Część 3

Sieci komputerowe

INF.02

KODY



Podręcznik do nauki zawodu

TECHNIK INFORMATYK

WSiP

Autorzy: **Sylwia Osetek, Krzysztof Pytel**

Typ szkoły: **technikum**
Zawód: **technik informatyk**
Kwalifikacja: **INF.02. Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych**

© Copyright by Wydawnictwa Szkolne i Pedagogiczne
Warszawa 2022

Wydanie I (2022)

ISBN 978-83-02-20852-2 (część 3.) (podręcznik w postaci elektronicznej – flipbook)
ISBN 978-83-02-20847-8 (całość) (podręcznik w postaci elektronicznej – flipbook)
ISBN 978-83-02-20371-8 (część 3.) (podręcznik w postaci papierowej)
ISBN 978-83-02-20373-2 (całość) (podręcznik w postaci papierowej)

Opracowanie merytoryczne i redakcyjne: **Tomasz Kompanowski**, **Sebastian Jabłoński**
Redakcja językowa: **Tomasz Karpowicz**, **wizjonerzytekstu.pl**
Redakcja techniczna: **Elżbieta Walczak**
Projekt okładki: **Dominik Krajewski**
Fotoedycja: **Marta Bażyńska**
Skład i łamanie: **Ledor**

Wydawnictwa Szkolne i Pedagogiczne Spółka Akcyjna
00-807 Warszawa, Aleje Jerozolimskie 96
KRS 0000595068
Infolinia: 801 220 555
www.wsip.pl
Druk i oprawa: Orthdruk sp. z o.o., Białystok

QR Code (Kod QR) to zarejestrowany znak towarowy DENSO WAVE INCORPORATED
Odczytanie kodu QR wymaga urządzenia z zainstalowaną aplikacją do odczytywania kodów QR, obsługującą co najmniej kody w wersji czwartej, oraz aparatu o minimalnej rozdzielczości 5 Mpix.

Publikacja, którą nabyłaś / nabyłeś, jest dziełem twórcy i wydawcy. Prosimy, abyś przestrzegała / 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

SPIS TREŚCI

I Podstawy lokalnych sieci komputerowych

1 Podstawowe zagadnienia dotyczące sieci komputerowych 8
2 Zasady bezpieczeństwa w sieci 11
3 Jednostki miar w sieciach komputerowych 14
4 Rodzaje i charakterystyka medium transmisyjnego 17
5 Rodzaje, budowa i funkcje urządzeń sieciowych 20
6 Symbole graficzne urządzeń sieciowych 23
7 Dokumentacja techniczna urządzeń sieciowych 25
8 Topologie sieciowe (logiczna i fizyczna) 27
9 Metody dostępu do nośnika 31
10 Rodzaje środowisk sieciowych (klient–serwer i peer-to-peer) 34
11 Komunikacja w sieci 35
12 Modele warstwowe sieci 39
12.1. Model sieci ISO/OSI 39
12.2. Przepływ danych między warstwami 41
12.3. Stos protokołów TCP/IP 42
13 Protokoły warstwy łącza danych 46
13.1. Standard Ethernet 46
13.2. Domeny kolizyjne i rozgłoszeniowe 48
14 Protokoły warstwy sieci 52
14.1. Protokół IP 52
14.2. Protokoły routingu 53
14.3. Rozsyłanie grupowe informacji 55
14.4. Protokół ICMP 56
15 Adresowanie w sieci komputerowej. 58
15.1. Adresy fizyczne 58
15.2. Adresy logiczne 59
15.3. Adresy IPv4 59
15.4. Klasy adresów IP 61
15.5. Translacja i przydzielanie adresów 62
15.6. Zapobieganie wyczerpywaniu się puli adresów 63
15.7. Adresowanie bezklasowe 63
16 Zasady projektowania adresacji IP 69
17 Adresowanie IPv6 72
18 Protokoły warstwy transportowej 77
19 Protokoły warstwy aplikacji 79
20 Inne zestawy protokołów sieciowych 82

II Projektowanie lokalnych sieci komputerowych

21 Komputerowe systemy sieciowe 84
22 Zasady projektowania lokalnej sieci 86
23 Rodzaje materiałów i urządzeń do budowy sieci 89
24 Zasady doboru materiałów i urządzeń sieciowych 91
25 Struktura dokumentacji projektowej 93
26 Projektowanie okablowania strukturalnego 95
27 Zasady sporządzania harmonogramu prac wykonawczych 98

28 Zasady kosztorysowania prac ... 100
29 Normy, KNR, katalogi sprzętu sieciowego, cenniki ... 102
30 Czytanie rzutów poziomych i pionowych budynków ... 105
31 Obsługa przykładowych programów wspomagających projektowanie 2D ... 108
32 Obsługa przykładowych programów do kosztorysowania ... 113

III Projektowanie i montaż okablowania

33 Normy i zalecenia dotyczące montażu okablowania strukturalnego ... 120
33.1. Zalecenia dotyczące kabli w przebiegach poziomych ... 121
33.2. Wymagania instalacyjne dla przebiegów pionowych ... 122
33.3. Pozostałe wymagania instalacyjne ... 122
34 Funkcje urządzeń sieciowych ... 123
35 Symbole graficzne dotyczące lokalnych sieci komputerowych ... 125
36 Zasady bezpiecznej i higienicznej pracy podczas montażu ... 128
37 Zasady organizacji pracy i analizy harmonogramów prac ... 130
38 Narzędzia do montażu okablowania strukturalnego ... 132
39 Metody i zasady pomiarów okablowania strukturalnego ... 135
40 Metody pomiarów sieci logicznej ... 138
41 Rodzaje testów i pomiarów pasywnych ... 140
42 Rodzaje testów i pomiarów aktywnych ... 144
43 Cenniki materiałów do montażu okablowania ... 148

IV Modernizacja i rekonfiguracja lokalnych sieci komputerowych

44 Zasady modernizacji lokalnej sieci komputerowej ... 154
45 Zasady kosztorysowania prac modernizacyjnych ... 156
46 Przykładowe zadania projektowe do samodzielnego wykonania ... 159

V Konfiguracja i obsługa lokalnych sieci komputerowych

47 Metody dostępu do sieci ... 164
48 Uzyskiwanie dostępu do sieci internet ... 167
49 Symulatory programów konfiguracyjnych urządzeń sieciowych ... 172
50 Konfigurowanie urządzeń sieciowych ... 176
50.1. Routing statyczny i dynamiczny ... 182
51 Konfigurowanie urządzeń sieci bezprzewodowych ... 195
51.1. Uwierzytelnianie klientów Wi-Fi za pomocą serwera RADIUS ... 204
51.2. Sieci Wi-Fi zarządzane przez kontroler sieci ... 209
51.3. Anteny ... 217
52 Funkcje przełączników zarządzalnych ... 220
53 Wirtualne sieci lokalne ... 236
53.1. Wirtualna sieć lokalna ... 236
53.2. Routing między wirtualnymi sieciami lokalnymi ... 244
54 Zasady modernizacji sieci wirtualnych ... 255
55 Korzystanie z wirtualnych sieci prywatnych ... 260
56 Rodzaje i sposób obsługi urządzeń telefonii internetowej ... 277
56.1. Konfigurowanie usługi VoIP w sieci lokalnej ... 282
56.2. Konfigurowanie telefonów VoIP i protokołu SIP ... 289
57 Programy do administrowania lokalnymi sieciami komputerowymi ... 292
58 Zdalne zarządzanie stacjami roboczymi ... 298
59 Zasady aktualizowania oprogramowania urządzeń sieciowych ... 304

60 Gwarantowanie jakości usług QoS 311
61 Konfiguracja sprzętowej zapory sieciowej 318

VI Diagnostyka i naprawa lokalnych sieci komputerowych

62 Urządzenia pomiarowe i diagnostyczne 330
63 Oprogramowanie monitorujące lokalne sieci 335
63.1. Monitorowanie danych przesyłanych przez przełącznik sieciowy 340
64 Rodzaje awarii sieciowych i ich przyczyny 346
65 Procedury serwisowe dotyczące urządzeń sieciowych 349
66 Sposoby naprawy okablowania strukturalnego 353

VII Korzystanie z wybranych usług oferowanych przez sieciowe systemy operacyjne

67 Współpraca systemu Windows z serwerem sieci lokalnej 356
68 Typy sieci komputerowych 357
69 Korzystanie z usług sieciowych – serwis stron WWW 360
70 Korzystanie z usługi transferu plików 362
71 Korzystanie z usług poczty elektronicznej 368
72 Korzystanie z usługi telnet 371
73 Korzystanie z usługi bezpiecznego terminala 373
74 Korzystanie z usługi bezpiecznego kopiowania plików 375
75 Sieć peer-to-peer, grupy robocze, udostępnianie folderów w grupie roboczej 378

Wykaz podstawowych pojęć w języku angielskim i niemieckim 384

- Podstawowe pojęcia dotyczące sieci komputerowych
- Zasady bezpieczeństwa w sieci
- Jednostki miar w sieciach komputerowych
- Rodzaje i 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 (klient–serwer i peer-to-peer)
- 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

Podstawy lokalnych sieci komputerowych

I

1 Podstawowe zagadnienia dotyczące sieci komputerowych

ZAGADNIENIA

Elementy składowe sieci komputerowej **Cel budowy sieci komputerowych** **Rodzaje adresów sieciowych** **Podział sieci ze względu na obszar ich działania** **Podział sieci ze względu na architekturę**

We współczesnym świecie komunikacja pełni ważną funkcję w przekazywaniu informacji. Komunikujemy się z innymi bezpośrednio za pomocą np. głosu, znaków i 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** (ang. *Computer network*) to system komunikacyjny służący do przesyłania danych, łączący co najmniej dwa komputery lub inne urządzenia komputerowe bądź peryferyjne.

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

- **sieci osobiste** PAN (ang. *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 (ang. *Local Area Network*) – sieci łączące użytkowników na niewielkim obszarze (pomieszczenie, budynek). W sieciach LAN prędkość przesyłania danych jest duża i korzysta się z samodzielnie zarządzanych łączy. Przykładem sieci lokalnej może być sieć szkolna;
- **sieci miejskie** MAN (ang. *Metropolitan Area Network*) – sieci o zasięgu miasta, najczęściej szybkie. Umożliwiają połączenia między sieciami lokalnymi uczelni, ośrodków naukowych, organów administracji i centrów przemysłowych w aglomeracji miejskiej;
- **sieci rozległe** WAN (ang. *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.

Zależnie od sposobu pracy w sieci (tzw. architektury) rozróżnia się następujące rodzaje sieci:

- **peer-to-peer** – w której wszystkie systemy komputerowe są równoprawne;
- **klient–serwer** – w której jeden z systemów komputerowych odgrywa rolę nadrzędną (tzw. serwer).

Sieci komputerowe umożliwiają m.in.:

- współużytkowanie programów i plików;
- współużytkowanie innych zasobów, takich jak: drukarki, plotery, pamięci masowe, dostęp do internetu;

- 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 i programowe. Do elementów sprzętowych sieci zalicza się:

- **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** – odpowiedzialne za formatowanie danych w taki sposób, aby nadawały się one do przesyłania w sieci. Odpowiadają także za umieszczanie danych w sieci i ich odbieranie. W sieci lokalnej urządzeniami dostępu są karty sieciowe. W sieciach rozległych urządzeniami dostępu są modemy;
- **urządzenia wzmacniania przesłanych sygnałów** – urządzenia odbierające przesyłane sygnały, wzmacniające je i wysyłające z powrotem do sieci. W sieciach lokalnych tę funkcję pełni koncentrator, umożliwiający ponadto przyłączanie do sieci wielu urządzeń.

Składnikami programowymi sieci są:

- **protokoły** (ang. *protocols*) – określają sposoby komunikowania się urządzeń; przykładem protokołu może być IP;
- **sterowniki urządzeń** (ang. *drivers*) – programy umożliwiające działanie urządzeniom, np. kartom sieciowym;
- **oprogramowanie komunikacyjne** (ang. *communication software*) – korzysta z protokołów i sterowników do wymiany danych. Są to np. programy do udostępniania zasobów, programy przesyłania plików, programy do obsługi poczty elektronicznej, przeglądarki internetowe.

Dane w sieci są przesyłane między nadawcą a odbiorcą przez **łącza komunikacyjne** (ang. *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** (ang. *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** (ang. *switches*), a w sieciach rozległych stosuje się **routery** (ang. *routers*).

W sieci istnieje wiele komputerów, których zadaniem jest świadczenie pewnych usług innym urządzeniom w sieci, np. udostępnianie plików, drukarek lub innych zasobów. Taki komputer nazywa się **serwerem** (ang. *server*), a urządzenie korzystające z tych usług – **klientem** (ang. *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 i wydajne procesory.

Profesjonalne urządzenia sieciowe, takie jak przełączniki, routery, serwery, są przystosowane do montażu w specjalnych szafach dystrybucyjnych typu **RACK**. Standardowa szerokość urządzeń wynosi 19" (19 cali, 482 mm). Wysokość urządzeń określa się 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 1 U). 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.



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

Aby dane mogły niezawodnie przemieszczać się między poszczególnymi punktami sieci, każdy z takich punktów musi być jednoznacznie oznaczony. Każde urządzenie pracujące w sieci i każdy komputer mają przypisane identyfikatory, które jednoznacznie identyfikują je w sieci. Taki identyfikator nazywa się **adresem sieciowym** (ang. *network address*). W sieciach stosuje się różne systemy adresowania, np. w internecie obowiązują adresy IP, a w sieciach Ethernet każde urządzenie ma unikatowy adres fizyczny (MAC).

Przed przesłaniem danych przez sieć dzieli się je na mniejsze części, np. ramki lub pakiety, które łatwiej przesyłać. Każda z tych części jest zaopatrzona w adres miejsca źródłowego i docelowego, dzięki czemu można określić, kto jest nadawcą i adresatem danych. Mogą one przemieszczać się w sieci niezależnie od innych.

SPRAWDŹ SWOJĄ WIEDZĘ

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

2 Zasady bezpieczeństwa w sieci

ZAGADNIENIA

- **Najczęściej używane usługi internetu**
- **Netykieta**
- **Wady korzystania z internetu**
- **Zasady bezpiecznego korzystania z internetu**

Internet jako sieć komputerowa obejmuje zasięgiem cały świat. Cieszy się tak dużą popularnością, że wiele osób nie potrafi sobie wyobrazić bez niego życia. Służy do różnych celów, np. do pracy, nauki i rozrywki, a używają go zarówno osoby młode, jak i starsze. Internet nie jest ani dobry, ani zły. To od jego użytkowników zależy, czy będzie bezpieczny. O bezpieczeństwo w internecie należy dbać tak, jak o bezpieczeństwo w świecie realnym. Internet oferuje wiele usług, dostępnych dla każdego użytkownika. Najczęściej używa się:

- **wyszukiwarek internetowych** – umożliwiają przeszukiwanie sieci i zwracają wyniki poszukiwania w postaci listy stron zawierających wyszukiwane słowa lub ciągi znaków. Do najbardziej popularnych wyszukiwarek należą: Google, Yahoo, Bing i standardowe wyszukiwarki portali internetowych, takich jak WP, Interia, Onet;
- **komunikatorów i czatów** – pozwalają na prowadzenie rozmów z ludźmi na całym świecie. Do najpopularniejszych należą Messenger i Skype;
- **rozwiązania ukierunkowane na rozrywkę** – wiele portali rozrywkowych umożliwia swoim klientom gry w sieci, oglądanie zdjęć, czytanie wiadomości i książek, uczestnictwo w konkursach i wiele innych form spędzania czasu w sieci;
- **innych usług** – pozwalają wykonywać wiele czynności, które wcześniej były realizowane w świecie realnym, np. zakupy w sklepach i na aukcjach internetowych oraz usługi bankowe, umożliwiające opłacanie rachunków, wykonywanie przelewów, sprawdzanie salda itp.

Podobnie jak w życiu realnym, również w internecie obowiązują zasady dobrego zachowania. Nazywa się je **netykietą**. Jest to opis form przyzwoitego zachowania się w internecie. Wynikają one z ogólnych zasad przyzwoitości lub są odzwierciedleniem reguł niemożliwych do opisania w standardach ograniczeń technicznych.

Najważniejsze zalecenia netykiety:

- zakaz używania wulgaryzmów;
- zakaz spamowania (m.in. wysyłania niechcianych wiadomości lub linków do stron) i wysyłania tzw. łańcuszków szczęścia;
- zakaz wysyłania e-maili do wielu osób naraz z jawnymi adresami poczty elektronicznej;
- zakaz pisania nie na temat;
- zakaz floodowania, czyli wysyłania tej samej wiadomości lub wielu różnych wiadomości w bardzo krótkich odstępach;
- zakaz nagabywania osób, które sobie tego nie życzą;
- nakaz przestrzegania zasad dotyczących znaków diakrytycznych – użytkownicy niektórych kanałów IRC nie życzą sobie używania polskich liter, natomiast na forach internetowych pisanie bez polskich znaków diakrytycznych bywa źle widziane;

- zakaz ciągłego pisania wielkimi literami;
- zakaz pisania naprzemiennie wielkich i małych liter;
- nakaz używania emotikon z rozwagą: mają być dodatkiem do tekstu, a nie – główną treścią;
- w dyskusjach, np. na forach internetowych, zalecenie zwracania się do użytkowników z użyciem ich pseudonimu (nicka) lub imienia – jeśli rozmówca wyraża na to zgodę (najczęściej zwracamy się do siebie „per ty", zamiast w formie grzecznościowej, choć nie należy się również obawiać używania takiej formy).

Oprócz zalet, korzystanie z internetu ma również pewne wady, na które szczególnie są narażone osoby młode. Do najczęściej wymienianych wad i zagrożeń internetu należą:

- **anonimowość** – może być zaletą, ale również okazać się zagrożeniem. Wbrew powszechnemu mniemaniu użytkownik w internecie nie jest całkowicie anonimowy i w pewnych okolicznościach może być poddany kontroli społecznej lub zidentyfikowany, np. przez służby do tego uprawnione;
- **wirusy i inne rodzaje niechcianego oprogramowania** – wirusy komputerowe umieszcza się na wielu stronach WWW, w wiadomościach e-mail i w plikach pobieranych z sieci. Najlepszą ochroną przed nimi jest skuteczny i regularnie aktualizowany program antywirusowy lub program typu „internet security", zawierający oprócz antywirusowego również inne moduły, np. firewall (blokujący dostęp do komputera), moduły ochrony rodzicielskiej;
- **spam** – wiadomości, oferty i reklamy rozsyłane bez wiedzy i zgody użytkownika za pomocą poczty elektronicznej lub wyświetlane przez strony internetowe. Aby się zabezpieczyć przed spamem, można używać filtrów antyspamowych;
- **wyłudzenia** – wtedy, gdy po zamówieniu i opłaceniu produktu z serwisu aukcyjnego przesyłka z zamówionym towarem nie dociera pod wskazany adres lub zawiera towar niezgodny z opisem. Aby zabezpieczyć się przed zawarciem feralnej transakcji, należy przeczytać komentarze innych użytkowników na temat danego sprzedawcy lub wybrać formę płatności przy odbiorze;
- **uzależnienie** – zbyt częste korzystanie z internetu może skutkować izolowaniem się użytkowników od społeczności i utrudniać kontakty w życiu realnym. Uzależnienie od internetu może zarówno mieć negatywne skutki mentalne, jak i powodować schorzenia, takie jak: fobie społeczne (lęk przed kontaktem z ludźmi w realnym świecie, strach przed opuszczeniem mieszkania), wady wzroku i postawy, ograniczoną sprawność fizyczną, a także bezsenność, nerwicę i depresję;
- **piractwo komputerowe** – przestępstwo komputerowe przeciwko mieniu polegające na nielegalnym nabywaniu bądź rozpowszechnianiu materiałów chronionych prawem autorskim z pomocą technologii komputerowych, np. obrót nielegalnym oprogramowaniem bądź materiałami multimedialnymi, zwłaszcza muzyką i filmami. Sankcjami karnymi są zagrożone również nabywanie programów komputerowych bez umowy licencyjnej i ich instalowanie na swoim komputerze, pobieranie z internetu treści objętych prawami autorskimi w celu uzyskania korzyści majątkowych;
- **szkodliwe treści** – możliwość dostępu do treści np. dotyczących przemocy, narkotyków, rasizmu;
- **wirtualna prostytucja** (np. webkamerki) – użytkownicy mogą być mimowolnym odbiorcą treści pornograficznych, np. filmów i zdjęć pornograficznych;
- **utrata prywatności** – usługi i strony w sieci mogą zbierać i gromadzić informacje dotyczące użytkowników korzystających z sieci i ich preferencji lub zainteresowań. Informacje w założeniu mające służyć lepszej obsłudze klienta mogą zostać wykorzystane w sposób niezgodny z planowanym przeznaczeniem i narazić go na nieprzyjemności, ujawnienie danych osobowych, a w konsekwencji – również na straty materialne;

- **cyberprzemoc** – przemoc z użyciem technologii informacyjnych i komunikacyjnych. Użytkownicy mogą paść ofiarą agresji online ze strony innych użytkowników, np. stalkingu, nękania.

Aby ograniczyć możliwość negatywnych konsekwencji, które mogą spotkać użytkowników sieci, należy przestrzegać zasad bezpiecznego korzystania z internetu:

1. Nie podawać swoich prywatnych danych osobom poznanym w sieci. Nie udostępniać swoich prywatnych danych nieznanym osobom.
2. Nie spotykać się z osobami poznanymi przez internet.
3. Nigdy nie podawać komuś swojego hasła.
4. Wymyślić swój internetowy pseudonim (nick) i używać go w portalach społecznościowych. Nie ujawniać w nim daty urodzenia ani wieku, np. jan2005 czy ania16.
5. Nie wierzyć we wszystkie informacje przeczytane w sieci.
6. Nigdy nie używać webkamery podczas rozmowy z nieznaną osobą.
7. Nigdy nie wysyłać nieznajomym swoich zdjęć.
8. Nie dokuczać innym.
9. Nie odpowiadać na zaczepki w sieci.
10. Nie spędzać zbyt dużo czasu przy komputerze. Zbyt długie korzystanie z komputera szkodzi zdrowiu i może być przyczyną wielu innych problemów.
11. Używać programów antywirusowych i antyspamowych.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Skorzystaj z dowolnego źródła w internecie i odszukaj, co to są dane osobowe wrażliwe. Informacje zapisz w zeszycie przedmiotowym.
2. Skorzystaj z dowolnego źródła w internecie i odszukaj nazwy co najmniej pięciu programów antywirusowych i antyspamowych. Informacje zapisz w zeszycie przedmiotowym.
3. Wybierz internetowy pseudonim (nick), którego będziesz używać w portalach społecznościowych.

3 Jednostki miar w sieciach komputerowych

ZAGADNIENIA

Jednostki używane do wyrażenia zmian względnych wielkości fizycznych **Sposób wyrażania wartości szumów w telekomunikacji** **Jednostki przesyłania danych** **Obliczanie czasu potrzebnego do przesłania 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** powszechnie przyjęto w informatyce i stosuje się go również do określania parametrów transmisji danych. Ilość pamięci potrzebna do zapisania jednej z tych wartości jest podstawową jednostką i nazywa się **bitem** (ang. *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 przesyła się kolejno) jest bit na sekundę. Ta jednostka 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). Liczbę symboli przesyłanych w ciągu jednej sekundy mierzy się w jednostkach nazywanych **bodami** (ang. *baud*). Przykładowo: 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 przesyła się 300 bitów.

W marynarce przed wprowadzeniem łączności radiowej wykorzystywano do komunikacji alfabet semaforowy, w którym sygnalista za pomocą pozycji rąk przekazywał informacje. Pojedyncza flaga sygnalizacyjna mogła być umieszczona w jednej z ośmiu pozycji: podniesiona w górę, w lewo w górę (pod stałym kątem 45 stopni), w lewo, w lewo w dół, w dół, w prawo w dół, w prawo i w prawo w górę. W systemie dwójkowym taka informacja byłaby zapisana na 3 bitach (osiem różnych wartości). Jeżeli sygnalista zmieniałby położenie ręki 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 liczbę bitów) przy niezmienionej liczbie przesłanych symboli.

Gdy u **dostawcy usług internetowych** (ang. *Internet Service Provider*, ISP) zamawia się 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 i 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 takie łącza mogą odbierać i wysyłać mniej danych. Jest to jednak ograniczenie techniczne, wprowadzone przez dostawcę w celu zróżnicowania oferty.

Sieciom lokalnym zbudowanym w standardzie Ethernet odpowiadają różne prędkości przesyłania danych. Pierwsze wersje Ethernetu zbudowanego z wykorzystaniem łączy kablowych oferowały prędkość do 10 Mb/s. Później wprowadzono Fast Ethernet o prędkości 100 Mb/s. Obecnie najczęściej stosuje się standard Gigabit Ethernet, a do wysoko wydajnych sieci wprowadza się prędkość 10 Gigabit Ethernet lub 40 Gigabit Ethernet.

Ponieważ wielkość plików zwykle podaje się w bajtach, należy uwzględnić różnice w jednostkach. Aby obliczyć prędkość pobierania plików, których rozmiar podano w bajtach, prędkość przesyłania należy podzielić przez 8 (zamienić bajty na bity, oznaczane literą B: 1 bajt to 8 bitów, a zatem 1 B = 8 b), czyli transfer 256 kb/s jest równoznaczny pobieraniu 32 kB/s.

Tabela 3.1. Jednostki szybkości transmisji danych

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

Wyniki testowania sieci, np. światłowodowych lub bezprzewodowych, można podawać w decybelach. **Decybeli** (dB) używa się 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 *Pk* dostarczonej do odbiornika do mocy *Pp* 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** (ang. *signal-to-noise ratio*, SNR). **Szum** to niepożądany sygnał pochodzący ze źródeł naturalnych, np. wyładowań elektrycznych w czasie burzy, lub sztucznych, np. przewodów energetycznych lub urządzeń elektrycznych. 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.

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 całą przepustowość wykorzystano do transmisji pliku (bez dodatkowego narzutu związanego z transmisją).
2. Oblicz, ile danych możesz pobrać z internetu w czasie dwóch godzin przy założeniu, że przepustowość łącza jest stała i wynosi 60 Mb/s.
3. Ile czasu potrzeba do pobrania pliku wielkości 1 GB przy założeniu, że przepustowość łącza jest stała i wynosi 10 Mb/s?
4. W jakim czasie prześlemy plik o wielkości 100 MB przez łącze 8 Mb/s?
5. Oblicz (w Mb/s), jaka jest przepustowość łącza, jeśli w ciągu 3 godzin można pobrać 30 GB danych.
6. Co będzie przesłane szybciej: zawartość CD (rozmiar 700 MB) przez sieć Fast Ethernet czy zawartość DVD (4,7 GB) przez sieć Gigabit Ethernet? Zapisz obliczenia, aby uzasadnić odpowiedź. Przyjmij, że cała przepustowość jest wykorzystana do transmisji danych (bez dodatkowego narzutu związanego z transmisją). Wyniki i wnioski z obliczeń przekaż nauczycielowi do sprawdzenia.

4 Rodzaje i charakterystyka medium transmisyjnego

ZAGADNIENIA

Funkcje mediów transmisyjnych **Media wykorzystywane do budowy sieci komputerowych** **Dobór medium transmisyjnego w sieci**

Aby wymieniać informacje, urządzenia sieciowe 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 do budowy sieci lokalnych jest **skrętka**. Składa się ona z czterech par przewodów umieszczonych we wspólnej osłonie. Aby zmniejszyć oddziaływanie elektromagnetyczne przewodów na siebie, wspólnie się je skręca. Najpopularniejsze typy skrętki to:

- **nieekranowana** UTP (ang. *Unshielded Twisted Pair*) – stosowana w większości sieci;
- **ekranowana** STP (ang. *Shielded Twisted Pair*) – wyposażona w specjalną warstwę (ekran) chroniącą przed wpływem zakłóceń elektromagnetycznych;
- **ekranowana** FTP (ang. *Foiled Twisted Pair*) – skrętka ekranowana za pomocą folii z przewodem uziemiającym, przeznaczona głównie do budowy sieci komputerowych w miejscach o dużych zakłóceniach elektromagnetycznych; w sieciach Gigabit Ethernet stosowana przy użyciu wszystkich czterech par przewodów.

  Odmiany skrętki ekranowanej różnią się sposobem wykonania ekranu.

Skrętkę wykorzystuje się w telekomunikacji do przesyłania danych zarówno w postaci analogowej, jak i cyfrowej. Przydatność skrętki do transmisji danych określa się za pomocą kategorii. Odpowiednie do budowy sieci są:

- 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;
- kategoria 8 (CAT 8) – stosowana wyłącznie do centrów danych, w których odległości między routerami a serwerami są zazwyczaj krótkie; rozwiązanie umożliwiające niezwykle szybką transmisję danych bez konieczności użycia kabli światłowodowych.

W budowie lokalnych sieci komputerowych wykorzystuje się następujące rodzaje skrętki komputerowej:

- **U/UTP** – skrętka nieekranowana;
- **F/UTP** – skrętka foliowana;

- **U/FTP** – skrętka z każdą parą przewodów w osobnym ekranie z folii;
- **F/FTP** – skrętka z każdą parą przewodów w osobnym ekranie z folii i dodatkowo w ekranie z folii;
- **SF/UTP** – skrętka ekranowana folią i siatką;
- **S/FTP** – skrętka z każdą parą przewodów foliowaną dodatkowo w ekranie z siatki;
- **SF/FTP** – skrętka z każdą parą przewodów foliowaną dodatkowo w ekranie z folii i siatki.

Większość nowych sieci komputerowych wykonuje się z wykorzystaniem skrętki kategorii 5e lub wyższych. Maksymalna długość połączeń wykonanych za pomocą skrętki, zapewniających standardowe parametry transmisji, wynosi 100 m. Skrętkę przyłącza się do karty sieciowej za pomocą złącza RJ-45[1]. W starszych sieciach jako medium transmisyjne wykorzystywano **kabel koncentryczny** (ang. *coaxial cable*), zbudowany z miedzianego rdzenia umieszczonego w osi kabla i otoczonego izolatorem oraz ekranem. Maksymalna prędkość transmisji przesyłanych nim danych wynosiła 10 Mb/s. Istnieją dwa rodzaje kabla koncentrycznego:

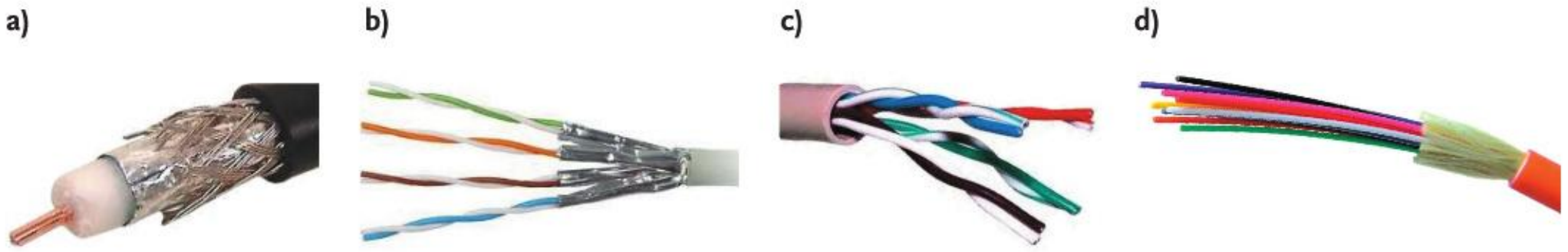
- **gruby ethernet** – o średnicy ok. 1 cm, pozwalający transmitować dane na maksymalną odległość 500 m;
- **cienki ethernet** – o średnicy ok. 0,5 cm, pozwalający transmitować dane na maksymalną odległość 185 m.

Najnowocześniejszym nośnikiem transmisji przewodowej jest światłowód (ang. *fiber optic cable*). Rdzeń światłowodu, wykonany ze szkła kwarcowego lub specjalnego tworzywa sztucznego, jest okryty płaszczem i warstwą ochronną. Transmisja polega na przesyłaniu przez rdzeń światłowodu wiązki światła, generowanej przez diodę lub laser. Dane koduje się w postaci impulsów światła. Do transmisji danych używa się pary przewodów, z których jeden służy do wysyłania danych, a drugi – do ich odbierania. W nowszych rozwiązaniach jest możliwe przesyłanie danych w obu kierunkach jednocześnie przez pojedyncze włókno, pod warunkiem używania różnych długości fali świetlnej dla każdego kierunku transmisji. Ze względu na wysoką cenę, duże prędkości przesyłania danych i zasięg światłowody najczęściej stosuje się 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 wykorzystuje się fale elektromagnetyczne. Najczęściej używa się:

- **fali elektromagnetycznych w zakresie podczerwieni IR** (ang. *infrared*) – jako źródła światła wykorzystuje się diody LED lub diody laserowe. Zasięg i prędkość transmisji są niewielkie, stosowane do przyłączania, np. klawiatury lub myszy;
- **fali radiowych** – 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 standardy oznaczone 802.11a, 802.11b, 802.11g, 802.11n i 802.1ac, zapewniające różne prędkości transmisji. Najbardziej popularnym standardem jest 802.11n, zapewniający prędkość transmisji do 600 Mb/s. Fale radiowe wykorzystuje się również w innych typach łączności bezprzewodowej, np. w technologii Bluetooth, sieci 802.16 WiMAX lub w telefonii komórkowej 5G-UMTS/4G-LTE.

[1] Terminu RJ-45 używa się powszechnie, mimo że właściwa nazwa to 8P8C.



Rys. 4.1. **Przykłady mediów transmisyjnych: a) kabel koncentryczny, b) skrętka ekranowana, c) skrętka nieekranowana, d) kabel światłowodowy**

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jakich mediów transmisyjnych używa się w twojej szkole?
2. Jakie medium zapewnia najwyższe bezpieczeństwo przesyłanych danych i dlaczego?
3. Przerysuj poniższą tabelę do zeszytu przedmiotowego, a następnie zapisz w niej zalety i wady wymienionych mediów transmisyjnych.

Rodzaj medium transmisyjnego	Zalety	Wady
Kabel koncentryczny gruby		
Skrętka nieekranowana		
Światłowód wielomodowy		

4. Przepisz zdania do zeszytu przedmiotowego i je uzupełnij:
   - Do montażu kabla sieciowego w pomieszczeniach z dużą liczbą rogów, ścian działowych i załamań najlepiej nadaje się skrętka o przewodach miedziowych w postaci .....
   - Na potrzeby sieci bezprzewodowych w standardzie 802.11 najczęściej wykorzystuje się częstotliwości ..... i .....
   - UTP określa skrętkę .....
   - Najczęściej wykorzystywaną kategorią skrętki jest .....
   - Na końcach kabla koncentrycznego należy instalować .....

5 Rodzaje, budowa i funkcje urządzeń sieciowych

ZAGADNIENIA

Urządzenia stosowane do budowy sieci komputerowych **Rola urządzeń sieciowych w przesyłaniu danych**

Sieci komputerowe zbudowano, aby wymieniać dane między komputerami. Wymianę zapewnia zastosowanie odpowiedniego sprzętu i 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 (ang. *MOdulator DEModulator*) to urządzenie, które zamienia cyfrowe dane, generowane przez komputer, na sygnały analogowe i wysyła je za pomocą sieci telefonicznej. Podczas odbierania danych z sieci sygnały analogowe zamienia się na cyfrowe i przekazuje do komputera. Modem może być wykorzystywany do połączenia komputera lub sieci LAN z internetem za pośrednictwem stacjonarnej linii telefonicznej lub do przesyłania danych między sieciami LAN. Zaletą modemu jest powszechna dostępność tej usługi. Modemy stosuje się również w sieciach telewizji kablowej i telefonii komórkowej (np. modemy 3G/4G).

Karta sieciowa to urządzenie łączące komputer z lokalną siecią komputerową. Głównym zadaniem karty sieciowej jest przekształcanie ramek danych w sygnały, które przesyła się w sieci komputerowej. Karta sieciowa w standardzie **Ethernet** (najczęściej spotykanym) ma unikatowy w skali światowej **adres fizyczny MAC** (ang. *MAC address*), przyporządkowany jej podczas produkcji i zapisany w pamięci ROM. Karty mogą pracować z różnymi prędkościami. Standardem w przypadku sieci przewodowych są karty sieciowe pracujące z prędkością 100 Mb/s lub 1 Gb/s. W bezprzewodowych kartach sieciowych wykorzystuje się do przesyłania danych 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 (ang. *repeater*), zwany również regeneratorem, to urządzenie wykorzystywane w miejscach wymagających wzmocnienia lub regeneracji sygnału, ponieważ okazuje się to niezbędne do zwiększenia zasięgu sieci. Rzadko jest to samodzielne urządzenie. Najczęściej funkcję wzmacniaka pełni urządzenie sieciowe mające własne zasilanie w energię elektryczną, np. koncentrator.

Koncentrator (ang. *hub*) to urządzenie wyposażone w 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 (ang. *bridge*) to urządzenie z dwoma portami, służącymi 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 (ang. *switch*) oferuje te same funkcje co koncentrator, a dodatkowo pozwala, podobnie jak most, podzielić sieć na segmenty. Urządzenie ma 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 siecią i jej monitoringu.

Punkt dostępowy (ang. *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 przyłącza się laptopy, palmtopy, smartfony i 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 (ang. *gateway*) to urządzenie, za którego pośrednictwem komputery z sieci lokalnej komunikują się z komputerami w innych sieciach. W sieci TCP/IP domyślna brama oznacza router, do którego komputery z sieci lokalnej mają wysyłać pakiety adresowane do innej sieci, np. do internetu. Niektóre bramy umożliwiają komunikację między sieciami, w których działają różne protokoły.

Bramka VoIP (ang. *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 i sygnały wybierania numeru telefonicznego na sygnały VoIP.

Zapora sieciowa (ang. *firewall*) to 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 odgrywać 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 przedstawiono na rys. 5.1.

a)



b)



c)



d)



Rys. 5.1. Przykłady urządzeń sieciowych: a) modem, b) karta sieciowa, c) router z punktem dostępowym, d) bramka VoIP

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jakie urządzenia sieciowe wykorzystuje się w twojej szkole?
2. W których miejscach w twojej szkole znajdują się poszczególne urządzenia sieciowe?
3. Jakie urządzenia sieciowe wykorzystujesz w domu?
4. Poniżej przedstawiono krótką charakterystykę trzech urządzeń sieciowych. Na tej podstawie podaj nazwę każdego z nich.
   a) To urządzenie pozwala na nawiązanie połączenia z internetem przez port ADSL lub port Ethernet WAN, dzięki czemu umożliwia użytkownikom korzystanie z łącza ADSL lub modemu kablowego.
   b) To urządzenie umożliwia podłączenie komputera do sieci za pośrednictwem fal radiowych. Dzięki temu można wygodnie wymieniać się plikami lub korzystać z dostępu do internetu w dowolnym miejscu. Ma popularny interfejs USB, co pozwala na podłączenie go do komputera stacjonarnego lub laptopa.
   c) To urządzenie pozwala na rozszerzenie istniejącej sieci bezprzewodowej. Działa ze wszystkimi routerami Wi-Fi i umożliwia stworzenie dwupasmowej sieci pokrywającej obszar kilku pomieszczeń lub nawet budynku. Niektóre modele mają dodatkowo port RJ-45 do podłączenia innych urządzeń sieciowych.
4. Na urządzeniach sieciowych i zewnętrznych urządzeniach peryferyjnych często występuje przycisk o nazwie WPS. Opisz funkcję, zasadę działania oraz zalety i wady technologii WPS.

6 Symbole graficzne urządzeń sieciowych

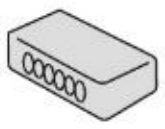
ZAGADNIENIA

Symbole urządzeń i łączy stosowane w schematach sieci **Programy wykorzystywane do rysowania schematów sieci**

Sieć komputerowa może składać się z dwóch komputerów połączonych kablem. Natomiast sieć internetowa 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. U nas schematy będą najczęściej dotyczyć budowy sieci lokalnej, np. w szkole lub w pracowni.

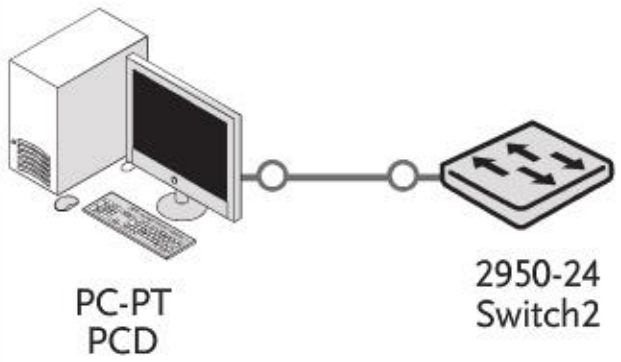
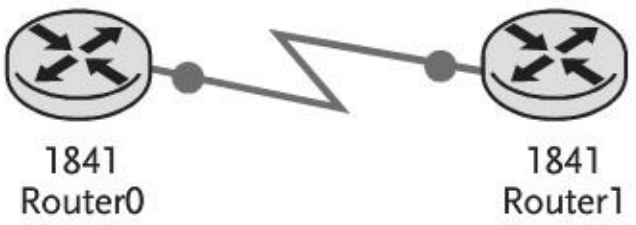
Do sporządzania schematów sieci można wykorzystać wiele programów, np. Microsoft Visio (program komercyjny) lub bezpłatny program Dia (dostępny na stronie https://wiki.gnome.org/Apps/Dia w wersji dla systemów Linux i Windows). We wcześniejszym rozdziale omówiono wybrane urządzenia stosowane do budowy sieci. Każdemu z tych urządzeń przypisano symbol graficzny, za którego pomocą jest on reprezentowany w schematach. Wybrane symbole urządzeń używane w schematach zebrano w tabeli 6.1.

Tabela 6.1. Symbole graficzne wybranych urządzeń używane w schematach

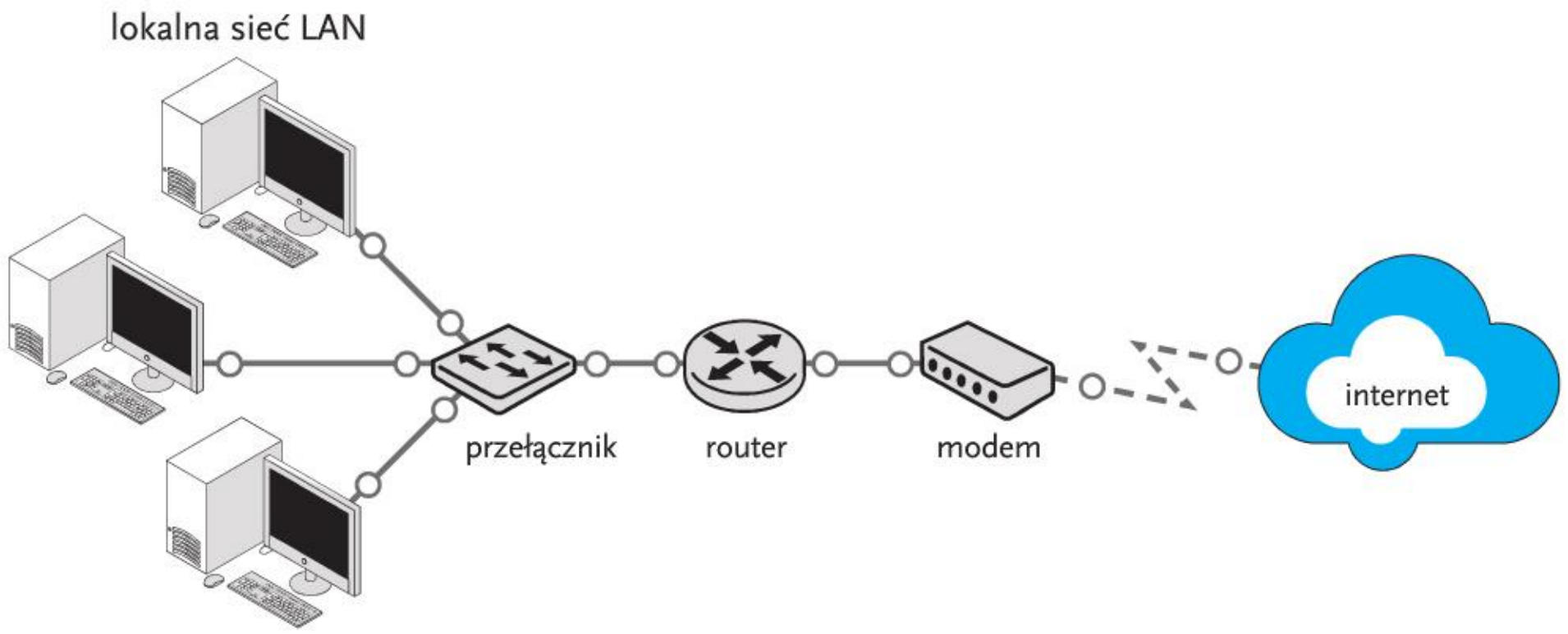
Symbol	Znaczenie	Symbol	Znaczenie
	modem		punkt dostępowy
	koncentrator		router
	most		stacja robocza
	przełącznik		zapora sieciowa

Połączenia między urządzeniami mogą być wykonywane za pomocą różnych typów łączy. Wybrane symbole łączy używane w schematach zebrano w tabeli 6.2.

Tabela 6.2. Symbole graficzne łączy używane w schematach

Symbol	Znaczenie	Symbol	Znaczenie
	kabel ethernetowy prosty		kabel szeregowy
	kabel ethernetowy krosowany		kabel światłowodowy

Przykładowy schemat prostej sieci przedstawiono na rys. 6.1.



Rys. 6.1. Schemat prostej sieci

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Za pomocą dowolnego programu narysuj schemat sieci komputerowej w twojej szkole.
2. Na rys. 6.1 przedstawiono schemat prostej sieci komputerowej. Wymień trzy aktywne urządzenia sieciowe, które na nim występują.

7 Dokumentacja techniczna urządzeń sieciowych

ZAGADNIENIA

Informacje umieszczane w dokumentacji technicznej dokumentacji technicznej i osoba za nią odpowiedzialna **Język sporządzania** **Korzystanie z dokumentacji technicznej urządzeń**

Celem **dokumentacji technicznej** jest dostarczanie informacji dotyczących urządzenia, jego instalowania i działania. Dokumentacja techniczna powinna zawierać wszystkie informacje wykazujące zgodność wyrobu z wymaganiami dotyczącymi danego urządzenia. Sporządza się ją w jednym z oficjalnych języków Unii Europejskiej, natomiast instrukcja użytkowania i deklaracja zgodności muszą być dostępne także w języku rynku docelowego.

Odpowiedzialność za wprowadzenie – zgodnego z dokumentacją – wyrobu do obrotu i za dysponowanie dokumentacją techniczną spoczywa na wytwórcy lub na importerze danego urządzenia. Dokumentację techniczną urządzenia opracowuje się dla każdego urządzenia osobno. Powinna ona zawierać:

- charakterystykę (parametry techniczne);
- rysunek zewnętrzny;
- wykaz wyposażenia podstawowego i specjalnego;
- schemat elektryczny;
- schematy funkcjonowania;
- instrukcję obsługi i konserwacji;
- instrukcję bhp;
- wykaz części zamiennych i zapasowych;
- wykaz faktycznego wyposażenia;
- wykaz dołączonych rysunków.

Właściwie opracowana dokumentacja techniczna ułatwia konfigurację urządzenia, dzięki której pracuje ono efektywnie i zachowuje wyższy poziom bezpieczeństwa podczas użytkowania. Producenci urządzeń sieciowych udostępniają na swoich stronach internetowych dodatkowe informacje dotyczące problemów pojawiających się podczas eksploatacji urządzeń oraz aktualizacje oprogramowania firmowego, jak również świadczą pomoc techniczną związaną z eksploatacją urządzeń.

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

- typ urządzenia;
- obsługiwane standardy i protokoły;
- liczbę i typy portów;

- napięcie zasilania;
- wymiary gabarytowe;
- inne cechy zależne od typu urządzenia.

PRZYKŁAD 7.1

Analizowanie specyfikacji przełącznika

Odszukaj w internecie na stronie dowolnego dystrybutora sprzętu sieciowego specyfikację przełącznika wskazanego przez nauczyciela. Na podstawie specyfikacji odczytaj dane:

- wymiary urządzenia;
- liczbę i typy portów;
- pojemność tablicy adresów MAC;
- metody zarządzania przełącznikiem.

PRZYKŁAD 7.2

Dobór przełącznika na podstawie wymagań użytkownika

Odszukaj w internecie na stronie dowolnego dystrybutora sprzętu sieciowego specyfikację przełączników wskazanych przez nauczyciela. Wybierz model przełącznika spełniającego następujące wymagania:

- liczba portów 100 Mb/s – co najmniej 24;
- liczba portów 1 Gb/s – co najmniej 2;
- obudowa typu RACK;
- obsługa protokołu Spanning-Tree;
- prędkość magistrali wewnętrznej – co najmniej 32 Gb/s.

Podaj oznaczenie przełącznika i jego cenę.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Na podstawie dokumentacji technicznej przełącznika, który jest używany w pracowni komputerowej w twojej szkole, odczytaj parametry: typ i liczbę portów, wymiary zewnętrzne, liczbę adresów MAC w tablicy przełączania, obsługiwane protokoły. Jeżeli szkoła nie dysponuje papierową wersją dokumentacji, to odszukaj i pobierz dokumentację ze strony internetowej producenta.

8 Topologie sieciowe (logiczna i fizyczna)

ZAGADNIENIA

Funkcje topologii sieci **Rodzaje topologii** **Zalety i wady 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 na logicznej. **Topologia fizyczna** określa geometryczną organizację sieci lokalnej – graficznie przedstawia 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" (ang. *first come, first serve*). Przykładem takiej topologii jest sieć Ethernet.

Topologia przekazywania tokenu (żetonu) polega na kontrolowaniu dostępu do sieci przez przekazywanie elektronicznego tokenu (specjalnej ramki danych). Host, który w danym momencie ma token, może skorzystać z medium. Jeżeli 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:

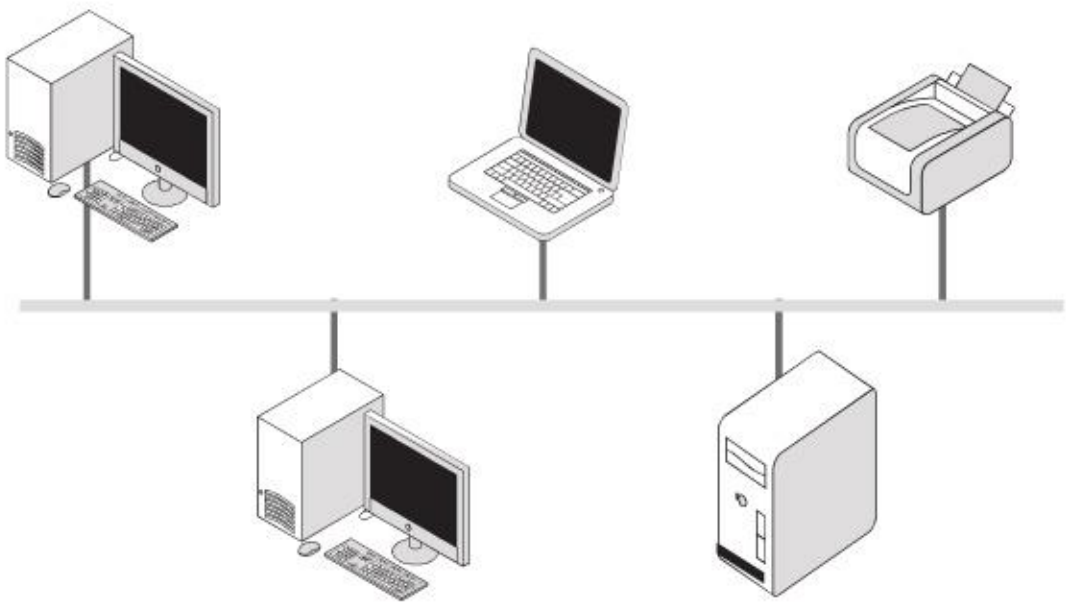
- magistrala (ang. *bus*);
- pierścień (ang. *ring*);
- gwiazda (ang. *star*).

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

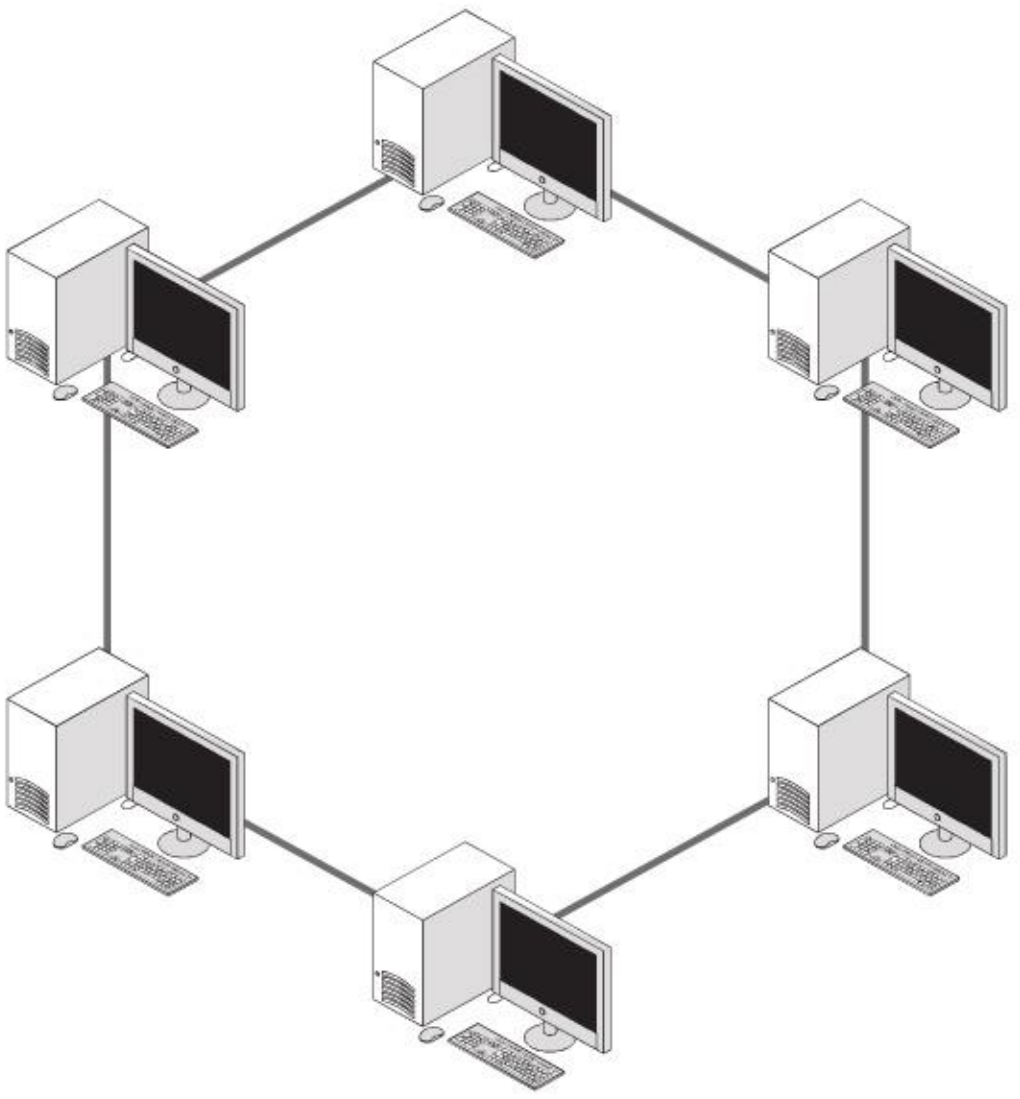
- rozszerzonej gwiazdy;
- siatki pełnej lub niepełnej.

W topologii **magistrali** (rys. 8.1) wszystkie węzły sieci (np. komputery, drukarki sieciowe) łączy się za pomocą pojedynczego kabla koncentrycznego, obsługującego tylko jeden kanał i nazwanego magistralą. Węzły dołącza się do wspólnej magistrali za pomocą tzw. trójników, w sposób charakterystyczny dla sieci równorzędnej. Oba końce magistrali muszą być zakończone elementami ograniczającymi, zwanymi terminatorami i chroniącymi 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. Tę topologię stosowano w małych sieciach.

