klasy C. Należy przydzielić komputerom adresy w taki sposób, aby jak najwięcej adresów pozostało do dyspozycji w przyszłości. Komputery nie mogą mieć możliwości wymiany danych z urządzeniami z innej pracowni. Określ:
   - maskę podsieci, jednakową dla wszystkich komputerów,
   - adres sieci i rozgłoszeniowy dla wszystkich podsieci,
   - adresy IP, jakie będą przypisane do komputerów w poszczególnych podsieciach,
   - maksymalną liczbę podsieci w szkole,
   - maksymalną liczbę komputerów w podsieci.

15 Zasady projektowania adresacji IP

ZAGADNIENIA

- **Jakie reguły obowiązują przy przydzielaniu adresów w sieci?**
- **W jakim celu stosowane są podsieci o zmiennej długości maski?**
- **Jak efektywnie zarządzać dostępnymi adresami IP?**

Podczas nadawania urządzeniom w sieci adresów IP należy przestrzegać następujących reguł:

- wszystkie urządzenia w jednym fizycznym segmencie sieci powinny mieć ten sam adres sieci;
- część adresu IP określająca hosta musi być unikatowa dla każdego urządzenia w segmencie sieci;
- nie można stosować adresów składających się z samych jedynek, tzn. 255.255.255.255 – jest to adres rozgłoszeniowy całej sieci;
- nie można stosować adresów, w których wszystkie bity mają wartość zero tzn. 0.0.0.0 – jest to adres używany w tablicach routingu do oznaczania trasy domyślnej;
- nie można stosować adresów, w których w części hosta są same zera – jest to adres podsieci;
- nie można stosować adresów, w których w części hosta są same jedynki – jest to adres rozgłoszeniowy podsieci;
- długość maski podsieci dobrać tak, aby zapewnić wystarczającą liczbę dostępnych adresów, dla wszystkich urządzeń w podsieci.

Podczas projektowania struktury adresów IP należy dobrać wielkości podsieci tak, aby maksymalnie wykorzystać dostępne adresy, a jednocześnie struktura adresów była czytelna dla administratora sieci i użytkowników. W celu lepszego wykorzystania dostępnych adresów wprowadzono technikę **podsieci o zmiennej długości maski VLSM** (*Variable Length Subnet Mask*). Technika ta pozwala na używanie w jednej przestrzeni adresowej wielu masek sieci o różnej długości. Zastosowanie tej techniki jest jednak możliwe tylko w sieciach korzystających z nowoczesnych protokołów routingu, takich jak OSPF, EIGRP lub RIPv2.

PRZYKŁAD 15.1.

Projektowanie sieci z wykorzystaniem techniki VLSM

Sieć (rys. 15.1) obejmuje 5 miast: Sieradz i Łódź (po 10 komputerów w podsieci), Warszawa, Wrocław i Poznań (po 25 komputerów w podsieci). Należy przydzielić każdej podsieci odpowiednią ilość adresów IP z puli adresów klasy C, np. 192.168.1.0 z maską 255.255.255.0.

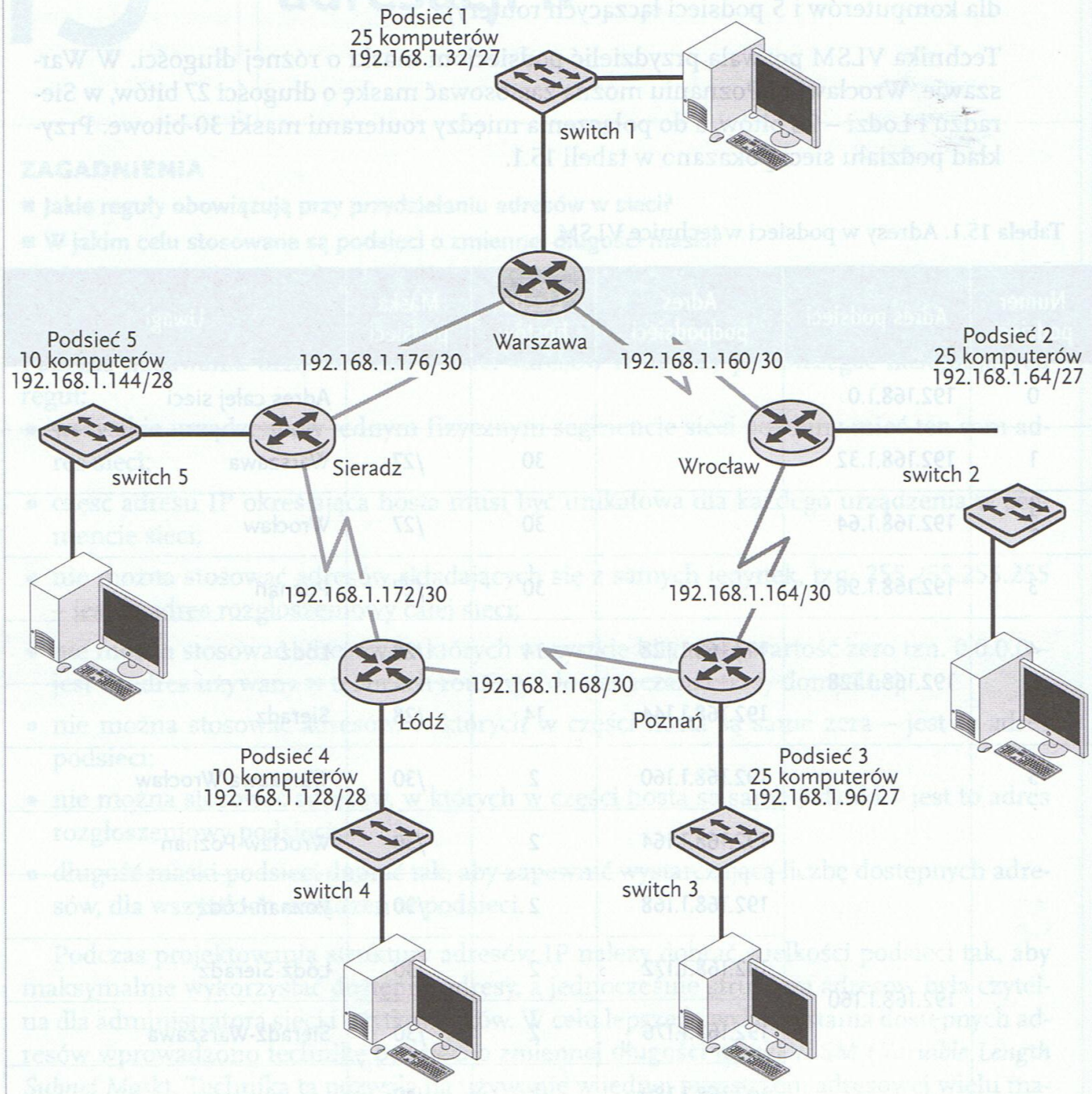
Liczba komputerów w największej podsieci wynosi 25. Na część hosta należy więc przeznaczyć 5 bitów. Na adres podsieci pozostają 3 bity, co pozwala na efektywne zaadresowanie 6 podsieci. Zastosowanie jednakowej maski do wszystkich podsieci powoduje, że w każdej podsieci pozostaną niewykorzystane adresy, natomiast dla czterech podsieci zabraknie adresów z dostępnej puli (należy utworzyć 5 podsieci dla komputerów i 5 podsieci łączących routery).

Technika VLSM pozwala przydzielić podsieciom maski o różnej długości. W Warszawie, Wrocławiu i Poznaniu można zastosować maskę o długości 27 bitów, w Sieradzu i Łodzi – 28 bitów, a do połączenia między routerami maski 30-bitowe. Przykład podziału sieci pokazano w tabeli 15.1.

Tabela 15.1. Adresy w podsieci w technice VLSM

Numer podsieci	Adres podsieci	Adres podpodsieci	Liczba hostów	Maska podsieci	Uwagi
0	192.168.1.0				Adres całej sieci
1	192.168.1.32		30	/27	Warszawa
2	192.168.1.64		30	/27	Wrocław
3	192.168.1.96		30	/27	Poznań
4	192.168.1.128	192.168.1.128	14	/28	Łódź
		192.168.1.144	14	/28	Sieradz
5	192.168.1.160	192.168.1.160	2	/30	Warszawa-Wrocław
		192.168.1.164	2	/30	Wrocław-Poznań
		192.168.1.168	2	/30	Poznań-Łódź
		192.168.1.172	2	/30	Łódź-Sieradz
		192.168.1.176	2	/30	Sieradz-Warszawa
		192.168.1.180	2	/30	
		192.168.1.184	2	/30	
		192.168.1.188	2	/30	
6	192.168.1.192		30	/27	
7	192.168.1.224				Adres rozgłoszeniowy całej sieci

Dzięki technice VLSM można nie tylko przydzielić każdej z podsieci wymaganą liczbę adresów, ale jeszcze część adresów pozostanie wolna z możliwością wykorzystania w przyszłości.



Rys. 15.1. Schemat adresowania sieci w technice VLSM

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Na potrzeby sieci komputerowej przeznaczono jedną podsieć klasy B. Zaprojektuj strukturę adresów IP dla sieci obejmującej 7 miast: Warszawa i Moskwa po 50 hostów, Berlin i Praga po 20 hostów, Paryż, Londyn i Rzym po 12 hostów. Dobierz schemat adresowania, w którym do wszystkich podsieci zastosowano jednakową maskę podsieci oraz schemat z maskami o zmiennej długości. Podaj adresy sieci i rozgłoszeniowe oraz zakresy dopuszczalnych adresów dla każdej podsieci, zakładając, że maksymalna liczba adresów powinna pozostać do wykorzystania w przyszłości.

16 Adresowanie IPv6

ZAGADNIENIA

- **W jakim celu wprowadzono protokół IPv6?**
- **Jak reprezentowane są adresy IPv6?**
- **Jakie typy adresów obsługuje IPv6?**

Adresowanie IPv6 wprowadzono ze względu na wyczerpywanie się dostępnej puli adresów IPv4. Adresy IPv6 mają długość 128 bitów, co pozwala na uzyskanie 2^{128} adresów ($3{,}4 \cdot 10^{38}$). Protokół IPv6 nie jest zgodny z protokołem IPv4. Aby host lub router rozpoznawał i przetwarzał obie wersje adresów, musi korzystać zarówno z protokołu IPv4, jak i IPv6. Protokół IPv6 obsługuje zarówno konfigurację adresów przy wykorzystaniu serwera DHCP, jak i bez tego serwera. Do IPv6 dodano nową wersję protokołu dynamicznej konfiguracji hostów DHCPv6 (*Dynamic Host Configuration Protocol for IPv6*) umożliwiającego komputerom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci. Jego specyfikacja została opisana w RFC 3315. Hosty podłączone do tego samego łącza mogą automatycznie konfigurować dla siebie adresy lokalne dla łącza i komunikować się bez konfiguracji ręcznej. Adres IPv6 składa się ze 128 bitów podzielonych na 16-bitowe fragmenty, oddzielone dwukropkami. Każdy 16-bitowy blok reprezentowany jest za pomocą 4-cyfrowej liczby szesnastkowej, np. adres:
0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010
reprezentowany jest:
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

Reprezentacja IPv6 może zostać uproszczona poprzez usunięcie poprzedzających zer z każdego 16-bitowego bloku. W tym uproszczeniu każdy blok musi posiadać przynajmniej jeden znak. Po pominięciu poprzedzających zer reprezentacja adresu wygląda następująco:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

Dozwolone jest pominięcie ciągu bloków składających się wyłącznie z zer. Pomijając bloki zer, wprowadza się separator bloków :: (podwójny dwukropek). Dopuszczalny jest tylko jeden podwójny dwukropek :: w adresie. Poniższe adresy są równoznaczne:

2001:0db8:0000:0000:0000:0000:1234: abcd
2001:0db8:0:0:0:0:1234: abcd
2001:0db8:0:0:: 1234: abcd
2001:0db8:: 1234: abcd
2001:db8:: 1234: abcd

W adresacji wykorzystywanej w protokole IPv6 używane są trzy typy adresów:

- **unicast** – identyfikujące pojedynczy interfejs,
- **multicast** – identyfikujące grupę interfejsów (mogą one należeć do różnych węzłów),
- **anycast** – podobnie jak adresy multicast, identyfikują one grupę interfejsów, jednak pakiet wysyłany na adres anycast jest dostarczany do najbliższego węzła, np. najbliższego serwera DNS.

W protokole IPv6 nie występuje pojęcie komunikacji broadcastowej (dane rozsyłane do wszystkich węzłów w danej podsieci). Aby wysyłać dane do wielu odbiorców jednocześnie, należy korzystać z komunikacji multicastowej. W IPv6 rozróżniane są zakresy adresów:

Adresy lokalne dla łącza (*link-local address*) – wykorzystywane tylko do komunikacji w jednym segmencie sieci lokalnej lub przy połączeniu typu point-to-point. Routery nie przekazują pakietów z adresami lokalnymi. Adresy te mają prefiks FE80::/10. Każdy interfejs musi mieć przydzielony co najmniej jeden adres lokalny dla łącza, nawet jeżeli posiada adres globalny lub unikalny adres lokalny. Zakres ten odpowiada zakresowi APIPA w IPv4 (169.254.0.0/16).

Unikalne adresy lokalne (*unique local adress*) – adresy będące odpowiednikami adresów prywatnych z protokołu IPv4. Adresy te mają prefiks FC00::/7.

Adresy globalne (*global unicast address*) – adresy będące odpowiednikami adresów publicznych z protokołu IPv4. Adresy te to wszystkie inne nie wymienione we wcześniejszych punktach.

W protokole IPv6 zdefiniowano również adresy specjalne, np.:

- ::/128 – adres nieokreślony (zawierający same zera);
- ::1/128 – pętla zwrotna (*loopback*) – adres wskazujący na host lokalny;
- 2001:db8::/32 – pula wykorzystywana w przykładach i dokumentacji – nigdy nie będzie wykorzystywana produkcyjnie;
- ff00::/8 – pula multicastowa używana do komunikacji multicast.

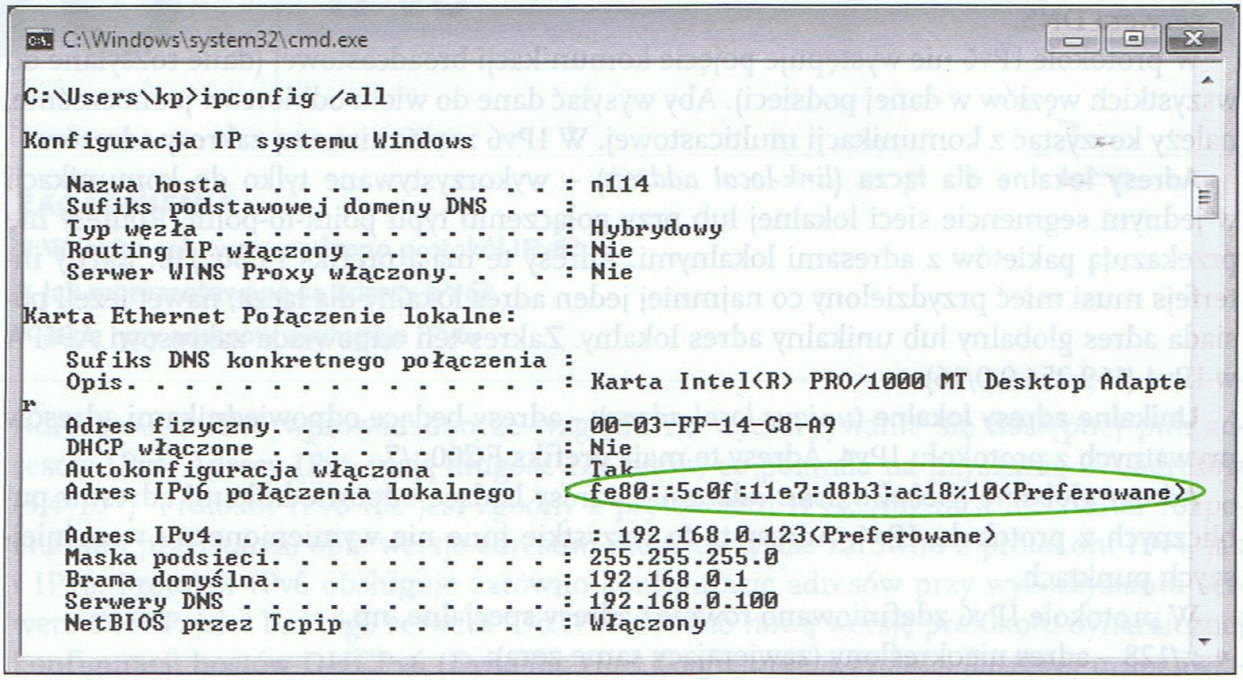
Nagłówek pakietu w protokole IPv6 został uproszczony (składa się z mniejszej liczby pól) i jest łatwiejszy w przetwarzaniu przez routery. Składa się z nagłówka podstawowego i nagłówków rozszerzających. Nagłówki rozszerzające, następujące po nagłówku głównym IPv6, są opcjonalne i zawierają dodatkowe opcje protokołu.

W skład podstawowego nagłówka wchodzą pola:

- wersja (4 bity) – definiująca wersję protokołu, w przypadku IPv6 pole to zawiera wartość 6 (bitowo 0110);
- klasa ruchu (8 bitów) – określa priorytet przesyłania pakietu (odpowiednik pola *Type of Service* z IPv4);
- etykieta przepływu (20 bitów) – pole służące do oznaczania strumienia pakietów IPv6;
- długość danych (16 bitów) – wielkość pakietu, nie wliczając długości podstawowego nagłówka (wliczając jednak nagłówki rozszerzające);
- następny nagłówek (8 bitów) – identyfikuje nagłówek rozszerzający występujący bezpośrednio po nagłówku IPv6;
- limit przeskoków (8 bitów) – ilość węzłów sieci, po przejściu których pakiet zostaje usunięty z sieci (odpowiednik pola TTL z IPv4);
- adres źródłowy (128 bitów) – adres węzła, który wysłał pakiet;
- adres docelowy (128 bitów) – adres węzła, do którego adresowany jest pakiet.

Na rysunku 16.1 ramką zakreślono adres IPv6, przypisany do połączenia lokalnego w komputerze z zainstalowanym systemem Windows 7. Adresy IPv6 można skonfigurować również w systemie Windows XP i we wszystkich nowszych od XP oraz w większości nowych dystrybucji Linuksa.

Mimo zalet oraz gotowości systemów operacyjnych do obsługi, adresowanie IPv6 nie jest jeszcze powszechnie stosowane. Jest to spowodowane koniecznością wymiany sprzętu sieciowego (lub przynajmniej oprogramowania) u dostawców internetu, co jest operacją kosztowną i wymaga czasu.



Rys. 16.1. Konfiguracja adresu IPv6 połączenia lokalnego

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sprawdź, czy Twój komputer ma przydzielony adres IPv6 (polecenie ipconfig).
   - Jeżeli Twój komputer ma przydzielony adres IPv6, to sprawdź, czy odpowiada na ping (polecenie ping -6 ::1).
   - Jeżeli Twój komputer ma przydzielony adres IPv6, to sprawdź, czy komputer kolegi odpowiada na ping (polecenie ping -6 <adresIPv6>).

17 Protokoły warstwy transportowej

ZAGADNIENIA

- **Jakie protokoły używane są w warstwie transportowej?**
- **Jak zbudowane są nagłówki protokołów warstwy transportowej?**
- **Do czego są wykorzystywane porty i gniazda?**
- **Jak działa mechanizm potwierdzania odebrania segmentów danych?**
- **Do czego wykorzystywany jest protokół UDP?**

W warstwie transportowej w stosie protokołów TCP/IP może działać protokół połączeniowy TCP lub protokół bezpołączeniowy UDP.

Protokół **TCP** (*Transmission Control Protocol*) działa w warstwie transportowej w trybie połączeniowym. Korzystanie z trybu połączeniowego umożliwia zagwarantowanie dostarczenia danych do odbiorcy. Połączenia TCP są połączeniami wirtualnymi, rozpoznawanymi po adresach i portach urządzeń docelowych i źródłowych. Połączenia takie charakteryzują się możliwościami sterowania przepływem, potwierdzaniem odbioru, zachowywaniem kolejności danych, kontrolą błędów i przeprowadzaniem retransmisji. Segmenty TCP składają się z nagłówka i danych. Budowa nagłówka TCP jest pokazana na rysunku 17.1.

Najważniejszymi polami nagłówka TCP są:

- port źródłowy,
- port docelowy,
- numer sekwencyjny,
- numer potwierdzenia,
- szerokość okna.

<table>
<tr><td colspan="2">1 bajt</td><td>2 bajt</td><td colspan="2">3 bajt</td><td>4 bajt</td></tr>
<tr><td colspan="3">Port źródłowy</td><td colspan="3">Port docelowy</td></tr>
<tr><td colspan="6">Numer sekwencyjny</td></tr>
<tr><td colspan="6">Numer potwierdzenia</td></tr>
<tr><td>Dł. Nag.</td><td>Rezerwa</td><td>Znaczniki</td><td colspan="3">Wskaźnik pilności</td></tr>
<tr><td colspan="5">Opcje</td><td></td></tr>
<tr><td colspan="6">Dane</td></tr>
</table>

Rys. 17.1. Budowa segmentu TCP

Ponieważ na komputerze posiadającym jeden adres IP może jednocześnie działać wiele aplikacji, to do ich identyfikacji wykorzystuje się **porty.** Porty reprezentowane są przez liczby naturalne z zakresu od 0 do 65535. Numery portów od 0 do 1023 są ogólnie znane (*well-known port numbers*) i zarezerwowane dla usług, np. WWW korzysta z portu 80, a telnet z portu 23. Dzięki portom możemy określić, dla jakiej aplikacji jest przeznaczony segment danych (port docelowy) lub z którego portu wysłano dane (port źródłowy).

Komunikacja między aplikacjami może się odbywać za pomocą **gniazd** (*socket*). Gniazdo to kombinacja adresu IP i numeru portu. Jednoznacznie określa proces w sieci lub zakończenie logicznego łącza komunikacyjnego między dwoma aplikacjami. Jeśli aplikacje uruchomione są na dwóch różnych komputerach, to para odpowiadających im gniazd definiuje połączenie. Gniazdo możemy traktować jako kanał komunikacyjny – jeden program wpisuje do niego dane, a drugi je odbiera. Serwer otwiera gniazdo i oczekuje na połączenie. Klient łączący się z otwartym gniazdem musi znać sieciowy adres komputera oraz numer portu. Każdy przesyłany segment danych jest oznaczany kolejnym **numerem sekwencyjnym**. Przed rozpoczęciem transmisji nadawca i odbiorca wymieniają między sobą te numery. Odbiorca wiadomości na podstawie numeru sekwencyjnego ustala kolejność segmentów oraz sprawdza, czy wszystkie segmenty dotarły do miejsca przeznaczenia. Potwierdzenie odebrania segmentu polega na wysłaniu przez odbiorcę numeru kolejnego segmentu, który powinien być przesłany. Na przykład, jeżeli ostatni poprawnie odebrany segment miał numer 123, to odbiorca wyśle numer potwierdzenia 124 (numer następnego segmentu, który ma być przesłany). Potwierdzenie jest wysyłane po odebraniu pewnej liczby danych, określonych w polu **okno**. Jeżeli w sieci występuje dużo błędów, to wielkość okna jest zmniejszana, aby częściej otrzymywać potwierdzenia i przez to zmniejszyć liczbę segmentów danych wymagających retransmisji. Jeżeli liczba błędów się zmniejsza, to rozmiar okna jest powiększany, aby zapewnić większą przepustowość sieci.

Protokół UDP (*User Datagram Protocol*) działa w warstwie transportowej w trybie bezpołączeniowym. Protokół ten nie gwarantuje dostarczenia danych do odbiorcy. Jeżeli pakiet nie dotrze do odbiorcy lub dotrze uszkodzony, UDP nie podejmie żadnych działań zmierzających do retransmisji danych, a zapewnienie niezawodności pozostawi warstwie wyższej. Nagłówek protokołu UDP (rys. 17.2) jest prostszy niż TCP. Protokół jest wykorzystywany do szybkiego przesyłania danych w niezawodnych sieciach.

1 bajt	2 bajt	3 bajt	4 bajt
Port źródłowy		Port docelowy	
Długość		Suma kontrolna	
Dane			

Rys. 17.2. Budowa datagramu UDP

Dzięki temu, że istnieją dwa alternatywne względem siebie protokoły w warstwie transportowej, TCP i UDP, jest możliwy dobór przez aplikacje odpowiedniego dla siebie rozwiązania.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyszukaj w internecie, np. na stronie http://pl.wikipedia.org/wiki/User_Datagram_Protocol informacje dotyczące zastosowania protokołu UDP.
2. Wyszukaj w internecie, np. na stronie http://pl.wikipedia.org/wiki/Port_protokołu numerów portów, z których korzystają protokoły: DNS, DHCP, FTP, TFTP, TELNET, SSH.

18 Protokoły warstwy aplikacji

ZAGADNIENIA

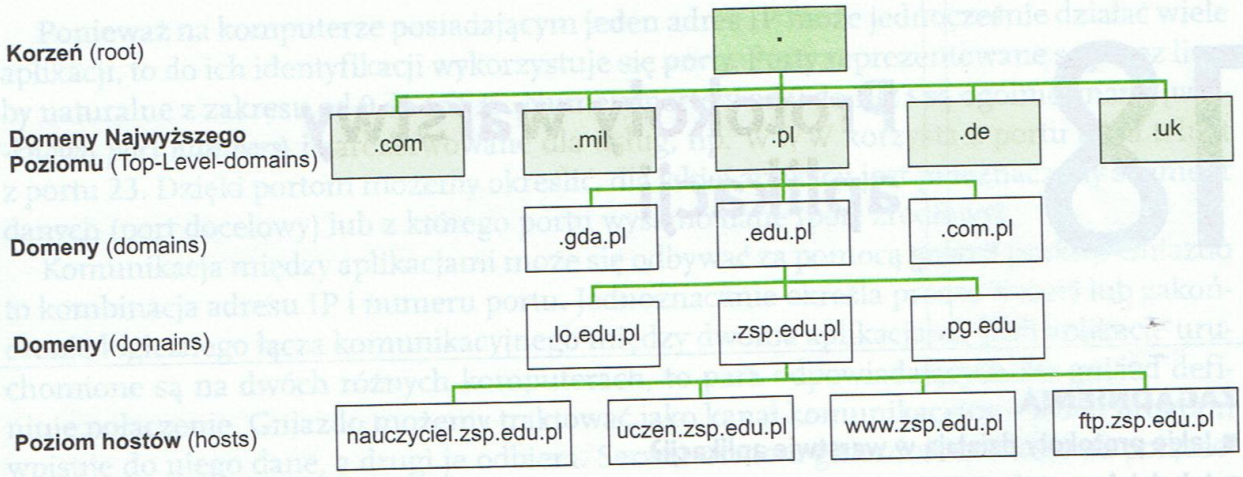
- **Jakie protokoły działają w warstwie aplikacji?**
- **Jak działa system DNS?**
- **Kto zajmuje się rejestrowaniem nazw domenowych?**
- **Czym są domeny najwyższego poziomu?**
- **Jakie jest przeznaczenie głównych serwerów nazw?**
- **Jak sprawdzić działanie systemu DNS?**

W warstwie aplikacji modelu TCP/IP funkcjonuje wiele protokołów umożliwiających świadczenie usług dla użytkowników. Podczas przesyłania danych przez sieci dane mogą być przesyłane za pomocą różnych technologii. Dla autora listu poczty elektronicznej pracującego w warstwie aplikacji nie ma znaczenia, czy jego list przesyłany będzie do internetu za pomocą sieci lokalnej, modemu, DSL (*Digital Subscriber Line*) czy innej technologii. Dane mogą być przesyłane przy wykorzystaniu różnych mediów, np. najpierw z laptopa za pomocą fal radiowych, później kablem miedzianym, a w końcu łączem światłowodowym. Dzięki standaryzacji warstwa aplikacji jest niezależna od protokołów warstw niższych oraz używanych mediów transmisyjnych. Aplikacje mogą być wykorzystywane niezależnie od tego, czy pracujemy w sieci lokalnej, czy globalnej. Najczęściej używanymi protokołami warstwy aplikacji są:

- **FTP** (*File Transfer Protocol*) – do przesyłania plików w sieci,
- **HTTP** (*Hypertext Transfer Protocol*) – do pobierania stron WWW,
- **SMTP** (*Simple Mail Transfer Protocol*) – do wysyłania poczty elektronicznej,
- **POP3** (*Post Office Protocol v* 3) – do pobierania poczty elektronicznej,
- **IMAP** (*Internet Message Access Protocol*) – do pobierania poczty elektronicznej,
- **DNS** (*Domain Name System*) – do zamiany nazw domenowych na adresy IP,
- **TFTP** (*Trivial File Transfer Protocol*) – uproszczona wersja protokołu FTP wykorzystywana np. do instalacji systemów operacyjnych w urządzeniach sieciowych, takich jak routery lub przełączniki.

Większość z wymienionych wyżej protokołów wykorzystywana jest przez usługi umożliwiające wykonanie określonych zadań w sieci, np. wysłanie lub odebranie poczty elektronicznej, pobranie pliku lub strony WWW. Wyjątkiem jest usługa DNS.

Korzystając z sieci komputerowej, należy zidentyfikować komputer, z którego zasobów chce się skorzystać. W tym celu można wykorzystać jego adres IP, ale zapamiętanie długiego ciągu liczb jest dla przeciętnego użytkownika trudne. Ludzie łatwiej zapamiętują nazwy niż ciągi liczb. Komputerom w sieci zaczęto więc nadawać unikatowe nazwy wykorzystywane do ich identyfikacji. Nazwy te tworzą drzewiastą strukturę domen. Uproszczony schemat struktury domen pokazano na rysunku 18.1.



Rys. 18.1. Schemat struktury domen

Poszczególne domeny są oddzielone od siebie kropkami. Na samym szczycie drzewa znajdują się **Domeny Najwyższego Poziomu** (*Top-Level-Domains*). Domeny te grupują serwery według ich przeznaczenia, np.:

- .com – instytucje komercyjne,
- .edu – instytucje edukacyjne,
- .gov – instytucje państwowe, agendy rządowe,
- .mil – organizacje wojskowe,
- .net – firmy oferujące usługi sieciowe,
- .org – organizacje niekomercyjne,

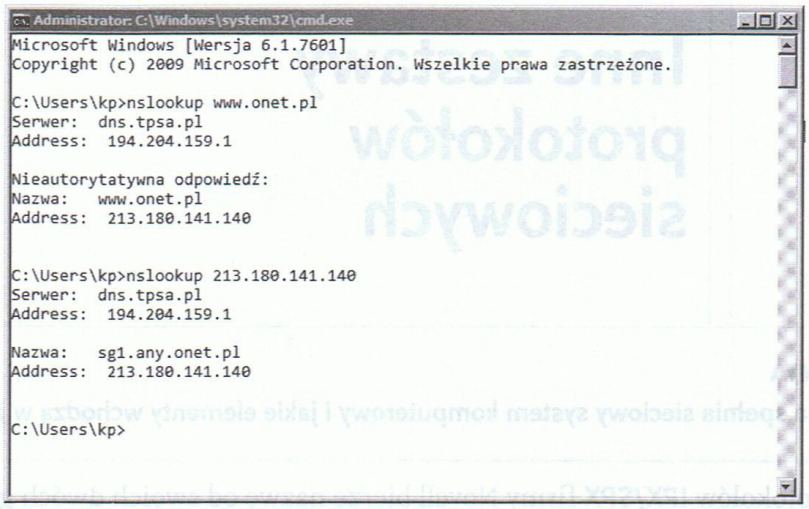
lub położenia geograficznego, np.:

- .pl – Polska,
- .it – Włochy,
- .de – Niemcy,
- .fr – Francja itd.

Lista domen krajowych i funkcjonalnych jest uzupełniana, tworzona i zarządzana przez organizację IANA (*Internet Assigned Numbers Authority*) i korporację ICANN (*The Internet Corporation for Assigned Names and Numbers*). Nowe domeny są tworzone w ramach jednej z istniejących domen, np. onet.pl jest utworzona jako poddomena domeny .pl.

System **DNS** to hierarchiczna usługa nazw przeznaczona dla hostów w sieci TCP/IP. Pozwala nadawać komputerom świadczącym pewne usługi w sieci nazwy domenowe i tłumaczy je na używane przez komputery adresy IP. Gdy w przeglądarce internetowej wpisze się w okno adres domeny internetowej (adres mnemoniczny), przeglądarka komunikuje się z serwerami DNS i uzyskuje informacje o adresie IP komputera, na którego dysku są umieszczone pliki danej strony. System DNS jest rozproszoną bazą danych obsługiwaną przez wiele serwerów, z których każdy posiada tylko informacje o domenie, którą zarządza, oraz o adresie serwera nadrzędnego. Główne serwery nazw (*root level servers*) zlokalizowane są w Stanach Zjednoczonych i podłączone są do szybkich sieci szkieletowych internetu. Przechowują one adresy serwerów nazw dla domen najwyższego poziomu, np. **.com**, **.edu**, **.org**, oraz domen krajowych, np. **.pl**, **.de**, **.uk**. Adresy serwerów głównych muszą być znane każdemu innemu serwerowi nazw. Wewnątrz każdej domeny można tworzyć tzw. subdomeny, np. wewnątrz domeny **.pl** utworzono wiele domen regionalnych, jak **.waw.pl**, **.lodz.pl** itp., oraz funkcjonalnych, jak **.com.pl**, **.gov.pl** lub **.org. pl**, należących do firm, organizacji lub osób prywatnych.

Do testowania działania serwera DNS można wykorzystać narzędzie nslookup. Narzędzie to wysyła zapytanie do serwera oraz zwraca dokładne informacje dotyczące



Rys. 18.2. Wyszukiwanie danych w systemie DNS

poszukiwanego komputera. Jeżeli jako argumentu dla polecenia użyje się nazwy komputera, to uzyska się adres IP komputera (pod warunkiem, że taka nazwa istnieje w systemie DNS). Jeżeli jako argumentu dla polecenia użyje się adresu IP, to uzyska się nazwę komputera. Przykład działania polecenia nslookup jest pokazany na rys. 18.2. Aby móc testować działanie systemu DNS, należy ustawić w opcjach połączenia sieciowego adres serwera DNS.

PRZYKŁAD 18.1.

Wyszukiwanie informacji w systemie DNS

Uruchom wiersz polecenia systemu Windows. Za pomocą narzędzia nslookup sprawdź:

- adres IP serwera www.wp.pl oraz serwera udostępniającego stronę WWW Twojej szkoły,
- nazwę komputera o adresie IP: 194.204.159.1.

Ogólne zasady przyznawania nazw domen i adresów IP nadzorują dwie instytucje: **IANA** i **ICANN**. Instytucje te przekazują swoje uprawnienia na lokalne instytucje i firmy, np. w Polsce nadzór nad domeną **.pl** jako całością oraz obsługą rejestrowania domen takich, jak **.com.pl, .biz.pl, .org.pl, .net.pl** oraz innych domen funkcjonalnych, pełni **NASK** *(Naukowa i Akademicka Sieć Komputerowa)*. Aby móc pracować w internecie, komputer musi znać adresy IP serwerów DNS, które udzielają odpowiedzi na zapytania. Serwery te mogą być zlokalizowane poza domeną użytkownika, np. serwery openDNS, lub w obrębie domeny, co pozwala na szybsze uzyskanie odpowiedzi i samodzielne konfigurowanie wydzielonej poddomeny. Zazwyczaj dla każdej domeny utrzymywane są dwa niezależne serwery nazw, dzięki czemu w razie awarii lub zbyt dużego obciążenia **podstawowego serwera DNS** (*primary name server*) można korzystać z **serwera rezerwowego** (*secondary name server*). Informacje o hostach w obrębie domeny są replikowane na inne serwery DNS w celu poprawy odporności na uszkodzenia i/lub dla poprawy wydajności.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sprawdź adres IP podstawowego i zapasowego serwera DNS używanego w Twojej sieci.
2. W jakiej domenie umieszczona jest strona Twojej szkoły? Wypisz wszystkie domeny i poddomeny.

19 Inne zestawy protokołów sieciowych

ZAGADNIENIA

- **Jakie zadania spełnia sieciowy system komputerowy i jakie elementy wchodzą w jego skład?**

Zestaw protokołów **IPX/SPX** firmy Novell bierze nazwę od swoich dwóch głównych protokołów: międzysieciowej wymiany pakietów **IPX** (*Internet Packet Exchange*) i sekwencyjnej wymiany pakietów **SPX** (*Sequential Packet Exchange*). Protokół IPX/SPX zyskał popularność jako protokół wykorzystywany w sieci Novell NetWare. NetWare był faktycznym standardem sieciowego systemu operacyjnego dla sieci lokalnych w latach dziewięćdziesiątych XX w. Protokół IPX przypomina IP; jest protokołem bezpołączeniowym, który nie wymaga ani nie zapewnia potwierdzenia każdego transmitowanego pakietu. Protokół IPX korzysta z SPX w zakresie porządkowania kolejności i innych usług połączeniowych warstwy transportu. Protokół SPX jest protokołem połączeniowym, zapewniającym transmisję danych. SPX zapewnia niezawodność transmisjom IPX, zarządzając połączeniem i udostępniając sterowanie strumieniem danych, kontrolę błędów i porządkowanie kolejnych pakietów. Stos protokołów IPX/SPX obejmuje cztery warstwy funkcjonalne: dostępu do nośnika, łącza danych, internetu i aplikacji. Głównym protokołem warstwy aplikacji jest **protokół rdzenia NetWare** (NCP). Protokół NCP można wykorzystać do drukowania, współdzielenia plików, poczty elektronicznej i dostępu do folderów.

Protokół NetBEUI (*NetBIOS Extended User Interface*) został opracowany przez IBM. Jest małym, ale wydajnym protokołem komunikacyjnym. Nie wymaga wprowadzania żadnych informacji podczas konfiguracji, a stacje wyszukują obecne w sieci komputery za pomocą komunikatów rozgłoszeniowych. Jego zastosowanie ogranicza się do sieci lokalnych, w których pracują komputery wykorzystujące systemy operacyjne firmy Microsoft. Protokół ten do identyfikowania komputerów w sieci używa ich nazw i nie umożliwia wyznaczania tras, domyślnie był stosowany w sieci Windows 3.11 i Windows 95.

AppleTalk to zestaw protokołów komunikacyjnych stworzonych przez firmę Apple Computer, umożliwiających tworzenie sieci komputerowych i podstawowych usług sieciowych dla komputerów Macintosh. Urządzenia AppleTalk regularnie ogłaszają swoje nazwy w całej sieci. Stacje klienckie otrzymują listę wszystkich dostępnych urządzeń, co pozwala użytkownikowi na wybór urządzenia, z którym zamierza wymieniać dane. Firma Apple zaprzestała rozwijania protokołu AppleTalk i obecnie wykorzystuje w swoich produktach TCP/IP.

Najpopularniejszymi sieciowymi systemami operacyjnymi są: Novell NetWare, Microsoft Windows Server oraz systemy Unix i Linux.