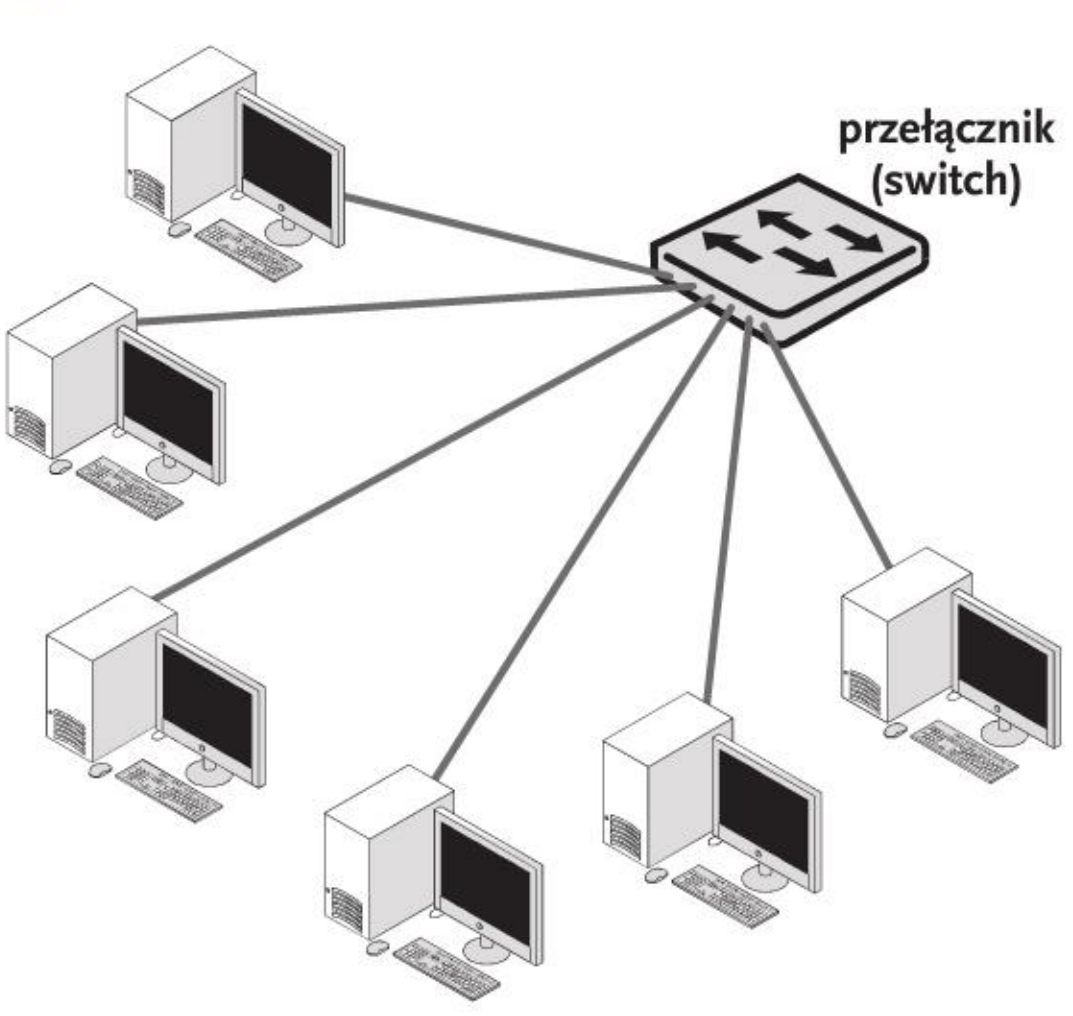
Zaletami magistrali są: krótkie odcinki kabla użyte do budowy sieci, brak konieczności stosowania dodatkowych urządzeń (koncentratorów, przełączników) i łatwość przyłączenia nowego



Rys. 8.1. **Topologia magistrali**



Rys. 8.2. **Topologia pierścienia**



Rys. 8.3. **Topologia gwiazdy**

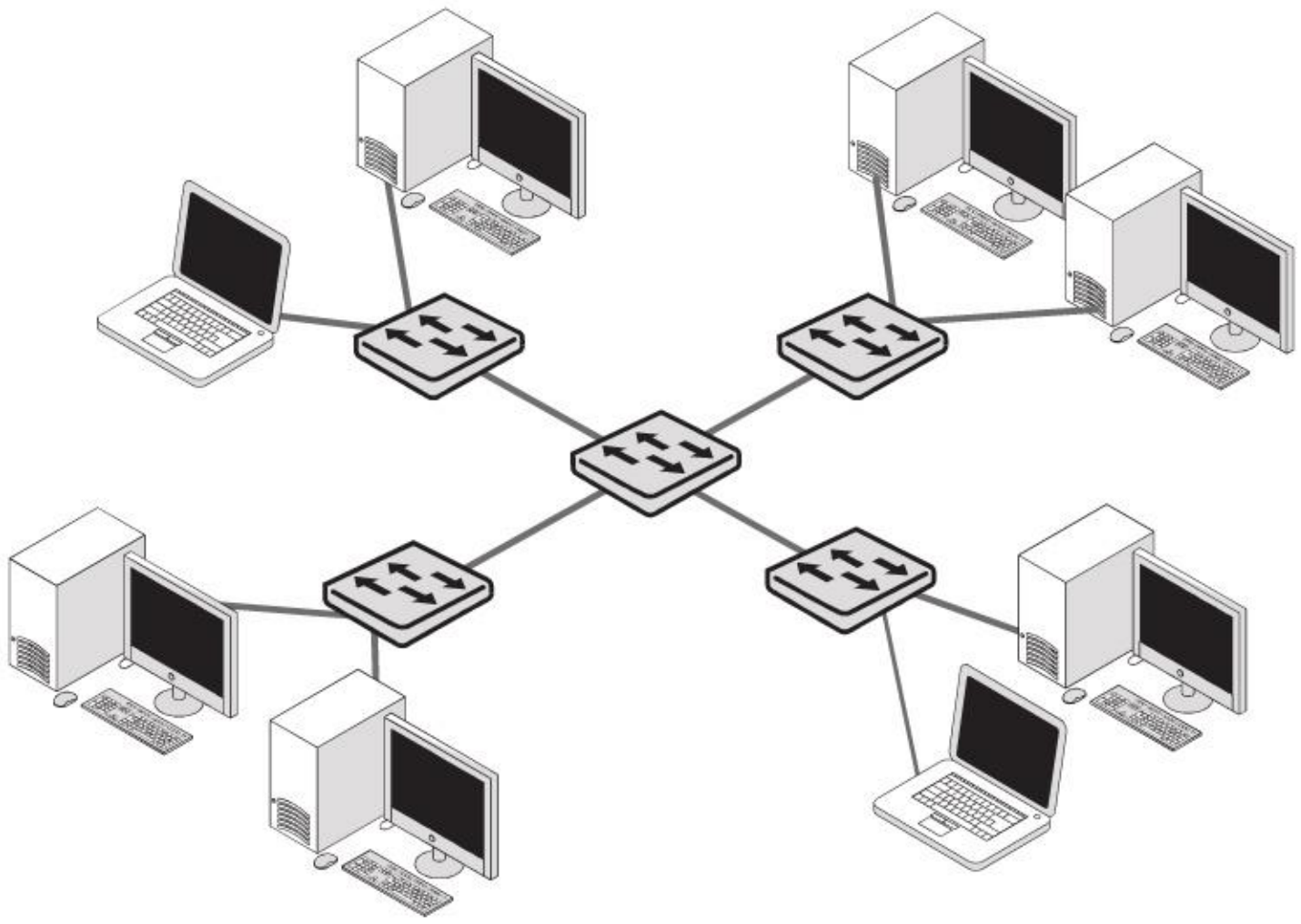
urządzenia. Wadą magistrali jest trudna lokalizacja uszkodzenia kabla. Możliwa jest tylko jedna transmisja w danym momencie, a awaria kabla może spowodować podział sieci na dwa segmenty lub unieruchomienie całej sieci.

W topologii **pierścienia** (rys. 8.2) każda stacja robocza przyłączona do sieci ma dwa połączenia – po jednym do każdego najbliższego sąsiada. Połączenie tworzy fizyczną pętlę, czyli pierścień. Dane przesyła się wokół pierścienia w jednym kierunku. Każda stacja robocza działa podobnie jak wzmacniak: pobiera pakiety do niej zaadresowane i odpowiada na nie, a także przesyła pozostałe pakiety do następnej stacji roboczej. Im więcej urządzeń przyłączono do pierścienia, tym czas odpowiedzi jest dłuższy. Czas można jednak określić, co nie jest możliwe dla innych topologii.

Wada pierścienia polega na tym, że awaria pojedynczego przewodu lub komputera powoduje problemy z działaniem sieci. Problemy można jednak rozwiązać, jeżeli zastosuje się podwójny pierścień lub układy obejściowe.

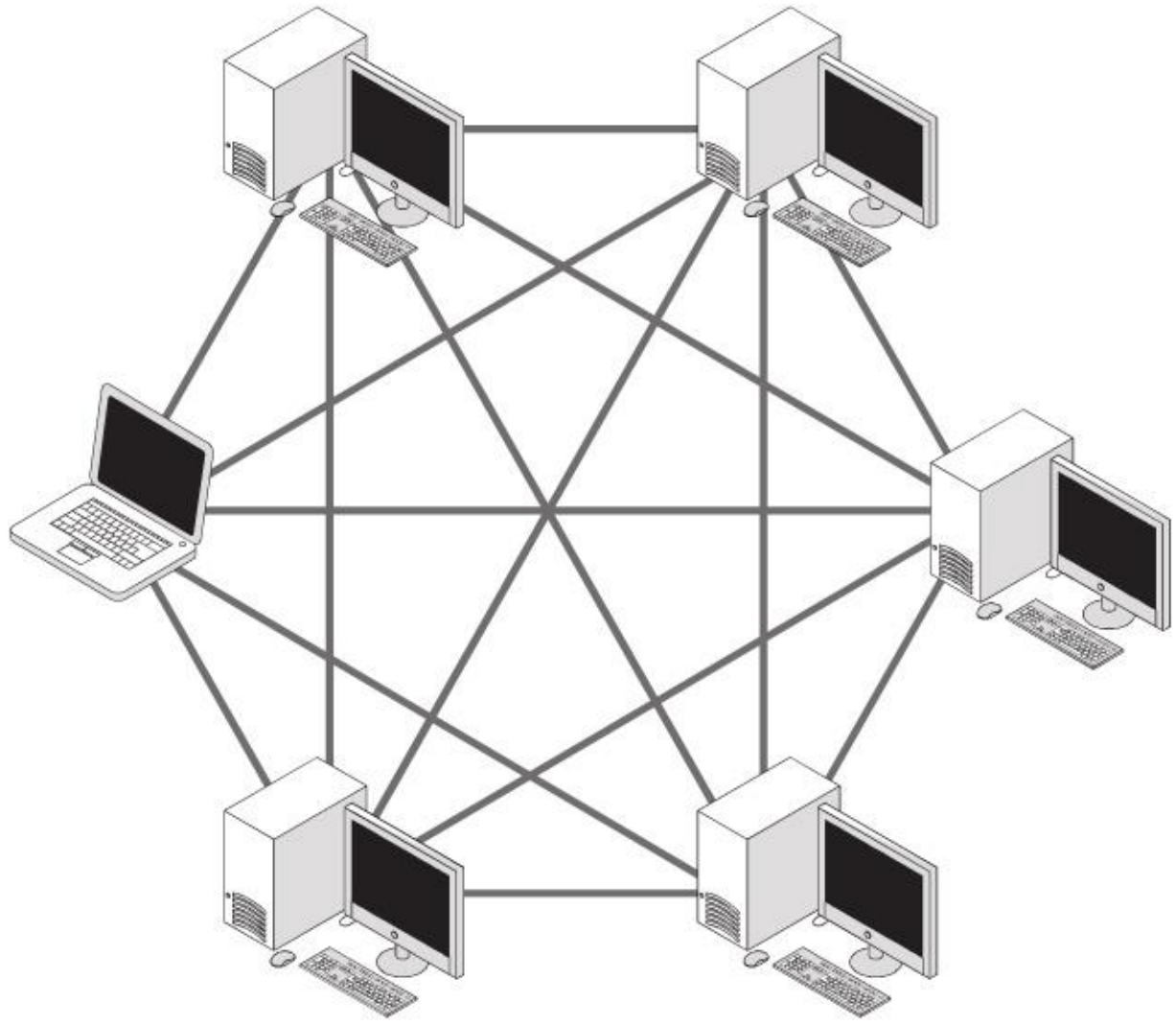
W topologii **gwiazdy** (rys. 8.3) połączenia sieci rozchodzą się z centralnego punktu, którym może być koncentrator albo przełącznik. Każde urządzenie przyłączone do sieci może uzyskiwać dostęp do współdzielonego nośnika. Zaletami topologii gwiazdy są duża przepustowość i łatwa lokalizacja uszkodzeń. W razie awarii łącza lub komputera pozostała część sieci pracuje bez zakłóceń. Wadami są większe zapotrzebowanie na kable i konieczność stosowania koncentratorów lub przełączników, których awaria może unieruchomić całą sieć. Topologia gwiazdy dominuje we współczesnych sieciach LAN. Są one elastyczne, skalowalne i stosunkowo tanie.

Topologia **rozgałęzionej gwiazdy** (rys. 8.4) opiera się na topologii gwiazdy. Pojedyncze gwiazdy łączy się za pomocą koncentratorów lub przełączników. Stosuje się ją w przypadku dużych sieci, gdy obszar, który ma być pokryty siecią, jest większy, niż pozwala na to topologia gwiazdy. Zaletami topologii rozgałęzionej gwiazdy są ograniczenie liczby urządzeń, które muszą być połączone z centralnym węzłem, i możliwość ograniczenia ruchu lokalnego do pojedynczej gwiazdy.



Rys. 8.4. **Topologia rozgałęzionej gwiazdy**

Topologię **siatki** (rys. 8.5) wykorzystuje się wtedy, gdy każdy węzeł ma własne połączenia z wszystkimi pozostałymi. Zaletą jest niezawodność uzyskana przez możliwość przesyłania danych wieloma różnymi ścieżkami, natomiast wadami – wysoki koszt i skomplikowana budowa. W sieciach rozległych, np. w internecie, stosuje się topologię siatki częściowej. Między routerami odgrywającymi rolę węzłów, za których pomocą przyłącza się sieci lokalne, istnieje wiele ścieżek do dowolnego miejsca, lecz nie ma połączeń między wszystkimi węzłami.

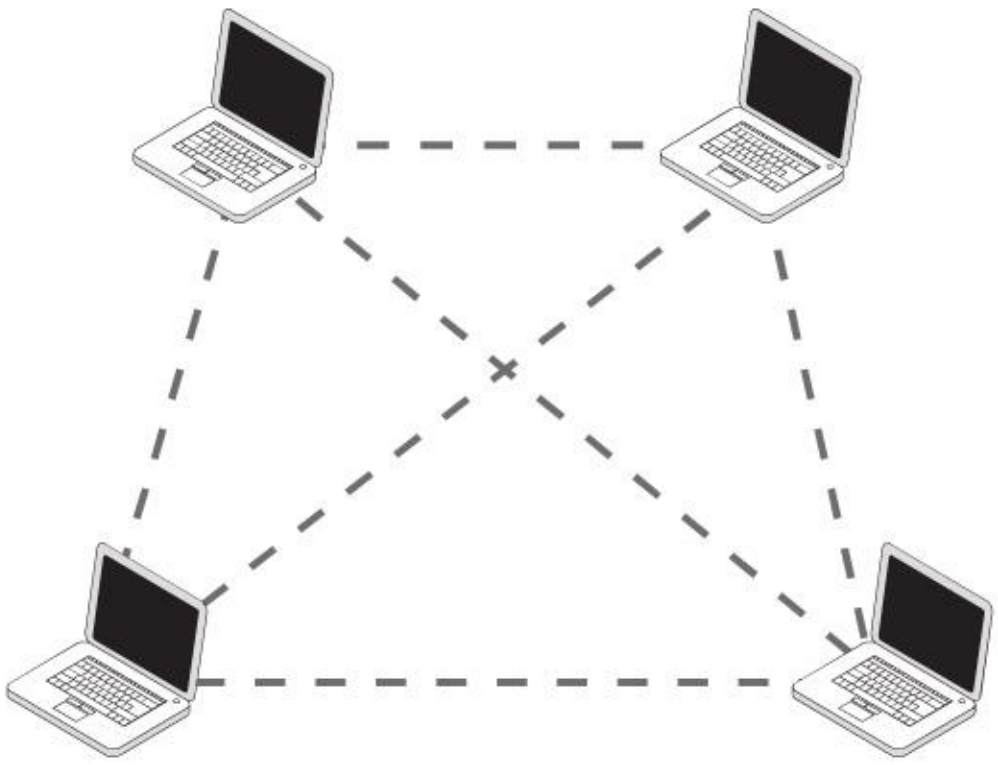


Rys. 8.5. **Topologia siatki**

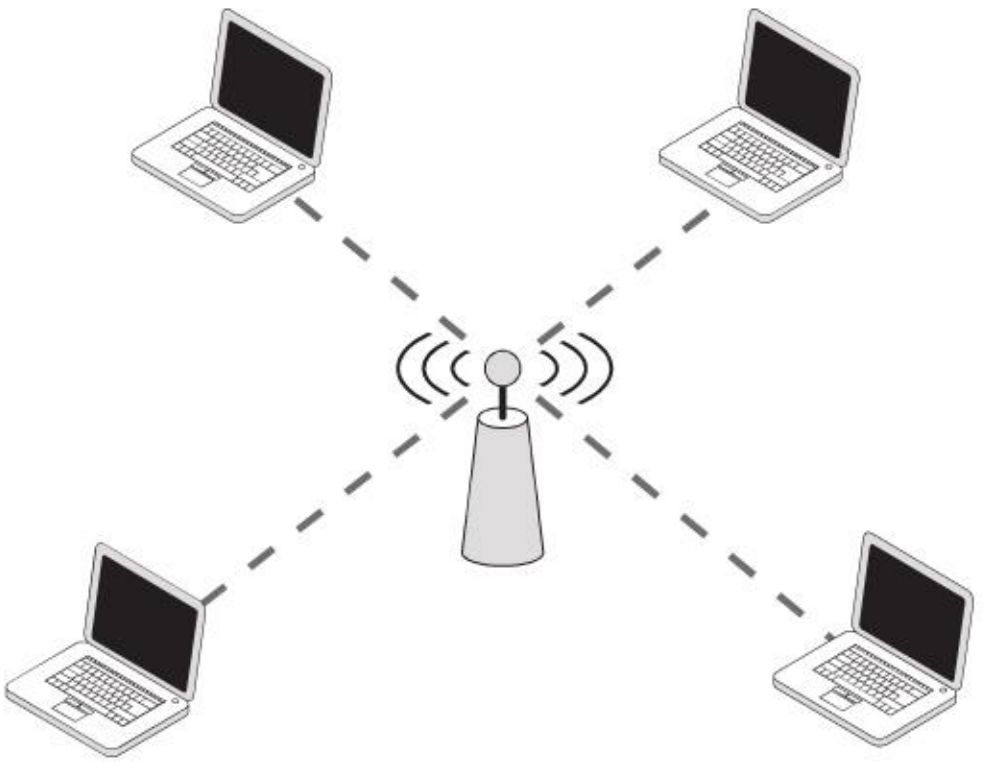
Małe sieci bezprzewodowe mogą być budowane w trybie **ad hoc** (rys. 8.6). Urządzenia komunikują się ze sobą bezpośrednio zależnie od potrzeb przez stosunkowo krótki czas. Przykładem sieci ad hoc jest sieć złożona z dwóch telefonów komórkowych połączonych do przesłania pliku. Do przekazywania danych nie jest wymagane istnienie żadnej

infrastruktury sieciowej, gdyż pakiety dostarcza się do odbiorcy przez inne, dowolnie zlokalizowane urządzenie w tej sieci. Po zakończeniu wymiany danych sieć się demontuje.

Większe sieci bezprzewodowe wymagają **trybu infrastruktury** (rys. 8.7). Wszystkie urządzenia komunikują się z punktami dostępowymi, które pełnią funkcję bramy (do sieci przewodowej) i pośredniczą w komunikacji między urządzeniami sieci bezprzewodowej.



Rys. 8.6. **Sieć bezprzewodowa w trybie ad hoc**



Rys. 8.7. **Sieć bezprzewodowa w trybie infrastruktury**

Każda topologia charakteryzuje się następującymi cechami:

- rodzajem możliwego do zastosowania medium transmisyjnego;
- rodzajem dostępu do sieci;
- rodzajem wykorzystanych urządzeń aktywnych i pasywnych;
- możliwością rozbudowy i naprawy;
- długością segmentu sieci;
- kosztem i niezawodnością;
- przepustowością i transferem danych.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Którą topologię fizyczną wykorzystuje się w twojej szkole?
2. Którą ze strategii znanych z algorytmiki zastosujesz do lokalizacji miejsca awarii w topologii magistrali? Opisz, jak ta zasada będzie realizowana w lokalizowaniu awarii.
3. Wymień elementy i urządzenia, które są niezbędne, aby zbudować lokalną sieć komputerową na podstawie topologii magistrali.
4. Na podstawie opisu podaj nazwę topologii fizycznej sieci:
   a) W tej topologii wszystkie urządzenia połączono ze sobą za pomocą kabla koncentrycznego. Na końcu segmentu sieciowego znajduje się terminator.
   b) W tej topologii każdy komputer połączono z kolejnym za pomocą pojedynczego lub podwójnego okablowania. Jest odporna na powstawanie kolizji pakietów w sieci.
   c) Wymaga centralnego urządzenia sieciowego nadzorującego ruch w sieci. Jest łatwo skalowalna i pozwala na szybkie zdiagnozowanie uszkodzenia.

9 Metody dostępu do nośnika

ZAGADNIENIA

Kanał komunikacyjny **Różnica między transmisją szerokopasmową a transmisją w paśmie podstawowym** **Kontrola dostępu urządzeń do nośnika danych**

Urządzenia w sieci łączy się za pomocą łączy. Dane między urządzeniami przesyła się 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. Zależnie od sposobu wykorzystania łączy wyróżnia się:

- **transmisję w paśmie podstawowym** (ang. *baseband*) – polega na utworzeniu w łączu tylko jednego kanału transmisyjnego, za którego pomocą przesyła się tylko jeden ciąg sygnałów;
- **transmisję szerokopasmową** (ang. *broadband*) – polega na podziale pojedynczego łącza na wiele kanałów przez przydzielenie im różnych częstotliwości lub przez podział czasu transmisji na szczeliny czasowe, w których przesyła się dane z różnych kanałów. Przykładowo: w telewizji kablowej jednocześnie jednym kablem przesyła się 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 spotyka się również technologie Token Ring i FDDI. Technologię **Ethernet** opracowano w latach siedemdziesiątych w firmie Xerox. Obecnie ta nazwa odnosi się do wszystkich sieci pochodnych, korzystających z dostępu do nośnika metodą **CSMA/CD** (ang. *Carrier Sense Multiple Access with Collision Detection*). W tej metodzie urządzenia **rywalizują** 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 swoje próby w takich samych odstępach, co skutkowałoby kolejnymi kolizjami.

W sieciach bezprzewodowych stosuje się metodę **CSMA/CA** (ang. *Carrier Sense Multiple Access with Collision Avoidance*). Transmisja w sieci z unikaniem kolizji może zostać zrealizowana przez 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 sprawdza. Jeśli upłynął czas t, stacja zgłasza żądanie transmisji i czeka przez ustalony czas t (jednakowy dla wszystkich stacji w danej sieci): nasłuchuje, czy

inna stacja nie zgłosiła żądania. Jeżeli stwierdzi inne żądanie, czeka przez losowy czas i zaczyna procedurę od początku. W innym przypadku zaczyna nadawać.

Technologię **Token Ring** opracowano w latach siedemdziesiątych w firmie IBM. W tej sieci stacje sieciowe są podłączone bezpośrednio do urządzeń **MAU** (ang. *Multi Access Unit*), które są ze sobą połączone tak, aby tworzyły jeden duży pierścień. Token Ring stosuje metodę dostępu do nośnika, nazywaną przekazywaniem żetonu (ang. *Token-Passing*). W pierścieniu krąży specjalna ramka – żeton (ang. *token*). Stacja sieciowa uzyskuje prawo do transmisji danych tylko wtedy, gdy ma żeton. Jeżeli stacja sieciowa ma 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 następnej stacji w pierścieniu. Stacja mająca żeton przekształca go w ramkę, następnie dodaje dane przeznaczone do przesłania i wysyła tę ramkę 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 stacji nadawczej, w której 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 na wygenerowanie nowego żetonu. Ponieważ w pierścieniu może być tylko jeden żeton, w sieciach Token Ring nie występują kolizje.

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

Metodę dostępu na zasadzie **priorytetu żądań** wykorzystuje się w sieciach opartych na specyfikacji IEEE 802.12, np. w sieci VG-AnyLAN opracowanej przez Hewlett-Packard. W tej metodzie 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 realizuje się za pomocą przełączników. Przełącznik to wieloportowe urządzenie, które uczy się adresów fizycznych urządzeń i zapamiętuje je w wewnętrznej tabeli. Następnie tworzy między nadawcą i odbiorcą tymczasowe ścieżki przełączane, którymi przesyła się dane. W protokołach wykorzystujących mechanizm rywalizacji przełączanie portu powoduje, że rozmiar domeny kolizji zmniejsza się do dwóch urządzeń – przełączanego portu i 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.

10 Rodzaje środowisk sieciowych (klient–serwer i peer-to-peer)

ZAGADNIENIA

Różnica między architekturą równorzędną i klient–serwer **Cechy architektury równorzędnej i klient–serwer**

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

Komputer – lub inne urządzenie korzystające z zasobów udostępnianych przez serwer – będzie nazywany **klientem**. Zależnie od tego, jak zostanie zorganizowane udostępnianie i korzystanie z udostępnionych zasobów w sieci, można mówić o architekturze sieci równorzędnej lub o architekutrze opartej na serwerach. W architekturze **równorzędnej** (ang. *peer-to-peer*) każdy użytkownik może jednocześnie udostępniać zasoby swojego komputera i 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. To rozwiązanie stosuje się w małych sieciach (do dziesięciu komputerów). Wszystkie informacje o udostępnionych zasobach i użytkownikach uprawnionych do ich wykorzystania zapisuje się na komputerze udostępniającym dany zasób. Jeżeli korzysta się z wielu serwerów, na których jest zapisana lokalnie informacja o zasobach, to na każdym z nich trzeba uzyskać prawo do korzystania z zasobów, co oznacza, że trzeba wpisywać hasło na każdym serwerze. Taka sieć 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** (ang. *client-server*) istnieje jeden komputer lub więcej 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 i przechowuje wspólnie wykorzystywaną bazę danych o zasobach sieci, jej użytkownikach i uprawnieniach użytkowników do zasobów. Stacja robocza, pełniąca funkcję klienta, komunikuje się z serwerem, do czego wykorzystuje oprogramowanie 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 instalowanych na serwerach i klientach.
2. Jaki typ sieci zaproponujesz na potrzeby swojej szkoły? Uzasadnij wybór.
3. Gdzie i dlaczego używa się sieci równorzędnych?
4. Jak zidentyfikować serwer w sieci?
5. W jaki sposób zidentyfikować architekturę używaną w danej sieci?

11 Komunikacja w sieci

ZAGADNIENIA

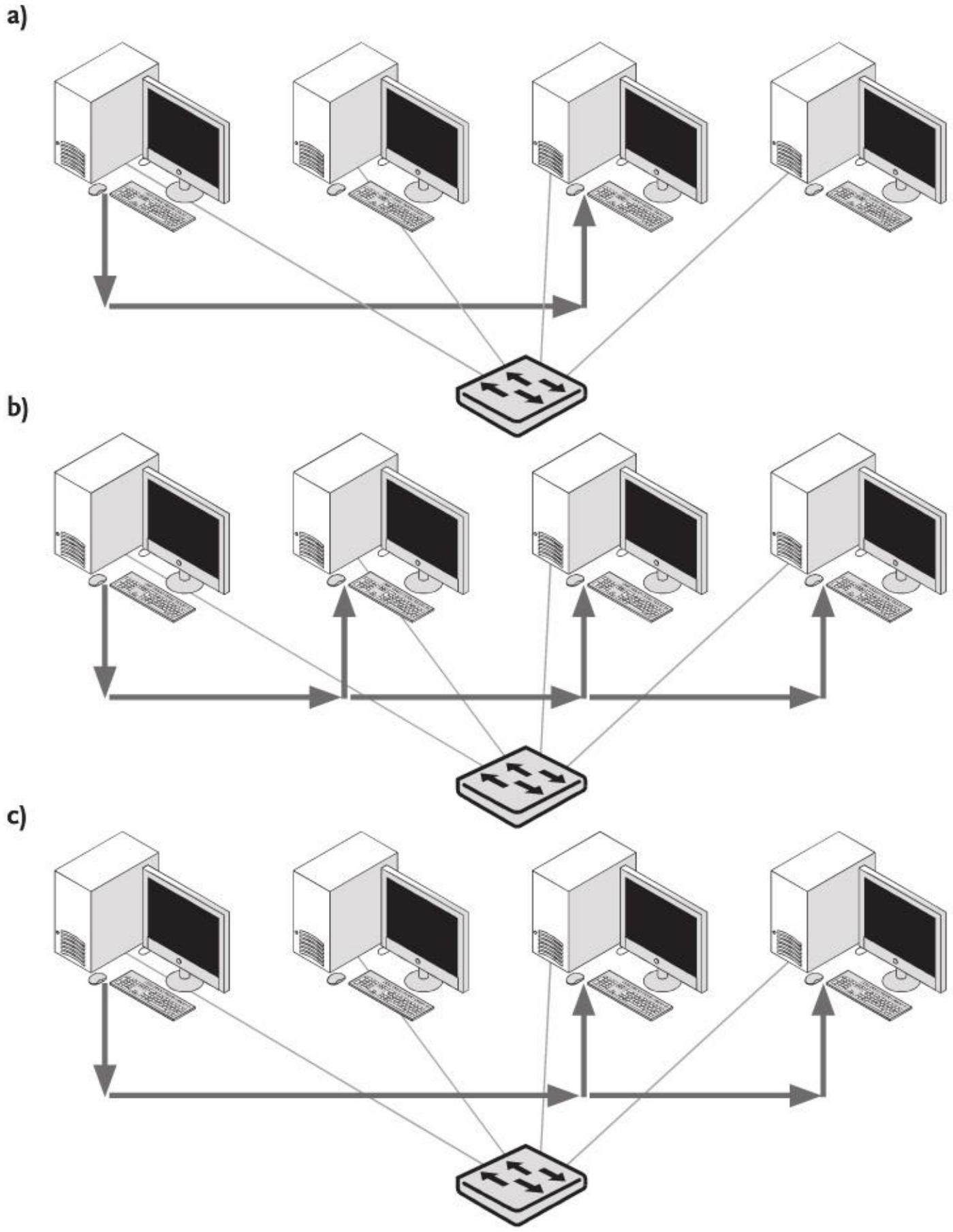
Protokół komunikacyjny **Transmisja danych w trybach połączeniowym i bezpołączeniowym** **Rodzaje transmisji** **Transmisja jednokierunkowa w trybach półdupleksu i pełnego dupleksu** **Wymagania aplikacji dotyczące przepustowości łącza** **Transmisje szeregowa i równoległa** **Transmisje synchroniczna i asynchroniczna** **Pobieranie i wysyłanie danych**

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

Tryb połączeniowy polega na ustanowieniu logicznego połączenia między dwoma komunikującymi się 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 przekazuje się niezależnie, np. podczas przekazywania 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 nazywa się **jednostkowym** (ang. *unicast*). W sieciach rozwiązano to w ten sposób, że każde urządzenie ma unikatowy adres. Dane wysyłane przez nadawcę docierają do wielu urządzeń, ale są odbierane tylko przez to urządzenie, którego adres jest adresem docelowym (reszta urządzeń ignoruje dane, które nie są przeznaczone dla nich). Urządzenie nadawcze może wysłać informację do wszystkich dostępnych urządzeń. Wtedy adresem docelowym staje się specjalny adres, nazywany **rozgłoszeniowym** (ang. *broadcast*). Urządzenia traktują transmisje na adres rozgłoszeniowy tak, jakby były one adresowane na ich adres jednostkowy.

W rozgłaszaniu **grupowym** (ang. *multicast*) dane przeznacza się 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 informację przekazuje się jednokrotnie. W protokole IPv6 wprowadzono nowy tryb komunikacji **do najbliższego węzła** (ang. *anycast*). W tym trybie dane wysyła się do topologicznie najbliższego (czyli teoretycznie najlepszego) odbiorcy. Komunikacja ma jednego nadawcę i może mieć wielu odbiorców, przy czym dane odbiera tylko jeden z nich. Anycast może być wykorzystywany np. w usłudze DNS, w której zapytania kieruje się do grupy serwerów, ale tylko jeden z nich obsługuje dane zapytanie. Klient nie może jednak wybrać, które urządzenie z grupy zostanie wybrane do obsługi zapytania.

Transmisja **jednokierunkowa** (ang. *simplex*) to transmisja, w której odbiornik nie może przesłać odpowiedzi ani innych danych. Przykładem tego typu transmisji, spoza obszaru sieci komputerowych, jest emisja audycji radiowych, podczas której słuchacz przy odbiorniku radiowym może tylko odbierać informacje pochodzące z nadajnika. Tego typu transmisji nie stosuje się w sieciach komputerowych.



Rys. 11.1. Tryb transmisji:
a) jednostkowa,
b rozgłoszeniowa,
c) grupowa

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

Transmisja danych cyfrowych może być szeregowa lub równoległa. W **transmisji równoległej** dane przesyła się jednocześnie kilkoma przewodami, z których każdy przenosi jeden bit informacji, np. port LPT w komputerze. Zasięg transmisji równoległej jest mniejszy niż zasięg transmisji szeregowej. W **transmisji szeregowej** poszczególne bity informacji przesyła się kolejno po sobie wraz z dodatkowymi danymi pozwalającymi na kontrolę tej transmisji, np. port COM w komputerze. Transmisja szeregowa pozwala na wysyłanie danych na duże odległości. Transmisja szeregowa umożliwia przesyłanie danych w sposób:

- **asynchroniczny** – dane poprzedza się **bitem startu** (stan logiczny: 0), który jest sygnałem rozpoczęcia transmisji. Po bicie startu przesyła się **bity danych** (od 5 do 8), od najmłodszego do najstarszego, **bit parzystości** (jeśli jest używany) oraz **bity stopu** (sygnał odstępu przed następnym znakiem – stan logiczny: 1). Każdy znak przesyła się i interpretuje niezależnie od innych. Po wykryciu stanu logicznego 0 układ odbierający odmierza czas równy 1/2 czasu przesyłania bitu i sprawdza, czy nadal jest stan 0 (jeśli nie, jest to traktowane jako błąd). Następnie odmierza czas równy czasowi przesyłania 1 bitu i odczytuje wartości poszczególnych bitów danych;
- **synchroniczny** – dane przesyła się w wyznaczonych momentach, określonych dodatkowym sygnałem, tzw. sygnałem zegarowym CLK, wspólnym dla nadajnika i odbiornika. Dane przesyła się bez dodatkowych bitów startu i stopu, ale poprzedza informacją wstępną, pozwalającą wykryć ich początek – bajtami synchronizacji SYN, po których następuje znak rozpoczynający **ramkę SOH** (ang. *start of header*), i zakończone sekwencją oznaczającą **koniec ramki ETX** (ang. *end of text*). Ramka może zawierać w nagłówku dodatkowe informacje sterujące, np. adres nadawcy i odbiorcy. Koniec tych dodatkowych informacji i początek danych oznacza się **znakiem STX** (ang. *start of text*). Jeśli znak początku lub końca ma wystąpić w przesyłanych danych, to poprzedza się go znakiem wyłączającym jego interpretację. Do sprawdzenia poprawności transmisji ramka zwykle zawiera sumę kontrolną, np. CRC.

Dane, np. pliki, mogą być **pobierane** (ang. *download*) z serwerów w sieci lub **wysyłane** (ang. *upload*) do serwera lub komputera należącego do innego użytkownika. Łącze internetowe umownie dzieli się na dwa kanały: kanał wysyłania i kanał pobierania. Przepustowość tych kanałów określa się w bitach na sekundę (b/s lub bps) lub jednostkach wielokrotnych, np. Mb/s, Gb/s. W warunkach domowych użytkownik zwykle więcej danych pobiera, niż wysyła, np. wysyła adres strony, której zawartość chciałby pobrać. Ze względu na koszt w takim wypadku stosuje się łącza **asymetryczne** (mają one zwykle niską przepustowość kanału umożliwiającego wysyłanie i większą przepustowość kanału pobierania). Firmy i użytkownicy udostępniający dane, np. za pomocą serwera WWW, powinni korzystać z łączy **symetrycznych**, w których przepustowość wysyłania i przepustowość pobierania są jednakowe.

Aby usługi i aplikacje sieciowe mogły działać poprawnie, 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, wymagają niezawodnego przesyłania danych. Nadawca i odbiorca komunikują się ze sobą, aby się upewnić, że wszystkie dane dotarły bez błędów i w odpowiedniej kolejności. W razie błędów te protokoły żądają retransmisji uszkodzonych lub zagubionych danych. Dla tych usług stosuje się 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 stosuje się

protokoły zawodnego transportu danych. Nie oznacza to, że dane nie dotrą do miejsca przeznaczenia – tylko że protokoły nie gwarantują bezbłędnego dostarczenia danych.

Aby działać bez zakłóceń, niektóre aplikacje muszą transmitować lub odbierać dane z określoną prędkością. Przykładowo: aplikacja odtwarzająca pliki multimedialne musi odbierać taką ilość danych, która jest niezbędna do wyświetlania filmu lub do odtwarzania muzyki. Wymaga zatem określonej przepustowości. Jeżeli ten warunek nie zostanie spełniony, to aplikacja nie będzie działała prawidłowo (lub w ogóle się nie uruchomi) albo rozpocznie pracę przy innych parametrach, np. niższej rozdzielczości obrazu lub jakości dźwięku.

Istnieje pewna grupa aplikacji pracujących w tzw. **czasie rzeczywistym**, które dopuszczają niewielki czas opóźnienia przesyłanych danych. Przykładem może być telekonferencja, w której opóźnienia w transmisji danych skutkują przerwami 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 internecie. Komputery w internecie komunikują się za pomocą protokołu **IP** (ang. *Internet Protocol*), działającego w warstwie sieciowej, i **TCP** (ang. *Transmission Control Protocol*) lub **UDP** (ang. *User Datagram Protocol*), działających w warstwie transportowej. Inne protokoły, takie jak **HTTP** (ang. *Hypertext Transfer Protocol*), wykorzystuje się w warstwie aplikacji.

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

Dane przesyłane w internecie dzieli się w warstwie sieciowej modelu ISO na **pakiety**. Każdy pakiet jest opatrzony nagłówkiem IP, zawierającym m.in. adresy nadawcy i odbiorcy. Na podstawie tych informacji routery podejmują decyzję, jaką drogą dany pakiet powinien zostać dostarczony do miejsca przeznaczenia. Protokół IP nie sprawdza, czy pakiet dotarł do miejsca przeznaczenia. W tym celu używa się protokołu TCP. Do każdego pakietu dołącza on swój nagłówek, w którym m.in. numeruje wszystkie wychodzące pakiety. Jeżeli nie otrzyma od adresata potwierdzenia otrzymania pakietu, wysyła go ponownie. W nagłówku TCP znajduje się również numer portu identyfikującego 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.
3. Wymień sytuacje, w których korzystniej jest korzystać z łączy symetrycznych i asymetrycznych.
4. Wyszukaj, np. na stronie wybranego dostawcy, nazwy aktualnie dostępnych technologii oferujących dostęp symetryczny i asymetryczny do internetu.

12 Modele warstwowe sieci

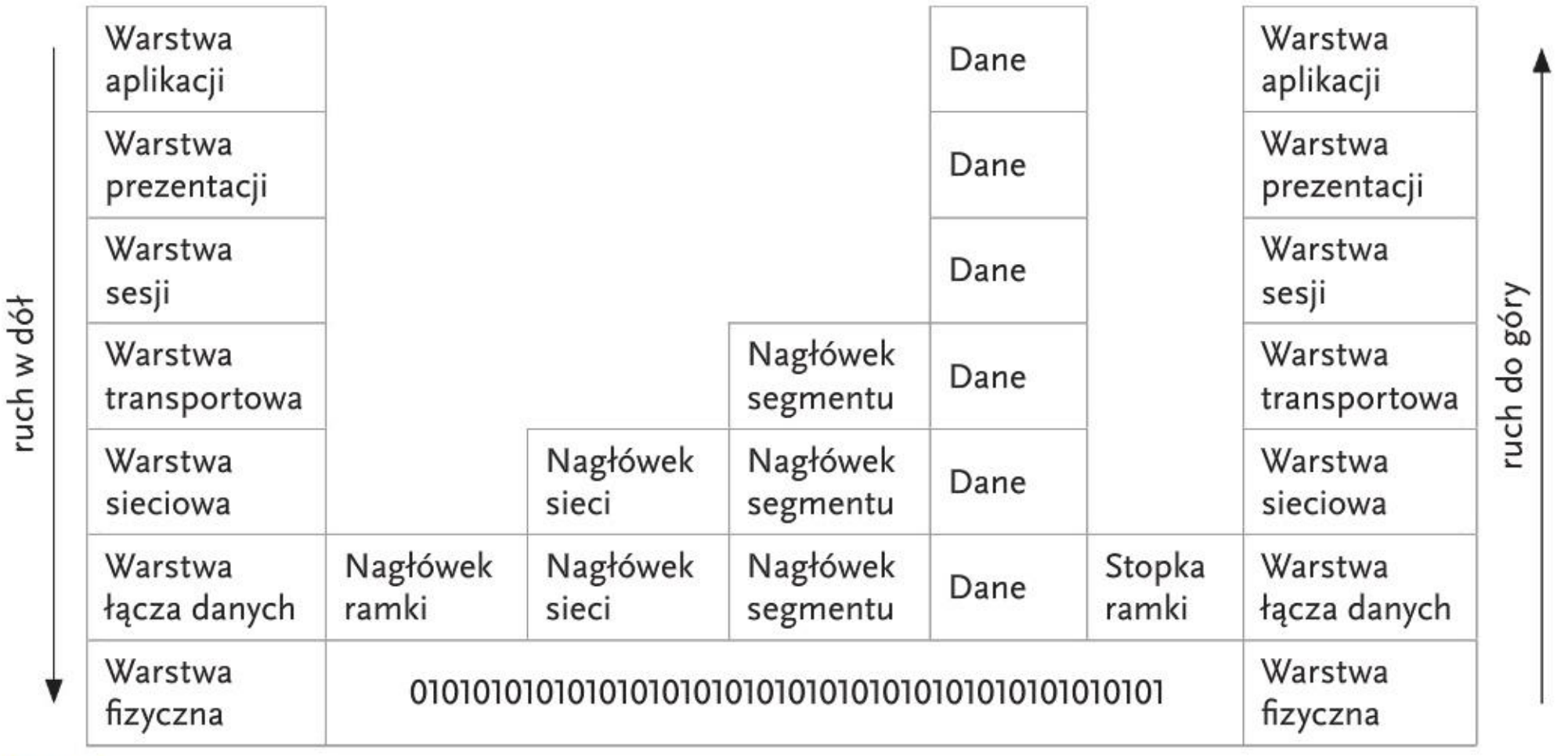
ZAGADNIENIA

Warstwy modelu sieci ISO/OSI i modelu TCP/IP Rola poszczególnych warstw w komunikacji Jednostki danych w poszczególnych warstwach Przepływ danych między warstwami Proces enkapsulacji i dekapsulacji Protokoły działające w poszczególnych warstwach Protokół ARP

W początkowym okresie wprowadzania sieci komputerowych każdy dostawca sieci stosował własne firmowe rozwiązania. Później pojawił się pomysł, aby ujednolicić budowę sieci i umożliwić współpracę sieci pochodzących od różnych dostawców. Podjęto więc próbę wprowadzenia standardów w budowie sieci i protokołów sieciowych. Ponieważ sieci komputerowe mogą być skomplikowane, nadaje się im strukturę warstwową, aby ułatwić zrozumienie i opis sposobu ich działania. Istnieje kilka modeli warstwowych opisujących budowę i działanie sieci.

12.1. Model sieci ISO/OSI

Według modelu **OSI** (ang. *Open Systems Interconnection*) wyróżnia się siedem takich warstw (rys. 12.1). Każda warstwa komunikuje się tylko z warstwą bezpośrednio wyższą i z warstwą bezpośrednio niższą. Warstwy wyższe korzystają z usług warstw niższych, a warstwy niższe świadczą usługi na rzecz warstw wyższych. Trzy warstwy górne (aplikacji, prezentacji i sesji) zapewniają współpracę z oprogramowaniem realizującym zadania użytkownika systemu komputerowego. Tworzą one interfejs pozwalający na komunikację z warstwami niższymi.



Rys. 12.1. **Przepływ danych między warstwami modelu OSI**

Warstwa **aplikacji** zajmuje się specyfikacją interfejsu, który aplikacje wykorzystują do przesyłania danych do sieci. Świadczy ona usługi końcowe dla aplikacji. Na tym poziomie działają aplikacje sieciowe dostępne bezpośrednio dla użytkownika, takie jak klient poczty elektronicznej czy przeglądarka stron WWW. Jeżeli użytkownik posługuje się oprogramowaniem działającym w architekturze klient – serwer, to po jego stronie znajduje się klient, a serwer działa na komputerze podłączonym do sieci. Serwer i klient działają w warstwie aplikacji.

Zadaniem warstwy **prezentacji** jest przetworzenie danych pochodzących z warstwy aplikacji do postaci standardowej, której wymagają warstwy niższe. Gdy informacje płyną w kierunku warstwy aplikacji, warstwa prezentacji tłumaczy dane otrzymane z warstw niższych na format zgodny z aplikacją, dla której są przeznaczone. Odpowiada także za kompresję i szyfrowanie danych.

Zadaniem warstwy **sesji** jest zarządzanie przebiegiem komunikacji podczas połączenia między dwoma komputerami. Przepływ tej komunikacji nazywa się **sesją**. Warstwa nadzoruje połączenie i kontroluje, która aplikacja łączy się z inną, dzięki czemu może zapewnić właściwy kierunek przepływu danych. W razie przerwania połączenia nawiązuje je ponownie. Ponadto określa, czy komunikacja może zachodzić w jednym kierunku czy w obydwu, a także gwarantuje zakończenie wykonywania bieżącego żądania przed przyjęciem kolejnego.

Zadaniem czterech najniższych warstw jest transmisja danych. Te warstwy zajmują się odnajdywaniem odpowiedniej drogi do miejsca przekazania konkretnej informacji. Dzielą dane na odpowiednie dla danej warstwy **jednostki danych PDU** (ang. *Protocol Data Unit*). Dodatkowo mogą zapewniać weryfikację bezbłędności przesyłanych danych. Warstwy dolne to: transportowa, sieciowa, łącza danych i fizyczna.

Warstwa **transportowa** przesyła wiadomość kanałem stworzonym przez warstwę sieciową. W tym celu dzieli dane otrzymane z warstwy sesji na **segmenty** (ang. *segment*), które kolejno wysyła się do stacji docelowej. Może zapewniać właściwą kolejność otrzymanych segmentów, a w razie zaginięcia lub uszkodzenia segmentu – zażądać jego retransmisji. Stacja docelowa może również wysyłać potwierdzenie odebrania segmentu.

Warstwa **sieciowa**, jako jedyna, dysponuje wiedzą dotyczącą fizycznej topologii sieci. Rozpoznaje, jakimi trasami połączono poszczególne komputery oraz sieci, i na tej podstawie decyduje, którą trasę wybrać. Jednostką danych w tej warstwie jest **pakiet** (ang. *packet*). Ta warstwa odpowiada za adresowanie logiczne węzłów sieci (np. adresy IP).

Warstwa **łącza danych** nadzoruje warstwę fizyczną i steruje fizyczną wymianą bitów. Umożliwia zmianę parametrów pracy warstwy fizycznej tak, aby obniżyć liczbę błędów pojawiających się podczas przekazu. Definiuje mechanizmy **kontroli błędów CRC** (ang. *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** (ang. *frame*). Warstwa łącza danych dzieli się na dwie podwarstwy:

- **LLC** (ang. *Logical Link Control*) – podwarstwa sterowania łączem danych – kontroluje poprawność transmisji i obsługuje tworzenie ramek. Współpracuje przede wszystkim z warstwą sieciową;
- **MAC** (ang. *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.

12.2. Przepływ danych między warstwami

Aplikacje użytkownika działają w warstwie aplikacji: generują strumień danych, który przesyła się do niższych warstw modelu OSI. W warstwie transportowej dzieli się go na segmenty. Każdy z segmentów ma nagłówek warstwy czwartej, który zostaje nadany przez właśnie tę warstwę. W nagłówku umieszcza się m.in. **numer sekwencyjny**, potrzebny do ustalenia kolejności przesyłania danych. Warstwa sieciowa jest odpowiedzialna za podzielenie danych na pakiety i za opatrzenie każdego pakietu nagłówkiem. W nagłówku pakietu umieszcza się m.in. adres IP nadawcy i odbiorcy. Adres IP odbiorcy wykorzystuje router do ustalenia optymalnej trasy, po której pakiet będzie przesłany. Pakiet przesyła się do warstwy łącza danych i dzieli na ramki. Każda z ramek ma nagłówek zawierający m.in. adresy MAC nadawcy i odbiorcy oraz stopkę z polem 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 nazywa się **enkapsulacją** (ang. *encapsulation*). Proces odwrotny, realizowany podczas odbierania informacji i przesyłania danych do górnych warstw, nazywa się **dekapsulacją** (ang. *decapsulation*). Przepływ danych między warstwami modelu OSI przedstawiono na rys. 12.1.

Dane, przechodzące przez różne urządzenia sieciowe, dochodzą do różnych warstw modelu OSI. Zasięg danych w urządzeniu przedstawiono na rys. 12.2. Zależnie od zasięgu danych analizowanych przez urządzenia można zaklasyfikować je do poszczególnych warstw, np. router będzie urządzeniem warstwy 3, przełącznik, most i karta sieciowa są urządzeniami warstwy 2.

<table>
<tr><td>Warstwa aplikacji</td><td></td><td></td><td></td></tr>
<tr><td>Warstwa prezentacji</td><td></td><td></td><td></td></tr>
<tr><td>Warstwa sesji</td><td></td><td></td><td></td></tr>
<tr><td>Warstwa transportowa</td><td></td><td></td><td></td></tr>
<tr><td>Warstwa sieciowa</td><td>Warstwa sieciowa</td><td></td><td></td></tr>
<tr><td>Warstwa łącza danych</td><td>Warstwa łącza danych</td><td>Warstwa łącza danych</td><td></td></tr>
<tr><td>Warstwa fizyczna</td><td>Warstwa fizyczna</td><td>Warstwa fizyczna</td><td>Warstwa fizyczna</td></tr>
<tr><td>Brama</td><td>Router</td><td>Przełącznik, most, karta sieciowa</td><td>Koncentrator, regenerator</td></tr>
</table>

Rys. 12.2. **Zasięg danych w urządzeniach**

> **! UWAGA**
>
> W ofercie różnych producentów można spotkać również **przełączniki warstwy trzeciej** – przełączniki routujące (ang. *switch layer 3, routing switch*). Są to urządzenia – podobnie jak router – przekazujące pakiety, tyle że za pomocą specjalnych układów scalonych **ASIC** (ang. *Application Specific Integrated Circuit*), natomiast w routerach przełączanie pakietów odbywa się programowo, z wykorzystaniem mikroprocesora. Przełącznik warstwy trzeciej jest zazwyczaj szybszy w działaniu niż router, lecz nie wykonuje wszystkich funkcji routera i ma mniejsze możliwości konfiguracji.

Zalety modelu OSI:
- pozwala podzielić zadania sieciowe na części łatwiejsze do analizy;
- 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 – jak może się wydawać – komunikuje się bezpośrednio z odpowiadającą jej aplikacją uruchomioną na innym komputerze, to ta komunikacja nie jest bezpośrednia. W celu przekształcenia danych i dostarczenia ich do miejsca docelowego aplikacja wywołuje funkcje oferowane przez warstwę prezentacji. Podobnie warstwa prezentacji lokalnego systemu wirtualnie porozumiewa się z warstwą prezentacji systemu zdalnego, a w rzeczywistości wywołuje funkcje warstwy sesji pozwalające na sterowanie sesją i na dostarczenie danych do warstwy prezentacji systemu zdalnego. Tego rodzaju wirtualna komunikacja zachodzi na poziomie każdej warstwy, oprócz fizycznej, na której poziomie dwa urządzenia są połączone za pomocą określonego nośnika i kontaktują się rzeczywiście (fizycznie).

Model OSI to podstawowy model komunikacji sieciowej. Jest on najlepszym narzędziem służącym do nauki wysyłania i odbierania danych w sieci. Pozwala obserwować funkcje poszczególnych warstw sieci. Model OSI traktuje się jako model odniesienia (wzorzec) dla większości rodzin protokołów komunikacyjnych. Jest on otwarty, co oznacza, że każdy może z niego korzystać bez wnoszenia opłat licencyjnych.

12.3. 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 powszechnie stosuje się m.in. w internecie. Podobnie jak w modelu OSI, można w nim wyróżnić warstwy, jednak funkcje są różne, mimo że niektóre z nich mają 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 bądź 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, m.in.: HTTP, FTP, TELNET, SSH, SMTP, POP3.

Podstawowym zadaniem **warstwy transportowej** jest zapewnienie komunikacji między programami użytkownika. Może ona zarządzać przepływem informacji i zapewniać niezawodność przesyłania przez porządkowanie segmentów danych i retransmisję uszkodzonych lub zagubionych segmentów. W komputerze może działać wiele aplikacji wymieniających dane w sieci z wykorzystaniem **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 tej warstwie działają **protokół połączeniowy TCP** i **protokół bezpołączeniowy UDP**.

Warstwa internetowa przyjmuje segmenty z warstwy transportowej razem z informacjami identyfikującymi odbiorcę. Jej zadaniem 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 i dodaje nagłówek zawierający m.in. adresy IP nadawcy i odbiorcy. Na podstawie adresu IP miejsca docelowego podejmuje się decyzję, 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. Ten proces określa się jako **trasowanie** lub **routing**. Warstwa zajmuje się także pakietami przychodzącymi: sprawdza ich poprawność i stwierdza za pomocą algorytmu trasowania, czy należy je przesłać dalej, czy też przetwarzać na miejscu. W pakietach adresowanych do maszyny lokalnej oprogramowanie tej warstwy usuwa nagłówek pakietu i wybiera protokół transportowy, który go będzie dalej obsługiwał. Warstwa 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 i adresuje dane do podsieci, na podstawie adresów fizycznych. Zapewnia sprawdzanie błędów przesyłu danych za pomocą sumy kontrolnej ramki.

Na rys. 12.3 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></td></tr>
<tr><td>Warstwa sieciowa</td><td>Warstwa internetowa</td><td colspan="2">IP, ICMP, IGMP, RIP, OSPF, BGP</td><td>ARP</td></tr>
<tr><td>Warstwa łącza danych</td><td rowspan="2">Warstwa dostępu do sieci</td><td colspan="3" rowspan="2"></td></tr>
<tr><td>Warstwa fizyczna</td></tr>
</table>

Rys. 12.3. Porównanie modelu OSI i TCP/IP

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

adresu wykorzystuje się protokół ARP. Gdy komputer potrzebuje 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: przesyła 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 komunikować za pośrednictwem adresu fizycznego tylko w obrębie danej sieci lokalnej (w warstwie drugiej modelu OSI). Jeśli jakieś informacje mają być przesłane do innej sieci, to protokół ARP wykorzystuje się do uzyskania informacji o adresie bramy sieciowej. Na rys. 12.4 przedstawiono zawartość tablicy ARP komputera, który komunikował się z innymi urządzeniami. Protokół odwrotny **RARP** (ang. *Reverse Address Resolution Protocol*) pozwala na ustalenie adresu IP na podstawie adresu fizycznego MAC.

```
WybierzWiersz polecenia
C:\Users\kp>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\kp>arp -a

Interface: 169.254.58.11 --- 0xd
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  238.38.68.61          01-00-5e-26-44-3d     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.1.3 --- 0xf
  Internet Address      Physical Address      Type
  192.168.1.11          00-22-15-17-c8-a9     dynamic
  192.168.1.100         00-11-32-0b-0f-80     dynamic
  192.168.1.254         00-12-2a-b7-be-d1     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  238.38.68.61          01-00-5e-26-44-3d     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Rys. 12.4. Tablica ARP komputera

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skorzystaj z metody opisanej w rozdziale i 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 maksymalnych całkowitych rozmiarach pakietu i ramki Ethernet.
3. Na podstawie opisu funkcji podaj nazwę odpowiedniej warstwy modelu OSI (transportu, prezentacji, aplikacji, sesji, fizyczna):
   a) Zarządza przebiegiem komunikacji między aplikacjami działającymi w komputerach danej sieci.
   b) Określa specyfikację interfejsu wykorzystywanego przez aplikacje do przesyłania danych w sieci.
   c) Odpowiada za przetworzenie danych pochodzących z warstwy aplikacji do postaci zrozumiałej przez warstwy niższe.
   d) Odpowiada za transmisję danych między składnikami sieci.
   e) Zapewnia transport danych od nadawcy do odbiorcy.

13 Protokoły warstwy łącza danych

ZAGADNIENIA

Wersje Ethernetu **Budowa ramki w sieci Ethernet** **Zasady oznaczania nośników w sieci Ethernet** **Standardy ustalania kolejności kabli w złączu RJ-45** **Typy kabli wykorzystywane do łączenia urządzeń** **Kolizje i domeny kolizyjne** **Ograniczanie liczby kolizji** **Zmniejszanie rozmiaru domeny rozgłoszeniowej**

13.1. Standard Ethernet

Podstawowym standardem wykorzystywanym w budowie sieci lokalnych jest **Ethernet**. Został on opisany 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 dzieli się na fragmenty, nazywane **ramkami**. Budowę ramki Ethernet przedstawiono na rys. 13.1.

7	1	6	6	2	46-1500	4
Preambuła	SFD	MAC odbiorcy	MAC nadawcy	Typ ramki/ długość	Dane	FCS

Rys. 13.1. Budowa ramki Ethernet

W kolejnych polach ramki zawarto takie elementy, jak:

- preambuła – 7 bajtów złożonych z naprzemiennych jedynek i zer, pozwalających na szybką synchronizację odbiorników;
- SFD (ang. *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, są uzupełniane zerami;
- suma kontrolna FCS (ang. *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 przeciwnym razie ramka jest odrzucana.

W sieciach Ethernet mogą być stosowane różne rodzaje nośników, charakteryzujących się różnymi prędkościami przesyłania danych. Ogólny schemat oznaczania prędkości przesyłania danych i 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** (ang. *baseband*);
  - Broad – **transmisja szerokopasmowa** z wykorzystaniem częstotliwości nośnej (ang. *broadband*);
- rodzaj zastosowanego medium:
  - 2 – cienki kabel koncentryczny (ang. *thin Ethernet*);
  - 5 – gruby kabel koncentryczny (ang. *thick Ethernet*);
  - T – skrętka (ang. *twisted pair*);
  - F – światłowód (ang. *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 m;
- 10BaseT – długość kabla ograniczona do 100 m, litera T symbolizuje skrętkę jako nośnik fizyczny.

Najczęściej stosowane nośniki danych dla sieci Fast Ethernet:

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

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 100 km).

Najpopularniejszym medium transmisyjnym stosowanym w budowie sieci komputerowych jest **skrętka**. Kabel składa się z czterech skręconych par przewodów, oznakowanych za pomocą kolorów izolacji. Każdy tego typu kabel jest zakończony wtyczką typu RJ-45. Kolejność przewodów we wtyku jest określona za pomocą standardów TIA/ EIA 568A i TIA/EIA 568B (tabela 13.1).

Tabela 13.1. **Kolejność przewodów we wtyku RJ-45**

PIN	Kolor według standardu	
	TIA/EIA 568A	TIA/EIA 568B
1	biało-zielony	biało-pomarańczowy
2	zielony	pomarańczowy

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

Do łączenia urządzeń stosuje się dwa rodzaje kabli:

- **prosty** (ang. *straight-through*) – wtyki na obu końcach są wykonane według jednego standardu. Stosuje się go do łączenia urządzeń różnego typu, np. komputera z przełącznikiem lub z koncentratorem i routera z przełącznikiem lub z koncentratorem;
- **skrosowany** (ang. *crossover*) – wtyk na jednym końcu jest wykonany według standardu 568A, a na drugim zgodnie ze standardem 568B. Kable tego rodzaju stosuje się do łączenia urządzeń tego samego typu, np. komputera z komputerem, przełącznika lub koncentratora z przełącznikiem lub z koncentratorem, komputera z routerem.



Rys. 13.2. **Wtyczka RJ-45**

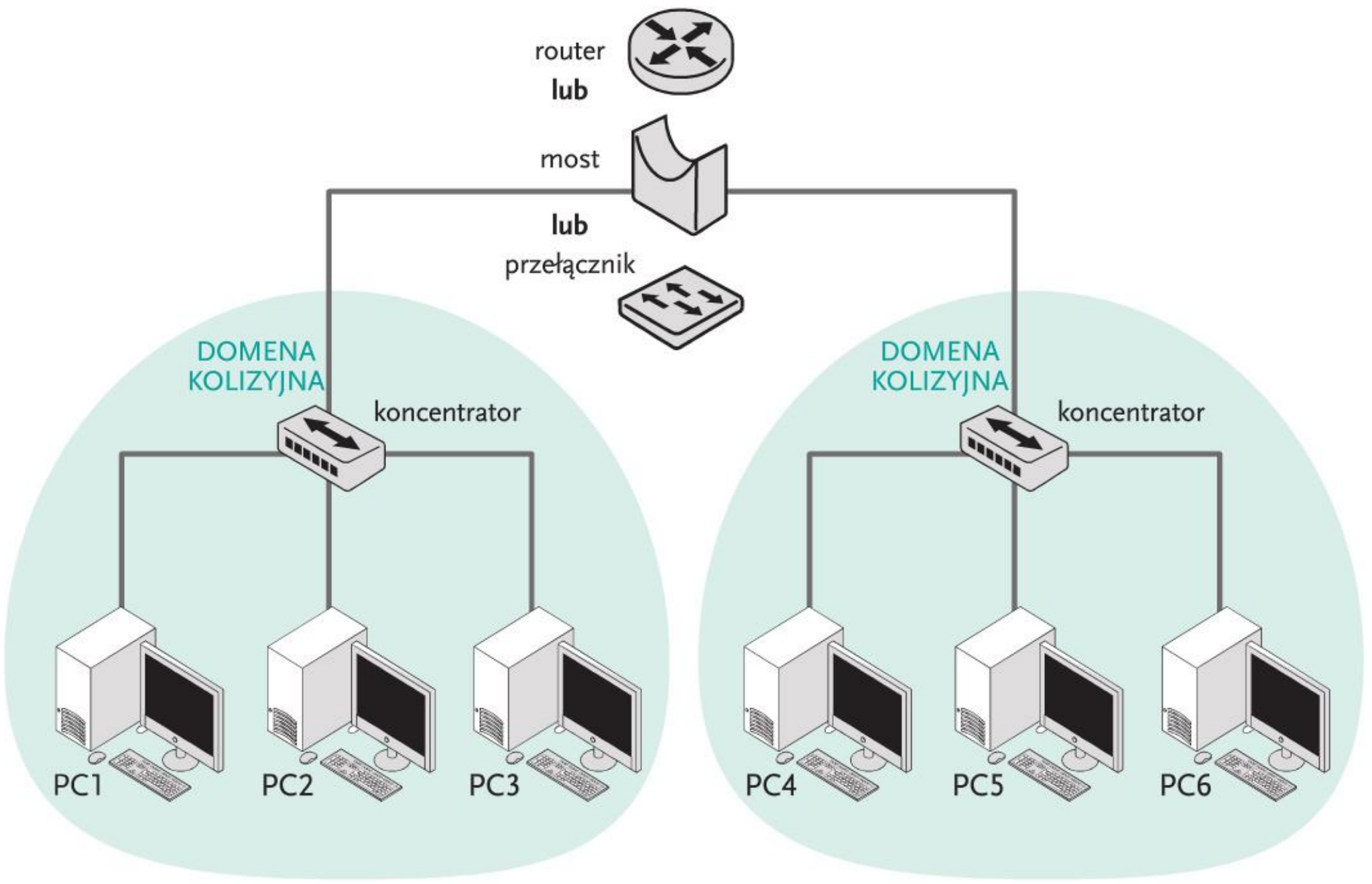
Większość nowoczesnych urządzeń sieciowych jest wyposażona w funkcję **Auto MDI/MDIX** (ang. *automatic MDI/MDIX crossover*). Ta funkcja polega na automatycznym rozpoznaniu przez to urządzenie, czy podłączony kabel sieciowy jest prosty czy skrosowany. Dzięki niej do portu takiego urządzenia można podłączyć zarówno kabel prosty, jak i skrosowany. W starszych urządzeniach stosowano specjalne porty typu uplink (zazwyczaj współdzielone z portem pierwszym) lub ręczne przełączniki normal/uplink, umożliwiające wewnętrzne „skrosowanie" portu. Wtyczkę RJ-45 przedstawiono na rys. 13.2.

13.2. 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, którą realizują dwa urządzenia lub więcej 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 można ich uniknąć. Obszar sieci, w którym może dojść do kolizji danych nadawanych przez różne stacje, nazywa się **domeną kolizyjną** (ang. *collision domain*). W domenie kolizyjnej maksymalna

liczba urządzeń wynosi 1024, lecz im jest ich więcej, tym prawdopodobieństwo wystąpienia kolizji jest większe. Ryzyko wystąpienia kolizji można ograniczyć przez odpowiednie zaprojektowanie sieci i stosowanie urządzeń ograniczających wielkość domen kolizyjnych, takich jak mosty, przełączniki lub routery.

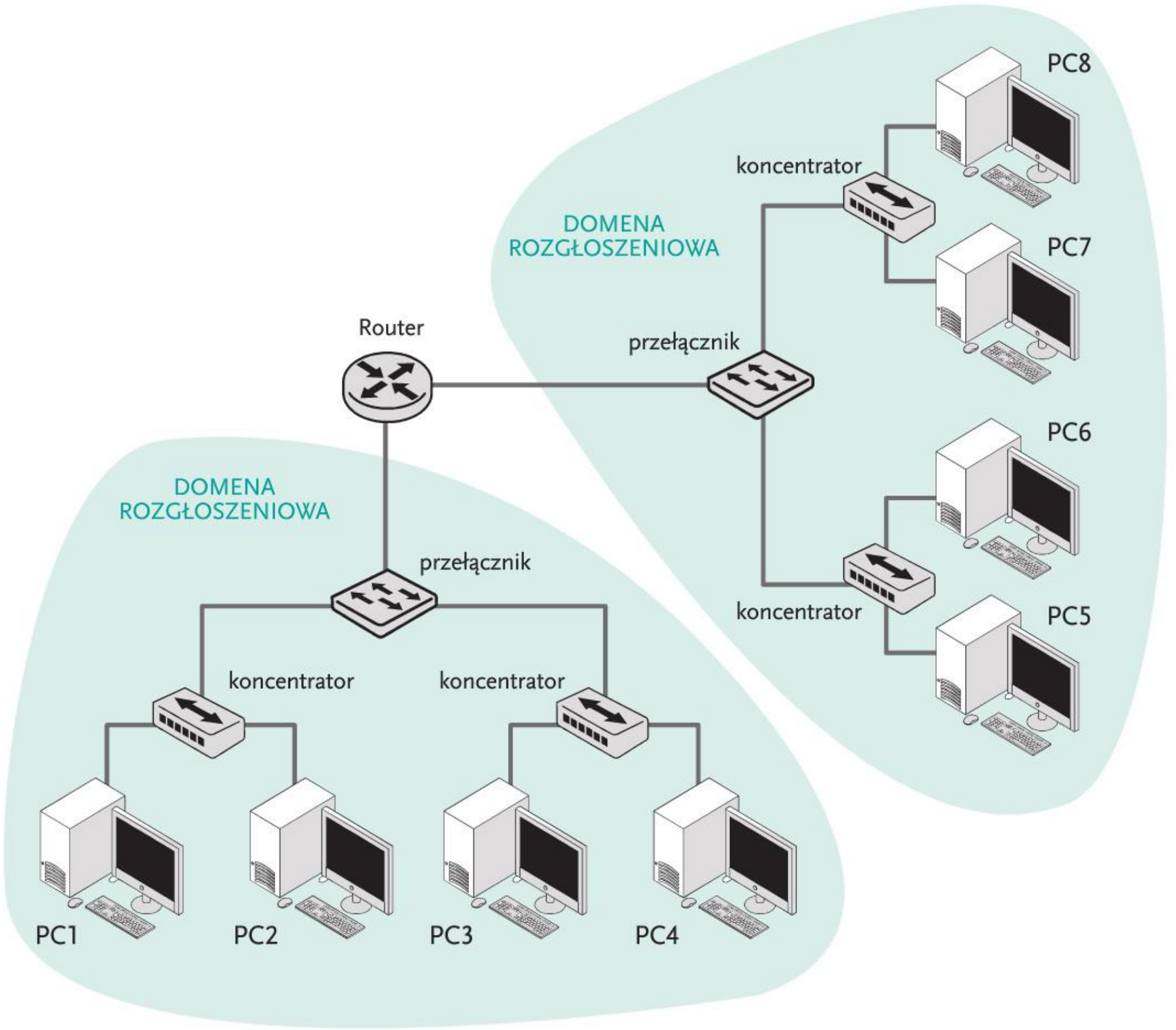
Efektywne projektowanie sieci prowadzi do organizacji struktury sieci w taki sposób, aby domeny kolizyjne były jak najmniejsze. Urządzenia, takie jak przełącznik, most lub router, pozwalają na zmniejszenie obszaru domeny kolizyjnej. Transmisje realizowane między urządzeniami w obrębie domeny kolizyjnej nie są przesyłane przez mosty, przełączniki i routery do innych domen. Jeżeli komputer PC1 (rys. 13.3) 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.



Rys. 13.3. Podział sieci na domeny kolizyjne

W sieci mogą być również przesyłane komunikaty rozgłoszeniowe. Obszar sieci, w którym następuje emisja komunikatu rozgłoszeniowego wysyłanego przez jedną stację do wszystkich innych, nazywa się **domeną rozgłoszeniową** (ang. *broadcast domain*). Urządzenia warstwy pierwszej (koncentrator i wzmacniak) i warstwy drugiej (most i przełącznik) przekazują ruch rozgłoszeniowy. Te urządzenia rozszerzają domenę rozgłoszeniową, natomiast urządzenia warstwy trzeciej (np. router) ograniczają jej rozmiar. Rozmiar domeny rozgłoszeniowej można ograniczyć również przez zdefiniowanie sieci **wirtualnych VLAN** (ang. *Virtual Local Area Network*).

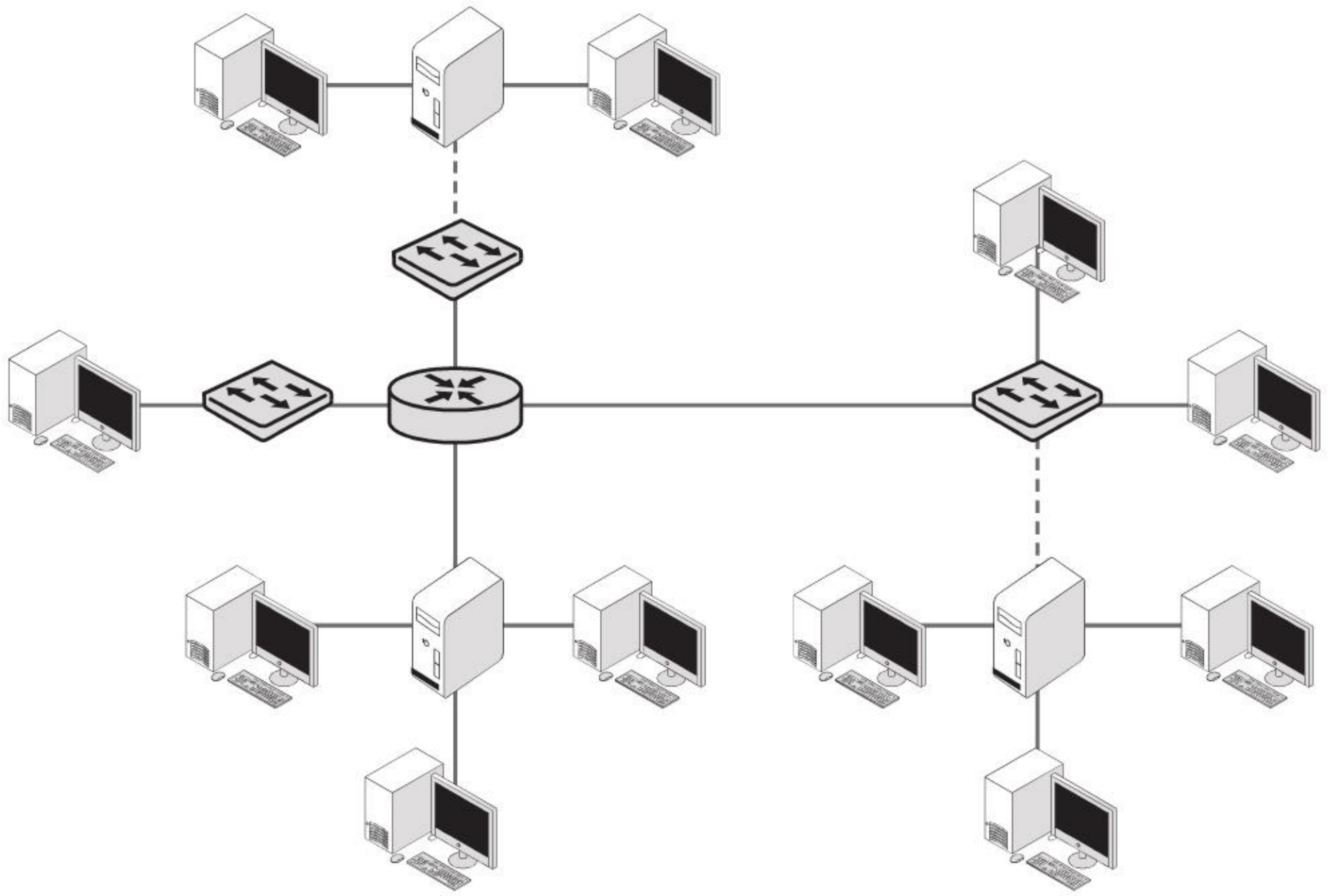
Komunikacja między sieciami wirtualnymi musi się odbywać za pośrednictwem routera (urządzenia warstwy trzeciej). Komunikaty rozgłoszeniowe wysyłane przez komputer, np. PCl, będą docierać tylko do komputerów PC2, PC3 i PC4. Przesyłanie ich do pozostałych komputerów w sieci zostanie zablokowane przez router (rys. 13.4).



Rys. 13.4. **Podział sieci na domeny rozgłoszeniowe**

SPRAWDŹ SWOJĄ WIEDZĘ

1. Sprawdź, według którego standardu wykonano kabel, którym twój komputer jest podłączony do sieci.
2. Narysuj schemat sieci w twojej szkole. Oblicz liczbę domen kolizyjnych i rozgłoszeniowych.
3. Ile domen kolizyjnych i rozgłoszeniowych widać na rys. 13.5?



Rys. 13.5. **Podział na domeny**

14 Protokoły warstwy sieci

ZAGADNIENIA

Funkcje protokołu IP **Budowa nagłówka pakietu IP** **Tablica routingu** **Protokoły routingu** **Przykładowe protokoły routingu i zasada ich działania** **Rozsyłanie grupowe informacji**

14.1. Protokół IP

Protokół IP jest odpowiedzialny za przesyłanie pakietów między użytkownikami sieci. To protokół bezpołączeniowy, 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.

Podstawowe funkcje protokołu IP to:

- 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 odkryto 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 wykorzystuje się do transportu danych między urządzeniem źródłowym a urządzeniem docelowym. Budowę nagłówka przedstawiono na rys. 14.1.

1 bajt		2 bajt	3 bajt	4 bajt
Wersja	Dł. Nag.	Typ usług	Całkowita długość pakietu	
Identyfikacja			Flagi	Przesunięcie fragmentu
Czas życia		Protokół	Suma kontrolna	
Adres źródłowy				
Adres docelowy				
Opcje				
Dane				

Rys. 14.1. Budowa nagłówka protokołu IP

Znaczenie wybranych pól nagłówka:

- **Czas życia** (ang. *Time To Live*, **TTL**) – 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 zostać przekazany do bramy łączącej sieci. Decyzję o wyborze trasy podejmuje router na podstawie adresu IP urządzenia docelowego, umieszczonego w nagłówku pakietu, i na podstawie informacji posiadanych w **tablicy routingu**. W tej tablicy 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 z wykorzystaniem **trasy domyślnej** (jeżeli ją zdefiniowano) lub pakiet jest kasowany. Przykładową tablicę routingu przedstawiono na rys. 14.2.

```
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. 14.2. **Przykładowa tablica routingu**

Z tej tablicy 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` będą wysyłane interfejsem Serial0.

14.2. 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 informacji o trasach lub topologii sieci. Na podstawie tych informacji

ustala się optymalne trasy prowadzące do poszczególnych sieci i umieszcza się te trasy w tablicy routingu. Przykładami protokołów routingu są RIP, OSPF, IGRP, EIGRP.

Protokół **RIP** (ang. *Routing Information Protocol*) jest protokołem wykorzystującym **algorytm wektora odległości** (ang. *distance-vector*). Ze względu na niskie wymagania sprzętowe może być używany przez wszystkie routery. Router, na którym uruchomiono protokół RIP, wysyła do swoich bezpośrednich sąsiadów zawartość swojej tablicy routingu w określonych, stałych przedziałach czasu, standardowo co trzydzieści sekund. Po przyjęciu aktualizacji od sąsiada router porównuje ją z własną tablicą routingu i w razie konieczności ją uaktualnia. W tablicy routingu znajdują się najlepsze trasy do wszystkich sieci. Jako **miarę jakości trasy** (metrykę) w protokole RIP przyjęto **liczbę przeskoków** (ang. *hops*) między routerami, które pakiet musi wykonać, aby dotrzeć do celu. Gdy router przyjmie uaktualnienie tablicy routingu zawierające 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, tzn. takich, w których wszystkie łącza mają jednakową przepustowość.

Protokół **OSPF** (ang. *Open Shortest Path First*) jest (podobnie jak RIP) protokołem otwartym, co oznacza, że jego specyfikacja jest ogólnie dostępna. To protokół **routingu stanu łącza** (ang. *link-state*), wykorzystujący **algorytm SPF** (algorytm Dijkstry) do obliczania najkrótszych ścieżek. Metryką w protokole OSPF jest koszt, który wiąże się z przepustowością łączy (im większa przepustowość, tym niższy koszt). Protokół OSPF jest przeznaczony do dużych sieci. Taka sieć może być podzielona na obszary. Routery w danym obszarze, na których uruchomiono protokół OSPF, wymieniają się wzajemnie krótkimi komunikatami **LSA** (ang. *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 zostać dołączony do obszaru 0 (szkieletowego), co pozwala na połączenie sieci w całość. Zmiany przeprowadzone w jednym z obszarów nie powodują konieczności uruchomienia algorytmu SPF w pozostałych. 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** (ang. *Interior Gateway Routing Protocol*) i jego następcę **EIGRP** (ang. *Extended IGRP*) opracowała firma 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 ma cechy algorytmów routingu z wykorzystaniem wektora odległości i według stanu łącza. Protokół EIGRP do wyznaczania tras stosuje algorytm **DUAL** (ang. *Diffusing Update Algorithm*). Zaleca się go do stosowania przez CISCO.

Współcześnie liczba routerów w internecie jest tak duża, że żaden z nich nie zdołałby przechowywać tras do wszystkich sieci. Aby temu zapobiec i ułatwić zarządzanie w internecie, wprowadzono hierarchię routingu. Największą jednostką w hierarchii jest system **autonomiczny AS** (ang. *Autonomous System*), który jest zbiorem sieci pod wspólną administracją, z ustaloną wspólną strategią routingu. System AS można podzielić na pewną liczbę **obszarów** (ang. *areas*), które są grupami sąsiednich sieci i przyłączonych hostów. Poszczególne obszary są sprzęgane przez **routery graniczne obszaru** (ang. *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** (ang. *Interior Gateway Protocol*) i mogą działać wewnątrz systemu autonomicznego. Do ustalania tras między systemami autonomicznymi wykorzystuje się **zewnętrzne protokoły routingu EGP** (ang. *Exterior Gateway Protocol*), np. protokół BGP.

14.3. Rozsyłanie grupowe informacji

Normalna komunikacja z wykorzystaniem protokołu IP odbywa się między jednym nadawcą a jednym odbiorcą (jeśliby nie liczyć pakietów rozgłoszeniowych). Dla niektórych aplikacji użyteczne okazuje się **rozgłaszanie grupowe** (ang. *multicasting*), czyli 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 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** (ang. *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 multicastowej.

Dane są przesyłane na specjalne adresy multicastowe określające grupę, która jest zainteresowana konkretnym typem danych. Wszystkie multicastowe adresy IP[2] mieszczą się w zakresie od **224.0.0.0** do **239.255.255.255**. Ten zakres określa tylko grupę odbiorców, nadawcy mają zawsze adres unicastowy. Adresy w zakresie od **224.0.0.0** do **224.0.0.255** zarezerwowano dla protokołów w sieciach lokalnych i nie mogą być przekazywane przez routery, np. adresy **224.0.0.5** i **224.0.0.6** są wykorzystywane 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 i przez internet. Część z nich zarezerwowano dla niektórych aplikacji, np. **224.0.1.1** – dla protokołu NTP (ang. *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. 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 odbywa się za pomocą zapytań o członkostwo hosta, które są kierowane 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. Ten pakiet zawiera adres IP pożądanej grupy. Przyłączenie hosta do grupy obejmuje dwa procesy u klienta:

- host wysyła powiadomienie do routera, że chce przyłączyć się do odpowiedniej grupy;
- host wiąże dynamicznie IP z adresem grupowym zarezerwowanym dla danej aplikacji i z zarezerwowanym adresem Ethernet.

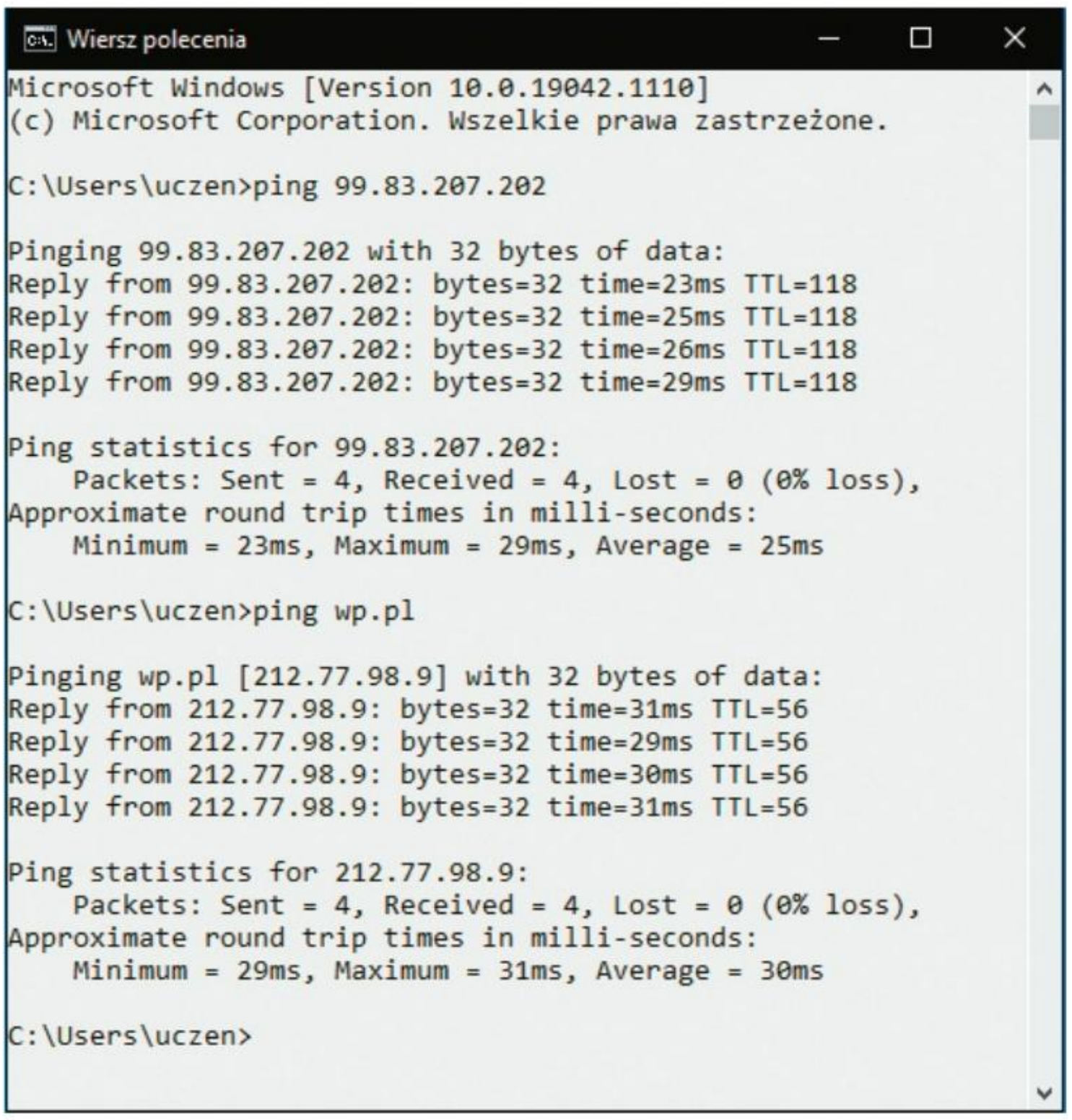
Host, który podłączy się do nowej grupy multicastowej, ma obowiązek wysłać natychmiastowy raport do tej grupy, bez czekania na zapytanie od routera. Aby korzystać z transmisji multicastowych, należy dysponować odpowiednią aplikacją obsługującą ten rodzaj transmisji.

[2] Więcej informacji o adresach IP w rozdziale 15.

14.4. Protokół ICMP

Ściśle związany z protokołem IP jest protokół **ICMP** (ang. *Internet Control Message Protocol*). Protokół IP, jako bezpołączeniowy, nie ma mechanizmów informowania o błędach w funkcjonowaniu sieci IP i diagnostyki sieci. Do tego celu przeznaczono protokół ICMP. Umożliwia on przesyłanie między komputerami lub routerami informacji o błędach występujących w funkcjonowaniu sieci IP. Najczęściej używanymi poleceniami korzystającymi z protokołu ICMP są **ping** i **tracert**.

Ping 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 i czasu potrzebnego na ich transmisję. Ping wysyła pakiety żądania echa ICMP (ang. *echo request*) i odbiera **odpowiedzi na żądanie echa ICMP** (ang. *echo reply*). Jako argument dla polecenia ping można podać adres IP lub nazwę domenową komputera testowanego (rys. 14.3).



Rys. 14.3. **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 wysyła pakiet żądania echa z **polem TTL** ustawionym na kolejne wartości, od 1 do 30. Wartość TTL jest zmniejszana podczas

przechodzenia 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 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 przedstawiono na rys. 14.4.

```
Wiersz polecenia
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\uczen>tracert onet.pl

Tracing route to onet.pl [99.83.207.202]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     1 ms    <1 ms    <1 ms  192.168.0.1
  3    14 ms     7 ms    12 ms  100.95.0.1
  4     6 ms    12 ms    12 ms  172.25.145.1
  5    26 ms    28 ms    21 ms  172.17.0.10
  6    23 ms    23 ms    24 ms  172.17.64.2
  7    26 ms    25 ms    25 ms  172.17.64.2
  8    43 ms    26 ms    23 ms  99.83.65.250
  9    45 ms    31 ms    32 ms  52.93.18.191
 10    27 ms    29 ms    26 ms  aafc88a28d9997374.awsglobalaccelerator.com [99.83.207.202]

Trace complete.

C:\Users\uczen>
```

Rys. 14.4. **Działanie programu tracert**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sprawdź, jakiego adresu IP używają komputer, z którego korzystasz w szkole, i twój komputer 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 (np.: Wirtualnej Polski, Onetu, Ministerstwa Edukacji i Nauki).
4. Sprawdź czas odpowiedzi serwera witryny firmy Cisco.
5. Wyszukaj, do czego służą polecenia: **`pathping`**, **`netstat`** i **`net view`**. Przetestuj ich działanie i uzasadnij odpowiedź.

15 Adresowanie w sieci komputerowej

ZAGADNIENIA

Rodzaje adresów używanych w sieciach komputerowych Budowa i reprezentowanie adresów MAC i IP Przeliczanie liczb dwójkowych na dziesiątkowe i dziesiątkowych na dwójkowe Klasy adresów IP i adresy specjalne Odpowiedzialność za przydzielanie adresów IP Adresy prywatne i ich zastosowanie NAT i adresy APIPA Metody zapobiegające wyczerpywaniu się dostępnej puli adresów Adresowanie bezklasowe i jego stosowanie Wyznaczanie adresu sieci, adresu rozgłoszeniowego, liczb podsieci i liczb hostów na podstawie adresu IP i maski podsieci Obliczanie, czy komputery będą mogły się komunikować w sieci

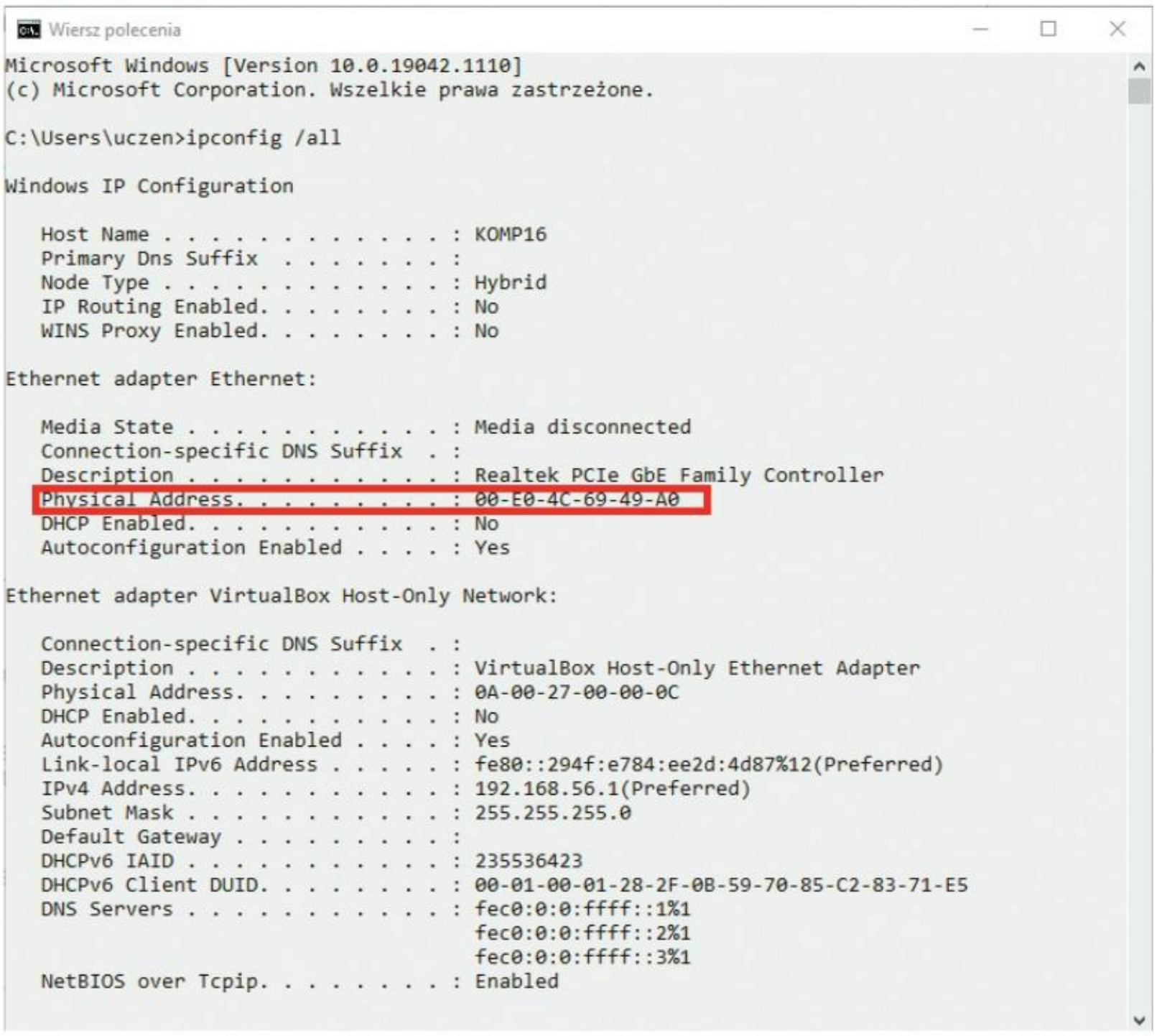
Do sieci komputerowej mogą być podłączone różne urządzenia, np. serwery, komputery, drukarki. Każde z nich musi mieć możliwość wymiany danych z innymi. Aby to było możliwe, jest potrzebny mechanizm pozwalający na zidentyfikowanie każdego urządzenia podłączonego do sieci. Identyfikacja odbywa się za pomocą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

- **fizyczne** – w sieci Ethernet nazywane również adresami MAC;
- **logiczne** – adresy IP.

15.1. Adresy fizyczne

Adres fizyczny jest nadawany przez producenta w każdej **karcie sieciowej NIC** (ang. *NetWork Interface Card*) podczas jej wytwarzania. Ten adres jest niepowtarzalny i umieszczony w pamięci ROM karty. Długość adresu fizycznego w Ethernecie wynosi 48 bitów, lecz jest przedstawiany w zapisie heksadecymalnym (szesnastkowym), np. 00-22-15-17-C8-A9. Na rys. 15.1 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`**.



Rys. 15.1. Wyświetlanie adresu fizycznego karty sieciowej

15.2. Adresy logiczne

Adres logiczny wskazuje punkt przyłączenia do sieci, który nazywa się **interfejsem**. Komputer pracujący w sieci, wyposażony w kilka interfejsów, może mieć kilka adresów logicznych – po jednym dla każdego z tych interfejsów. Ponadto do każdego interfejsu można przypisać wiele adresów. Interfejsy to zwykle urządzenia fizyczne, np. karty sieciowe, ale mogą być nimi również urządzenia logiczne, np. w routerach i niektórych kartach sieciowych tworzy się podinterfejsy.

Adresy logiczne nadaje administrator sieci. Taki adres może określać urządzenie, np. komputer, grupę urządzeń (adres grupowy) lub całą sieć (adres sieci). Może on być przypisany przez administratora lub uzyskany za pośrednictwem specjalnego **serwera DHCP** (ang. *Dynamic Host Configuration Protocol*). Niezależnie jednak od sposobu uzyskania adresu logicznego, w danej sieci nie mogą istnieć dwa urządzenia o takim samym adresie.

Obecnie funkcjonują dwie wersje adresów IP:

- IPv4 – starsza wersja, bardzo rozpowszechniona;
- IPv6 – nowsza wersja, mniej popularna.

15.3. Adresy IPv4

Adres IP w wersji 4 ma zawsze długość 32 bitów. Jest on podzielony na cztery 8-bitowe bloki, zwane **oktetami**. Administratorzy najczęściej przedstawiają adresy w postaci dziesiętnej (notacja dziesiętna z kropkami). Na rys. 15.2 każdy oktet jest zastąpiony liczbą dziesiętną z zakresu 0–255.

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	0	0	0	0	0	1	1
192									168									0									3							

Rys. 15.2. **Adres IP w zapisie binarnym (dwójkowym) i dziesiętnym**

PRZYKŁAD 15.1

Zamiana adresów z postaci dwójkowej na dziesiętną

System komputerowy przetwarza adresy w postaci dwójkowej. Dla człowieka zapamiętanie adresu złożonego z 32 bitów jest prawie niemożliwe. Wygodniej jest posługiwać się adresami, w których każdy oktet zamieniono na liczbę dziesiętną z zakresu od 0 do 255. Na zajęciach z matematyki podawano algorytmy przeliczania liczb dwójkowych na dziesiętne. W tym miejscu przedstawimy inną prostą metodę wykonywania tych obliczeń. Każdemu bitowi należy przypisać jego wartość wynikającą z pozycji w liczbie dwójkowej (rys. 15.3). 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. 15.3. **Przeliczanie liczby dwójkowej na dziesiętną**

PRZYKŁAD 15.2

Zamiana adresów z postaci dziesiętnej na dwójkową

Adres podany w postaci dziesiętnej należy zamieniać na postać dwójkową. Spośród wartości dziesiętnych poszczególnych bitów trzeba wybrać te, których suma jest równa zamienianej liczbie. To zadanie jest dość trudne, dlatego wyjaśnimy je 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.

15.4. Klasy adresów IP

Teoretycznie, gdy mamy do dyspozycji 32 bity, możemy wygenerować 2^{32} (= 4 294 967 296) adresów IP. Adresy IP jednak tak zaprojektowano, aby określić, która część jest związana z adresem całej sieci, a która – z adresem poszczególnych stacji, nazywanych hostami. Adresy IP podzielono na klasy A, B, C, D i E.

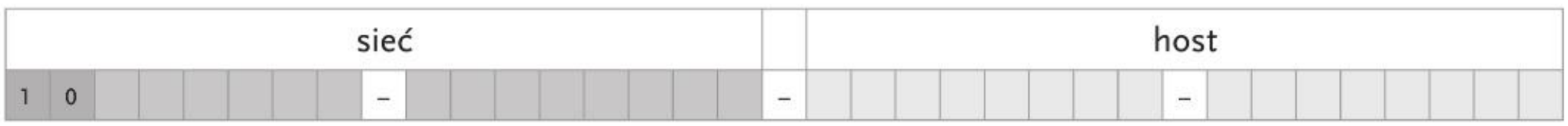
Adresy **klasy A** przeznaczono do obsługi bardzo dużych sieci. Adres sieci zajmuje pierwszy oktet, natomiast adres hosta – pozostałe trzy. Pierwszy bit adresu klasy A jest zawsze równy 0. Ostatnie 24 bity (3 oktety) adresu klasy A są adresem hosta. Podział bitów w adresie klasy A przedstawiono na rys. 15.4.



Rys. 15.4. **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) przeznaczono do innych celów i nie mogą one 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 przedstawiono na rys. 15.5.



Rys. 15.5. **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. Ostatnich 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 przedstawiono na rys. 15.6.



Rys. 15.6. **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 mogą istnieć 2 097 150 sieci klasy C.

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** (ang. *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** (ang. *network address*). Adres, w którym w części przeznaczonej dla hosta znajdują się same jedynki, jest **adresem rozgłoszeniowym** (ang. *broadcast*). Tych adresów nie można przypisać hostom. Ponadto istnieją jeszcze inne specjalne adresy, opisane w tabeli 15.1.

Tabela 15.1. 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 nim samym
255.255.255.255	adres rozgłoszeniowy w sieci lokalnej	komunikacja hosta ze wszystkimi hostami w ramach jednej sieci fizycznej

15.5. 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*). Stowarzyszenie zajmuje się administracyjną i techniczną koordynacją 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). Takie adresy nazywa się **publicznymi**; można je uzyskać w urzędzie IANA lub od dostawcy usług internetowych. W tej drugiej sytuacji otrzymuje się adres z puli przydzielonej 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 niemających 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** (ang. *RIPE Database*), zawierającą dane dotyczące przydzielonych zasobów internetowych.

Adres publiczny IP można uzyskać od dostawcy usług internetowych, z przydzielonej mu puli. Aby umożliwić wszystkim komputerom w danej instytucji, np. w szkole, korzystanie z internetu, należałoby przydzielić każdemu z nich indywidualny adres publiczny. Taka sytuacja byłaby niekorzystna z powodu szybkiego wyczerpania dostępnej puli adresów. Aby rozwiązać ten problem, zarezerwowano pule **adresów prywatnych**. Te adresy można dowolnie stosować w sieciach lokalnych, nie są one natomiast widoczne w internecie. Adresy prywatne mogą się powtarzać w różnych sieciach lokalnych i nie powodować przy tym 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** (ang. *Network Address Translation*). Tłumaczenie adresów odbywa się w bramie internetowej umieszczonej między siecią prywatną a internetem.

W systemach Windows wykorzystuje się usługę **APIPA** (ang. *Automatic Private IP Addressing*). Ta usługa 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 przydziela się 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.

15.6. Zapobieganie wyczerpywaniu się puli adresów

Początkowo sieć komputerowa była zbudowana z kilku komputerów. Dostępna liczba adresów (ponad 4 mld) 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. Przykładowo: jeżeli 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.

15.7. Adresowanie bezklasowe

W celu zapewnienia większej elastyczności w przydzielaniu adresów IP wprowadzono pojęcie **maski podsieci** (ang. *Subnetwork Mask*), oznaczonej skrótem SM. Maska podsieci określa, ile bitów w adresie jest przeznaczonych do identyfikacji **sieci** i **podsieci** (ang. *ID network*), a ile – do identyfikacji **hosta** (ang. *ID host*). Maska podsieci składa się z tej samej liczby bitów co adres IP. W masce w części **sieci** (ang. *ID network*) i **podsieci** (ang. *ID subnetwork*) występują same jedynki (w systemie dwójkowym), a w części **hosta** (ang. *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 15.2.

Tabela 15.2. 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** (ang. *Classless Inter Domain Routing*), informuje o liczbie 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 rys. 15.7.

	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. 15.7. **Podział bitów w adresie sieci bezklasowej**

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

PRZYKŁAD 15.3

Wyznaczanie adresu sieci

Każdy z komputerów, któremu przydzielono adres IP, musi należeć do jakiejś sieci. Aby ustalić, do jakiej sieci należy komputer, konieczne staje się wykonanie obliczeń w systemie dwójkowym. W tym celu należy najpierw przedstawić adres komputera i jego maski podsieci w systemie dwójkowym. Omówimy przykład komputera o adresie **`192.168.0.123`** i masce podsieci **`255.255.255.224`**. Adres komputera w postaci dwójkowej przedstawiono na rys. 15.8, a maski podsieci – na rys. 15.9.

	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. 15.8. **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. 15.9. **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 rys. 15.10:

- przepisz z adresu IP (rys. 15.10, 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	0	0	0	0	0
	192									168									0									96							

Rys. 15.10. **Wyznaczanie adresu sieci**

Komputer należy do podsieci **192.168.0.96**.

PRZYKŁAD 15.4

Wyznaczanie adresu rozgłoszeniowego

Adres rozgłoszeniowy (ang. *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 przedstawimy adres komputera i jego maski podsieci w systemie dwójkowym. Omówimy ten sam przykład: komputer o adresie **192.168.0.123** i masce podsieci **255.255.255.224**. Adres komputera w postaci dwójkowej przedstawiono na rys. 15.8, a maski podsieci – na rys. 15.9.
Jaki jest adres rozgłoszeniowy w tej podsieci?

PORADA

Aby odpowiedzieć na to pytanie, postępuj tak, jak pokazano na rys. 15.11:

- przepisz z adresu IP wszystkie bity na pozycjach, w których w masce podsieci jest wartość 1;
- w pozostałych miejscach wpisz 0.

	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. 15.11. **Wyznaczanie adresu rozgłoszeniowego**

Adres rozgłoszeniowy w tej podsieci to **192.168.0.127**.

PRZYKŁAD 15.5

Obliczanie ilości podsieci

Liczba możliwych do utworzenia podsieci zależy od liczby bitów z części hosta przeznaczonych do utworzenia podsieci. W powyższym przykładzie na podsieci

przeznaczono 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 będą mogły być wykorzystane, 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 zawsze możemy wykorzystać tylko 6. Do obliczenia liczby podsieci można wykorzystać poniższe wzory:

$$n_p = 2^p,$$

gdzie:
n_p – liczba podsieci;
p – liczba bitów przeznaczonych na podsieć.

$$n_{pef} = 2^p - 2,$$

gdzie:
n_{pef} – liczba podsieci efektywnych;
p – liczba bitów przeznaczonych na podsieć.

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

PRZYKŁAD 15.6

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. Te adresy są zarezerwowane i nie wolno ich przypisać do żadnego urządzenia w sieci. Oznacza to, że w omawianej podsieci może być maksymalnie 30 hostów.
Do obliczenia liczby hostów można wykorzystać poniższy wzór:

$$n_h = 2^h - 2,$$

gdzie:
n_h – liczba hostów;
h – liczba bitów przeznaczonych na hosta.

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 15.7

Przydzielanie adresów IP

W tabeli 15.3 zebrano wszystkie informacje o adresach w sieci analizowanej we wcześniejszym przykładzie.

Tabela 15.3. **Adresy IP w podsieciach**

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).

Postępuj tak jak w omówionym przykładzie i wypisz w tabeli wszystkie informacje o adresach w sieci **`192.168.16.0`** z maską **`255.255.255.240`**.

PRZYKŁAD 15.8

Sprawdzanie komunikacji między komputerami

Komputery będą mogły bezpośrednio się komunikować, jeżeli znajdą się w tej samej sieci, tzn. będą miały taki sam adres sieci i jednakową maskę 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 przykładzie 15.3 – wyznaczyć i porównać adresy sieci obu komputerów. Przykładowo: weźmy dwa komputery, którym przydzielono adresy – odpowiednio – **`10.20.30.40`** i **`10.20.30.140`** oraz maskę podsieci **`255.255.255.240`**. Na rys. 15.12 przedstawiono sposób obliczania adresu sieci komputera o adresie **`10.20.30.40`**.

IP	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
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	1	0	0	0	0
	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. 15.12. **Wyznaczanie adresu sieci komputera o adresie IP 10.20.30.40**

Na rys. 15.13 przedstawiono sposób obliczania adresu sieci komputera o adresie **10.20.30.140**.

IP	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
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	1	0	0	0	0
	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									128							

Rys. 15.13. **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 sześciu 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 adres rozgłoszeniowy dla wszystkich podsieci;
   - adresy IP, które będą przypisane do komputerów w poszczególnych podsieciach;
   - maksymalną liczbę podsieci w szkole;
   - maksymalną liczbę komputerów w podsieci.
2. Przekształć podane adresy IP na postać binarną, a następnie określ klasę adresu:
   a) **145.32.59.24**
   b) **200.42.129.16**
   c) **191.107.2.10**

16 Zasady projektowania adresacji IP

ZAGADNIENIA

Reguły obowiązujące podczas przydzielania adresów w sieci **Cel stosowania podsieci o zmiennej długości maski** **Efektywne zarządzanie 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 trzeba 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** (ang. *Variable Length Subnet Mask*). Ta technika 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 16.1

Projektowanie sieci z wykorzystaniem techniki VLSM

Sieć (rys. 16.1) obejmuje pięć miast: Sieradz i Łódź (po 10 komputerów w podsieci), Warszawa, Wrocław i Poznań (po 25 komputerów w podsieci). Należy przydzielić każdej podsieci odpowiednią liczbę adresów IP z puli adresów klasy C, np. `192.168.1.0` z maską `255.255.255.0`.

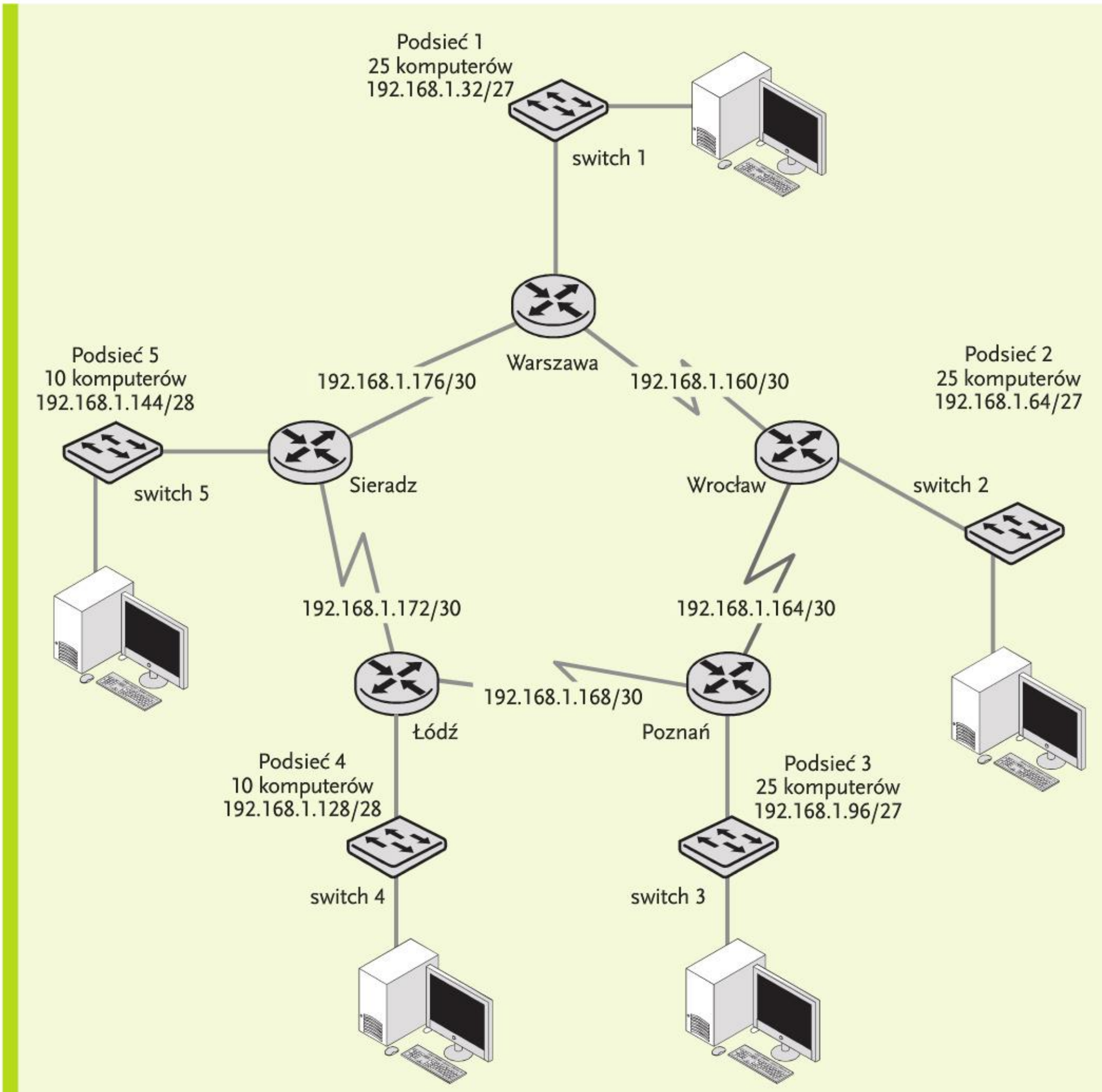
Liczba komputerów w największej podsieci wynosi 25. Na część hosta należy więc przeznaczyć 5 bitów. Na adres podsieci pozostają 3 bity, co pozwala na efektywne zaadresowanie 6 podsieci. Zastosowanie jednakowej maski do wszystkich podsieci powoduje, że w każdej podsieci pozostaną niewykorzystane adresy, 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 przedstawiono w tabeli 16.1.

Tabela 16.1. **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. 16.1. **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 siedem 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 i schemat z maskami o zmiennej długości. Podaj adresy sieci i rozgłoszeniowe oraz zakresy dopuszczalnych adresów dla każdej podsieci.

17 Adresowanie IPv6

ZAGADNIENIA

Cel wprowadzenia protokołu IPv6 **Reprezentowanie adresów IPv6** **Typy adresów obsługiwane przez 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 (ang. *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 specyfikację opisano 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 jest reprezentowany za pomocą 4-cyfrowej liczby szesnastkowej, np. adres:

```
0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010
```

jest reprezentowany:

```
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
```

Reprezentację IPv6 można uprościć przez usunięcie poprzedzających zer z każdego 16-bitowego bloku. W tym uproszczeniu każdy blok musi mieć 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. Jeżeli pomija się 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 używa się trzech typów 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 są rozróżniane zakresy adresów:

- **adresy lokalne dla łącza** (ang. *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. Te adresy mają prefiks **`FE80::/10`**. Każdy interfejs musi mieć przydzielony co najmniej jeden adres lokalny dla łącza, nawet jeżeli ma adres globalny lub unikatowy adres lokalny. Ten zakres odpowiada zakresowi APIPA w IPv4 (**`169.254.0.0/16`**).
- **unikalne adresy lokalne** (ang. *unique local adress*) – adresy będące odpowiednikami adresów prywatnych z protokołu IPv4. Mają prefiks **`FC00::/7`**.
- **adresy globalne** (ang. *global unicast address*) – będące odpowiednikami adresów publicznych z protokołu IPv4. Te adresy to wszystkie inne niewymienione we wcześniejszych punktach.

W protokole IPv6 zdefiniowano również adresy specjalne, np.:

- **`::/128`** – adres nieokreślony (zawierający same zera);
- **`::1/128`** – pętla zwrotna (ang. *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.

Pulę adresów IPv6 podzielono w sposób przedstawiony w tabeli 17.1.

Tabela 17.1. **Podział puli adresów IPv6**

Prefiks	Zasięg	Opis
`::/128`	nieokreślony	adres nieokreślony
`::/0`	globalny	adres trasy domyślnej w routingu (ang. *default*)
`::1/128`	interfejsu	adres loopback odpowiednik adresu IPv4 **`127.0.0.1`**
`2000::/3`	globalny	adresy unicastowe
`FC00::/7`	lokalny	nieroutowalne adresy prywatne odpowiednik adresów IPv4 **`10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/24`**
`FE80::/10`	lokalny	adresy autokonfiguracji łącza
`FF00::/8`	określony w adresie	adresy multicastowe

Adresy IPv6 mają zdefiniowany **zasięg** (ang. *scope*), określający, jakiej części sieci ten adres dotyczy. Zasięg określa się na podstawie czterech najmniej znaczących bitów pierwszego bloku liczb szesnastkowych w adresie (ostatnia cyfra). Dla adresów multicastowych zdefiniowano zasięgi przedstawione w tabeli 17.2.

Tabela 17.2. **Zasięg multicastowych adresów IPv6**

Wartość	Zasięg	Opis
0×1	interface-local scope	adres o zasięgu interfejsu, np. adres loopback `::1/128`
0×2	link-local scope	adres o zasięgu segmentu sieci lokalnej (do najbliższego routera), np. adresy autokonfiguracji łącza `fe80::/10`
0×4	admin-local scope	adres o najmniejszym administracyjnie wyznaczonym zasięgu
0×5	site-local scope	adres o zasięgu wyznaczonym administracyjnie, np. oddział firmy
0×8	organization-local scope	adres o zasięgu wyznaczonym administracyjnie dla całej organizacji (firmy)
0×E	global scope	adres o zasięgu globalnym

Rzeczywisty zasięg i wykorzystanie adresów typu admin-local, site-local i organization-local zależą od administracyjnej konfiguracji routerów. Przykłady adresów multicastowych przedstawiono w tabeli 17.3.

Tabela 17.3. **Przykłady multicastowych adresów IPv6**

Adres	Opis	Dostępne zakresy
`ff0x::1`	wszystkie węzły	zakres `1`: `ff01::1` wszystkie węzły w zasięgu interface-local zakres `2`: `ff02::1` wszystkie węzły w zasięgu link-local
`ff0x::2`	wszystkie routery	zakres `1`: `ff01::1` wszystkie routery w zasięgu interface-local zakres `2`: `ff02::1` wszystkie routery w zasięgu link-local zakres `3`: `ff05::1` wszystkie routery w zasięgu site-local

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 to pole 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, bez uwzględnienia długości podstawowego nagłówka (jednak z uwzględnieniem nagłówków rozszerzających);
- następny nagłówek (8 bitów) – identyfikuje nagłówek rozszerzający występujący bezpośrednio po nagłówku IPv6;
- limit przeskoków (8 bitów) – liczba węzłów sieci, po których przejściu 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 jest adresowany pakiet;
- nagłówki rozszerzeń.