II. Projektowanie lokalnych sieci komputerowych

- Komputerowe systemy sieciowe
- Zasady projektowania lokalnej sieci komputerowej
- Rodzaje materiałów i urządzeń do budowy sieci komputerowej
- Zasady doboru materiałów i urządzeń sieciowych
- Struktura dokumentacji projektowej
- Projektowanie okablowania strukturalnego
- Zasady sporządzania harmonogramu prac wykonawczych
- Zasady kosztorysowania prac
- Dokumenty źródłowe, pomocne przy sporządzaniu budżetu projektu
- Czytanie rzutów poziomych i pionowych budynków
- Obsługa przykładowych programów wspomagających projektowanie 2D
- Obsługa przykładowych programów kosztorysujących

20 Komputerowe systemy sieciowe

ZAGADNIENIA

- **Czym jest hierarchiczny model sieci komputerowej?**
- **Jakie funkcje realizują serwery i jakie są ich typy?**

Serwery, stacje robocze, urządzenia sieciowe i okablowanie to sprzętowy szkielet sieci, który wraz z oprogramowaniem sieciowym i użytkowym tworzy **komputerowy system sieciowy**. Do prawidłowego funkcjonowania tego systemu niezbędny jest odpowiedni sprzęt i oprogramowanie. Głównym celem komputerowego systemu sieciowego jest umożliwienie współużytkowania zasobów sieciowych, np. drukarek, dysków twardych i łączy komunikacyjnych, przez klientów sieci. Oprogramowanie sieciowe realizuje swoje funkcje niezależnie od posiadanego sprzętu i systemu operacyjnego. Przesyłanie danych poprzez sieć realizowane jest na podstawie modelu warstwowego sieci, np. ISO/OSI lub TCP/IP. Oprogramowanie sieciowe jest zbiorem współpracujących ze sobą programów. Niektóre z tych programów działają na komputerach pełniących rolę serwerów, inne z kolei działają na stacjach roboczych pełniących rolę klientów.

Na serwerach instalowane są **sieciowe systemy operacyjne**. Umożliwiają one równoczesny dostęp wielu użytkowników do baz danych, plików na dyskach, drukarek i innych urządzeń i jednocześnie sterują tym dostępem. Najpopularniejszymi sieciowymi systemami operacyjnymi są: Novell NetWare, Microsoft Windows Server oraz systemy Unix i Linux.

W sieci mogą występować serwery:

- **Serwery plików** – udostępniają klientom przestrzeń dysków twardych. Serwery plików obsługują żądania odczytu i zapisu danych, które są odbierane z programów użytkowych klientów. Przykładowo, serwer WWW, który odbierze od przeglądarki internetowej klienta żądanie udostępnienia strony, przygotowuje pliki i wysyła je do klienta. Do grupy serwerów plików zalicza się również serwery baz danych i serwery aplikacji, na których zazwyczaj działa dodatkowe oprogramowanie, np. system zarządzania bazą danych.
- **Serwery wydruków** – udostępniają drukarki do wspólnego użytkowania w sieci. Serwery wydruków przyjmują zadania drukowania z aplikacji działających na stacjach klienckich i przechowują je w postaci plików w specjalnym podkatalogu (buforze wydruku). Pliki zadań oczekują w kolejce na wolną drukarkę. Wydruk może następować w kolejności wpływania zadań lub na podstawie priorytetu przyznanego zadaniom.
- **Serwery komunikacyjne** – mogą działać jak bramy do sieci, umożliwiające komunikacje z innymi sieciami, np. internetem. Serwery komunikacyjne mogą również świadczyć usługi umożliwiające wymianę danych, np. poczty elektronicznej pomiędzy użytkownikami sieci lub pomiędzy urządzeniami, np. DNS, DHCP, proxy.

W każdej sieci może występować jeden lub kilka serwerów z każdego rodzaju. Serwery świadczące różne usługi mogą działać na tym samym komputerze w sieci lub zadania te mogą być rozdzielone na różne komputery.

Sieciowe systemy operacyjne składają się z wielu różnych modułów obsługujących poszczególne usługi. Ponadto występuje dodatkowe oprogramowanie wspomagające prace serwerów, np. obsługujące kolejki żądań, buforowanie dysku i kolejek do interfejsów sieciowych, zarządzanie zasobami w sieci.

Oprogramowanie sieciowe na stacjach roboczych (klientach) umożliwia korzystanie z zasobów sieciowych tak, jakby były one podłączone lokalnie. Dzięki temu aplikacje, z których korzystają użytkownicy stacji roboczych, nie muszą posiadać żadnych funkcji sieciowych. Przykładowo, edytując tekst, nie musimy zastanawiać się, czy zapisać plik na dysku lokalnym, na serwerze lub „w chmurze".

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Jakie serwery działają w Twojej szkole? Podaj ich adresy IP.
2. Sprawdź, jaki jest adres IP serwera WWW, na którym udostępniana jest strona Twojej szkoły.
3. Sprawdź, jaki jest adres IP serwera poczty elektronicznej, z którego korzystasz.

21 Zasady projektowania lokalnej sieci komputerowej

ZAGADNIENIA

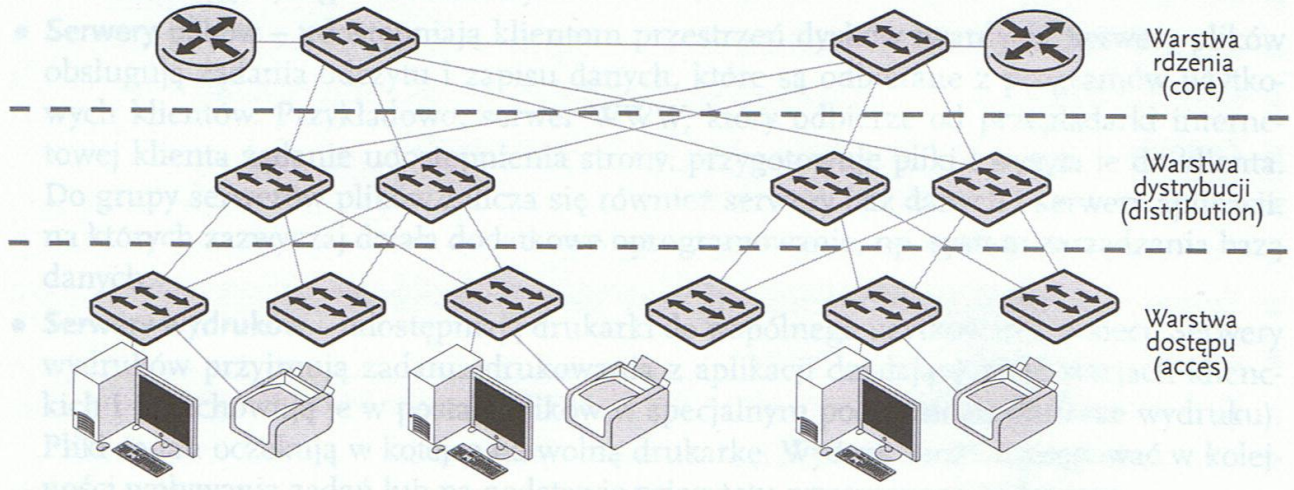
- **Co to jest model hierarchiczny sieci komputerowej?**
- **Z jakich warstw składa się model hierarchiczny?**
- **Jaką rolę pełnią warstwy w modelu hierarchicznym?**
- **Jakie cechy powinna mieć sieć komputerowa, aby można było nią łatwo zarządzać?**

Podczas projektowania architektury komutowanej sieci LAN (*switched LAN*) używa się modelu hierarchicznego sieci. Sieci w modelu hierarchicznym dzieli się na odrębne warstwy. Każda z nich realizuje określone funkcje, które definiują rolę danej warstwy w ogólnym modelu sieci. Budowa sieci przyjmuje postać modułową, co zwiększa jej skalowalność i efektywność działania.

W modelu hierarchicznym można wyróżnić trzy warstwy:

- warstwa dostępu (*access layer*),
- warstwa dystrybucji (*distribution layer*),
- warstwa rdzenia (*core layer*).

Sieć hierarchiczna jest łatwiejsza do zarządzania i rozbudowy, a ewentualne problemy rozwiązuje się szybciej. Na rysunku 21.1. pokazano model hierarchiczny sieci przełączanej. W małych sieciach stosuje się model uproszczony z 2 warstwami lub nie stosuje się modelu warstwowego.



Rys. 21.1. Model hierarchiczny budowy sieci przełączanej

Warstwa dostępu jest sprzężona z takimi urządzeniami końcowymi, jak komputery PC, drukarki i telefony IP, a jej celem jest zapewnienie dostępu do pozostałych składników danej sieci. Jej głównym zadaniem jest:

- umożliwienie połączenia urządzeń z siecią,
- umożliwienie kontroli nad komunikowaniem się urządzeń w sieci.

W warstwie dostępu mogą występować przełączniki, mosty, koncentratory i bezprzewodowe punkty dostępowe.

Warstwa dystrybucji gromadzi dane otrzymywane z przełączników z warstwy dostępu przed ich transmisją do warstwy rdzenia. Warstwa ta kontroluje przepływ danych w sieci oraz wyznacza domeny rozgłoszeniowe. Może również realizować routing między wirtualnymi sieciami LAN (*VLAN – Virtual LAN*), jeżeli na poziomie warstwy dostępu utworzono takie sieci.

Warstwę rdzenia stanowią szybkie łącza szkieletowe. W warstwie tej gromadzi się ruch sieciowy ze wszystkich urządzeń warstwy dystrybucji, a zatem musi być ona w stanie szybko przekazywać duże ilości danych. Warstwa rdzenia może być połączona z zasobami internetowymi.

Aby zapewnione zostały maksymalne korzyści przy minimalnym nakładzie pracy i środków, sieć komputerowa powinna posiadać następujące cechy:

- skalowalność,
- nadmiarowość,
- wydajność,
- bezpieczeństwo,
- łatwość zarządzania i utrzymania.

Skalowalność możemy rozumieć jako podatność sieci na rozbudowę. Rozrastanie się sieci o dużej skalowalności można łatwo zaplanować i realizować. Na przykład, przyjmijmy założenie, że na przełącznik z warstwy dystrybucji może przypadać dziesięć przełączników z warstwy dostępu. Wtedy dodatkowy przełącznik w warstwie dystrybucji trzeba będzie dodać do topologii sieci dopiero po przekroczeniu maksymalnej liczby dziesięciu podłączonych przełączników warstwy dostępu.

Zwiększenie niezawodności sieci można osiągnąć, wprowadzając **nadmiarowość** (redundancję) urządzeń lub/i ścieżek. W celu zapewnienia nadmiarowości poszczególne przełączniki z warstwy dostępu są łączone z więcej niż jednym przełącznikiem z warstwy dystrybucji (np. z dwoma różnymi przełącznikami z warstwy dystrybucji). Jeśli jeden z przełączników warstwy dystrybucji ulegnie awarii, to przełącznik z warstwy dostępu może współpracować z drugim przełącznikiem z tej warstwy. Z kolei przełączniki z warstwy dystrybucji są łączone z co najmniej dwoma przełącznikami z warstwy rdzenia. W warstwie dostępu nie występuje nadmiarowość – urządzenia końcowe (komputery, drukarki itp.) nie mogą być przyłączone do więcej niż jednego przełącznika. Jeśli w warstwie dostępu wystąpi awaria przełącznika, to będzie mieć wpływ tylko na urządzenia, które są do niego podłączone.

Wydajność komunikacji można poprawić, unikając transmisji danych przez niskowydajne przełączniki pośredniczące. W warstwie dystrybucji powinny być stosowane przełączniki o wydajności większej niż w warstwie dostępu. Przełączniki w warstwie rdzenia powinny mieć najwyższą wydajność, aby zapewnić szybkie przesyłanie dużej ilości danych. Zastosowanie w warstwie dostępu tańszych przełączników i zwiększenie nakładów na przełączniki z warstw dystrybucji i rdzenia pozwala uzyskać jednocześnie wysoką wydajność sieci i oszczędności finansowe.

Profesjonalne przełączniki umożliwiają zwiększenie **bezpieczeństwa** poprzez wprowadzenie zasad ograniczających dostęp do sieci. Przełączniki z warstwy dostępu można konfigurować, stosując różne opcje zabezpieczeń portów (*port security*) oraz sieci wirtualne VLAN, zapewniające kontrolę nad tym, które urządzenia mogą się łączyć z siecią.

W trakcie rozrastania się sieci jej utrzymanie staje się coraz bardziej skomplikowane. Urządzenia stosowane w danej warstwie powinny posiadać podobne parametry techniczne i konfigurację. Dla zapewnienia łatwości zarządzania **i utrzymania** można stosować jednakowe urządzenia. Jeśli trzeba będzie zmienić funkcjonalność jakiegoś przełącznika, np. z warstwy dostępu, to zmianę tę można powielić we wszystkich przełącznikach z tej warstwy, gdyż najprawdopodobniej wykonują one te same funkcje. Wdrażanie nowych przełączników jest ułatwione, ponieważ ich konfiguracje można skopiować z innych urządzeń i ewentualnie wprowadzić niewielkie modyfikacje.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zastanów się, czy sieć komputerowa w Twojej szkole została zbudowana zgodnie z modelem hierarchicznym. Jeśli nie, to co należałoby w niej zmienić?

22 Rodzaje materiałów i urządzeń do budowy sieci komputerowej

ZAGADNIENIA

- **Które urządzenia sieciowe zaliczane są do aktywnych, a które do pasywnych?**
- **Jaką rolę w sieci pełnią urządzenia aktywne i pasywne?**

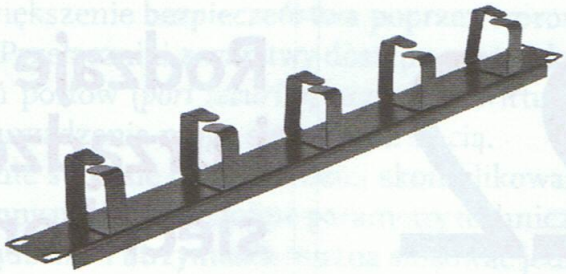
Sieć komputerowa jest systemem bardzo skomplikowanym, złożonym z wielu różnych urządzeń sieciowych aktywnych, pasywnych i oprogramowania. **Urządzenia aktywne**, takie jak koncentratory, przełączniki, routery, stanowią punkty, w których zbiegają się łącza prowadzące do serwerów, stacji roboczych i innych urządzeń sieciowych. Pomiędzy urządzeniami aktywnymi znajdują się **elementy pasywne**, nieprzetwarzające sygnału, a jedynie pośredniczące w ich przekazywaniu. Do elementów pasywnych zaliczamy:

- **Nośniki danych**, takie jak kable miedziane i światłowodowe.
- **Gniazda i wtyki komputerowe** – to końcówki, w których zarabiane są kable.
- **Szafy dystrybucyjne** – pozwalają na bezpieczne przechowywanie sprzętu aktywnego. Do szaf są prowadzone i zarabiane kable z pobliskich pomieszczeń, co zabezpiecza sieć przed dokonywaniem zmian w okablowaniu przez nieuprawnione osoby. Mogą być dodatkowo wyposażone w systemy wentylacji z termostatami, oświetlenia, półki, uchwyty do kabli itp.
- **Ramy montażowe** – pełnią taką samą funkcję, jak szafy, lecz nie są obudowane i zamykane.
- **Kanały kablowe** – umożliwiają bezpieczne prowadzenie kabli pomiędzy punktami dystrybucyjnymi i od szaf dystrybucyjnych do punktów abonenckich. Wykorzystywane są różne systemy prowadzania kabli, umożliwiające prowadzenie kabli pionowych i poziomych w różnych warunkach – wewnątrz i na zewnątrz budynków.
- **Panele krosowe** (*patch panel*) – służą do zarabiania kabli w szafach teleinformatycznych. Połączenia w szafie teleinformatycznej pomiędzy gniazdami panelu krosowego wykonuje się za pomocą krótkich kabli (tzw. patch cordów).
- **Organizery kabli** – ułatwiają prawidłowe prowadzenia kabli w szafach. Montowane są między panelami krosowymi. Dobrą praktyką jest korzystanie z nich pomiędzy przełącznikami i routerami. Ułatwiają organizowanie kabli w szafie.
- **Patch cord** – jest to krótki kabel sieciowy wykorzystywany do połączenia gniazd w panelach krosowych.

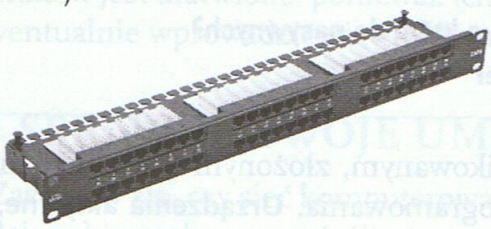
Wybrane urządzenia pasywne pokazano na rysunku 22.1.

a)

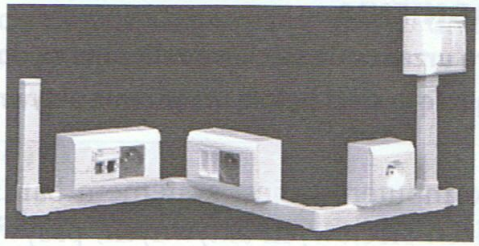
b)



c)



d)



Rys. 22.1. Wybrane urządzenia pasywne: a) gniazdo RJ-45, b) organizer kabli, c) panel krosowy, d) kanał kablowy z zainstalowanymi gniazdami

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Z jakich urządzeń aktywnych i pasywnych zbudowana jest sieć komputerowa w Twojej szkole? Jak Twoim zdaniem powinna być zbudowana?

23 Zasady doboru materiałów i urządzeń sieciowych

ZAGADNIENIA

- **Z czego wynika opóźnienie w przekazywaniu danych w sieci?**
- **W jaki sposób zmniejszać wielkość opóźnienia?**
- **W jaki sposób dobierać urządzenia sieciowe?**
- **Co należy wziąć pod uwagę podczas doboru medium transmisyjnego?**

Każde urządzenie w sieci, np. przełącznik, wprowadza pewne opóźnienie (*latency*) w przesyłaniu danych. **Opóźnienie urządzenia sieciowego** to czas poświęcony przez urządzenie na przetwarzanie pakietu lub ramki (każdy z przełączników musi odebrać ramkę, ustalić docelowy adres MAC ramki, sprawdzić zawartość swojej tablicy adresów MAC, a następnie przekazać ramkę przez właściwy port). Parametrem sieci pozwalającym na kontrolowanie wielkości opóźnienia jest średnica sieci. Średnicą sieci komputerowej określa się liczbę urządzeń, przez które dane muszą przejść, zanim dotrą do swojego miejsca docelowego. Utrzymując małą średnicę sieci, uzyskuje się niewielkie i przewidywalne opóźnienie. Przyjmuje się, że między komputerami może wystąpić maksymalnie siedem wzajemnie połączonych przełączników. Opóźnienie w sieci powodują również nośniki danych. Im większa jest ich długość, tym więcej czasu potrzeba na przesłanie danych z jednego końca na drugi. W poprawnie zbudowanych sieciach czasy tych opóźnień mierzone są w ułamkach sekund, ale przy projektowaniu sieci warto zwrócić uwagę na długość kabli (również ze względu na koszt instalacji).

Tworząc sieć o wysokiej dostępności, należy uwzględnić nadmiarowość, np. dublowanie połączeń sieciowych między urządzeniami bądź samych urządzeń. Implementacja nadmiarowych łączy może być przedsięwzięciem drogim i jest możliwa w warstwach dystrybucji i rdzenia. Niektórym awariom czy zdarzeniom losowym nie można nigdy zapobiec, np. gdy w całym mieście nastąpi awaria sieci energetycznej.

Dobór urządzeń sieciowych zaczyna się od poziomu warstwy dostępu, aby uwzględnić wszystkie urządzenia sieciowe, które wymagają dostępu do sieci. Następnie można określić, ile potrzeba przełączników w warstwie dostępu. Liczba przełączników warstwy dostępu oraz przewidywane generowane przez nie obciążenie pomagają ustalić, ile przełączników potrzebnych jest w warstwie dystrybucji, aby uzyskać wymaganą wydajność i nadmiarowość sieci. Po ustaleniu liczby przełączników warstwy dystrybucji można ustalić liczbę przełączników warstwy rdzenia.

Przy wyborze urządzeń sieciowych należy wziąć pod uwagę funkcje, jakie będą one pełnić w sieci. W ofercie producentów i dystrybutorów sprzętu występują **urządzenia o stałej konfiguracji**, w których nie istnieje możliwość dodania nowych funkcji, oraz **urządzenia modularne**. W urządzeniach modularnych w obudowie przewidziano specjalne porty, w których można zamontować moduły rozszerzające (podobnie jak karty rozszerzające montowane w płycie głównej komputera). Dzięki temu możliwa jest wymiana modułów lub rozbudowa urządzenia o dodatkowe funkcje, niedostępne wcześniej.

Połączenia między urządzeniami sieciowymi mogą być realizowane za pomocą różnego typu nośników i standardów. Ogólne zasady doboru połączeń powinny uwzględniać:

- **Długość łącza** – jeżeli łączna długość kabla nie przekracza 100 m, można stosować kable miedziane (skrętkę). Przy większych długościach stosuje się kable światłowodowe – wielomodowe (mniejsze długości) lub jednomodowe (większe długości).
- **Wymaganą przepustowość łącza** – dla większości sieci do transmisji danych odpowiedni jest FastEthernet (100MB/s). Dla sieci wymagających większych prędkości stosuje się GigabitEthernet lub 10GigabitEthernet.
- **Koszt instalacji** – kabel światłowodowy zapewnia wyższe przepustowości i odległości, lecz koszt instalacji i urządzeń jest wyższy niż w przypadku instalacji kabli miedzianych. Urządzenia pracujące z wyższymi prędkościami są droższe. Należy rozważyć wymagania użytkowników i koszty budowy sieci i podjąć decyzję o celowości ponoszenia większych kosztów.
- **Łatwość instalacji** – najłatwiejsze w instalacji są sieci zbudowane w oparciu o skrętkę. W niektórych przypadkach należy rozważyć inne wymagania, np. wykorzystanie mediów bezprzewodowych w zabytkowych budynkach, wymagających zgody konserwatora zabytku na instalację kabli lub kable światłowodowe, gdy wymagana jest odporność sieci na podsłuchiwanie.
- **Odporność na zakłócenia elektromagnetyczne** – gdy wymagana jest podwyższona odporność na zakłócenia stosuje się skrętkę ekranowaną lub kable światłowodowe (zupełnie niewrażliwe na zakłócenia elektromagnetyczne).

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyznacz maksymalną wielkość średnicy sieci w Twojej szkole.
2. Sprawdź, jakie medium transmisyjne wykorzystywane jest w Twojej szkole. Czy to rozwiązanie jest optymalne? Uzasadnij odpowiedź.

24 Struktura dokumentacji projektowej

ZAGADNIENIA

- **Jakie są charakterystyczne cechy projektu?**
- **Z jakich faz składa się realizacja projektu?**
- **Z jakich elementów powinna składać się dokumentacja projektowa?**

Struktura każdej sieci komputerowej składa się z takich samych elementów. Jednak każda sieć komputerowa posiada również indywidualne cechy, które odróżniają ją od innych tego typu sieci. Dlatego każda sieć komputerowa jest unikatowa, budowana na potrzeby konkretnej firmy, zgodnie z wymaganiami użytkowników.

Działania, których celem jest opracowanie czegoś nowego, np. nowej sieci komputerowej, wymagające nierutynowego podejścia, nazywa się **projektem**. Wiele zadań w dziedzinie informatyki jest realizowanych jako projekty, np. napisanie nowego programu komputerowego, stworzenie bazy danych lub strony internetowej. Projekt jest to przedsięwzięcie, na które składa się zespół czynności, które charakteryzują się tym, że mają:

- datę rozpoczęcia,
- specyficzne cele i limity,
- ustalone odpowiedzialności (obowiązki) realizatorów,
- budżet,
- rozkład czynności i datę ich ukończenia.

Projekty mogą być przedsięwzięciami bardzo skomplikowanymi, narażonymi na ryzyko niepowodzenia. Aby ograniczyć ryzyko, należy cały przebieg projektu dokładnie zaplanować i udokumentować, tak aby każdy z zainteresowanych realizacją projektu mógł uzyskać wszystkie niezbędne do realizacji informacje.

Realizacja projektu składa się z następujących faz:

- audytu (rozpoznania wymagań użytkownika),
- definiowania wymagań użytkownika,
- projektowania systemu,
- implementacji systemu,
- instalacji i testowania systemu oraz usuwania błędów,
- pielęgnacji i dalszego rozwoju systemu.

Dokumentacja projektu powinna być kompletna i uwzględniać wszystkie aspekty jego realizacji, miedzy innymi:

- nazwę pracowni projektowej, w której był sporządzony lub nazwisko projektanta,
- tytuł projektu,
- datę wykonania,
- ponumerowany spis rysunków i tabel,
- wykaz używanych w projekcie skrótów, np. MDF, IDF itp.,
- spis treści,

- krótki opis projektu i podstawę prawną jego stworzenia, np. kopia umowy o dzieło,
- cel projektu, np. „budowa sieci w szkole",
- zakres dokumentacji, np. „dokumentacja przedstawia wymagania dotyczące tych elementów sieci, które umożliwiają jej prawidłowe działanie",
- założenia projektu – sformułowane na podstawie audytu,
- dokumentację techniczną projektu:
  - plany budynków z zaznaczeniem punktów abonenckich, tras kabli, punktów rozdzielczych itp.,
  - karty katalogowe każdego elementu użytego do budowy sieci,
  - schemat logiczny połączeń sprzętu,
  - dokumentacja centralnego punktu sieci i punktów rozdzielczych,
  - dokumentacja rejonów okablowania,
  - projekt koncepcyjny sieci i innych wyspecjalizowanych instalacji, np. klimatyzacji, systemu gaśniczego,
  - numeracja gniazd w panelach krosowych (*patch panels*) i punktach abonenckich,
  - opis procedur odbioru okablowania,
  - wyniki testów i pomiarów,
  - spis komponentów i ich rozmieszczenie,
  - protokół odbioru,
  - kosztorys.

Dokumentacja projektu stanowi podstawowy dokument w relacjach pomiędzy zamawiającym (inwestorem) a wykonawcą projektu. Powinna być zaakceptowana i przestrzegana przez obie strony.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wybierz temat projektu sieci komputerowej, który chciałbyś zrealizować. Opisz, jakich działań będzie wymagała realizacja projektu.

25 Projektowanie okablowania strukturalnego

ZAGADNIENIA

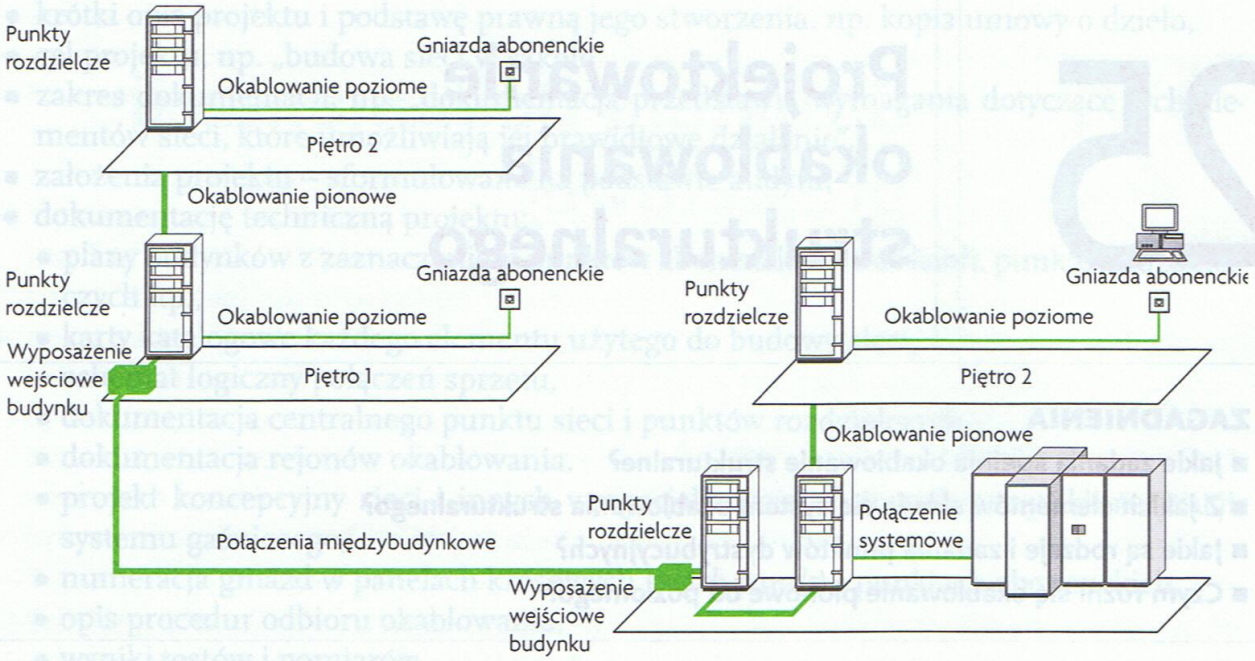
- Jakie zadania spełnia okablowanie strukturalne?
- Z jakich elementów składa się system okablowania strukturalnego?
- Jakie są rodzaje i zadania punktów dystrybucyjnych?
- Czym różni się okablowanie pionowe od poziomego?

W początkowym okresie powstawania sieci komputerowych większość firm posiadała jedynie jeden komputer centralny i kilka terminali zlokalizowanych blisko niego. Do połączeń jednostki centralnej z terminalami wykorzystywane były różne typy okablowania. W późniejszym okresie opracowano rozwiązanie polegające na obsłudze prawie wszystkich popularnych systemów danych przez skrętkę nieekranowaną (*Unshielded Twisted Pair – UTP*). Pozwala to na doprowadzenie tego samego, pojedynczego kabla do każdego gniazdka telekomunikacyjnego w budynku. Już na etapie projektowania nowego budynku można zaplanować strukturę okablowania uwzględniającą przyszłe potrzeby użytkownika.

Celem **okablowania strukturalnego** jest zbudowanie systemu modularnego, pozwalającego na realizację określonej konfiguracji połączeń dla systemu teleinformatycznego, z możliwością zmian konfiguracji oraz rozbudowy z użyciem takich samych elementów. Umożliwia to każdemu użytkownikowi włączenie dowolnego sprzętu i skorzystanie z dowolnej usługi systemu. Okablowanie strukturalne jest systemem zaprojektowanym dla konkretnego budynku. Posiada więcej punktów przyłączeniowych, niż jest to niezbędne do obsługi wszystkich urządzeń, rozmieszczonych w regularnych odstępach w całym budynku (zakłada się jeden podwójny punkt abonencki 2 x RJ-45 na każde 10 metrów kwadratowych powierzchni biurowej).

System okablowania strukturalnego (rys. 25.1) składa się z następujących elementów:

- **Założenia projektowe systemu** – określenie rodzaju nośnika danych, protokołów sieciowych, zgodności z określonymi normami i innych zasadniczych cech instalacji.
- **Okablowanie pionowe** (wewnątrz budynku) – kable miedziane lub/i światłowodowe ułożone zazwyczaj w głównych pionach telekomunikacyjnych budynków, realizujące połączenia między punktami rozdzielczymi systemu.
- **Punkty rozdzielcze** – węzły sieci w topologii gwiazdy, w których zbiega się okablowanie poziome i pionowe.
- **Okablowanie poziome** – część okablowania między punktem rozdzielczym a gniazdem użytkownika.
- **Gniazda abonenckie** – punkty przyłączenia użytkownika do sieci.
- **Połączenia systemowe** – połączenia między serwerami a szkieletem sieci.
- **Połączenia telekomunikacyjne budynków** (okablowanie międzybudynkowe lub kampusowe) – okablowanie pionowe łączące różne budynki.



Rys. 25.1. Schemat okablowania strukturalnego

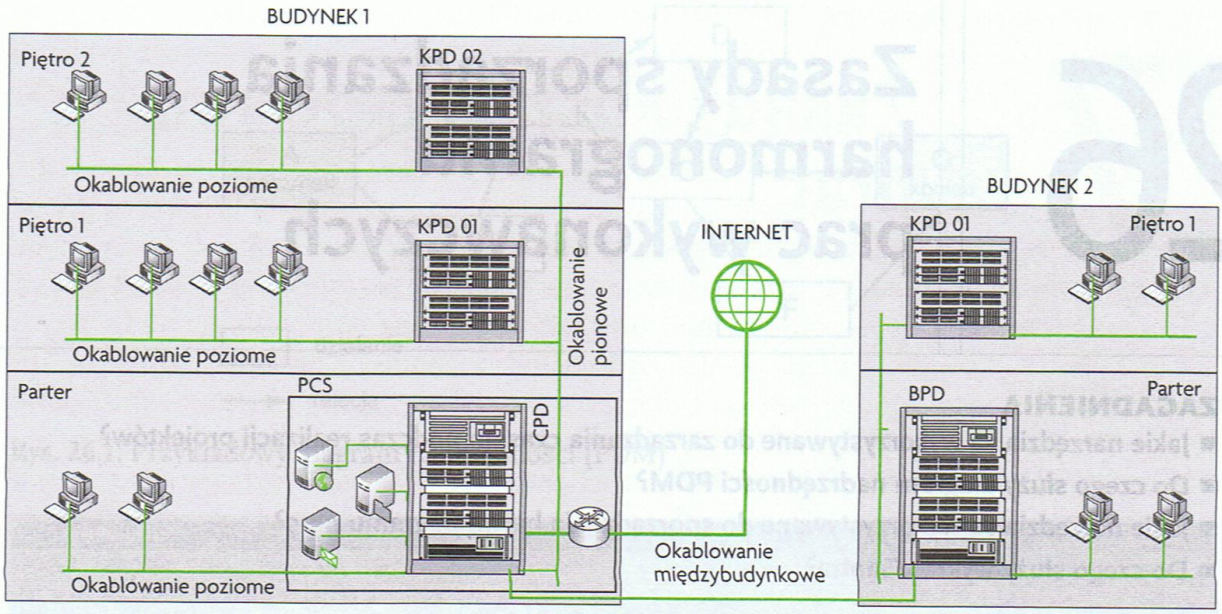
W schemacie okablowania wyróżnić można punkty rozdzielcze, czyli miejsca, w których znajdują się wszystkie elementy aktywne łączące okablowanie pionowe z poziomym. Fizycznie jest to szafa lub rama rozdzielcza z panelami oraz elementami do podłączania kabli. Według nazewnictwa polskiego do okablowania strukturalnego zaliczamy następujące elementy:

- **Punkt centralny sieci PCS** – zawiera farmę serwerów, punkt dostępu do sieci internet oraz centralny punkt dystrybucyjny. Jest to główny punkt infrastruktury teleinformatycznej.
- **Centralny punkt dystrybucyjny CPD** – w tym punkcie zbiega się okablowanie pionowe i międzybudynkowe.
- **Budynkowy punkt dystrybucyjny BPD** – łączy całe okablowanie z budynku oraz centralny punkt dystrybucyjny. W punkcie tym zbiegają się również kable z kondygnacyjnych punktów dystrybucyjnych.
- **Kondygnacyjny punkt dystrybucyjny KPD** – obejmuje zasięgiem całe piętro budynku.
- **Lokalny punkt dystrybucyjny LPD** – jest stosowany w przypadku dużych budynków, gdy kondygnacyjny punkt dystrybucyjny nie jest w stanie objąć całego piętra. LPD przedłuża zasięg KPD.

Schemat logiczny okablowania strukturalnego, zgodnie z terminologią polską pokazany jest na rysunku 25.2,.

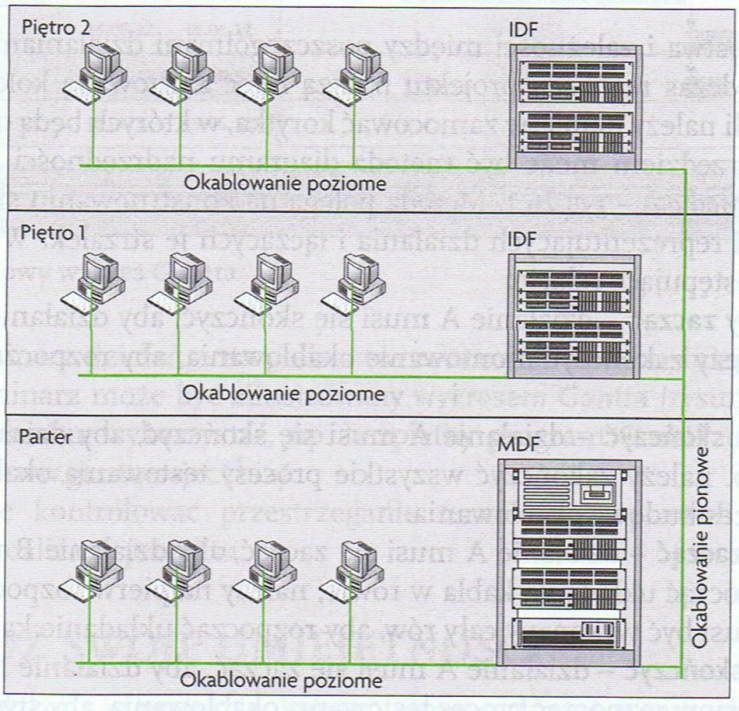
W nazewnictwie angielskim występuje mniej elementów. Ze względu na pełnioną w sieci rolę można wyróżnić:

- **Główny punkt dystrybucyjny** (*Main Distribution Facility* – MDF) – stanowi centrum okablowania w topologii gwiazdy. Zbiegają się w nim kable z sąsiednich budynków, pięter i miejskiej centrali telefonicznej oraz odchodzą przebiegi pionowe (do pośrednich punktów IDF w obiekcie) i poziome do punktów abonenckich zlokalizowanych w pobliżu MDF (do 90 m). Zwykle jest on umieszczony na parterze lub na środkowej kondygnacji budynku, w jego pobliżu znajduje się centralka telefoniczna, serwery (farma serwerów) i inny sprzęt aktywny.
- **Pośredni punkt dystrybucyjny** (*Intermediate Distribution Facility* – IDF) – jest lokalnym punktem rozdzielczym, obsługującym najczęściej dany obszar roboczy lub piętro. Jeżeli



Rys. 25.2. Schemat logiczny okablowania strukturalnego zgodny z terminologia polską

obszar obsługiwany przez IDF jest zbyt duży lub odległość z IDF do punktu abonenckiego przekracza 90 m, to należy utworzyć kolejny punkt dystrybucyjny. Przykładowy schemat rozmieszczenia punktów dystrybucyjnych w budynku, zgodnie z nazewnictwem angielskim, pokazano na rys 25.3.



Rys. 25.3. Schemat rozmieszczenia punktów dystrybucyjnych w budynku, zgodnie z nazewnictwem angielskim

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sporządź schemat sieci komputerowej w Twojej szkole. Na schemacie zaznacz punkty dystrybucyjne, okablowanie pionowe i poziome.