Budowę nagłówka IPv6 pokazano na rys. 17.1

Wersja (4)	Klasa ruchu (8)	Etykieta przepływu (20)	
Długość danych (16)		Następny nagłówek (8)	Limit przeskoków (8)
Adres źródłowy (128)			
Adres docelowy (128)			
Nagłówki rozszerzeń			

Rys. 17.1. Budowa nagłówka IPv6

Na rys. 17.2 ramką zakreślono adres IPv6, przypisany do połączenia lokalnego w komputerze z zainstalowanym systemem Windows 10. Adresy IPv6 można skonfigurować również w systemie Windows XP i we wszystkich nowszych od XP oraz w większości nowych dystrybucji Linuksa. Mimo zalet i 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 okazuje się operacją kosztowną i wymaga czasu.

```
Wiersz polecenia
Microsoft Windows [Version 10.0.19042.1110]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\uczen>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : KOMP16
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 00-E0-4C-69-49-A0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0C
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::294f:e784:ee2d:4d87%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 235536423
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-2F-0B-59-70-85-C2-83-71-E5
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Rys. 17.2. **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>`**).

18 Protokoły warstwy transportowej

ZAGADNIENIA

Protokoły używane w warstwie transportowej **Budowa nagłówków protokołów warstwy transportowej** **Wykorzystywanie portów i gniazd** **Mechanizm potwierdzania odebrania segmentów danych** **Wykorzystywanie protokołu UDP**

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

Protokół TCP działa w warstwie transportowej w trybie połączeniowym. Ten tryb jest gwarancją dostarczenia danych do odbiorcy. Połączenia TCP są połączeniami wirtualnymi, rozpoznawanymi po adresach i portach urządzeń docelowych i źródłowych. Charakteryzują się możliwościami sterowania przepływem, potwierdzaniem odbioru, zachowywaniem kolejności danych, kontrolą błędów i przeprowadzaniem retransmisji. Segment TCP składa się z nagłówka i danych. Budowę nagłówka TCP przedstawiono na rys. 18.1.

<table>
<tr><td colspan="2">1 bajt</td><td>2 bajt</td><td>3 bajt</td><td>4 bajt</td></tr>
<tr><td colspan="3">Port źródłowy</td><td colspan="2">Port docelowy</td></tr>
<tr><td colspan="5">Numer sekwencyjny</td></tr>
<tr><td colspan="5">Numer potwierdzenia</td></tr>
<tr><td>Długość nagłówka</td><td>Rezerwa</td><td>Znaczniki</td><td colspan="2">Okno</td></tr>
<tr><td colspan="3">Suma kontrolna</td><td colspan="2">Wskaźnik pilności</td></tr>
<tr><td colspan="5">Opcje i dopełnienie</td></tr>
<tr><td colspan="5">Dane</td></tr>
</table>

Rys. 18.1. Budowa segmentu TCP

Najważniejszymi polami nagłówka TCP są:

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

Ponieważ na komputerze mającym jeden adres IP może jednocześnie działać wiele aplikacji, do ich identyfikacji wykorzystuje się **porty**. Porty są reprezentowane przez liczby naturalne z zakresu od 0 do 65535. Numery portów od 0 do 1023 są **dobrze znane** (ang. *well-known port numbers*) i zarezerwowane dla usług, np. WWW korzysta z portu 80, a telnet – z portu 23. Dzięki portom

można określić, dla jakiej aplikacji przeznaczono segment danych (port docelowy) lub z którego portu wysłano dane (port źródłowy).

Komunikacja między aplikacjami może się odbywać za pomocą **gniazd** (ang. *socket*). Gniazdo to kombinacja adresu IP i numeru portu. Jednoznacznie określa proces w sieci lub zakończenie logicznego łącza komunikacyjnego między dwiema aplikacjami. Jeśli aplikacje uruchomiono na dwóch różnych komputerach, to para odpowiadających im gniazd definiuje połączenie. Gniazdo można 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 i 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 i sprawdza, czy wszystkie segmenty dotarły do miejsca przeznaczenia.

Potwierdzenie odebrania segmentu polega na wysłaniu przez odbiorcę numeru kolejnego bajtu, który powinien być przesłany. Przykładowo: jeżeli ostatni poprawnie odebrany bajt miał numer 123, to odbiorca wyśle numer potwierdzenia 124 (numer następnego bajtu, 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 dzięki temu zmniejszyć liczbę segmentów danych wymagających retransmisji. Jeżeli liczba błędów się zmniejsza, to rozmiar okna jest powiększany, aby zapewnić większą przepustowość sieci.

Protokół UDP działa w warstwie transportowej w trybie bezpołączeniowym. Nie gwarantuje on 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. 18.2) jest prostszy niż TCP. Protokół wykorzystuje się do szybkiego przesyłania danych w niezawodnych sieciach.

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

Rys. 18.2. Budowa datagramu UDP

Dzięki temu, że istnieją dwa alternatywne względem siebie protokoły w warstwie transportowej, TCP i UDP, możliwy staje się dobór najodpowiedniejszego rozwiązania przez aplikacje.

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, numery portów, z których korzystają protokoły: DNS, DHCP, FTP, TFTP, TELNET, SSH, HTTPS, POP3.
3. Który z protokołów – TCP czy UDP – zostanie wykorzystany w przypadku:
   a) komunikacji audio-wideo?
   b) komunikacji tekstowej?
   Odpowiedź uzasadnij.

19 Protokoły warstwy aplikacji

ZAGADNIENIA

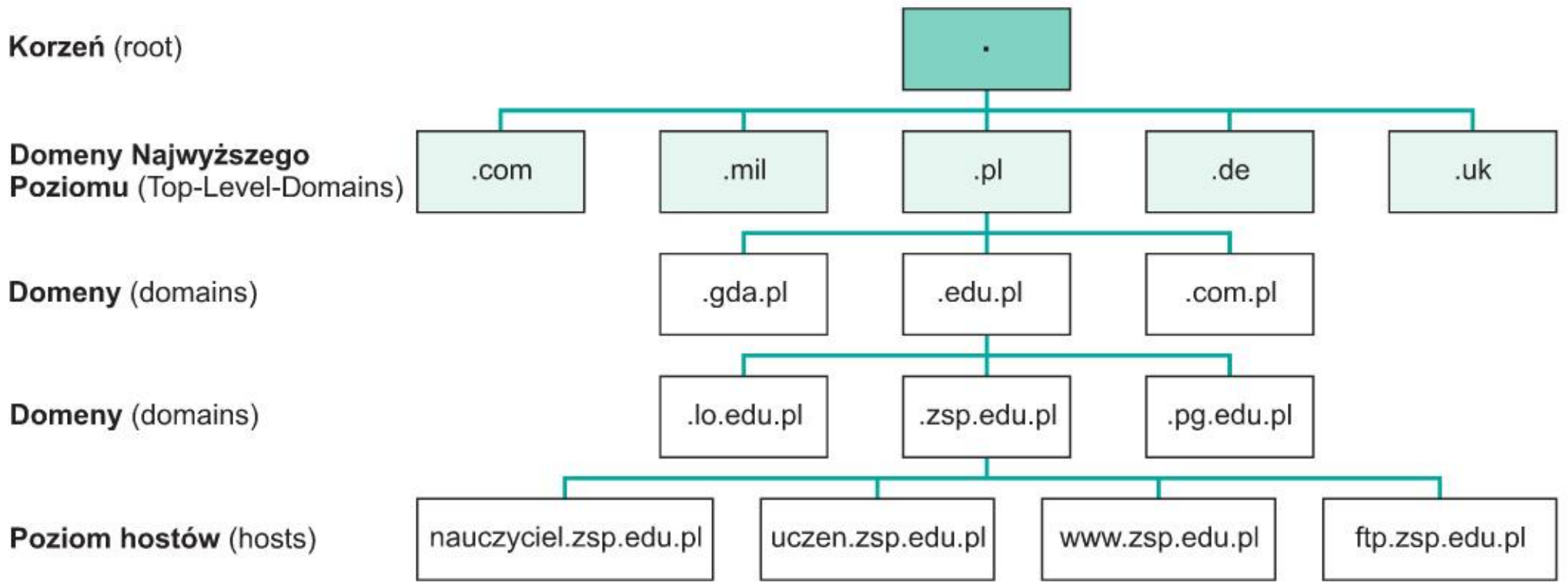
Protokoły działające w warstwie aplikacji **Działanie systemu DNS** **Odpowiedzialność za rejestrowanie nazw domenowych** **Domeny najwyższego poziomu** **Przeznaczenie głównych serwerów nazw** **Sprawdzanie działania systemu DNS**

W warstwie aplikacji modelu TCP/IP funkcjonuje wiele protokołów umożliwiających świadczenie usług dla użytkowników. Przez sieci przesyła się dane za pomocą różnych technologii. Dla autora listu poczty elektronicznej pracującego w warstwie aplikacji nie ma znaczenia, czy jego list będzie przesyłany do internetu za pomocą sieci lokalnej, modemu, DSL (ang. *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. Standaryzacja sprawia, że warstwa aplikacji jest niezależna od protokołów warstw niższych i używanych mediów transmisyjnych. Aplikacje mogą być wykorzystywane niezależnie od tego, czy pracuje się w sieci lokalnej, czy – w globalnej. Najczęściej używanymi protokołami warstwy aplikacji są:

- **FTP** (ang. *File Transfer Protocol*) – do przesyłania plików w sieci;
- **HTTP** (ang. *Hypertext Transfer Protocol*) – do pobierania stron WWW;
- **SMTP** (ang. *Simple Mail Transfer Protocol*) – do wysyłania poczty elektronicznej;
- **POP3** (ang. *Post Office Protocol – Version 3*) – do pobierania poczty elektronicznej;
- **IMAP** (ang. *Internet Message Access Protocol*) – do pobierania poczty elektronicznej;
- **DNS** (ang. *Domain Name System*) – do zamiany nazw domenowych na adresy IP;
- **TFTP** (ang. *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 protokołów jest wykorzystywana przez usługi umożliwiające wykonanie określonych zadań w sieci, np. wysłanie lub odebranie poczty elektronicznej, pobranie pliku lub strony WWW. Wyjątkiem jest usługa DNS.

Gdy korzysta się 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. Te nazwy tworzą drzewiastą strukturę domen. Uproszczony schemat struktury domen przedstawiono na rys. 19.1.



Rys. 19.1. Schemat struktury domen

Poszczególne domeny są oddzielone od siebie kropkami. Na samym szczycie drzewa znajdują się **Domeny Najwyższego Poziomu** (ang. *Top-Level-Domains*). Grupują one 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;

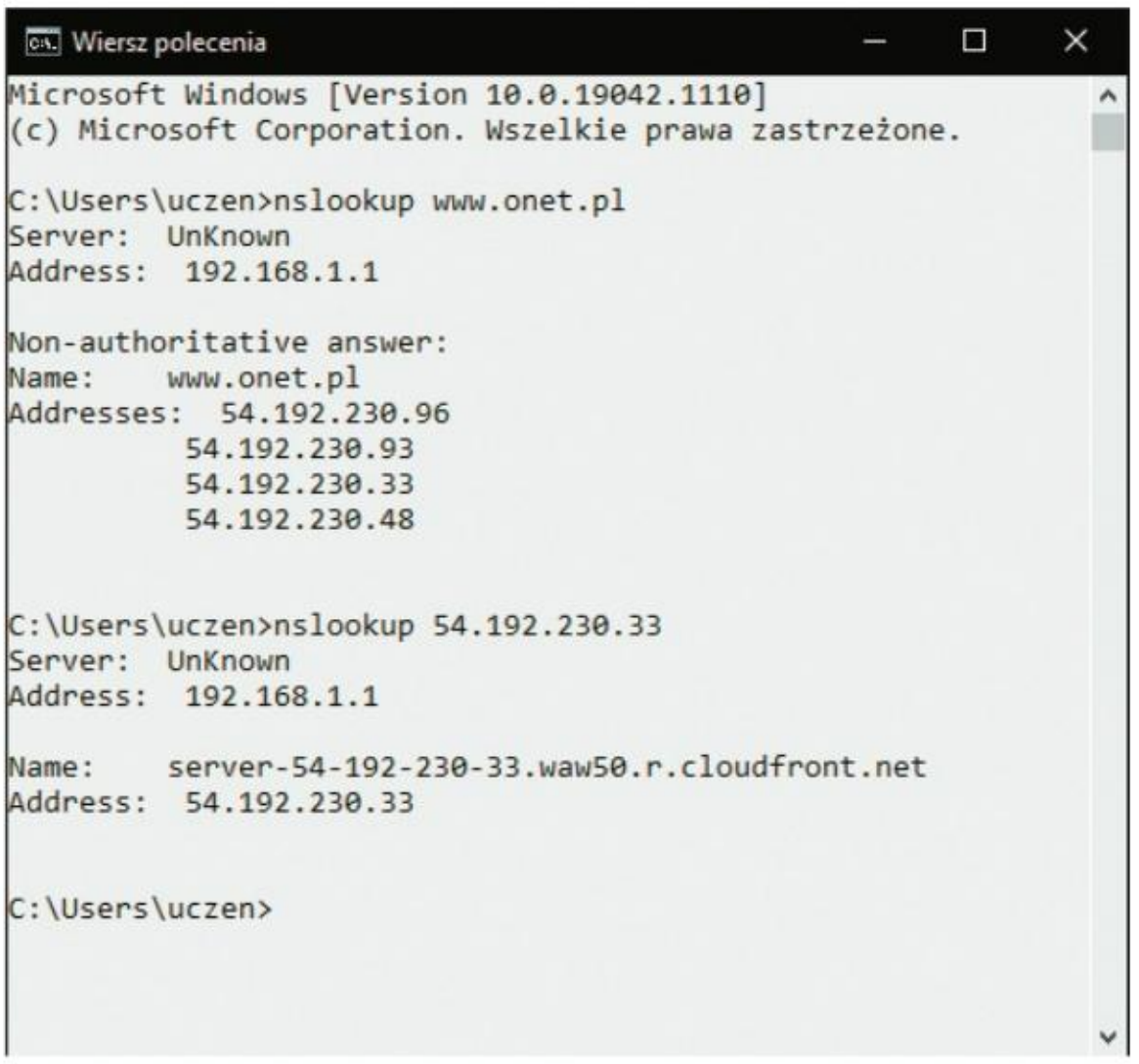
lub położenia geograficznego, np.:

- **`.pl`** – Polska;
- **`.it`** – Włochy;
- **`.de`** – Niemcy;
- **`.fr`** – Francja itd.

Lista domen krajowych i funkcjonalnych jest uzupełniana, tworzona i zarządzana przez organizację **IANA** i korporację **ICANN** (ang. *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 umieszcza się pliki danej strony. System DNS jest **rozproszoną bazą danych** obsługiwaną przez wiele serwerów. Każdy z nich ma informacje tylko o domenie, którą zarządza, i o adresie serwera nadrzędnego. **Główne serwery nazw** (ang. *root level servers*) zlokalizowano w Stanach Zjednoczonych i podłączono do szybkich sieci szkieletowych internetu. Przechowują one adresy serwerów nazw dla **domen najwyższego poziomu**, np. **`.com`**, **`.edu`**, **`.org`**, i 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`**, i 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**. Wysyła ono zapytanie do serwera i zwraca dokładne informacje dotyczące 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 przedstawiono na rys. 19.2. Aby móc testować działanie systemu DNS, należy ustawić w opcjach połączenia sieciowego adres serwera DNS.



Rys. 19.2. Wyszukiwanie danych w systemie DNS

PRZYKŁAD 19.1

Wyszukiwanie informacji w systemie DNS

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

- adres IP serwera www.wp.pl i 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**. Przekazują one swoje uprawnienia na lokalne instytucje i firmy, np. w Polsce nadzór nad domeną **.pl** jako całością i obsługą rejestrowania domen takich jak **.com.pl**, **.biz.pl**, **.org.pl**, **.net.pl** i innych domen funkcjonalnych pełni **NASK**. Aby móc pracować w internecie, komputer musi znać adresy IP serwerów DNS, które udzielają odpowiedzi na zapytania. Serwery 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 utrzymuje się dwa niezależne serwery nazw, dzięki czemu w razie awarii lub zbyt dużego obciążenia **podstawowego serwera DNS** (ang. *primary name server*) można korzystać z **serwera rezerwowego** (ang. *secondary name server*). Informacje o hostach w obrębie domeny są replikowane na inne serwery DNS w celu poprawy odporności na uszkodzenia lub z myślą o poprawie wydajności.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sprawdź adres IP podstawowego i zapasowego serwera DNS używanego w twojej sieci.
2. W jakiej domenie umieszczono stronę internetową twojej szkoły? Wypisz wszystkie domeny i poddomeny.

20 Inne zestawy protokołów sieciowych

ZAGADNIENIA

- **Zadania realizowane przez inne protokoły sieciowe**

Zestaw protokołów **IPX/SPX** firmy Novell bierze nazwę od swoich dwóch głównych protokołów: międzysieciowej wymiany pakietów **IPX** (ang. *Internet Packet Exchange*) i sekwencyjnej wymiany pakietów **SPX** (ang. *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: zarządza połączeniem oraz udostępnia 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** (ang. *NetBIOS Extended User Interface*) został opracowany przez IBM. Jest małym, ale wydajnym protokołem komunikacyjnym. Nie wymaga wprowadzania żadnych informacji podczas konfiguracji, a każda stacja wyszukuje komputery obecne w sieci za pomocą komunikatów rozgłoszeniowych. Jego zastosowanie ogranicza się do sieci lokalnych, w których pracują komputery wykorzystujące systemy operacyjne firmy Microsoft. Ten protokół do identyfikowania komputerów w sieci używa ich nazw i nie umożliwia wyznaczania tras. Domyślnie stosowano go 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.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Scharakteryzuj działanie zestawu protokołów IPX/SPX.
2. Co to są protokoły zdalnego dostępu? Wyszukaj je i opisz. Podaj przykłady.

- Komputerowe systemy sieciowe
- Zasady projektowania lokalnej sieci
- Rodzaje materiałów i urządzeń do budowy sieci
- Zasady doboru materiałów i urządzeń sieciowych
- Struktura dokumentacji projektowej
- Projektowanie okablowania strukturalnego
- Zasady sporządzania harmonogramu prac wykonawczych
- Zasady kosztorysowania prac
- Normy, KNR, katalogi sprzętu sieciowego, cenniki
- Czytanie rzutów poziomych i pionowych budynków
- Obsługa przykładowych programów wspomagających projektowanie 2D
- Obsługa przykładowych programów do kosztorysowania

Projektowanie lokalnych sieci komputerowych

II

21 Komputerowe systemy sieciowe

ZAGADNIENIA

Funkcje realizowane przez serwery **Typy serwerów**

Serwery, stacje robocze, urządzenia sieciowe i okablowanie to sprzętowy szkielet sieci, który wraz z oprogramowaniem sieciowym i użytkowym tworzy **komputerowy system sieciowy**. Do właściwego funkcjonowania tego systemu są niezbędne 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 sprzętu i systemu operacyjnego. Przesyłanie danych przez sieć jest realizowane na podstawie modelu warstwowego sieci, np. ISO/OSI lub TCP/IP. Oprogramowanie sieciowe jest zbiorem współpracujących programów. Niektóre z nich działają na komputerach pełniących funkcję serwerów, inne z kolei – na stacjach roboczych pełniących funkcję klientów.

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

W sieci mogą występować serwery świadczące różne usługi, np.:

- **serwery plików** – udostępniają klientom przestrzeń dysków twardych. 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. 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 komunikację z innymi sieciami, np. internetem. Mogą również świadczyć usługi umożliwiające wymianę danych, np. poczty elektronicznej między użytkownikami sieci lub między urządzeniami, np. DNS, DHCP, proxy.

W każdej sieci może występować jeden lub kilka serwerów każdego rodzaju. Serwery świadczące różne usługi mogą działać na tym samym komputerze w sieci lub te zadania są rozdzielane 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 mieć żadnych funkcji sieciowych. Przykładowo: gdy edytujemy tekst, nie musimy się zastanawiać, czy zapisać plik na dysku lokalnym, na serwerze czy 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 jest udostępniana strona twojej szkoły.
3. Sprawdź, jaki jest adres IP serwera poczty elektronicznej, z którego korzystasz.

22 Zasady projektowania lokalnej sieci

ZAGADNIENIA

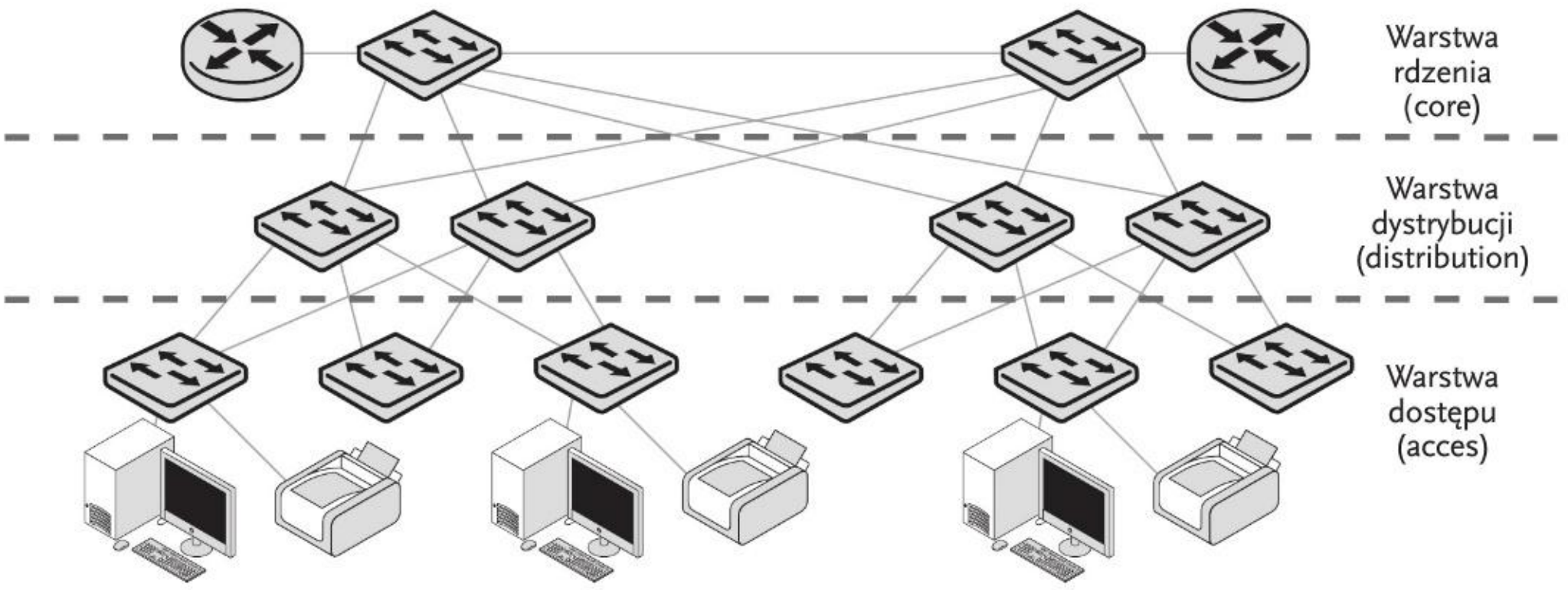
Model hierarchiczny sieci komputerowej **Warstwy modelu hierarchicznego** **Rola warstw w modelu hierarchicznym** **Cechy łatwej do zarządzania sieci komputerowej**

Podczas projektowania architektury **komutowanej sieci LAN** (ang. *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:

- warstwę **dostępu** (ang. *access layer*);
- warstwę **dystrybucji** (ang. *distribution layer*);
- warstwę **rdzenia** (ang. *core layer*).

Sieć hierarchiczna jest łatwiejsza do zarządzania i rozbudowy, a ewentualne problemy rozwiązuje się szybciej. Na rys. 22.1. przedstawiono model hierarchiczny sieci przełączanej. W małych sieciach stosuje się model uproszczony z dwiema warstwami lub nie stosuje się modelu warstwowego.



Rys. 22.1. **Model hierarchiczny budowy sieci przełączanej**

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

- 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. Kontroluje ona przepływ danych w sieci i wyznacza domeny rozgłoszeniowe. Może również realizować routing między **wirtualnymi sieciami LAN** (ang. *virtual LAN*, VLAN), jeżeli na poziomie warstwy dostępu utworzono takie sieci.

Warstwę rdzenia stanowią szybkie łącza szkieletowe. Gromadzi się w niej 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 zostały zapewnione maksymalne korzyści przy minimalnym nakładzie pracy i środków, sieć komputerowa powinna mieć następujące cechy:

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

Skalowalność można rozumieć jako podatność sieci na rozbudowę. Rozrastanie się sieci o dużej skalowalności można łatwo zaplanować i realizować. Przykładowo: przyjmijmy, że na przełącznik z warstwy dystrybucji może przypadać dziesięć przełączników z warstwy dostępu. Można dodawać nowe przełączniki w warstwie dostępu, aż do przekroczenia ich maksymalnej liczby dziesięciu. Po przekroczeniu tej liczby należy dodać dodatkowy przełącznik w warstwie dystrybucji, co umożliwi rozbudowę sieci o kolejne przełączniki w warstwie dostępu.

Zwiększenie niezawodności sieci można osiągnąć po wprowadzeniu **nadmiarowości** (redundancji) urządzeń lub 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 wpłynie ona tylko na urządzenia, które są do niego podłączone.

Wydajność komunikacji można poprawić, jeżeli uniknie się transmisji danych przez niskowydajne przełączniki pośredniczące. W warstwie dystrybucji należy stosować 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 pozwalają uzyskać jednocześnie wysoką wydajność sieci i oszczędności finansowe.

Profesjonalne przełączniki umożliwiają zwiększenie **bezpieczeństwa** przez wprowadzenie zasad ograniczających dostęp do sieci. Przełączniki z warstwy dostępu można konfigurować dzięki zastosowaniu różnych opcji **zabezpieczeń portów** (ang. *port security*) i sieci wirtualnych VLAN, zapewniających 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 mieć podobne parametry techniczne i konfigurację. Aby zapewnić łatwość **zarządzania** i **utrzymania**, można stosować jednakowe urządzenia.

Jeśli trzeba będzie zmienić funkcjonalność jakiegoś przełącznika, np. z warstwy dostępu, to tę zmianę 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. Łatwo można również urządzenie, np. uszkodzone, wymienić na inne sprawne.

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?

23 Rodzaje materiałów i urządzeń do budowy sieci

ZAGADNIENIA

Urządzenia sieciowe zaliczane do aktywnych i do pasywnych **Role urządzeń aktywnych i pasywnych w sieci**

Sieć komputerowa jest systemem bardzo skomplikowanym, złożonym z wielu różnych urządzeń sieciowych aktywnych, pasywnych i oprogramowania. **Urządzenia aktywne**, takie jak koncentratory, przełączniki, routery, służą do przetwarzania danych. 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 zalicza się:

- **nośniki danych** – np. kable miedziane i światłowodowe;
- **gniazda i wtyki komputerowe** – zarabia się w nich kable;
- **szafy dystrybucyjne** – pozwalające na bezpieczne przechowywanie sprzętu aktywnego. Do szaf prowadzi się i zarabia kable z pobliskich pomieszczeń, co zabezpiecza sieć przed wprowadzaniem 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 między punktami dystrybucyjnymi i od szaf dystrybucyjnych do punktów abonenckich. Wykorzystuje się różne systemy prowadzania kabli, umożliwiające prowadzenie kabli pionowych i poziomych w różnych warunkach – wewnątrz i na zewnątrz budynków;
- **panele krosowe** (ang. *patch panel*) – służą do zarabiania kabli w szafach teleinformatycznych. Połączenia w szafie teleinformatycznej między gniazdami panelu krosowego wykonuje się za pomocą krótkich kabli (tzw. patch cordów);
- **organizery kabli** – ułatwiają prawidłowe prowadzenia kabli w szafach. Montuje się je między panelami krosowymi. Dobrą praktyką jest korzystanie z nich między przełącznikami a routerami. Ułatwiają organizowanie kabli w szafie;
- **patch cord** – krótki kabel sieciowy wykorzystywany do połączenia gniazd w panelach krosowych.

Wybrane urządzenia pasywne przedstawiono na rys. 23.1.

a)



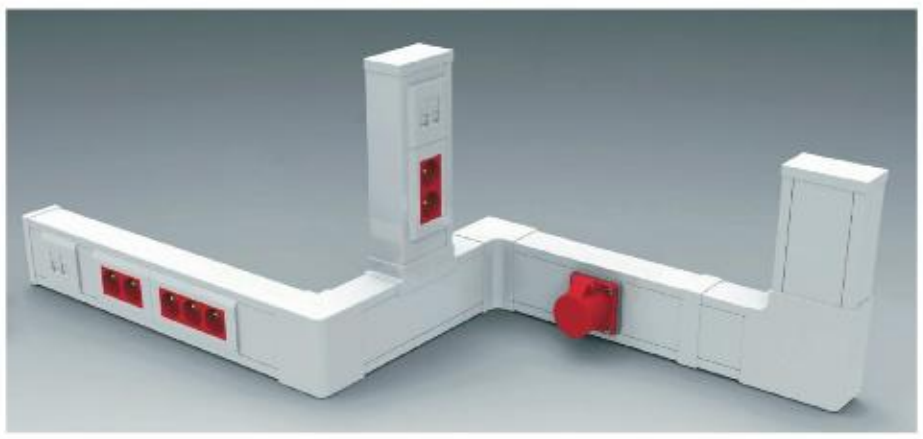
b)



c)



d)



Rys. 23.1. **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 jest zbudowana sieć komputerowa w twojej szkole? Jak – twoim zdaniem – powinna być zbudowana?
2. Z jakich urządzeń aktywnych i pasywnych jest zbudowana sieć komputerowa w twoim domu? Jak – twoim zdaniem – powinna być zbudowana?
3. Wyszukaj na stronie producentów ceny poszczególnych urządzeń pasywnych, z których jest zbudowana twoja sieć domowa. Oblicz koszt urządzeń. Wskaż adresy stron producentów (wyłącznie w celach dydaktycznych).

24 Zasady doboru materiałów i urządzeń sieciowych

ZAGADNIENIA

Przyczyny opóźnień w przekazywaniu danych w sieci **Zmniejszanie wielkości opóźnienia** **Dobieranie urządzeń sieciowych** **Dobór medium transmisyjnego**

Każde urządzenie w sieci, np. przełącznik, skutkuje pewnym **opóźnieniem** (ang. *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**. Oznacza ona liczbę urządzeń, przez które dane muszą przejść, zanim dotrą do swojego miejsca docelowego. Mała średnica sieci przekłada się na 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 mierzy się w ułamkach sekund, ale podczas projektowania sieci warto zwrócić uwagę na długość kabli (również ze względu na koszt instalacji).

Gdy tworzy się 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 bądź 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 i przewidywane generowane przez nie obciążenie pomagają ustalić, ile przełączników jest potrzebnych w warstwie dystrybucji, aby uzyskać wymaganą wydajność i nadmiarowość sieci. Po ustaleniu liczby przełączników warstwy dystrybucji można ustalić liczbę przełączników warstwy rdzenia.

Podczas wyboru 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, i **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 jest możliwa 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). W przypadku większych długości stosuje się kable światłowodowe – wielomodowe (mniejsze długości) lub jednomodowe (większe długości);
- **wymaganą przepustowość łącza** – dla większości sieci do transmisji danych odpowiedni jest Fast Ethernet (100 Mb/s). Dla sieci wymagających większych prędkości stosuje się Gigabit Ethernet lub 10 Gigabit Ethernet;
- **koszt instalacji** – kabel światłowodowy zapewnia wyższe przepustowości i odległości transmisji, lecz koszt instalacji i urządzeń jest wyższy niż w przypadku instalacji z 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 okazują się sieci zbudowane z wykorzystaniem skrętki. Niekiedy należy rozważyć inne wymagania, np. wykorzystanie mediów bezprzewodowych w zabytkowych budynkach, wymagających zgody konserwatora zabytków na instalację kabli, lub kable światłowodowe, gdy jest wymagana odporność sieci na podsłuchiwanie;
- **odporność na zakłócenia elektromagnetyczne** – gdy jest wymagana podwyższona odporność na zakłócenia, stosuje się skrętkę ekranowaną lub kable światłowodowe (zupełnie niewrażliwe na zakłócenia elektromagnetyczne).

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyznacz wielkość średnicy sieci w twojej szkole.
2. Sprawdź, jakie medium transmisyjne wykorzystuje się w twojej szkole. Czy to rozwiązanie jest optymalne? Odpowiedź uzasadnij.

25 Struktura dokumentacji projektowej

ZAGADNIENIA

- **Cechy charakterystyczne projektu**
- **Fazy składające się na realizację projektu**
- **Elementy składowe dokumentacji projektowej**

Struktura każdej sieci komputerowej składa się z takich samych elementów. Jednak każda sieć komputerowa ma również cechy indywidualne, odróżniające ją od innych sieci tego typu. Dlatego każda 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 realizuje się jako projekty, np. napisanie nowego programu komputerowego, stworzenie bazy danych lub strony internetowej. **Projekt** to przedsięwzięcie, na które składa się zespół czynności charakteryzujących 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 informacje niezbędne do realizacji.

Realizacja projektu składa się z następujących faz wykonywanych cyklicznie, w pętli:

- 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, m.in.:

- nazwę pracowni projektowej, w której go sporządzono, lub nazwisko projektanta;
- tytuł projektu;
- datę wykonania;
- ponumerowany spis rysunków i tabel;
- wykaz używanych w projekcie skrótów, np. MDF, IDF;
- 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 właściwe 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;
  - dokumentację centralnego punktu sieci i punktów rozdzielczych;
  - dokumentację rejonów okablowania;
  - projekt koncepcyjny sieci i innych wyspecjalizowanych instalacji, np. klimatyzacji, systemu gaśniczego;
  - numerację gniazd w panelach krosowych 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 między zamawiającym (inwestorem) a wykonawcą projektu. Powinna być zaakceptowana i przestrzegana przez obie strony.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

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

26 Projektowanie okablowania strukturalnego

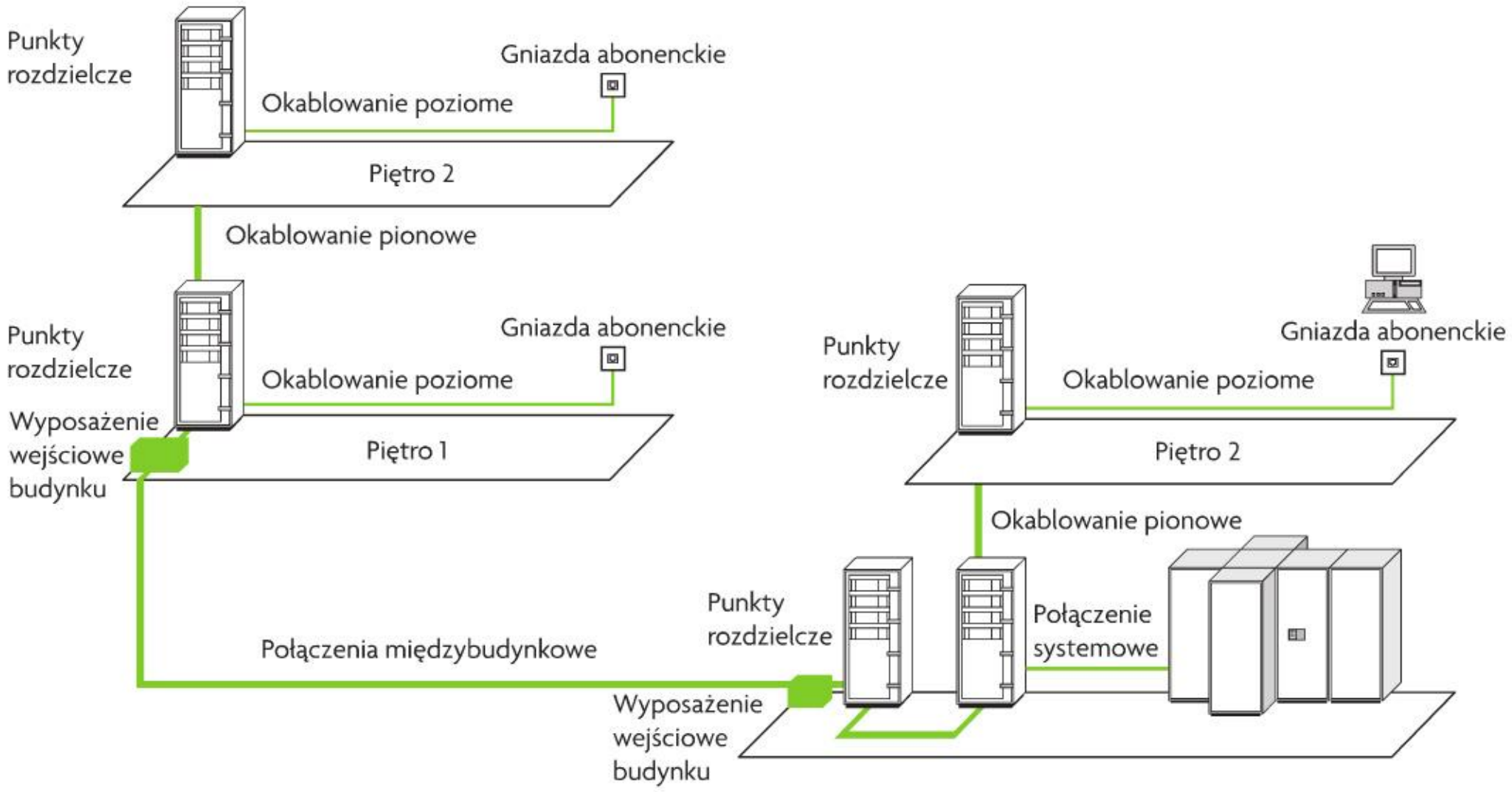
ZAGADNIENIA

Funkcje okablowania strukturalnego **Elementy systemu okablowania strukturalnego** **Rodzaje i zadania punktów dystrybucyjnych** **Różnice między okablowaniem pionowym a poziomym**

W początkowym okresie powstawania sieci komputerowych większość firm miała jedynie jeden komputer centralny i kilka terminali zlokalizowanych blisko niego. Do połączeń jednostki centralnej z terminalami wykorzystywano różne typy okablowania. W późniejszym okresie opracowano rozwiązanie polegające na obsłudze prawie wszystkich popularnych systemów danych przez **skrętkę nieekranowaną** (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 i 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. Ma więcej punktów przyłączeniowych, niż to niezbędne do obsługi wszystkich urządzeń, rozmieszczonych w regularnych odstępach w całym budynku (zakłada się jeden podwójny punkt abonencki 2 × RJ-45 na każde 10 m^2 powierzchni biurowej). System okablowania strukturalnego (rys. 26.1) składa się z następujących elementów:

- **założenia projektowe systemu** – określenie rodzaju nośnika danych, protokołów sieciowych, zgodności z 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 zbiegają się okablowanie poziome i okablowanie 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. 26.1. Schemat okablowania strukturalnego

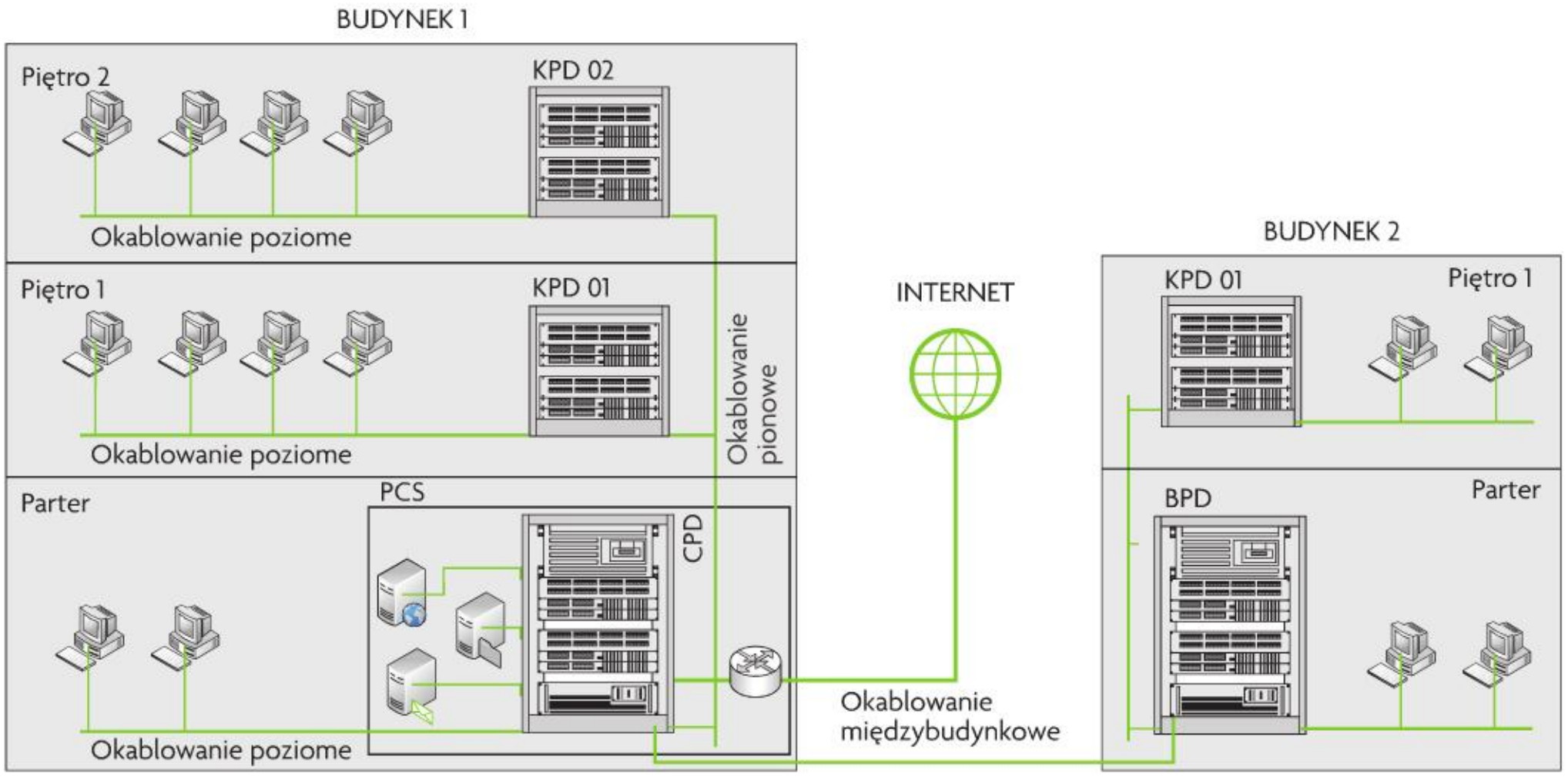
W schemacie okablowania można wyróżnić punkty rozdzielcze, czyli miejsca, w których znajdują się wszystkie elementy aktywne łączące okablowanie pionowe z poziomym. Fizycznie jest to szafa albo rama rozdzielcza z panelami i elementami do podłączania kabli. Według nazewnictwa polskiego, do okablowania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

- **punkt centralny sieci** (**PCS**) – zawiera farmę serwerów, punkt dostępu do sieci internet i centralny punkt dystrybucyjny. Jest to główny punkt infrastruktury teleinformatycznej;
- **centralny punkt dystrybucyjny** (**CPD**) – zbiegają się w nim okablowanie pionowe i okablowanie międzybudynkowe;
- **budynkowy punkt dystrybucyjny** (**BPD**) – łączy całe okablowanie z budynku i centralny punkt dystrybucyjny. W tym punkcie zbiegają się również kable z kondygnacyjnych punktów dystrybucyjnych;
- **kondygnacyjny punkt dystrybucyjny** (**KPD**) – obejmuje zasięgiem całe piętro budynku;
- **lokalny punkt dystrybucyjny** (**LPD**) – 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, przedstawiono na rys. 26.2.

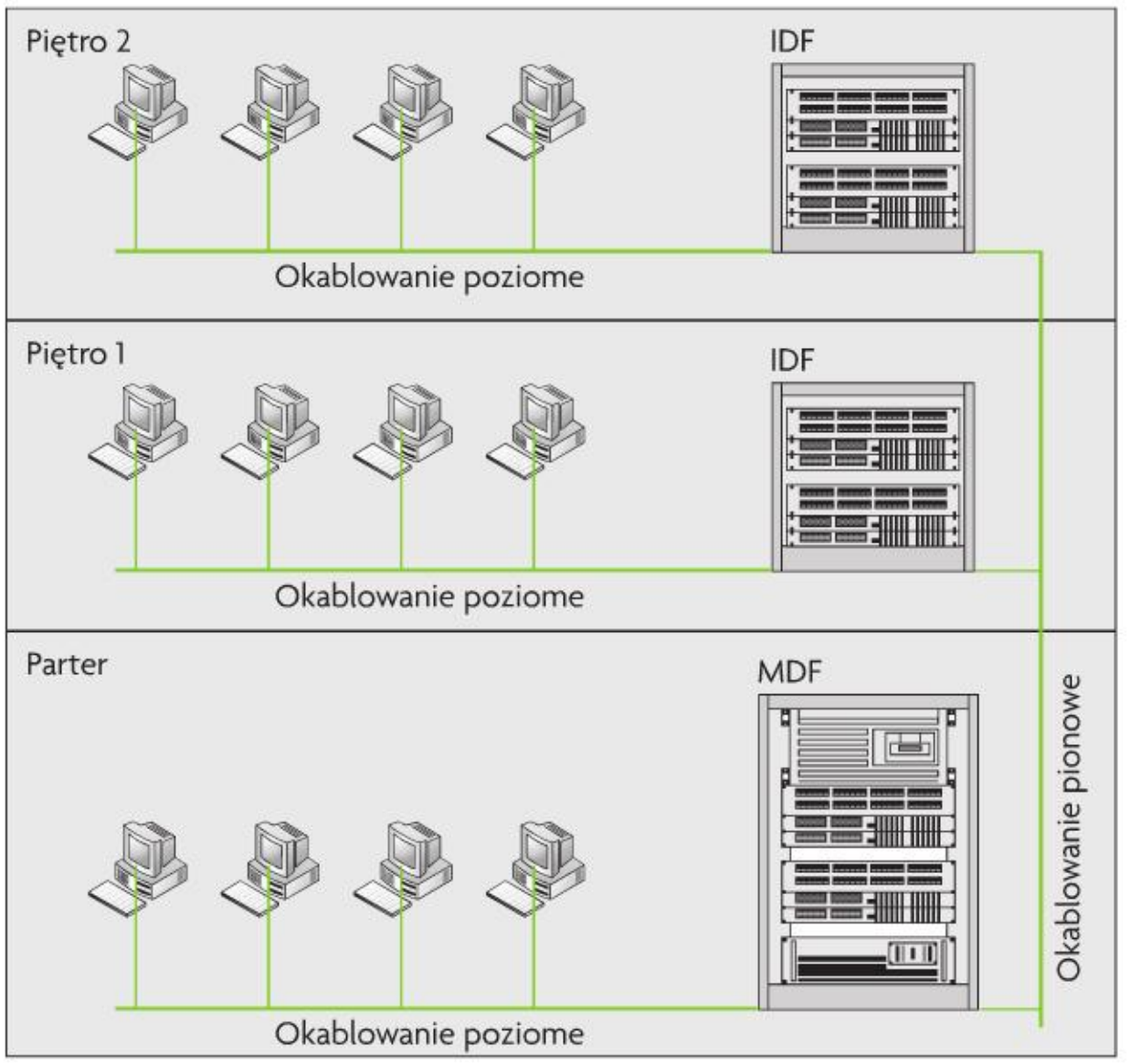
W nazewnictwie angielskim występuje mniej elementów. Ze względu na odgrywaną w sieci rolę można wyróżnić:

- **główny punkt dystrybucyjny** (ang. *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 znajdują się centralka telefoniczna, serwery (farma serwerów) i inny sprzęt aktywny;
- **pośredni punkt dystrybucyjny** (ang. *Intermediate Distribution Facility*, IDF) – jest lokalnym punktem rozdzielczym, obsługującym najczęściej dany obszar roboczy lub piętro. Jeżeli obszar obsługiwany przez IDF jest zbyt duży lub odległość z IDF do punktu abonenckiego przekracza 90 m, to należy utworzyć kolejny punkt dystrybucyjny.



Rys. 26.2. Schemat logiczny okablowania strukturalnego zgodny z terminologią polską

Przykładowy schemat rozmieszczenia punktów dystrybucyjnych w budynku, zgodnie z nazewnictwem angielskim, przedstawiono na rys. 26.3.



Rys. 26.3. 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.

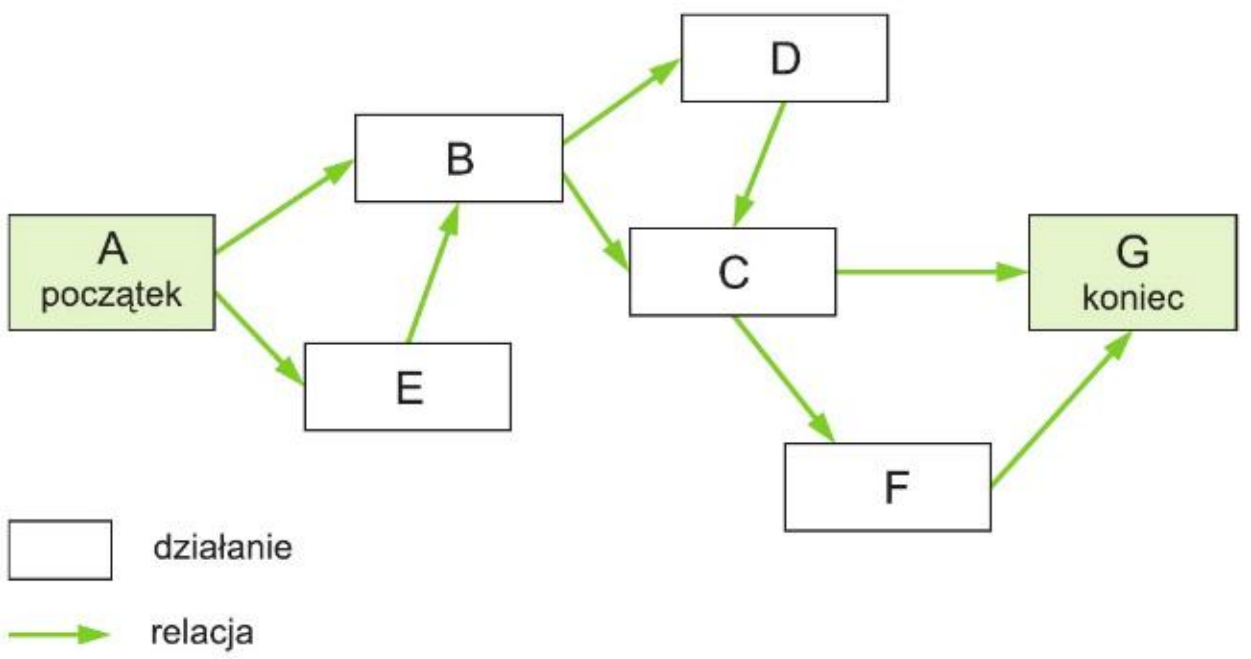
27 Zasady sporządzania harmonogramu prac wykonawczych

ZAGADNIENIA

Narzędzia wykorzystywane do zarządzania czasem podczas realizacji projektów Diagram nadrzędności PDM Narzędzia wykorzystywane do sporządzania harmonogramu prac Wykres Gantta

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

1. **Zdefiniować działania**, które muszą zostać wykonane do 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** (ang. *Precedence Diagramming Method*), którą przedstawiono na rys. 27.1.



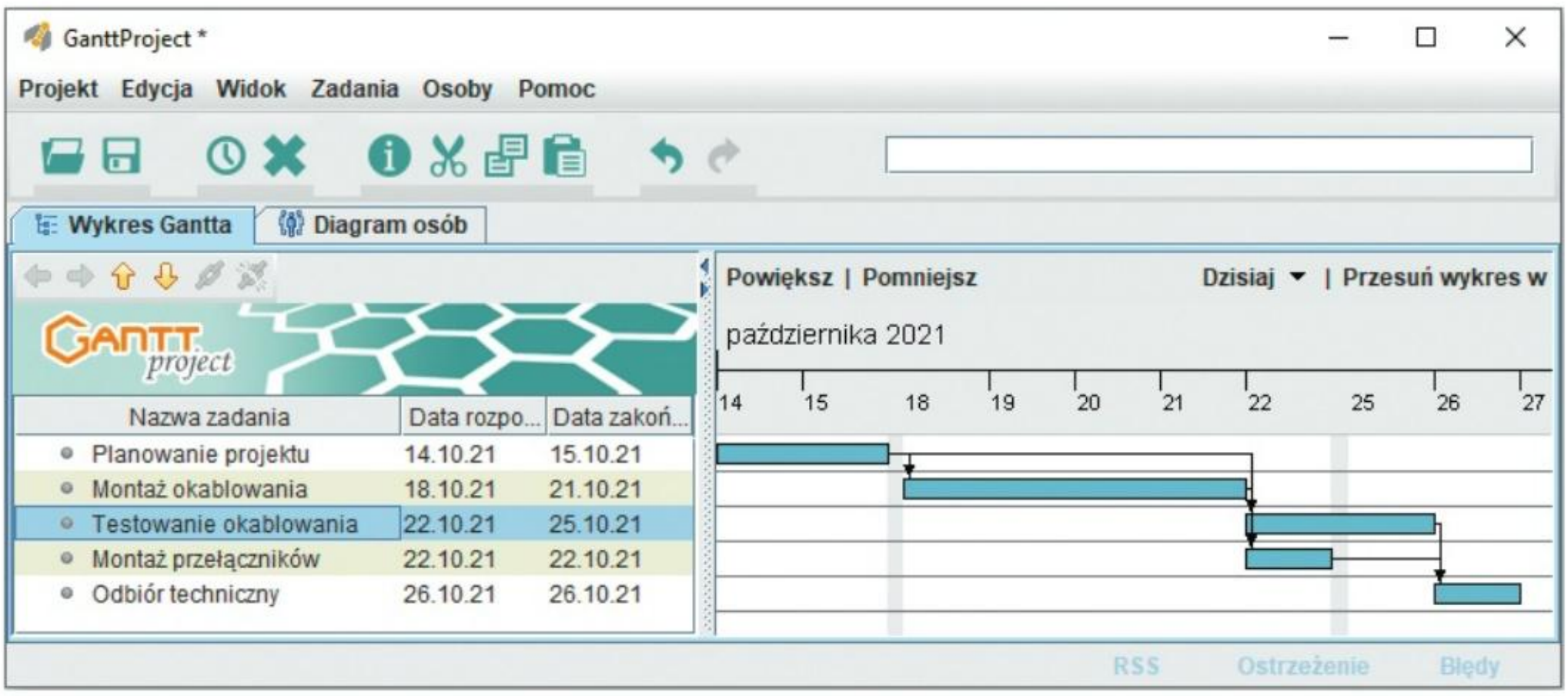
Rys. 27.1. **Przykładowy diagram nadrzędności (PDM)**

Metoda polega na konstruowaniu sieci projektu za pomocą 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;