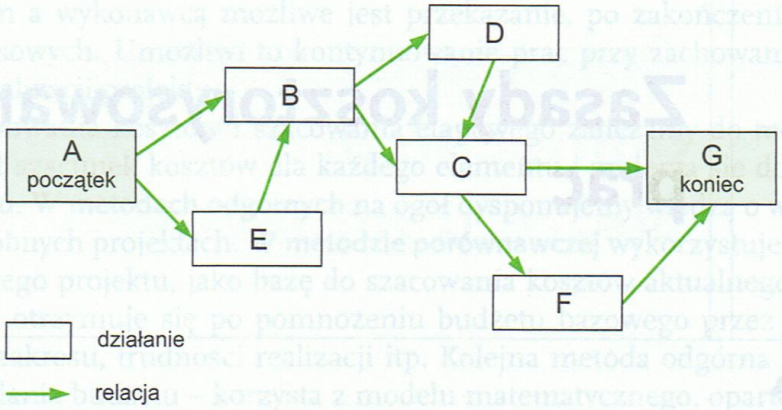
26 Zasady sporządzania harmonogramu prac wykonawczych

ZAGADNIENIA

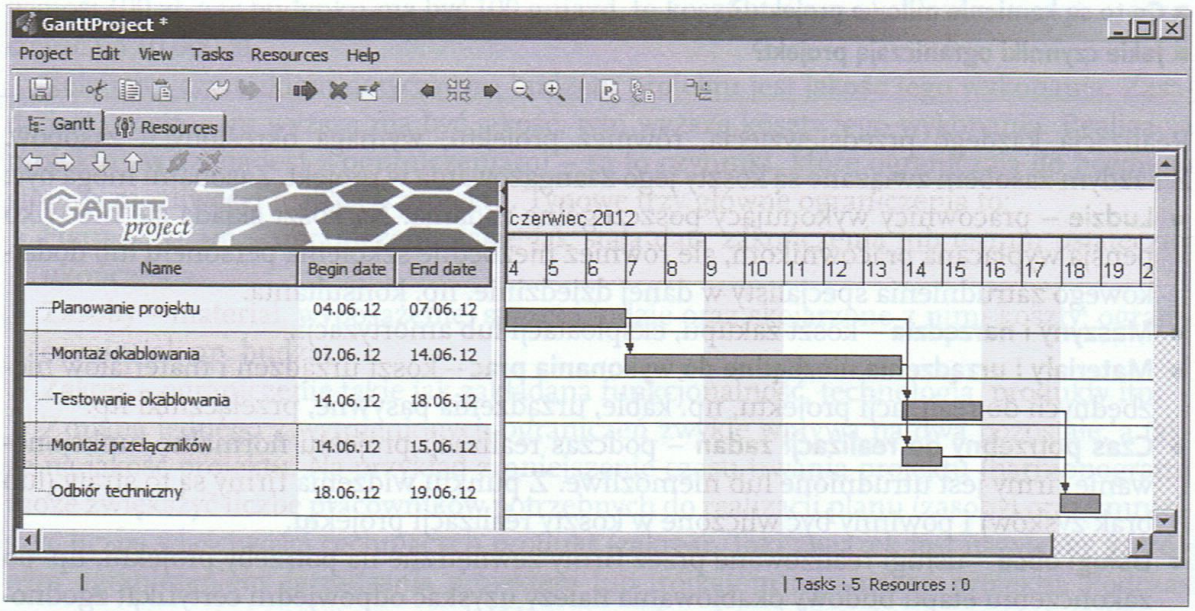
- **Jakie narzędzia są wykorzystywane do zarządzania czasem podczas realizacji projektów?**
- **Do czego służy diagram nadrzędności PDM?**
- **Jakie narzędzia są wykorzystywane do sporządzania harmonogramu prac?**
- **Do czego służy wykres Gantta?**

Znane powiedzenie mówi, że czas to pieniądz. Realizacja projektu, np. okablowania strukturalnego budynku, powinna być tak zaplanowana, aby jego zakończenie nastąpiło w uzgodnionym z odbiorcą terminie. W celu zapewnienia prawidłowego zarządzania czasem realizacji poszczególnych zadań w projekcie należy:

1. Zdefiniować działania, które muszą zostać wykonane dla osiągnięcia celów projektu – najlepiej sporządzić **listę działań** zawierającą wszystkie działania przewidziane w projekcie.
2. Określić następstwa i zależności między poszczególnymi działaniami – działania podejmowane podczas realizacji projektu muszą mieć zachowaną kolejność, np. przed ułożeniem kabli należy najpierw zamocować korytka, w których będą one umieszczone. Pomocnym narzędziem może być metoda diagramu nadrzędności PDM (*Precedence Diagramming Method*) – rys.26.1. Metoda polega na konstruowaniu sieci projektu przy użyciu symboli reprezentujących działania i łączących je strzałek. W diagramie mogą występować następujące relacje:
   - **Skończyć, aby zacząć** – działanie A musi się skończyć, aby działanie B mogło się zacząć, np. należy zakończyć montowanie okablowania, aby rozpocząć proces jego testowania.
   - **Kończyć, aby skończyć** – działanie A musi się skończyć, aby działanie B mogło się skończyć, np. należy zakończyć wszystkie procesy testowania okablowania, aby zakończyć proces budowy okablowania.
   - **Zacząć, aby zacząć** – działanie A musi się zacząć, aby działanie B mogło się zacząć, np. aby rozpocząć układanie kabla w rowie, należy najpierw rozpocząć kopanie tego rowu (nie musi być wykopany cały rów, aby rozpocząć układanie kabla).
   - **Zacząć, aby skończyć** – działanie A musi się zacząć, aby działanie B mogło się skończyć, np. musimy rozpocząć proces testowania okablowania, aby stwierdzić, czy instalacja została wykonana poprawnie.
3. Oszacować czas potrzebny do wykonania poszczególnych działań – ma na celu oszacowanie liczby godzin, dni lub miesięcy przewidywanych do wykonania poszczególnych zadań. W oszacowaniu czasu prac pomocne mogą być normy dotyczące prac montażowych oraz znajomość rozmiaru zadania. Przykładowo, jeżeli pracownik układa średnio 100 m kabla w ciągu godziny, a jest do położenia odcinek 500 m, to możemy oszacować czas wykonania pracy na 5 godzin.



Rys. 26.1. Przykładowy diagram nadrzędności (PDM)



Rys. 26.2. Przykładowy wykres Gantta

4. Stworzyć terminarz działań – na podstawie zebranych we wcześniejszych etapach informacji. Terminarz może być zilustrowany **wykresem Gantta** (rysunek 26.2). Do jego sporządzenia można wykorzystać, np. bezpłatny program GanttProject, dostępny na stronie http://www.ganttproject.biz/.
5. Systematycznie kontrolować przestrzeganie terminów – pozwoli zminimalizować opóźnienia w realizacji projektu.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyodrębnij działania w projekcie, którego temat wybrałeś w temacie 25. Określ i narysuj diagram nadrzędności. Oszacuj czas poszczególnych działań i narysuj wykres Gantta.

27 Zasady kosztorysowania prac

ZAGADNIENIA

- **Jakie zasoby są niezbędne do realizacji projektu?**
- **W jaki sposób tworzy się budżet projektu?**
- **Co to są kamienie milowe projektu?**
- **Jakie czynniki ograniczają projekt?**

Realizacja każdego przedsięwzięcia, również projektu, wymaga określonych zasobów. Z każdym zasobem związane są koszty jego zaangażowania w projekt. Zasobami mogą być:

- **Ludzie** – pracownicy wykonujący poszczególne zadania. Na koszt składa się nie tylko pensja wypłacana pracownikom, ale również niezbędne szkolenia personelu lub dodatkowego zatrudnienia specjalisty w danej dziedzinie, np. konsultanta.
- **Maszyny i narzędzia** – koszt zakupu, eksploatacji lub amortyzacji.
- **Materiały i urządzenia niezbędne do wykonania prac** – koszt urządzeń i materiałów niezbędnych do realizacji projektu, np. kable, urządzenia pasywne, przełączniki itp.
- **Czas potrzebny do realizacji zadań** – podczas realizacji projektu normalne funkcjonowanie firmy jest utrudnione lub niemożliwe. Z punktu widzenia firmy są to straty (lub brak zysków) i powinny być wliczone w koszty realizacji projektu.
- **Usługi obce** – usługi realizowane przez firmy zewnętrzne na potrzeby projektu, np. po zakończeniu etapu budowy okablowania należy uzyskać odpowiedni certyfikat zgodności - zatrudnić specjalistę posiadającego odpowiednie uprawnienia.
- **Środki finansowe**
- **Inne zasoby**, np. wiedza pracowników, doświadczenie w realizacji i zdolności przywódcze kadry kierowniczej, budynki i pomieszczenia itp.

Przed rozpoczęciem realizacji projektu należy oszacować jego budżet; inwestor powinien wiedzieć, czy jego zasoby są wystarczające do ukończenia projektu. Powinien również wiedzieć, jakie zasoby i w jakich ilościach będą potrzebne w danym momencie realizacji. W czasie realizacji projektu zwykle występują jakieś okoliczności, nieprzewidziane na etapie planowania. Dlatego warto posiadać pewien zapas zasobów na wypadek pojawiających się problemów.

Istnieje wiele metod tworzenia budżetu. W przypadku małych projektów można zastosować metodę **sumowania kosztów** – sporządzić listę wszystkich produktów niezbędnych do realizacji, a następnie zsumować ich koszty. W metodzie tej istnieje jednak niebezpieczeństwo pominięcia ważnych szczegółów i wystąpienia dużego błędu.

Mniejsze niebezpieczeństwo występuje przy **szacowaniu etapowym**. Cały projekt podzielony zostaje na etapy. Zakończenie każdego etapu uzależnione jest od spełnienia określonego warunku lub zrealizowania pewnego produktu cząstkowego (tzw. **kamienie milowe**). Realizacja projektu etapami pozwala na dokładniejsze szacowanie kosztów poszczególnych etapów, a następnie ich zsumowanie. W zależności od umowy pomię-

dzy inwestorem a wykonawcą możliwe jest przekazanie, po zakończeniu etapu, części środków finansowych. Umożliwi to kontynuowanie prac przy zachowaniu kontroli nad przebiegiem realizacji projektu.

Metodę sumowania kosztów i szacowania etapowego zaliczamy do **metod oddolnych** – tworzony jest szacunek kosztów dla każdego elementu i zmierza się do uzyskania całkowitego kosztu. W **metodach odgórnych** na ogół dysponujemy wiedzą o wcześniej zrealizowanych podobnych projektach. W **metodzie porównawczej** wykorzystuje się rzeczywisty budżet podobnego projektu, jako bazę do szacowania kosztów aktualnego projektu. Szacowany budżet otrzymuje się po pomnożeniu budżetu bazowego przez współczynniki, np. wielkości, zakresu, trudności realizacji itp. Kolejna metoda odgórna – **metoda parametryczna** ustalania budżetu – korzysta z modelu matematycznego, opartego na znanych parametrach. Parametrem może być np. koszt okablowania przypadający na pojedyncze gniazdo abonenckie. Przykładowo, jeżeli koszt średni koszt okablowania strukturalnego wynosi 100 zł, a w budynku ma być 100 gniazd, to koszt budowy okablowania można oszacować na 10 000 zł.

Kolejnym czynnikiem dotyczącym budżetu projektu jest **jakość** jego wykonania. Zasada jest prosta – im wyższa ma być jakość, tym wyższe koszty jego wykonania. Realizacja projektu związana jest z ograniczeniami – są to czynniki, które ograniczają do pewnego stopnia możliwości realizacji projektu. Typowe trzy główne ograniczenia to:

- **Harmonogram** – ograniczenia takie jak stała data zakończenia lub termin ostateczny ukończenia.
- **Zasoby** – materiał, wyposażenie, sprzęt i ludzie oraz skojarzone z nimi koszty; ograniczenie, jak np. budżet.
- **Zakres** – ograniczenie takie jak zakładana funkcjonalność, technologia, produkty itp.

Zmiana jednego z wymienionych ograniczeń zwykle wpływa na dwa pozostałe, a także na jakość projektu. Na przykład zmniejszenie czasu trwania projektu (harmonogram) może zwiększyć liczbę pracowników potrzebnych do realizacji planu (zasoby) oraz zmniejszyć liczbę właściwości cechujących produkt (zakres). Taki związek jest nazywany **potrójnym ograniczeniem zarządzania projektem** lub trójkątem ograniczeń projektu. Podczas procesu planowania należy sporządzić listę ograniczeń projektu, aby upewnić się, że wszyscy uczestnicy projektu zostali o niej powiadomieni i mogą się do niej odnieść. Należy również uzgodnić sposób reakcji na niespodziewane ograniczenia, które mogą ujawnić się w czasie trwania projektu. Na przykład, jeżeli koszty pracy okażą się wyższe od przewidywanych, to wykonawcy mogą zażądać zmniejszenia zakresu projektu lub zwiększenia budżetu.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wypisz zasoby potrzebne do zrealizowania Twojego projektu.
2. Podziel projekt na etapy tworzenia i określ kamienie milowe projektu.

28 Dokumenty źródłowe, pomocne przy sporządzaniu budżetu projektu

ZAGADNIENIA

- **Do czego służą jednostkowe nakłady rzeczowe?**
- **Co to jest katalog nakładów rzeczowych KNR?**
- **W jaki sposób obliczać koszt prac?**

Opracowanie budżetu jest zadaniem bardzo trudnym, ale koniecznym dla właściwej realizacji projektu. W przypadku, gdy budżet jest nieoszacowany, czyli do jego realizacji zaplanowano zbyt małe środki, może zdarzyć się sytuacja, że projekt nie zostanie dokończony – straty poniesie inwestor i wykonawca. Gdy szacowany budżet jest zbyt duży, inwestor poniesie koszty niższe od planowanych, ale może mieć wątpliwości dotyczące kompetencji wykonawcy lub jakości wykonania. Niedopuszczalna jest sytuacja, w której wykonawca nie informuje inwestora o rzeczywistych, niższych od planowanych, kosztach – nieuczciwość w biznesie nie jest mile widziana i taki wykonawca więcej już nie będzie mógł liczyć na kolejne zlecenia.

Podczas szacowania budżetu można korzystać z jednostkowych nakładów rzeczowych. Jednostkowy nakład rzeczowy, to wielkość danego nakładu, przypadająca na wybraną jednostkę obmiarową (czyli jeden etap) danego rodzaju robót. Nakłady jednostkowe określa się w odniesieniu do poszczególnych rodzajów robót:

- **Robocizny** – wyrażane są w roboczogodzinach [r-g], na jednostkę obmiarową danej roboty, np. instalacja systemu operacyjnego na pojedynczym komputerze (czyli jeden etap instalacji systemu operacyjnego w firmie) – 1 roboczogodzina.
- **Materiałów** – wyrażane są w wybranej jednostce miary ilości danego materiału (np. kg, m^3, m, szt. itp), na jednostkę obmiarową danej roboty, np. w okablowaniu strukturalnym na każde 10 m^2 powierzchni powinno przypadać jedno podwójne gniazdo abonenckie.
- **Czasu pracy sprzętu** – wyrażane są w maszynogodzinach [m-g], na jednostkę obmiarową danej roboty, np. koparka w ciągu godziny pracy może wykopać rów o długości 100 m.

Nakłady rzeczowe przypadające na dany rodzaj robót mogą być obliczone jako iloczyn ilości robót i jednostkowego nakładu rzeczowego. Jednostkowe nakłady rzeczowe mogą być ustalane na podstawie gotowych **katalogów nakładów rzeczowych** KNR. W tabeli 28.1 pokazano przykładowe jednostkowe nakłady związane z budową okablowania strukturalnego. Informacje te pochodzą z katalogu nakładów rzeczowych dla prac związanych z montażem sieci „Okablowanie strukturalne w technologii firmy TYCO", oznaczonego symbolem KNR AT-28.

W tabeli 28.2 można odczytać, że montaż nieekranowego modułu RJ-45 wymaga:

- 0,07 roboczogodziny montera-instalatora grupy V (robocizna),
- 1 kpl. modułu nieekranowego RJ-45 (materiały),
- 0,07 maszynogodziny narzędzia z matrycą do zarabiania gniazd (czas pracy sprzętu).

Nakłady związane z realizacją całego projektu są sumą wszystkich nakładów cząstkowych.

Tabela 28.1. Tabela 0102 z KNR AT-28

Poziome okablowanie strukturalne (układanie kabla do gniazda użytkownika)

Wyszczególnienie robót: 1. Przygotowanie trasy przebiegu kabla pod względem technologii instalacyjnej. 2. Przygotowanie kabla. 3. Instalacja kabla zgodnie z przyjętą technologią. 4. Sprawdzenie poprawności ułożenia kabla.

Nakłady na 100 m ułożonego kabla — Tablica 0102

Lp.	Symbol eto	Wyszczególnienie	Jm.	Układanie odcinków					
				poziomych		pionowych		Każdy następny kabel w wiązce	
				1 kabel					
				miedziany do 8 mm	światłowodowy	miedziany do 8 mm	światłowodowy	miedziany do 8 mm	światłowodowy
a	b	C	d	01	02	03	04	05	06
01	315	Monter-instalator – grupa V	r-g	0,86	1,06	1,08	1,33	0,41	0,55
02	315	Monter-instalator – grupa V	r-g	0,65	0,96	0,86	1,13	0,41	0,55
20		Kabel okablowania strukturalnego miedziany Tyco Electronics/AMP NETCONNECT	m	110	–	110	–	110	–
21		Kabel okablowania strukturalnego światłowodowy Tyco Electronics/AMP NETCONNECT	m	–	110	–	110	–	110

Tabela 28.2. Tabela 0108 z KNR-AT28

Montaż na skrętce 4-parowej modułu RJ45 i złącza krawędziowego

Wyszczególnienie robót: 1. Usunięcie izolacji z kabla. 2. Obcięcie ekranu kabla (kol.02). 3. Ułożenie par wg kolejności zaznaczonej na matrycy. 4. Montaż modułu matrycy. 5. Zaciśnięcie modułu z jednoczesnym obcięciem naddatków żył. 6. Połączenie ekranu kabla (kol.02). 7. Kontrola poprawności montażu.

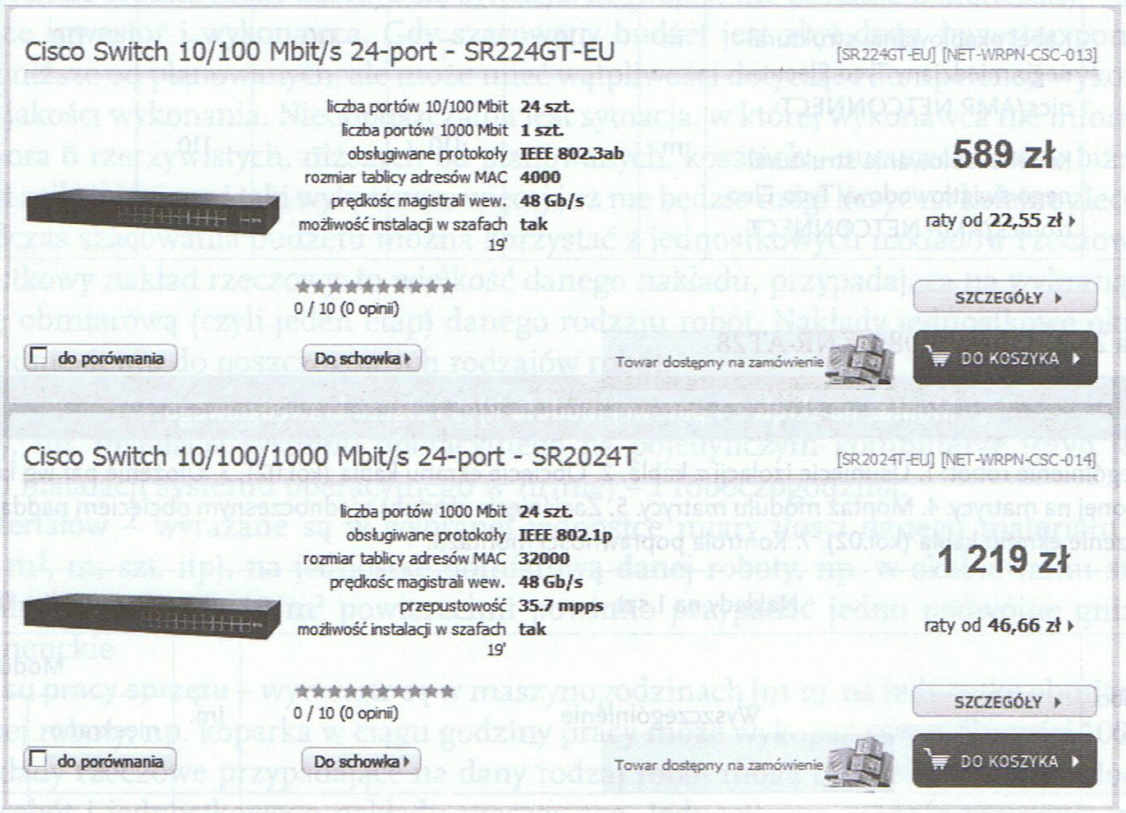
Nakłady na 1 szt. — Tablica 0108

Lp.	Symbol eto	Wyszczególnienie	Jm.	Moduł	
				nieekranowany	ekranowany
a	b	C	d	01	02
01	315	Monter-instalator – grupa V	r-g	0,07	0,01
20		Moduł nieekranowany RJ45 SL Tyco Electronics/AMP NETCONNECT	kpl.	1	–
21		Moduł ekranowany RJ45 SL Tyco Electronics/AMP NETCONNECT	kpl.	–	1
22		Moduł ekranowany RJ45 AWC Tyco Electronics/AMP NETCONNECT	kpl.	–	(1)
23		Ekranowane złącze krawędziowe Tyco Electronics/AMP NETCONNECT	kpl.	–	(1)
70		Narzędzie z matrycą do zarabiania gniazd SL i złącz krawędziowych	m-g	0,07	0,1

Aby wyznaczyć wysokość budżetu, wykonawca powinien sporządzić i przedstawić do zaakceptowania kalkulację stawki godzinowej pracownika. Jej wysokość może być również ustalana jako „wartość rynkowa", negocjowana pomiędzy wykonawcą a inwestorem. Stawki godzinowe mogą być różne dla pracowników o odmiennych kwalifikacjach i uprawnieniach. Całkowity koszt robocizny będzie iloczynem całkowitych nakładów pracy i stawki godzinowej. Jeżeli przyjmiemy stawkę godzinową 14 zł/h, to wartość pracy wyniesie 0,98 zł.

W podobny sposób ustalana jest stawka maszynogodziny pracy maszyn i narzędzi. Jeżeli dla narzędzia do zarabiania gniazd przyjmiemy stawkę 45 zł/h, to wartość pracy wyniesie 3,15 zł.

Koszt materiałów niezbędnych do wykonania pracy można ustalić na podstawie cenników dostawców. Katalogi wyrobów i cenniki materiałów i urządzeń dostępne są na stronach internetowych dostawców lub producentów. W cennikach oprócz ceny podawane są również najważniejsze informacje charakteryzujące dane urządzenie. Przykład fragmentu cennika pokazano na rysunku 28.1. Do kosztów producenta dodaje się koszt zakupu – zwykle obliczany procentowo od wartości zakupu (np. 5 %). Jeżeli przyjmiemy, że cena wtyczki RJ-45 wynosi 0,45 zł i zsumujemy wszystkie koszty to łączny budżet dla naszego przykładu wyniesie 4,58 zł.



Rys. 28.1. Fragment cennika sieciowego sprzętu aktywnego

Na rynku dostępnych jest wiele aplikacji komputerowych wspomagających kosztorysanta. Kosztorysant wybiera w takim programie podstawę wyceny i liczbę jednostek obmiarowych, a program sam wykonuje wszystkie niezbędne obliczenia.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Korzystając z katalogu KNR AT-28, oblicz koszt montażu 1000 m skrętki nieekranowanej (okablowanie poziome) i wykonania dziesięciu złączy RJ-45.

29 Czytanie rzutów poziomych i pionowych budynków

ZAGADNIENIA

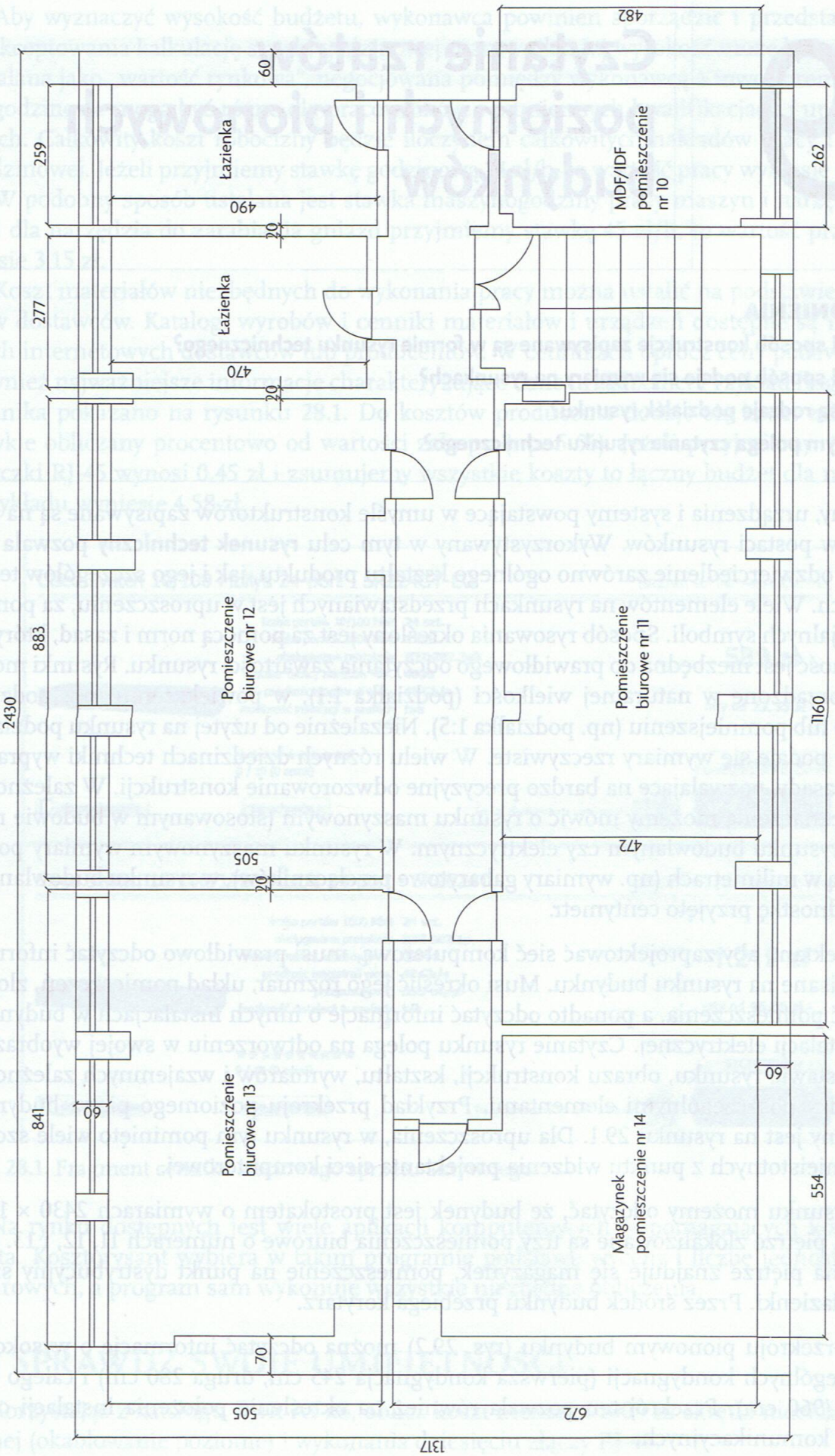
- W jaki sposób konstrukcje zapisywane są w formie rysunku technicznego?
- W jaki sposób podaje się wymiary na rysunkach?
- Jakie są rodzaje podziałek rysunku?
- Na czym polega czytanie rysunku technicznego?

Maszyny, urządzenia i systemy powstające w umyśle konstruktorów zapisywane są na papierze w postaci rysunków. Wykorzystywany w tym celu **rysunek techniczny** pozwala na wierne odzwierciedlenie zarówno ogólnego kształtu produktu, jak i jego szczegółów technicznych. Wiele elementów na rysunkach przedstawianych jest w uproszczeniu, za pomocą specjalnych symboli. Sposób rysowania określony jest za pomocą norm i zasad, których znajomość jest niezbędna do prawidłowego odczytania zawartości rysunku. Rysunki mogą być sporządzone w naturalnej wielkości (podziałka 1:1), w powiększeniu (np. podziałka 10:1) lub pomniejszeniu (np. podziałka 1:5). Niezależnie od użytej na rysunku podziałki zawsze podaje się wymiary rzeczywiste. W wielu różnych dziedzinach techniki wypracowano zasady, pozwalające na bardzo precyzyjne odwzorowanie konstrukcji. W zależności od przeznaczenia możemy mówić o rysunku maszynowym (stosowanym w budowie maszyn), rysunku budowlanym czy elektrycznym. W rysunku maszynowym wymiary podawane są w milimetrach (np. wymiary gabarytowe przełączników), w rysunku budowlanym jako jednostkę przyjęto centymetr.

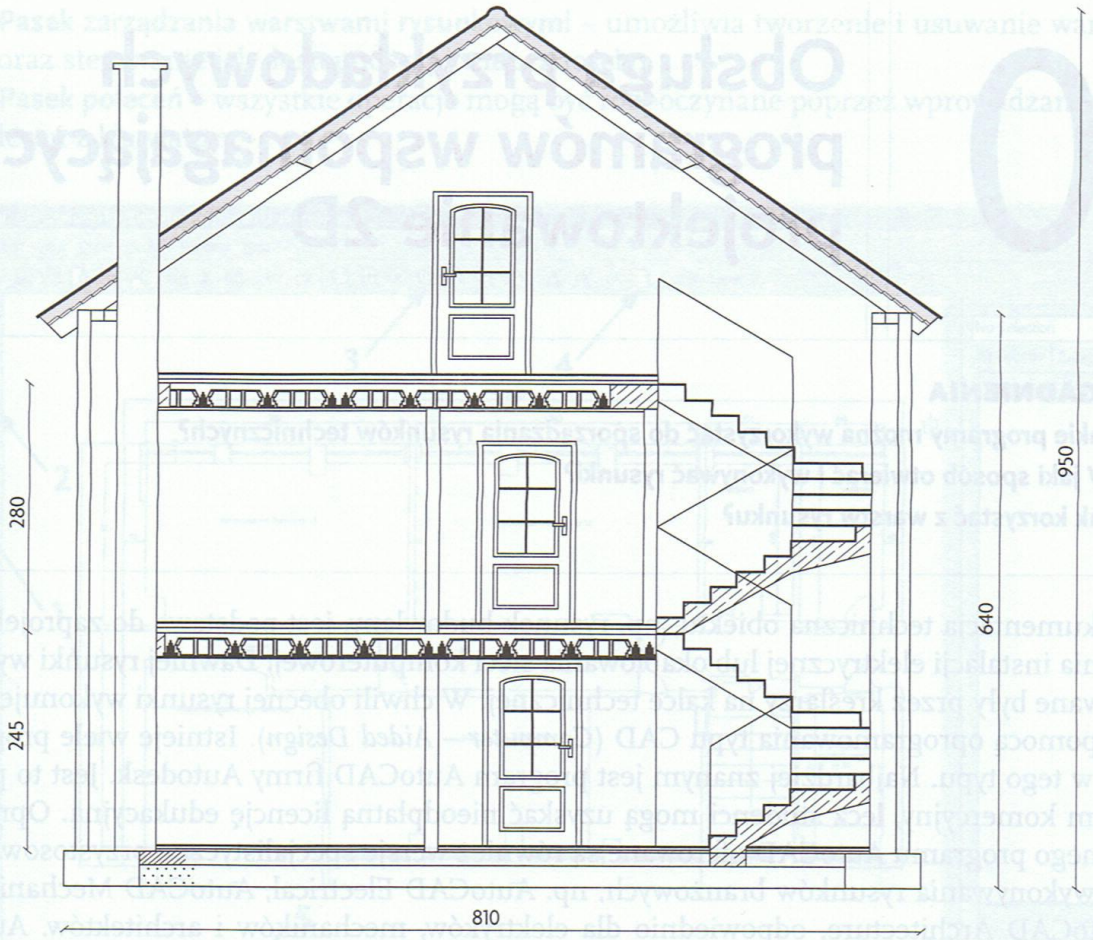
Projektant, aby zaprojektować sieć komputerową, musi prawidłowo odczytać informacje zapisane na rysunku budynku. Musi określić jego rozmiar, układ pomieszczeń, zlokalizować pomieszczenia, a ponadto odczytać informacje o innych instalacjach w budynku, np. instalacji elektrycznej. Czytanie rysunku polega na odtworzeniu w swojej wyobraźni, na podstawie rysunku, obrazu konstrukcji, kształtu, wymiarów i wzajemnych zależności pomiędzy poszczególnymi elementami. Przykład przekroju poziomego piętra budynku pokazany jest na rysunku 29.1. Dla uproszczenia, w rysunku tym pominięto wiele szczegółów nieistotnych z punktu widzenia projektanta sieci komputerowej.

Z rysunku możemy odczytać, że budynek jest prostokątem o wymiarach 2430 × 1317 cm. Na piętrze zlokalizowane są trzy pomieszczenia biurowe o numerach 11, 12, i 13. Ponadto na piętrze znajduje się magazynek, pomieszczenie na punkt dystrybucyjny sieci i dwie łazienki. Przez środek budynku przebiega korytarz.

W przekroju pionowym budynku (rys. 29.2) można odczytać informacje o wysokości poszczególnych kondygnacji (pierwsza kondygnacja 245 cm, druga 280 cm) i całego budynku (960 cm). Przekrój ten pozwala również na określenie położenia instalacji oraz ciągów komunikacyjnych.



Rys. 29.1. Rysunek techniczny piętra budynku



Rys. 29.2. Przekrój pionowy budynku

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Przyjmując normę 1 podwójne gniazdko RJ-45 na każde 10 m^2 powierzchni biurowej, określ liczbę gniazdek w każdym z pomieszczeń biurowych, przedstawionych na rysunku 29.1.
2. W przygotowywanym przez Ciebie projekcie, korzystając z rysunku 29.2 budynku:
   - oblicz ilość gniazdek abonenckich w poszczególnych pomieszczeniach,
   - zaznacz rozmieszczenie punktów dystrybucyjnych,
   - oblicz długość poszczególnych kabli poziomych i pionowych oraz ich łączną długość.

30 Obsługa przykładowych programów wspomagających projektowanie 2D

ZAGADNIENIA

- **Jakie programy można wykorzystać do sporządzania rysunków technicznych?**
- **W jaki sposób otwierać i wykonywać rysunki?**
- **Jak korzystać z warstw rysunku?**

Dokumentacja techniczna obiektu, np. rysunek budowlany, jest podstawą do zaprojektowania instalacji elektrycznej lub okablowania sieci komputerowej. Dawniej rysunki wykonywane były przez kreślarzy na kalce technicznej. W chwili obecnej rysunki wykonuje się za pomocą oprogramowania typu CAD (*Computer – Aided Design*). Istnieje wiele programów tego typu. Najbardziej znanym jest program AutoCAD firmy Autodesk. Jest to program komercyjny, lecz studenci mogą uzyskać nieodpłatną licencję edukacyjną. Oprócz samego programu AutoCAD oferowane są również wersje specjalistyczne przystosowane do wykonywania rysunków branżowych, np. AutoCAD Electrical, AutoCAD Mechanical, AutoCAD Architecture, odpowiednio dla elektryków, mechaników i architektów. AutoCAD jest systemem bardzo rozbudowanym, umożliwiającym wykonywanie rysunków 2D i 3D. Do wykonywania rysunków 2D można wykorzystać bezpłatne programy A9CAD lub QCad.

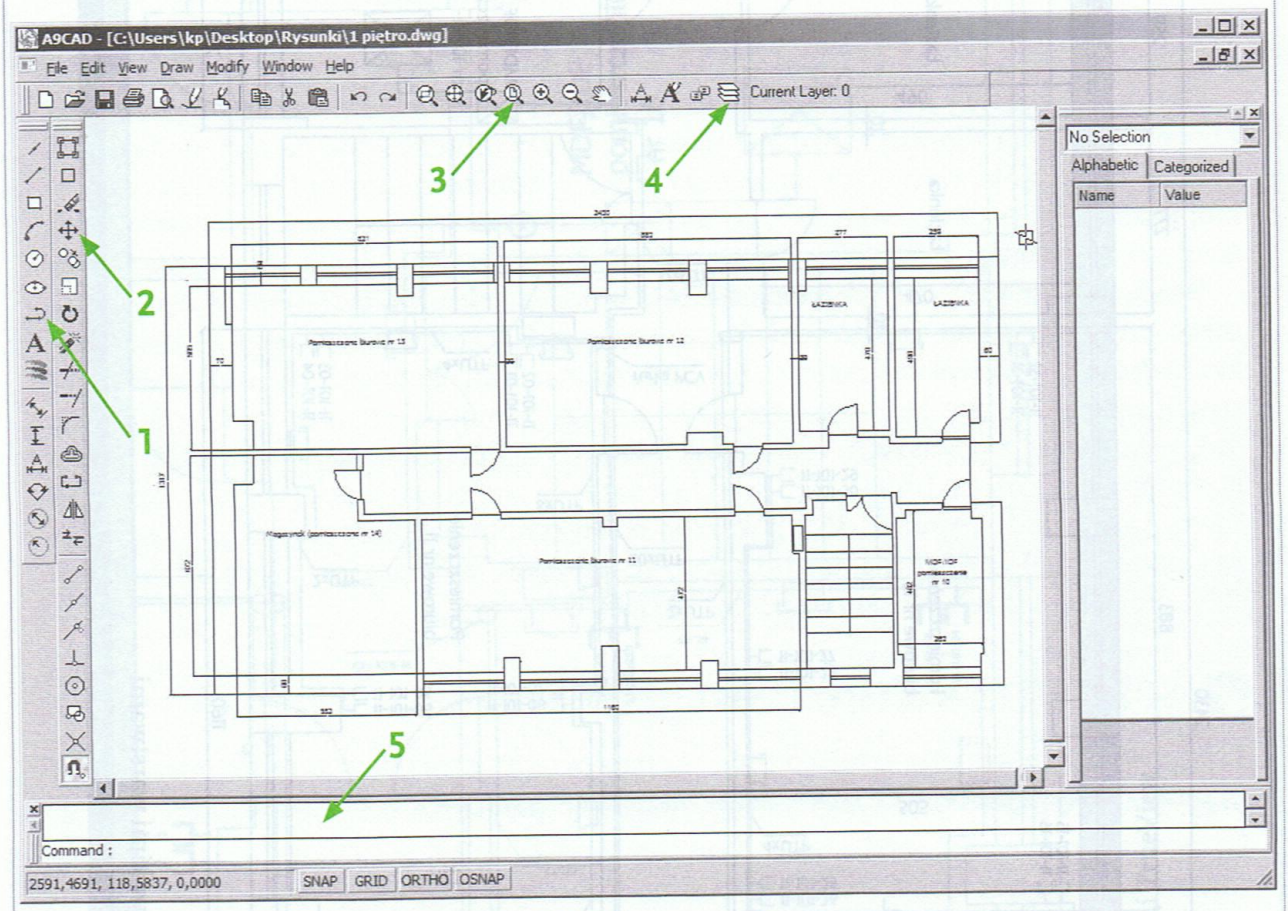
Rysunki zapisywane są jako grafika wektorowa. Standardowymi rozszerzeniami plików są *.dwg lub *.dxf. Programy te umożliwiają wprowadzanie danych z bardzo dużą dokładnością. W profesjonalnych biurach projektowych pracę kreślarzom ułatwiają tablety graficzne (rys. 30.1), wykorzystywane do szybkiego i precyzyjnego rysowania za pomocą specjalnego pióra.