- **skończyć, 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. trzeba rozpocząć proces testowania okablowania, aby stwierdzić, czy instalacja została wykonana właściwie.

3. **Oszacować czas potrzebny do wykonania poszczególnych działań** – należy oszacować liczbę godzin, dni lub miesięcy przewidywanych do wykonania poszczególnych zadań. W oszacowaniu czasu prac mogą być pomocne normy dotyczące prac montażowych i znajomość rozmiaru zadania. Przykładowo: jeżeli pracownik układa średnio 100 m kabla w ciągu godziny, a jest do położenia odcinek 500 m, to można oszacować czas wykonania pracy na 5 godzin.
4. **Stworzyć terminarz działań** – na podstawie zebranych we wcześniejszych etapach informacji. Terminarz może być zilustrowany **wykresem Gantta** (rys. 27.2). Do jego sporządzenia można wykorzystać np. bezpłatny program GanttProject, dostępny na stronie http://www.ganttproject.biz/.
5. **Systematycznie kontrolować przestrzeganie terminów** – pozwoli to zminimalizować opóźnienia w realizacji projektu.



Rys. 27.2. **Przykładowy wykres Gantta**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyodrębnij działania w projekcie wybranym przez ciebie.
2. Określ i narysuj diagram nadrzędności. Oszacuj czas poszczególnych działań i narysuj wykres Gantta.

28 Zasady kosztorysowania prac

ZAGADNIENIA

Zasoby niezbędne do realizacji projektu **Budżet projektu** **Kamienie milowe projektu** **Czynniki ograniczające projekt**

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

- **ludzie** – pracownicy wykonujący poszczególne zadania. Na koszt składają się nie tylko wynagrodzenia wypłacane pracownikom, lecz także niezbędne szkolenia personelu lub dodatkowe zatrudnienie 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 należy je wliczyć 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 z odpowiednimi uprawnieniami;
- **środki finansowe**;
- **inne zasoby**, np. wiedza pracowników, doświadczenie w realizacji i zdolności przywódcze kadry kierowniczej, budynki i pomieszczenia.

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

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

Mniejsze niebezpieczeństwo występuje podczas **szacowania etapowego**. Cały projekt dzieli się na etapy. Zakończenie każdego etapu zależy od spełnienia określonego warunku lub od zrealizowania pewnego produktu cząstkowego (tzw. **kamienie milowe**).

Realizacja projektu etapami pozwala na dokładniejsze szacowanie kosztów poszczególnych etapów, a następnie ich zsumowanie. Zależnie od umowy między inwestorem a wykonawcą możliwe jest przekazanie, po zakończeniu etapu, części środków finansowych. Umożliwi to kontynuowanie prac przy zachowaniu kontroli nad przebiegiem realizacji projektu.

Metody sumowania kosztów i szacowania etapowego zalicza się do **metod oddolnych** – tworzy się szacunek kosztów dla każdego elementu i zmierza do uzyskania całkowitego kosztu. W **metodach odgórnych** na ogół dysponuje się 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. 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 średni koszt wykonania gniazda 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 wykonania. Realizacja projektu jest związana z ograniczeniami – są to czynniki ograniczające do pewnego stopnia możliwości realizacji projektu. Typowe trzy główne ograniczenia to:

- **harmonogram** – ograniczenia takie jak stała data zakończenia lub termin ostateczny ukończenia;
- **zasoby** – ograniczenie to np. budżet przeznaczony na materiał, na wyposażenie, sprzęt i na wynagrodzenia oraz skojarzone z nimi koszty;
- **zakres** – ograniczenie takie jak zakładana funkcjonalność, technologia, produkty.

Zmiana jednego z wymienionych ograniczeń zwykle wpływa na dwa pozostałe, a także – na jakość projektu. Przykładowo: zmniejszenie czasu trwania projektu (harmonogram) może zwiększyć liczbę pracowników potrzebnych do realizacji planu (zasoby) i zmniejszyć liczbę właściwości cechujących produkt (zakres). Taki związek nazywa się **potrójnym ograniczeniem zarządzania projektem** lub **trójkątem ograniczeń projektu**. Podczas procesu planowania należy sporządzić listę ograniczeń projektu, aby się upewnić, 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. Przykładowo: 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.

29 Normy, KNR, katalogi sprzętu sieciowego, cenniki

ZAGADNIENIA

Jednostkowe nakłady rzeczowe **Katalog nakładów rzeczowych – KNR** **Obliczanie kosztu pracy**

Opracowanie budżetu jest zadaniem bardzo trudnym, ale koniecznym do właściwej realizacji projektu. Jeżeli budżet jest niedoszacowany, czyli do jego realizacji zaplanowano zbyt małe środki, może zdarzyć się sytuacja, że projekt nie zostanie dokończony – straty poniosą 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 popłaca i taki wykonawca nie będzie mógł już 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 w roboczogodzinach [rg.], na jednostkę obmiarową danej pracy, np. instalacja systemu operacyjnego na pojedynczym komputerze (czyli jeden etap instalacji systemu operacyjnego w firmie) – 1 rg.
- **materiałów** – wyrażane w wybranej jednostce miary ilości danego materiału (np.: kg, m^3, m, szt.), na jednostkę obmiarową danej pracy, np. w okablowaniu strukturalnym na każde 10 m^2 powierzchni powinno przypadać jedno podwójne gniazdo abonenckie;
- **czasu pracy sprzętu** – wyrażane w maszynogodzinach [mg.], na jednostkę obmiarową danej pracy, 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 29.1 przedstawiono przykładowe jednostkowe nakłady związane z budową okablowania strukturalnego. Informacje pochodzą z katalogu nakładów rzeczowych dla prac związanych z montażem sieci *Okablowanie strukturalne w technologii firmy TYCO*, oznaczonego symbolem KNR AT-28.

W tabeli 29.2 można odczytać, że montaż nieekranowego modułu RJ-45 wymaga:

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

Tabela 29.1. **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	rg.	0,86	1,06	1,08	1,33	0,41	0,55
02	315	Monter-instalator – grupa V	rg.	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 29.2. **Tabela 0108 z KNR AT-28**

Montaż na skrętce 4-parowej modułu RJ-45 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	
				nieekrano-wany	ekrano-wany
a	b	c	d	01	02
01	315	Monter-instalator – grupa V	rg.	0,07	0,01
20		Moduł nieekranowany RJ-45 SL Tyco Electronics/AMP NETCONNECT	kpl.	1	–
21		Moduł ekranowany RJ-45 SL Tyco Electronics/AMP NETCONNECT	kpl.	–	1
22		Moduł ekranowany RJ-45 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	mg.	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 między wykonawcą a inwestorem. Stawki godzinowe są zwykle różne dla pracowników o odmiennych kwalifikacjach i uprawnieniach. Całkowity koszt robocizny będzie iloczynem całkowitych nakładów pracy i stawki godzinowej. Jeżeli przyjmie się stawkę godzinową 18,30 zł/h, to wartość pracy wyniesie 1,28 zł (18,30 zł/h · 0,07 rg. = 1,28 zł).

Podobnie ustala się stawkę maszynogodziny pracy maszyn i narzędzi. Jeżeli dla narzędzia do zarabiania gniazd przyjmie się stawkę 5 zł/h, to koszt jej pracy wyniesie 0,35 zł (5 zł/h · 0,07 mg. = 0,35 zł).

Koszt materiałów niezbędnych do wykonania pracy można ustalić na podstawie cenników dostawców. Katalogi wyrobów oraz cenniki materiałów i urządzeń są dostępne na stronach internetowych dostawców lub producentów. W cennikach oprócz ceny podaje się również najważniejsze informacje charakteryzujące dane urządzenie. Przykład fragmentu cennika przedstawiono na rys. 29.1. Do kosztów producenta dodaje się koszt zakupu – zwykle obliczany procentowo od wartości zakupu (np. 5 %). Nakłady związane z realizacją całego projektu są sumą wszystkich nakładów cząstkowych. Jeżeli przyjmiemy, że cena wtyczki RJ-45 (wraz z kosztami zakupu) wynosi 1 zł, i zsumujemy wszystkie koszty, to łączny budżet dla naszego przykładu wyniesie 2,63 zł.



Rys. 29.1. Fragment cennika sieciowego sprzętu aktywnego

Na rynku jest dostępnych 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. Skorzystaj z katalogu KNR AT-28 i oblicz koszt montażu 1000 m skrętki nieekranowanej (okablowanie poziome) i wykonania 10 złączy RJ-45.

30 Czytanie rzutów poziomych i pionowych budynków

ZAGADNIENIA

Sposób zapisywania konstrukcji w formie rysunku technicznego **Sposób podawania wymiarów na rysunkach** **Rodzaje podziałek rysunku** **Czytanie rysunku technicznego**

Maszyny, urządzenia i systemy powstające w umyśle konstruktorów zapisuje się na papierze lub w formie elektronicznej 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 przedstawia się w uproszczeniu, za pomocą specjalnych symboli. Sposób rysowania określono za pomocą norm i zasad, których znajomość jest niezbędna do prawidłowego odczytania zawartości rysunku.

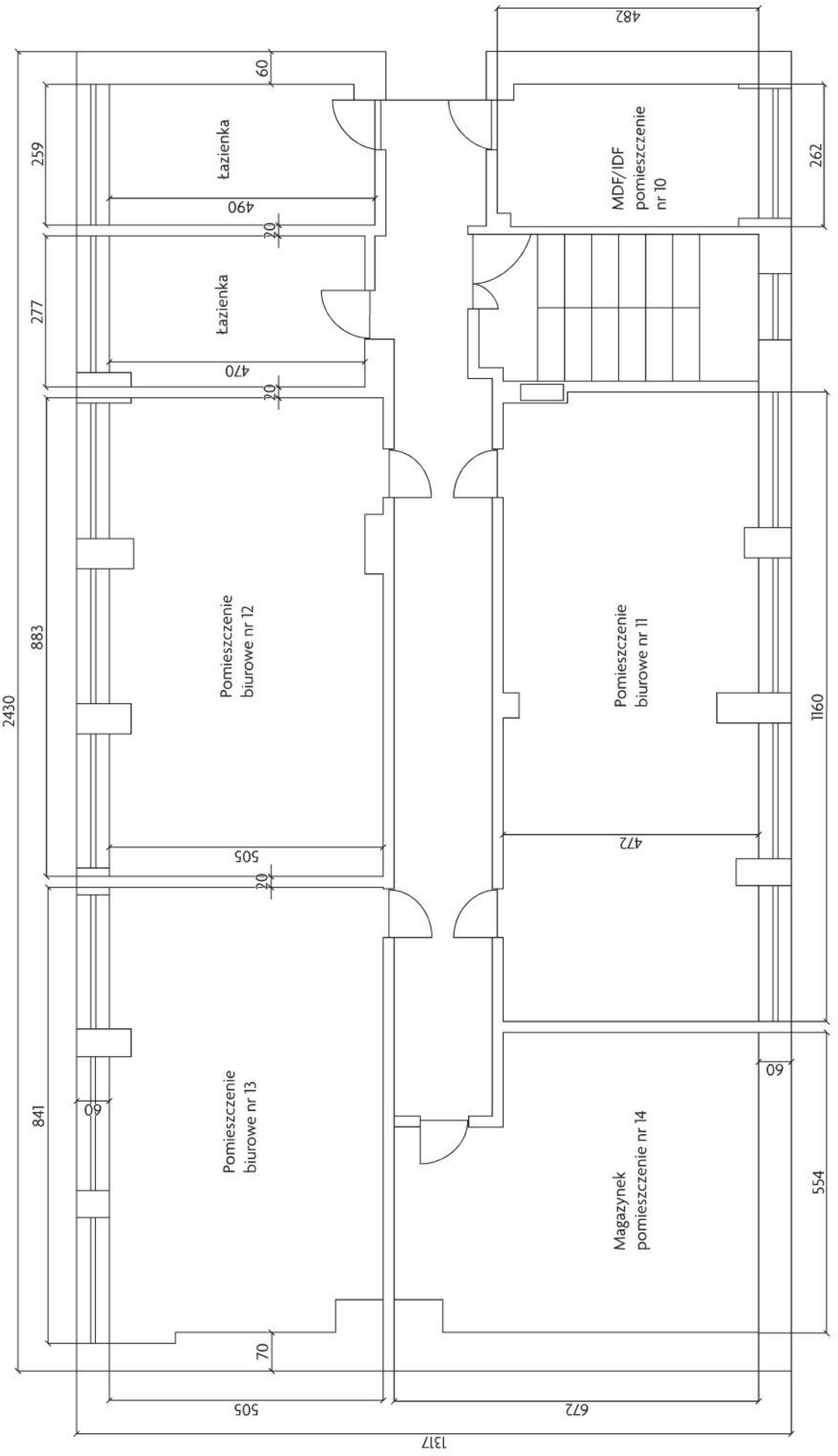
Rysunki mogą być sporządzone w **naturalnej wielkości** (podziałka 1 : 1), w **powiększeniu** (np. podziałka 10 : 1 oznacza dziesięciokrotne powiększenie) lub **pomniejszeniu** (np. podziałka 1 : 5 oznacza pięciokrotne pomniejszenie). Niezależnie od użytej podziałki, na rysunku zawsze podaje się wymiary rzeczywiste. W wielu różnych dziedzinach techniki wypracowano zasady pozwalające na bardzo precyzyjne odwzorowanie konstrukcji.

Zależnie od przeznaczenia, można mówić o rysunku maszynowym (stosowanym w budowie maszyn), rysunku budowlanym bądź rysunku elektrycznym. W rysunku maszynowym wymiary podaje się w milimetrach (np. wymiary gabarytowe przełączników), natomiast w rysunku budowlanym za jednostkę przyjęto centymetr.

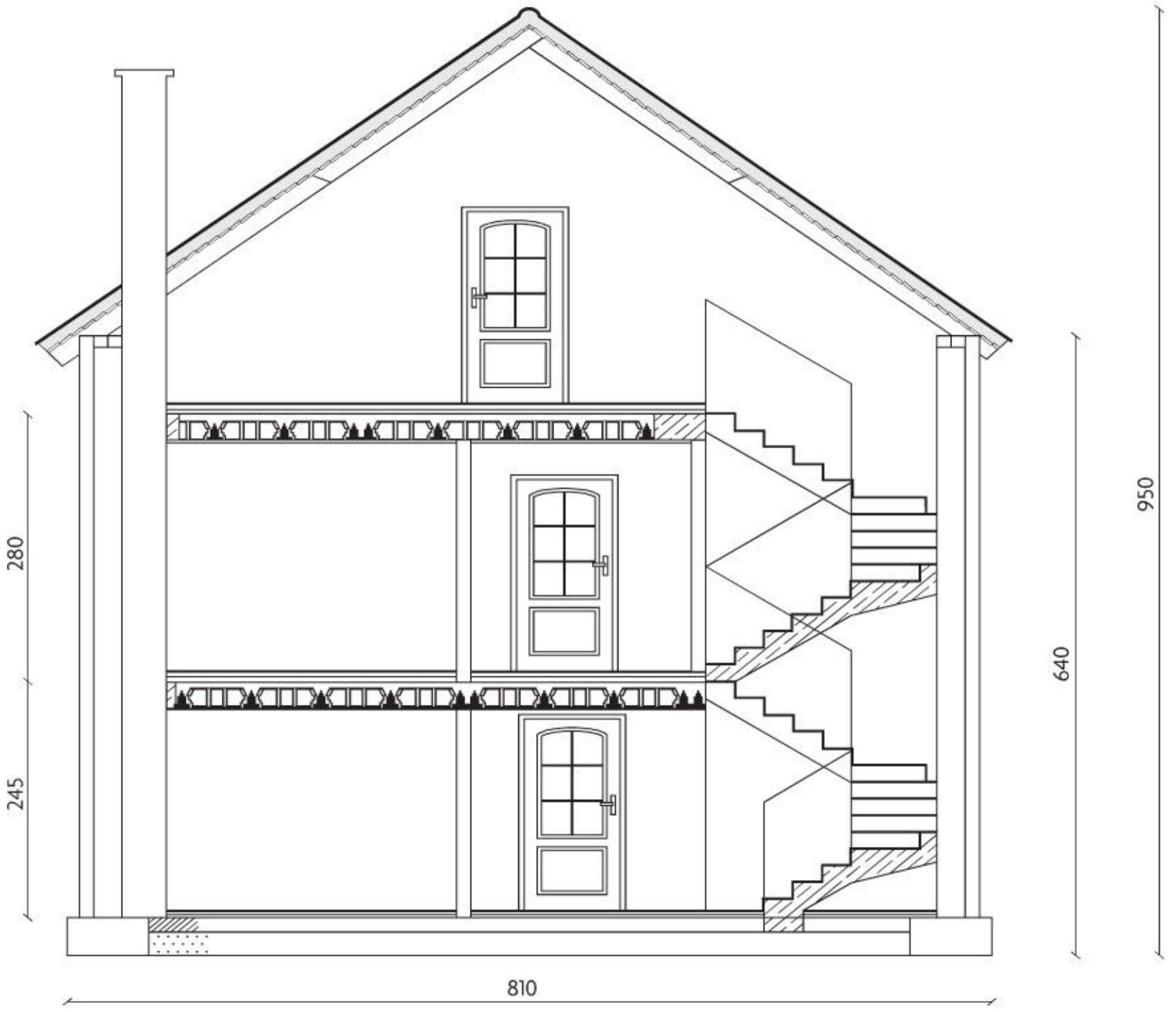
Aby zaprojektować sieć komputerową, projektant musi prawidłowo odczytać informacje zapisane na rysunku budynku. Określa on rozmiar budynku i układ pomieszczeń, lokalizuje pomieszczenia, a ponadto odczytuje informacje o innych instalacjach w budynku, np. o instalacji elektrycznej. Czytanie rysunku polega na odtworzeniu w swojej wyobraźni, na podstawie rysunku, obrazu konstrukcji, kształtu, wymiarów i wzajemnych zależności między poszczególnymi elementami. Przykład przekroju poziomego piętra budynku przedstawiono na rys. 30.1. Z myślą o uproszczeniu pominięto w rysunku wiele szczegółów nieistotnych z punktu widzenia projektanta sieci komputerowej.

Z rysunku można odczytać, że budynek ma kształt prostokąta o wymiarach 2430 cm × 1317 cm. Na piętrze zlokalizowano trzy pomieszczenia biurowe o numerach 11, 12, i 13. Ponadto na piętrze znajdują się magazynek, pomieszczenie na punkt dystrybucyjny sieci i dwie łazienki. Przez środek budynku przebiega korytarz.

W przekroju pionowym budynku (rys. 30.2) można odczytać informacje o wysokości poszczególnych kondygnacji (pierwsza kondygnacja – 245 cm, druga – 280 cm) i całego budynku (950 cm). Przekrój pozwala również na określenie położenia instalacji i ciągów komunikacyjnych.



Rys. 30.1. Rysunek techniczny piętra budynku



Rys. 30.2. **Przekrój pionowy budynku**

UWAGA

Na rys. 30.1 i 30.2 nie przedstawiono tego samego budynku.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Przyjmij zgodnie z normą, że jedno podwójne gniazdko RJ-45 przypada na 10 m^2 powierzchni biurowej, i określ liczbę gniazdek w każdym z pomieszczeń biurowych przedstawionych na rys. 30.1.
2. W przygotowywanym przez ciebie projekcie:
   - oblicz liczbę gniazdek abonenckich w poszczególnych pomieszczeniach;
   - zaznacz rozmieszczenie punktów dystrybucyjnych;
   - oblicz długość poszczególnych kabli i ich łączną długość.

31 Obsługa przykładowych programów wspomagających projektowanie 2D

ZAGADNIENIA

Programy wykorzystywane do sporządzania rysunków technicznych **Sposób otwierania i wykonywania rysunków** **Korzystanie z warstw rysunku**

Dokumentacja techniczna obiektu, np. rysunek budowlany, jest podstawą do zaprojektowania instalacji elektrycznej lub okablowania sieci komputerowej. Dawniej rysunki wykonywali kreślarze na kalce technicznej. Obecnie rysunki powstają za pomocą oprogramowania typu **CAD** (ang. *Computer Aided Design*). Istnieje wiele programów tego typu. Najbardziej znany jest program AutoCAD firmy Autodesk. Jest to program komercyjny, lecz studenci mogą uzyskać nieodpłatną licencję edukacyjną. Oprócz samego programu AutoCAD, oferuje się 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 sporządzania rysunków 2D można wykorzystać bezpłatne programy A9CAD lub QCad.

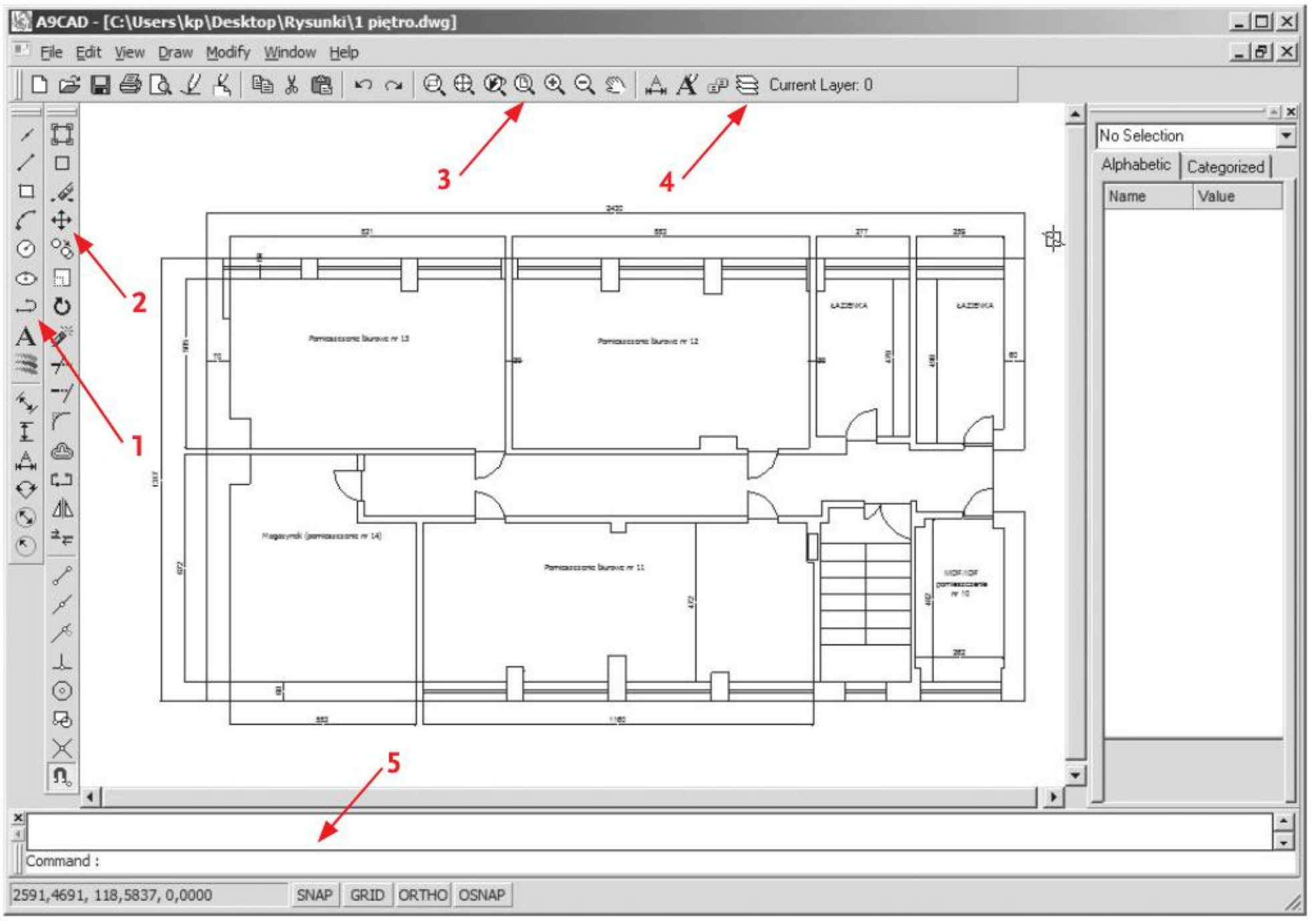


Rys. 31.1. **Tablet graficzny**

Rysunki są zapisywane jako grafika wektorowa. Standardowymi rozszerzeniami plików są *.dwg lub *.dxf. Wspomniane programy umożliwiają wprowadzanie danych z bardzo dużą dokładnością. W profesjonalnych biurach projektowych pracę kreślarzom ułatwiają tablety graficzne (rys. 31.1), wykorzystywane do szybkiego i precyzyjnego rysowania za pomocą specjalnego pióra.

Na rys. 31.2 przedstawiono okno główne programu A9CAD. Strzałkami zaznaczono paski narzędzi najczęściej wykorzystywane do edycji rysunków:

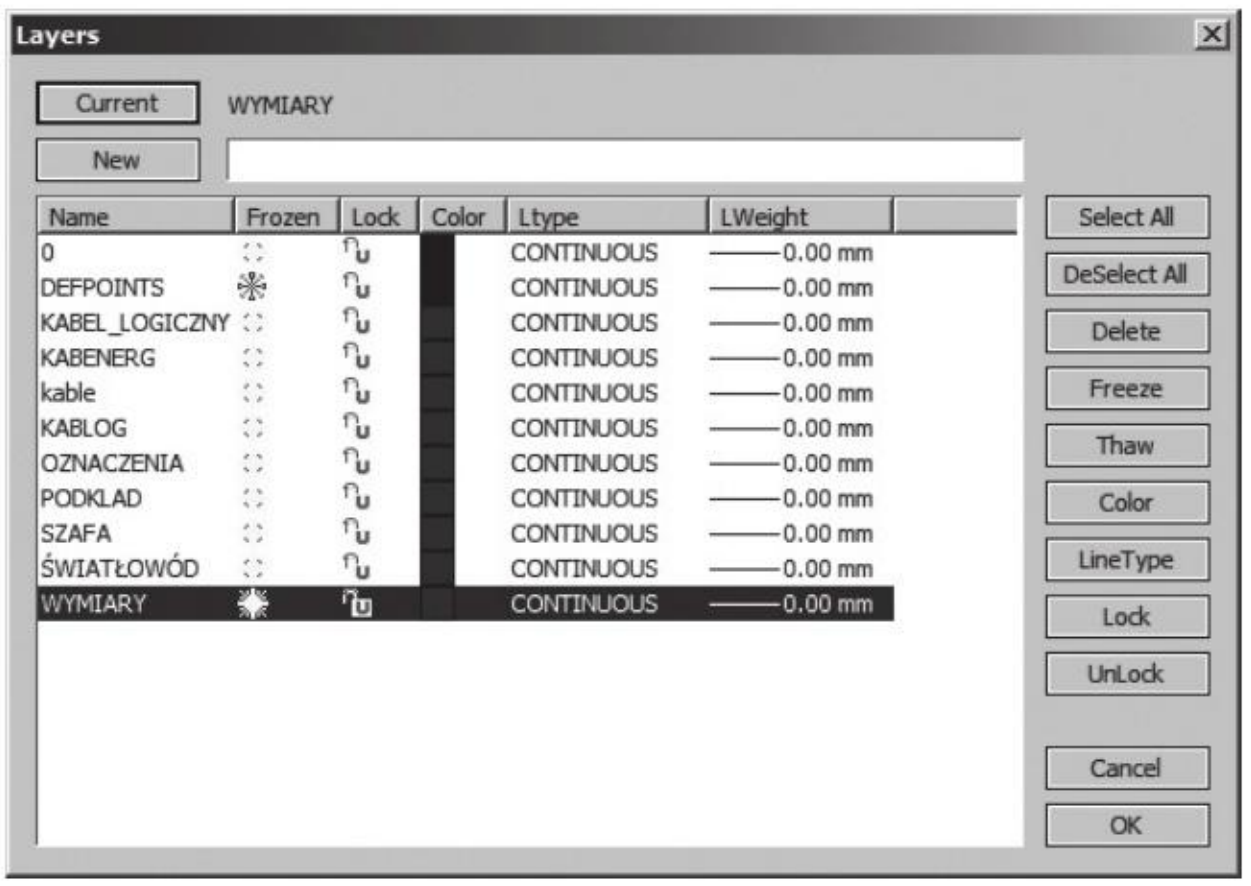
1. **Pasek narzędzi rysowania** – pozwala na rysowanie obiektów, takich jak punkty, linie, okręgi, a także na wprowadzanie wymiarów.
2. **Pasek modyfikacji** – pozwala na modyfikowanie obiektów istniejących na rysunku, np. ich obcinanie lub wydłużanie, przesuwanie, wykonywanie obrotu.
3. **Pasek narzędzi zoom** – umożliwia powiększanie i pomniejszanie wybranego obszaru roboczego okna.
4. **Pasek zarządzania warstwami rysunkowymi** – umożliwia tworzenie i usuwanie warstw oraz sterowanie ich dostępnością i widocznością.
5. **Pasek poleceń** – wszystkie operacje mogą być rozpoczynane przez wprowadzanie poleceń z klawiatury.



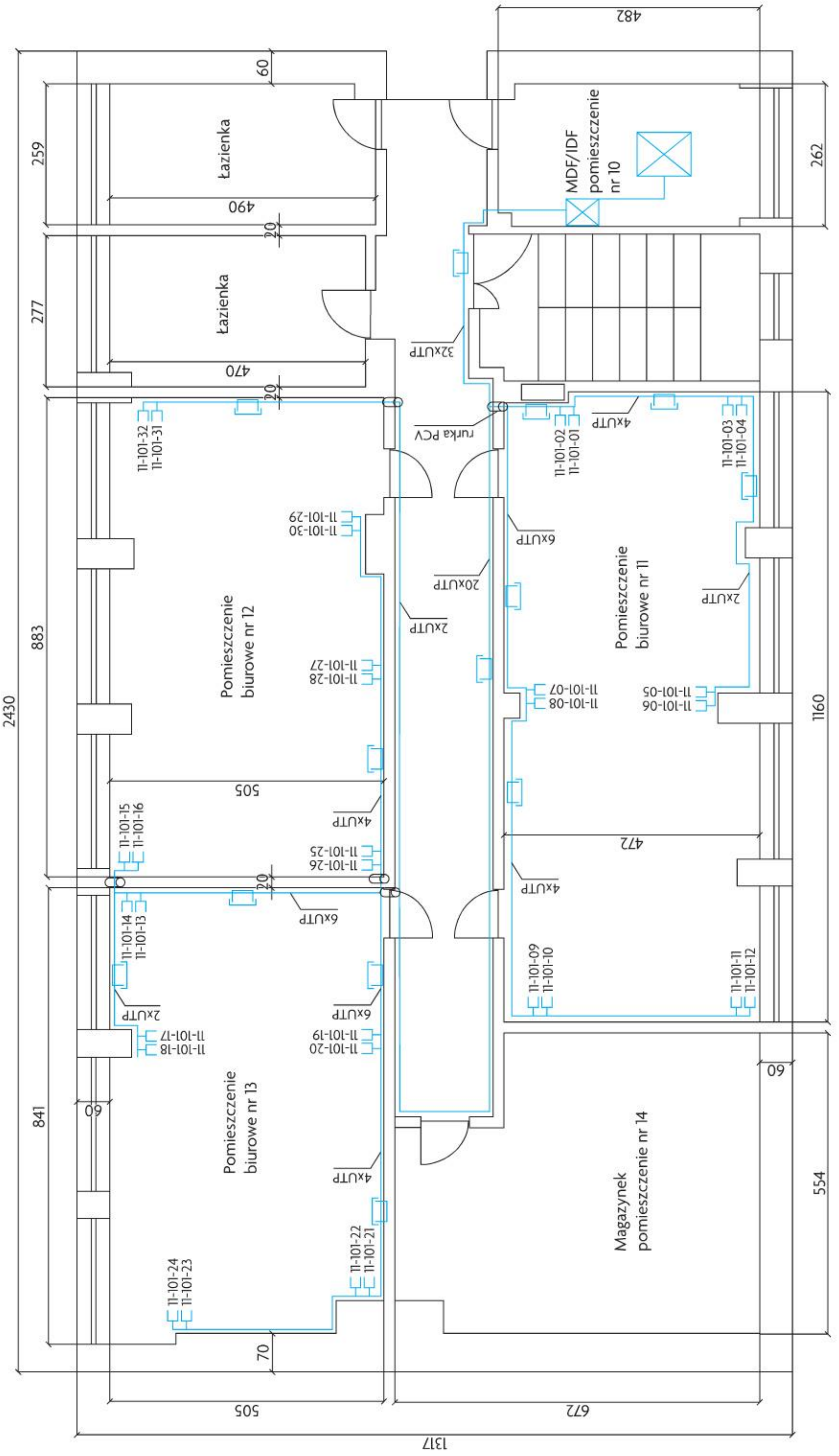
Rys. 31.2. **Paski narzędziowe programu A9CAD**

Rysunek techniczny może zawierać bardzo dużo informacji. Nie wszystkie z nich są potrzebne w danej chwili, a ich nadmiar może sprawić, że odczytanie szczegółów i zrozumienie konstrukcji stanie się trudniejsze. Z tego powodu bardzo często stosuje się rysowanie w **warstwach**. Warstwy można sobie wyobrazić jako przezroczyste folie zawierające elementy rysunku, nakładane na siebie. Pozwalają one na wybór lub ukrycie szczegółów z danej warstwy. W każdym rysunku musi być zdefiniowana warstwa 0 – można ją wykorzystać np. do narysowania fundamentów budynku. W innej warstwie wykonuje się wymiarowanie, w innej – rysunek instalacji elektrycznej, jeszcze w innej – sieci komputerowej itd. Przykład zdefiniowanych warstw przedstawiono na rys. 31.3.

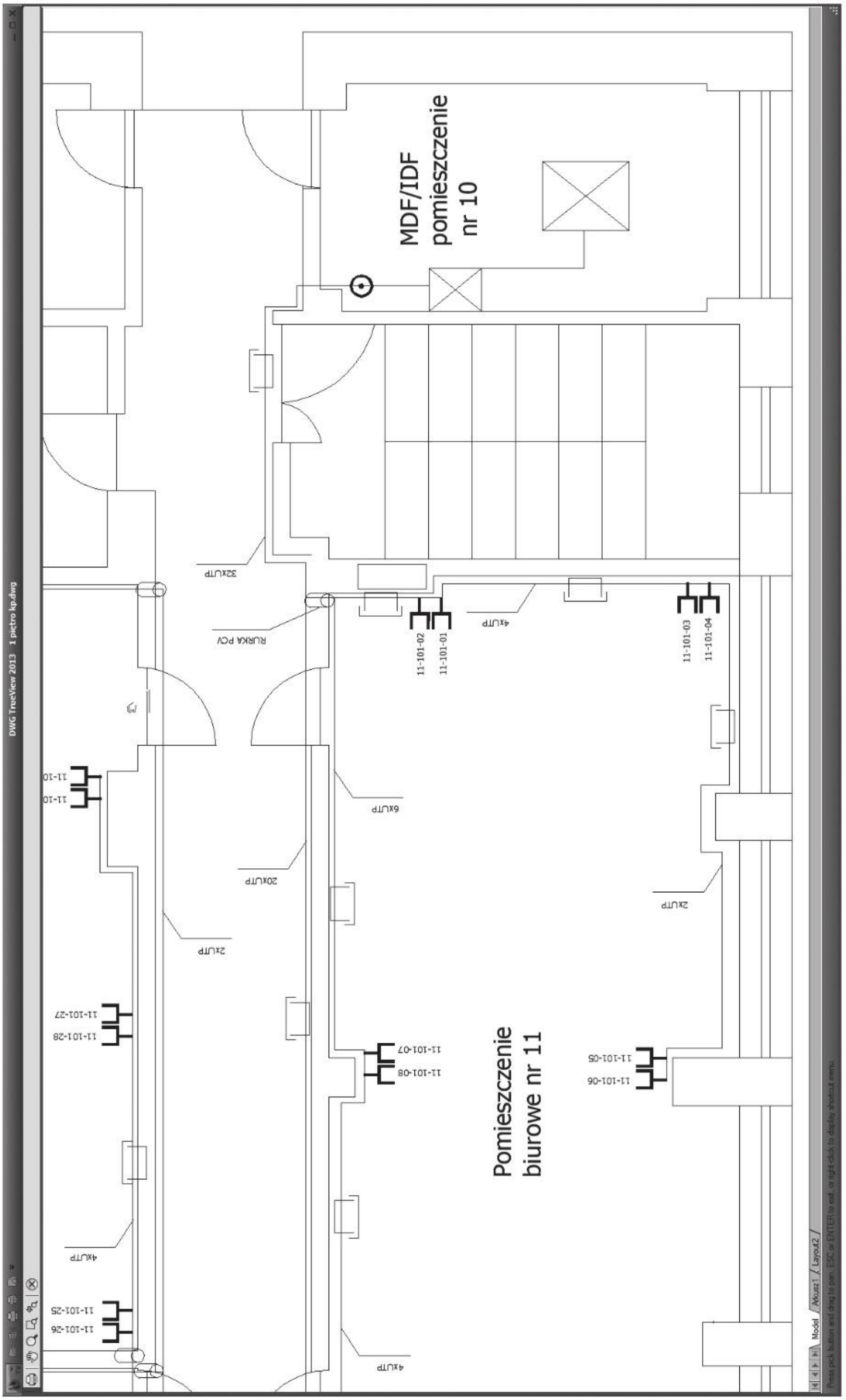
Dla każdej warstwy można zdefiniować typ i kolor linii. Ponadto warstwa może zostać zamrożona (ikona **Freeze**) – zostanie ukryta, a obiekty umieszczone na niej nie będą widoczne, lub zablokowana – zabezpieczona przed wprowadzeniem zmian (ikona **Lock**). Przekrój poziomy piętra z rys. 30.1, po wyświetleniu zawartości wszystkich warstw, przedstawiono na rys. 31.4.



Rys. 31.3. **Okno zarządzania warstwami**



Rys. 31.4. Przekrój poziomy budynku z widocznymi wszystkimi warstwami



Rys. 31.5. Przeglądanie rysunku za pomocą przeglądarki TrueView

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 rys. 31.5 przedstawiono 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).

32 Obsługa przykładowych programów do kosztorysowania

ZAGADNIENIA

Programy wykorzystywane do sporządzenia kosztorysu **Obsługiwanie przykładowego programu do sporządzania kosztorysów** **Koszty pośrednie i sposób ich uwzględniania w kosztorysie**

Niezbędnym elementem każdego projektu jest sporządzenie kosztorysu. **Kosztorys** to kalkulacja kosztów wykonania określonych robót sporządzona według ogólnie przyjętych metod i standardów. Ten dokument jest potrzebny inwestorowi do oceny nakładów, jakie musi ponieść, i do 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 poskutkować brakiem środków w budżecie, a w konsekwencji – niepowodzeniem całego projektu. Obecnie na rynku jest wiele programów, które ułatwiają sporządzenie kosztorysu. Należy jednak pamiętać, że taki program wykonuje obliczenia, ale nie może 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, zalicza się: systemy Norma PRO, Zuzia, Winbud, Rodos. Są to programy komercyjne, lecz wiele z nich jest dostępnych 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, ułatwiających sporządzanie kosztorysów obejmujących prace niewystępujące w standardowej konfiguracji programu.

Obsługa wszystkich programów do kosztorysowania jest podobna. W tym podręczniku za przykład posłuży program RODOS. Jest on również dostępny w bezpłatnej wersji studenckiej przeznaczonej dla uczniów szkół średnich i studentów.

Program umożliwia sporządzanie różnego rodzaju kosztorysów, np.:

- **kosztorysu inwestorskiego** – sporządzanego przez zamawiającego w celu ustalenia całkowitego kosztu, który inwestor jest gotów ponieść;
- **kosztorysu ofertowego** – sporządzanego przez potencjalnego wykonawcę w celu ustalenia wynagrodzenia, za które oferent jest gotów wykonać zlecenie;
- **kosztorysu powykonawczego** – sporządzanego przez wykonawcę, jeżeli w momencie zawierania umowy nie było możliwe precyzyjne ustalenie wszystkich kosztów prac.

W takim wypadku umowa powinna zawierać reguły sporządzania kosztorysu zaakceptowane przez obie strony. Kosztorys powinien zawierać:

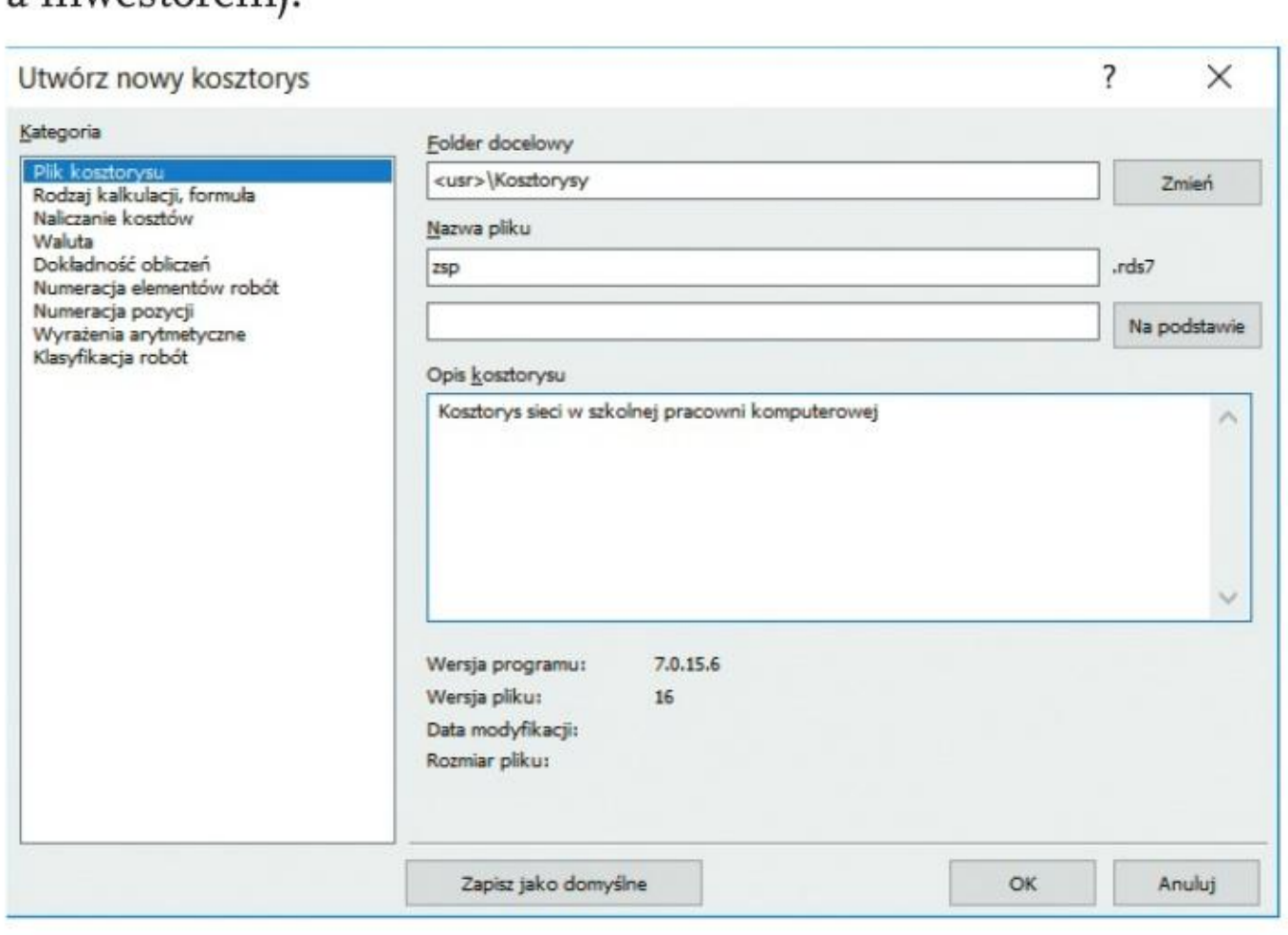
- stronę tytułową:
  - nazwę obiektu lub robót i ich lokalizację;
  - nazwę i adres zamawiającego;
  - nazwę jednostki lub nazwisko i imię osoby opracowującej kosztorys;
  - wartość robót;
  - datę opracowania kosztorysu;
- charakterystykę obiektu lub robót wraz z parametrami określającymi wielkość lub zakres robót;
- przedmiar lub obmiar robót;
- kalkulacje kosztów;
- tabelę wartości scalonych zawierającą zsumowane zestawienia wartości, łącznie z narzutami i zyskiem;
- załączniki, np. kalkulacje szczegółowe cen jednostkowych, analizy nakładów rzeczowych, cen czynników produkcji, wskaźników narzutów.

W celu ustalenia ilości robót do wykonania sporządza się **przedmiar**. Przedmiar może być sporządzony na podstawie dokumentacji. **Obmiar** przeprowadza się po wykonaniu robót na podstawie rzeczywiście wykonanych prac.

Przyjmijmy, że z przedmiaru robót wynika, że w pracowni należy zainstalować 20 gniazd, położyć 200 m kabla i zamontować szafę serwerową stojącą (robocizna). Do wykonania tego zadania jest niezbędna praca montera-instalatora (gr. V). Średnie stawki godzinowe pracowników różnych specjalności w różnych regionach kraju można odszukać w bazach cen i materiałów, np. INTERCENBUD, SEKOCENBUD (cenniki trzeba 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 kabla wynosi 1 zł/m, koszt gniazda – 20 zł, a koszt szafy – 2000 zł (materiały). Ponadto monter będzie używał narzędzi (maszyny), których godzina eksploatacji kosztuje 10 zł/h dla narzędzia uderzeniowego, 5 zł/h dla ściągacza izolacji, 20 zł/h dla przyrządu pomiarowego i 10 zł/h dla środka łączności bezprzewodowej (wartości można przyjąć na podstawie baz danych, indywidualnie sporządzanych kalkulacji lub po negocjacjach między wykonawcą a inwestorem).

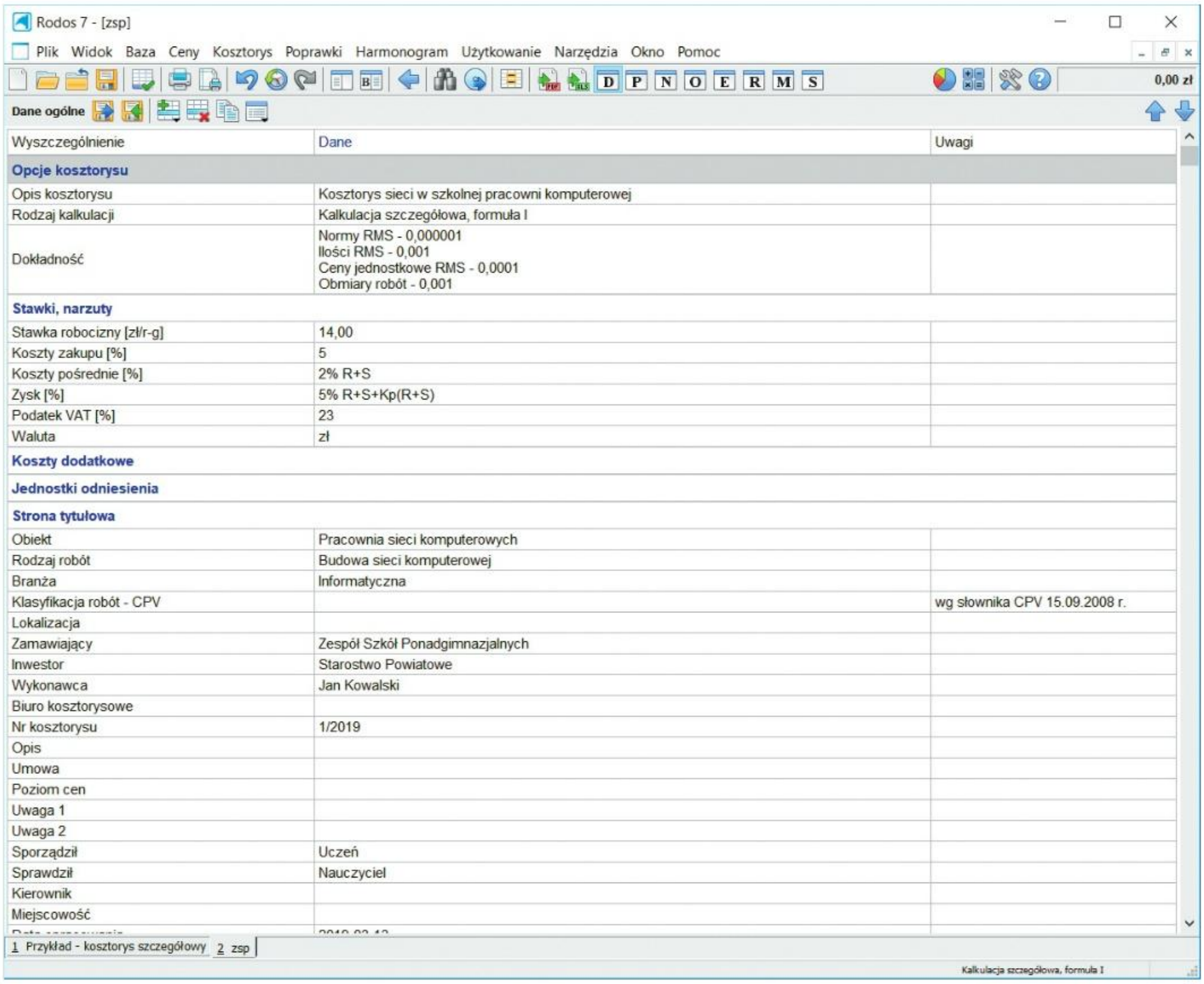
Opracowanie kosztorysu obejmuje następujące czynności:

1. Utworzenie nowego kosztorysu i naniesienie informacji podstawowych, np. nazwy pliku i typu kosztorysu (rys. 32.1).



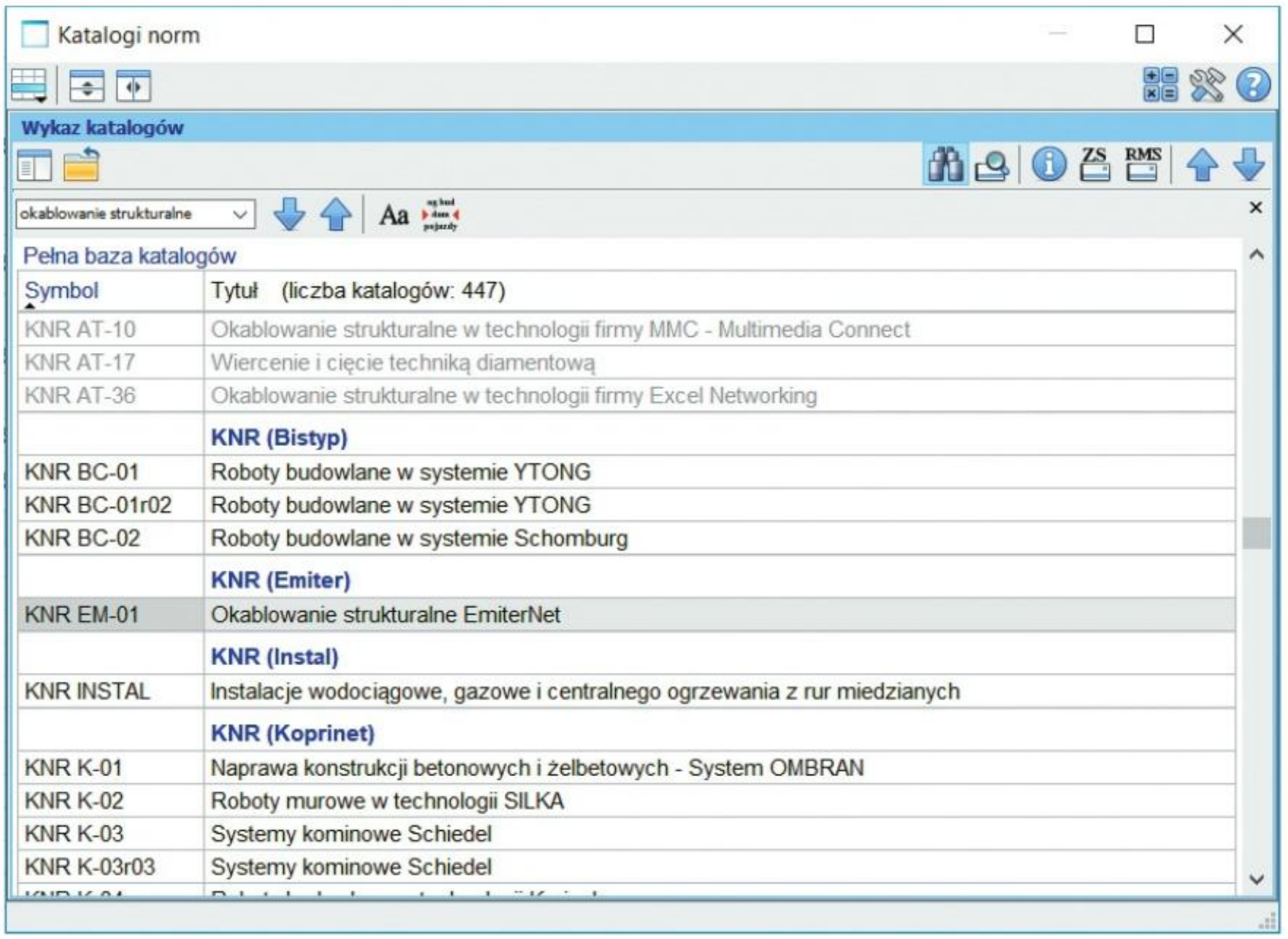
Rys. 32.1. **Utworzenie nowego kosztorysu**

2. Wprowadzenie informacji na stronę tytułową projektu. Należy kliknąć przycisk **Dane ogólne** – oznaczony literą D (rys. 32.2). W programie jest możliwe zdefiniowanie dodatkowych narzutów, zawierających zysk wykonawcy i koszty, których nie można określić bezpośrednio, podawane jako wartości procentowe od kosztów bezpośrednich, np.:
   - koszty zakupu;
   - koszty pośrednie;
   - zysk;
   - VAT.



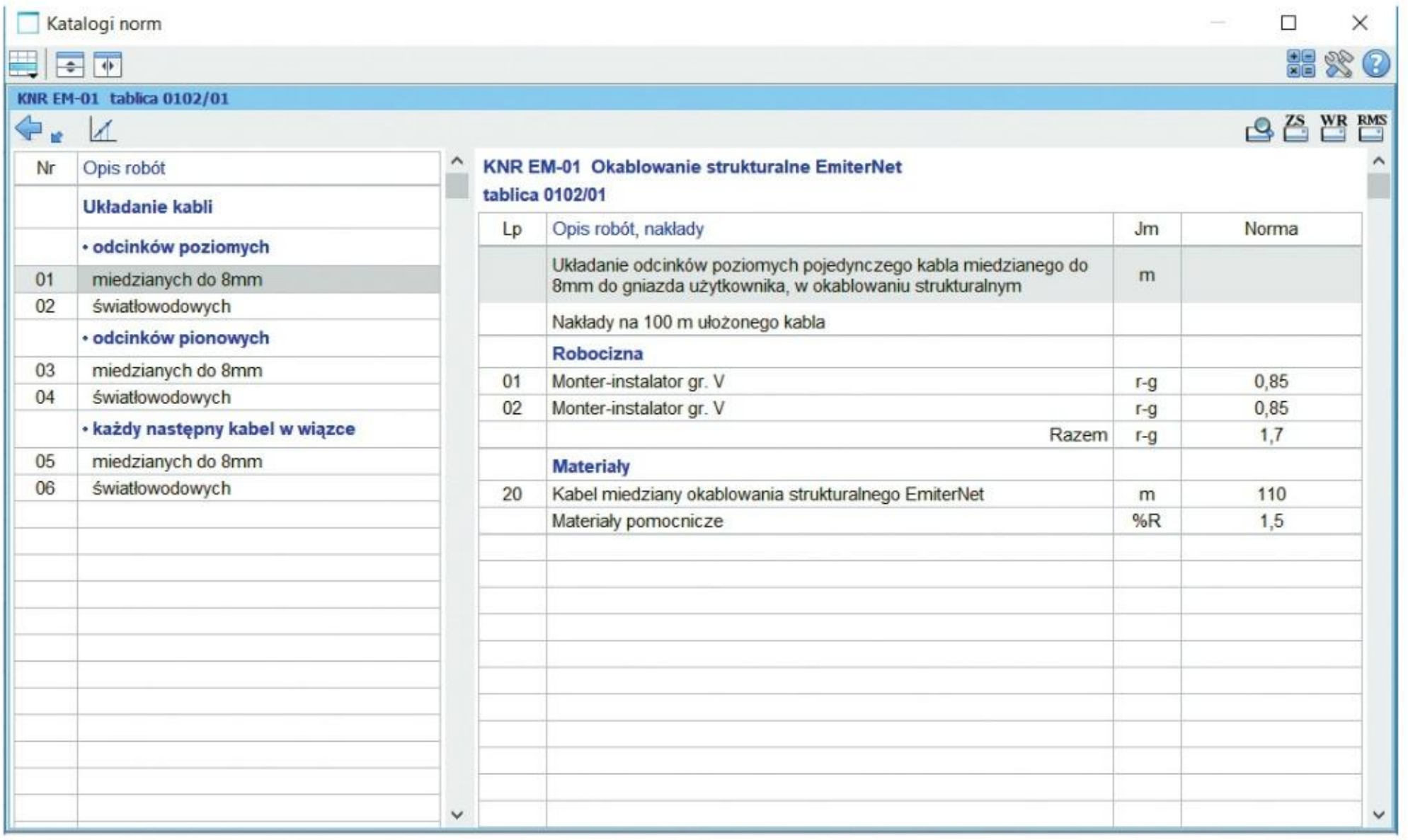
Rys. 32.2. **Wprowadzenie informacji na stronę tytułową projektu**

3. Wybrać zakładkę **Pozycje** – przycisk oznaczony literą **P**.
4. Dodać nowy element. Kliknąć prawym przyciskiem myszy kolumnę **Numer pozycji** i w menu wybrać **Dopisz element**. W polu **Opis** dodać opis elementu, np. **Okablowanie poziome**.
5. Dodać nową pozycję. Kliknąć prawym przyciskiem myszy kolumnę **Numer pozycji** i w menu wybrać **Dopisz pozycję**. Kliknąć prawym przyciskiem myszy kolumnę **Podstawa** i w menu wybrać **Katalogi norm** (rys. 32.3). W oknie wyszukiwania wpisać „okablowanie strukturalne" i odszukać katalog nakładów rzeczowych **KNR EM-01 Okablowanie strukturalne EmiterNet**. Kliknąć nazwę katalogu.



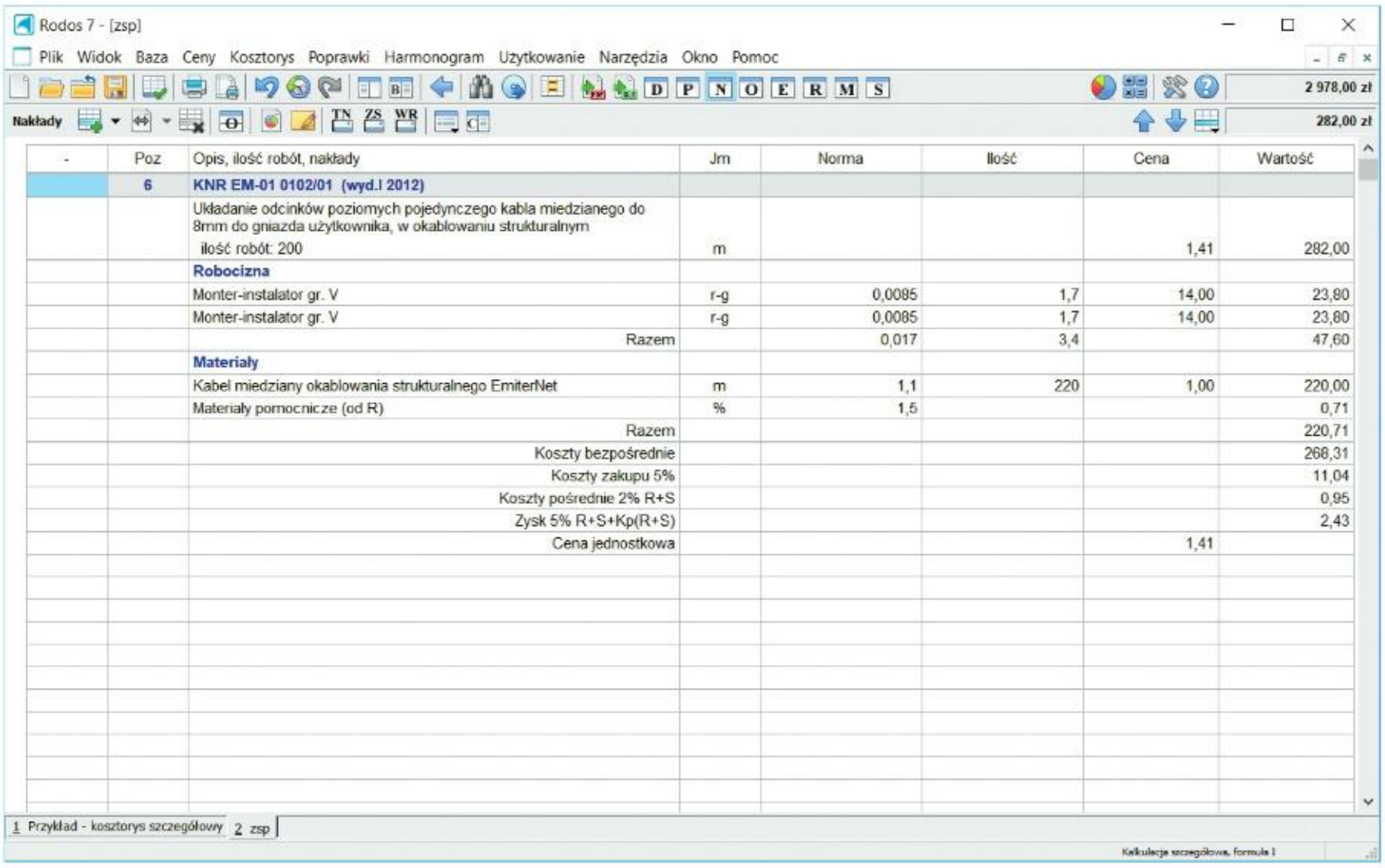
Rys. 32.3. **Dodawanie nowej pozycji**

6. Wybrać opis robót, np. **Poziome okablowanie strukturalne** (tablica 0102). W tabeli wybrać rodzaj robót na podstawie opisu, np. **Układanie kabli/odcinków poziomych/miedzianych do 8 mm** (rys. 32.4). Zatwierdzić wybór klawiszem **Enter**. Pozycja powinna zostać dopisana do kosztorysu.



Rys. 32.4. **Wybór opisu robót z katalogu KNR**

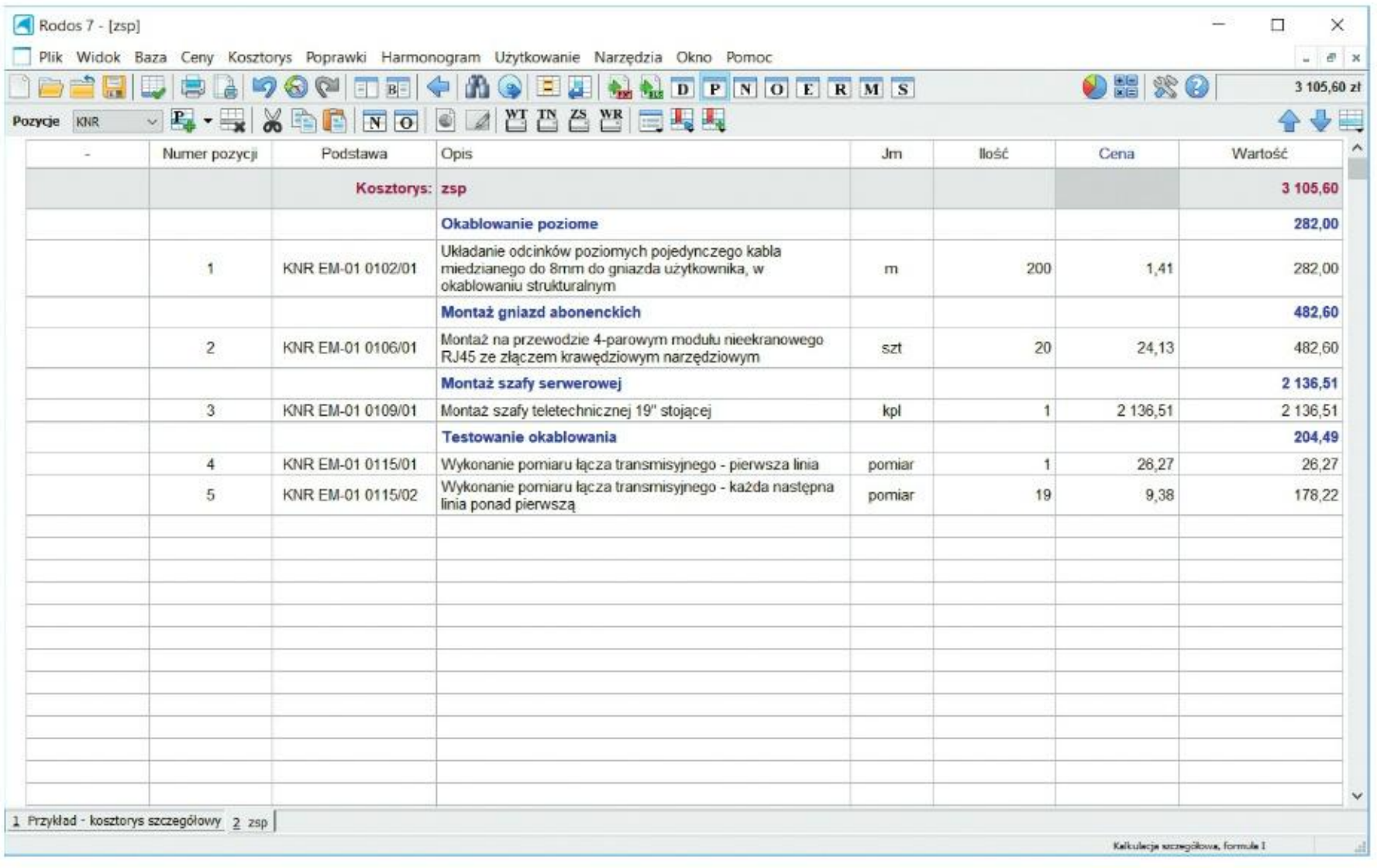
7. Wprowadzić liczbę jednostek pomiarowych, np. 200 m.
8. Kliknąć lewym przyciskiem myszy w kolumnę **Cena**. Wprowadzić koszt robocizny dla montera-instalatora, np. 14 zł, i koszt kabla, np. 1 zł. Pozostałe wartości powinny zostać obliczone automatycznie (rys. 32.5). Powrócić do zakładki **Pozycje** (przycisk **P**).



-	Poz	Opis, ilość robót, nakłady	Jm	Norma	Ilość	Cena	Wartość
	6	**KNR EM-01 0102/01 (wyd.I 2012)**					
		Układanie odcinków poziomych pojedynczego kabla miedzianego do 8mm do gniazda użytkownika, w okablowaniu strukturalnym ilość robót: 200	m			1,41	282,00
		Robocizna					
		Monter-instalator gr. V	r-g	0,0085	1,7	14,00	23,80
		Monter-instalator gr. V	r-g	0,0085	1,7	14,00	23,80
		Razem		0,017	3,4		47,60
		Materiały					
		Kabel miedziany okablowania strukturalnego EmiterNet	m	1,1	220	1,00	220,00
		Materiały pomocnicze (od R)	%	1,5			0,71
		Razem					220,71
		Koszty bezpośrednie					268,31
		Koszty zakupu 5%					11,04
		Koszty pośrednie 2% R+S					0,95
		Zysk 5% R+S+Kp(R+S)					2,43
		Cena jednostkowa				1,41	

Rys. 32.5. Wprowadzanie kosztów pozycji

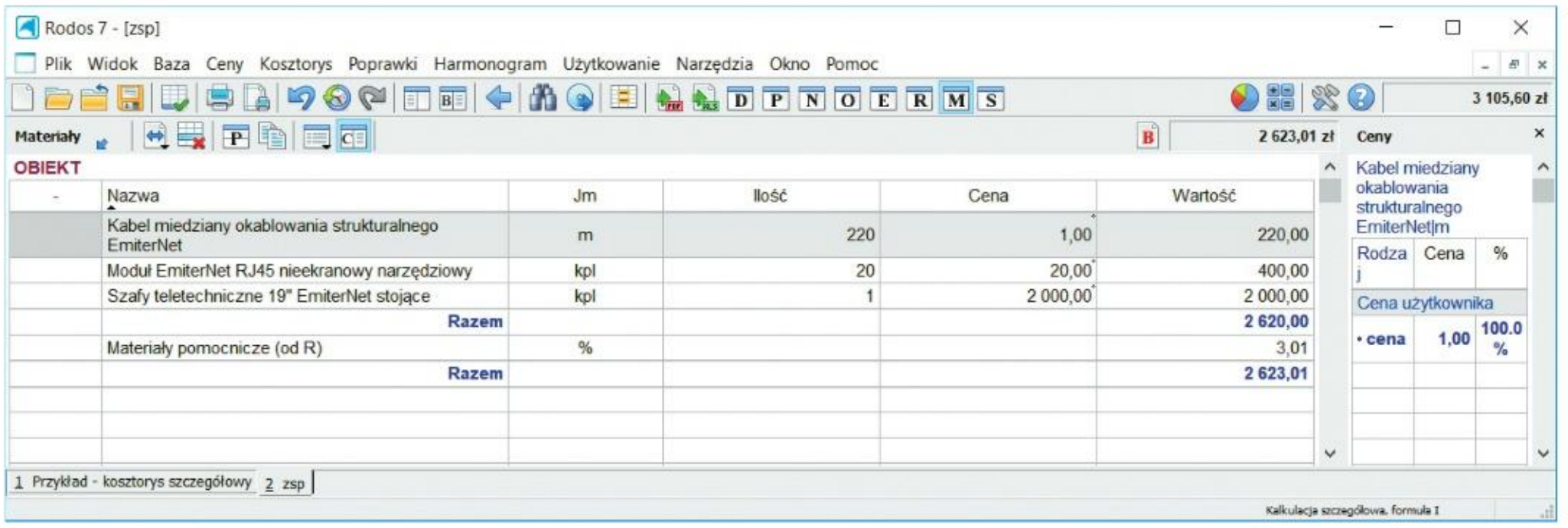
9. Wprowadzić pozostałe pozycje: montaż gniazd abonenckich, montaż szafy serwerowej, testowanie okablowania. Podsumowanie wszystkich kosztów przedstawiono na rys. 32.6. W kosztach brutto uwzględniono również VAT w wysokości 23 % ceny kosztów pośrednich.



-	Numer pozycji	Podstawa	Opis	Jm	Ilość	Cena	Wartość
		Kosztorys:	**zsp**				**3 105,60**
			Okablowanie poziome				**282,00**
	1	KNR EM-01 0102/01	Układanie odcinków poziomych pojedynczego kabla miedzianego do 8mm do gniazda użytkownika, w okablowaniu strukturalnym	m	200	1,41	282,00
			Montaż gniazd abonenckich				**482,60**
	2	KNR EM-01 0106/01	Montaż na przewodzie 4-parowym modułu nieekranowego RJ45 ze złączem krawędziowym narzędziowym	szt	20	24,13	482,60
			Montaż szafy serwerowej				**2 136,51**
	3	KNR EM-01 0109/01	Montaż szafy teletechnicznej 19" stojącej	kpl	1	2 136,51	2 136,51
			Testowanie okablowania				**204,49**
	4	KNR EM-01 0115/01	Wykonanie pomiaru łącza transmisyjnego - pierwsza linia	pomiar	1	26,27	26,27
	5	KNR EM-01 0115/02	Wykonanie pomiaru łącza transmisyjnego - każda następna linia ponad pierwszą	pomiar	19	9,38	178,22

Rys. 32.6. Podsumowanie wszystkich kosztów

Przeglądanie kosztorysu możliwe jest również w poszczególnych kategoriach: robocizna, materiały lub koszt pracy maszyn. W tym celu na zakładkach R, M, S należy zaznaczyć odpowiednią ikonę, np. M – koszty materiałów. Na rys. 32.7 przedstawiono fragment kosztorysu dotyczący kosztów materiałów.



Rys. 32.7. Koszty materiałów do wykonania okablowania

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

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

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

- 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

Projektowanie i montaż okablowania

III

33 Normy i zalecenia dotyczące montażu okablowania strukturalnego

ZAGADNIENIA

Organizacje ustanawiające normy dotyczące okablowania strukturalnego **Normy dotyczące okablowania strukturalnego obowiązujące w Polsce** **Najważniejsze zalecenia wynikające z norm okablowania strukturalnego** **Maksymalne długości kabla poziomego** **Minimalny promień gięcia** **Minimalna odległość kabla od źródeł zakłóceń**

Okablowanie strukturalne ma pozwolić na 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 zalicza się m.in.:

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

Dzięki stosowaniu standardów instalacyjnych w sieciach okablowania strukturalnego możliwe staje się 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 przeprowadzić odpowiednie zmiany w szafie dystrybucyjnej. Prace standaryzacyjne nad okablowaniem strukturalnym zapoczątkowano w USA. Pierwszą normą dotyczącą okablowania strukturalnego była norma amerykańska EIA/TIA 568. Na niej są wzorowane normy międzynarodowa ISO 11801 i europejska EN 50173. W Polsce obowiązują ponadto normy krajowe:

- PN-EN 50174-1:2018-08. Technika informatyczna -- Instalacja okablowania -- Część 1: Specyfikacja instalacji i zapewnienie jakości.
- PN-EN 50174-2:2018-08. Technika informatyczna -- Instalacja okablowania -- Część 2: Planowanie i wykonywanie instalacji wewnątrz budynków.
- PN-EN 50174-3:2014-02. Technika informatyczna -- Instalacja okablowania -- Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków.

Najważniejsze zalecenia wynikające z powyższych norm:

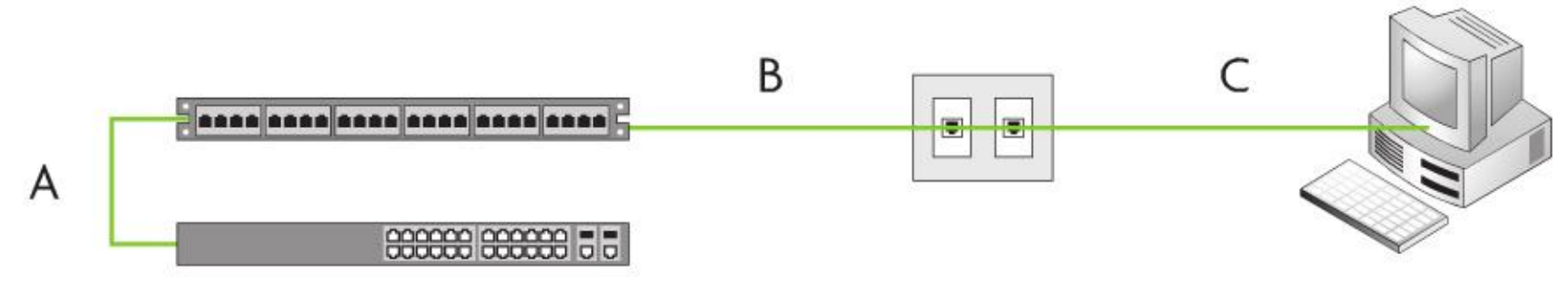
1. Okablowanie poziome powinno tworzyć nieprzerwane połączenie od punktu dystrybucyjnego do punktu abonenckiego.
2. Należy umieścić jeden punkt abonencki (2 × RJ-45) na każde 10 m^2 powierzchni biurowej.
3. Na każdym piętrze budynku powinien być punkt dystrybucyjny (w przypadku małej liczby punktów abonenckich 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 mieć pełną dokumentację.

33.1. 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 między punktem abonenckim a punktem dystrybucyjnym w panelu krosowym (patch panel) wynosi 90 m (na rys. 33.1 oznaczona literą B). Maksymalna długość kabli krosowych między panelem krosowym a przełącznikiem wynosi 6 m (na rys. 33.1 oznaczona literą A). Łączna długość kabla stacyjnego i krosowego może mieć maksymalnie 10 m (A + C).



Rys. 33.1. Kanał kablowy poziomy

Podczas układania kabla w przebiegach poziomych należy przestrzegać następujących zasad:

- Kable biegnące ponad sufitem podwieszanym nie powinny być mocowane do konstrukcji sufitu.
- Odległości między punktami mocowania kabli poziomych nie powinny być większe niż 1,2–1,5 m.
- Aby zachować przejrzystość instalacji i ułatwić obsługę, wszystkie kable należy 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).
- Podczas instalowania kabli trzeba 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.
- Na całej długości od gniazda abonenckiego do punktu dystrybucyjnego kable muszą 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°, a promień ich zagięć w kanałach 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 – zależnie od sposobu wykonania od 10 do 20 średnic.

Podczas ustalania trasy 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.

33.2. Wymagania instalacyjne dla przebiegów pionowych

Do budowy przebiegów pionowych zaleca się użycie kabli światłowodowych lub – w wyjątkowych sytuacjach – skrętki. Do prowadzenia kabli między piętrami stosuje się 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 na całej trasie kabla między najwyższym piętrem a piwnicą. Kabel należy połączyć z żyłą podtrzymującą co 90 cm, przy czym na jedno piętro powinny przypadać co najmniej trzy punkty wiązania. Dla dużych ilości kabli lub dla kabli wyjątkowo ciężkich powinna zostać użyta obejma lub osłona dla grupy kabli z każdego piętra. Ze względu na ochronę przeciwpożarową przejścia między piętrami muszą być uszczelnione za pomocą specjalnych uszczelniaczy, powłoki przeciwpożarowej, pianki, kitu itp.

33.3. Pozostałe wymagania instalacyjne

Po rozszyciu kabla w gnieździe przewody nie mogą wystawać więcej niż 25 mm poza płaszcz, a pary – być rozkręcone na długości większej niż 13 mm. Gdy instaluje się 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. Podczas prowadzenia 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 m. IDF należy podzielić na logiczne sekcje, grupujące połączenia o podobnej funkcji, o analogicznym obszarze itp. Tablice z uchwytami na kable należy zlokalizować 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 sieci projektowanej przez ciebie.

34 Funkcje urządzeń sieciowych

ZAGADNIENIA

Sprzęt montowany w szafach dystrybucyjnych **Funkcje urządzeń w warstwach dostępu, dystrybucji i rdzenia**

W punktach dystrybucyjnych gromadzi się sprzęt aktywny, taki jak przełączniki i routery, umożliwiający przyłączenie urządzeń do sieci i przyłączenie sieci do internetu. Urządzenia montuje się 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 przedstawiono na rys. 34.1.



Rys. 34.1. **Przykładowe rozmieszczenie urządzeń w szafie dystrybucyjnej**

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

- **zabezpieczenia portów** – funkcja umożliwia przełącznikowi decydowanie, ile urządzeń może się łączyć z przełącznikiem lub jakie konkretne urządzenia mogą to robić. Te decyzje najczęściej podejmuje się 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**) – ta funkcja powinna być stosowana tylko wtedy, gdy jest wymagana obsługa telefonów IP lub są bezprzewodowe punkty dostępowe i trudno doprowadzić zasilanie do żądanego miejsca;
- **obsługa jakości usług** (**QoS**) – umożliwia nadawanie priorytetu określonym rodzajom danych, które administrator chciałby traktować w sposób szczególny, np. przesyłać szybciej niż inne rodzaje danych;
- **agregacja łączy** – ta funkcja pozwala przełącznikowi na wykorzystywanie jednocześnie kilku portów jako jednego łącza logicznego o dużej szerokości pasma. Najczęściej będzie wykorzystywana 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 większa wydajność przetwarzania i funkcjonalności warstwy 3);
- **stosowanie zaawansowanych zasad zapewniających bezpieczeństwo ruchu w sieci** – listy kontroli dostępu ACL (ang. *Access Control List*) umożliwiają przełącznikowi zezwalanie na określony typ ruchu i niezezwalanie na inny, jak również 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 i umożliwiały takie zaprojektowanie infrastruktury, że w razie 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, a zagregowane łącza – do warstwy 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. Muszą cechować się dużą nadmiarowością, np. być zaopatrzone w nadmiarowe zasilacze, które można wymieniać bez przerywania pracy przełącznika, oraz w funkcje chłodzenia z możliwością wymiany wentylatorów bez konieczności wyłączania przełącznika. 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.

35 Symbole graficzne dotyczące lokalnych sieci komputerowych

ZAGADNIENIA

Symbole używane do reprezentowania elementów sieci lokalnych **Umieszczanie na rysunkach dodatkowych oznaczeń, np. sposób prowadzenia kabli**

Sieci komputerowe w dokumentacji przedstawia się za pomocą schematów, w których poszczególne urządzenia zastępuje się symbolami. Na rysunkach schematycznych przedstawia się zasadnicze elementy bez określania szczegółów, np. wyglądu, wymiarów urządzeń. Schemat logiczny okablowania strukturalnego sieci przedstawiono na rys. 35.1. Na schemacie można zobaczyć zależności i połączenia logiczne między punktami dystrybucyjnymi sieci.

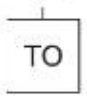
Użyte symbole oznaczają:



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

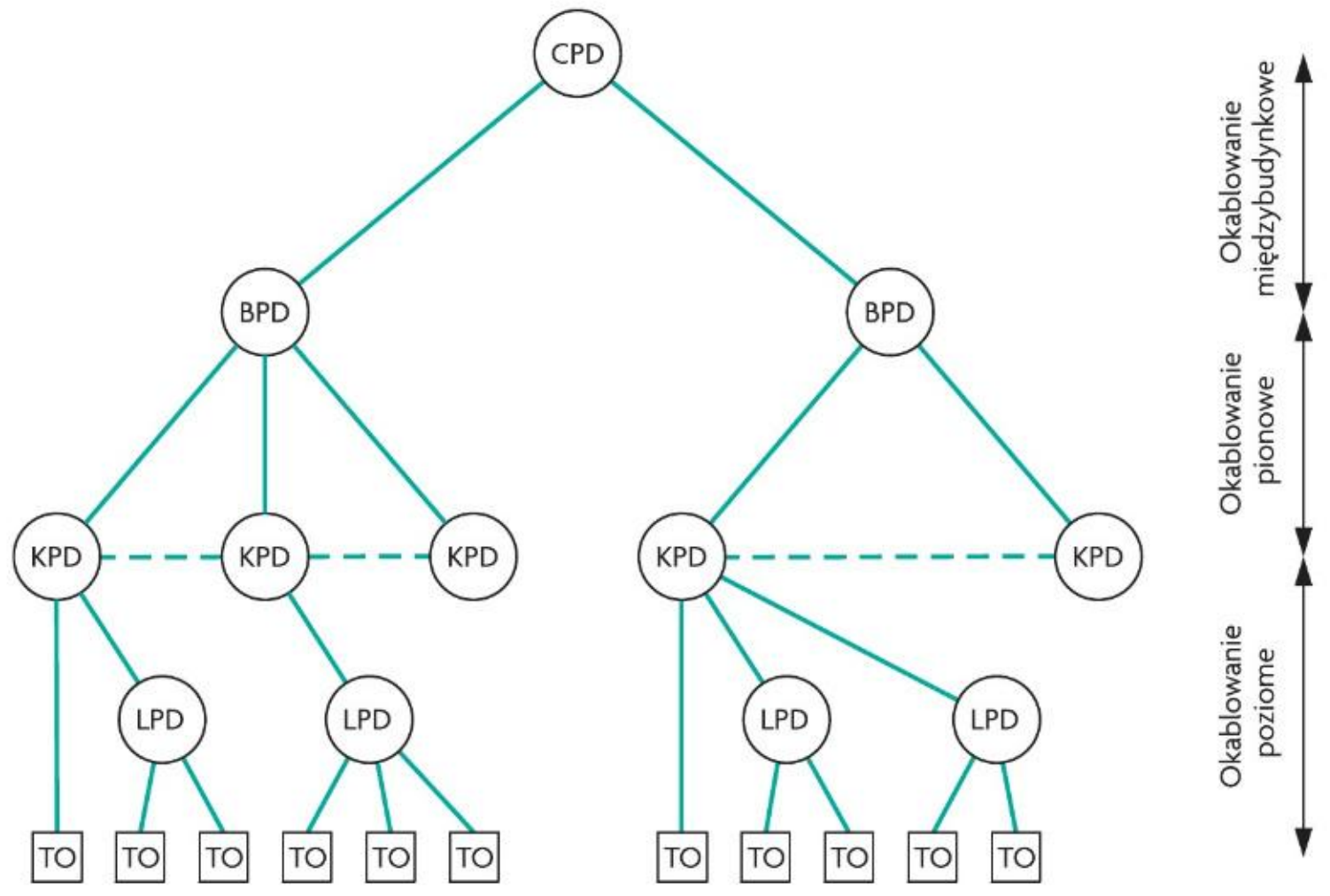


– lokalny punkt dystrybucyjny LPD;



– gniazdo telekomunikacyjne TO.

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



Rys. 35.1. **Schemat logiczny sieci komputerowej**

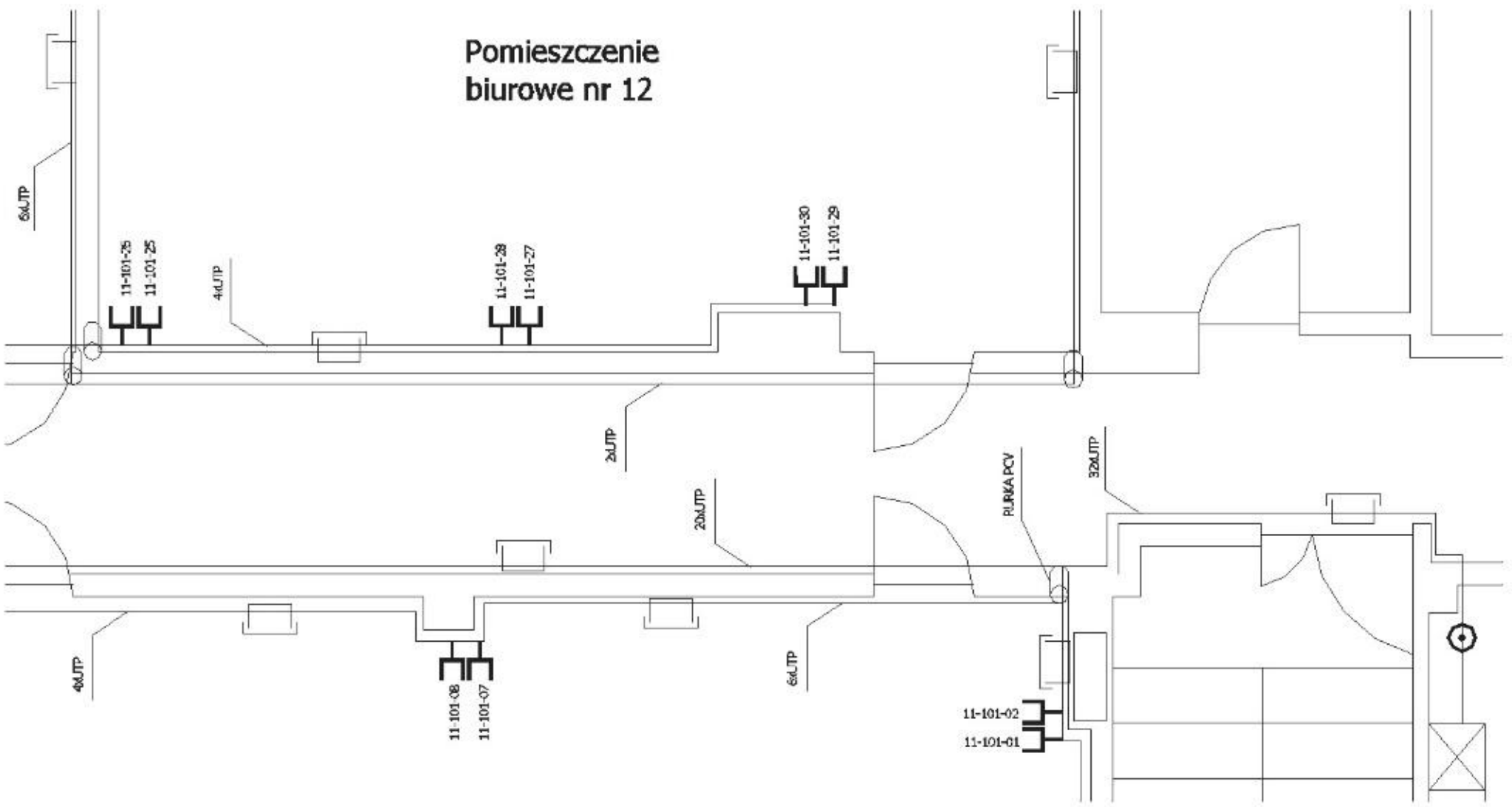
Monter sieci komputerowej w pracy posługuje się planem instalacji, na którym zaznaczono rozmieszczenie gniazd oraz liczbę i sposób prowadzenia kabli. W planach stosuje się symbole

używane w rysunku technicznym elektrycznym opisane w normie PN-EN 60617[3]. Symbole graficzne stosowane w schematach. Przykłady symboli i ich znaczenie podano w tabeli 35.1.

Tabela 35.1. 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

Oprócz symboli, na planach umieszcza się również dodatkowe opisy, określające np. oznaczenia gniazd lub liczbę i typ kabli. Przykład fragmentu planu z naniesionymi oznaczeniami przedstawiono na rys. 35.2.



Rys. 35.2. Fragment planu instalacji okablowania strukturalnego

[3] Norma wycofana.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Użyj symboli do wykonania schematu projektowanej sieci.
2. Na rysunek techniczny budynku nanieś oznaczenia gniazd, kabli i sposób ich prowadzenia (skorzystaj z oddzielnej warstwy).

36 Zasady bezpiecznej i higienicznej pracy podczas montażu

ZAGADNIENIA

Przepisy prawne regulujące kwestie związane z bhp **Podstawowe zasady bhp podczas prac montażowych**

Podstawowym aktem prawnym regulującym w ogólny sposób sprawy bezpieczeństwa i higieny pracy jest ***Kodeks pracy*** (**kp**). Do *Kodeksu pracy* wydano wiele aktów prawnych wykonawczych, w których omówiono 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; usunąć wszystkie zbędne przedmioty, które mogłyby krępować swobodę ruchów i spowodować niebezpieczeństwo.
3. Pomieszczenia, w których wykonuje się prace, powinny być niedostępne dla osób niezatrudnionych bądź ruch w tych pomieszczeniach powinien być ograniczony do niezbędnych przypadków.
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 napisy ostrzegawcze. Wszystkich pracowników i inne osoby trzeba 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 i za właściwe 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. Aby w razie wypadku umożliwić doraźną pomoc medyczną, należy umieścić apteczki w miejscach widocznych i dostępnych.
13. Podczas prac na wysokości narzędzia trzeba 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 muszą być używane drabiny, rusztowania itp.
14. Na drabinie może przebywać tylko jedna osoba. Nie wolno wiązać ze sobą dwóch krótkich drabin w celu uzyskania jednej dłuższej. Osoba, która wchodzi na drabinę, musi mieć obie ręce wolne, aby lepiej się jej trzymać.
15. Przed rozpoczęciem pracy ze sprzętem i narzędziami o napędzie elektrycznym, np. wiertarkami, należy sprawdzić, czy działają one prawidłowo.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Scharakteryzuj zasady bhp związane z pracami montażowymi.

37 Zasady organizacji pracy i analizy harmonogramów prac

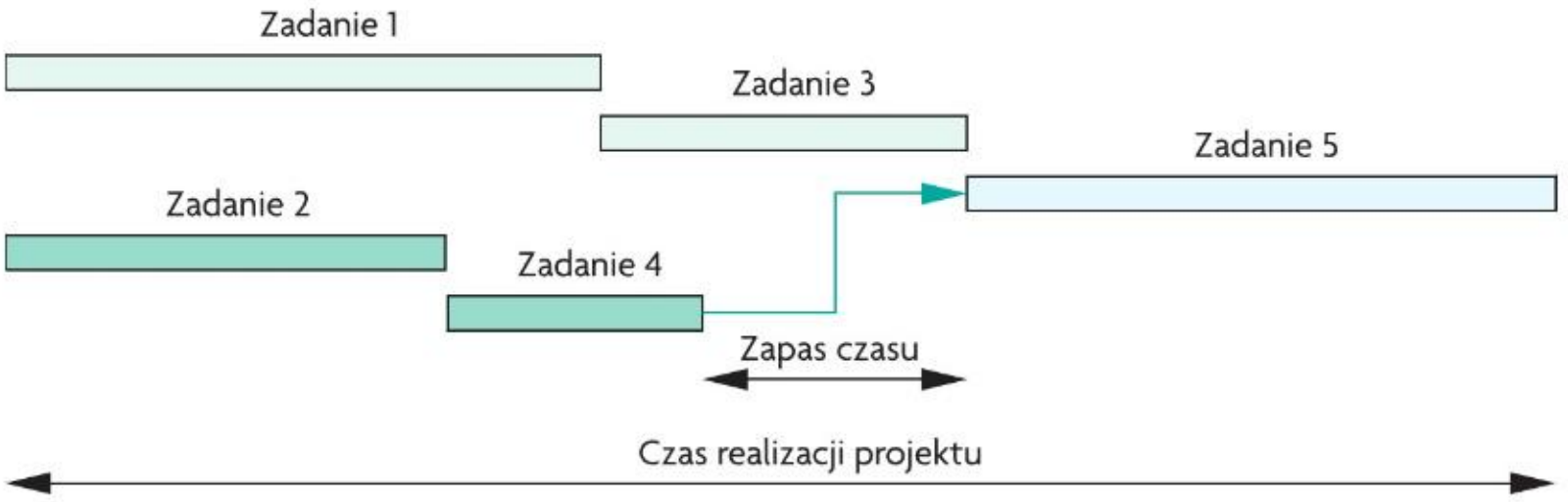
ZAGADNIENIA

- **Ścieżka krytyczna i sposób jej wyznaczania**
- **Właściwości ścieżki krytycznej**

Realizacja projektu, np. okablowania strukturalnego, wymaga zaangażowania materiałów i 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 końca. Istotnym czynnikiem jest zapewnienie odpowiedniego **harmonogramu pracy**, tak aby każdy pracownik zaangażowany w projekt wiedział, jakie zadanie i kiedy ma je 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 nazywa się **ścieżką**. W każdym projekcie można wyróżnić ścieżkę krytyczną. Jest to nieprzerwany ciąg zadań o najdłuższym czasie realizacji. Wszystkie zadania znajdujące się na ścieżce krytycznej nazywa się **zadaniami krytycznymi**. Opóźnienie któregokolwiek z nich poskutkuje późniejszym zakończeniem całego projektu.

Przykład wykresu Gantta z pięcioma zadaniami przedstawiono na rys. 37.1. 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. 37.1. 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 jest równoznaczne z zakończeniem projektu.

- Od czasu trwania ścieżki krytycznej zależy czas trwania całego projektu. Jeżeli istnieje więcej niż jedna ścieżka krytyczna, to wszystkie ścieżki krytyczne mają ten sam sumaryczny czas trwania.
- Ścieżka krytyczna może się zmienić w czasie trwania projektu, jeśli czas wykonania poszczególnych zadań będzie się różnił od początkowo zakładanego.

Skrócenie czasu realizacji zadania w niektórych przypadkach jest możliwe przez zaangażowanie większych zasobów, np. przez zwiększenie liczby pracowników. Jeżeli w zadaniu występuje szeroki front robót, a pracochłonność jakiegoś zadania jest obliczona, np. na 10 rg., 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 przełoży się na wydłużenie czasu realizacji, np. jeżeli istnieje konieczność przeprowadzenia uzgodnień dotyczących wykonywanej pracy między 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 mogą być związane z wykorzystaniem zasobów, np. ludzkich, sprzętu. Stopień wykorzystania budżetu projektu powinien być porównywany z poziomem zaawansowania prac. Najczęściej te analizy sporządza się po zakończeniu pewnego etapu prac, po spełnieniu określonego warunku lub po zrealizowaniu pewnego produktu cząstkowego (tzw. kamienie milowe projektu). W razie rozbieżności należy wprowadzić modyfikacje, aby jak najwcześniej zapobiec przekroczeniu budżetu.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zidentyfikuj w swoim projekcie ścieżkę krytyczną. Wymień wszystkie zadania krytyczne.
2. Czy w twoim projekcie występuje zapas czasu? Jeśli tak, to na którym etapie i ile wynosi?

38 Narzędzia do montażu okablowania strukturalnego

ZAGADNIENIA

Narzędzia wykorzystywane do montażu okablowania strukturalnego **Posługiwanie się narzędziami do montażu okablowania strukturalnego** **Spawanie światłowodu**

Instalator okablowania strukturalnego musi posługiwać się różnymi narzędziami i urządzeniami. Zależnie 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 i instalacji pomocniczych, np. koryt kablowych. Do najczęściej używanych narzędzi do montażu okablowania miedzianego zalicza się:

- **narzędzie uderzeniowe** – nóż krosowniczy, urządzenie (rys. 38.1) wykorzystywane do „zaszywania" kabli sieciowych i telefonicznych w nożach (złączach) LSA/KRONE, gniazdkach komputerowych, telefonicznych, panelach krosowych w szafach itp. Wyposażone w obcinacz nadmiaru kabla wystającego poza złącze i 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 RJ-45** – wtyk RJ-45 z odpowiednio ułożonymi żyłami kabla należy wsunąć w gniazdo narzędzia (rys. 38.2), a następnie zacisnąć dźwignię;



Rys. 38.1. Narzędzie uderzeniowe do montażu kabli



Rys. 38.2. Narzędzie zaciskowe do wtyków RJ-45

- **narzędzie do zdejmowania izolacji** (rys. 38.3) – pozwala na szybkie i wygodne zdjęcie izolacji zewnętrznej kabla. Zabezpiecza kabel przed zbyt mocnym nacięciem izolacji, co mogłoby uszkodzić przewód.



Rys. 38.3. **Narzędzie do zdejmowania izolacji**

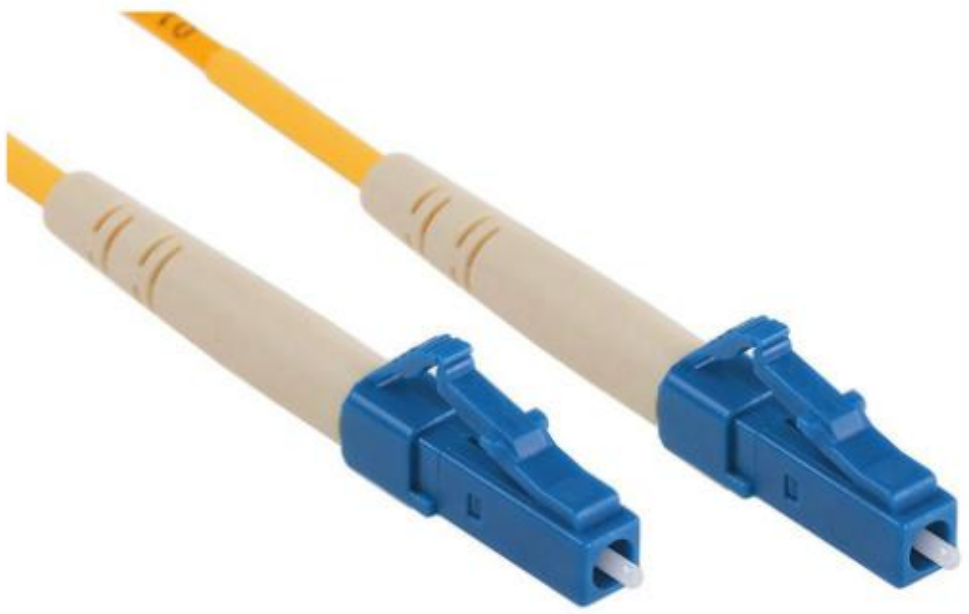
Montaż okablowania światłowodowego jest znacznie trudniejszy. Należy pamiętać, że podczas uruchamiania urządzeń aktywnych mamy do czynienia ze światłem o dużej mocy, zwykle emitowanym przez laser lub diodę LED. Typowe długości fali optycznej w transmisji danych są bliskie podczerwieni i wynoszą od 850 nm do 1550 nm – tego światła nie widać, jednak może ono poważnie uszkodzić oczy (nie warto patrzeć w nadajnik ani we włókno światłowodu, bo i tak nic nie zobaczymy, a możemy ucierpieć).

W montażu okablowania światłowodowego wykorzystuje się przygotowane wcześniej kable o określonej długości, zakończone odpowiednimi końcówkami (można je kupić u producentów lub w wyspecjalizowanych firmach). Wybór typu końcówki jest zwykle narzucony przez standard, w którym wykonano urządzenia aktywne. Najczęściej wykorzystuje się końcówki:

- **SC** (rys. 38.4) – plastikowa obudowa i pewne połączenie;
- **LC** (rys. 38.5) – mniejsze od poprzedniego, dość popularne ze względu na małe gabaryty i na wykorzystanie w modułach SFP;
- **ST** (rys. 38.6) – metalowe, przypominające elektryczne złącze BNC, stosowane częściej w sieciach wielomodowych.



Rys. 38.4. **Końcówka kabla SC**



Rys. 38.5. **Końcówka kabla LC**



Rys. 38.6. **Końcówka kabla ST**

Jeżeli wykorzystanie gotowego kabla z zamontowanymi końcówkami jest niemożliwe, można kupić prefabrykowane tzw. **pigtaile** (rys. 38.7): z jednej strony zakończone złączem, a z drugiej – gołym włóknem. Pigtail należy zespawać z włóknami kabla za pomocą **spawarki do światłowodów** (rys. 38.8).



Rys. 38.7. **Pigtail**



Rys. 38.8. **Spawarka do światłowodów**

Spawanie światłowodu polega na zetknięciu dwóch włókien czołami i nadtopieniu ich łukiem elektrycznym, tak aby zostały trwale połączone. Dobrze wykonany spaw jest w zasadzie niewidoczny dla światła. Spawanie wymaga wysokich kwalifikacji pracowników, jak również poniesienia dużych nakładów na zakup spawarki oraz urządzeń testujących. Istnieje możliwość wykonania tzw. spawów mechanicznych – jest 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 i 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 *patch panelu*. Przetestuj, czy złącze jest wykonane poprawnie.
4. Wyszukaj w internecie informacji, jaki zestaw narzędzi jest potrzebny do pracy z kablami światłowodowymi. Wymień nazwy używanych narzędzi. Jaki jest koszt zakupu spawarki do światłowodów?

39 Metody i zasady pomiarów okablowania strukturalnego

ZAGADNIENIA

Pomiary okablowania wykonywane podczas montażu i odbioru sieci **Normy i standardy dotyczące pomiarów okablowania sieci** **Parametry 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 i brak przejść. W czasie odbioru 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 do transmisji wykorzystuje się tylko dwie pary przewodów. Dlatego zgodnie z biuletynem TIA/EIA/TSB-67 L.II wystarczy przeprowadzić pomiar takich parametrów, jak:

- **przesłuch zbliżny** (ang. *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 wartość bezwzględna NEXT, tym lepsza jest odporność na zakłócenia pochodzące od sygnałów w innych parach kabla. Wartość parametru NEXT jest silnie zależna od częstotliwości. Dlatego należy przeprowadzić pomiar w paśmie częstotliwości od 1 MHz do 100 MHz;
- **tłumienie** (ang. *attenuation*) – określa, o ile zmniejszy się moc sygnału w danej parze przewodów po przejściu przez cały tor kablowy. Parametr jest ściśle zależny od częstotliwości. Pomiar przeprowadza się w paśmie od 1 MHz do 100 MHz;
- **mapa połączeń** (ang. *wire map*) – określa, w jakiej sekwencji są ułożone w złączu lub gnieździe poszczególne pary przewodów. Najczęściej spotykanymi sekwencjami są EIA-568A i EIA-568B. Parametr służy do wykrycia błędów instalacyjnych, takich jak:
  - zamienione pary (ang. *crossed pairs*);
  - zamienione poszczególne przewody (ang. *split pairs*);
  - zamienione przewody w parze (ang. *reversed pairs*);
- **długość** (ang. *length*) – określa długość mierzonego toru transmisyjnego. Długość toru transmisyjnego na ogół jest większa od długości kabla, ponieważ pary są skręcone ze sobą, a dodatkowo – wokół wspólnej osi. Rzeczywistą długość toru transmisyjnego wyznacza się przez pomiar czasu propagacji impulsu elektrycznego lub świetlnego przy znanej prędkości propagacji w danym typie kabla.

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

Wymagania stawiane okablowaniu dla sieci pracujących z prędkością 1 Gb/s są znacznie wyższe (w transmisji wykorzystuje się wszystkie pary przewodów). 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 między pomiarami parametrów NEXT i PowerSum NEXT polega na tym, że podczas pomiaru PowerSum NEXT mierzy się 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 przewodów;
- **PowerSum ACR** (ang. *attenuation to crosstalk ratio*) – określa różnicę między 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;
- **przesłuch zdalny FEXT** (ang. *far end crosstalk*) – w przeciwieństwie do przesłuchu zbliżnego NEXT mierzy się go 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. Dlatego 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** (ang. *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 między wartością parametru FEXT a wartością tłumienia dla danego toru transmisyjnego;
- **PowerSum ELFEXT** – parametr uwzględnia, że zakłócenia mogą pochodzić nie tylko od jednej, lecz także od trzech pozostałych par (w kablu czteroparowym). Jest wynikiem obliczeń z wartości parametru ELFEXT dla każdej pary przewodów w kablu.
- **straty odbiciowe** (ang. *return loss*) – parametr określający stosunek mocy sygnału wprowadzonego do toru transmisyjnego do mocy sygnału odbitego, który powstaje na skutek niedopasowania impedancji toru transmisyjnego. Sygnał może być źródłem zakłóceń dla sygnału użytecznego, co jest bardzo istotne dla transmisji w dwóch kierunkach w tym samym torze transmisyjnym;
- **Propagation Delay Skew** – określa różnicę opóźnienia transmisji między najszybszą a 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 mógł poprawnie zdekodować 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. Poza tym długość kanału nie może być większa niż ta podana przez producenta. Jeśli w kanale stosuje się większą liczbę 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** (ang. *Optical Time-Domain Reflectometer*, OTDR). Umożliwia on pomiar lub certyfikację światłowodów, przeprowadzanie testów PASS/FAIL, pomiar odległości i tłumienia.

Podczas odbioru instalacji okablowania strukturalnego wykonuje się pomiary wszystkich torów komunikacyjnych. Pomiary przeprowadza 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.

40 Metody pomiarów sieci logicznej

ZAGADNIENIA

Strategie testowania sieci komputerowej **Odczytywanie informacji o wartości sygnału i szumu w sieci bezprzewodowej** **Wykonywanie skanowania pasma radiowego wykorzystywanego przez sieci bezprzewodowe**

Sieć komputerowa ze względu na swoją budowę jest obiektem trudnym do testowania. W sieciach może pojawiać się wiele błędów z powodu złożoności i różnorodności struktury sieci LAN, różnych mediów transmisyjnych i znacznej liczby producentów sprzętu. Ich lokalizacją i usuwaniem zajmuje się administrator. W większości przypadków niewłaściwa 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: odgórne i oddolne. **Testowanie odgórne** (ang. *top down*) rozpoczyna się od najwyższej warstwy sieciowej, po czym kolejno diagnozuje się 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. Tę metodę stosuje się głównie w sieciach już działających. W strategii **testowania oddolnego** (ang. *bottom up*) testowanie rozpoczyna się od warstwy najniższej, czyli od 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 obu sposobów diagnozowania sieci.

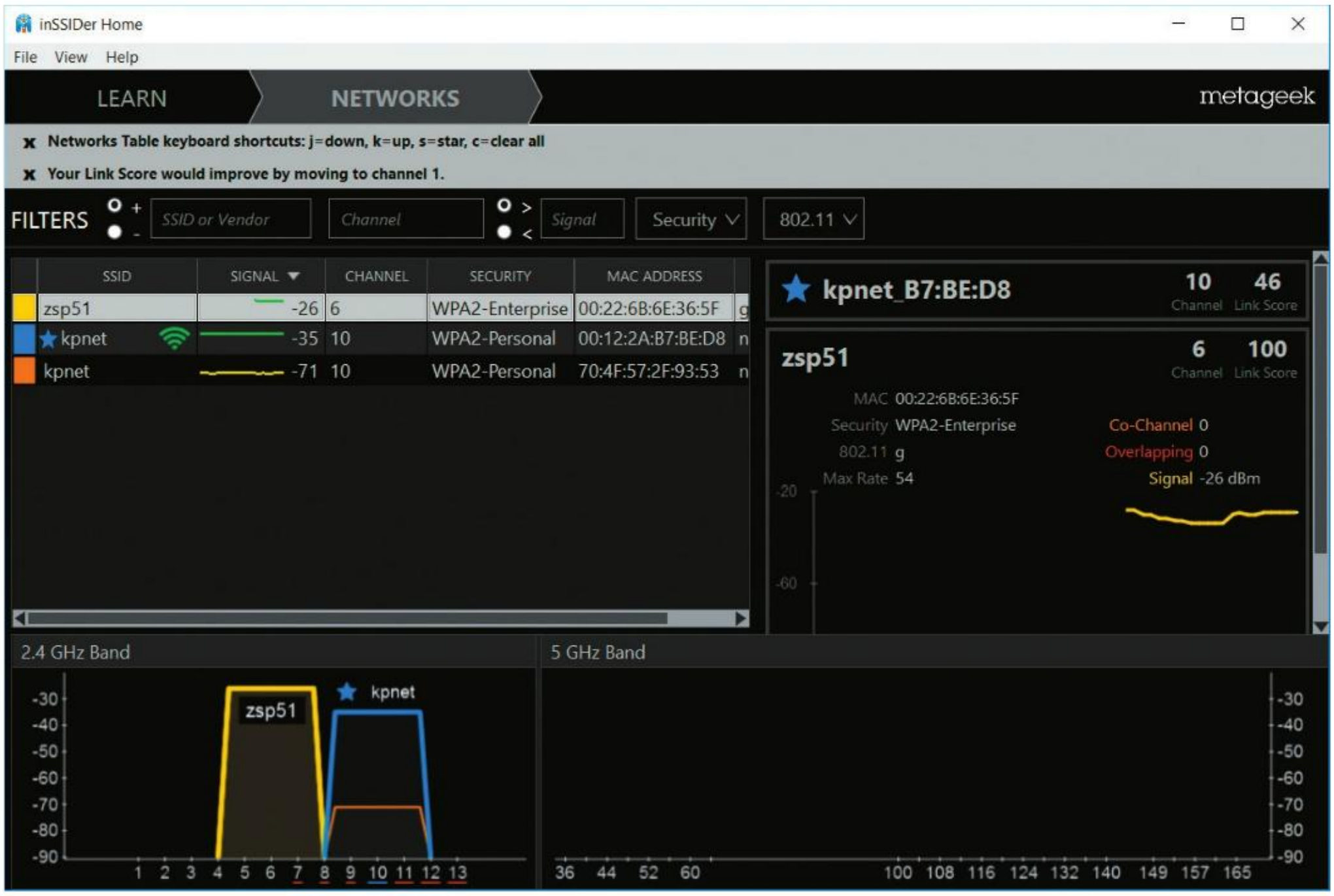
W sieciach komputerowych wykorzystuje się model sieci ISO/OSI i przyporządkowuje błędy do poszczególnych warstw modelu. Dzięki temu testowanie staje się prostsze, ponieważ w każdej warstwie występują inne typy błędów. Pomiary sieci komputerowych można podzielić na: **pomiary parametrów fizycznych okablowania** (miedzianego lub światłowodowego), **pomiary pasywne**, przeprowadzane wyłącznie przez obserwację funkcjonowania sieci, i **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 bezprzewodowych sieciach komputerowych duże znaczenie ze względu na szybkość i stabilność połączenia mają: siła sygnału radiowego, wartość szumu i stosunek sygnału do szumu docierającego do karty sieciowej. Na rys. 40.1 przedstawiono wynik skanowania pasma radiowego wykorzystywanego przez sieci bezprzewodowe. Do skanowania użyto programu **inSSIDer**.

Najlepszą moc sygnału ma sieć zsp51, pracująca na kanale 6. Jej **wskaźnik mocy odbieranego sygnału radiowego** (ang. *Received Signal Strength Indication*, **RSSI**) jest najlepszy. Im wartość RSSI jest wyższa (mniejsza wartość ujemna), tym moc sygnału jest większa. Zakłada się, że jeżeli wskaźnik spadnie poniżej –70 dBm, to w sieci mogą pojawić się problemy wynikające ze zbyt słabego sygnału.



Rys. 40.1. Wynik skanowania pasma radiowego wykorzystywanego przez sieci Wi-Fi

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?

41 Rodzaje testów i pomiarów pasywnych

ZAGADNIENIA

Pomiary pasywne sieci **Przechwytywanie za pomocą sniffera danych przesyłanych w sieci** **Analizowanie danych przechwyconych przez sniffera**

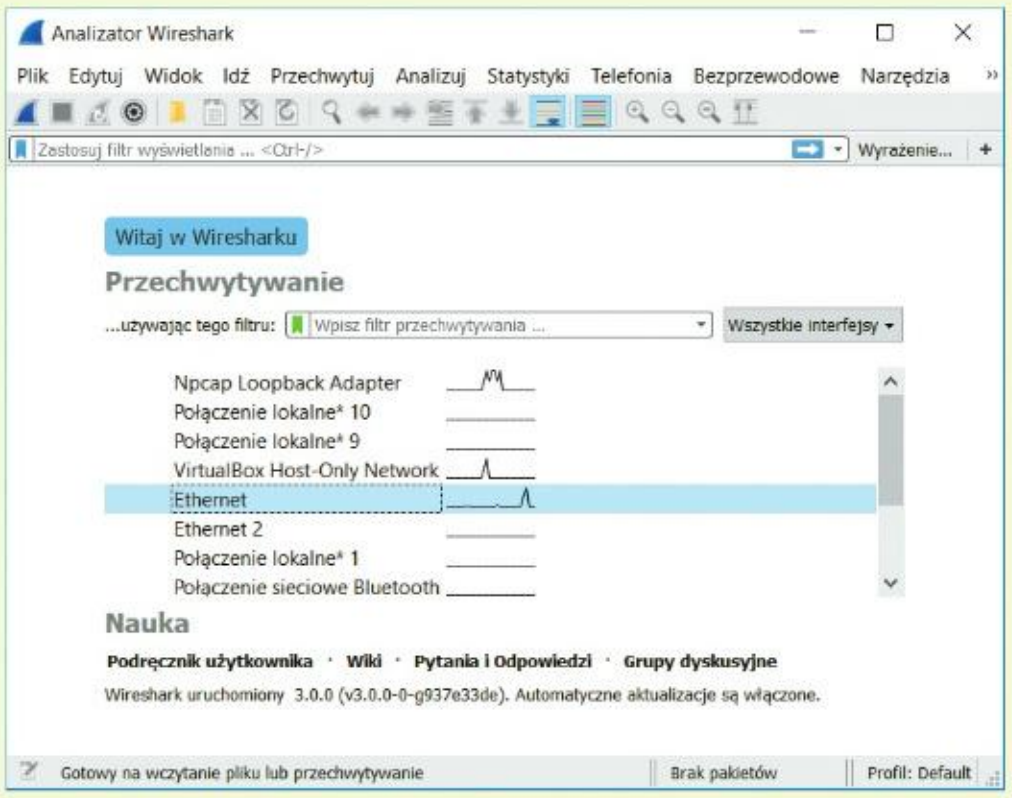
Podczas wykonywania **testów pasywnych** administrator tylko obserwuje funkcjonowanie sieci. W wielu sytuacjach jest to wystarczające do zebrania informacji o sposobie jej działania. Dużo informacji dotyczących funkcjonowania sieci administrator może uzyskać dzięki monitorowaniu ruchu pakietów między urządzeniami. Treści nagłówków jednostek danych umożliwiają dokładną analizę ruchu i jego zawartości. Programy wykorzystywane do tego celu nazywa się 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 i ramki rozgłoszeniowe. Sniffer przełącza kartę sieciową w tryb mieszany (ang. *promiscuous*), w którym urządzenie odbiera wszystkie ramki z segmentu sieci. Sniffery wykorzystuje się do analizowania ruchu w sieci zarówno przez administratorów, jak i przez 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**. Jest on dostępny w wersji na platformy Windows, Linux i MacOS X. Program można bezpłatnie pobrać ze strony http://www.wireshark.org/download.html. Pracuje on w środowisku graficznym, choć w środowisku Windows wymaga zainstalowanej biblioteki WinPcap (najnowsze wersje są dostarczane razem z biblioteką).

PRZYKŁAD 41.1

Przechwytywanie danych i analiza nagłówków

1. Uruchomić program Wireshark.
2. W oknie wyboru interfejsu (rys. 41.1) wskazać, który interfejs ma być ustawiony w trybie przechwytywania danych.
3. Uruchomić dowolny program generujący przepływ danych w sieci, np. polecenie **`ping`**, albo zaczekać na pojawienie się ruchu w sieci.
4. Obserwować w oknie głównym programu przychwytywane dane. Po zebraniu wymaganej liczby danych zatrzymać przechwytywanie poleceniem **`Przechwytuj/Stop`**. W oknie rozwinąć gałęzie Ethernet II i Internet Protocol Version 4.

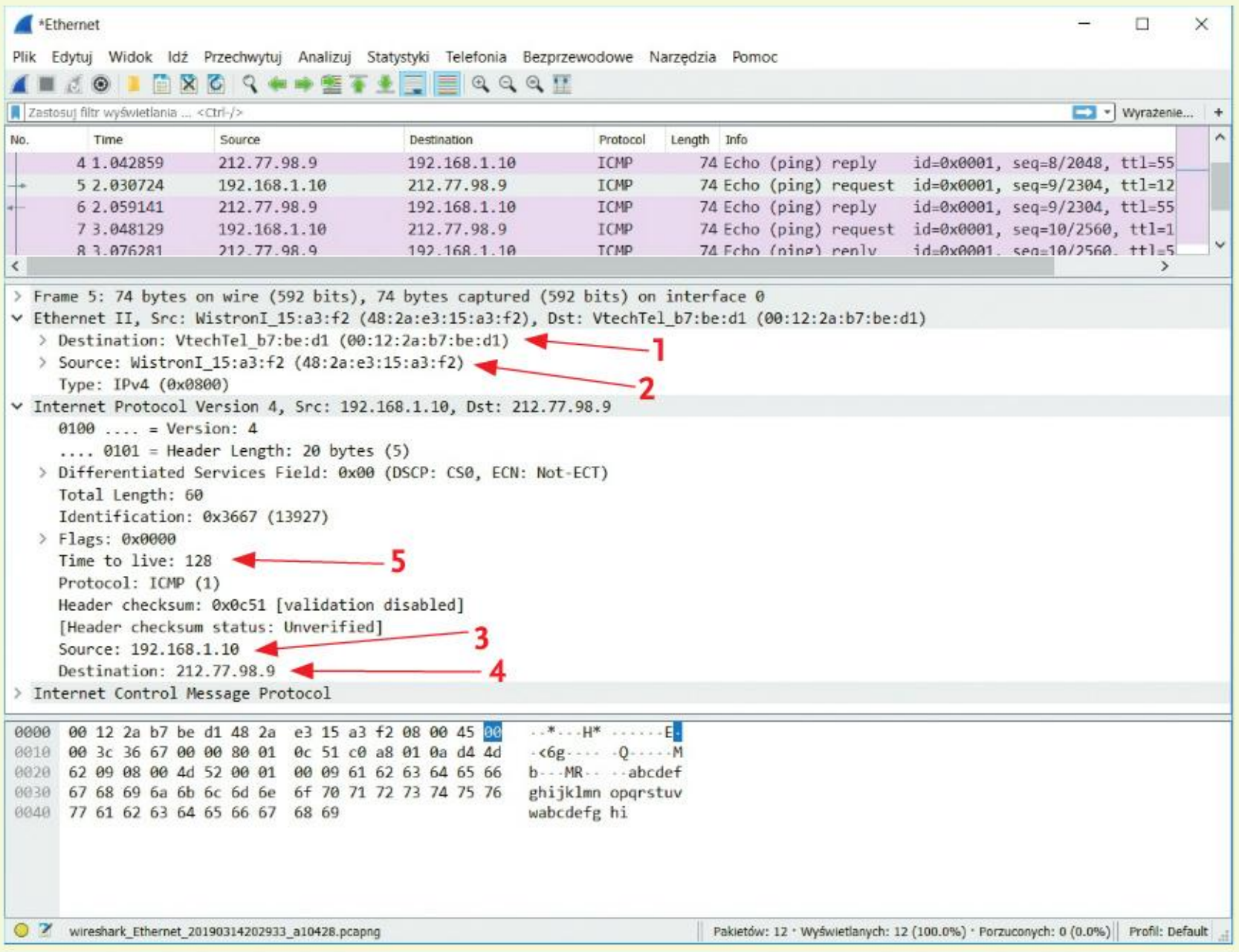


Rys. 41.1. Włączenie przechwytywania danych

Na rys. 41.2 strzałkami zaznaczono 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 pozwala na ustalenie adresów fizycznych i logicznych komputerów biorących udział w transmisji danych.



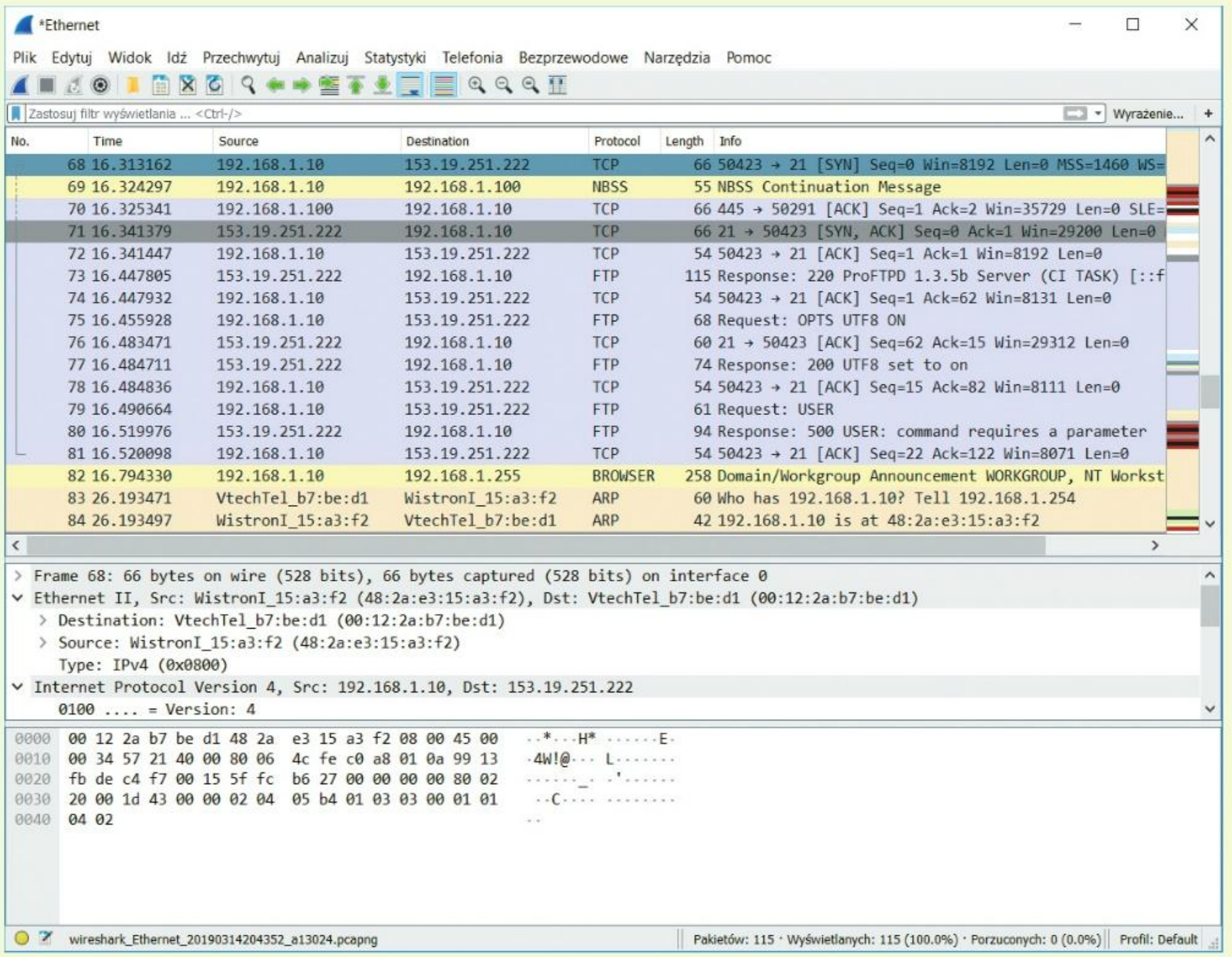
Rys. 41.2. Analiza nagłówków przechwyconych danych

PRZYKŁAD 41.2

Analiza danych przesyłanych w sieci

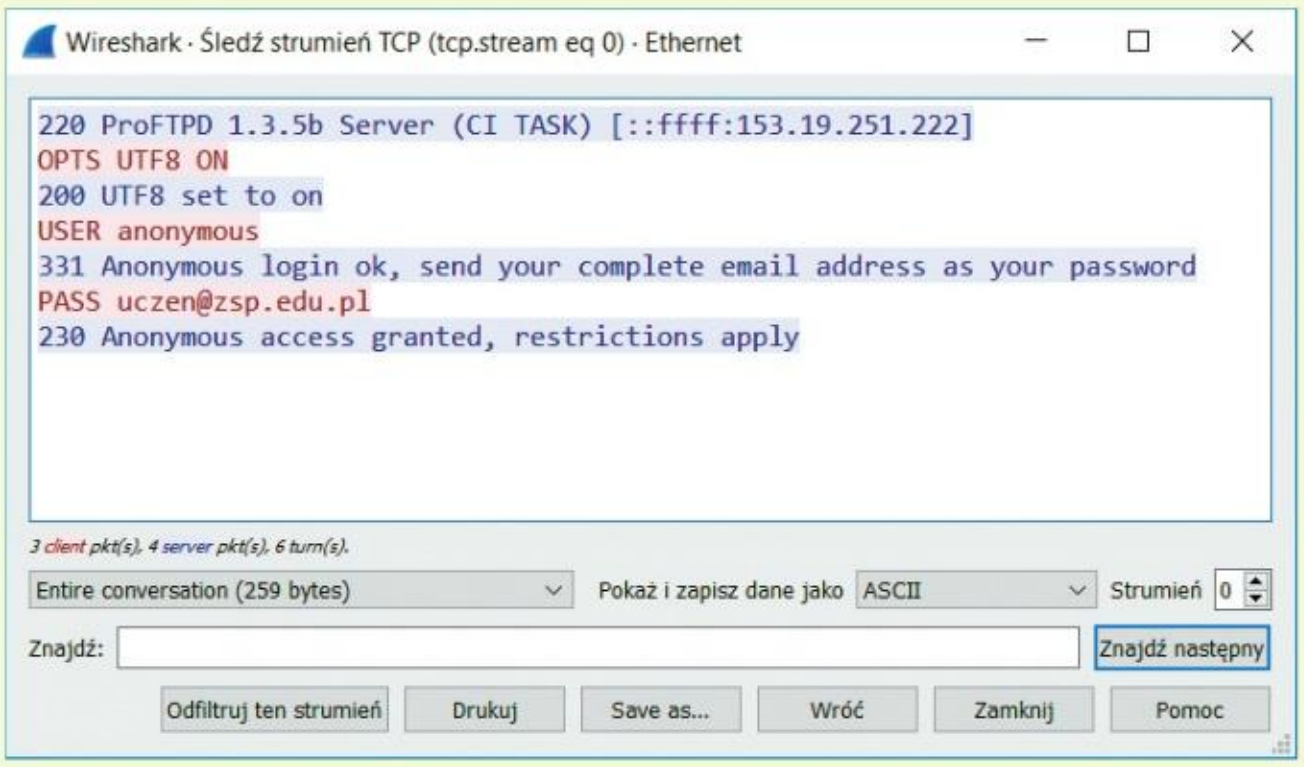
Aby przeanalizować dane przesyłane w sieci, należy wykonać następujące czynności:

1. Uruchomić program Wireshark.
2. W oknie wyboru interfejsu wskazać, który interfejs ma być ustawiony w trybie przechwytywania danych.
3. Uruchomić dowolny program generujący przepływ danych w sieci, np. program przesyłający dane w sieci za pomocą protokołu FTP. Nawiązać połączenie z serwerem FTP.
4. Obserwować w oknie głównym programu przychwytywane dane. Po zebraniu wymaganej liczby danych zatrzymać przechwytywanie poleceniem **`Przechwytuj/Stop`**.
5. Odszukać w oknie dowolny fragment transmisji związanej z nawiązywaniem połączenia FTP. Na rys. 41.3 pakiet o numerze 68 rozpoczyna proces nawiązywania sesji między klientem a serwerem FTP. W pakiecie 73 jest przesyłana odpowiedź serwera na próbę nawiązania połączenia (jest to jeden z pakietów związanych z transmisją) – można kliknąć ten pakiet lub inny należący do tej samej sesji.



Rys. 41.3. Wyszukiwanie pakietów związanych z połączeniem FTP

6. Z paska poleceń wybrać **Analizuj/Podążaj/Strumień TCP**. W nowym oknie zostaną zebrane dane z całego strumienia danych, a następnie wyświetlone w postaci tekstowej (rys. 41.4).



Rys. 41.4. **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 rys. 41.4.

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 uzyskaniem adresu i po jego otrzymaniu,
   - komunikaty: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK.

! UWAGA

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

42 Rodzaje testów i pomiarów aktywnych

ZAGADNIENIA

Przeprowadzanie pomiarów aktywnych w sieci **Mierzenie jakości usług sieciowych** **Odpowiedzialność za ustanawianie standardów dotyczących jakości usług sieciowych** **Parametry służące do oceny jakości usług sieciowych** **Wykorzystanie programów ping i traceroute do pomiarów sieci**

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

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

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

W celu zapewnienia porównywalności wyników pomiary aktywne wykonuje się 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 uznaje się za dostępne, jeśli pakiet dotrze w określonym czasie;
- **opóźnienie w jednym kierunku** (ang. *One-way Delay*, **OWD**) – czas przekazu pakietu między dwoma punktami w sieci. OWD mierzy się jako czas od momentu, w którym źródło wysłało pierwszy bit pakietu, do momentu, w którym urządzenie docelowe odebrało ostatni bit pakietu. Wielkość pakietu pomiarowego wpływa na opóźnienie i musi zostać zdefiniowana przed pomiarem. Wartość metryki podaje się w postaci parametrów statystycznych próbki:
  - **minimalne opóźnienie OWD** (ang. *One-way Delay Minimum*) – najmniejsza wartość opóźnienia w próbce;
  - **średnie opóźnienie OWD** (ang. *Average One-way Delay*) – średnia wartość opóźnienia w próbce;
  - **percentyl opóźnienia OWD** (ang. *One-way Delay Percentile*) – x-ty percentyl opóźnienia danej próbki;
  - **mediana opóźnienia OWD** (ang. *One-way Delay Median*) – wartość mediany danej próbki;

- **zmienność opóźnienia przekazu pakietów IPDV** (ang. *IP Packet Delay Variation*) – różnica między wartościami OWD dla dwóch pakietów w mierzonej próbce pakietów (zwykle przyjmuje się różnicę opóźnienia sąsiednich pakietów);
- **opóźnienie pakietów w pętli RTD** (ang. *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** (ang. *One-way Loss*) – w razie poprawnego odebrania pakietu przyjmuje wartość 0, w przeciwnym wypadku wynosi ona 1;
- **poziom strat pakietów IPLR** (ang. *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**. Pozwala on na sprawdzenie, czy istnieje połączenie między dwoma punktami w sieci. Umożliwia on zmierzenie liczby zgubionych pakietów i opóźnień w ich transmisji. Program korzysta z protokołu ICMP, wysyła pakiety ICMP Echo Request i odbiera ICMP Echo Reply. Aby wykonać test z wykorzystaniem 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 s nie nadeszła odpowiedź na polecenie ping. Informacje o dodatkowych opcjach programu można uzyskać przez 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, natomiast 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 rys. 42.1 przedstawiono wynik działania programu ping. Pierwsze polecenie testuje połączenie z bramą. Wysłano pięć pakietów testowych o standardowym rozmiarze. Wszystkie dostarczono w czasie poniżej 1 milisekundy. Drugie polecenie testuje połączenie z serwerem w sieci. Zastosowano pakiet o rozmiarze 64 bajtów. Również wszystkie pakiety dostarczono, ale czas przesyłu był dłuższy. Parametr TTL oznacza czas życia pakietu i pozwala na określenie liczby routerów na trasie.

Do badania trasy, po której przesyła się pakiety, i do mierzenia czasu między poszczególnymi routerami można wykorzystać program **traceroute** (w systemie Windows – tracert). Działanie traceroute opiera się na protokole ICMP. Wysyła się pakiety z polem **TTL** ustawionym na kolejne wartości, zaczynając od 1. Wartość 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 jest wysyłany pakiet z polem TTL ustawionym na 1, co pozwala na ustalenie adresu IP pierwszego routera na trasie. Następnie jest wysyłany 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, a przy tym wyśle komunikat do komputera źródłowego. Testowanie kończy się po osiągnięciu miejsca docelowego lub po przekroczeniu dopuszczalnej liczby routerów (standardowo 30).

Na rys. 42.2 pokazano wyniki działania programu tracert. W pierwszym poleceniu testowano trasę do bramy; trasa składała się tylko z jednego routera. Trasa do serwera w internecie była dłuższa i składała się z dziesięciu routerów (ich adresy lub nazwy znajdują się po prawej stronie rysunku). Na podstawie pomiaru administrator może określić łącza, w których występuje największe opóźnienie.