Na rys. 30.2 pokazano okno główne programu A9CAD. Strzałkami zaznaczono paski narzędzi najczęściej wykorzystywane do edycji rysunków:

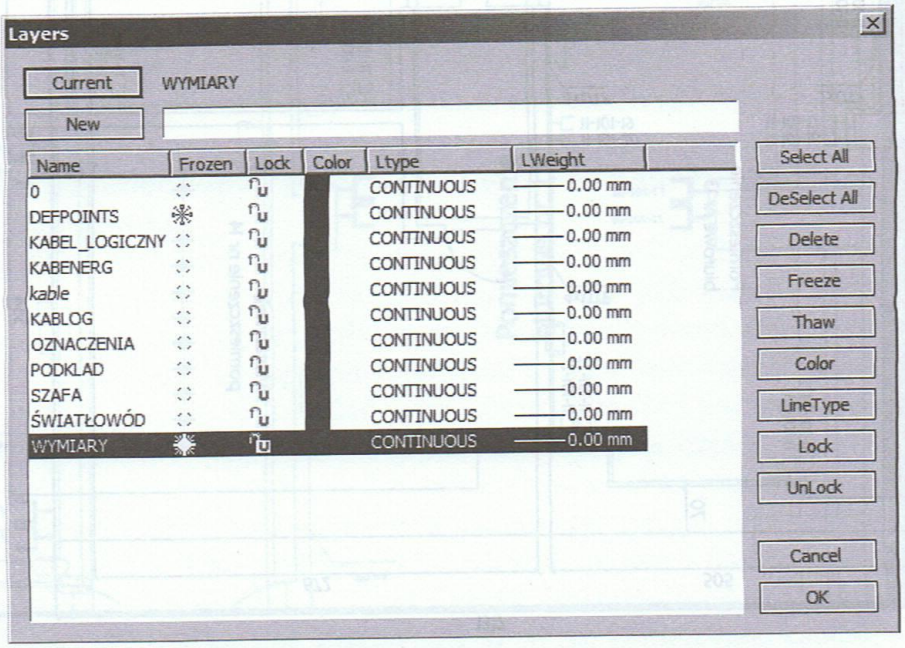
1. **Pasek narzędzi rysowania** – pozwala na rysowanie obiektów, takich jak punkty, linie, okręgi itp., a także na wprowadzania wymiarów.
2. **Pasek modyfikacji** – pozwala na modyfikowanie istniejących na rysunku obiektów, np. ich obcinanie lub wydłużanie, przesuwanie, wykonywanie obrotu itp.
3. **Pasek narzędzi zoom** – umożliwia powiększanie i pomniejszanie wybranego obszaru roboczego okna.

Rys. 30.1. Tablet graficzny

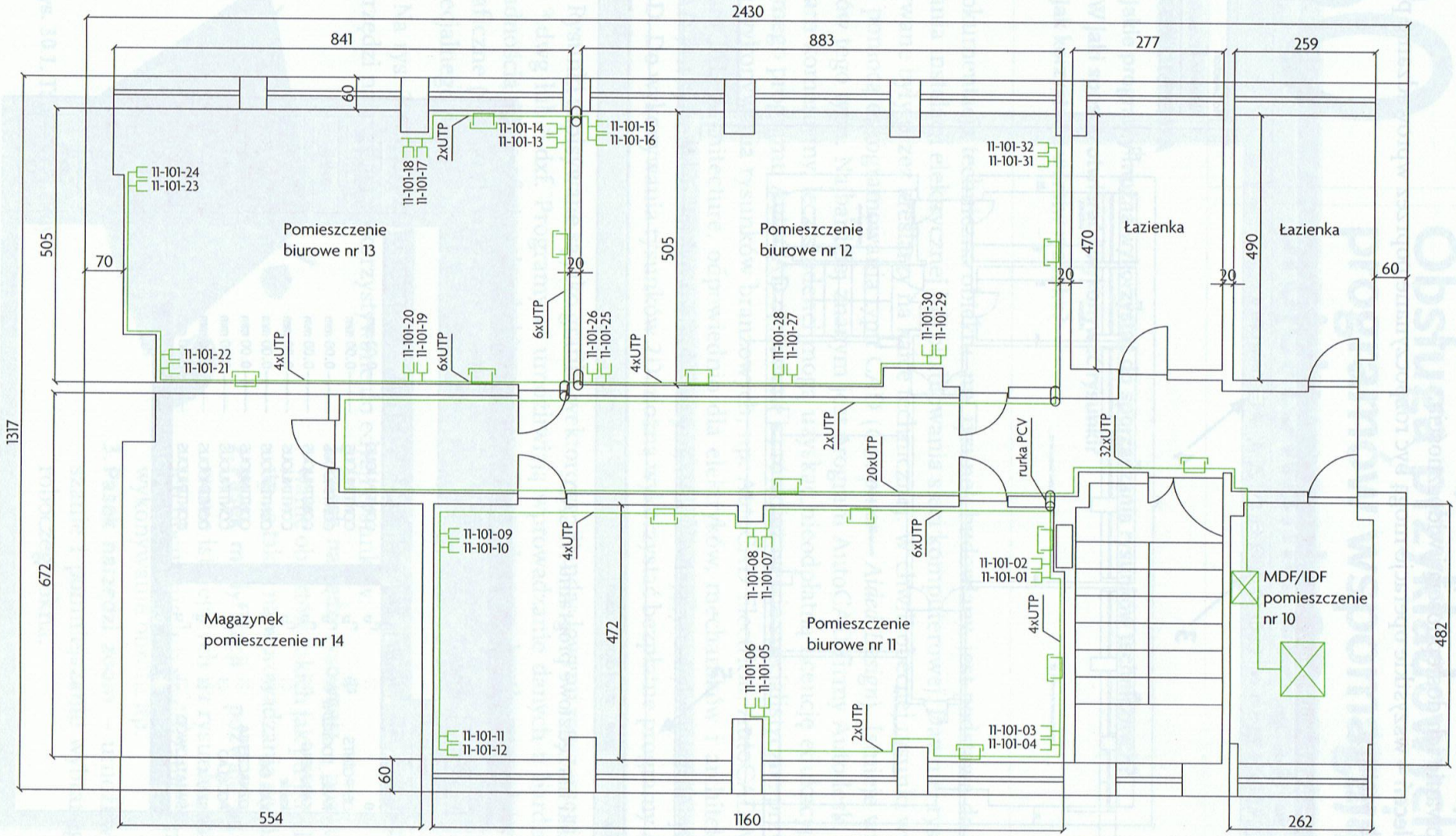
4. **Pasek zarządzania warstwami rysunkowymi** – umożliwia tworzenie i usuwanie warstw oraz sterowanie ich dostępnością i widocznością.
5. **Pasek poleceń** – wszystkie operacje mogą być rozpoczynane poprzez wprowadzanie poleceń z klawiatury.



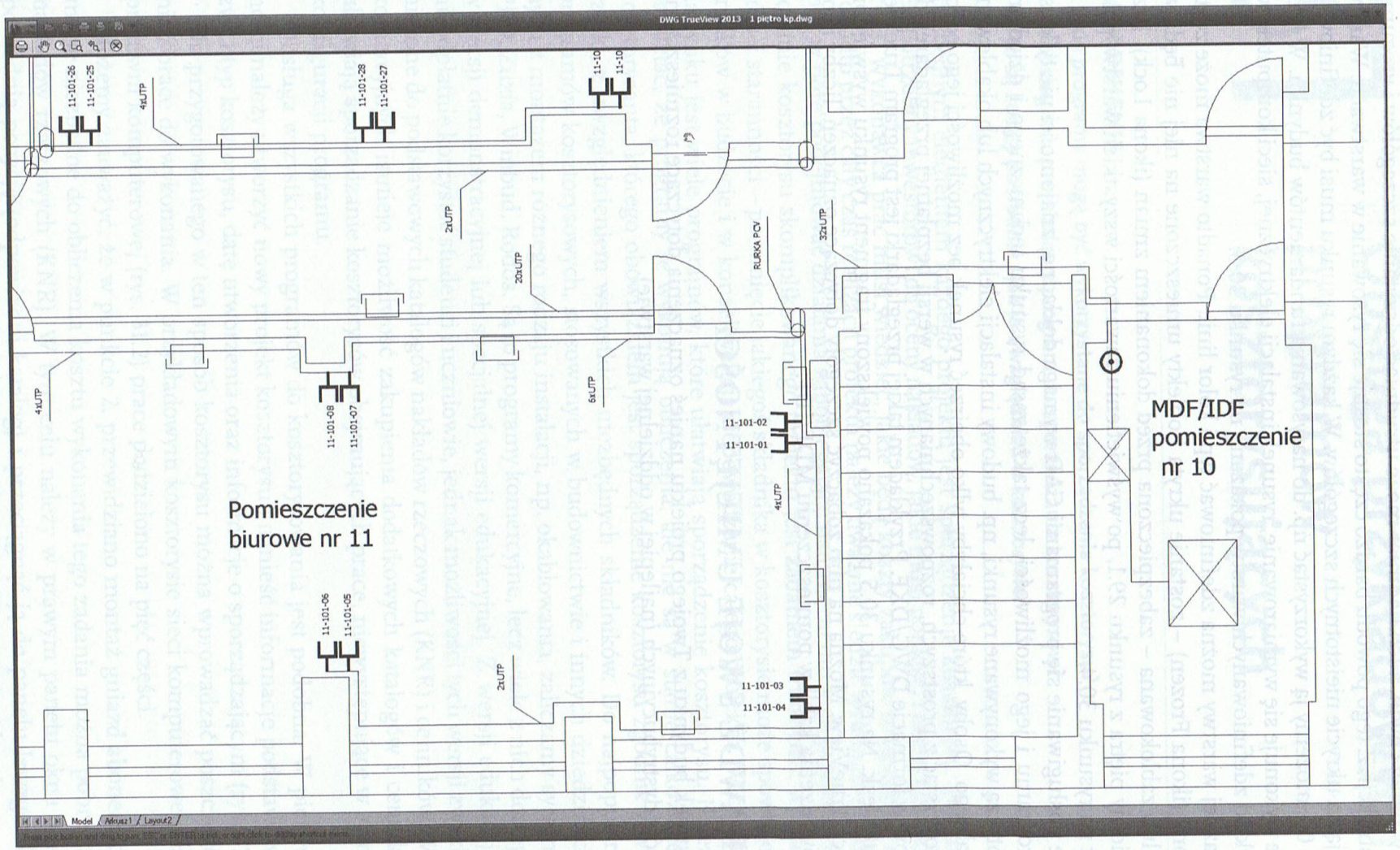
Rys. 30.2. Paski narzędziowe programu A9CAD



Rys. 30.3. Okno zarządzania warstwami



Rys. 30.4. Przekrój poziomy budynku z widocznymi wszystkimi warstwami



Rys. 30.5. Przeglądanie rysunku za pomocą przeglądarki TrueView

Rysunek techniczny może zawierać bardzo dużo informacji. Nie wszystkie z nich są potrzebne w danej chwili, a ich nadmiar może utrudniać odczytanie szczegółów i zrozumienie konstrukcji. Z tego powodu bardzo często stosuje się rysowanie w warstwach. Warstwy pozwalają na ukrycie nieistotnych szczegółów. W każdym rysunku musi być zdefiniowana warstwa 0 – możemy ją wykorzystać np. do narysowania fundamentów budynku. W innej warstwie wykonuje się wymiarowanie, rysunek instalacji elektrycznej, sieci komputerowej itd. Przykład zdefiniowanych warstw pokazano na rysunku 30.3.

Dla każdej warstwy można zdefiniować typ i kolor linii. Ponadto warstwa może zostać zamrożona (ikona Frozen) – zostanie ukryta i obiekty umieszczone na niej nie będą widoczne, lub zablokowana – zabezpieczona przed dokonaniem zmian (ikona Lock). Przekrój poziomy piętra z rysunku 29.1, po wyświetleniu zawartości wszystkich warstw, pokazany jest na rysunku 30.4.

Biegłe posługiwanie się programami CAD wymaga dokładnej znajomości nie tylko samego programu i jego możliwości, lecz także zasad rysunku technicznego i dziedziny, której dotyczą wykonywane rysunki, np. budowy instalacji elektrycznych lub okablowania strukturalnego. Osoby, które chciałyby tylko obejrzeć rysunek bez możliwości jego edycji, mogą skorzystać z prostszych, rozpowszechnianych w wersji bezpłatnej przeglądarek dokumentów w formacie DWG/DXF. Przykładem takiej przeglądarki jest program TrueView firmy Autodesk. Na rysunku 30.5 pokazano powiększony fragment rysunku wyświetlony za pomocą TrueView. Można na nim zobaczyć szczegóły dotyczące oznaczeń, liczby i sposobu prowadzenia kabli w pomieszczeniu MDF/IDF.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Na rysunek budynku z Twojego projektu nanieś oznaczenia dotyczące rozmieszczenia punktów dystrybucyjnych (najlepiej w oddzielnej warstwie).

31 Obsługa przykładowych programów kosztorysujących

ZAGADNIENIA

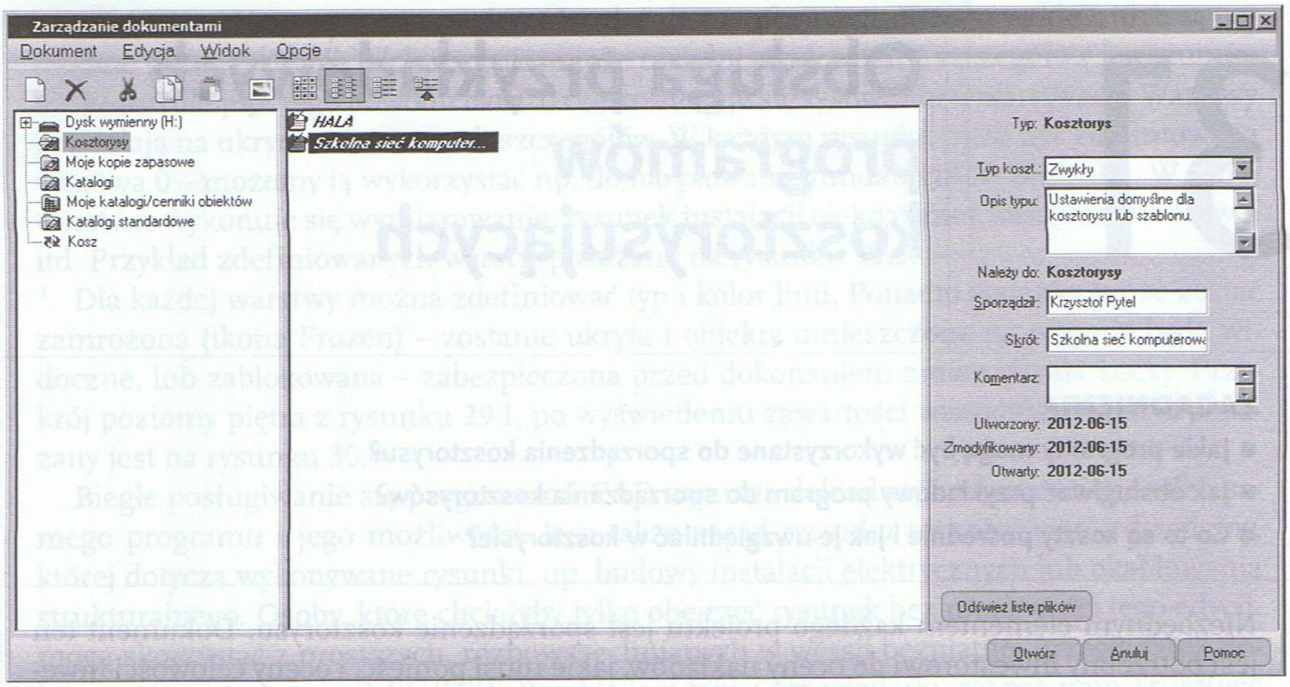
- **Jakie programy mogą być wykorzystane do sporządzenia kosztorysu?**
- **Jak obsługiwać przykładowy program do sporządzania kosztorysów?**
- **Co to są koszty pośrednie i jak je uwzględniać w kosztorysie?**

Niezbędnym elementem każdego projektu jest sporządzenie kosztorysu. Dokument ten jest potrzebny inwestorowi do oceny nakładów, jakie musi ponieść, i oceny celowości inwestycji. Wykonawca prac musi wiedzieć, jakie będą koszty zakupów materiałów, usług itp. Ponadto przez cały czas realizacji projektu należy uważnie śledzić wykonanie budżetu, aby móc w porę podejmować działania zapobiegające nadmiernemu jego przekroczeniu. Wykonanie kosztorysu skomplikowanego projektu jest zadaniem trudnym i wymaga szczególnej staranności – pominięcie jakiegoś składnika w kosztorysie może spowodować brak środków w budżecie i w konsekwencji niepowodzenie całego projektu. W chwili obecnej na rynku jest wiele programów, które ułatwiają sporządzenie kosztorysu. Należy jednak pamiętać, że programy te wykonują obliczenia, ale nie są w stanie całkowicie zastąpić kosztorysanta, którego obowiązkiem jest sporządzenie kosztorysu zgodnie z wymogami sztuki, z uwzględnieniem wszystkich niezbędnych składników. Do najpopularniejszych programów kosztorysowych, stosowanych w budownictwie i innych dziedzinach związanych z montażem różnego rodzaju instalacji, np. okablowania, zaliczamy systemy Norma PRO, Zuzia, Winbud, Rodos. Są to programy komercyjne, lecz wiele z nich dostępnych jest w wersji demonstracyjnej lub specjalnej wersji edukacyjnej. Z wersji edukacyjnej mogą nieodpłatnie korzystać studenci i uczniowie, jednak możliwości tych wersji zwykle są ograniczone do podstawowych katalogów nakładów rzeczowych (KNR) i cenników. W wersjach komercyjnych istnieje możliwość zakupienia dodatkowych katalogów i cenników, które ułatwiają sporządzanie kosztorysów obejmujących prace, niewystępujące w standardowej konfiguracji programu.

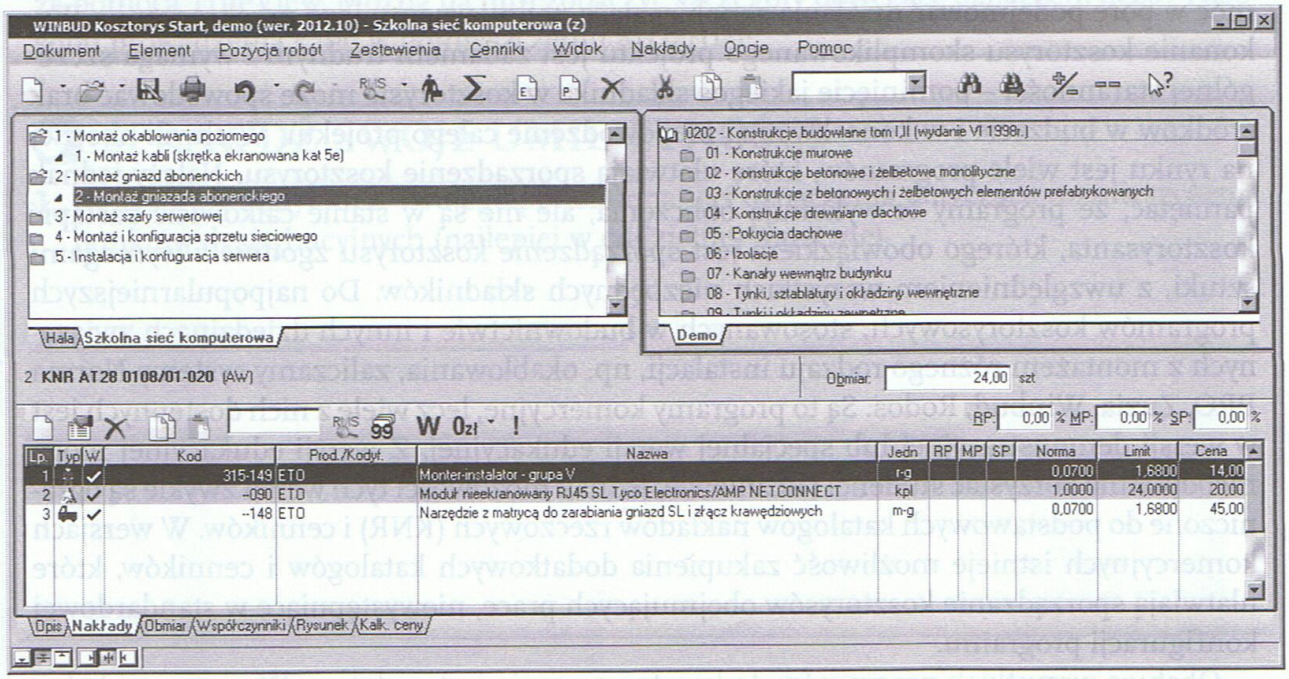
Obsługa wszystkich programów do kosztorysowania jest podobna. W pierwszej kolejności należy utworzyć nowy projekt kosztorysu i nanieść informacje podstawowe, np. nazwę i typ kosztorysu, datę utworzenia oraz informacje o sporządzającym (rys. 31.1).

Do przygotowanego w ten sposób kosztorysu można wprowadzać poszczególne zadania i prace do wykonania. W przykładowym kosztorysie sieci komputerowej dla szkolnej pracowni komputerowej (rys. 31.2) prace podzielono na pięć części.

Możemy zauważyć, że w punkcie 2. przewidziano montaż gniazd abonenckich. Informacje niezbędne do obliczenia kosztu wykonania tego zadania można pobrać z katalogu nakładów rzeczowych (KNR). W tym celu należy w prawym panelu okna odszukać odpowiednią pozycję (odpowiedni katalog) i przeciągnąć ją do panelu lewego. W przykładzie wykorzystany został katalog KNR AT-28. W wersji komercyjnej katalog ten może być



Rys. 31.1. Zarządzanie dokumentami kosztorysu

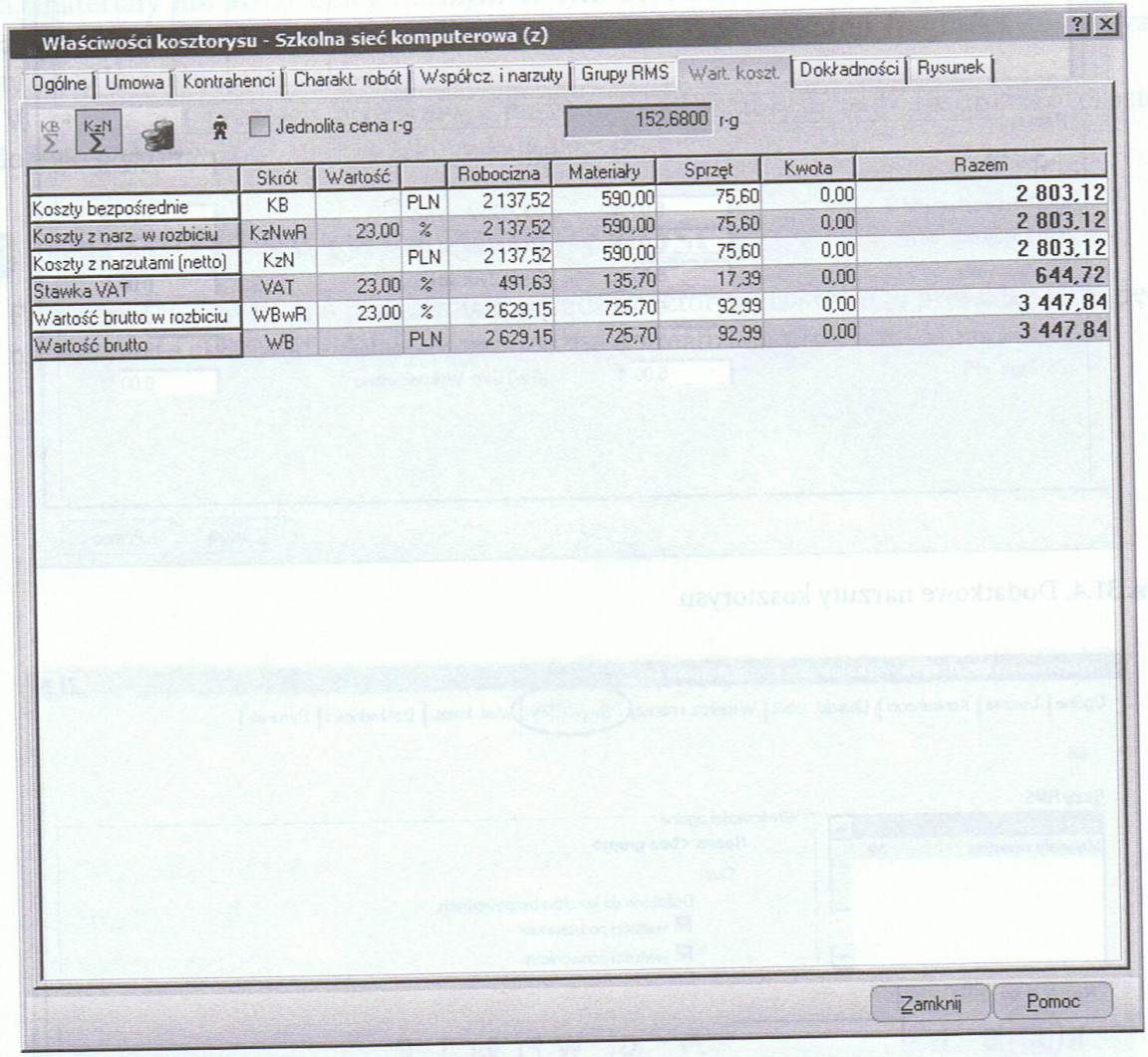


Rys. 31.2. Zadania do realizacji zdefiniowane w kosztorysie

dodatkowo zakupiony, natomiast w wersji demonstracyjnej wszystkie informacje należy wprowadzić ręcznie. Z obmiaru robót wynika, że w pracowni należy zainstalować 24 gniazda. Do wykonania tego zadania niezbędna jest praca montera-instalatora (według normy z nakładem pracy 0,07 r-g na każde gniazdo). Średnie stawki godzinowe pracowników różnych specjalności, w różnych regionach kraju można odszukać w bazach cen i materiałów, np. INTERCENBUD, SECOCENBUD (cenniki te również należy dodatkowo zakupić i okresowo aktualizować). Podawane ceny stanowią jedynie odniesienie do średnich cen i powinny być dostosowane do warunków realizacji konkretnego projektu. W naszym przykładzie przyjęto stawkę godzinową pracy montera – 14 zł/h. Koszt gniazda (materia-

łów) wynosi 20 zł. Ponadto monter będzie używał narzędzia (maszyny), którego godzina eksploatacji kosztuje 45 zł (wartość można przyjąć na podstawie baz danych, indywidualnie sporządzanych kalkulacji lub po negocjacjach pomiędzy wykonawcą a inwestorem).

Podsumowanie wszystkich kosztów pokazano na rysunku 31.3. W kosztach brutto uwzględniony został również podatek VAT w wysokości 23% ceny kosztów bezpośrednich.



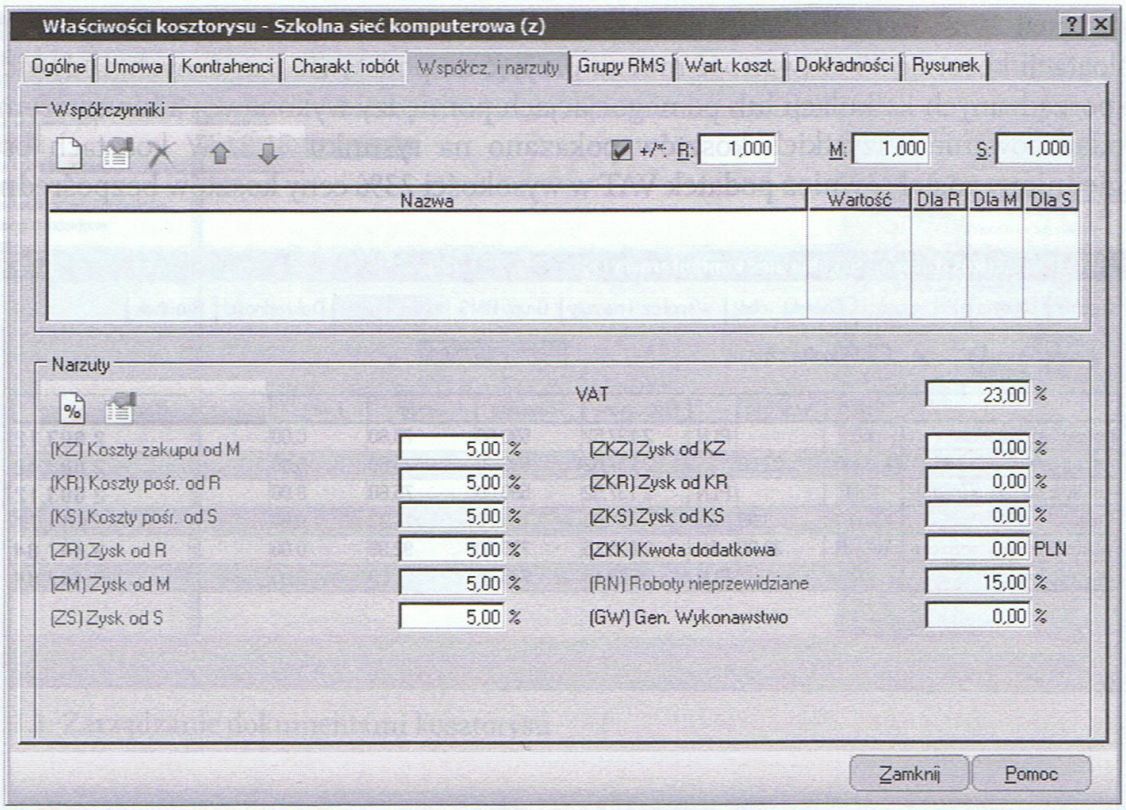
	Skrót	Wartość		Robocizna	Materiały	Sprzęt	Kwota	Razem
Koszty bezpośrednie	KB		PLN	2 137,52	590,00	75,60	0,00	2 803,12
Koszty z narz. w rozbiciu	KzNwR	23,00	%	2 137,52	590,00	75,60	0,00	2 803,12
Koszty z narzutami (netto)	KzN		PLN	2 137,52	590,00	75,60	0,00	2 803,12
Stawka VAT	VAT	23,00	%	491,63	135,70	17,39	0,00	644,72
Wartość brutto w rozbiciu	WBwR	23,00	%	2 629,15	725,70	92,99	0,00	3 447,84
Wartość brutto	WB		PLN	2 629,15	725,70	92,99	0,00	3 447,84

Rys. 31.3. Podsumowanie kosztorysu

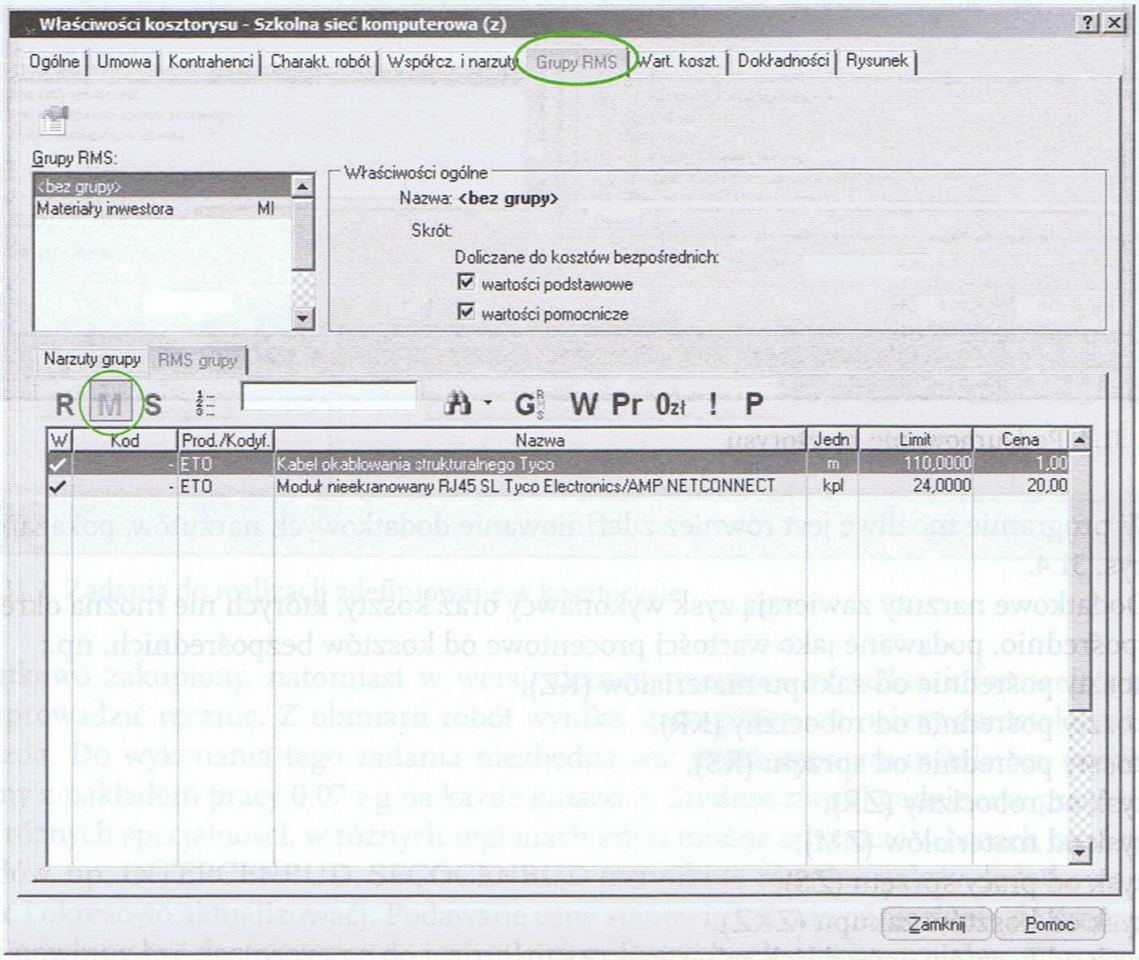
W programie możliwe jest również zdefiniowanie dodatkowych narzutów, pokazanych na rys. 31.4.

Dodatkowe narzuty zawierają zysk wykonawcy oraz koszty, których nie można określić bezpośrednio, podawane jako wartości procentowe od kosztów bezpośrednich, np.:

- koszty pośrednie od zakupu materiałów (KZ),
- koszty pośrednie od robocizny (KR),
- koszty pośrednie od sprzętu (KS),
- zysk od robocizny (ZR),
- zysk od materiałów (ZM),
- zysk od pracy sprzętu (ZS),
- zysk od kosztów zakupu (ZKZ),
- zysk od kosztów pośrednich robocizny (ZKR),
- zysk od kosztów pośrednich sprzętu (ZKS).



Rys. 31.4. Dodatkowe narzuty kosztorysu



Rys. 31.5. Koszty materiałów do wykonania okablowania

Ponadto mogą wystąpić takie składniki, jak:
- kwota dodatkowa (ZKK),
- roboty nieprzewidziane (RN),
- generalne wykonawstwo (GW).

Przeglądanie kosztorysu możliwe jest również w poszczególnych kategoriach: robocizna, materiały lub koszt pracy maszyn. W tym celu na zakładce Grupy RMS należy zaznaczyć ikonę M – koszty materiałów. Na rysunku 31.5 pokazano fragment kosztorysu dotyczący kosztów materiałów.

W przypadku prostych projektów, sporządzenie kosztorysu jest stosunkowo proste, a do jego wykonania wystarczy arkusz kalkulacyjny.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Przy pomocy dowolnego programu sporządź kosztorys dla swojego projektu. Uwzględnij wszystkie składniki i działania konieczne do realizacji projektu.

III. Projektowanie i montaż okablowania

- Normy i zalecenia dotyczące montażu okablowania strukturalnego
- Funkcje urządzeń sieciowych
- Symbole graficzne dotyczące lokalnych sieci komputerowych
- Zasady bezpiecznej i higienicznej pracy podczas montażu
- Zasady organizacji pracy i analizy harmonogramów prac
- Narzędzia do montażu okablowania strukturalnego
- Metody i zasady pomiarów okablowania strukturalnego
- Metody pomiarów sieci logicznej
- Rodzaje testów i pomiarów pasywnych
- Rodzaje testów i pomiarów aktywnych
- Cenniki materiałów do montażu okablowania strukturalnego

III. Projektowanie i montaż okablowania

- Normy i zalecenia dotyczące montażu okablowania strukturalnego
- Funkcje urządzeń sieciowych
- Symbole graficzne dotyczące lokalnych sieci komputerowych
- Zasady bezpiecznej i higienicznej pracy podczas montażu
- Zasady organizacji pracy i analizy harmonogramów prac
- Narzędzia do montażu okablowania strukturalnego
- Metody i zasady pomiarów okablowania strukturalnego
- Metody pomiarów sieci logicznej
- Rodzaje testów i pomiarów pasywnych
- Rodzaje testów i pomiarów aktywnych
- Cenniki materiałów do montażu okablowania strukturalnego

32 Normy i zalecenia dotyczące montażu okablowania strukturalnego

ZAGADNIENIA

- **Jakie organizacje ustanawiają normy dotyczące okablowania strukturalnego?**
- **Jakie normy dotyczące okablowania strukturalnego obowiązują w Polsce?**
- **Jakie są najważniejsze zalecenia wynikające z norm okablowania strukturalnego?**
- **Jakie są maksymalne długości kabla poziomego?**
- **Jakie wartości przyjmuje minimalny promień gięcia?**
- **Jaka jest minimalna odległość kabla od źródeł zakłóceń?**

Okablowanie strukturalne ma za zadanie umożliwić przyłączenie do sieci dowolnego sprzętu wyprodukowanego przez różnych wytwórców. Aby to było możliwe, urządzenia muszą być zgodne ze standardami opracowanymi przez instytucje standaryzacyjne. Do organizacji standaryzacyjnych zaliczamy między innymi:

- **ANSI** (*American National Standards Institute*) – amerykańska organizacja standaryzacyjna. ANSI jest prywatną, pozarządową instytucją typu „non-profit". Zajmuje się normami technologicznymi, np. opracowała jeden ze standardów kodowania liter w komputerach.
- **IEEE** (*The Institute of Electrical and Electronics Engineers*) – organizacja zrzeszająca inżynierów z całego świata (opracowała między innymi standardy dotyczące Ethernetu).
- **ISO** (*International Organization for Standarization*) – międzynarodowa organizacja standaryzacyjna (opracowała między innymi model sieci ISO/OSI).
- **IETF** (*Internet Engineering Task Force*) – organizacja, która publikuje dokumenty RFC (*Request for Comments*), regulujące rozwój internetu.
- **Unia Europejska** - publikuje normy europejskie (EN).
- **EIA/TIA** (*Electronics Industry Association/Telecommunications Industry Association*) – organizacje, które stworzyły wiele standardów dotyczących komunikacji, np. normy RS-232 dotyczące wtyczek i kabli portów szeregowych (COM).

Stosowanie standardów instalacyjnych w sieciach okablowania strukturalnego umożliwia dołączanie sprzętu aktywnego pochodzącego od różnych producentów do infrastruktury kablowej. Standardy zapewniają elastyczność w momencie, gdy zachodzi potrzeba wymiany sprzętu lub zmiany jego umiejscowienia. W nowym miejscu wystarczy podłączyć sprzęt do istniejącego już przyłącza sieciowego i dokonać odpowiednich zmian w szafie dystrybucyjnej. Prace standaryzacyjne nad okablowaniem strukturalnym zapoczątkowane zostały w USA. Pierwszą normą dotyczącą okablowania strukturalnego była norma amerykańska EIA/TIA 568. Na niej wzorowane są normy międzynarodowa ISO 11801 i europejska EN 50173. W Polsce obowiązują ponadto normy krajowe:

- PN-EN 50174-1. Technika informatyczna, instalacja okablowania. Cz. 1. Specyfikacja i zapewnienie jakości.