```
Wiersz polecenia
C:\Users\kp>ping -n 5 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\kp>ping -l 64 www.wp.pl

Pinging www.wp.pl [212.77.98.9] with 64 bytes of data:
Reply from 212.77.98.9: bytes=64 time=27ms TTL=55
Reply from 212.77.98.9: bytes=64 time=27ms TTL=55
Reply from 212.77.98.9: bytes=64 time=27ms TTL=55
Reply from 212.77.98.9: bytes=64 time=27ms TTL=55

Ping statistics for 212.77.98.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 27ms, Average = 27ms

C:\Users\kp>
```

Rys. 42.1. **Wynik działania programu ping**

```
Wiersz polecenia
C:\Users\kp>tracert 192.168.1.254

Tracing route to netiaspot.home [192.168.1.254]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  netiaspot.home [192.168.1.254]

Trace complete.

C:\Users\kp>tracert www.wp.pl

Tracing route to www.wp.pl [212.77.98.9]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  netiaspot.home [192.168.1.254]
  2    21 ms    18 ms    18 ms  Lodz-bras2.inetia.pl [195.114.190.184]
  3    23 ms    23 ms    22 ms  warsc001rt06.inetia.pl [83.238.250.193]
  4    28 ms    31 ms    30 ms  83.238.249.64
  5    29 ms    30 ms    31 ms  JawoH001RT05-JawoH001RT09.inetia.pl [83.238.248.129]
  6    27 ms    26 ms    26 ms  83.238.251.83
  7     *        *       27 ms  87.204.227.4
  8    27 ms    27 ms    27 ms  TczeR001-hat.dsl.star.bdi.inetia.pl [213.17.213.102]
  9    27 ms    28 ms    27 ms  rtr-int-2.rtr1.adm.wp-sa.pl [212.77.96.46]
 10    27 ms    27 ms    27 ms  www.wp.pl [212.77.98.9]

Trace complete.

C:\Users\kp>
```

Rys. 42.2. **Wynik działania programu tracert**

UWAGA

Na działanie polecenia ping może wpływać 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?

43 Cenniki materiałów do montażu okablowania

ZAGADNIENIA

Systemy okablowania strukturalnego **Elementy składające się na systemy okablowania strukturalnego** **Dobór systemu okablowania strukturalnego**

Wykonanie instalacji okablowania strukturalnego wymaga poniesienia nakładów finansowych. Ich wysokość powinna zostać oszacowana przed przystąpieniem do realizacji zadania, tak aby zamawiający miał świadomość kosztów koniecznych do poniesienia. Po zakończeniu inwestycji należy sporządzić dokładny kosztorys powykonawczy, aby rozliczyć się z zamawiającym.

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

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

Podczas obliczania kosztów materiałów należy uwzględnić koszty zarówno materiałów bezpośrednich, np. kable, złącza, jak i pośrednich, np. listwy montażowe, kołki mocujące. Wielu producentów oferuje systemy instalacji okablowania (rys. 43.1) zawierające różne elementy umożliwiające wykonanie instalacji (rys. 43.2).

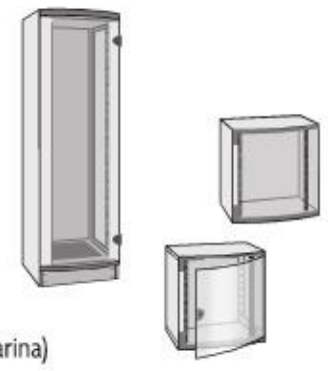
Wspomniane systemy składają się z kanałów kablowych oraz zestawu typowych gniazd i elementów łączących, np. łączników, narożników. Ceny jednostkowe tych materiałów można znaleźć na stronach internetowych producentów lub dystrybutorów – w cennikach materiałów. Fragment cennika producenta systemu okablowania przedstawiono na rys. 43.3, a fragment cennika producenta kabli – na rys. 43.4.

Podczas ustalania 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.

Składniki systemu

Produkty

- SZAFY DYSTRYBUCYJNE
- SZAFY WOLNO STOJĄCE
- Szeroki wybór głębokości (600, 800 1000 mm), szerokości (600, 800), od 24 do 47 U



- SZAFKI WISZĄCE
- Głębokości 400, 580 i 600 mm, od 6 do 21 U, stałe i odchylane
- Rama montażowa VDI do zastosowania w szafach o podwyższonym IP (Atlantic, Marina)

- PANELE KROSOWE
- Dostarczane niewyposażone lub wyposażone w gniazda (1-24)
- Dostępne opcje ze zintegrowanym panelem porządkującym



- MIEDZIANE I ŚWIATŁOWODOWE KABLE TRANSMISYJNE I KROSOWE



- STREFOWY PUNKT KONSOLIDACYJNY
- Przy pomocy od 1 do 12 gniazd RJ 45 rozprowadza sygnały niskoprądowe
- Konsoliduje połączenia, zapewniając elastyczność instalacji oraz jej łatwą rozbudowę

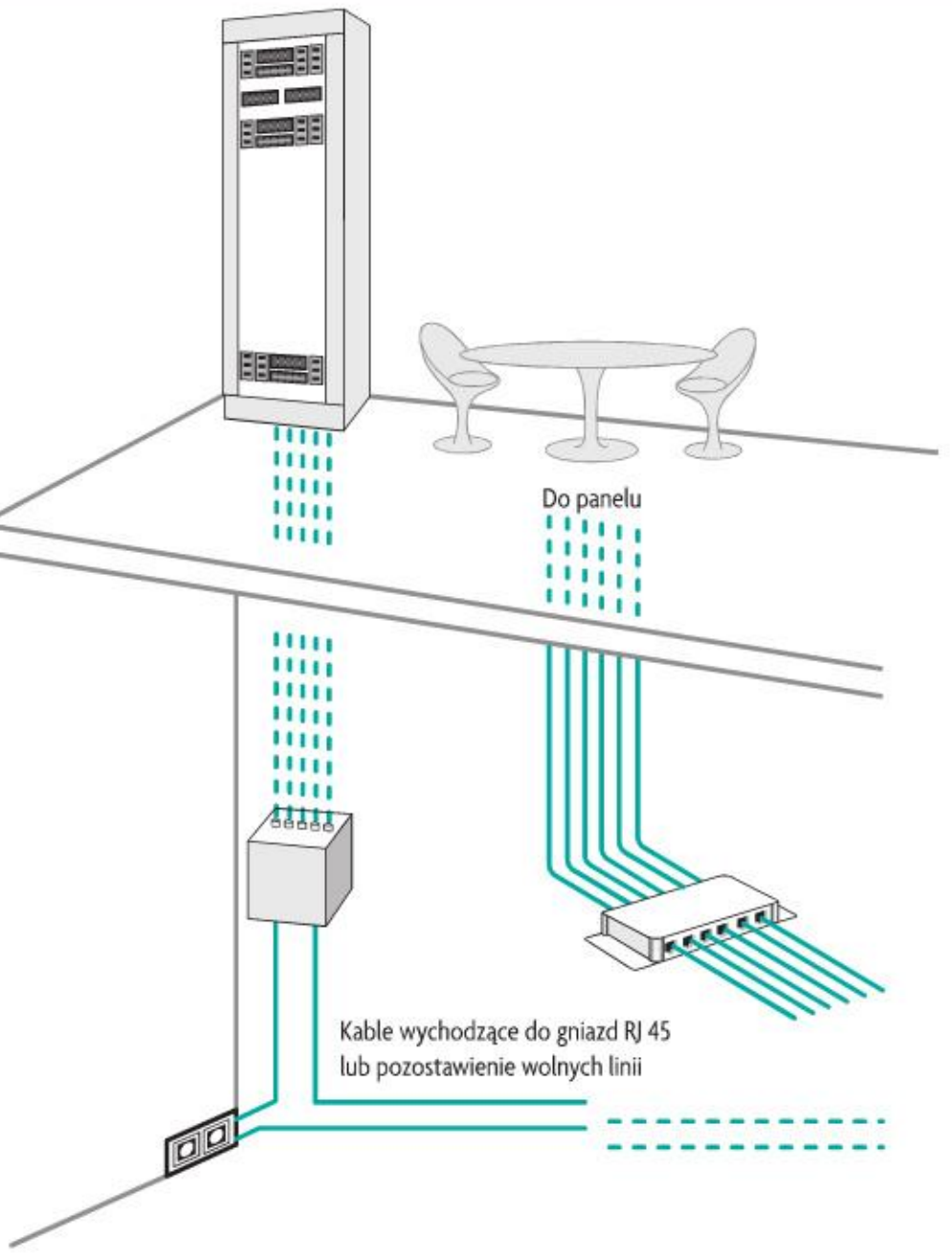


- PUNKTY DOSTĘPOWE WI-FI I GNIAZDA RJ 45
- Beznarzędziowy szybki montaż
- Wykończenie w estetyce Mosaic
- Instalacja podtynkowa lub natynkowa

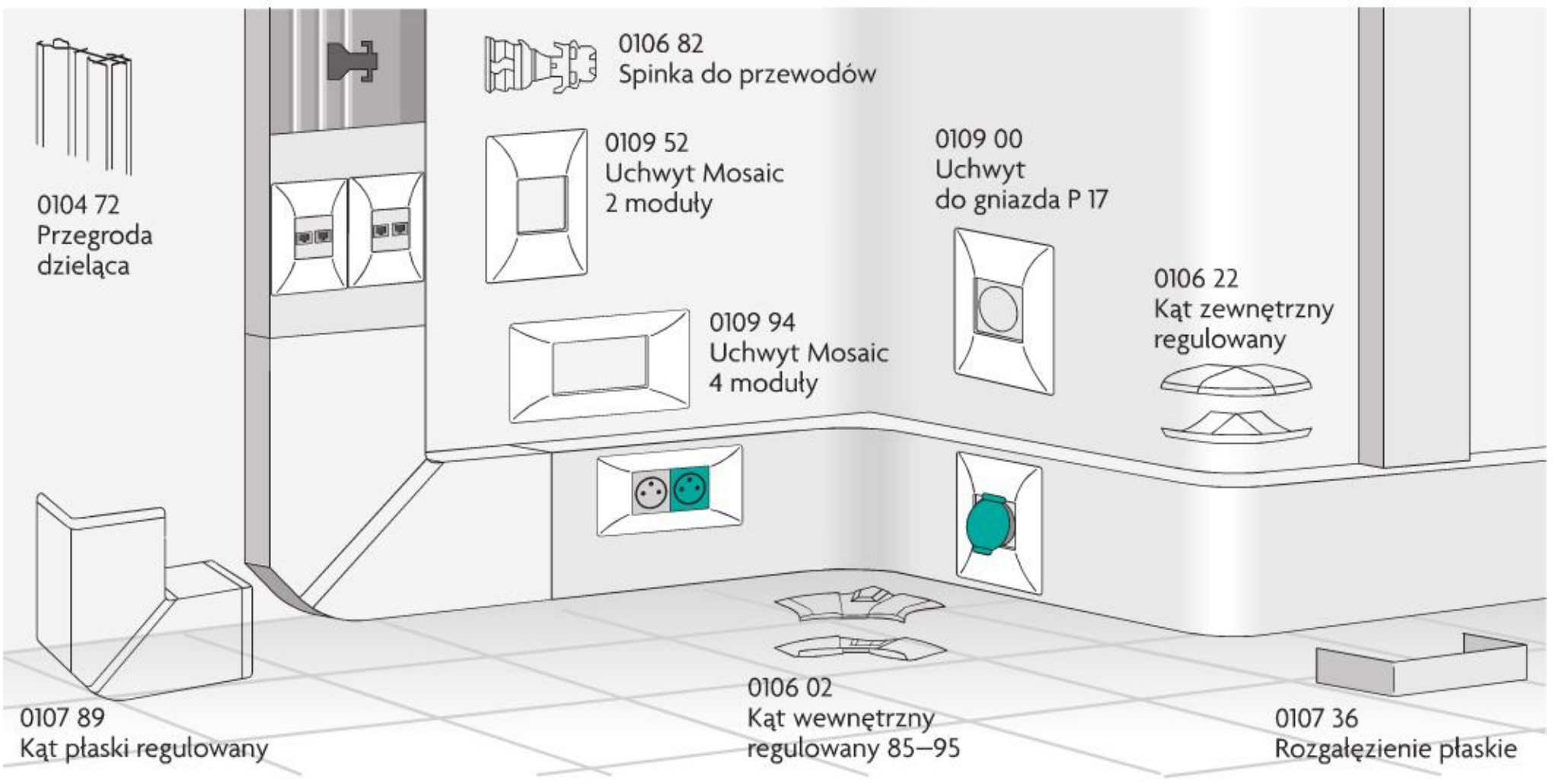


- GNIAZDA OPTYCZNE PROGRAMU MOSAIC
- 2 moduły
- Do połączenia 2 włókien
- Standarty ST/SC/LC





Rys. 43.1. Składniki systemu okablowania strukturalnego



Rys. 43.2. Elementy systemu okablowania strukturalnego



KONTAKT-SIMON 10 Zaślepka gniazda 1x RJ biała

Symbol: **74.0442**

Ocena: ★★★★★

Stan na magazynie: **48 SZT**

48h

1,55
PLN brutto



Kółka skrętne do szaf RACK 19" NEKU TS/TD komplet 4szt.

Symbol: **22.9075**

Ocena: ★★★★★

Stan na magazynie: **93 KPL**

48h

60,00
PLN brutto



Listwa zasilająca ACAR 504WF 5gn. 1,5m + filtr

Symbol: **63.0003**

Ocena: ★★★★★

Stan na magazynie: **7 SZT**

48h

86,00
PLN brutto

Rys. 43.3. **Fragment cennika producenta systemu okablowania**



Kabel FTP kat.5e F/UTP 4x2x0,5 Alantec

Symbol: **01.0003**

Ocena: ★★★★★

Stan na magazynie: **2936 MB**

48h

2,04
PLN brutto



Kabel FTP kat.5e F/UTP 4x2x0,5 Bitner

Symbol: **01.0007**

Ocena: ★★★★★

Stan na magazynie: **27539 MB**

48h

2,20
PLN brutto



Kabel FTP kat.5e F/UTP 4x2x0,48 linka szara Alantec

Symbol: **01.0024**

Ocena: ★★★★★

Stan na magazynie: **1870 MB**

48h

2,07
PLN brutto

Rys. 43.4. **Fragment cennika kabli miedzianych**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

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

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

Modernizacja i rekonfiguracja lokalnych sieci komputerowych

IV

44 Zasady modernizacji lokalnej sieci komputerowej

ZAGADNIENIA

Czynniki uwzględniane podczas planowania modernizacji sieci **Etapy modernizacji lokalnej sieci komputerowej** **Czynniki, które należy brać pod uwagę w trakcie podejmowania 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 zależnie od potrzeb użytkownika. Najtrudniejsze do modernizacji lub wymiany jest okablowanie strukturalne. Ponieważ modernizacja okablowania strukturalnego najczęściej wiąże się z remontem pomieszczeń, czas pracy okablowania planuje się na kilkanaście lat.

Modernizację lub wymianę infrastruktury sieciowej najczęściej wykonuje się, gdy:

- firma się rozwija 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.

Podczas projektowania modernizacji 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: platformę sprzętową, 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 one niższy koszt inwestycji w zakup sprzętu i instalację systemu, lecz 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 i aktualnym wyposażeniem w sprzęt i oprogramowanie. Na podstawie inwentaryzacji 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 najważniejszą decyzją związaną z modernizacją systemu informatycznego w każdej firmie. Przede wszystkim należy podjąć decyzję odnośnie do 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 wpływa na dobór sprzętu komputerowego i systemów operacyjnych serwerów i stacji roboczych. Trzeba więc wybrać tak, żeby oprogramowanie jak najlepiej odpowiadało potrzebom firmy. Oprogramowanie 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 z uwzględnieniem zasad ekonomii i zdrowego rozsądku. Nie zawsze powody modernizacji to większa moc obliczeniowa lub szybkość działania nowego sprzętu komputerowego. Czasami ważniejsze okazuje się 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 staje się wtedy prewencyjna – koszt wymiany jest niższy niż koszt usunięcia 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.

45 Zasady kosztorysowania prac modernizacyjnych

ZAGADNIENIA

- **Kosztorys modernizacji sieci**
- **Koszty prac związanych z demontażem urządzeń**
- **Koszty materiałów pomocniczych**
- **Koszty utylizacji starego sprzętu komputerowego**

Przygotowanie projektu modernizacji sieci wymaga sporządzenia kosztorysu prac. **Kosztorys modernizacji** sporządza się tak samo jak kosztorys nowej sieci, tyle że należy uwzględnić pewne dodatkowe zadania, które nie występują podczas budowy nowej sieci. Przed sporządzeniem kosztorysu konieczne jest przeprowadzenie **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 z uwzględnieniem rachunku ekonomicznego, jednak niekiedy bardzo trudno ocenić skutki ekonomiczne podejmowanych działań. Przykładowo: wdrożenie nowego systemu informatycznego wymaga czasu i wiąże się z dodatkowym nakładem pracy i kosztów pośrednich, takich jak straty spowodowane przerwą w funkcjonowaniu przedsiębiorstwa, jak również z kosztami migracji danych do nowego systemu czy jego testowania, a także ze szkoleniami pracowników w obsłudze nowego systemu. Ponadto należy liczyć się z tym, 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. Do wyceny kosztów demontażu urządzeń okablowania strukturalnego należy stosować nakłady robocizny na montaż z odpowiednich tablic katalogów KNR z następującymi współczynnikami:

- 0,6 – podczas demontażu materiałów przeznaczonych do ponownego montażu;
- 0,4 – podczas demontażu materiałów nienadających się do ponownego montażu.

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

Jednostkowe nakłady rzeczowe mogą być ustalane na podstawie **katalogów nakładów rzeczowych KNR**. W tabeli 45.1 pokazano przykładowe jednostkowe nakłady związane z montażem gniazd abonenckich. Informacje 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 podano jednostkowe nakłady związane z realizacją poszczególnych zadań, np. w kolumnie 05 są jednostkowe nakłady na montaż modułów RJ-45 w gnieździe.

Tabela 45.1. **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		Jednostki miary Oznaczenia		Gniazdo			
	Symbol eto	Rodzaje zawodów, materiałów i sprzętu	Cyfrowe	Literowe	Natynkowe	Podtynkowe	Kanałowe	Podłogowe
a	b	c	d	e	01	02	03	04
01	315	Monter-instalator – grupa V	149	rg.	0,30	0,21	0,18	0,28
		Razem	149	rg.	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		Jednostki miary Oznaczenia		Gniazdo			
	Symbol eto	Rodzaje zawodów, materiałów i sprzętu	Cyfrowe	Literowe	Montaż modułu RJ45 w gnieździe	Montaż wkładki ACO	Montaż adaptera światłowodowego SC/MT-RJ	Montaż puszki
a	b	c	d	e	05	06	07	08
01	315	Monter-instalator – grupa V	149	rg.	0,015	0,014	0,090	0,085
		Razem	149	rg.	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 podtynkowego do montażu wynosi 0,21, instalacji puszki montażowej – 0,085, montażu modułów RJ-45 w gnieździe – 0,015. Zgodnie z zasadami koszt jednostkowy demontażu takiego gniazda wyniesie 0,124, jeżeli gniazdo ma być użyte ponownie, lub 0,084, jeżeli gniazdo nie będzie ponownie używane.

Wartość kosztorysową materiałów ustala się 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. Z myślą o sprzęcie aktywnym, np. komputerów, monitorów, drukarek, 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 jest przyłączony do przełącznika.

46 Przykładowe zadania projektowe do samodzielnego wykonania

ZAGADNIENIA

Wykonanie własnego projektu sieci komputerowej **Wymagania dotyczące własnego projektu** **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 z metodami rozwiązywania tych problemów.

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

Warunki zaliczenia projektu:

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

Dokumentacja projektowa powinna składać się z następujących elementów:

1. Strony tytułowej (według 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 i 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 i uzasadnić ich wybór.
7. Proponowanej topologii sieci.
8. Prezentacji proponowanych topologii wszystkich segmentów sieci, z uwzględnieniem wymagań proponowanych technologii i wymagań projektu. Propozycje powinny dotyczyć także połączeń dla sieci WAN i 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 między nimi), rozmieszczenie punktów dystrybucyjnych i 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 i wszelkich opłat dotyczących połączeń WAN.

Kryteria oceny projektu

Na ocenę końcową składają się trzy elementy:

1. ocena zawartości, w tym:
   - zawartości merytorycznej, treści;
   - zgodności z tematem projektu;
   - oryginalności;
   - stopnia wykorzystania materiałów źródłowych;
2. wkład ucznia w realizację projektu, w tym:
   - zaangażowanie ucznia, pracowitość;
   - pomysłowość i innowacyjność;
   - umiejętność pracy w grupie;
   - stopień trudności zadań;
   - terminowość wykonania przydzielonych zadań;
   - udział w prezentacji;
3. ocena prezentacji, w tym:
   - poprawności językowej;
   - słownictwa specjalistycznego;
   - efektu artystycznego;
   - atrakcyjności;
   - estetyki;
   - techniki prezentacji;
   - stopnia zainteresowania odbiorców;
   - poprawności 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 uczeń uzyskał co najmniej 50 % punktów możliwych do zdobycia za każdy z elementów.

Tabela 46.1. 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 między pracowniami możliwa tylko za pośrednictwem routera.
2. Projekt okablowania biblioteki. W bibliotece dostęp do katalogów w formie elektronicznej (10 komputerów), w czytelni (20 komputerów) i hotspot. Dla pracowników – 10 komputerów.
3. Projekt okablowania dla firmy mieszczącej się w jednym budynku trzykondygnacyjnym. Pracownicy firmy są podzieleni na działy: administracja, księgowość, informatycy, handlowcy.
4. Projekt okablowania dla firmy mieszczącej się w dwóch budynkach oddalonych od siebie o 500 m. W dwukondygnacyjnym budynku A są zlokalizowani pracownicy działu: administracji i księgowości, w trzykondygnacyjnym budynku B – informatycy i handlowcy.
5. Projekt okablowania dla hotelu. Przewodowy dostęp do internetu w każdym pokoju. W sali konferencyjnej dostęp bezprzewodowy. Dla pracowników – 10 komputerów.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jakie są warunki zaliczenia projektu?
2. Z czego powinna składać się dokumentacja projektowa?
3. Jakie są kryteria oceny projektu sieci?

- Metody dostępu do sieci
- Uzyskiwanie dostępu do sieci internet
- Symulatory programów konfiguracyjnych urządzeń sieciowych
- Konfigurowanie urządzeń sieciowych
- Konfigurowanie urządzeń sieci bezprzewodowych
- Funkcje przełączników zarządzalnych
- Wirtualne sieci lokalne
- Zasady modernizacji sieci wirtualnych
- Korzystanie z wirtualnych sieci prywatnych
- Rodzaje i sposób obsługi urządzeń telefonii internetowej
- Programy do administracji lokalnymi sieciami komputerowymi
- Zdalne zarządzanie stacjami roboczymi
- Zasady aktualizowania oprogramowania urządzeń sieciowych
- Gwarantowanie jakości usług QoS
- Konfiguracja sprzętowej zapory sieciowej

Konfiguracja i obsługa lokalnych sieci komputerowych

V

47 Metody dostępu do sieci

ZAGADNIENIA

Pojęcie dostawcy usług internetowych **Metody dostępu do sieci internet** **Zasady wyboru metody dostępu do sieci internet**

Internet to ogólnoświatowa sieć komputerowa, logicznie połączona w jednorodną sieć adresową opartą na protokole **IP** (ang. *Internet Protocol*). Początki internetu sięgają końca lat sześćdziesiątych XX w. i wiążą się z projektem ARPANET, realizowanym na potrzeby Departamentu Obrony Stanów Zjednoczonych. Projekt miał na celu stworzenie sieci komunikacyjnej dla wojska, odpornej na zniszczenie. Z tego powodu ta sieć ma charakter zdecentralizowany.

Internet nie jest jedną siecią, lecz związkiem wielu mniejszych połączonych sieci lokalnych. Każdy komputer pracujący w dowolnej części internetu może nawiązać łączność z dowolnym innym użytkownikiem sieci. Poszczególne sieci lokalne często różnią się sposobem komunikacji, rodzajem sprzętu, ale mogą się komunikować dzięki odpowiednim protokołom i standardom. Protokoły internetowe dbają o to, aby odmienne właściwości poszczególnych podsieci były niewidoczne dla aplikacji internetowych.

Przyłączenie sieci lokalnej lub komputera użytkownika do internetu odbywa się za pośrednictwem łączy **dostawcy usług internetowych** (**ISP**). W tym celu można wykorzystywać różne technologie oparte na światłowodach, kable miedziane lub komunikację bezprzewodową.

W latach dziewięćdziesiątych XX w. dostawcy oferowali usługi dostępu do internetu dla klientów indywidualnych za pomocą **modemu telefonicznego** i połączeń wdzwanianych. Połączenie realizowano za pośrednictwem analogowej publicznej sieci telefonicznej o maksymalnej przepustowości 56 kb/s lub **sieci cyfrowej ISDN** (o przepustowości 64 kb/s dla 1 kanału lub 128 kb/s przy wykorzystaniu 2 kanałów). Połączenie następowało przez wybranie odpowiedniego numeru telefonicznego i zalogowanie się do usługi przy użyciu protokołu PPP. Koszt połączenia był zależny od czasu trwania połączenia (impuls naliczany co 3 min). Klient otrzymywał tymczasowy adres IP za pośrednictwem serwera DHCP.

Stały dostęp do internetu SDI (bez konieczności wdzwaniania do sieci) był możliwy za pomocą Home Internet Solution (HIS). Usługa oferowała maksymalną prędkość 115,2 kb/s (bez ograniczeń czasowych) oraz możliwość jednoczesnego prowadzenia rozmów głosowych i pobierania danych (podczas rozmów prędkość przesyłania danych była zmniejszana do 70 kb/s). Klient opłacał stały abonament i otrzymywał stały adres IP.

Dla użytkowników komercyjnych przewidziano dostęp za pomocą **linii dzierżawionych**. Użytkownik dzierżawił kabel łączący lokal klienta z urządzeniami dostawcy, co gwarantowało wyłączny dostęp i uzgodnioną prędkość przesyłu danych. Opłata była zależna od przepustowości łącza i długości kabla (użytkownik ponosił pełne koszty eksploatacji łącza).

Obecnie dostawcy oferują dostęp szerokopasmowy: **stacjonarny** lub **mobilny**. Dostęp stacjonarny zapewniają łącza miedziane lub światłowodowe o dużej przepustowości, bez limitu przesyłanych danych. Najczęściej stosowane technologie to:

- **DSL** (ang. *Digital Subscriber Line*) – usługa wykorzystuje istniejące okablowanie miedziane sieci telefonicznej do jednoczesnego przesyłania danych i prowadzenia rozmów telefonicznych. Istnieje wiele odmian tej technologii, zapewniającej komunikację zarówno asymetryczną, jak i symetryczną. Maksymalna prędkość przesyłania danych to 80 Mb/s. Użytkownik opłaca abonament miesięczny zależny od przepustowości łącza. Wadą technologii jest niewielki zasięg (maksymalna odległość użytkownika od centrali to kilka kilometrów);
- **DOCSIS** (ang. *Data Over Cable Service Interface Specification*) – usługa transmisji danych w istniejących hybrydowych sieciach kablowych, wykorzystywanych przez telewizję kablową. Użytkownik sieci kablowej wyposażony w modem kablowy może korzystać z wielu usług, np. telewizji, dostępu do internetu, telefonii stacjonarnej. Do połączeń wykorzystuje się kable koncentryczne lub światłowody;
- **DPL/PLC** (ang. *Digital Power Line/Power Line Communication*) – technologia wykorzystująca do transmisji danych istniejące linie energetyczne i podstacje energetyczne, w których montuje się kontrolery łączące światłowodową sieć informatyczną z siecią energetyczną niskiego napięcia. W budynku, w którym mają być odbierane przesyłane dane, montuje się kolejny kontroler, dzięki czemu sygnał pojawia się we wszystkich gniazdkach mieszkania. Taki sygnał jest doprowadzany do komputera przez specjalny modem PLC;
- **technologia światłowodowa** (ang. *Fiber Optic*) – technologia umożliwiająca wspólną realizację różnorodnych usług telekomunikacyjnych i telewizyjnych, np. szybkiego dostępu do internetu, wideo na żądanie, wideokonferencje, wideotelefon o przepustowości powyżej 2 Mb/s. Istnieje wiele odmian abonenckiej sieci światłowodowej, doprowadzających włókna optyczne o wysokiej przepustowości do abonenta. Do najczęściej używanych należą sieci doprowadzające światłowód do: bezpośredniego otoczenia domów i biur (FTTC, ang. *Fiber to the Curb*), budynków (FTTB, ang. *Fiber to the Building*), biurka (FTTD, ang. *Fiber to the Desk*), domu (FTTH, ang. *Fiber to the Home*), biura FTTO (ang. *Fiber to the Office*);
- łącze **optyczne FSO** (ang. *Free Space Optics*) – transmisja cyfrowa za pomocą światła lasera w wolnej przestrzeni. Łącze składa się z dwóch głowic nadawczo-odbiorczych, umieszczonych w linii prostej (niezbędna jest wzajemna widoczność). Osiąga się zasięgi transmisji rzędu 1,5 km o prędkości transmisji do 2,5 Gb/s. Wadą jest zależność od warunków atmosferycznych, np. mgła, opady mogą utrudnić komunikację;
- łącza **satelitarne** – wyróżnia się łącza jednokierunkowe i dwukierunkowe. Łącze jednokierunkowe zapewnia tylko odbiór sygnałów z satelity. Transmisja od użytkownika musi się odbywać z wykorzystaniem drugiego łącza, np. modemowego, które pozwala na wysyłanie informacji.

Technologie dostępu mobilnego:

- **WLAN** – bezprzewodowe sieci LAN (ang. *Wireless Local Area Network*) jako medium transmisyjnego używają fal radiowych. IEEE zdefiniowało standardy dla sieci bezprzewodowych, m.in.:
  - 802.11a (Wi-Fi 2): pasmo 5 GHz, szybkość transmisji do 54 Mb/s;
  - 802.11b (Wi-Fi 1): pasmo 2,4 GHz, szybkość transmisji do 11 Mb/s;
  - 802.11g (Wi-Fi 3): pasmo 2,4 GHz, szybkość transmisji do 54 Mb/s;
  - 802.11n (Wi-Fi 4): pasmo 2,4 lub 5 GHz, szybkość transmisji do 600 Mb/s;
  - 802.11ac (Wi-Fi 5): pasmo 5 GHz, szybkość transmisji do 1300 Mb/s;
  - 802.11ax (Wi-Fi 6): pasmo 2,4 lub 5 GHz, oraz 6 GHz, szybkość transmisji do 9,6 Gb/s.

  W warunkach europejskich moc nadajników nie może przekraczać 100 mW, co gwarantuje działanie systemu w zasięgu 20–50 m w pomieszczeniach zamkniętych i kilkuset metrów na zewnątrz budynków;

- **WiMAX** (ang. *Worldwide Interoperability for Microwave Access*) – technika bezprzewodowej, radiowej transmisji danych, stworzona dla szerokopasmowego radiowego dostępu na dużych obszarach;
- **rozwiązania transmisji danych w sieciach GSM** – możliwość korzystania z internetu w każdym miejscu, które jest w zasięgu działania sieci operatora. Prędkości dorównują tym spotykanym przy dostępie stacjonarnym, ale istnieje ograniczanie ilości odbieranych i wysyłanych danych. Limity transferowe zależą od operatora i od wykupionego abonamentu. Do grupy rozwiązań mobilnych należą techniki GPRS, EDGE, WCDMA, HSPA, 4G LTE, 5G – udostępniane w sieciach komórkowych różnych generacji.

Podczas wyboru metody dostępu do sieci należy uwzględnić następujące czynniki:

- dostępność operatorów: w dużych miastach dostępność usług oferowanych przez dostawców jest pełna (ADSL, internet mobilny, telewizja kablowa, światłowód); w mniejszych miastach lub na wsi dostępność usług może być ograniczona do 1–2 operatorów;
- dodatkowe usługi, np. telefon (oferta ADSL) lub pakiet telewizji kablowej;
- mobilność;
- przepustowość połączenia z internetem – jeśli internet wykorzystuje się tylko do przeglądania stron internetowych, odbierania poczty i pobierania niewielkich plików, to przepustowość może być niewielka, rzędu kliku Mb/s; jeżeli pobiera się duże pliki lub intensywnie wykorzystuje usługi multimedialne w jakości HD, to należy wybrać szybsze łącze, o przepustowości kilkudziesięciu bądź kilkuset Mb/s;
- symetryczne czy asymetryczne – większość operatorów proponuje łącza asymetryczne (większa prędkość pobierania, mniejsza wysyłania); jeżeli planuje się uruchomienie serwera i wysyłanie dużej ilości plików, warto wybrać łącze symetryczne (takie same prędkości pobierania i wysłania);
- cena.

Po przeprowadzeniu analizy powyższych czynników można wybrać propozycję, która w najwyższym stopniu spełnia oczekiwania klienta.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyszukaj w internecie ofertę usług dostępu do internetu w twojej miejscowości. Wybierz ofertę optymalną dla użytkownika domowego i dla firmy udostępniającej serwer WWW.

48 Uzyskiwanie dostępu do sieci internet

ZAGADNIENIA

Podłączenie sieci lokalnej do internetu **Działanie usługi NAT** **Działanie translacji adresów źródłowych i docelowych** **Działanie serwera proxy** **Skonfigurowanie przeglądarki internetowej do współpracy z serwerem proxy**

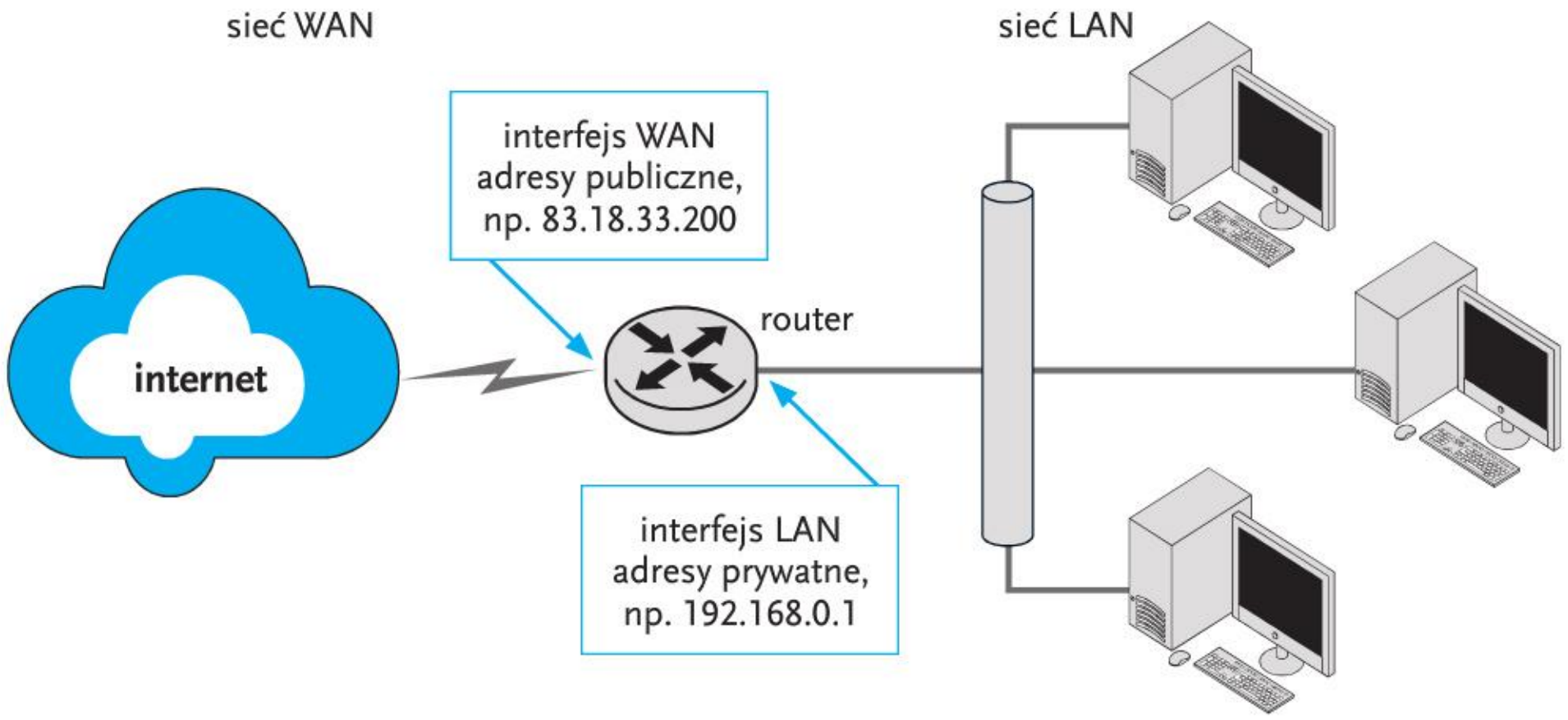
Komputer może być przyłączony do internetu bezpośrednio za pomocą modemu (DSL, telefonicznego, telewizji kablowej, 4G) lub przez lokalną sieć komputerową. Gdy buduje się sieć lokalną, np. w szkole, można komputerom przypisać adresy prywatne (nie trzeba uzyskiwać zgody na ich wykorzystanie). Te same adresy prywatne mogą być wykorzystywane wielokrotnie, np. w sąsiedniej szkole, bez niebezpieczeństwa wystąpienia konfliktu adresów. Każda z sieci lokalnych jest przyłączona do internetu za pośrednictwem urządzenia nazywanego routerem.

Router (ang. *router*) jest urządzeniem służącym do łączenia różnych sieci komputerowych. Mogą to być np. dwie sieci lokalne lub sieć lokalna i internet. Router jest wyposażony 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). Rolę routera może odgrywać komputer wyposażony np. w dwie karty sieciowe i odpowiednie oprogramowanie (router programowy) albo specjalnie do tego celu zaprojektowane urządzenie sieciowe (router sprzętowy).

W sieci lokalnej można używać **adresów prywatnych**. Przyłączenie sieci do internetu wymaga co najmniej jednego adresu **publicznego**, który będzie przypisany do interfejsu zewnętrznego routera. Od strony internetu cała sieć lokalna będzie widziana pod tym adresem. Router będzie pełnił funkcję bramy, przez którą pakiety danych są wysyłane z komputera w sieci lokalnej do internetu. Komputer zlokalizowany w sieci LAN, który wysyła dane do serwera w internecie, kieruje je do interfejsu LAN routera.

W routerze jest uruchomiona **usługa translacji adresów NAT**. Jest ona odpowiedzialna za tłumaczenie adresów używanych w sieci lokalnej na jeden lub kilka adresów publicznych (uzyskanych od dostawcy usług internetowych). Router zapisuje na specjalnej tablicy translacji informacje o sesji nawiązanej między komputerem z sieci lokalnej a serwerem w internecie. Następnie zamienia prywatny adres IP (używany w sieci LAN) na adres publiczny (używany w sieci WAN) i wysyła pakiety do kolejnego routera. Wybór kolejnego routera na trasie odbywa się na podstawie adresu IP miejsca docelowego i informacji zgromadzonych na tablicy routingu każdego kolejnego routera na trasie. Ostatni router na trasie przesyła dane do serwera. Dane przeznaczone dla komputera w sieci lokalnej trafiają najpierw do interfejsu sieci WAN w routerze. Router porównuje adresy z nagłówka pakietu z informacjami z tablicy translacji na temat nawiązanych sesji i na tej podstawie zamienia docelowy publiczny adres IP na adres prywatny komputera, do którego kieruje dane. Ta metoda ma dodatkową zaletę, polegającą na tym, że z komputerami w sieci lokalnej nie można nawiązać bezpośredniego połączenia

z internetu. Połączenie z komputerem w sieci lokalnej może udostępnić administrator routera – dzięki jego odpowiedniemu skonfigurowaniu. Schemat sieci lokalnej przyłączonej do internetu za pomocą routera przedstawiono na rys. 48.1.



Rys. 48.1. **Schemat sieci lokalnej przyłączonej do internetu**

Istnieją dwie odmiany translacji adresów:

- **translacja adresów źródłowych SNAT** (ang. *Source NAT*) – umożliwia komputerom w sieci prywatnej dostęp do internetu. W pakietach, których źródłem są komputery w sieci lokalnej, opuszczających sieć źródłową, router zamienia prywatny adres IP źródła na adres publiczny swojego interfejsu, a numer portu źródłowego – na inny, wolny numer portu. Router zapamiętuje tę zamianę na tablicy translacji w postaci odwzorowania:

  lokalny adres IP: lokalny port → publiczny adres IP: publiczny port

  Pakiet z odpowiedzią jest kierowany na adres interfejsu zewnętrznego routera. Na podstawie tablicy translacji router będzie mógł przetłumaczyć adres i numer portu zgodnie z zapamiętanym odwzorowaniem i skierować pakiet do odpowiedniego komputera w sieci lokalnej. Numer portu pozwala na jednoczesne korzystanie z jednego adresu IP przez wiele komputerów w sieci lokalnej;
- **translacja adresów docelowych DNAT** (ang. *Destination NAT*) – umożliwia komputerom z sieci publicznej, np. z internetu, dostęp do usług oferowanych przez serwery znajdujące się w sieci lokalnej. W pakietach, których źródłem są komputery w internecie, docelowy adres IP jest ustawiony na publiczny adres zewnętrznego interfejsu routera. Router zamienia ten adres na adres serwera zgodnie z odwzorowaniem zapisanym w konfiguracji. Numer portu docelowego na ogół się nie zmienia. Gdy router otrzymuje odpowiedź od serwera w sieci lokalnej, przeprowadza translację prywatnego adresu źródłowego na adres publiczny swojego zewnętrznego interfejsu i przesyła pakiet do komputera w internecie. Przykład konfiguracji interfejsów routera sprzętowego przedstawiono na rys. 48.2.

Prędkość transmisji danych w sieci lokalnej jest zazwyczaj większa od prędkości łącza, za pomocą którego sieć lokalna uzyskuje dostęp do internetu. Ponadto z przepustowości tego łącza korzystają wszystkie komputery i urządzenia w sieci lokalnej. Aby zmniejszyć obciążenie i przyśpieszyć pobieranie danych z internetu, można zastosować **serwer pośredniczący** (ang. *proxy server*).



Rys. 48.2. **Konfiguracja interfejsów routera sprzętowego**

Serwer pośredniczący to specjalny serwer, którego zadaniem jest buforowanie na dysku lokalnym stron WWW odwiedzonych wcześniej. Serwer proxy może być skonfigurowany na komputerze w sieci lokalnej. Przeglądarka WWW najpierw sprawdza, czy żądanych stron nie ma na serwerze proxy. Jeśli są, to pobiera je z serwera, z wykorzystaniem sieci lokalnej. Wtedy pobieranie stron wcześniej przeglądanych, np. przez innego użytkownika sieci, nie wymaga pobrania

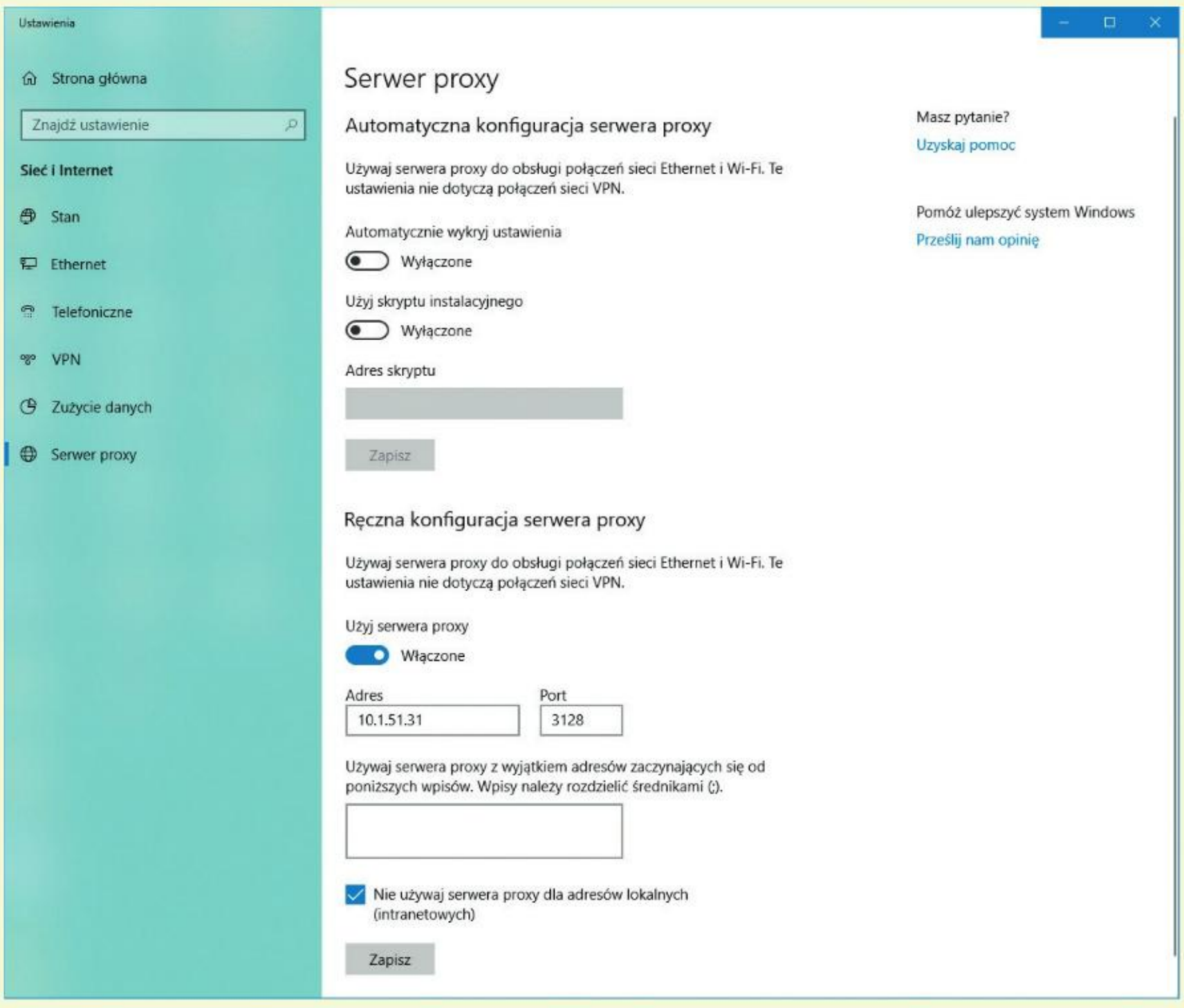
danych z internetu. Jeśli strony nie ma w buforze, to serwer proxy pobiera ją z internetu, zapisuje w buforze i udostępnia klientom w sieci. Korzystanie z proxy zmniejsza obciążenie połączenia z internetem i skraca jednocześnie czas oczekiwania na dane (ale dotyczy to tylko stron wcześniej odwiedzonych). Korzystanie z serwera proxy pozwala ponadto na ukrycie przed serwerem np. stron internetowych, adresu IP klienta. Serwer WWW może uzyskać informacje o adresie IP urządzenia pobierającego dane w sposób bezpośredni. Ponieważ dane pobiera serwer proxy, a dopiero później przekazuje je klientowi, serwer WWW nie może poznać adresu klienta, który z tych danych korzysta.

PRZYKŁAD 48.1

Konfiguracja przeglądarki do współpracy z serwerem proxy

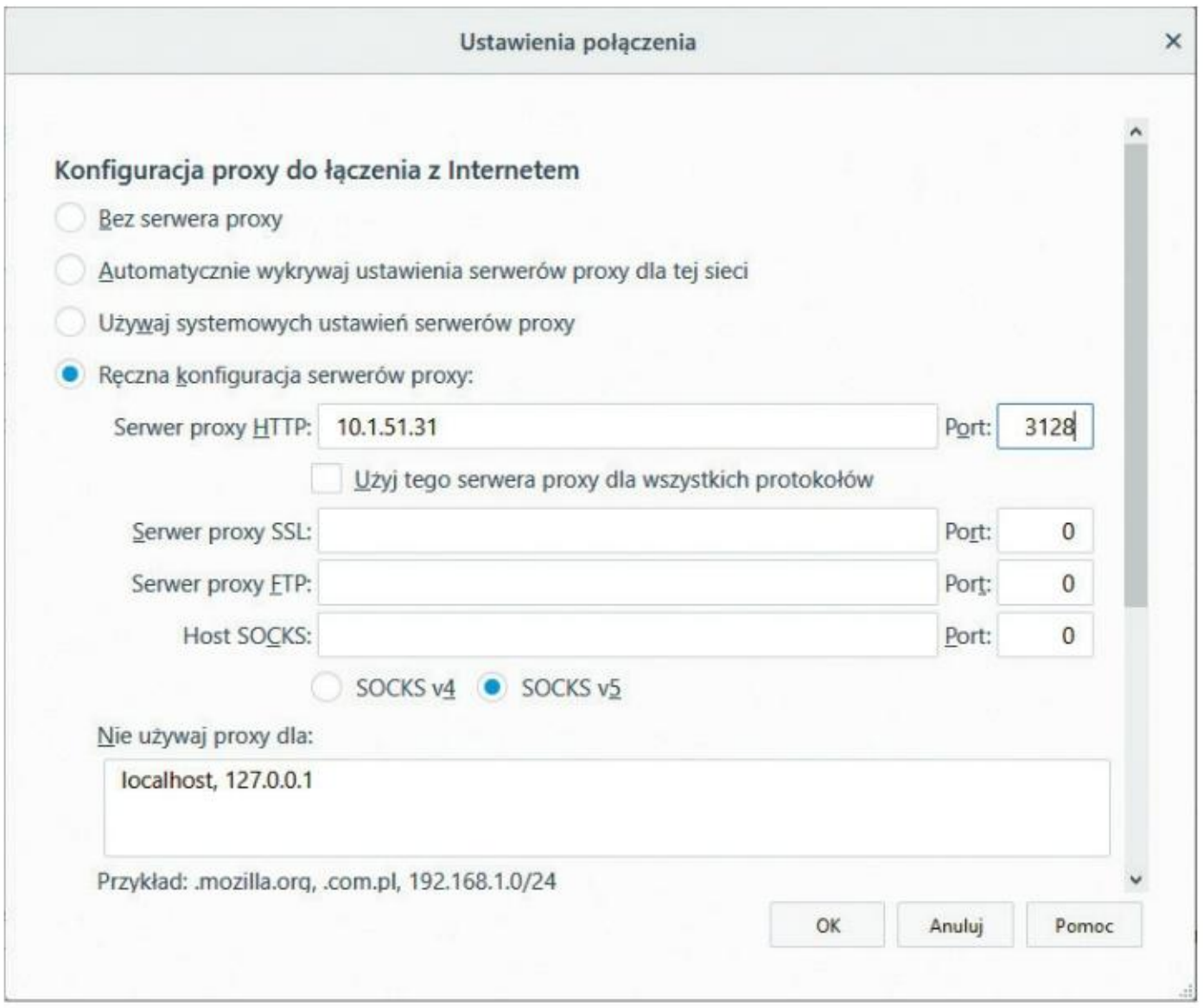
Aby skonfigurować przeglądarkę Microsoft Edge do współpracy z serwerem proxy, należy:

1. Uruchomić przeglądarkę.
2. Wybrać z menu polecenie …**/Ustawienia/System**.
3. Kliknąć odnośnik **Otwórz ustawienia serwera proxy komputera**.
4. Włączyć opcję **Użyj serwera proxy**, a następnie wprowadzić adres i numer portu, na którym nasłuchuje serwer proxy.
5. Zaznaczyć opcję **Nie używaj serwera proxy dla adresów lokalnych**.
6. Kliknąć przycisk **Zapisz**.



Rys. 48.3. Konfiguracja serwera proxy w przeglądarce Microsoft Edge

Inne przeglądarki internetowe, np. **Firefox**, **Chrome** lub **Opera**, oferują podobne funkcje, a ich konfiguracja przebiega w sposób zbliżony do procedury opisanej w przykładzie 48.1. Na rys 48.4 przedstawiono okno konfiguracji serwerów proxy w przeglądarce **Firefox**.



Rys. 48.4. Konfiguracja serwera proxy w przeglądarce Firefox

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

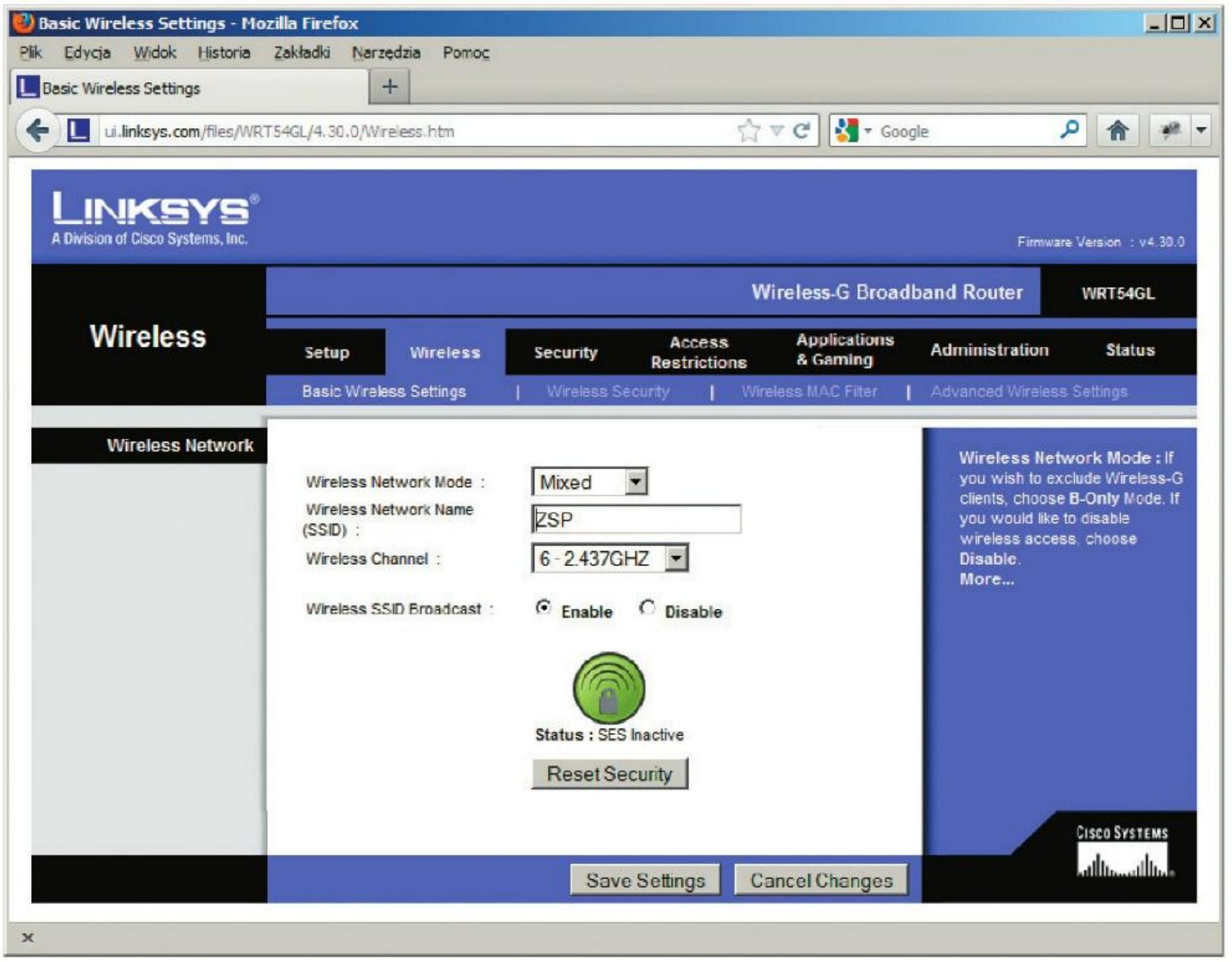
1. Narysuj schemat podłączenia do internetu sieci lokalnej w twojej szkole. Zaznacz używane adresy w sieci LAN i WAN.
2. Skonfiguruj przeglądarkę do współpracy z serwerem proxy w twojej szkole. Jeżeli w twojej szkole nie jest używany serwer proxy, to odszukaj w internecie adres dowolnego ogólnodostępnego serwera proxy lub poproś nauczyciela o skonfigurowanie serwera w szkole na czas testu.

49 Symulatory programów konfiguracyjnych urządzeń sieciowych

ZAGADNIENIA

- **Metody konfigurowania urządzeń sieciowych**
- **Przetestowanie możliwości konfiguracyjnych urządzeń przed zakupem**

Urządzenia sieciowe, takie jak przełączniki, routery i inne, umożliwiają konfigurowanie za pomocą różnych narzędzi np. wiersza poleceń czy przeglądarki internetowej. Konfigurowanie profesjonalnego sprzętu najczęściej wykonuje się za pomocą poleceń wydawanych w interfejsie tekstowym. Producenci dostarczają również specjalne programy narzędziowe ułatwiające konfigurowanie urządzeń, np. **Cisco Security Device Manager** (**SDM**). Jest to program, który ułatwia konfigurowanie urządzeń wyprodukowanych przez Cisco. Niestety, programy tego typu nie zawsze są udostępniane w wersji nieodpłatnej. Przykładem darmowego programu może być **Winbox** do konfigurowania urządzeń sieciowych Mikrotik.



Rys. 49.1. Okno konfiguracji sieci bezprzewodowej routera WRT54GL

Sprzęt używany w domu lub małej sieci jest zazwyczaj konfigurowany za pomocą interfejsu opartego na przeglądarce internetowej. Producenci sprzętu sieciowego oferują usługę pozwalającą na interaktywne przetestowanie interfejsu administratora urządzenia. Użytkownik może przed zakupem sprawdzić, jakie są możliwości konfiguracji, jak wygląda interfejs administratora, a także porównać poziom trudności konfiguracji z innymi urządzeniami. Przykładowo: firma Linksys udostępnia na stronie http://ui.linksys.com/ wykaz urządzeń, które można dowolnie testować. Przykład konfiguracji sieci bezprzewodowej routera WRT54GL przedstawiono na rys. 49.1.

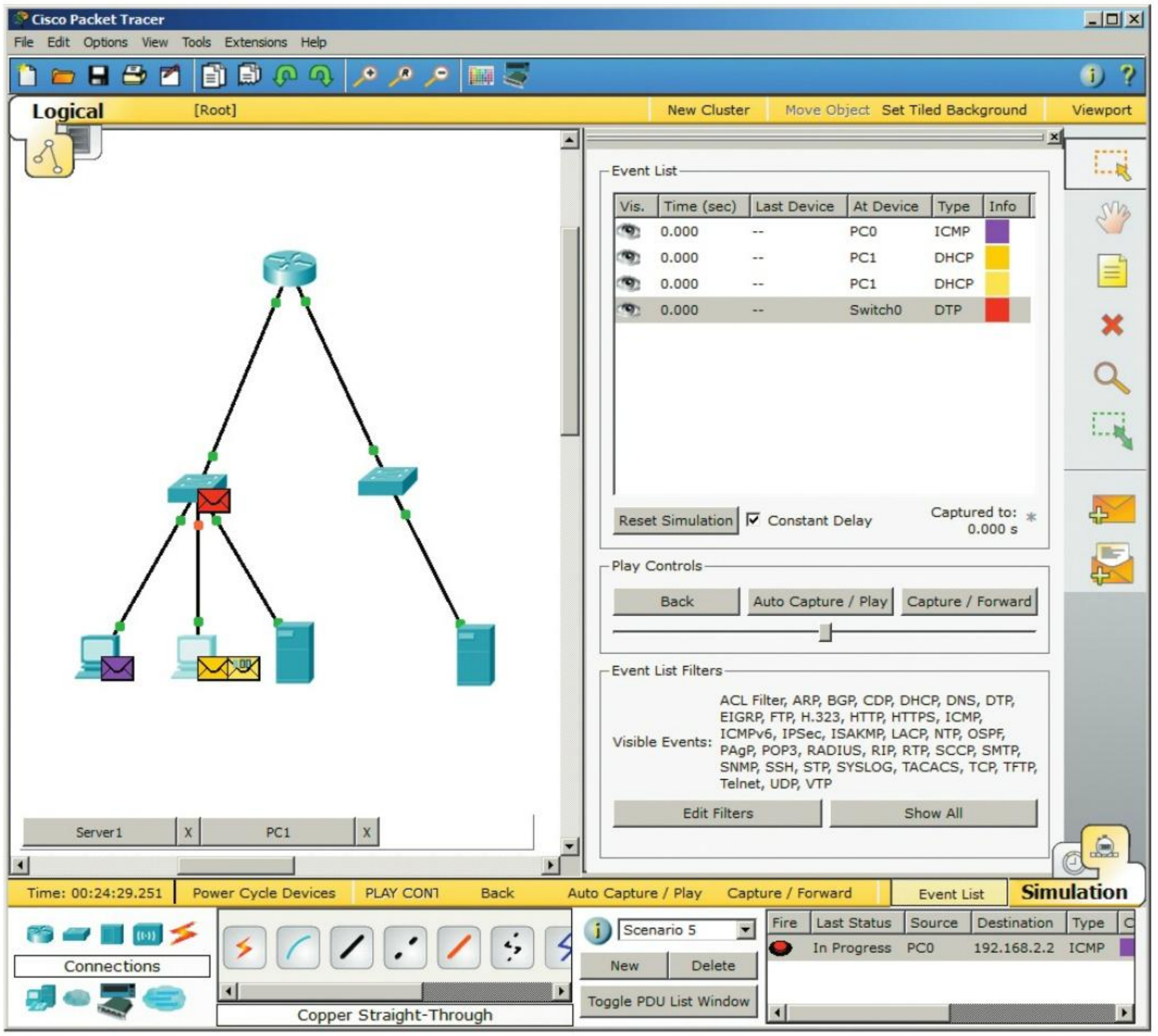
Na rys. 49.2 przedstawiono okno konfiguracji sieci WAN w routerze TP-Link TL-WDR3600. Aby uzyskać możliwość testowania tego routera, należy połączyć się z pomocą techniczną dostępną pod adresem https://www.tp-link.com/pl/emulators.html, a następnie wskazać wybrany model urządzenia.



Rys. 49.2. Okno konfiguracji sieci WAN w routerze TL-WDR3600

Firma CISCO opracowała i udostępnia słuchaczom szkoleń realizowanych w ramach Akademii Sieci CISCO symulator umożliwiający wykonanie konfiguracji sieci i urządzeń sieciowych o nazwie **Packet Tracer**. Przykład konfiguracji prostej sieci wykonany za pomocą tego narzędzia przedstawiono na rys. 49.3.

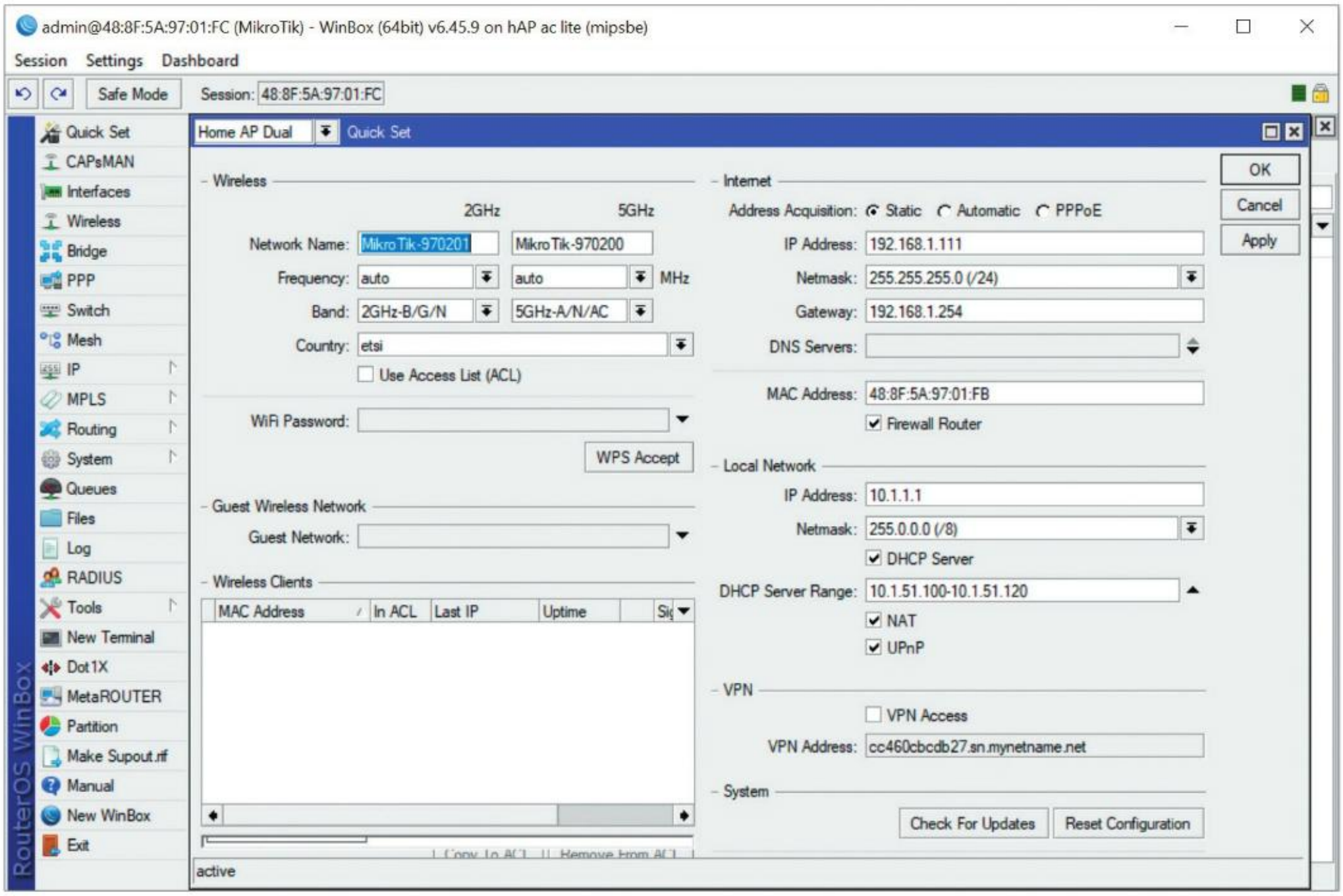
Symulatory urządzeń sieciowych są bardzo przydatne w czasie nauki i umożliwiają zapoznanie się z podstawowymi zasadami konfiguracji, jednak należy pamiętać, że nie są one wyposażone we wszystkie funkcje oferowane przez rzeczywiste urządzenia.



Rys. 49.3. **Okno symulacji działania sieci w programie Packet Tracer**

> **! UWAGA**
>
> Większość ćwiczeń opisywanych w podręczniku, a dotyczących konfiguracji sieci komputerowych można wykonać z wykorzystaniem symulatora **Cisco Packet Tracer**. Jednak symulator nie oddaje wiernie wszystkich cech i funkcji rzeczywistych urządzeń. Jeżeli szkoła dysponuje odpowiednimi urządzeniami, to zaleca się wykonanie ćwiczeń z wykorzystaniem tych urządzeń.

Program **Winbox** umożliwia nawiązanie połączenia i konfigurowanie urządzeń sieciowych firmy Mikrotik. Przykładowe okno szybkiej konfiguracji routera przedstawiono na rys. 49.4.



Rys. 49.4. **Okno szybkiej konfiguracji routera w programie Winbox**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sprawdź w internecie, czy producent routera używanego w twojej szkole udostępnia interfejs do jego testowania. Nawiąż połączenie z panelem administracyjnym i przetestuj możliwości konfiguracji. Jeżeli dla routera używanego w twojej szkole interfejs testowy jest niedostępny, to skorzystaj z adresów urządzeń podanych wyżej.

50 Konfigurowanie urządzeń sieciowych

ZAGADNIENIA

Połączenie komputera z routerem i nawiązanie sesji **Połączenie za pomocą dwóch routerów dwóch odległych sieci lokalnych** **Procedura konfiguracji routera** **Skonfigurowanie interfejsu routera** **Skonfigurowanie protokołu routingu na routerze**

Skonfigurowanie routera z wykorzystaniem interfejsu przeglądarki internetowej

Router sprzętowy jest urządzeniem służącym do łączenia sieci, np. dwóch sieci lokalnych. Można go wykorzystać do przyłączenia sieci lokalnej do internetu. Może on być traktowany jako wyspecjalizowany komputer, wyposażony w swój procesor, pamięć, system operacyjny i inne podzespoły. Router musi ponadto mieć co najmniej dwa interfejsy – po jednym dla każdej z sieci.

Dzięki systemowi operacyjnemu routera możliwe staje się uruchomienie protokołu routingu. Bardziej zaawansowane routery pozwalają na uruchomienie wielu różnych protokołów routingu (zwykle administrator routera wybiera jeden spośród dostępnych protokołów) i dodatkowych usług, takich jak usługa translacji adresów NAT, filtrowanie pakietów za pomocą list kontroli dostępu, serwer DHCP i wiele innych. Parametrów konfiguracyjnych routera jest bardzo dużo, ale żeby zapewnić jego funkcjonowanie przy minimalnym nakładzie pracy, wystarczy skonfigurować interfejsy i protokół routingu.

Na rys. 50.1 przedstawiono prostą sieć złożoną z dwóch sieci lokalnych połączonych za pomocą dwóch routerów i łącza szeregowego. Minimalny zestaw poleceń niezbędnych do konfiguracji routera obejmuje:

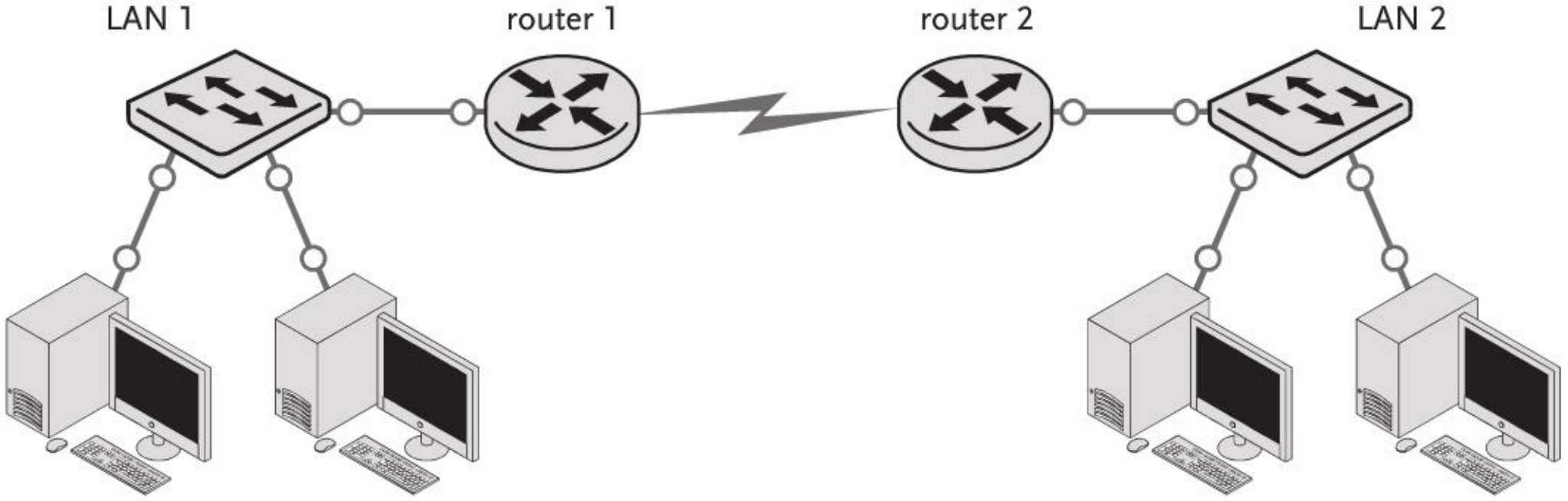
- konfigurację interfejsu LAN routera;
- konfigurację interfejsu szeregowego routera;
- konfigurację protokołu routingu.

Konfigurowanie urządzeń sieciowych w tym rozdziale pokazano na przykładzie urządzeń firmy CISCO. Sprzęt innych producentów może się różnić, jeśli chodzi o szczegóły konfiguracji, ale same zasady konfiguracji pozostają takie same. Jeżeli w twojej szkole jest wykorzystywany inny typ sprzętu, różniący się sposobem konfiguracji, to zapytaj nauczyciela, jak należy ten sprzęt konfigurować. W tym podręczniku korzystamy z routerów serii ISR4321 i z przełączników serii C2960. Jeżeli w twojej szkole są routery z innej wersji, np. starszej – C1841, to większość poleceń będzie działała tak samo, ale oznaczenia interfejsów mogą być inne. Sprawdź w instrukcji lub zapytaj nauczyciela o oznaczenia interfejsów.

Konfigurowanie profesjonalnych routerów, np. CISCO, i zarządzanie nimi może się odbywać z wykorzystaniem **interfejsu wiersza poleceń CLI** (ang. *Command-Line Interface*). Router jest wyposażony w przynajmniej dwa porty umożliwiające podłączenie sieci LAN/WAN, a także

w specjalne porty umożliwiające zarządzanie, np. w port konsoli. Router od chwili włączenia wykonuje sekwencję poleceń mającą na celu przygotowanie go do pracy. Najpierw ładuje **program rozruchowy** (ang. *boot loader*) – niewielki program przechowywany w **nieulotnej pamięci RAM** (NVRAM). Program rozruchowy wykonuje następujące operacje:

- Przeprowadza niskopoziomową inicjację procesora (inicjuje rejestry procesora kontrolujące miejsce odwzorowania pamięci fizycznej, pojemność pamięci i jej szybkość).
- Przeprowadza test wewnętrzny (POST) podsystemu procesora – testuje pamięć procesora i część pamięci flash tworzącej system plików flash.
- Inicjuje oparty na pamięci flash system plików na płycie systemowej.
- Ładuje do pamięci domyślny obraz systemu operacyjnego i przeprowadza rozruch routera.
- System operacyjny inicjuje interfejsy i wprowadza inne opcje konfiguracji – posługuje się poleceniami zawartymi w pliku konfiguracyjnym systemu operacyjnego (dla routerów CISCO jest to plik **`startup-config`**).



Rys. 50.1. Połączenie dwóch sieci lokalnych

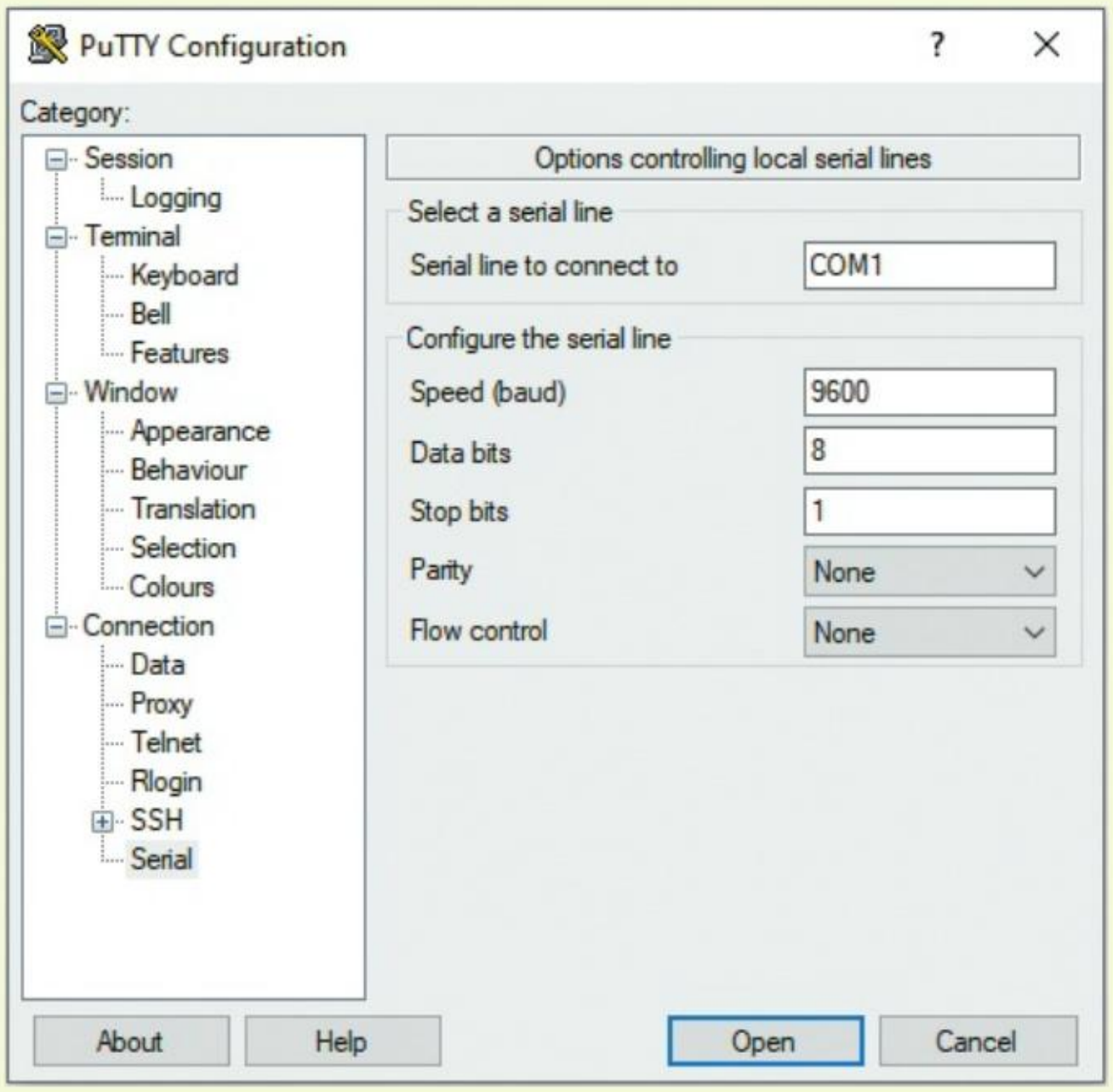
Aby skonfigurować router CISCO, należy połączyć port szeregowy komputera (COM) z portem konsoli i ustanowić sesję komunikacyjną. Jeśli korzystasz z innego typu routera, zapytaj nauczyciela, jak wykonać to zadanie z wykorzystaniem sprzętu dostępnego w twojej szkole.

PRZYKŁAD 50.1

Połączenie portu COM komputera z portem konsoli w routerze

Aby nawiązać połączenie między komputerem a routerem CISCO za pomocą portu konsoli, należy:

1. Za pomocą **kabla konsolowego** (ang. *rollover*) połączyć port konsoli routera z portem COM komputera.
2. Uruchomić na komputerze program **Putty**. W wyświetlonym oknie dialogowym (rys. 50.2) za pomocą przycisku radiowego należy wybrać typ połączenia **`Serial`** i nazwę portu szeregowego komputera (np. **`COM1`**). Wybrać w sekcji **`Category`** opcję **`Serial`** i ustawić prędkość połączenia (**`Speed: 9600`**) oraz sterowanie przepływem (**`Flow Control: None`**). Pozostałe parametry połączenia, takie jak bit parzystości, ilość bitów danych, bity stopu można pozostawić jako wartości domyślne. Po kliknięciu przycisku **`Open`** połączenie zostanie nawiązane, co jest sygnalizowane znakiem gotowości routera.



Rys. 50.2. **Konfiguracja programu Putty do połączenia za pomocą portu konsoli**

Trybem domyślnym pracy routera jest **tryb EXEC użytkownika** – w symbolu zachęty występuje znak „większe niż" (>). W trybie EXEC użytkownika liczba poleceń jest ograniczona, ponieważ są dostępne tylko podstawowe polecenia służące do wyświetlania ustawień terminala, do wykonywania podstawowych testów i do wyświetlania informacji o systemie. Polecenie **`enable`** służy do przełączania użytkownika z trybu EXEC na **uprzywilejowany tryb EXEC** – w symbolu zachęty występuje znak „#". W zestawie poleceń uprzywilejowanego trybu EXEC, oprócz polecenia **`configure`**, są osiągalne także wszystkie polecenia dostępne w trybie EXEC użytkownika. Po wydaniu polecenia **`configure`** możliwe staje się uzyskanie dostępu do pozostałych trybów poleceń.

W uprzywilejowanym trybie wykonawczym (EXEC) użytkownik ma dostęp do wszystkich opcji konfiguracyjnych routera Cisco. Polecenia umożliwiające zmianę trybu poleceń w routerze przedstawiono na rys. 50.3.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Rys. 50.3. **Polecenia umożliwiające zmianę trybu poleceń w routerze**

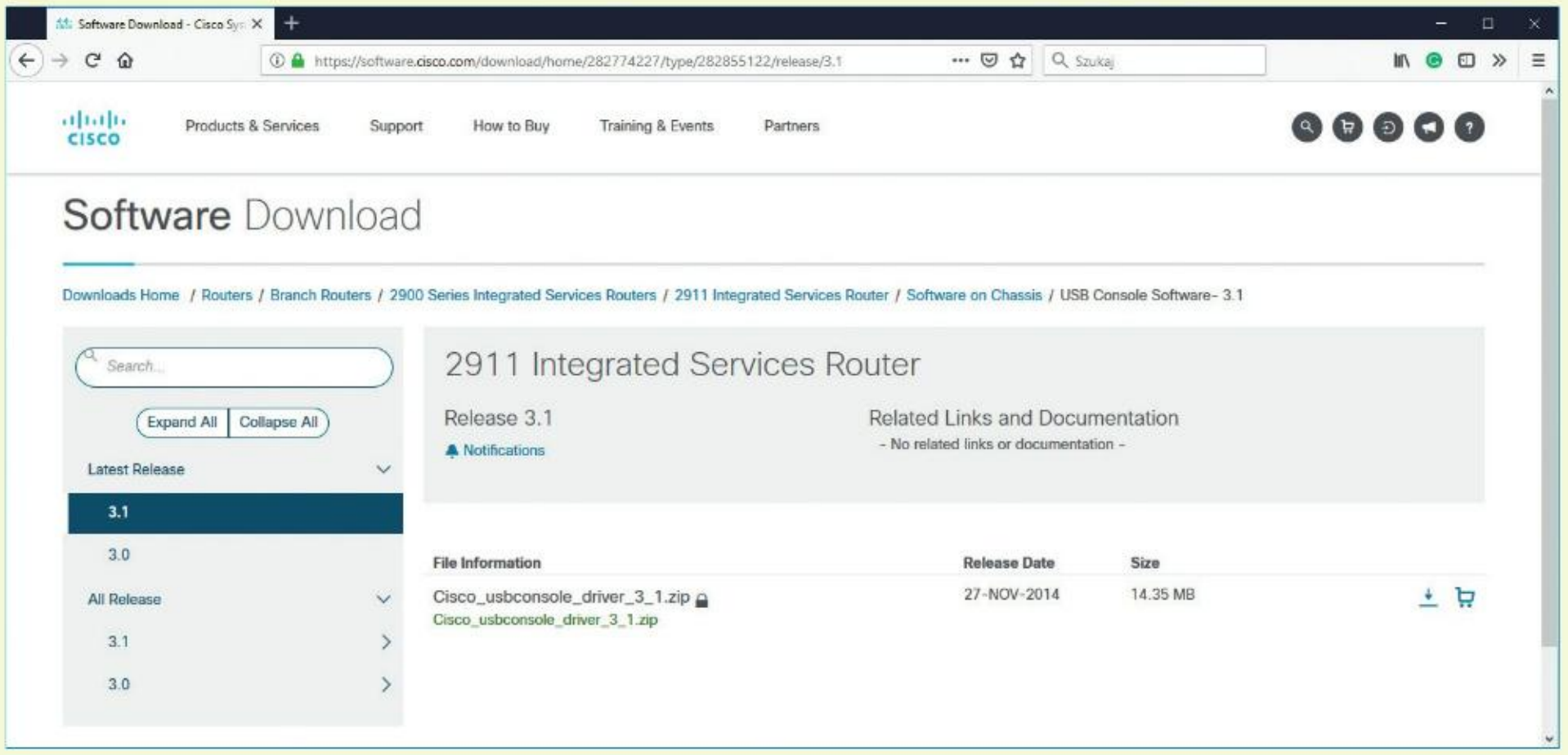
Nową serię urządzeń CISCO wyposażono również w porty konsoli w standardzie USB (typ mini-B). Porty mogą być wykorzystywane zamiennie, ale w danym momencie aktywny jest tylko jeden typ portu.

PRZYKŁAD 50.2

Połączenie komputera z portem konsoli w routerze za pomocą kabla USB

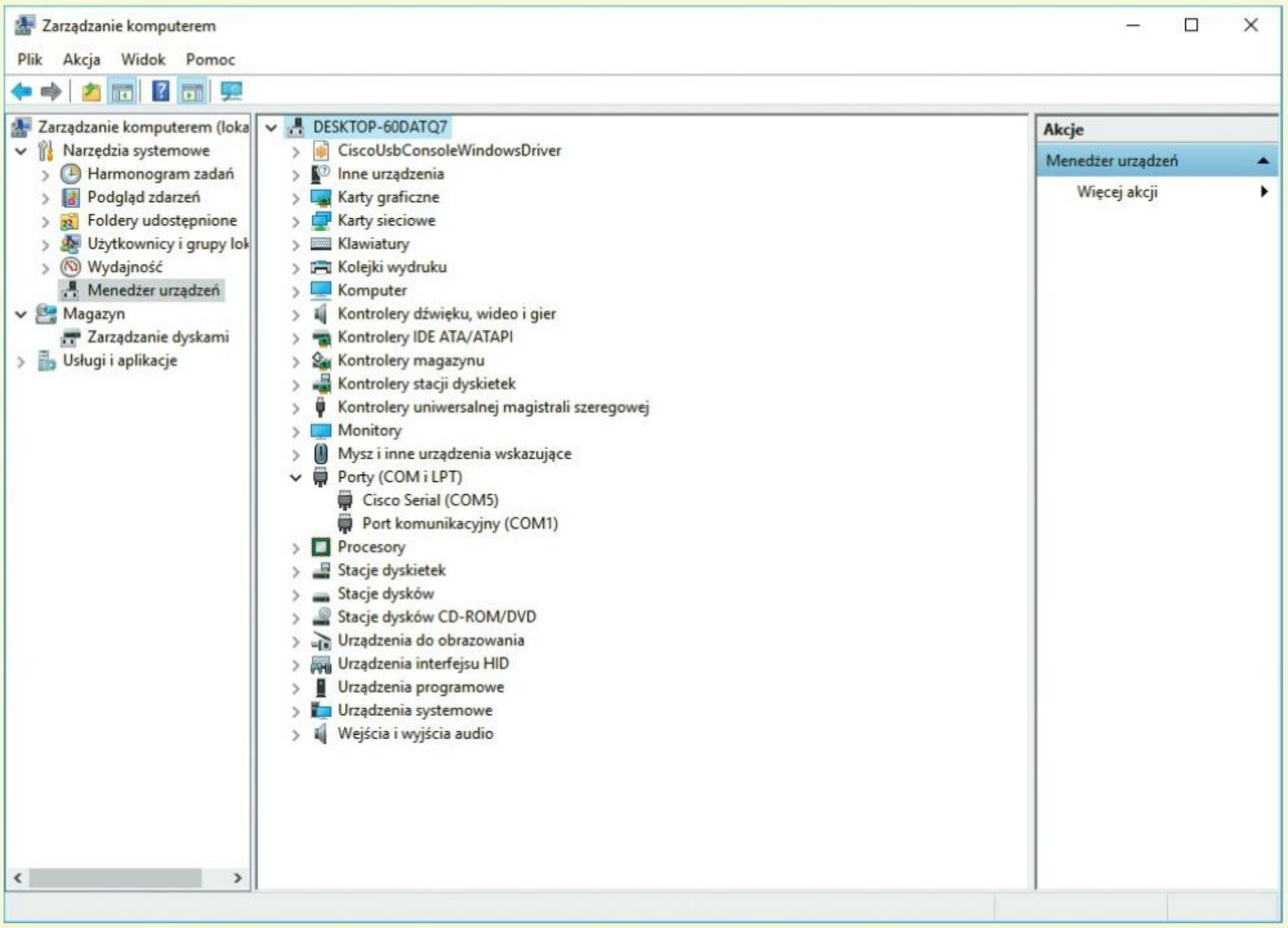
Aby nawiązać połączenie między komputerem a routerem CISCO za pomocą portu konsoli w standardzie USB, należy:

1. Pobrać i zainstalować na komputerze sterownik ze strony CISCO, np. https://software.cisco.com/download/home/282774227/type/282855122/release/3.1 (rys. 50.4). Sterownik umożliwia obsługę konsoli przez porty USB. Pobieranie jest możliwe tylko dla osób mających aktywne konto w systemie. Poproś nauczyciela o pobranie i udostępnienie sterowników.



Rys. 50.4. Strona pobierania sterowników i oprogramowania CISCO

2. Za pomocą kabla konsolowego (USB typ A – USB mini-B) połączyć port konsoli routera (USB mini-B) z portem USB komputera.
3. Sprawdzić w menedżerze urządzeń oznaczenie portu nadane dla nowego portu Cisco Serial (rys. 50.5).
4. Uruchomić na komputerze program Putty. W wyświetlonym oknie dialogowym za pomocą przycisku radiowego należy wybrać typ połączenia **`Serial`** i nazwę portu szeregowego komputera (np. **`COM5`**). Wybrać w sekcji **`Category`** opcję **`Serial`** i ustawić prędkość połączenia (**`Speed: 9600`**) oraz sterowanie przepływem (**`Flow Control: None`**). Pozostałe parametry połączenia, takie jak bit parzystości, ilość bitów danych, bity stopu, można pozostawić jako wartości domyślne. Po kliknięciu przycisku **`Open`** połączenie zostanie nawiązane, co jest sygnalizowane znakiem gotowości routera.



Rys. 50.5. **Informacja o porcie Cisco Serial**

PRZYKŁAD 50.3

Konfigurowanie interfejsu LAN routera

Interfejs LAN routera będzie odgrywał rolę bramy dla komputerów w sieci LAN1. Zwykle przydziela mu się pierwszy z dopuszczalnej puli adresów dla sieci (dla sieci LAN1 zostaną przydzielone adresy z sieci `192.168.1.0` z maską `255.255.255.0`). Sposób konfigurowania interfejsu Gigabit Ethernet przedstawiono na rys. 50.6.

Aby skonfigurować interfejs, należy wykonać następujące polecenia:

1. Polecenie **`enable`** (linijka pierwsza) uruchamia tryb użytkownika uprzywilejowanego.
2. Polecenie **`configure terminal`** powoduje przejście do globalnego trybu konfiguracyjnego routera.
3. W globalnym trybie konfiguracyjnym należy wybrać interfejs, do którego jest przyłączona sieć lokalna (w naszym przypadku – to pierwszy interfejs Gigabit Ethernet) – polecenie **`interface gigabitethernet 0/0/0`**.
4. Przydzielić interfejsowi adres IP i maskę podsieci poleceniem **`ip address 192.168.1.1 255.255.255.0`**.
5. Włączyć interfejs – standardowo interfejsy routera są wyłączone, więc poleceniem **`no shutdown`** należy włączyć interfejs.
6. Powrócić do trybu użytkownika uprzywilejowanego poleceniem **`end`**. Analogiczne polecenia należy wykonać na routerze drugim (trzeba przydzielić inny adres, np. **`192.168.2.1`** z maską **`255.255.255.0`**).

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitethernet 0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

Router(config-if)#
```