- PN-EN 50174-2. Technika informatyczna, instalacja okablowania. Cz. 2. Planowanie i wykonawstwo instalacji wewnątrz budynków.
- PN-EN 50174-3. Technika informatyczna, instalacja okablowania. Cz. 3. Planowanie i wykonawstwo instalacji na zewnątrz budynków.

Najważniejsze zalecenia wynikające z powyższych norm:

1. Okablowanie poziome powinno tworzyć nieprzerwane połączenie od punktu dystrybucyjnego do punktu abonenckiego.
2. Należy umieścić jeden punkt abonencki (2xRJ-45) na każde 10 m^2 powierzchni biurowej.
3. Na każdym piętrze budynku powinien być punkt dystrybucyjny (w przypadku małej liczby punktów abonenckich możliwe jest ich przyłączenie do punktu dystrybucyjnego na innym piętrze).
4. Wszystkie kable muszą być zakończone w gniazdach abonenckich i szafach dystrybucyjnych.
5. W obrębie całej sieci powinno się stosować jednakowe przewody (kable miedziane o jednakowej impedancji i średnicy, a kable światłowodowe o jednakowych włóknach).
6. Rozplot kabla UTP nie powinien być większy niż 13 mm.
7. Każdy element systemu powinien być czytelnie oznaczony (jednakowe oznaczenie na obu końcach kabla).
8. Sieć musi posiadać pełną dokumentację.

32.1. Zalecenia dotyczące kabli w przebiegach poziomych

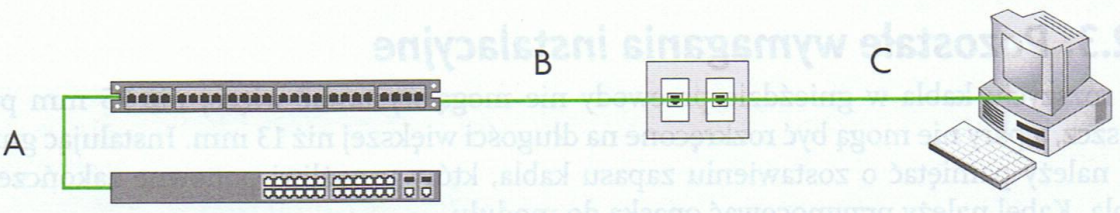
Normy zalecają stosowanie 4-parowego symetrycznego kabla STP lub UTP kategorii co najmniej 5e dla wszystkich kanałów poziomych. Kabel musi spełniać parametry wymagane przez normy:

- średnica przewodów: 0,45/0,65 mm,
- nominalna impedancja: 100 Ω ± 15%,
- tłumienność: dla kategorii 5 przy f = 100 MHz – 24,0 dB, dla kategorii 6 przy f = 100 MHz – 21,1 dB.

Całkowita długość kanału nie może przekroczyć 100 m. W okablowaniu poziomym maksymalna długość przebiegu kabla poziomego pomiędzy punktem abonenckim a punktem dystrybucyjnym w panelu krosowym (*patch panel*) wynosi 90 m (na rysunku 32.1 oznaczona literą B). Maksymalna długość kabli krosowych pomiędzy panelem krosowym a przełącznikiem wynosi 6 m (na rysunku 32.1. oznaczona literą A). Łączna długość kabla stacyjnego i krosowego może mieć maksymalnie 10 m (na rysunku 32.1. oznaczona literą A+C).

Podczas układania kabla w przebiegach poziomych należy przestrzegać następujących zasad:

- kable biegnące ponad sufitem podwieszanym nie powinny być mocowane do konstrukcji sufitu;



Rys. 32.1. Kanał kablowy poziomy

- odległości pomiędzy punktami mocowania kabli poziomych nie powinny być większe niż 1,2 – 1,5 m;
- aby zachować przejrzystość instalacji i ułatwić obsługę, należy wszystkie kable prowadzić prostopadle lub równolegle do korytarza;
- kable wchodzące i wychodzące do/z pomieszczeń (pod kątem 90°) powinny skręcać łagodnie (minimalny promień skrętu = 8 średnic kabla);
- instalując kable, należy sprawdzać, czy nie są naprężone na końcach i na całym swoim przebiegu. Jeżeli kable znajdują się na otwartej przestrzeni, powinny być umieszczone w jednej płaszczyźnie, nie wolno owijać kabli dookoła rur, kolumn, itp.;
- kable, na całej długości od gniazda abonenckiego do punktu dystrybucyjnego, powinny być wolne od sztukowań, zagnieceń i nacięć lub złamań;
- nie można rozdzielać par przewodów na dwa kanały komunikacyjne;
- kable powinny być wyprowadzane i wprowadzane z głównych tras przebiegu pod kątem 90°, zaś promień ich zagięć w kanałach powinien być zgodny z zaleceniami producenta kabla. Jeżeli producent nie zaleci inaczej, przyjmuje się minimalny promień zgięcia:
  - dla skrętki UTP – 4 średnice kabla,
  - dla skrętki STP – 6 średnic kabla,
  - dla kabla światłowodowego od 10 do 20 średnic w zależności od sposobu wykonania.

Ustalając trasę przebiegu kabla, należy zachować następujące odległości od źródeł zasilania:

- 30 cm od wysokonapięciowego oświetlenia (świetlówki),
- 90 cm od przewodów elektrycznych 5 KVA lub więcej,
- 100 cm od transformatorów i silników.

32.2. Wymagania instalacyjne dla przebiegów pionowych

Do budowy przebiegów pionowych zalecane jest używanie kabli światłowodowych lub – w wyjątkowych przypadkach – skrętki. Do prowadzenia kabli między piętrami stosowany jest rękaw lub szyb. Zaleca się rękawy o średnicy co najmniej 10 cm (mogą one wystawać od 2,5 cm do 10 cm powyżej płaszczyzny podłogi) lub prostokątne szyby o minimalnym wymiarze 15 cm × 22,5 cm.

Jeżeli trasa przebiegu kabli pionowych obejmuje więcej niż dwa piętra lub gdy kable są wyjątkowo ciężkie (np. wieloparowe kable miedziane), muszą być one mocowane. Mocowanie można wykonać np. za pomocą specjalnej żyły podtrzymującej, ułożonej po całej trasie kabla między najwyższym piętrem i piwnicą. Kabel należy połączyć z żyłą podtrzymującą co 90 cm, przy czym na jedno piętro powinny przypadać minimum trzy punkty wiązania. Dla dużych ilości kabli lub dla kabli wyjątkowo ciężkich powinna być użyta obejma lub osłona dla grupy kabli z każdego piętra. Ze względu na ochronę przeciwpożarową przejścia pomiędzy piętrami powinny być uszczelnione za pomocą specjalnych uszczelniaczy, powłoki przeciwpożarowej, pianki, kitu itp.

32.3. Pozostałe wymagania instalacyjne

Po rozszyciu kabla w gnieździe przewody nie mogą wystawać więcej niż 25 mm poza płaszcz, a pary nie mogą być rozkręcone na długości większej niż 13 mm. Instalując gniazda, należy pamiętać o zostawieniu zapasu kabla, który umożliwi ponowne zakończenie kabla. Kabel należy przymocować opaską do modułu.

Kable doprowadzone do punktów dystrybucyjnych powinny być logicznie pogrupowane, aby ułatwić ich zakończenie w szafie. Należy zapewnić odpowiedni zapas kabla, który umożliwi przeprowadzenie prac konserwacyjnych. Przy prowadzeniu kabli na panelu z wieszakami należy zwrócić uwagę na zapewnienie minimalnego promienia zagięcia.

Punkty dystrybucyjne umożliwiają krosowanie przebiegów poziomych do portów sprzętu aktywnego lub do przebiegów pionowych. Każdy punkt dystrybucyjny powinien być zlokalizowany tak, aby przebiegi poziome nie przekraczały 90 metrów. IDF powinny być podzielone na logiczne sekcje, grupujące połączenia o podobnej funkcji, obszarze itp. Tablice z uchwytami na kable powinny być zlokalizowane powyżej i poniżej sekcji krosowań. Boczne wieszaki należy mocować w odstępie 3 do 4 pozycji (U), aby ułatwić trzymanie kabli krosowych poza obszarem pola krosowego.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sporządź wskazówki dla montera, który będzie instalował okablowanie w projektowanej przez Ciebie sieci.

33 Funkcje urządzeń sieciowych

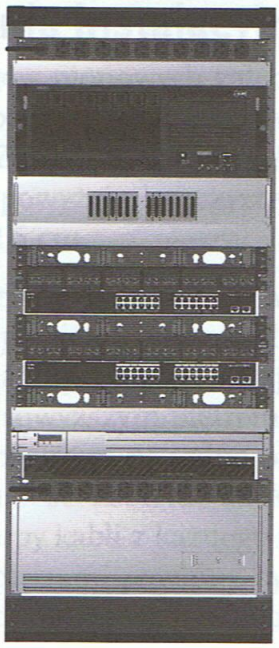
ZAGADNIENIA

- **Jaki sprzęt jest montowany w szafach dystrybucyjnych?**
- **Jakie funkcje powinny posiadać urządzenia w warstwach dostępu, dystrybucji i rdzenia?**

W punktach dystrybucyjnych gromadzony jest sprzęt aktywny, taki jak przełączniki i routery, umożliwiający przyłączenie do sieci urządzeń oraz przyłączenie sieci do internetu. Urządzenia te montowane są w specjalnych szafach dystrybucyjnych lub ramach montażowych – najczęściej typu RACK o szerokości 19". Oprócz tych urządzeń w szafach może znajdować się również inny sprzęt niezbędny do funkcjonowania sieci, taki jak:

- serwery (w obudowie typu RACK),
- moduły pamięci zewnętrznej,
- urządzenia aktywne zabezpieczające sieć, np firewalle, IPS/IDS,
- zasilacze UPS.

Przykładowe rozmieszczenie urządzeń w szafie pokazano na rysunku 33.1.



Rys. 33.1. Przykładowe rozmieszczenie urządzeń w szafie dystrybucyjnej

W pośrednich punktach dystrybucyjnych najczęściej będą umieszczane przełączniki obsługujące warstwę dostępu. Przełączniki obsługujące warstwę dystrybucji i rdzenia najczęściej będą umieszczane w głównym punkcie dystrybucyjnym. Przełączniki obsługujące warstwę dostępu umożliwiają podłączenie urządzeń końcowych do sieci. Z tego powodu przełączniki te muszą być wyposażone w takie funkcje, jak:

- **Zabezpieczenia portów** – umożliwia przełącznikowi podejmowanie decyzji, ile urządzeń może się łączyć z przełącznikiem lub jakie konkretne urządzenia mogą to robić. Decyzje te najczęściej podejmowane są na podstawie adresu fizycznego MAC przyłączonego urządzenia.
- **Obsługa sieci VLAN** – umożliwiają oddzielenie społeczności użytkowników lub różnych rodzajów ruchu, np. dane głosowe mogą być przesyłane w osobnej sieci VLAN, dzięki czemu można im zapewnić większą szerokość pasma.
- **Obsługa standardu Fast Ethernet/Gigabit Ethernet** – Fast Ethernet jest odpowiedni dla telefonii IP i transmisji danych w większości sieci, Gigabit Ethernet jest szybszy, ale przełączniki obsługujące ten standard są droższe (choć różnica w cenie jest coraz mniejsza, co skłania użytkowników do budowania nowych sieci w standardzie Gigabit Ethernet).
- **Zasilanie przez Ethernet (PoE)** – funkcja ta powinna być stosowana tylko wtedy, gdy jest wymagana obsługa telefonów IP lub bezprzewodowe punkty dostępowe i trudno jest doprowadzić zasilanie do żądanego miejsca.
- **Obsługę jakości usług (QoS)** – umożliwia nadawanie priorytetu określonych rodzajom danych, które administrator chciałby traktować w sposób szczególny, np. przesyłać szybciej niż inne rodzaje danych.
- **Agregacja łączy** – funkcja ta pozwala przełącznikowi na wykorzystywanie jednocześnie kilku portów jako jednego łącza logicznego o dużej szerokości pasma. Najczęściej wykorzystywane będzie do połączenia z przełącznikiem warstwy dystrybucji.

Przełączniki z warstwy dystrybucji odbierają dane pochodzące ze wszystkich przełączników z warstwy dostępu i przekazują te dane do przełączników z warstwy rdzenia. Przełączniki z warstwy dystrybucji powinny zapewniać:

- **funkcję routingu między sieciami VLAN** (wymagana jest większa wydajność przetwarzania oraz funkcjonalności warstwy 3);
- **stosowanie zaawansowanych zasad zapewniających bezpieczeństwo ruchu w sieci** – listy kontroli dostępu (*Access Control List*, ACL) umożliwiają przełącznikowi zezwalanie na określony typ ruchu i niezezwalanie na inny oraz decydowanie, które urządzenia sieciowe mogą się komunikować w sieci;
- **nadmiarowość** – zaleca się, aby współpracowały z więcej niż jednym zasilaczem energii elektrycznej, zdolnym do wymiany w ruchu bez konieczności wyłączenia urządzenia oraz umożliwiały takie zaprojektowanie infrastruktury, że w przypadku awarii pojedynczych elementów nie nastąpi przerwa w działaniu sieci;
- **agregację łączy** – nowsze przełączniki pozwalają korzystać z zagregowanych łączy nadrzędnych 10 Gigabit Ethernet prowadzących do przełączników z warstwy rdzenia oraz dostępu;
- **obsługę jakości usług (QoS)** – aby został utrzymany priorytet danych przychodzących z przełączników z warstwy dostępu, w których zaimplementowano mechanizmy QoS.

Przełączniki z warstwy rdzenia są odpowiedzialne za obsługę większości danych przesyłanych w komutowanej sieci LAN i powinny zapewnić bardzo dużą szybkość przesyłania danych. Powinny cechować się dużą nadmiarowością, np. być zaopatrzone w nadmiarowe zasilacze, które można wymieniać bez przerywania pracy przełącznika, funkcje chłodzenia z możliwością wymiany wentylatorów bez konieczności wyłączania przełącznika itp. Przełączniki z warstwy rdzenia powinny współpracować ze zagregowanymi połączeniami 10 Gigabit Ethernet i zapewniać obsługę jakości usług (QoS).

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Dobierz przełączniki (liczbę i typ), które będą używane w projektowanej przez Ciebie sieci.

34 Symbole graficzne dotyczące lokalnych sieci komputerowych

ZAGADNIENIA

- **Jakie symbole są używane do reprezentowania elementów sieci lokalnych?**
- **W jaki sposób na rysunkach umieszczać dodatkowe oznaczenia, np. sposób prowadzenia kabli?**

Sieci komputerowe w dokumentacji przedstawiane są za pomocą schematów, w których poszczególne urządzenia zastępowane są za pomocą symboli. Na rysunkach schematycznych przedstawia się zasadnicze elementy bez określania szczegółów, np. wyglądu, wymiarów urządzeń itp. Schemat logiczny okablowania strukturalnego sieci pokazano na rysunku 34.1. Na schemacie tym można zobaczyć zależności i połączenia logiczne pomiędzy punktami dystrybucyjnymi sieci.

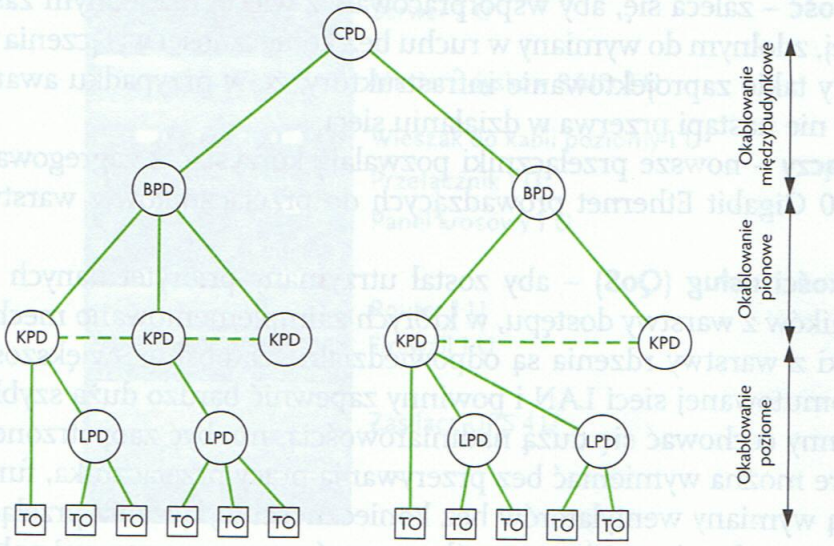
Na schemacie użyto symboli:

KPD – punkt dystrybucyjny odpowiednio KPD-kondygnacyjny, BPD-budynkowy, CPD – kampusowy centralny,

LPD – lokalny punkt dystrybucyjny LPD,

TO – gniazdo telekomunikacyjne TO.

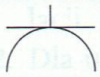
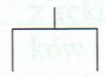
Linią przerywaną zaznaczono kable opcjonalne, np. zapewniające nadmiarowość sieci.

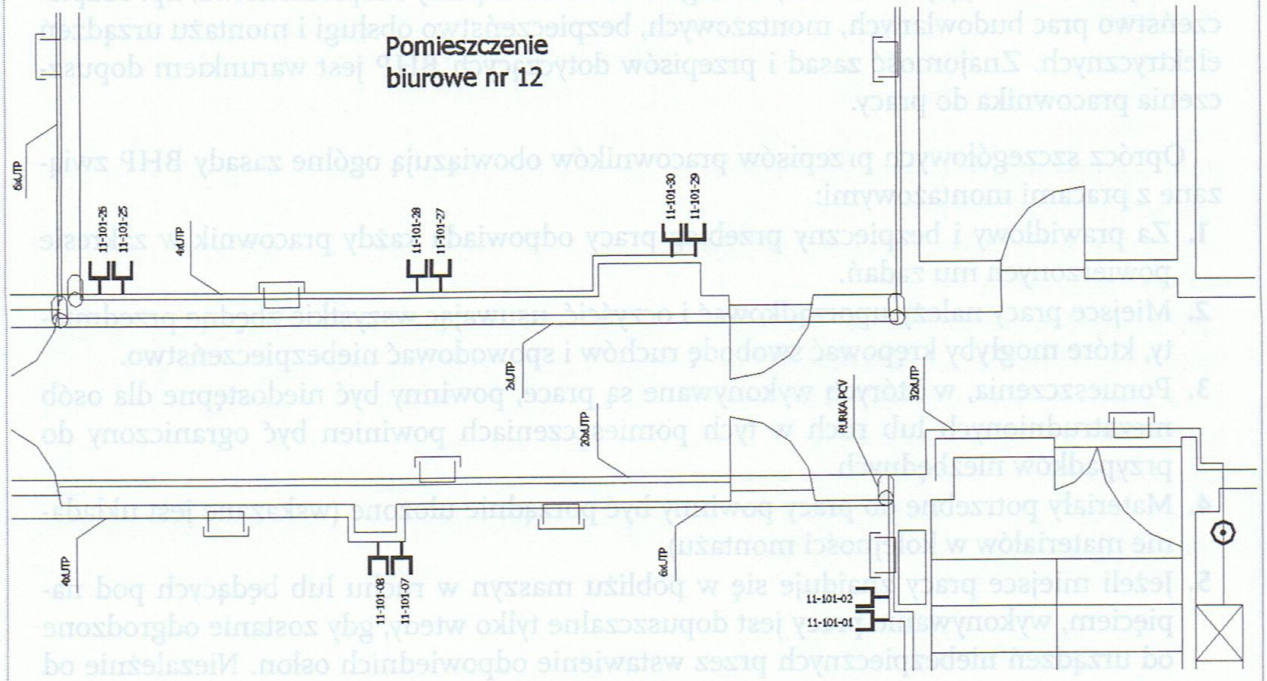


Rys. 34.1. Schemat logiczny sieci komputerowej

Monter sieci komputerowej w pracy posługuje się planem instalacji, na którym zaznaczono rozmieszczenie gniazd oraz liczbę i sposób prowadzenia kabli. W planach stosowane są symbole używane w rysunku technicznym elektrycznym opisane w normie PN- 92/E-01200. Symbole graficzne stosowane są w schematach. Przykłady symboli i ich znaczenie podano w tabeli 34.1.

Tabela 34.1. Przykłady symboli używanych w planach instalacji

Symbol	Opis symbolu	Symbol	Opis symbolu
	Gniazdo elektryczne ze stykiem ochronnym		Linia odchodząca w dół
	Gniazdo elektryczne		Linia przychodząca z dołu
	Gniazdo telekomunikacyjne – symbol ogólny		Korytko kablowe kryte
	Linia odchodząca w górę		Korytko kablowe kryte – oznaczenie końca
	Linia przychodząca z góry		Linia w rurze ochronnej



Rys. 34.2. Fragment planu instalacji okablowania strukturalnego

Oprócz symboli na planach umieszcza się również dodatkowe opisy, określające np. oznaczenia gniazd lub liczbę i typ kabla. Przykład fragmentu planu z naniesionymi oznaczeniami pokazano na rysunku 34.2.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Używając symboli, wykonaj schemat projektowanej sieci.
2. Na rysunek techniczny budynku nanieś oznaczenia gniazd, kabli i sposobu ich prowadzenia (skorzystaj z oddzielnej warstwy).

35 Zasady bezpiecznej i higienicznej pracy podczas montażu

ZAGADNIENIA

- **Jakie przepisy prawa regulują kwestie związane z BHP?**
- **Jakie są podstawowe zasady BHP podczas prac montażowych?**

Podstawowym aktem prawnym regulującym w ogólny sposób sprawy bezpieczeństwa i higieny pracy jest *Kodeks pracy*. Do *Kodeksu pracy* wydano wiele aktów prawnych wykonawczych, omawiających bardziej szczegółowo różne aspekty bezpieczeństwa, np. bezpieczeństwo prac budowlanych, montażowych, bezpieczeństwo obsługi i montażu urządzeń elektrycznych. Znajomość zasad i przepisów dotyczących BHP jest warunkiem dopuszczenia pracownika do pracy.

Oprócz szczegółowych przepisów pracowników obowiązują ogólne zasady BHP związane z pracami montażowymi:

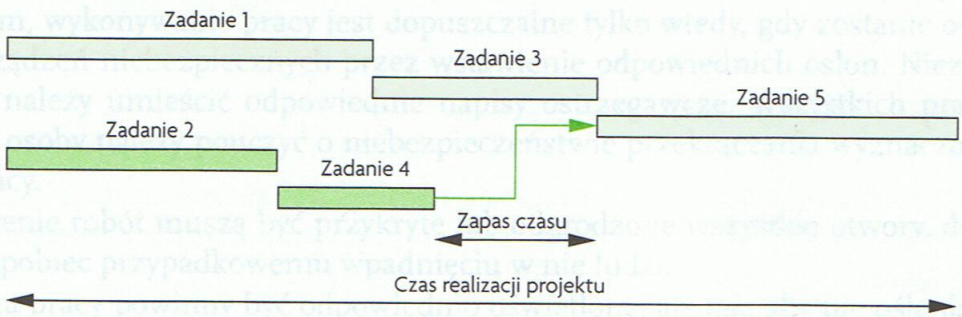
1. Za prawidłowy i bezpieczny przebieg pracy odpowiada każdy pracownik w zakresie powierzonych mu zadań.
2. Miejsce pracy należy uporządkować i oczyścić, usuwając wszystkie zbędne przedmioty, które mogłyby krępować swobodę ruchów i spowodować niebezpieczeństwo.
3. Pomieszczenia, w których wykonywane są prace, powinny być niedostępne dla osób niezatrudnionych lub ruch w tych pomieszczeniach powinien być ograniczony do przypadków niezbędnych.
4. Materiały potrzebne do pracy powinny być porządnie ułożone (wskazane jest układanie materiałów w kolejności montażu).
5. Jeżeli miejsce pracy znajduje się w pobliżu maszyn w ruchu lub będących pod napięciem, wykonywanie pracy jest dopuszczalne tylko wtedy, gdy zostanie odgrodzone od urządzeń niebezpiecznych przez wstawienie odpowiednich osłon. Niezależnie od osłon należy umieścić odpowiednie napisy ostrzegawcze. Wszystkich pracowników i inne osoby należy pouczyć o niebezpieczeństwie przekraczania wyznaczonego terenu pracy.
6. Na terenie robót muszą być przykryte lub odgrodzone wszystkie otwory, doły i rowy, aby zapobiec przypadkowemu wpadnięciu w nie ludzi.
7. Miejsca pracy powinny być odpowiednio oświetlone, ale tak, aby nie oślepiać pracowników.
8. Na każdym stanowisku powinna być zapewniona możliwość korzystania ze sprzętu zapewniającego bezpieczną pracę.
9. Monter odpowiada za dobre wykonanie montażu powierzonych mu instalacji, za bezpieczeństwo własne i swoich współpracowników, za oszczędne zużycie materiałów oraz za prawidłowe posługiwanie się narzędziami.

10. W czasie kucia otworów i bruzd w murach należy używać okularów ochronnych, bez których praca jest wzbroniona.
11. Podczas pracy należy zwracać szczególną uwagę na to, aby nie uszkodzić innych instalacji.
12. Dla umożliwienia doraźnej pomocy medycznej w razie wypadku, należy w miejscach widocznych i dostępnych umieścić apteczki.
13. Przy wykonywaniu prac na wysokości, narzędzia należy przechowywać w specjalnej torbie narzędziowej. Należy uważać, aby w czasie pracy nie wypuszczać narzędzi z ręki, gdyż upadając, mogą one skaleczyć innych pracowników. Zależnie od warunków i rodzaju miejsca pracy używane muszą być drabiny, rusztowania itp.
14. Na drabinie może przebywać tylko jedna osoba. Nie wolno wiązać ze sobą dwóch krótkich drabin w celu uzyskania jednej dłuższej. W czasie wchodzenia na drabinę obie ręce powinny być wolne, aby lepiej się jej trzymać.
15. Przed rozpoczęciem pracy przy użyciu sprzętu i narzędzi o napędzie elektrycznym, np. wiertarki, należy sprawdzić, czy działają one prawidłowo.

36 Zasady organizacji pracy i analizy harmonogramów prac

ZAGADNIENIA
- **Czym jest ścieżka krytyczna i jak się ją wyznacza?**
- **Jakie właściwości ma ścieżka krytyczna?**

Realizacja projektu, np. okablowania strukturalnego, wymaga zaangażowania materiałów oraz określonych środków zarówno ludzkich, jak i finansowych. Projekt powinien być zakończony w określonym czasie. Przez cały okres realizacji projektu podlega on procesowi zarządzania, mającemu na celu doprowadzenie go do szczęśliwego końca. Istotnym czynnikiem jest zapewnienie odpowiedniego harmonogramu pracy, tak aby każdy pracownik zaangażowany w projekt wiedział, jakie zadanie i kiedy ma wykonać oraz z jaką dokładnością. Wszystkie zadania prowadzące do realizacji projektu mogą być uporządkowane zgodnie z terminami ich wykonania i zilustrowane, np. za pomocą wykresu Gantta lub diagramu nadrzędności (PDM). Seria połączonych zadań prowadzących od początku do końca projektu nazywana jest ścieżką. W każdym projekcie można wyróżnić ścieżkę krytyczną. Jest to nieprzerwany ciąg zadań o najdłuższym czasie realizacji. Wszystkie zadania znajdujące się na ścieżce krytycznej nazywamy zadaniami krytycznymi. Opóźnienie któregokolwiek z nich spowoduje późniejsze zakończenie całego projektu. Przykład wykresu Gantta z 5 zadaniami pokazany został na rysunku 36.1. Kolorem jaśniejszym zaznaczono zadania krytyczne. Można zauważyć, że w zadaniach nieznajdujących się na ścieżce krytycznej (zaznaczonych kolorem ciemniejszym) występuje **zapas czasu** – opóźnienie któregoś z tych zadań nie spowoduje opóźnienia całego projektu (pod warunkiem, że opóźnienie nie będzie większe niż zapas czasu).



Rys. 36.1. Przykład ścieżki krytycznej

Wyróżnia się następujące właściwości ścieżki krytycznej:
- w projekcie jest co najmniej jedna ścieżka krytyczna – na ogół tylko jedna;
- pierwsze zadanie ścieżki krytycznej zaczyna się wraz z początkiem projektu;
- każde kolejne zadanie ścieżki krytycznej może się zacząć dopiero po zakończeniu poprzedniego;

- zakończenie ostatniego zadania ścieżki krytycznej oznacza zakończenie projektu;
- czas trwania ścieżki krytycznej determinuje czas trwania całego projektu; w przypadkach, gdy istnieje więcej niż jedna ścieżka krytyczna, wówczas wszystkie ścieżki krytyczne mają ten sam sumaryczny czas trwania;
- ścieżka krytyczna może się zmienić w czasie trwania projektu, jeśli czasy wykonania poszczególnych zadań będą się różniły od początkowo zakładanych.

Skrócenie czasu realizacji zadania w niektórych przypadkach jest możliwe poprzez zaangażowanie większych zasobów, np. zwiększenie liczby pracowników. Jeżeli w zadaniu występuje szeroki front robót, a pracochłonność jakiegoś zadania jest obliczona np. na 10 roboczogodzin, to jeden pracownik będzie potrzebował dwa razy więcej czasu niż dwóch pracowników. W niektórych pracach lepsze efekty przynosi współdziałanie pracowników, np. zlecenie montażu okablowania dwóm pracownikom pozwala na szybsze wykonanie prac niż w przypadku, gdyby każdy z nich pracował oddzielnie. Istnieją jednak zadania, w których z przyczyn technologicznych skrócenie czasu realizacji jest niemożliwe, np. podczas kopania tunelu zwiększenie liczby pracowników nie powoduje zwiększenia wydajności, ponieważ tylko ograniczona liczba pracowników ma dostęp do miejsca pracy. W krańcowym przypadku może zajść sytuacja, w której zwiększenie zespołu pracowników spowoduje wydłużenie czasu realizacji, np. jeżeli istnieje konieczność przeprowadzenia uzgodnień dotyczących wykonywanej pracy pomiędzy pracownikami. Im większy zespół, tym więcej czasu trzeba poświęcić na komunikację wewnętrzną.

Zarządzanie projektem dotyczy również spraw związanych z finansami. Koszty ponoszone w trakcie realizacji projektu związane mogą być z wykorzystaniem zasobów, np. ludzkich, sprzętu itp. Stopień wykorzystania budżetu projektu powinien być porównywany z poziomem zaawansowania prac. Najczęściej analizy te sporządza się po zakończeniu pewnego etapu prac, spełnienia określonego warunku lub zrealizowania pewnego produktu cząstkowego (tzw. kamienie milowe projektu). W przypadku rozbieżności należy wprowadzić modyfikacje, aby jak najwcześniej zapobiegać przekroczeniu budżetu.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zidentyfikuj w swoim projekcie ścieżkę krytyczną. Określ wszystkie zadania krytyczne.
2. Czy w Twoim projekcie występuje zapas czasu? Jeśli tak, to jaki i w którym miejscu?

37 Narzędzia do montażu okablowania strukturalnego

ZAGADNIENIA

- **Jakie narzędzia są wykorzystywane do montażu okablowania strukturalnego?**
- **Jak posługiwać się narzędziami do montażu okablowania strukturalnego?**
- **Dlaczego nie należy zaglądać do światłowodu?**
- **Na czym polega i jak wykonać spawanie światłowodu?**

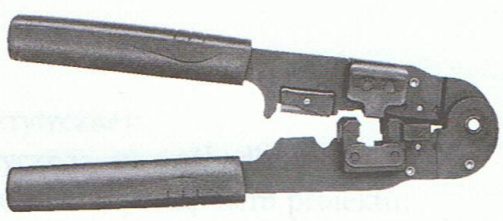
Instalator okablowania strukturalnego w swojej pracy musi posługiwać się różnymi narzędziami i urządzeniami. W zależności od rodzaju nośnika mogą to być narzędzia do kabli miedzianych lub światłowodowych. Generalnie można je podzielić na:

- narzędzia pracy,
- urządzenia diagnostyczne i pomiarowe.

Narzędzia pracy służą do wykonywania typowych zadań związanych z montażem danego typu nośnika oraz instalacji pomocniczych, np. koryt kablowych. Do najczęściej używanych narzędzi do montażu okablowania miedzianego zaliczamy:

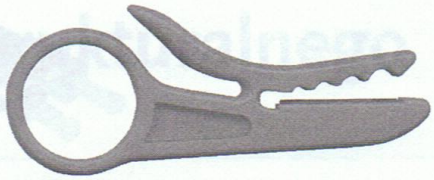
- **Narzędzie uderzeniowe** – urządzenie (rysunek 37.1) wykorzystywane do „zaszywania" kabli sieciowych i telefonicznych w nożach (złączach) LSA/KRONE, gniazdkach komputerowych, telefonicznych, panelach krosowych w szafach itp. Narzędzie wyposażone jest w obcinacz nadmiaru kabla wystającego poza złącze oraz haczyki do demontowania zaszytych kabli. Aby zaszyć kabel w złączu LSA, należy umieścić poszczególne żyły w gniazdach (bez ściągania izolacji), przyłożyć nóż do złącza i energicznym ruchem wcisnąć kabel w złącze. Nóż po dojściu do końca złącza wyda charakterystyczny dźwięk, a nadmiar kabla zostanie obcięty.
- **Narzędzie zaciskowe do wtyków RJ45** – wtyk RJ-45 z odpowiednio ułożonymi żyłami kabla należy wsunąć w gniazdo narzędzia (rysunek 37.2), a następnie zacisnąć dźwignie.

Rys. 37.1. Narzędzie uderzeniowe do montażu kabli



Rys. 37.2. Narzędzie zaciskowe do wtyków RJ-45

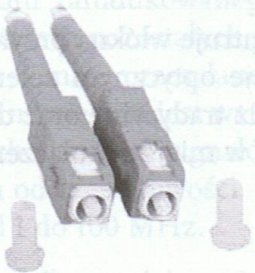
- **Narzędzie do zdejmowania izolacji** (rysunek 37.3) – pozwala na szybkie i wygodne zdjęcie izolacji zewnętrznej kabla. Narzędzie zabezpiecza kabel przed zbyt mocnym nacięciem izolacji, co mogłoby spowodować uszkodzenie przewodu.



Rys. 37.3. Narzędzie do zdejmowania izolacji

Montaż okablowania światłowodowego jest znacznie trudniejszy. Należy pamiętać, że przy uruchamianiu urządzeń aktywnych mamy do czynienia ze światłem o dużej mocy, zwykle emitowanym przez laser lub diodę LED. Typowe długości fali optycznej w transmisji danych są bliskie podczerwieni i wynoszą od 850 nm do 1550 nm – światła tego nie widać, jednak może ono poważnie uszkodzić oczy (nie warto patrzeć w nadajnik ani we włókno światłowodu, bo nawet jeśli nie uszkodzimy wzroku to i tak nic nie zobaczymy). W montażu okablowania światłowodowego wykorzystuje się gotowe, przygotowane wcześniej kable o określonej długości, zakończone odpowiednimi końcówkami (można je zakupić u producentów lub w wyspecjalizowanych firmach). Wybór typu końcówki jest zwykle narzucony poprzez standard, w którym wykonane są urządzenia aktywne. Najczęściej wykorzystywane są końcówki:

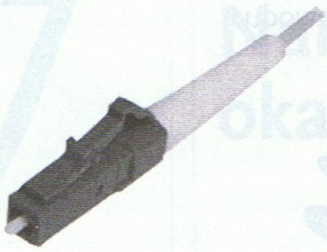
- **SC** (rysunek 37.4) – plastikowa obudowa i pewne połączenie,



Rys. 37.4. Końcówka kabla SC

- **LC** (rysunek 37.5) – mniejsze od poprzedniego, dość popularne ze względu na małe gabaryty i na użycie go w modułach SFP,
- **ST** (rysunek 37.6) – metalowe, przypominające elektryczne złącze BNC, stosowane częściej w sieciach wielomodowych.

Jeżeli wykorzystanie gotowego kabla z zamontowanymi końcówkami jest niemożliwe, można zakupić prefabrykowane tzw. pigtaile – z jednej strony zakończone złączem, a z drugiej gołym włóknem. Pigtail należy zespawać z włóknami kabla przy pomocy spawarki do światłowodów (rys. 37.7). Spawanie światłowodu polega na zetknięciu dwóch włókien czołami i nadtopieniu ich łukiem elektrycznym, tak aby zostały trwale połączone. Dobrze wykonany spaw jest praktycznie niewidoczny dla światła. Spawanie wymaga wysokich kwalifikacji pracowników i poniesienia dużych nakładów na zakup spawarki oraz urządzeń testujących. Istnieje możliwość wykonania tzw. „spawów mechanicznych" – jest



Rys. 37.5. Końcówka kabla LC

Rys. 37.6. Końcówka kabla ST

Rys. 37.7. Spawarka do światłowodów

to specjalny mechanizm, który centruje włókna przylegające do siebie i ewentualne przerwy i niedoskonałości kompensuje optycznym żelem wewnątrz. Połączenia wykonane taką techniką są gorszej jakości niż tradycyjne oraz droższe, ponieważ mechanizm „spawu" pozostaje na każdym włóknie w miejscu połączenia, jednak nie jest konieczny zakup spawarki.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sporządź listę narzędzi potrzebnych do wykonania okablowania w Twoim projekcie.
2. Wykonaj zaciskanie wtyku RJ-45. Przetestuj, czy złącze jest wykonane poprawnie.
3. Wykonaj montaż kabla w patchpanelu. Przetestuj, czy złącze jest wykonane poprawnie.

38 Metody i zasady pomiarów okablowania strukturalnego

ZAGADNIENIA

- **Jakie pomiary okablowania wykonuje się podczas montażu, a jakie podczas odbioru sieci?**
- **Jakie obowiązują normy i standardy dotyczące pomiarów okablowania sieci?**
- **Jakie parametry są mierzone przed wystawieniem certyfikatu zgodności okablowania?**

Podczas wykonywania okablowania strukturalnego instalator wykorzystuje urządzenia zdolne do sprawdzenia instalacji pod względem zgodności montażu i ciągłości kabli. Do tego celu można wykorzystać prosty tester okablowania, który pozwala na wykrycie usterek, takich jak niewłaściwe połączenia oraz brak przejść. Przy odbiorze instalacji okablowania należy wykonać bardziej szczegółowe testy, mające na celu sprawdzenie dodatkowych parametrów okablowania zgodnie z przyjętymi standardami i normami. W sieciach Ethernet pracujących z prędkością do 100 MB/s wykorzystywane do transmisji są tylko dwie pary przewodów. Dlatego zgodnie z biuletynem TIA/EIA/TSB-67 L.II, wystarczy przeprowadzić pomiar takich parametrów, jak:

Przesłuch zbliżny (*NEXT – Near End Crosstalk*) – pomiar przesłuchu zbliżnego NEXT polega na pomiarze poziomu sygnału zaindukowanego w jednej parze przewodów, od sygnału pochodzącego z dowolnej z trzech pozostałych par w kablu czteroparowym. Miarą parametru NEXT jest różnica mocy sygnału przesyłanego w parze zakłócającej i sygnału wytworzonego w parze zakłócanej. Im większa jest wartość bezwzględna NEXT, tym lepsza jest odporność na zakłócenia pochodzące od sygnałów w innych parach kabla. Wartość parametru NEXT jest silnie zależna od częstotliwości. W związku z tym należy dokonać pomiaru w paśmie częstotliwości od 1 do 100 MHz.

Tłumienie (*Attenuation*) – określa, o ile zmniejszy się moc sygnału w danej parze przewodów po przejściu przez cały tor kablowy. Parametr ten jest ściśle zależny od częstotliwości i pomiaru dokonuje się w paśmie od 1 do 100 MHz.

Mapa połączeń (*Wire map*) – określa, w jakiej sekwencji ułożone są w złączu lub gnieździe poszczególne pary przewodów. Najczęściej spotykanymi sekwencjami są EIA-568A i EIA-568B. Parametr ten służy do wykrycia błędów instalacyjnych, takich jak:

- zamienione pary (*crossed pairs*),
- zamienione poszczególne przewody (*split pairs*),
- zamienione przewody w parze (*reversed pairs*).

Długość (*Length*) – określa długość mierzonego toru transmisyjnego. Długość toru transmisyjnego na ogół jest większa od długości kabla, ponieważ pary są ze sobą skręcone, a dodatkowo wszystkie pary są skręcone wokół wspólnej osi. Rzeczywistą długość toru transmisyjnego wyznacza się poprzez pomiar czasu propagacji impulsu elektrycznego lub świetlnego przy znanej prędkości propagacji w danym typie kabla.

Wartości dopuszczalne poszczególnych parametrów wyspecyfikowane są w odpowiednich normach (np. EN 50173, TIA/EIA-568A).

Wymagania stawiane okablowaniu dla sieci pracujących z prędkością 1 GB/s są znacznie wyższe. Oprócz standardowych testów, zgodnie z biuletynem TIA/EIA/TSB-95, należy wykonać pomiar parametrów:

- **PowerSum NEXT** – jest rozwinięciem parametru NEXT, dodatkowo uwzględniającym wzajemne zakłócanie się par w kablu czteroparowym. Różnica pomiędzy pomiarem parametru NEXT i PowerSum NEXT polega na tym, że podczas pomiaru PowerSum NEXT mierzony jest poziom sygnału indukowanego w danej parze, pochodzący od sygnałów wszystkich pozostałych par. Przesłuch zbliżny mierzony metodą PowerSum ma znacznie większą wartość niż przesłuch mierzony metodą tradycyjną (NEXT) i lepiej oddaje charakter rzeczywistych przesłuchów występujących w torze transmisyjnym. PowerSum NEXT jest bardzo istotnym parametrem dla instalacji, w których będą działały protokoły transmisyjne wykorzystujące do transmisji wszystkie cztery pary.
- **PowerSum ACR** (*Attenuation to Crosstalk Ratio*) – określa różnicę pomiędzy tłumieniem a przesłuchem zbliżnym NEXT dla danej pary przewodów (odstęp sygnału użytecznego od szumu). Im większa wartość bezwzględna parametru ACR, tym lepiej. PowerSum ACR jest wynikiem obliczeń z parametrów mierzonych, czyli PowerSum NEXT i tłumienia.
- **FEXT** (*Far End Crosstalk*) – przesłuch zdalny – w przeciwieństwie do przesłuchu zbliżnego NEXT mierzony jest na przeciwnym końcu kabla niż sygnał wywołujący zakłócenie. Jest to parametr łatwy do pomiaru, ale trudny do wyspecyfikowania w normach, gdyż wartość jego jest zależna od długości (a więc tłumienia) kanału transmisji. W związku z tym im krótszy jest odcinek toru transmisyjnego, tym FEXT ma większy wpływ na jakość transmisji. Jest to parametr mierzony, ale rzadko podawany. Głównie służy on jako składowa do otrzymania parametru ELFEXT.
- **ELFEXT** (*Equal Level Far End Crosstalk*) – w odróżnieniu od FEXT jest niezależny od długości badanego toru, gdyż uwzględnia tłumienie wnoszone przez tor transmisyjny. Matematycznie jest to wynik otrzymany z różnicy pomiędzy wartością parametru FEXT i tłumienia dla danego toru transmisyjnego.
- **PowerSum ELFEXT** – parametr uwzględnia, że zakłócenia mogą pochodzić nie tylko od jednej, ale od trzech pozostałych par (w kablu czteroparowym). Jest wynikiem obliczeń z wartości parametru ELFEXT dla każdej pary przewodów w kablu.
- **Return Loss** – straty odbiciowe – parametr ten określa stosunek mocy sygnału wprowadzonego do toru transmisyjnego do mocy sygnału odbitego, który powstaje na skutek niedopasowania impedancji toru transmisyjnego. Sygnał ten może być źródłem zakłóceń dla sygnału użytecznego, co jest bardzo istotne w przypadku transmisji w dwóch kierunkach w tym samym torze transmisyjnym.
- **Propagation Delay Skew** – określa różnicę opóźnienia transmisji pomiędzy najszybszą i najwolniejszą parą w skrętce. Przy dużych prędkościach transmisji może powstać problem ze spójnością sygnału nadawanego wszystkimi parami skrętki na odległym końcu, gdyż odbiornik nie będzie w stanie zdekodować poprawnie informacji przychodzącej po wszystkich czterech parach przewodnika. Maksymalna dopuszczalna wartość różnicy opóźnień wynosi 45 – 50 ns.

Testowanie okablowania światłowodowego polega na sprawdzeniu tłumienia okablowania w oknach transmisyjnych. Światłowody wielomodowe korzystają z okien transmisyjnych dla fal o długości 850 nm i 1300 nm, a jednomodowe dla fal o długości 1310 nm i 1550 nm. Tłumienie należy sprawdzać w obu oknach transmisyjnych. Dodatkowo

długość kanału nie może być większa niż podana przez producenta. Jeśli w kanale jest stosowana większa liczba złączy i/lub spawów, to maksymalna długość kabla powinna być zmniejszona. Przed przyłączeniem miernika do toru optycznego należy przetrzeć złącza chusteczką nawilżoną spirytusem. Testowanie wykonuje się reflektometrem optycznym (*Optical Time-Domain Reflectometer – OTDR*). Umożliwia on pomiar lub certyfikację światłowodów, przeprowadzanie testów PASS/FAIL, pomiar odległości oraz tłumienia.

Podczas odbioru instalacji okablowania strukturalnego wykonuje się pomiary wszystkich torów komunikacyjnych. Pomiary wykonuje się w określonej kolejności: najpierw okablowanie pionowe, następnie okablowanie poziome i na końcu całość systemu (okablowanie pionowe, poziome łącznie z kablami krosowymi i stacyjnymi).

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyszukaj w internecie ofertę firmy (wskazanej przez nauczyciela lub działającej w Twojej miejscowości) świadczącej usługi certyfikacji sieci. Na podstawie cennika i liczby torów do przetestowania w Twoim projekcie oszacuj koszt uzyskania certyfikatu dla okablowania.

39 Metody pomiarów sieci logicznej

ZAGADNIENIA

- **Jakie są strategie testowania sieci komputerowej?**
- **Jak odczytać informacje o wartości sygnału i szumu w sieci bezprzewodowej?**
- **Jak wykonać skanowanie pasma radiowego wykorzystywanego przez sieci bezprzewodowe?**

Sieć komputerowa ze względu na swoją budowę jest obiektem trudnym do testowania. Z powodu złożoności, różnorodności struktury sieci LAN, różnych mediów transmisyjnych oraz znacznej liczby producentów sprzętu w sieciach może pojawiać się wiele błędów. Ich lokalizacja i usuwanie jest obowiązkiem administratora. W większości przypadków niepoprawna praca sieci komputerowej nie jest spowodowana fizycznym uszkodzeniem połączeń sieciowych, lecz jest wynikiem zakłóceń w kanale transmisyjnym lub niewłaściwej konfiguracji. Z tego powodu sieć powinna być w sposób ciągły testowana, a pojawiające się błędy usuwane. Istnieją dwie strategie testowania sieci: testowanie odgórne i oddolne. **Testowanie odgórne** (*top down*) rozpoczyna się od najwyższej warstwy sieciowej, po czym kolejno są diagnozowane coraz niższe warstwy sieci. Najpierw sprawdza się poprawność aplikacji między głównymi węzłami sieciowymi, następnie komunikację węzłów pośredniczących i dopiero na końcu poprawność poszczególnych kanałów fizycznych sieci teletransmisyjnej. Metoda ta jest stosowana głównie w sieciach już działających. W strategii **testowania oddolnego** (*bottom up*) testowanie rozpoczyna się od warstwy najniższej, czyli sprawdzania kabli i połączeń fizycznych, a następnie przechodzi się do warstw coraz wyższych. Testowanie oddolne stosuje się zwykle podczas uruchamiania sieci nowych, w praktyce używa się naprzemiennie obydwóch sposobów diagnozowania sieci.

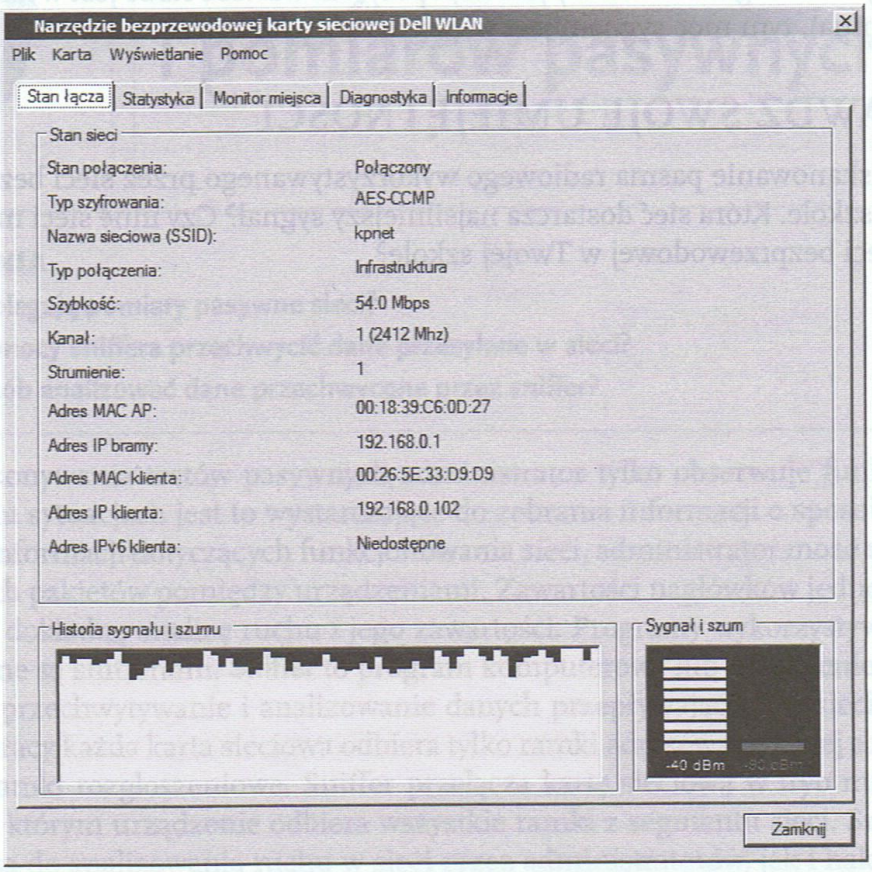
W sieciach komputerowych używa się modelu sieci ISO/OSI i przyporządkowuje błędy do poszczególnych warstw modelu. Upraszcza to testowanie, ponieważ w każdej warstwie występują inne typy błędów. Pomiary sieci komputerowych można podzielić na: **pomiary parametrów fizycznych** okablowania (miedzianego lub światłowodowego), **pomiary pasywne**, dokonywane wyłącznie przez obserwację funkcjonowania sieci, oraz **pomiary aktywne**, w których do sieci wprowadza się specjalne dane testowe.

Do najczęściej stosowanych procedur lokalizujących uszkodzenia i diagnozujących sieci komputerowe należą:

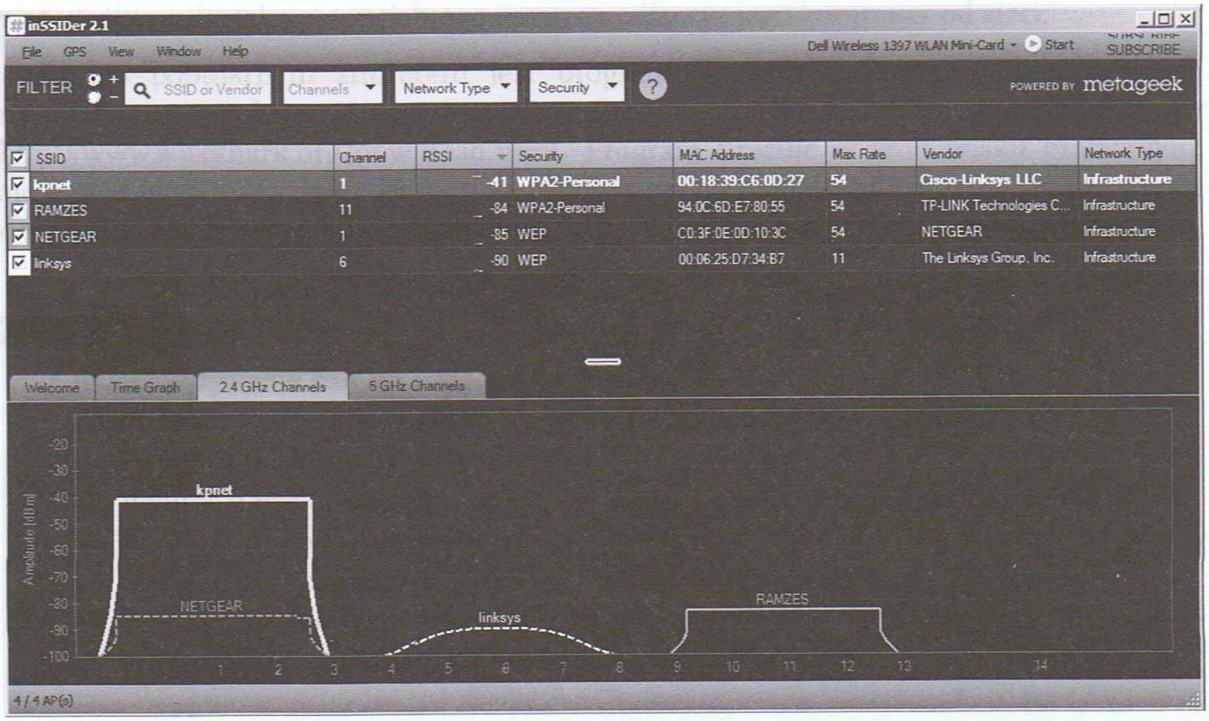
- testowanie okablowania,
- dekodowanie strumienia danych wraz z analizą pakietów i protokołów,
- testowanie połączeń między wybranymi węzłami sieci,
- statystyczna analiza ruchu sieciowego,
- analiza konfiguracji i bieżącego stanu sieci.

W przypadku bezprzewodowych sieci komputerowych duże znaczenie ze względu na szybkość i stabilność połączenia ma siła sygnału radiowego, wartość szumu i stosunek sygnału do szumu docierającego do karty sieciowej.

Informacje o wartości mocy sygnału i szumu można odczytać z programu obsługującego bezprzewodową kartę sieciową. Na przykład wartości te można odszukać w prawym dolnym rogu rysunku 39.1.



Rys. 39.1. Okno programu obsługującego bezprzewodową kartę sieciową



Rys. 39.2. Wynik skanowania pasma radiowego wykorzystywanego przez sieci wifi

Na rys 39.2. pokazano wynik skanowania pasma radiowego wykorzystywanego przez sieci bezprzewodowe za pomocą programu inSSIDer. Najlepszą moc sygnału posiada sieć kpnet, pracująca na kanale 1. Jej **RSSI** wskaźnik mocy odbieranego sygnału radiowego (*Received Signal Strength Indication*) jest najlepszy. Im wartość RSSI jest wyższa (mniejsza wartość ujemna), tym moc sygnału jest większa.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wykonaj skanowanie pasma radiowego wykorzystywanego przez sieci bezprzewodowe w Twojej szkole. Która sieć dostarcza najsilniejszy sygnał? Czy inne sieci mogą zakłócać sygnał sieci bezprzewodowej w Twojej szkole?

40 Rodzaje testów i pomiarów pasywnych

ZAGADNIENIA

- **Na czym polegają pomiary pasywne sieci?**
- **Jak przy pomocy sniffera przechwycić dane przesyłane w sieci?**
- **W jaki sposób analizować dane przechwycone przez sniffer?**

Podczas wykonywania testów pasywnych administrator tylko obserwuje funkcjonowanie sieci. W wielu sytuacjach jest to wystarczające do zebrania informacji o sposobie działania sieci. Dużo informacji dotyczących funkcjonowania sieci, administrator może uzyskać, monitorując ruch pakietów pomiędzy urządzeniami. Zawartości nagłówków jednostek danych umożliwiają dokładną analizę ruchu i jego zawartości. Programy wykorzystywane do tego celu nazywane są snifferami. **Sniffer** to program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i analizowanie danych przepływających w sieci. W normalnym trybie pracy każda karta sieciowa odbiera tylko ramki adresowane na jej adres fizyczny MAC oraz ramki rozgłoszeniowe. Sniffer przełącza kartę sieciową w tryb mieszany (*promiscuous*), w którym urządzenie odbiera wszystkie ramki z segmentu sieci. Sniffery wykorzystywane są do analizowania ruchu w sieci przez administratorów, jak i hakerów. Z tego powodu podczas pracy w sieci nie wolno bez powodu uruchamiać tego typu programów. Administrator sieci po wykryciu uruchomionego sniffera na komputerze może potraktować użytkownika jako potencjalnego intruza i odłączyć jego komputer od sieci.

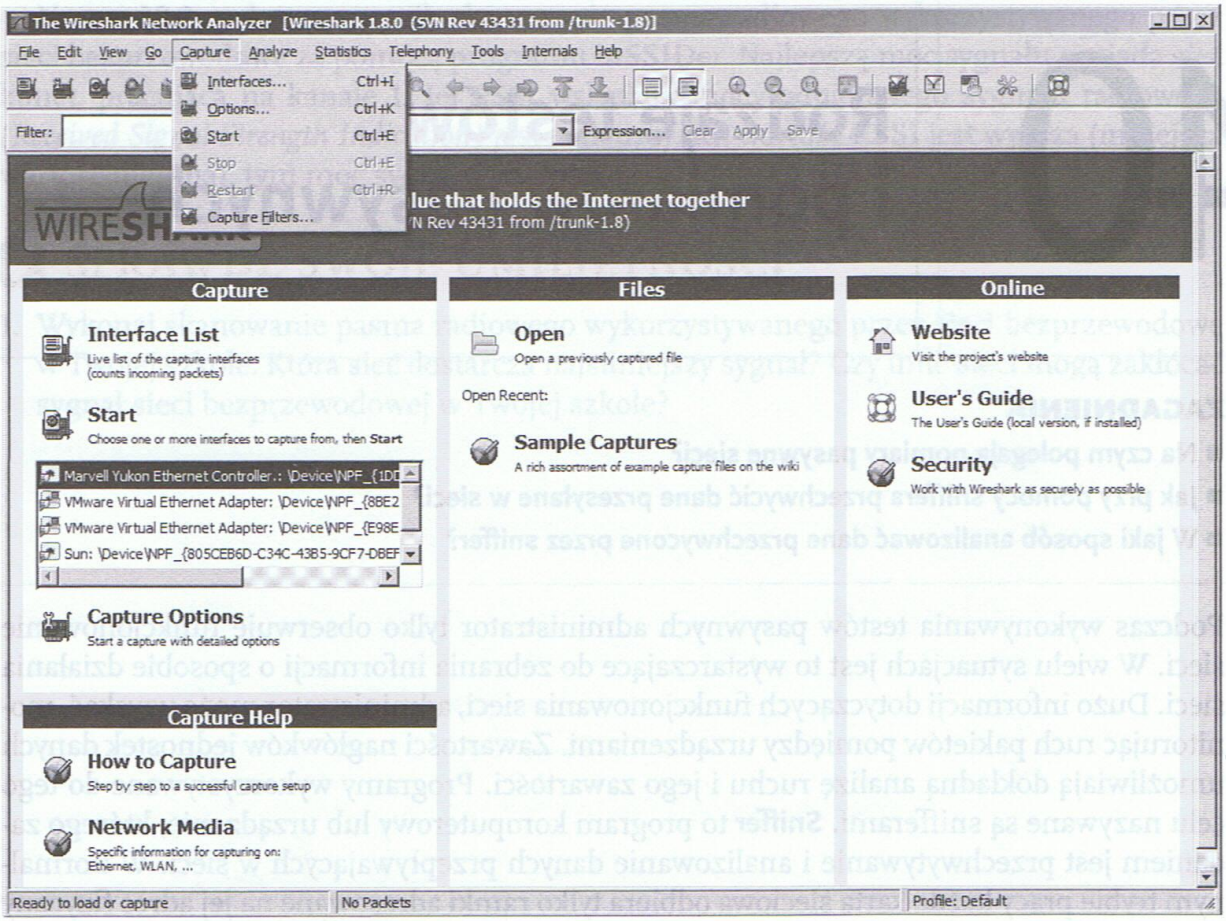
Bardzo popularnym snifferem jest program Wireshark. Dostępny jest w wersji na platformę Windows, Linux i MacOS X. Program można bezpłatnie pobrać ze strony http://www.wireshark.org/download.html. Program pracuje w środowisku graficznym, ale w środowisku Windows wymaga zainstalowanej biblioteki WinPcap (najnowsze wersje dostarczane są razem z biblioteką).

PRZYKŁAD 40.1.

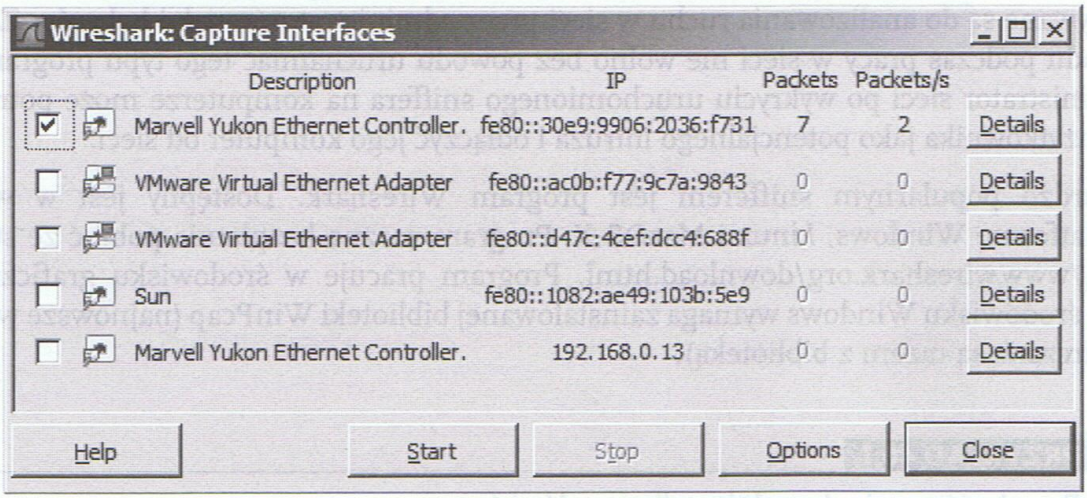
Przechwytywanie danych i analiza nagłówków

Aby przechwycić dane przesyłane w sieci i przeanalizować nagłówki, należy:

1. Uruchomić program Wireshark.
2. Wybrać z paska narzędzi polecenie Capture, a następnie Interfaces (rys. 40.1).
3. W oknie wyboru interfejsu (rys. 40.2) wskazać, który interfejs ma być ustawiony w trybie przechwytywania danych, i kliknąć przycisk Start.
4. Uruchomić dowolny program generujący przepływ danych w sieci, np. polecenie ping, albo zaczekać na pojawienie się ruchu w sieci.



Rys. 40.1. Włączenie przechwytywania danych

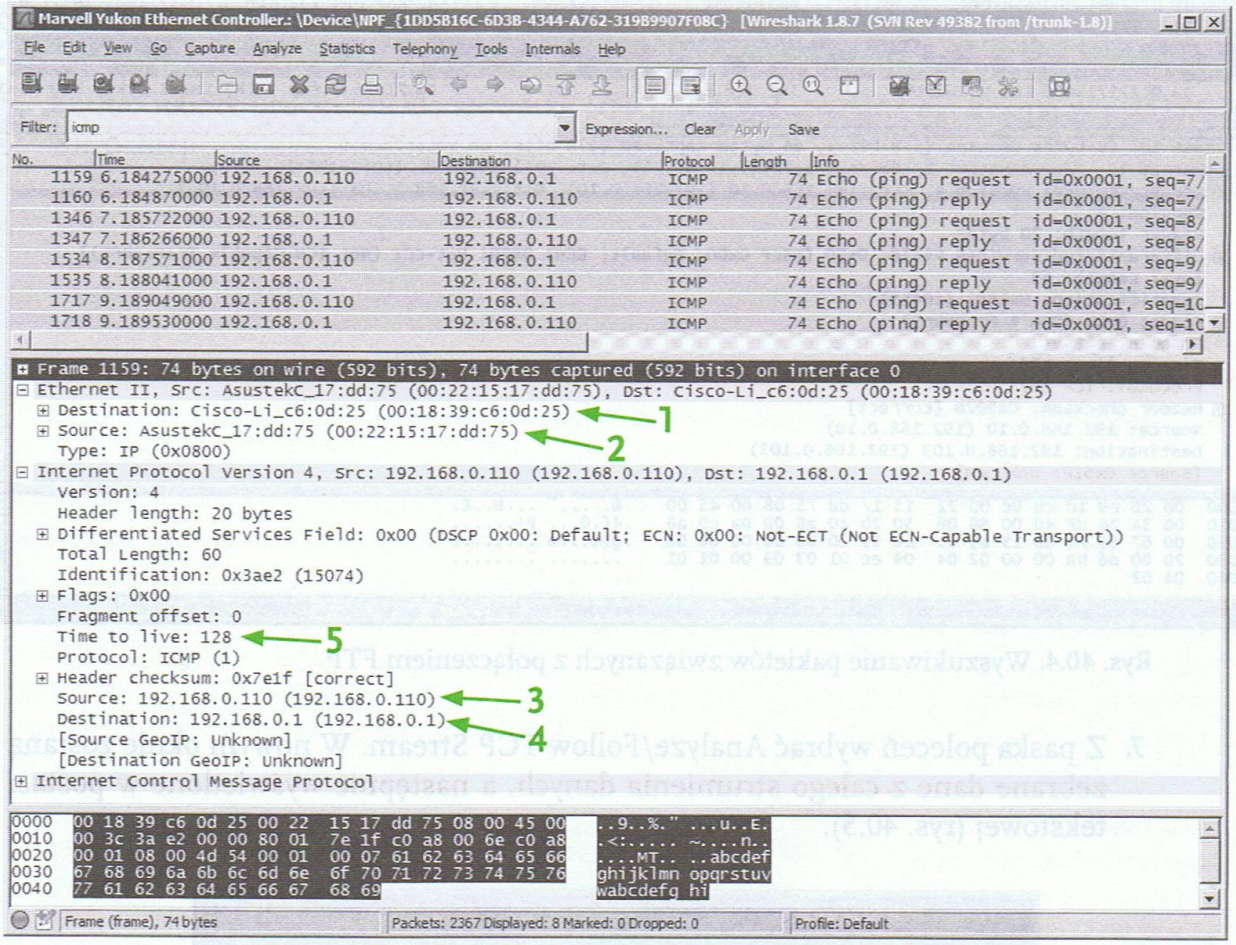


Rys. 40.2. Okno wyboru interfejsu do przechwytywania danych

5. Obserwować w oknie głównym programu przychwytywane dane. Po zebraniu wymaganej ilości danych zatrzymać przechwytywanie poleceniem Capture/Stop. W oknie rozwinąć gałęzie Ethernet II i Internet Protocol Version 4. Na rysunku 40.3 strzałkami zaznaczone są ważne informacje uzyskane z analizy nagłówków:
   - adres docelowy MAC – strzałka 1,
   - adres źródłowy MAC – strzałka 2,
   - adres źródłowy IP – strzałka 3,

- adres docelowy IP – strzałka 4,
- parametr TTL – strzałka 5.

Analiza ta pozwala na ustalenie adresów fizycznych i logicznych komputerów biorących udział w transmisji danych.



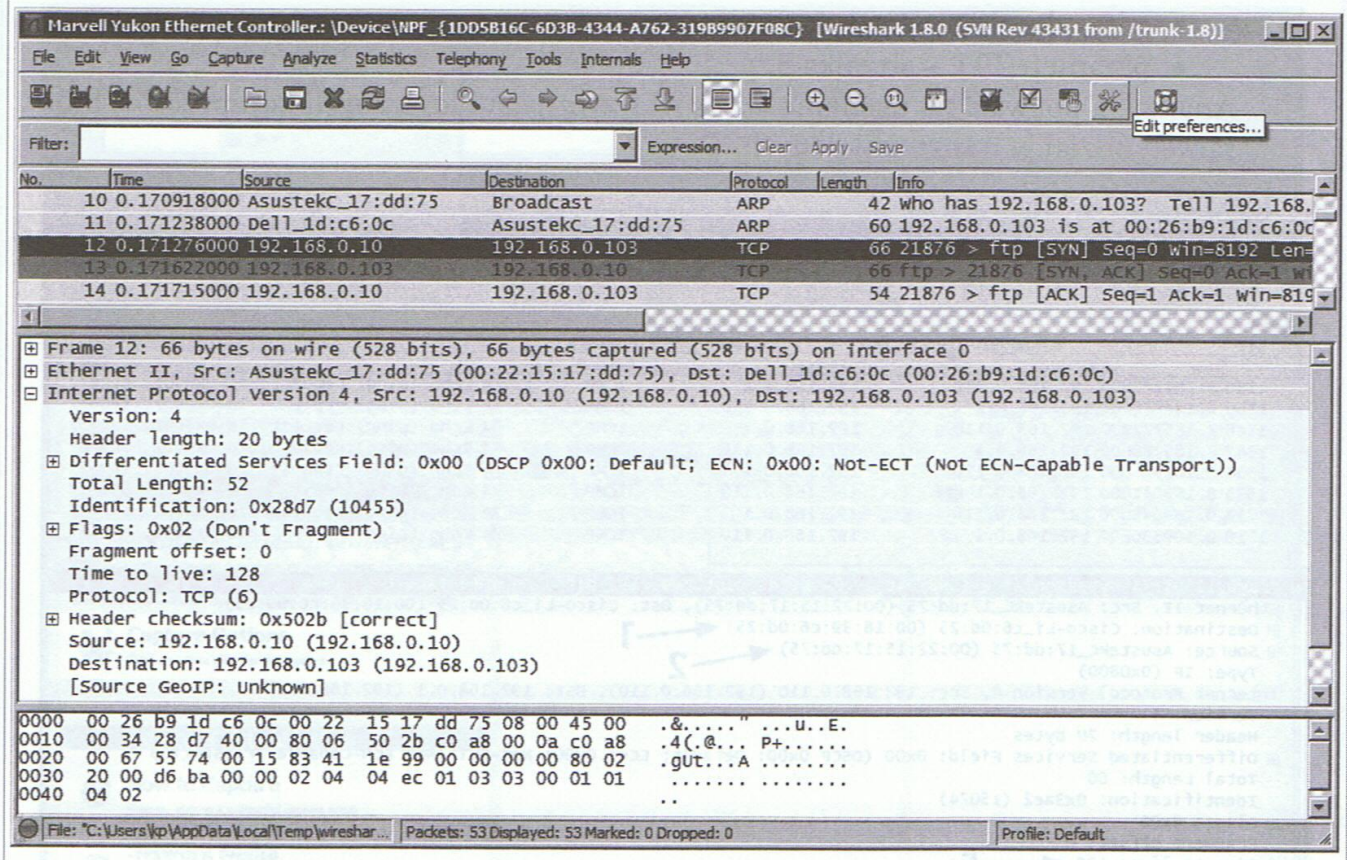
Rys. 40.3. Analiza nagłówków przechwyconych danych

PRZYKŁAD 40.2.

Analiza danych przesyłanych w sieci

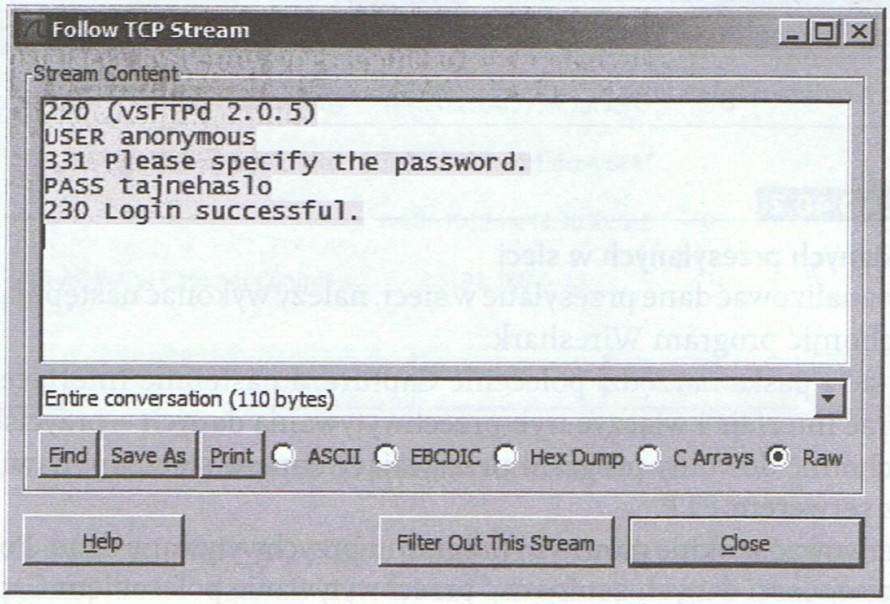
Aby przeanalizować dane przesyłane w sieci, należy wykonać następujące czynności:

1. Uruchomić program Wireshark.
2. Wybrać z paska narzędzi polecenie Capture, a następnie Interfaces.
3. Wybrać interfejs i włączyć tryb przechwytywania danych – przycisk Start.
4. Uruchomić dowolny program przesyłający dane w sieci, np. nawiązać połączenie z serwerem FTP.
5. Obserwować w oknie głównym programu przychwytywane dane. Po zebraniu wymaganej ilości danych zatrzymać przechwytywanie poleceniem Capture/Stop.
6. Odszukać w oknie dowolny fragment transmisji związanej z nawiązywaniem połączenia FTP. Na rysunku 40.4 pakiety o numerach 10 i 11 związane są z zapytaniem odpowiedzią protokołu ARP. W pakiecie 12 rozpoczyna się proces nawiązywania sesji między klientem a serwerem FTP (jest to jeden z pakietów związanych z transmisją) – można kliknąć ten pakiet lub inny należący do tej samej sesji.



Rys. 40.4. Wyszukiwanie pakietów związanych z połączeniem FTP

7. Z paska poleceń wybrać Analyze/Follow TCP Stream. W nowym oknie zostaną zebrane dane z całego strumienia danych, a następnie wyświetlone w postaci tekstowej (rys. 40.5).



Rys. 40.5. Przesyłane dane wyświetlone w postaci tekstowej

Uwaga

Jeżeli dane były wysyłane bez stosowania szyfrowania, to zostaną wyświetlone łącznie z nazwami użytkowników i hasłami, jak na rysunku 40.5.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Przechwyć i przeanalizuj przebieg transmisji danych związanych z uzyskiwaniem adresu za pomocą protokołu DHCP. W transmisji zlokalizuj:
   - adres MAC i IP klienta przed i po uzyskaniu adresu,
   - komunikaty: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK.

Uwaga
Sniffer należy uruchomić na serwerze DHCP lub pobrać dane dla klienta w maszynie witrualnej.

41 Rodzaje testów i pomiarów aktywnych

ZAGADNIENIA

- **Jak przeprowadzać pomiary aktywne w sieci?**
- **Jak zmierzyć jakość usług sieciowych?**
- **Kto ustanawia standardy dotyczące jakości usług sieciowych?**
- **Jakie parametry służą do oceny jakości usług sieciowych?**
- **Jak wykorzystać programy ping i traceroute do pomiarów sieci?**

Podczas wykonywania testów aktywnych administrator wprowadza do sieci dodatkowe dane, które ułatwiają wykonywanie pomiarów lub diagnozowanie sieci. Testy te mogą być wykonywane podczas normalnej eksploatacji sieci. Umożliwiają uzyskanie wiedzy o stanie sieci, jak również o zjawiskach w niej zachodzących. Metody aktywne uwzględniają podczas pomiarów obciążenie sieci ruchem generowanym przez aplikacje użytkowników, jak i samą sieć (np. protokoły routingu, DHCP, DNS).

Pomiary aktywne pozwalają na określenie **jakości usług sieciowych** (*Quality of Service* – QoS). QoS określa poziom gwarantowanych wartości parametrów sieciowych w celu osiągnięcia satysfakcji użytkownika. Użytkownicy w różny sposób oceniają jakość usług poprzez takie parametry, jak:

- przepustowość sieci,
- opóźnienie przesyłania danych,
- różnice opóźnienia poszczególnych pakietów,
- straty pakietów danych.

W celu zapewnienia porównywalności wyników, pomiary aktywne wykonywane są na podstawie metryki zdefiniowanej przez organizacje standaryzacyjne, np. ITU-T lub IETF. Przykładowo organizacja IETF zdefiniowała metryki:

- **Dostępność usługi** – możliwość przekazu pakietów między danym źródłem a urządzeniem docelowym. Urządzenie docelowe uznawane jest za dostępne, jeśli pakiet dotrze w określonym czasie.
- **Opóźnienie w jednym kierunku OWD** (*One Way Delay*) – czas przekazu pakietu między dwoma punktami w sieci. OWD jest mierzone jako czas od momentu, w którym źródło wysłało pierwszy bit pakietu, do momentu, w którym urządzenie docelowe odebrało ostatni bit pakietu. Wielkość pakietu pomiarowego ma wpływ na opóźnienie i musi być zdefiniowana przed pomiarem. Wartość metryki podawana jest w postaci parametrów statystycznych próbki:
  - minimalne opóźnienie OWD (*One Way Delay Minimum*) – najmniejsza wartość opóźnienia w próbce,
  - średnie opóźnienie OWD (*Mean One Way Delay*) – średnia wartość opóźnienia w próbce,

- percentyl opóźnienia OWD (*One Way Delay Percentile*) – x-ty percentyl opóźnienia danej próbki,
- mediana opóźnienia OWD (*One Way Delay Median*) – wartość mediany danej próbki.

- **Zmienność opóźnienia przekazu pakietów IPDV** (*IP Packet Delay Variation*) – różnica pomiędzy wartością OWD dla dwóch pakietów w mierzonej próbce pakietów (zwykle przyjmuje się różnicę opóźnienia sąsiednich pakietów).
- **Opóźnienie pakietów w pętli RTD** (*Round Trip Delay*) – opóźnienie przekazu pakietu mierzone na drodze źródło –> przeznaczenie –> źródło. Wartość mierzona jako czas od wysłania pierwszego bitu pakietu do odebrania ostatniego bitu pakietu przez źródło.
- **Straty pakietów OWL** (*One Way Loss*) – w przypadku poprawnego odebrania pakietu przyjmuje wartość 0, w przeciwnym wypadku – 1.
- **Poziom strat pakietów IPLR** (*IP Packet Loss Ratio*) – stosunek liczby pakietów straconych do liczby pakietów wysłanych w danym okresie pomiarowym.

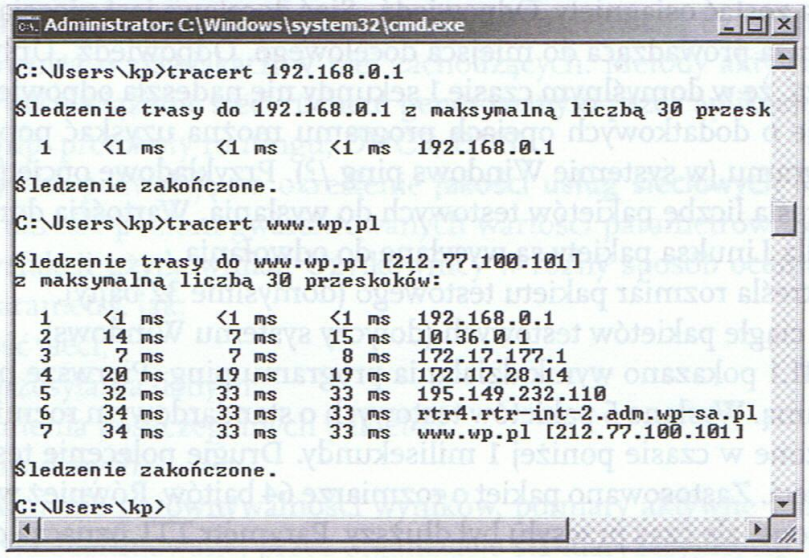
Podstawowym narzędziem do wykonywania testów aktywnych w sieciach opartych na protokole IP jest program ping. Ping pozwala na sprawdzenie, czy istnieje połączenie pomiędzy dwoma punktami w sieci. Umożliwia on zmierzenie liczby zgubionych pakietów oraz opóźnień w ich transmisji. Program korzysta z protokołu ICMP, wysyła pakiety *ICMP Echo Request* i odbiera *ICMP Echo Reply*. Aby wykonać test przy użyciu polecenia ping, należy w wierszu polecenia wpisać polecenie ping i adres IP lub nazwę domenową komputera, który ma zostać osiągnięty. Odpowiedź „Sieć docelowa jest nieosiągalna" oznacza, że nie istnieje trasa prowadząca do miejsca docelowego. Odpowiedź „Upłynął limit czasu żądania" oznacza, że w domyślnym czasie 1 sekundy nie nadeszła odpowiedź na polecenie ping. Informacje o dodatkowych opcjach programu można uzyskać poprzez wywołanie pomocy do programu (w systemie Windows ping /?). Przykładowe opcje programu ping:

- **n liczba** – określa liczbę pakietów testowych do wysłania. Wartością domyślną dla Windows jest 4, dla Linuksa pakiety są wysyłane do odwołania,
- **l rozmiar** – określa rozmiar pakietu testowego (domyślnie 32 bajty),
- **t** – wysyłanie ciągłe pakietów testowych (dotyczy systemu Windows).

Na rysunku 41.1 pokazano wynik działania programu ping. Pierwsze polecenie testuje połączenie z bramą. Wysłano 5 pakietów testowych o standardowym rozmiarze. Wszystkie zostały dostarczone w czasie poniżej 1 milisekundy. Drugie polecenie testuje połączenie z serwerem w sieci. Zastosowano pakiet o rozmiarze 64 bajtów. Również wszystkie pakiety zostały dostarczone, ale czas przesyłu był dłuższy. Parametr TTL oznacza czas życia pakietu i pozwala na określenie liczby routerów na trasie.

Do badania trasy, po której przesyłane są pakiety, i mierzenia czasu pomiędzy poszczególnymi routerami można wykorzystać program traceroute (w systemie Windows tracert). Działanie traceroute opiera się o protokole ICMP. Wysyłane są pakiety z polem TTL (*Time To Live*) ustawionym na kolejne wartości, zaczynając od 1. Wartość ta jest zmniejszana przez każdy router na trasie. Jeżeli pole TTL osiągnie wartość 0, to pakiet jest odrzucany, a router wysyła informację zwrotną do komputera źródłowego. W ten sposób komputer źródłowy uzyskuje kolejne adresy IP routerów na trasie. Na początku wysyłany jest pakiet z polem TTL ustawionym na 1, co pozwala na ustalenie adresu IP pierwszego routera na trasie. Następnie wysyłany jest pakiet z polem TTL 2. Pierwszy router zmniejszy tę wartość do 1 i przekaże do drugiego routera na trasie. Drugi router zmniejszy TTL do 0 i odrzuci pakiet, wysyłając komunikat do komputera źródłowego. Testowanie kończy się po osiągnięciu miejsca docelowego lub przekroczeniu dopuszczalnej liczby routerów (standardowo 30). Na rysunku 41.2. pokazano wyniki działania programu tracert. W pierwszym poleceniu testowano trasę do bramy; trasa składała się tylko z 1 routera. Trasa do serwera

Rys. 41.1. Wynik działania programu ping



Rys. 41.2. Wynik działania programu tracert

w internecie była dłuższa i składała się z siedmiu routerów (ich adresy lub nazwy znajdują sie po prawej stronie rysunku). Na podstawie pomiaru administrator może określić łącza, w których występuje największe opóźnienie.

Na działanie polecenia ping może mieć wpływ zapora sieciowa skonfigurowana na testowanym komputerze. Wiele zapór standardowo blokuje wysyłanie odpowiedzi na żądanie echa wysyłane przez program ping.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sprawdź możliwość komunikacji z bramą internetową w szkole, komputerem kolegi i z serwerem DNS.
2. Sprawdź adresy komputerów na trasie do dowolnego serwera w internecie. Na którym łączu występują największe opóźnienia?

42 Cenniki materiałów do montażu okablowania strukturalnego

ZAGADNIENIA

- **W jakim celu stworzono systemy okablowania strukturalnego?**
- **Z jakich elementów składają się systemy okablowania strukturalnego?**
- **Jak dobrać system okablowania strukturalnego?**

Wykonanie instalacji okablowania strukturalnego wymaga poniesienia nakładów finansowych. Wysokość tych nakładów powinna być oszacowana przed przystąpieniem do realizacji zadania, tak aby zamawiający miał świadomość koniecznych do poniesienia kosztów. Po zakończeniu inwestycji należy sporządzić dokładny kosztorys powykonawczy, aby rozliczyć z zamawiającym poniesione nakłady.

Podstawą do sporządzania kosztorysu powykonawczego jest dokumentacja budowy, która obejmuje:

- dokumentację techniczną wykonywanych robót,
- książkę obmiaru robót i potwierdzone przez zamawiającego zapisy w dzienniku budowy (dzienniku montażu),
- protokoły konieczności, np. zakupu dodatkowych materiałów, wprowadzenia zmian w projekcie,
- normy nakładów rzeczowych,
- ceny czynników produkcji – koszty robocizny, materiałów, sprzętu oraz dodatkowe koszty zakupu, koszty pośrednie i zysk, w wysokościach wynegocjowanych między zamawiającym i wykonawcą,
- obowiązujące zasady obliczania podatku VAT.

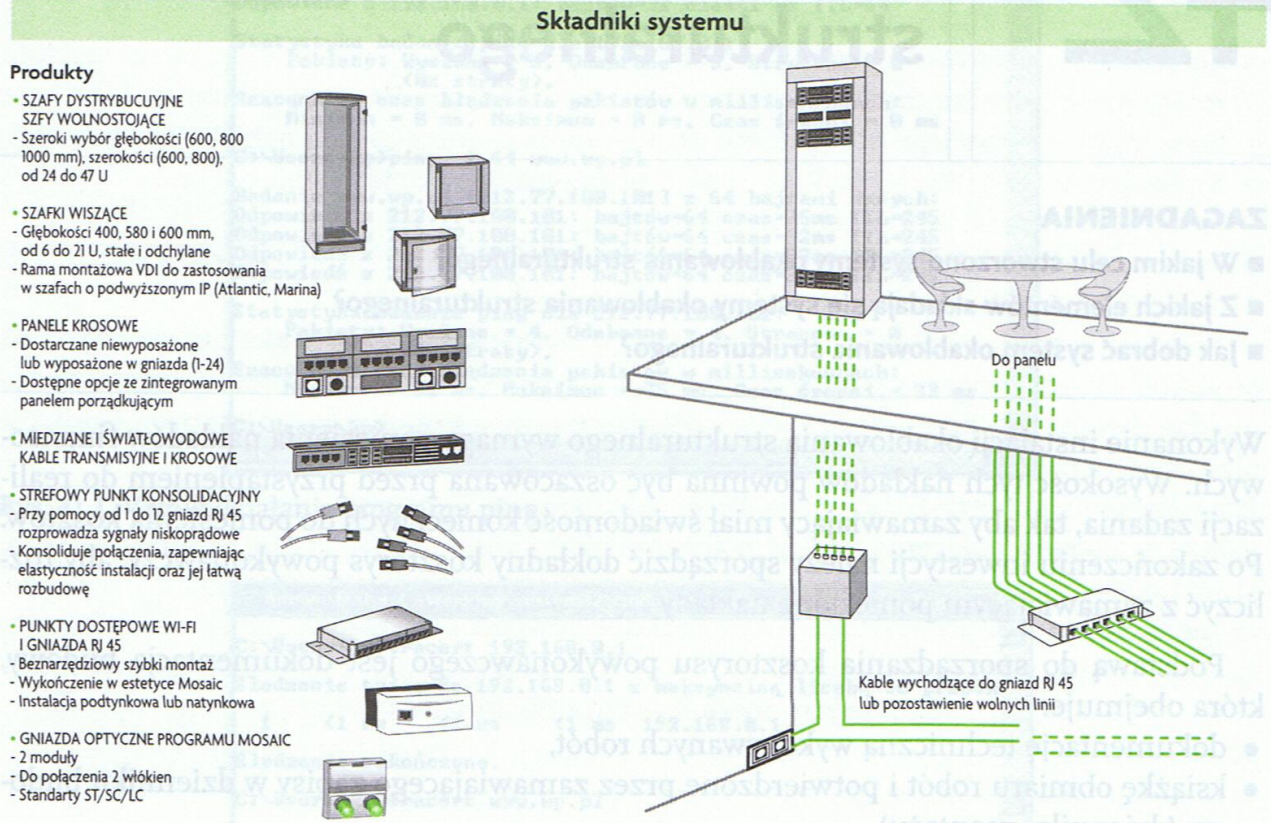
Przy obliczaniu kosztów materiałów należy uwzględnić koszty materiałów bezpośrednich, np. kable, złącza, jak i pośrednich, np. listwy montażowe, kołki mocujące itp. Wielu producentów oferuje systemy instalacji okablowania (rys. 42.1) zawierające różne elementy umożliwiające wykonanie instalacji (rys. 42.2).

Systemy te składają się z kanałów kablowych oraz zestawu typowych gniazd i elementów łączących, np. łączników, narożników itp.

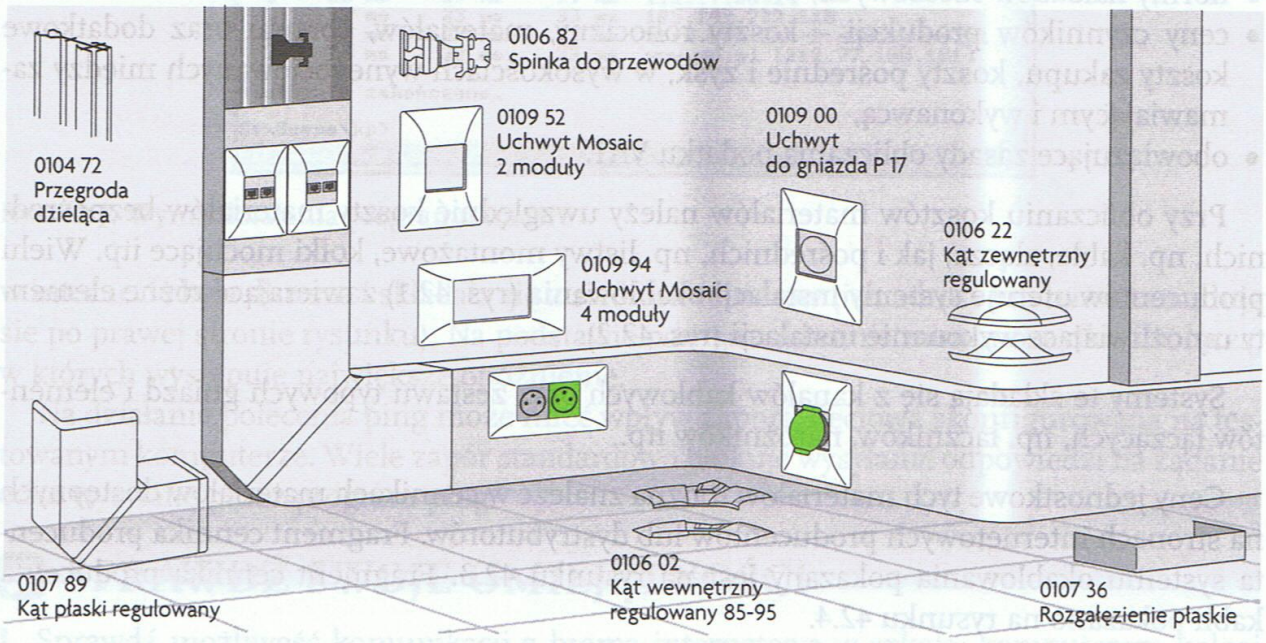
Ceny jednostkowe tych materiałów można znaleźć w cennikach materiałów dostępnych na stronach internetowych producentów lub dystrybutorów. Fragment cennika producenta systemu okablowania pokazany jest na rysunku 42.3. Fragment cennika producenta kabli pokazano na rysunku 42.4.

Przy ustalaniu kosztorysu okablowania należy wziąć również pod uwagę koszt związany z przeprowadzeniem odbioru instalacji. Aby sieć mogła uzyskać odpowiedni certyfikat potwierdzający zgodność wykonania z przyjętymi normami i standardami, należy

wykonać pomiary każdego toru transmisyjnego. Pomiar wykonuje uprawniony pracownik za pomocą urządzenia diagnostycznego. Ponieważ koszt takiego urządzenia jest bardzo wysoki, można zlecić wykonanie tej usługi firmie zewnętrznej lub wypożyczyć tester. Usługi tego typu świadczy wiele firm.



Rys. 42.1. Składniki systemu okablowania strukturalnego



Rys. 42.2. Elementy systemu okablowania strukturalnego

Rodzina handlowa	Numer referencyjny	Nazwa produktu	Cena bazowa	J. m.	Opakowanie	Grupa rabat.
		0104				
DLP-N	010411	DLP KANAŁ 35 x 80 BIAŁY B/POKR.	22,40	MB	20	C
DLP-N	010412	DLP KANAŁ 50 x 80 BIAŁY B/POKR.	33,19	MB	20	C
DLP-N	010421	DLP KANAŁ 35 x 105 BIAŁY B/POKR.	29,60	MB	20	C
DLP-N	010422	DLP KANAŁ 50 x 105 BIAŁY B/POKR.	41,84	MB	20	C
DLP-N	010432	DLP KANAŁ 50 x 150 BIAŁY B/POKR.	73,08	MB	10	C
DLP-N	010433	DLP KANAŁ 65 x 150 BIAŁY B/POKR.	77,22	MB	8	C
DLP-N	010453	DLP KANAŁ 65 x 195 BIAŁY B/POKR.	96,07	MB	8	C
DLP-N	010459	DLP KANAŁ 65 x 220 BIAŁY B/POKR.	104,01	MB	8	C
DLP-N	010472	DLP PRZEGR. DO POKR. DO WYS. 50	27,35	MB	48	C
DLP-N	010473	DLP PRZEGR. DO POKR. DO WYS. 65	29,96	MB	36	C
		0105				
DLP-N	010500	DLP POKRYWA BIAŁA SZER 40	13,73	MB	24	C
DLP-N	010501	DLP POKRYWA BIAŁA SZER 65	16,68	MB	36	C
DLP-N	010502	DLP POKRYWA BIAŁA SZER 85	18,57	MB	32	C
DLP-N	010504	DLP POKRYWA BIAŁA SZER 130	31,84	MB	20	C
DLP-N	010520	DLP POKRYWA B. ELASTYCZNA SZER. 40	11,76	MB	20	C
DLP-N	010521	DLP POKRYWA B. ELASTYCZNA SZER. 65	14,21	MB	20	C
DLP-N	010522	DLP POKRYWA B. ELASTYCZNA SZER. 85	15,83	MB	20	C
DLP-N	010524	DLP POKRYWA B. ELASTYCZNA SZER. 130	26,75	MB	8	C
DLP-N	010526	DLP POKRYWA B. ELASTYCZNA SZER. 180	36,47	MB	8	C
DLP-N	010580	DLP USZCZ. PRZYPODŁ.	23,77	MB	24	C
DLP-N	010582	DLP PRZEGR. SEP. DO WYS. 35/50	14,90	MB	24	C
DLP-N	010583	DLP PRZEGR. SEP. DO WYS. 65/80	15,96	MB	48	C
DLP-N	010584	DLP PRZEGR. SEP. KANAŁ 35 x 80	13,61	MB	16	C
		0106				

Rys. 42.3. Fragment cennika producenta systemu okablowania

Kategioria 5	
mm	zł/km
UTP 4x2x0,5 PVC	1 710
UTP dual 4x2x0,5 PVC	3 421
FTP 4x2x0,5 PVC	2 572
S-FTP 4x2x0,5 PVC	4 354
UTP 4x2x0,5 LSOH	1 971
UTP dual 4x2x0,5 LSOH	3 942
FTP 4x2x0,5 LSOH	2 943
S-FTP 4x2x0,5 LSOH	5 392

Kategoria 5e (+)	
mm	zł/km
UTP 4x2x0,5 PVC	1 886
UTP dual 4x2x0,5 PVC	3 766
FTP 4x2x0,5 PVC	2 835
UTP 4x2x0,5 LSOH	2 166
UTP dual 4x2x0,5 LSOH	4 330
FTP 4x2x0,5 LSOH	3 246

Kategoria 6	
mm	zł/km
STP 4x2x0,5 PVC	4 199
S-STP 4x2x0,5 PVC	5 241
STP 4x2x0,5 LSOH	4 807
S-STP 4x2x0,5 LSOH	6 019

Rys. 42.4. Fragment cennika kabli miedzianych

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyszukaj w internecie ofertę firmy (wskazanej przez nauczyciela lub działającej w Twojej miejscowości) produkującej lub będącej dystrybutorem systemów okablowania strukturalnego. Dobierz z jej oferty elementy potrzebne do wykonania okablowania Twojej sieci. Oblicz koszt instalacji.

IV. Modernizacja i rekonfiguracja lokalnych sieci komputerowych

- Zasady modernizacji lokalnej sieci komputerowej
- Zasady kosztorysowania prac modernizacyjnych
- Przykładowe zadania projektowe do samodzielnego wykonania

43 Zasady modernizacji lokalnej sieci komputerowej

ZAGADNIENIA

- **Jakie czynniki należy uwzględnić, planując modernizację sieci?**
- **Z jakich etapów składa się modernizacja lokalnej sieci komputerowej?**
- **Jakie czynniki należy brać pod uwagę przy podejmowaniu decyzji dotyczących wyboru oprogramowania i sprzętu?**

Sieć komputerowa składa się z wielu elementów tworzących całość: sprzętu komputerowego, okablowania i oprogramowania. Większość elementów sieci komputerowej można wymieniać lub modernizować w zależności od potrzeb użytkownika. Najtrudniejsze do modernizacji lub wymiany jest okablowanie strukturalne. Modernizacja okablowania strukturalnego najczęściej jest związana z remontem pomieszczeń, dlatego czas pracy okablowania planowany jest na kilkanaście lat.

Modernizacja lub wymiana infrastruktury sieciowej najczęściej wykonywana jest, gdy:

- Firma rozwija się i system telekomunikacyjny przestaje spełniać rosnące wymagania użytkowników.
- Pojawia się potrzeba zmniejszenia kosztów utrzymania i wykorzystania nowych technologii, np. wirtualizacji serwerów lub wprowadzenia nowych usług, takich jak możliwość prowadzenia wideokonferencji. Nowe technologie na ogół wymagają większej przepustowości sieci.
- Konkurencyjność i rozwój firmy wymuszają wprowadzanie nowych aplikacji wymagających modernizacji sieci.

Projektując modernizację sieci komputerowej, należy uwzględnić:

- funkcjonalność sieci – jakie usługi są wymagane przez użytkowników;
- zagrożenia dla bezpieczeństwa, np. włamania, wirusy;
- potrzeba połączeń między jednostkami organizacyjnymi (filie, oddziały);
- wymagania oprogramowania: platforma sprzętowa, oprogramowanie serwera i stacji roboczych, wykorzystywane aplikacje;
- czy dysponujemy wydzielonym pomieszczeniem – serwerownią;
- czy istnieje możliwość zastosowania okablowania strukturalnego wspólnego dla komputerów i telefonów;
- wykorzystanie nowych technologii, np. sieci bezprzewodowych – oferują niższy koszt inwestycji w zakup sprzętu i instalację systemu, ale mają ograniczoną przepustowość i zasięg.

Modernizacja istniejącego okablowania strukturalnego powinna przebiegać według schematu:

- Analiza potrzeb klienta – należy precyzyjnie ustalić, czego klient oczekuje, co i czy wymaga modernizacji, zarówno w zakresie okablowania, sprzętu, jak i oprogramowania.

- Inwentaryzacja istniejącego sprzętu i oprogramowania – pozwala zapoznać się z firmą, budową sieci oraz aktualnym wyposażeniem w sprzęt i oprogramowanie. W oparciu o inwentaryzację można zaplanować działania i oszacować ich koszty.
- Analiza warunków technicznych – możliwość rozbudowy, wykorzystania istniejących elementów i oprogramowania.
- Stworzenie koncepcji modernizacji.
- Wykonanie projektu – struktura sieci, dobór technologii, sprzętu i oprogramowania.
- Instalacja i przeprowadzenie testów.
- Wykonanie pomiarów dynamicznych wszystkich torów transmisyjnych w okablowaniu strukturalnym.
- Uruchomienie i konfiguracja.
- Wprowadzenie zmian w dokumentacji.
- Eksploatacja okablowania.

Oprogramowanie wykorzystywane w firmie obejmuje zarówno systemy operacyjne serwerów i stacji roboczych, pakiety biurowe (edytor tekstów, arkusz kalkulacyjny), jak i specjalistyczne programy wykorzystywane w firmie. Wybór oprogramowania jest to najważniejsza decyzja związana z modernizacją systemu informatycznego w każdej firmie. Przede wszystkim należy podjąć decyzję odnośnie oprogramowania specjalistycznego, wykorzystywanego do prowadzenia działalności firmy – pozostawić aktualnie wykorzystywane czy zakupić nowe? Powodem wymiany oprogramowania może być osiągnięcie granicy możliwości przez dotychczasowe oprogramowanie, co blokuje rozwój firmy, lub zmiana wymagań użytkownika w stosunku do oprogramowania. Wdrożenie nowego oprogramowania jest procesem, który trzeba dokładnie zaplanować; należy m.in. przewidzieć odpowiednio dużo czasu na migrację danych ze starego systemu do nowego. Wybór oprogramowania ma wpływ na dobór sprzętu komputerowego i systemów operacyjnych serwerów i stacji roboczych. Wyboru tego należy dokonać tak, by oprogramowanie jak najlepiej odpowiadało potrzebom firmy. Oprogramowanie to powinno też być skalowalne – zapewniać możliwość jego użytkowania w rozrastającej się sieci komputerowej. W dalszej kolejności należy zastanowić się nad aplikacjami innego typu, np. do prac biurowych.

Postęp technologiczny powoduje, że średnio co kilka lat sprzęt komputerowy powinien być modernizowany lub wymieniany na nowy. Decyzję o wymianie należy podejmować w oparciu o zasady ekonomii i zdrowy rozsądek. Nie zawsze powodem modernizacji jest większa moc obliczeniowa lub szybkość działania nowego sprzętu komputerowego. W niektórych przypadkach ważniejsze jest zapobieganie awariom – niektóre elementy i podzespoły pracujące bez przerwy zużywają się lub tracą swoje parametry, np. łożyska w dyskach twardych lub kondensatory elektrolityczne wlutowane w zasilacze i płyty główne. Wymiana sprzętu w takim przypadku ma charakter działania prewencyjnego – koszt wymiany jest niższy niż usuwanie awarii.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zastanów się, które elementy sieci w Twojej szkole należałoby wymienić. Zaproponuj optymalne Twoim zdaniem rozwiązanie sieci w szkole. Sporządź listę zmian i sprzętu do wymiany oraz oszacuj koszty modernizacji.

44 Zasady kosztorysowania prac modernizacyjnych

ZAGADNIENIA

- **Jak sporządzić kosztorys modernizacji sieci?**
- **Jak szacować koszty prac związanych z demontażem urządzeń?**
- **Jak szacować koszty materiałów pomocniczych?**
- **Jak uwzględniać koszty utylizacji starego sprzętu komputerowego?**

Przygotowanie projektu modernizacji sieci wymaga sporządzenia kosztorysu prac. Kosztorys modernizacji sporządza się w ten sam sposób, co kosztorys nowej sieci, należy jednak uwzględnić pewne dodatkowe zadania, które nie występują podczas budowy nowej sieci. Przed sporządzeniem kosztorysu konieczne jest sporządzenie inwentaryzacji istniejącego okablowania, sprzętu aktywnego i pasywnego oraz oprogramowania sieciowego. W porozumieniu z inwestorem należy ustalić, które elementy dotychczas działające w sieci mają być ponownie wykorzystane w nowej sieci. Większość decyzji w tej sprawie podejmuje się w oparciu o rachunek ekonomiczny, jednak w niektórych przypadkach bardzo trudno jest ocenić skutki ekonomiczne podejmowanych działań. Przykładowo, wdrożenie nowego systemu informatycznego wymaga czasu oraz wiąże się z dodatkowym nakładem pracy i kosztów pośrednich, takich jak straty spowodowane przerwą w funkcjonowaniu przedsiębiorstwa, kosztem migracji danych do nowego systemu, testowania systemu i szkoleniami pracowników w obsłudze nowego systemu. Ponadto należy uwzględnić fakt, że przez pewien czas potrzebny na zapoznanie się z nowym systemem wydajność pracowników może być niższa. W kosztorysie modernizacji należy uwzględnić koszty związane z demontażem starego systemu lub jego elementów. Dla wyceny kosztów demontażu urządzeń okablowania strukturalnego należy stosować nakłady robocizny na montaż z odpowiednich tablic katalogów KNR z następującymi współczynnikami:

- 0,6 przy demontażu materiałów przeznaczonych do ponownego montażu,
- 0,4 przy demontażu materiałów nie nadających się do ponownego montażu.

Ponadto należy uwzględnić pewne straty materiałów – nie wszystkie materiały z demontażu można będzie wykorzystać w nowej sieci.

Jednostkowe nakłady rzeczowe mogą być ustalane na podstawie **katalogów nakładów rzeczowych** KNR. W tabeli 44.1. pokazano przykładowe jednostkowe nakłady związane z montażem gniazd abonenckich. Informacje te pochodzą z katalogu nakładów rzeczowych dla prac związanych z montażem sieci „Okablowanie strukturalne w technologii firmy TYCO", oznaczonego symbolem KNR AT-28. Informacje o jednostkowych nakładach związanych z montażem gniazd abonenckich umieszczono w tabeli 0109 w tym katalogu. W poszczególnych kolumnach tej tabeli umieszczono jednostkowe nakłady związane z realizacją poszczególnych zadań, np. w kolumnie 05 podane są jednostkowe nakłady na montaż modułów RJ45 w gnieździe.

Tabela 44.1. Tabela 0109 z KNR AT-28

Montaż gniazd abonenckich

Wyszczególnienie robót: 1. Przygotowanie gniazda do montażu (kol. 01÷04). 2. Instalacja puszki montażowej (kol. 08). 3. Montaż modułów RJ45 (kol. 05). 4. Montaż adapterów RJ45 w gnieździe (kol. 06). 5. Uziemienie modułów ekranowanych (kol. 07). 6. Mocowanie gniazda na ścianie, w puszce podtynkowej, w kanale instalacyjnym, w podłodze (kol. 01÷04). 7. Przygotowanie i montaż etykiety opisowej gniazda (kol. 01÷04).

Nakłady na 1 szt. — Tablica 0109

Lp.	Wyszczególnienie: Symbol eto	Wyszczególnienie: Rodzaje zawodów, materiałów i sprzętu	Jednostki miary Oznaczenia: Cyfrowe	Jednostki miary Oznaczenia: Literowe	Gniazdo: Natynkowe	Gniazdo: Podtynkowe	Gniazdo: Kanałowe	Gniazdo: Podłogowe
a	b	c	D	e	01	02	03	04
01	315	Monter-instalator – grupa V	149	r-g	0,30	0,21	0,18	0,28
		Razem	149	r-g	0,30	0,21	0,18	0,28
20	–	Gniazdo natynkowe TYCO	090	kpl.	1	–	–	–
21	–	Gniazdo podtynkowe TYCO	090	kpl.	–	1	–	–
22	–	Gniazdo kanałowe TYCO	090	kpl.	–	–	1	–
23	–	Gniazdo podłogowe TYCO	090	kpl.	–	–	–	–

Nakłady na 1 szt. — cd tablicy 0109

Lp.	Wyszczególnienie: Symbol eto	Wyszczególnienie: Rodzaje zawodów, materiałów i sprzętu	Jednostki miary Oznaczenia: Cyfrowe	Jednostki miary Oznaczenia: Literowe	Gniazdo: Montaż modułu RJ45 w gnieździe	Gniazdo: Montaż wkładki ACO	Gniazdo: Montażadaptera światłowodowego SC/MT-RJ	Gniazdo: Montaż puszki
a	b	c	D	e	05	06	07	08
01	315	Monter-instalator – grupa V	149	r-g	0,015	0,014	0,090	0,085
		Razem	149	r-g	0,015	0,014	0,090	0,085
20	–	Gniazdo natynkowe TYCO	090	kpl.	–	–	–	–
21	–	Gniazdo podtynkowe TYCO	090	kpl.	–	–	–	–
22	–	Gniazdo kanałowe TYCO	090	kpl.	–	–	–	–
23	–	Gniazdo podłogowe TYCO	090	kpl.	–	–	–	–
24	–	Wkładka ACO TYCO	090	kpl.	–	–	–	–
25	–	Adapter światłowodowy SC/MT-RJ TYCO	090	kpl.	–	1	–	–
26	–	Puszka instalacyjna	090	kpl.	–	–	1	–
					–	–	–	1

Koszt jednostkowy przygotowania gniazda natynkowego do montażu wynosi 0,30, instalacji puszki montażowej 0,085, montażu modułów RJ-45 w gnieździe 0,015. Zgodnie z zasadami koszt jednostkowy demontażu takiego gniazda wyniesie 0,24, jeżeli gniazdo ma być użyte ponownie, lub 0,16, jeżeli gniazdo nie będzie ponownie używane.

Wartość kosztorysowa materiałów ustalana jest na podstawie cenników producentów lub dystrybutorów (z uwzględnieniem dodatku związanego z kosztami zakupu). Sposób postępowania jest taki sam jak dla sporządzania kosztorysu nowej sieci. Wartość kosztorysową materiałów pomocniczych ustala się przez zastosowanie stawki 1,5%, liczonej od sumy kosztów robocizny ujętej w poszczególnych kolumnach.

Sprzęt elektroniczny, w tym również komputerowy, podlega szczególnym przepisom o ochronie środowiska. W przypadku sprzętu aktywnego, np. komputerów, monitorów, drukarek itp, który nie będzie użytkowany w nowej sieci, należy przewidzieć koszty jego utylizacji.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wykonaj kosztorys naprawy (wymiany w całości) toru kablowego, którym Twój komputer przyłączony jest do przełącznika.

45 Przykładowe zadania projektowe do samodzielnego wykonania

ZAGADNIENIA
- **Jak należy wykonać własny projekt sieci komputerowej?**
- **Jakie są wymagania dotyczące własnego projektu?**
- **Jakie obowiązują zasady oceniania projektów?**

Najbardziej skuteczną metodą nauki tworzenia projektów - jest metoda praktyczna. Samodzielne opracowanie projektu sieci stwarza możliwości zapoznania się z problemami pojawiającymi się podczas tworzenia i realizacji projektu oraz metodami rozwiązywania tych problemów.

Celem projektu jest poznanie zasad projektowania okablowania sieci komputerowych, realizacja projektu sieci i przedstawienie przykładowych rozwiązań.

Warunki zaliczenia projektu

- Przedstawić projekt okablowania sieci komputerowej LAN spełniający określone wymagania projektowe, ustalone z prowadzącym zajęcia.
- Opracować dokumentację techniczną rozwiązania zgodnie z podanymi wymaganiami.
- Zadanie można realizować pojedynczo lub w grupach złożonych maksymalnie z dwóch osób.
- Dokumentację projektową, zredagowaną zgodnie z przyjętym opisem, należy w ustalonym terminie przekazać prowadzącemu.

Dokumentacja projektowa powinna składać się z następujących elementów

1. Strony tytułowej (wg wzoru podanego przez prowadzącego).
2. Spisu treści, spisu rysunków, spisu tabel, spisu literatury.
3. Wstępu, celu i zakresu realizowanego projektu, informacji o przeznaczeniu sieci.
4. Treści zadania i założeń ogólnych.
   Dokładna treść zadania wraz ze wszystkimi uzgodnionymi założeniami oraz rysunkami poglądowymi, w razie konieczności uzupełniona planami schematycznymi budynków i pomieszczeń.
5. Założeń dotyczących przepustowości sieci.
   Założenia dotyczące wymaganej przepustowości wszystkich segmentów sieci (w tym łączy WAN), ze szczególnym uwzględnieniem charakterystyki ruchu i koncentracji serwerów.
6. Koncepcji rozwiązania i proponowanych technologii.
   Propozycja wykonania sieci wraz z dokładnym wskazaniem technologii sieciowej wykonania każdego segmentu sieci. Rozwiązanie musi zapewniać właściwy poziom nadmiarowości. Należy krótko scharakteryzować zaproponowane technologie oraz uzasadnić ich wybór.

7. Proponowanej topologii sieci.
8. Prezentacji proponowanych topologii wszystkich segmentów sieci, z uwzględnieniem wymagań proponowanych technologii oraz wymagań projektu. Propozycje powinny dotyczyć także połączeń dla sieci WAN oraz rozmieszczenia punktów dostępowych dla lokalnych sieci bezprzewodowych.
9. Planu adresacji sieci.
   Podział sieci na VLAN-y zgodnie ze strukturą organizacyjną firmy lub instytucji. Propozycja adresacji IP projektowanej sieci ze wskazaniem adresów wszystkich sieci i ich masek, bez konieczności wskazywania adresów IP poszczególnych komputerów.
10. Doboru sprzętu.
    Szczegółowe wskazania dotyczące niezbędnego sprzętu aktywnego w sieci. Dobór powinien uwzględniać możliwość rozbudowy sieci. Dokładna specyfikacja wybranych urządzeń aktywnych, wraz z ich krótkim opisem i charakterystyką.
11. Projektu okablowania.
    Dokładny projekt okablowania strukturalnego sieci, z uwzględnieniem wszystkich norm i wymogów. Projekt powinien obejmować wskazanie torów kablowych z obliczonymi długościami kabli (w ramach budynków i pomiędzy nimi), rozmieszczenie punktów dystrybucyjnych oraz punktów abonenckich.
    Projekt wszystkich punktów dystrybucyjnych, obejmujący rozmieszczenie wszystkich urządzeń oraz paneli i innych wymaganych oraz zalecanych elementów w szafach dystrybucyjnych. W projektach szaf należy uwzględnić wymagania producentów urządzeń aktywnych. Wszystkie szafy punktów dystrybucyjnych powinny być przedstawione w postaci rysunków schematycznych.
12. Kosztorysu.
    Szacunkowy kosztorys wszystkich elementów projektowanej sieci komputerowej: elementów aktywnych sieci, elementów okablowania strukturalnego oraz wszelkich opłat dotyczących połączeń WAN.

Kryteria oceny projektu

Na ocenę końcową składają się trzy elementy:

1) ocena efektu końcowego, a w szczególności:
   a) zawartość merytoryczna, treść,
   b) zgodność z tematem projektu,
   c) oryginalność,
   d) stopień wykorzystania materiałów źródłowych;
2) wkład ucznia w realizację projektu, a w szczególności:
   a) zaangażowanie ucznia, pracowitość,
   b) pomysłowość i innowacyjność,
   c) umiejętność pracy w grupie,
   d) stopień trudności zadań,
   e) terminowość wykonania przydzielonych zadań,
   f) udział w prezentacji;
3) ocena prezentacji, w tym:
   a) poprawność językowa,
   b) słownictwo specjalistyczne,
   c) efekt artystyczny,
   d) atrakcyjność,

e) estetyka,
f) technika prezentacji,
g) stopień zainteresowania odbiorców,
h) poprawność udzielanych wyjaśnień, odpowiedzi na pytania.

Maksymalna liczba punktów przyznana za projekt wynosi 30. Za każdy z elementów można uzyskać od 0 do 10 punktów. Projekt uważa się za zrealizowany, jeżeli uzyskał minimum 50% punktów możliwych do zdobycia w każdym z elementów.

Tabela 45.1. Proponowana tabela ocen

Liczba punktów	Ocena	Liczba punktów	Ocena
poniżej 15	niedostateczny	21–24	dobry
15–18	dopuszczający	25–28	bardzo dobry
18–21	dostateczny	29–30 uczeń samodzielnie wykonał projekt w sposób wykraczający ponad poziom szkoły średniej	celujący

Przykładowe tematy projektów

1. Projekt okablowania szkolnej sieci komputerowej złożonej z 5 pracowni po 16 komputerów. Łączność pomiędzy pracowniami możliwa tylko za pośrednictwem routera.
2. Projekt okablowania biblioteki. W bibliotece dostęp do katalogów w formie elektronicznej (10 komputerów), w czytelni (20 komputerów) oraz hotspot. Dla pracowników 10 komputerów.
3. Projekt okablowania dla firmy mieszczącej się w jednym budynku 3-kondygnacyjnym. Pracownicy firmy podzieleni są na działy: administracja, księgowość, informatycy, handlowcy.
4. Projekt okablowania dla firmy mieszczącej się w dwóch budynkach oddalonych od siebie o 500 m. W 2-kondygnacyjnym budynku A zlokalizowani są pracownicy działu: administracji i księgowości, w 3-kondygnacyjnym budynku B – informatycy i handlowcy.
5. Projekt okablowania dla hotelu. Przewodowy dostęp do internetu w każdym pokoju. W sali konferencyjnej dostęp bezprzewodowy. Dla pracowników przeznaczyć 10 komputerów.

WYKAZ POJĘĆ

Adres fizyczny MAC (Media Access Control) – jest nadawany przez producenta każdej karcie sieciowej NIC (Network Interface Card) podczas jej wytwarzania.

Adres logiczny – jest nadawany przez administratora sieci, wskazuje punkt przyłączenia do sieci, który jest nazywany interfejsem.

Adres prywatny – adresy przeznaczone do stosowania w sieciach lokalnych, nie jest widoczny w internecie.

Adres rozgłoszeniowy (broadcast) – adres, dzięki któremu komputer może wysłać wiadomość do wszystkich urządzeń w danej sieci lub podsieci (domenie rozgłoszeniowej).

Adres sieci (network address) – adres identyfikujący całą sieć komputerową opartą na protokole IP.

Architektura klient-serwer (client-server) – organizacja sieci, w której istnieje jeden lub więcej komputerów spełniających tylko funkcję serwera.

Architektura równorzędna (peer-to-peer) – organizacja sieci, w której każdy użytkownik może jednocześnie udostępniać zasoby swojego komputera oraz korzystać z zasobów innych komputerów.

Bezprzewodowa sieć lokalna WLAN (Wireless Local Area Network) – jest to sieć, w której połączenia między urządzeniami sieciowymi zrealizowano bez użycia przewodów.

Brama sieciowa (gateway) to urządzenie, za pośrednictwem którego komputery z sieci lokalnej komunikują się z komputerami w innych sieciach.

Dekapsulacja (decapsulation) – proces łączenia jednostek danych i usuwania nagłówków, realizowany podczas odbierania informacji i przesyłania danych do górnych warstw modelu OSI.

Dokumentacja techniczna – zbiór informacji dotyczących urządzenia, jego instalowania oraz działania.

Domena kolizyjna (collision domain) – obszar sieci, w którym może dojść do kolizji danych nadawanych przez różne stacje.

Domeny Najwyższego Poziomu (Top-Level-Domains) – domeny na samym szczycie drzewa DNS obsługujące główne domeny, np. **.com**, **.edu**, **.org**, oraz domen krajowych, np. **.pl**, **.de**.

Domena rozgłoszeniowa (broadcast domain) – obszar sieci, w którym następuje emisja komunikatu rozgłoszeniowego wysyłanego przez jedną stację do wszystkich innych.

Dostawca usługi internetu ISP (Internet Service Provider) – firma oferująca usługę dostępu do internetu.

Ethernet, FastEthernet, GigabitEthernet – technologie używane w sieciach lokalnych.

Enkapsulacja (encapsulation) – proces podziału strumienia danych na jednostki danych i opatrywania ich nagłówkami.

Główny punkt dystrybucyjny MDF (Main Distribution Facility) – stanowi centrum okablowania w topologii gwiazdy.

Główne serwery nazw (root level servers) – serwery zlokalizowane w Stanach Zjednoczonych i podłączone do szybkich sieci szkieletowychinternetu. Przechowują adresy serwerów nazw dla domen najwyższego poziomu, np. **.com**, **.edu**, **.org**, oraz domen krajowych, np. **.pl**, **.de**, **.uk**.

Gniazda abonenckie – punkty przyłączenia użytkownika do sieci.

Host – stacja w sieci.

Internet – ogólnoświatowa sieć komputerowa, logicznie połączona w jednorodną sieć adresową opartą na protokole IP (Internet Protocol).

Jednostkowy nakład rzeczowy – wielkość danego nakładu przypadająca na wybraną jednostkę obmiarową danego rodzaju robót. Służy do szacowania kosztów.

Kabel koncentryczny (coaxial cable) – kabel zbudowany z miedzianego rdzenia umieszczonego w osi kabla, otoczonego izolatorem oraz ekranem.

Kabel prosty (straight-through) – wtyki na obu końcach są wykonane według jednego standardu.

Kabel skrosowany (crossover) – wtyk na jednym końcu jest wykonany według standardu 568A, a na drugim według standardu 568B.

Kamień milowy – warunek określający zakończenie etapu realizacji projektu.

Karta sieciowa (Network Interface Card) – to urządzenie łączące komputer z lokalną siecią komputerową.

Katalog nakładów rzeczowych – zbiór jednostkowych nakładów rzeczowych, będący podstawą szacowania kosztów.

Klient – dowolny komputer lub program nawiązujący połączenie z usługami lub żądający usług od innego komputera lub programu.

Komputerowy system sieciowy – system złożony z serwerów, stacji roboczych, urządzeń sieciowych i okablowania, wraz z oprogramowaniem sieciowym i użytkowym.

Koncentrator (hub) – urządzenie sieciowe posiadające wiele portów służących do przyłączania stacji roboczych lub innych urządzeń.

Łącze komunikacyjne – zespół środków technicznych służących do przesyłania sygnałów między oddalonymi stacjami sieci teleinformatycznej.

Łączność bezprzewodowa – rodzaj łączności, która do transmisji danych wykorzystuje fale elektromagnetyczne.

Maska podsieci (Subnetwork Mask) – określa, ile bitów w adresie jest przeznaczonych do identyfikacji sieci i podsieci, a ile bitów do identyfikacji hosta.

Medium transmisyjne – medium, przez które przesyłane są dane.

Model hierarchiczny sieci – trójwarstwowy model wykorzystywany do projektowania sieci przełączanych.

Modem (Modulator DEModulator) – urządzenie, które zamienia cyfrowe dane generowane przez komputer na sygnały analogowe i wysyła je za pomocą sieci.

Most (bridge) – urządzenie sieciowe posiadające dwa porty, służące do łączenia segmentów sieci.

Nadmiarowość – metoda zwiększenia niezawodności sieci.

Nagłówek IP – część pakietu IP zawierająca informacje niezbędne do przesyłania i kontroli pakietu (zawiera między innymi adresy IP nadawcy i odbiorcy oraz pole TTL).

Okablowanie pionowe (wewnątrz budynku) – kable miedziane lub/i światłowodowe ułożone zazwyczaj w głównych pionach telekomunikacyjnych budynków, realizujące połączenia między punktami rozdzielczymi systemu.

Okablowanie poziome – część okablowania między punktem rozdzielczym a gniazdem użytkownika.

Okablowanie strukturalne – system modularny, pozwalający na realizację połączeń systemu teleinformatycznego, z możliwością zmian konfiguracji oraz rozbudowy z użyciem takich samych elementów.

Oprogramowanie komunikacyjne (communication software) – oprogramowanie, które korzysta z protokołów i sterowników do wymiany danych.

Opóźnienie urządzenia sieciowego – czas poświęcony przez urządzenie na przetwarzanie pakietu lub ramki.

Pakiet – podstawowa jednostka informacji w warstwie sieciowej modelu OSI. Składa się z nagłówka sieci i obszaru danych.

Połączenia systemowe – połączenia między serwerami a szkieletem sieci.

Połączenia telekomunikacyjne budynków (okablowanie międzybudynkowe lub kampusowe) – okablowanie pionowe łączące różne budynki.

Port protokołu – liczba identyfikująca proces działający na odległym komputerze.

Pośredni punkt dystrybucyjny IDF (Intermediate Distribution Facility) – jest lokalnym punktem rozdzielczym, obsługującym najczęściej dany obszar roboczy lub piętro.

Projekt – działania, w których celem jest opracowanie czegoś nowego, wymagające nierutynowego podejścia.

Protokół IP (Internet Protocol) – protokół warstwy sieciowej, odpowiedzialny za przesyłanie pakietów między użytkownikami sieci.

Protokół UDP (User Datagram Protocol) – protokół warstwy transportowej w trybie bezpołączeniowym.

Protokół STP (Spanning-Tree Protocol) – protokół używany w sieciach przełączanych w celu utworzenia topologii logicznej bez pętli, na bazie topologii fizycznej z pętlami.

Protokół TCP (Transmission Control Protocol) – protokół warstwy transportowej w trybie połączeniowym.

Protokoły routingu – protokoły wykorzystywane przez routery do wymiany między sobą informacji o trasach lub topologii sieci.

Protokoły (protocols) – określają sposoby komunikowania się urządzeń, np. protokół IP.

Protokoły bezpołączeniowe – protokoły komunikacyjne, w których komunikaty przekazywane są niezależnie.

Protokoły internetowe – podzbiór protokołów komunikacyjnych stosowanych w sieci internet.

Protokoły komunikacyjne – zbiór reguł postępowania automatycznie wykonywanych przez urządzenia komunikacyjne w celu nawiązania łączności i wymiany danych.

Protokoły połączeniowe – protokoły komunikacyjne, w których ustanawia się logiczne połączenie pomiędzy dwoma komunikującymi się ze sobą urządzeniami.

Przekazywanie żetonu (Token-Passing) – metoda dostępu do nośnika, w której w pierścieniu krąży specjalna ramka (token).

Przełącznik (switch) – wieloportowe urządzenie sieciowe, które oferuje te same funkcje co koncentrator, a dodatkowo pozwala, podobnie jak most, podzielić sieć na segmenty.

Punkt dostępowy (Access Point) – urządzenie sieciowe zapewniające stacjom bezprzewodowym dostęp do zasobów sieci za pomocą bezprzewodowego medium transmisyjnego.

Punkty rozdzielcze – węzły sieci w topologii gwiazdy, w których zbiega się okablowanie poziome i pionowe.

Ramka – jednostka danych w warstwie łącza danych.

Router – urządzenie sieciowe łączące sieci, wyposażone w co najmniej dwa interfejsy sieciowe. Jeden z nich może być wykorzystywany do przyłączenia sieci do internetu (interfejs zewnętrzny WAN), drugi umożliwia przyłączenie sieci lokalnej (interfejs wewnętrzny LAN).

Rysunek techniczny – typ dokumentacji rysunkowej pozwalający na wierne odzwierciedlenie zarówno ogólnego kształtu produktu, jak i jego szczegółów technicznych.

Segment – jednostka danych w warstwie transportowej modelu OSI.

Serwer – komputer udostępniający zasoby innym komputerom w sieci.

Serwer pośredniczący (Proxy Server) – specjalny serwer, którego zadaniem jest buforowanie na dysku lokalnym odwiedzonych wcześniej stron WWW.

Sieciowy system operacyjny – system operacyjny instalowany na serwerze.

Sieć komputerowa (computer network) – grupa komputerów lub innych urządzeń, połączonych ze sobą w celu wymiany danych lub współdzielenia różnych zasobów.

Sieci osobiste PAN (Personal Area Network) – sieci o zasięgu kilku metrów, wykorzystywane np. do bezprzewodowego połączenia telefonu komórkowego ze słuchawką.

Sieci lokalne LAN (Local Area Network) – sieci łączące użytkowników na niewielkim obszarze (pomieszczenie, budynek).

Sieci miejskie MAN (Metropolitan Area Network) – sieci o zasięgu miasta, najczęściej szybkie.

Sieci rozległe WAN (Wide Area Network) – sieci, których zasięg przekracza granice miast, państw i kontynentów, np. internet.

Skalowalność – podatność sieci na rozbudowę.

Skrętka (Twisted Pair) – najpopularniejsze medium transmisyjne, używane obecnie do budowy sieci lokalnych.

Sniffer – program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i analizowanie danych przepływających w sieci.

Sterownik – oprogramowanie umożliwiające komputerowi komunikację ze sprzętem lub urządzeniami.

Szum – niepożądany sygnał pochodzący ze źródeł naturalnych lub sztucznych.

Ścieżka krytyczna – nieprzerwany ciąg zadań o najdłuższym czasie realizacji.

Średnica sieci komputerowej – liczba urządzeń, przez które dane muszą przejść, zanim dotrą do swojego miejsca docelowego.

Światłowód (Fiber Optic Cable) – nośnik transmisji przewodowej, wykonany ze szkła kwarcowego lub specjalnego tworzywa sztucznego, przystosowany do przesyłania wiązki światła.

TFTP (Trivial File Transfer Protocol) – prosty protokół wykorzystywany do przesyłania plików.

Token Ring – technologia sieciowa, w której stosuje metodę dostępu do nośnika, nazywaną przekazywaniem żetonu (Token-Passing).

Topologia fizyczna sieci – określa geometryczną organizację sieci lokalnej, graficznie przedstawiając jej kształt i strukturę.

Topologia logiczna sieci – opisuje reguły komunikacji, z których korzystają urządzenia komunikujące się w sieci.

Topologia sieci – określa sposób jej wykonania, czyli połączenia urządzeń komputerowych za pomocą medium transmisyjnego.

Transmisja dupleks (full-duplex) – transmisja jednoczesna i dwukierunkowa.

Transmisja grupowa (multicast) – transmisja, w której dane przeznaczone są tylko do wybranej grupy urządzeń.

Transmisja jednokierunkowa (simplex) – transmisja, w której odbiornik nie może przesłać odpowiedzi ani innych danych.

Transmisja jednostkowa (unicast) – w komunikacji biorą udział dwa urządzenia, jedno urządzenie wysyła dane do dokładnie jednego urządzenia.

Transmisja półdupleks (half-duplex) – transmisja dwukierunkowa, naprzemienna.

Transmisja rezgłoszeniowa (broadcast) – transmisja, w której dane przeznaczone są tylko dla wszystkich urządzeń w sieci.

Transmisja szerokopasmowa (broadband) – polega na podziale pojedynczego łącza na wiele kanałów.

Transmisja w paśmie podstawowym (baseband) – polega ona na utworzeniu w łączu tylko jednego kanału transmisyjnego, za pomocą którego jest przesyłany tylko jeden ciąg sygnałów.

Trasowanie, routing – proces wyznaczania trasy do miejsca przeznaczenia pakietów.

Urządzenia dostępu – są odpowiedzialne za formatowanie danych w taki sposób, aby nadawały się one do przesyłania w sieci, a także za umieszczanie danych w sieci oraz ich odbieranie.

Urządzenia transmisji – nośniki używane do transportu sygnałów biegnących przez sieć do miejsc docelowych.

Urządzenia wzmacniania przesłanych sygnałów – urządzenia, które odbierają przesyłane sygnały, wzmacniają je i wysyłają z powrotem do sieci

Usługa APIPA (Automatic Private IP Addressing) – usługa odpowiedzialna za automatyczne przydzielanie adresu IP komputerowi w przypadku, gdy karta sieciowa komputera jest skonfigurowana do żądania przyznania adresu IP z serwera DHCP, a serwer DHCP w danym momencie jest nieosiągalny.

Usługa NAT (Network Address Translation) – tłumaczenie adresów prywatnych na publiczne realizawane w bramie lub routerze.

Węzeł sieci – urządzenie sieciowe, w którym zbiega się wiele łączy komunikacyjnych.

Wirtualna sieć lokalna VLAN (Virtual Local Area Network) – to sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej.

Wykres Gantta – typ wykresu ilustrującego terminarz działań.

Wzmacniak, regenerator – urządzenie sieciowe wykorzystywane w miejscach, w których jest wymagane wzmocnienie lub regeneracja sygnału, niezbędne do zwiększenia zasięgu sieci.

Zapora sieciowa (firewall) – jedna z możliwości zabezpieczania sieci i systemów komputerowych przed nieuprawnionym dostępem, np. z internetu, lub przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz.

Zasilacz UPS (zasilacz awaryjny) – wtórne źródło energii elektrycznej, które prąd pobiera z wcześniej naładowanych akumulatorów.

Zasoby projektu – środki niezbędne do zrealizowania projektu.

WYKAZ SKRÓTÓW

ANSI (American National Standards Institute) – amerykańska organizacja standaryzacyjna.

APIPA (Automatic Private IP Addressing) – usługa odpowiedzialna za automatyczne przydzielanie adresu IP komputerowi w przypadku, gdy karta sieciowa komputera jest skonfigurowana do żądania przyznania adresu IP z serwera DHCP, a serwer DHCP w danym momencie jest nieosiągalny.

ARP (Address Resolution Protocol) – protokół, który pozwala na ustalenie adresu sprzętowego MAC hosta, gdy dany jest adres warstwy sieciowej IP.

BPD – budynkowy punkt dystrybucyjny.

CAD (Computer-aided design) – oprogramowanie wspomagające tworzenie dokumentacji rysunkowej.

CIDR (Classless Inter-Domain Routing) – bezklasowa metoda przydzielania adresów IP.

CLI (Command-line Interface) – interfejs wprowadzania poleceń za pomocą klawiatury.

CPD – centralny punkt dystrybucyjny.

CPU (Central Processing Unit) – urządzenie cyfrowe sekwencyjne, które pobiera dane z pamięci, interpretuje je i wykonuje jako rozkazy (procesor).

CRC (Cycling Redundancy Check) – mechanizm kontroli błędów stosowany w sieciach komputerowych.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) – metoda dostępu do nośnika stosowana w sieciach bezprzewodowych.

CSMA/CD (Carrier Sense Multiple Access Colision Detect) – metoda dostępu do nośnika na zasadzie rywalizacji.

DHCP (Dynamic Host Configuration Protocol) – protokół dynamicznego konfigurowania hostów.

DNS (Domain Name System) – system zapewniający zamianę adresów domenowych na adresy IP.

DSL (Digital Subscriber Line) – cyfrowa linia abonencka, rodzina technologii szerokopasmowego dostępu do internetu.

DUAL (Diffusing-Update ALgorithm) – algorytm wykorzystywany w protokole EIGRP.

EGP (Exterior Gateway Protocol) – protokoły routingu zewnętrznego.

EIA/TIA – (Electronics Industry Association/Telecommunications Industry Association) – organizacje, które stworzyły wiele standardów dotyczących komunikacji w sieci.

EIGRP (Extended IGRP) – protokół routingu opracowany przez CISCO.

ELFEXT (Equal Level Far End Crosstalk) – odmiana przesłuchu zdalnego FEXT, w odróżnieniu od FEXT jest niezależna od długości badanego toru, gdyż uwzględnia tłumienie wnoszone przez tor transmisyjny.

FEXT (Far End Crosstalk) – przesłuch zdalny.

FDDI (Fiber Distributed Data Interface) – cyfrowa sieć o topologii podwójnych przeciwbieżnych pierścieni oparta na nośniku światłowodowym.

FCS (Frame Check Sequence) - pole w ramce Ethernet przeznaczone na wartość sumy kontrolnej

FTP (File Transfer Protocol) – usługa umożliwiająca przesyłanie plików między komputerami.

HTTP (Hypertext Transfer Protocol) – protokół przesyłania dokumentów hipertekstowych, np. stron WWW.

IANA (Internet Assigned Numbers Authority) – organizacja przydzielająca adresy IP na świecie.

ICMP (Internet Control Message Protocol) – protokół zawierający mechanizmy informowania o błędach w funkcjonowaniu sieci IP oraz diagnostyki sieci.

IDF (Intermediate Distribution Facility) – pośredni punkt dystrybucyjny.

IEEE (The Institute of Electrical and Electronics Engineers) – organizacja zrzeszająca inżynierów z całego świata.

IETF (Internet Engineering Task Force) – organizacja, która publikuje dokumenty RFC (Request for Comments) regulujące rozwój internetu.

IGMP (Internet Group Management Protocol) – protokół wykorzystywany do rozsyłania wiadomości grupowych.

IGP (Interior Gateway Protocols) – protokoły routingu wewnętrznego.

IGRP (Interior-Gateway Routing Protocol) – protokół routingu opracowany przez CISCO.

IMAP (Internet Message Access Protocol) – protokół do pobierania poczty elektronicznej.

IP (Internet Protocol) – protokół komunikacyjny warstwy sieciowej modelu OSI.

IPX/SPX (Internet Packet EXchange/Sequential Packet EXchange) – zestaw protokołów komunikacyjnych firmy Novell.

ISO (International Organization for Standarization) – międzynarodowa organizacja standaryzacyjna.

ISP (Internet Service Provider) – dostawca usługi dostępu do internetu.

KNR – katalogów nakładów rzeczowych.

KPD – kondygnacyjny punkt dystrybucyjny.

LAN (Local Area Network) – lokalna (wewnętrzna) sieć komputerowa.

LPD – lokalny punkt dystrybucyjny.

MAC (Media Access Control) – adres fizyczny karty sieciowej.

MAN (Metropolitan Area Network) – miejska sieć komputerowa, duża sieć komputerowa, której zasięg obejmuje aglomerację lub miasto.

MDF (Main Distribution Facility) – główny punkt dystrybucyjny.

NASK (Naukowa i Akademicka Sieć Komputerowa) – jednostka badawczo-rozwojowa, działająca na terenie Polski, która prowadzi rejestr domen internetowych (DNS) .pl i przydziela adresy IP.

NAT (Network Address Translation) – usługa translacji adresów.

NetBEUI (NetBIOS Extended User Interface) – protokół komunikacyjny opracowany przez IBM.

NEXT (Near End Crosstalk) – przesłuch zbliżny.

NIC (Network Interface Card) – karta sieciowa, umożliwiająca komputerowi dostęp do sieci komputerowej.

OSI (Open Systems Interconnection) – siedmiowarstwowy model sieci komputerowej.

OSPF (Open Shortest Path First) – protokół routingu stanu łącza (link-state),

PAN (Personal Area Network) – sieci osobiste o zasięgu kilku metrów.

PCI (Peripheral Component Interconnect) – magistrala komunikacyjna służąca do przyłączania kart rozszerzeń do płyty głównej w komputerach klasy PC.

PCMCIA (Personal Computer Memory Card International Association) – standard kart rozszerzeń dla komputerów przenośnych.

PCS – punkt centralny sieci.

PDU (Protocol Data Unit) – jednostki danych w określonej warstwie modelu sieci.

PoE (Power over Ethernet) – zasilanie urządzeń przez Ethernet.

POP3 (Post Office Protocol v 3) – protokół do pobierania poczty elektronicznej.

POST (Power-On Self Test) – procedura podczas uruchamiania komputera, gdy system po raz pierwszy zostaje włączony.

PowerSum ACR (Attenuation to Crosstalk Ratio) – określa różnicę pomiędzy tłumieniem, a przesłuchem zbliżnym NEXT dla danej pary przewodów.

QoS (Quality of Service) – obsługa jakości usług.

RARP (Reverse Address Resolution Protocol) – protokół, który pozwala na ustalenie adresu IP na podstawie adresu fizycznego MAC.

RIP (Routing Information Protocol) – protokół routingu wektora odległości (distance-vector).

RIPE (fr. Reseaux IP Europeens) – stowarzyszenie odpowiedzialne za rozwój internetu w Europie.

SNR (signal-to-noise ratio) – stosunek sygnału do szumu.

STP (Shielded Twisted Pair) – skrętka ekranowana.

TCP (Transmission Control Protocol) – protokół kontroli transmisji używany w warstwie transportowej modelu OSI. Jest to protokół połączeniowy. Gwarantuje wyższym warstwom komunikacyjnym dostarczenie wszystkich pakietów w całości, z zachowaniem kolejności i bez duplikatów.

TCP/IP – stos protokołów opisany w warstwowym modelu TCP/IP, używany w sieciach lokalnych i Internecie.

TFTP (Trivial File Transfer Protocol) – uproszczona wersja protokołu FTP.

TTL (Time To Live) – określa maksymalny czas przebywania pakietu w sieci.

U – jednostka wysokości urządzeń sieciowych.

UDP (User Datagram Protocol) – protokół w warstwie transportowej modelu OSI. Jest to protokół bezpołączeniowy, który nie ma mechanizmów kontroli przepływu i retransmisji.

USB (Universal Serial Bus) – rodzaj sprzętowego portu komunikacyjnego komputerów, zastępującego stare porty szeregowe i porty równoległe.

UTP (Unshielded Twisted Pair) – nieekranowana skrętka.

VoIP (Voice over Internet Protocol) – technologia umożliwiająca wykonywanie połączeń telefonicznych tradycyjnym aparatem telefonicznym za pośrednictwem sieci komputerowej wykorzystującej protokół IP.

VLAN (Virtual Local Area Network) – to sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej.

VLSM (Variable Length Subnet Mask) – podsieci o zmiennej długości maski.

WAN (Wide Area Network) – rozległa siec komputerowa znajdująca się na obszarze wykraczającym poza jedno miasto lub kompleks miejski.

WWW (World Wide Web) – usługa umożliwiająca przeglądanie informacji znajdujących się na serwerach.

WYKAZ PODSTAWOWYCH POJĘĆ W JĘZYKACH POLSKIM, ANGIELSKIM I NIEMIECKIM

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
adres fizyczny MAC	physical address MAC- Media Access Control	Physische MAC Adresse (Media Access Control)
adres logiczny	logical address	die logische Adresse
adres prywatny	private IP address	die persönliche IP Adresse
adres rozgłoszeniowy	broadcast	die Sendeadresse
adres sieci	network address	die Netzwerkadresse
architektura klient-serwer	client-server model	das Klient-Server-Modell
architektura równorzędna	peer-to-peer model	das Parallele Model
bezprzewodowa sieć lokalna WLAN	WLAN – Wireless Local Area Network	Wireless Local Area Network
brama sieciowa	network gateway	das Gateway
dekapsulacja	decapsulation	die Dekapsulation
dokumentacja techniczna	technical documentation	die technische Dokumentation
domena kolizyjna	collision domain	die Kollisionsdomäin
Domeny Najwyższego Poziomu	top-level domains	die Domäne oberster Stufe
domena rozgłoszeniowa	broadcast domain	die Übertragungsdomäne
dostawca usługi Internetu ISP	ISP- Internet Service Provider	der Internet-Dienstanbieter
Ethernet / FastEthernet / GigabitEthernet	Ethernet / FastEthernet / GigabitEthernet	Ethernet / FastEthernet / GigabitEthernet
enkapsulacja	encapsulation	die Ummantelung / die Kapselung
główny punkt dystrybucyjny MDF	MDF – Main Distribution Facility	das Hauptabsatzkanal
główne serwery nazw	DNS – Domain Name System	das Domänennamesystem
gniazda abonenckie	socket (e.g. TV, telephone wall socket)	die Steckdose
host	host	der Host
internet	Internet	das Internet
jednostkowy nakład rzeczowy	unit pricing	die Einzelne Sachaufwendung
kabel koncentryczny	coaxial cable	das Koaxialkabel
kabel prosty	straight through/ patch cable	das Patchkabel
kabel skrosowany	crossover cable	das Crossover-Kabel
kamień milowy	milestone	der Meillenstein

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
karta sieciowa	network interface controller / adapter / card	die Netzwerkkarte
katalog nakładów rzeczowych	unit pricing/ material outlays catalog	der Sachaufwendungskatalog
klient	client	der Kunde / der Benutzer
komputerowy system sieciowy	network computer system	das Netzwerk – Computer – System
koncentrator	hub	der Hub
łącze komunikacyjne	communications link	die Kommunikationsverbindung / der Kommunikationslink
łączność bezprzewodowa	Wi-Fi	Wi-Fi (Drahtlose Übermittlung)
maska podsieci	subnet mask / IPv4 subnetting reference	die Subnetzmaske
medium transmisyjne	transmission medium	das Übertragungsmedium
model hierarchiczny sieci	hierarchical network model	das hierarchische Netzwerkmodell
modem	modem	das Modem
most	bridge	die Brücke / der Bus
nadmiarowość	redundancy	die Redundanz
nagłówek IP	IP header	IP-Überschrift
okablowanie pionowe (wewnątrz budynku)	horizontal cabling	die Horizontale Verkabelung
okablowanie poziome	vertical cabling	die Vertikale Verkabelung
okablowanie strukturalne	structured cabling	Struktivere / die gegliederte Verkabelung
oprogramowanie komunikacyjne	communications software	die Kommunikationssoftware
opóźnienie urządzenia sieciowego	propagation delay	die Netzwerkgeraet-Verzögerung
pakiet	packet/ suite (e.g. office suite)	das Paket
połączenia systemowe	system connection	die Systemverbindung
połączenia telekomunikacyjne budynków (okablowanie międzybudynkowe lub kampusowe)	cross-building structured cabling	die Kommunikationsverbindung
port protokołu	port protocol	die Protokoll Schnittstelle
pośredni punkt dystrybucyjny IDF	IDF – Intermediate Distribution Facility	der Indirekte Verteilungspunkt (IDF)
program antywirusowy	antivirus	das Antivirenprogramm
projekt	project	das Projekt
protokół IP	IP – Internet Protocol	das IP – Internet Protokoll
protokół UDP	UDP – User Datagram Protocol	das UPD – Benutzer Datagramm Protokoll
protokół TCP	TCP – Transmission Control Protocol	das TCP – Transmission Control Protokoll / das Übertragungssteuerungsprotokoll

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
protokół TFTP	TFTP – Trivial File Transfer Protocol	das TFTP Transmission Control Protokoll
protokoły routingu	routing protocol	das Routingprotokoll
protokoły	protocols	die Protokolle
protokoły bezpołączeniowe	connectionless protocols	die Verbindungslosen Protokolle
protokoły internetowe	Internet protocols	die Internetprotokolle
protokoły komunikacyjne	communications protocols	die Kommunikationsprotokolle
protokoły połączeniowe	connection-oriented protocols	das Connection Protokoll / das Verbindungsprotokoll
przełącznik	switch	der Umschalter
punkt dostępowy	AP – Access Point	der Anschlusspunkt / die Anschlussstelle
punkty rozdzielcze	distribution points	die Ausgabestellen
ramka	frame	der Rahmen
router	router	der Router
rysunek techniczny	technical drawing	die technische Zeichnung
segment	segment	das Segment
serwer	server	der Server
serwer pośredniczący	proxy server	das Segment / die Gruppe
sieciowy system operacyjny	NOS – Network Operating System	das Netzwerk-Betriebssystem
sieć komputerowa	computer network	das Computernetz
sieci osobiste PAN	PAN – Personal Area Network	das Personale Netz
sieci lokalne LAN	LAN – Local Area Network	das Lokale Netz
sieci miejskie MAN	MAN – Metropolitan Area Network / Municipal Area Network	das Metropolraumnetz
sieci rozległe WAN	WAN – Wide Area Network	das Weitverkehrsnetz (WAN)
skalowalność	scalability	die Skalierbarkeit
skrętka	twisted-pair cable	die Litze
sniffer	sniffer	der Sniffer / , das Suchgerat
sterownik	driver	der Treiber
szum	noise	die Geräusche / das Gerausch
ścieżka krytyczna	CPM – Critical Path Method	der kritische Pfad
średnica sieci komputerowej	network diameter	der Netzwerkdiameter

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
światłowód	fiber-optic cable / optical fibre	der Lichtleiter / die Lichtleitfaser
Token Ring	Token Ring	der Token Ring
przekazywanie żetonu	token passing	die Token-Übermittlung
topologia fizyczna sieci	physical network topology	die Physikalische Topologie des Netzwerks
topologia logiczna sieci	logical network topology	die Logische Topologie des Netzwerks
topologia sieci	network topology	die Netzwerktopologie
transmisja dupleks	duplex transmission	Duplex / die doppelseitige Übertragung
transmisja grupowa	multicasting transmission	das Multicast
transmisja jednokierunkowa	simplex communication	die Simplexkommunikation
transmisja jednostkowa	unicast transmission	die Einheitliche Übermittlung / die Unit-Transmission
transmisja półdupleks	half duplex	die Halbduplex-Übertragung
transmisja rozgłoszeniowa	broadcast transmission	die Übertragung / die Sendung
transmisja szerokopasmowa	broadband transmission	die Breitband-Übertragung
transmisja w paśmie podstawowym	baseband transmission	Übermittlung im Basisfrequenzband / die Grundfrequenzband
trasowanie / routing	routing	das Routing
urządzenia dostępu	access device	die Zugangsgeräte
urządzenia transmisji	DCE – Data Communications Equipment	die Übertragungseinrichtung
urządzenia wzmacniania przesłanych sygnałów	signal booster device	das Signalverstärkungsgerät
usługa APIPA	APIPA – Automatic Private IP Addressing	die Automatische private IP Adresseirung (APIPA)
usługa NAT	NAT – Network Address Translation	die NAT-Netzwerkadresseübersetzung
węzeł sieci	node network	der Netzknoten
wirtualna sieć lokalna VLAN	VLAN – Virtual Local Area Network	das Virtuelle Lokalnetzwerk (VLAN)
wykres Gantta	Gannt chart	das Gannt-Diagramm
wzmacniak, regenerator	repeater	der Repeater / der Verstärker
zapora sieciowa	firewall	die Firewall
zasilacz UPS	UPS – Uninterruptible Power Supply	UPS – ungestörte / die ununterbrochene Stromversorgung
zasoby projektu	project resources	die Projekt-Ressourcen

LITERATURA UZUPEŁNIAJĄCA

1. Bradford R., *Podstawy sieci komputerowych*, WKŁ, Warszawa, 2009.
2. Comer D.E.,*Sieci komputerowe i intersieci*, Helion, Gliwice 2012.
3. Danowski B., *Wi-Fi. Domowe sieci bezprzewodowe. Ilustrowany przewodnik*, Helion, Gliwice 2010.
4. Filocha M., Trusewicz M., *Ćwiczenia z Novell NetWare 5*, Mikom, Warszawa 2006.
5. Fry Ch., Nystrom M., *Monitoring i bezpieczeństwo sieci*, Helion, Gliwice 2010.
6. Hallberg B., *Sieci komputerowe – Kurs podstawowy*, Wydawnictwo Edition, Kraków 2000/2002.
7. Hunt C., *TCP/IP – Administracja sieci*, Oficyna Wydawnicza READ ME, Warszawa 1998.
8. Józefiok A., *Domowe sieci komputerowe. Gotowe rozwiązania*, Helion, Gliwice 2008.
9. Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2007.
10. McDonald R., Dye M., Rufi A.W., *Akademia sieci Cisco CCNA Exploration Semestr 1. Podstawy sieci + CD*, PWN, Warszawa 2008.
11. Lewis W., *Akademia sieci Cisco CCNA Exploration Semestr 3. Przełączanie sieci LAN i sieci bezprzewodowe + CD*, PWN, Warszawa 2007.
12. Michałowska A., Michałowski S., *Sieci komputerowe od A do Z*, Mikom, Warszawa 2000.
13. Pawlak R., *Okablowanie strukturalne sieci. Teoria i praktyka*, Helion, Gliwice 2011.
14. Serafin M., *Sieci VPN. Zdalna praca i bezpieczeństwo danych*, Helion, Gliwice 2011.
15. Shafer K., *Novell. Wielka Księga Sieci*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 1999.
16. Sloan J.D., *Narzędzia administrowania siecią*, Wydawnictwo RM, Warszawa 2002.
17. Sokół M., *E-mail – poczta elektroniczna dla każdego*, Helion, Gliwice 1999.
18. Sportack M., *Sieci komputerowe. Księga eksperta*, Helion, Gliwice 1999.
19. Strebe M., Perkins Ch., *Firewalls – ściany ogniowe*, Mikom, Warszawa 2000.
20. Tittel Ed., Stewart J.M., *Intranet – Biblia*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 1999.
23. Woźniak J., Nowicki K., *Sieci LAN, MAN i WAN – protokoły komunikacyjne*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 2000.
24. Wright R., *Elementarz Routingu IP*, Mikom, Warszawa 1999.

Źródła ilustracji i zdjęć

Okładka: (sieć komputerowa) megainarny/Shutterstock.com

Tekst główny: s. 8 (przykładowe szafy dystrybucyjne) K. Pytel, s. 13 (przykłady mediów transmisyjnych) K. Pytel, s. 16 (przykłady urządzeń sieciowych) K. Pytel, s. 18 (schematy prostej sieci) D. Krajewski, s. 22 (topologia magistrali) D. Krajewski, s. 23 (topologia pierścienia) D. Krajewski, s. 23 (topologia gwiazdy) D. Krajewski, s. 24 (topologia rozgałęzionej gwiazdy) D. Krajewski, s.24 (topologia siatki) D. Krajewski, s. 25 (sieć bezprzewodowa w trybie ad hoc) D. Krajewski, s. 25 (sieć bezprzewodowa w trybie infrastruktury) D. Krajewski, s. 31 (typy transmisji) D. Krajewski, s. 41 (wtyczka RJ-45) K. Pytel, s. 42 (podział sieci na domeny kolizyjne) D. Krajewski, s. 42 (podział sieci na domeny rozgłoszeniowe) D. Krajewski, s. 62 (schemat adresowania sieci w technice VLSM D), Krajewski, s. 76 (model hierarchicznej budowy sieci przełączanej) s. 80 (wybrane urządzenia pasywne) k. Pytel, s. 86 (schemat okablowania strukturalnego) S. Skryskiewicz, s. 87 (schemat logiczny okablowania strukturalnego zgodny z terminologią polską) S. Skryśkiewicz, s. 87 (schemat rozmieszczenia punktów dystrybucyjnych w budynku zgodnie z nazewnictwem angielskim) S. Skryśkiewicz, s. 96 (rysunek techniczny piętra budynku) S. Skryśkiewicz, s. 97 (przekrój pionowy budynku) S. Skryśkiewicz, s. 98 (tablet graficzny) K. Pytel, s. 100 (przekrój poziomy budynku z widocznymi wszystkimi warstwami) S. Skryśkiewicz, s. 111 (kanał kablowy poziomy) S. Skryśkiewicz, s. 114 (przykładowe rozmieszczenie urządzeń w szafie dystrybucyjnej) K. Pytel, s. 117 (fragment planu instalacji okablowania strukturalnego) S. Skryśkiewicz, s. 122 (narzędzie uderzeniowe do montażu kabli) K. Pytel, s. 122 (narzędzie zaciskowe do wtyków RJ-45) K. Pytel, s. 123 (narzędzie do zdejmowania izolacji) K. Pytel, s. 123 (końcówka kabla SC) K. Pytel, s. 124 (końcówka kabla LC) K. Pytel, s. 124 (końcówka kabla ST) K. Pytel, s. 124 (spawarka do światłowodów) K. Pytel, s. 140 (składniki systemu okablowania strukturalnego) S. Skryśkiewicz, s. 140 (elementy systemu okablowania strukturalnego) S. Skryśkiewicz

Wydawnictwa Szkolne i Pedagogiczne oświadczają, że podjęły starania mające na celu dotarcie do właścicieli i dysponentów praw autorskich wszystkich zamieszczonych utworów. Wydawnictwa Szkolne i Pedagogiczne, przytaczając w celach dydaktycznych utwory lub fragmenty, postępują zgodnie z art. 29 ustawy o prawie autorskim. Jednocześnie Wydawnictwa Szkolne i Pedagogiczne oświadczają, że są jedynym podmiotem właściwym do kontaktu autorów tych utworów lub innych podmiotów uprawnionych w wypadkach, w których twórcy przysługuje prawo do wynagrodzenia.

Kształcimy zawodowo!

Wszystkie wymagane kwalifikacje i **aprobata MEN**

Wydawnictwa Szkolne i Pedagogiczne polecają nowe podręczniki do nauki zawodów z branży informatycznej:

- **technik informatyk,**
- **technik teleinformatyk.**

Publikacje zgodne z nową podstawą programową

Podręczniki WSiP zapewnią Ci sukces na egzaminach potwierdzających kwalifikacje zawodowe!

Kwalifikacja E.12.1

Przygotowanie stanowiska komputerowego do pracy. Część 1

Kwalifikacja E.12.1

Przygotowanie stanowiska komputerowego do pracy. Część 2

Kwalifikacja E.12.2

Użytkowanie urządzeń peryferyjnych komputera osobistego

Kwalifikacja E.12.3

Naprawa komputera osobistego

Kwalifikacja E.13.1

Projektowanie i wykonywanie lokalnej sieci komputerowej

Kwalifikacja E.13.2

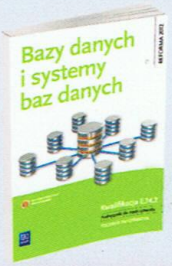
Konfigurowanie urządzeń sieciowych

Kwalifikacja E.13.3

Administrowanie sieciowymi systemami operacyjnymi

Kwalifikacja E.14.1

Witryny internetowe



Kwalifikacja E.14.2

Bazy danych i systemy baz danych

Kwalifikacja E.14.3

Aplikacje internetowe

Język angielski zawodowy w branży elektronicznej, informatycznej i elektrycznej. Zeszyt ćwiczeń

Język niemiecki zawodowy w branży elektronicznej, informatycznej i elektrycznej. Zeszyt ćwiczeń

Wszystkie nasze publikacje można zamówić w księgarni internetowej **sklep.wsip.pl**

WSiP WYDAWNICTWA SZKOLNE i PEDAGOGICZNE

wsip.pl | infolinia: 801 220 555

ISBN 978-83-02-13411-1

51

9 788302 134111