KODY

Rys. 50.6. **Konfigurowanie interfejsu Gigabit Ethernet w routerze**

PRZYKŁAD 50.4

Konfigurowanie interfejsu szeregowego routera

Interfejs umożliwi komunikację między routerami. Interfejs szeregowy wymaga, aby jedno z urządzeń wysyłało sygnał taktowania łącza. Takie urządzenie pracuje w trybie **DCE** (ang. *Data Communications Equipment*) i musi mieć ustawioną częstotliwość taktowania. Drugie urządzenie pracujące w trybie **DTE** (ang. *Data Terminal Equipment*) korzysta z sygnału taktowania wysyłanego przez DCE. Sposób konfigurowania interfejsu szeregowego przedstawiono na rys. 50.7.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial 0/1/0
Router(config-if)#clock rate 64000
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shut
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

KODY

Rys. 50.7. **Konfigurowanie interfejsu szeregowego w routerze**

Aby skonfigurować interfejs szeregowy, należy wykonać następujące czynności:

1. Wybrać polecenie **`enable`** (linijka pierwsza), aby uruchomić tryb użytkownika uprzywilejowanego.
2. Wybrać polecenie **`configure terminal`**, powodujące przejście do globalnego trybu konfiguracyjnego routera.

3. W globalnym trybie konfiguracyjnym należy wybrać interfejs wykorzystywany do połączenia z drugim routerem (w naszym przypadku to pierwszy interfejs szeregowy) – polecenie **`interface serial 0/1/0`**.
4. Wybrać polecenie **`clock rate 64000`**, aby ustawić częstotliwość taktowania (tylko na urządzeniu DCE).
5. Przydzielić interfejsowi adres IP i maskę podsieci po wybraniu polecenia **`ip address 10.0.0.1 255.0.0.0`**.
6. Włączyć interfejs – standardowo interfejsy routera są wyłączone, więc włączenie odbywa się za pomocą polecenia **`no shutdown`**.
7. Powrócić do trybu użytkownika uprzywilejowanego po wybraniu polecenia **`end`**. Analogiczne polecenia należy wykonać na routerze drugim (trzeba przydzielić inny adres, np. **`10.0.0.2`** z maską **`255.0.0.0`**, ale bez polecenia **`clock rate`**). Interfejs jest w trybie **wyłączonym** (ang. *down*), ponieważ drugie urządzenie nie zostało jeszcze skonfigurowane. Po prawidłowym skonfigurowaniu drugiego routera interfejs powinien przejść do trybu **włączonego** (ang. *up*).

50.1. Routing statyczny i dynamiczny

Każdy router pracujący w sieci IP korzysta z własnej **tablicy routingu**. Jest to struktura danych umożliwiająca podejmowanie decyzji o sposobie dostarczania danych do adresata. Router, który otrzyma pakiet danych, odszukuje w nagłówku pakiet adres miejsca docelowego (adres IP) i następnie porównuje ten adres z wpisami w tablicy routingu. Po dopasowaniu adresu docelowego do wpisu jest wykonywana akcja – przesłanie pakietu do wybranego interfejsu, za pomocą którego dane są przesyłane do kolejnego routera na trasie lub dostarczane do miejsca docelowego (jeśli router był ostatnim węzłem trasy). Ostatni wpis w tablicy może zawierać trasę domyślną, za pomocą której są wysyłane wszystkie pakiety, które nie zostały wcześniej dopasowane. Jeżeli nie ma trasy domyślnej i pakiet nie zostanie dopasowany do żadnej z tras, to jest on kasowany. Przykładową tablicę routingu przedstawiono na rys. 50.8.

W tablicy routingu na rys 50.8 są widoczne m.in. wpisy określające różne typy tras do sieci:

- **`10.1.2.0`** – sieć bezpośrednio przyłączona do routera (oznaczona literą C);
- **`192.168.1.0/24`** – trasa statyczna (oznaczona literą S);
- **`192.168.3.0/24`** – trasa uzyskana z protokołu RIP (oznaczona literą R);
- `0.0.0.0/0` – trasa domyślna (oznaczona S*).

Błędne lub nieaktualne wpisy w tablicy routingu mogą powodować powstanie pętli lub uniemożliwić pakietom osiągnięcie lokalizacji docelowej. Wpisy do tablicy routingu mogą być wprowadzane ręcznie przez administratora (**routing statyczny**) lub przez protokoły routingu (**routing dynamiczny**).

Zaletami **routingu statycznego** są:

- łatwa możliwość przewidzenia trasy – administrator samodzielnie wprowadza wszystkie trasy na wszystkich routerach i może je kontrolować;
- łącza sieci ani procesory routerów nieobciążane dodatkowo informacjami generowanymi przez protokoły routingu;
- łatwość skonfigurowania w małych sieciach.

```
Router#sh 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,
       ia - L1 - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       p - periodic downloaded static route

Gateway of last resort is 172.16.0.1 to network 0.0.0.0
  10.0.0.0/30 is subnetted, 2 subnets
C 10.1.2.0 is directly connected, Seria10/1/1
C 10.1.3.0 is directly connected, Seria10/1/0
C 172.16.0.0/16 is directly connected, FastEthernet0/1
S 192.168.1.0/24 is directly connected, Seria10/1/1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R 192.168.3.0/24 [120/1] via 10.2.3.1, 00:00:22, Seria10/1/0
S*0.0.0.0/0 [1/0] via 172.16.0.1

Router#
```

Rys. 50.8. **Przykładowa tablica routingu**

PRZYKŁAD 50.5

Konfigurowanie routingu statycznego

Sposób konfigurowania routingu statycznego dla sieci z rys. 50.1 przedstawiono na rys. 50.9. Aby skonfigurować routing statyczny na routerze, należy wykonywać polecenia:

1. Polecenie **`configure terminal`** skutkuje przejściem do globalnego trybu konfiguracyjnego routera.
2. W globalnym trybie konfiguracyjnym polecenie **`ip route 192.168.2.0 255.255.255.0 serial 0/1/0`** dodaje trasę statyczną.
3. Polecenie **`end`** pozwala powrócić do trybu użytkownika zaawansowanego.
4. Polecenie **`ip route 192.168.1.0 255.255.255.0 serial 0/1/0`** dodaje trasę statyczną na drugim routerze.

UWAGA

W poleceniu **`ip route`** można określić kolejny punkt trasy na dwa sposoby: podać identyfikator własnego interfejsu, np. **`serial 0/1/0`**, lub podać adresu IP kolejnego punktu na trasie (ang. *next hop*), np. **`10.0.0.2`**.

5. Sprawdzić możliwość komunikowania się między komputerami w sieciach lokalnych (poleceniem **`ping`**).

KODY

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.2.0 255.255.255.0 serial 0/1/0
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Rys. 50.9. **Konfigurowanie routingu statycznego**

Wadą routingu statycznego jest brak skalowalności – ręczne wprowadzenie wszystkich tras jest pracochłonne, a każdy błąd w konfiguracji może powodować problemy z komunikacją. Taką operację trzeba byłoby powtarzać po każdej zmianie topologii sieci.

Protokoły **routingu dynamicznego** są technologią, która umożliwia routerom samodzielne odkrywanie i utrzymywanie w tablicy routingu tras do wszystkich lokalizacji w sieci. Jeżeli do danej lokalizacji w sieci prowadzi wiele tras, to do tablicy routingu jest wprowadzana tylko najlepsza (z punktu widzenia danego protokołu) trasa – o najniższej metryce. **Metryka trasy** to funkcja określająca jakość trasy. Różne protokoły routingu używają różnych metryk, ale zawsze najlepsza trasa ma najniższą wartość metryki.

PRZYKŁAD 50.6

Konfigurowanie protokołu routingu

Najprostszy protokół routingu RIP umożliwi routerom wymianę informacji o dostępnych sieciach i trasach. Sposób konfigurowania protokołu przedstawiono na rys. 50.10.

Aby skonfigurować protokół RIP, należy wykonywać polecenia:

1. Polecenie **`configure terminal`** skutkuje przejściem do globalnego trybu konfiguracyjnego routera.
2. W globalnym trybie konfiguracyjnym poleceniem **`router rip`** włączamy tryb konfiguracji protokołu RIP.
3. Włączamy wersję 2 protokołu. RIP w wersji 1 jest protokołem klasowym i obsługuje tylko sieci z maskami /8, /16 i /24 (pełne klasy adresów A, B lub C).
   RIP w wersji 2 jest protokołem bezklasowym i obsługuje podsieci z maskami o dowolnej długości.
4. Poleceniem **`network`** określamy bezpośrednio przyłączone do routera sieci, z którymi ma wymieniać dane. Router ma wymieniać dane z sieciami **`192.168.1.0`** oraz **`10.0.0.0`** – należy więc wykonać dwa polecenia **`network`**. W poleceniu **`network`** podaje się adres klasowy sieci – niezależnie od wersji protokołu RIP.
5. Powrócić do trybu użytkownika zaawansowanego poleceniem **`end`**.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

KODY

Rys. 50.10. **Konfigurowanie protokołu RIP**

Analogicznie należy skonfigurować drugi router (trzeba pamiętać, że sieć lokalna przyłączona do routera ma adres 192.168.2.0). Po wykonaniu czynności konfiguracyjnych komputery w sieciach lokalnych mogą się ze sobą komunikować. Potwierdzeniem tego jest wynik polecenia **ping**, które wydano na konsoli komputera z sieci 192.168.1.0, przedstawiony na rys. 50.11.

```
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=23ms TTL=126
Reply from 192.168.2.2: bytes=32 time=22ms TTL=126
Reply from 192.168.2.2: bytes=32 time=20ms TTL=126
Reply from 192.168.2.2: bytes=32 time=20ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 23ms, Average = 21ms

PC>
```

Rys. 50.11. **Testowanie połączenia między sieciami lokalnymi**

! UWAGA

Można jednocześnie skonfigurować na routerze routing statyczny i routing dynamiczny (a nawet – kilka różnych protokołów routingu). Jeżeli do lokalizacji prowadzi trasa wprowadzona statycznie i uzyskana przez protokół routingu, to w tablicy routingu zawsze jest umieszczana trasa statyczna. Jeżeli trasa jest uzyskana przez różne protokoły routingu, to decyduje tzw. **dystans administracyjny**. Za najlepszy protokół routingu jest uznawany EIGRP (dystans 90), później – OSPF (dystans 110) i na końcu – RIP (dystans 120). Dystans administracyjny dla tras statycznych to 1.

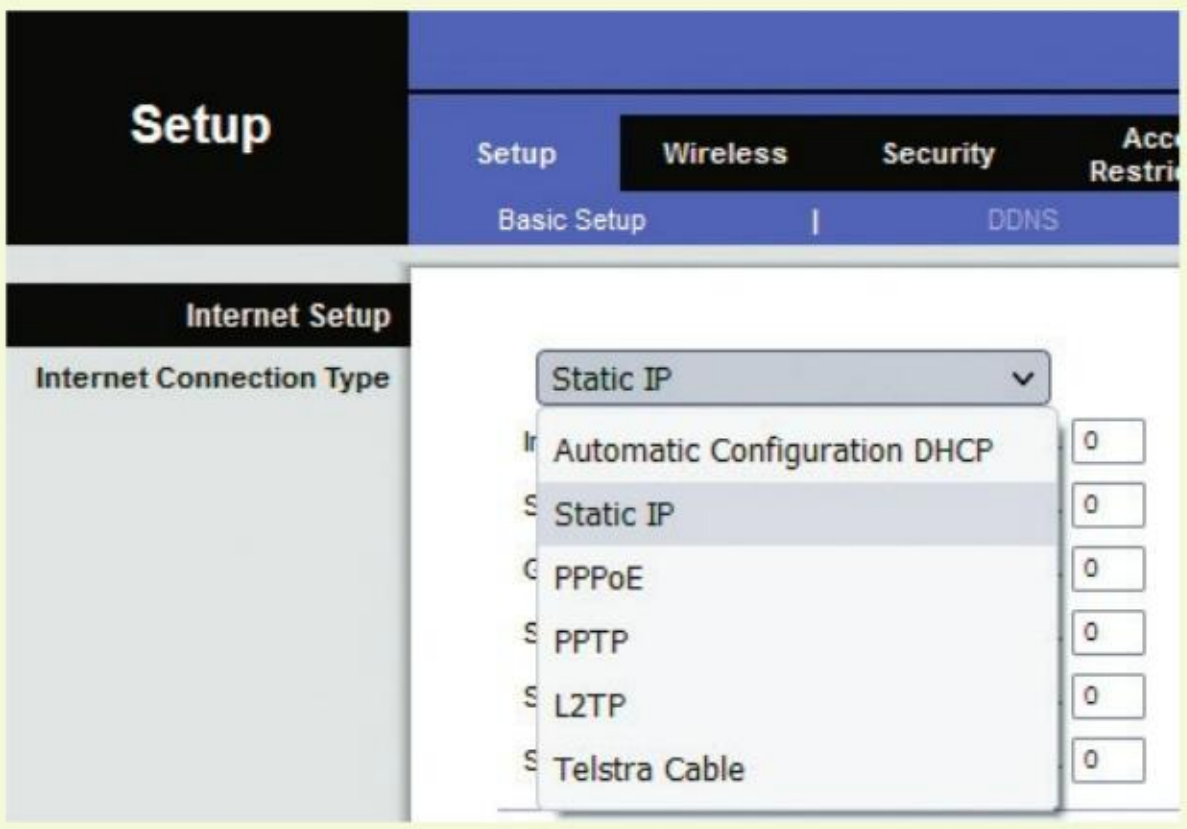
Proste routery używane w domu lub małej sieci mogą być konfigurowane za pomocą przeglądarki internetowej. Standardowa konfiguracja takiego routera umożliwia nawiązanie połączenia i wykonanie czynności konfiguracyjnych w środowisku graficznym. Coraz częściej także w routerach przeznaczonych dla dużych sieci jest dostępny interfejs WWW, chociaż nie zawsze udostępnia on wszystkie opcje konfiguracyjne możliwe do ustawienia z poziomu terminala.

PRZYKŁAD 50.7

Konfigurowanie interfejsów routera za pomocą przeglądarki internetowej

W tym przykładzie zostanie skonfigurowany router Linksys WRT54GL. Konfiguracja innych routerów przebiega podobnie (mogą wystąpić niewielkie różnice w nazwach opcji i sposobie dostępu do poszczególnych opcji). Jeżeli w twojej szkole jest używany inny typ routera, to zapytaj nauczyciela o sposób skonfigurowania. Aby skonfigurować router za pomocą przeglądarki internetowej, należy:

1. Połączyć kablem kartę sieciową komputera z interfejsem LAN routera.
2. Skonfigurować kartę sieciową komputera i interfejs LAN routera do pracy w tej samej sieci (informacje o standardowej konfiguracji routera można znaleźć w dokumentacji). Router Linksys WRT54GL standardowo ma przypisany adres: 192.168.1.1, maskę podsieci: 255.255.255.0, konto administratora: **`admin`** i hasło: **`admin`**. Jeżeli hasło konta administratora nie jest znane, to można przywrócić router do stanu fabrycznego – w tym celu należy nacisnąć i przytrzymać przez 30 s przycisk Reset z tyłu routera. Ta operacja usunie wszystkie ustawienia konfiguracyjne wprowadzone przez użytkownika.
3. W komputerze w oknie adres wyszukiwarki wpisać adres routera, np. 192.168.1.1, a w wyskakującym okienku podać nazwę konta administratora i hasło.
4. W zakładce **`Setup`** wybrać **`Basic setup`**, a następnie z listy rozwijanej wybrać sposób konfiguracji interfejsu. Wybór opcji **`statycznego przypisywania adresu IP`** (ang. *static IP*) jest dokonywany, gdy dostawca internetowy oferuje stały adres IP i udostępnia wszystkie dane niezbędne do konfiguracji interfejsu (adres IP, maskę podsieci, adres bramy, adresy serwerów DNS). Administrator routera będzie musiał samodzielnie wprowadzić te parametry. Jeżeli dostawca internetowy oferuje zmienny adres IP i dostarcza dane do konfiguracji za pomocą serwera DHCP, należy wybrać opcję **`automatycznego konfigurowania interfejsu`** (ang. *automatic configuration DHCP*). Wtedy wszystkie informacje niezbędne do konfiguracji interfejsu będą pobierane automatycznie. Na rys. 50.12 przedstawiono wybór opcji statycznego konfigurowania interfejsu WAN.

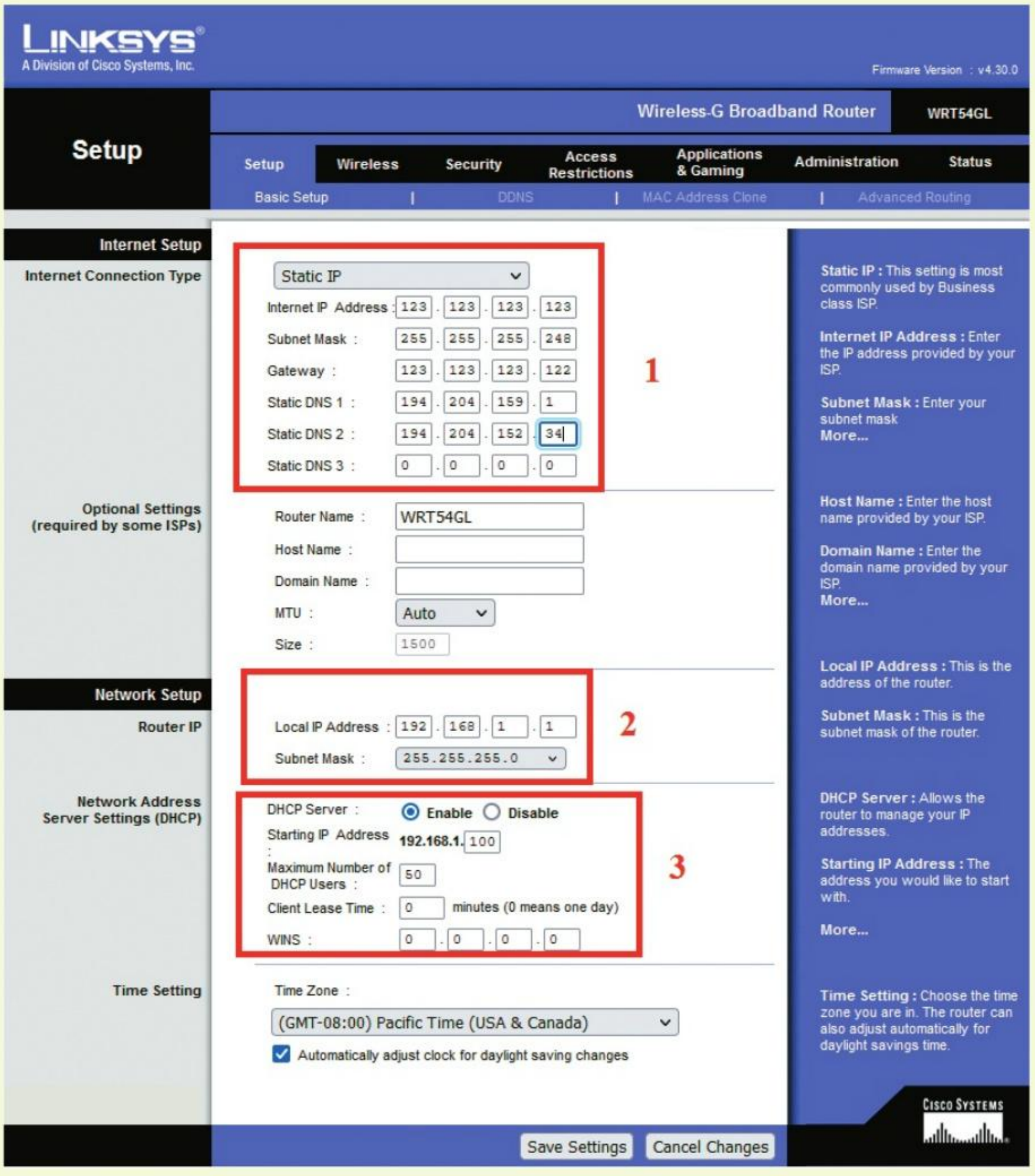


Rys. 50.12. **Wybór trybu konfigurowania interfejsu WAN routera**

5. Wprowadzić informacje o konfiguracji interfejsu WAN uzyskane od dostawcy internetowego (na rys. 50.13 – blok informacji oznaczony 1):

- adres IP (ang. *internet IP address*);
- maska podsieci (ang. *subnet mask*);
- domyślna brama (ang. *gateway*);
- adresy serwerów DNS (ang. *static DNS 1, static DNS 2*).

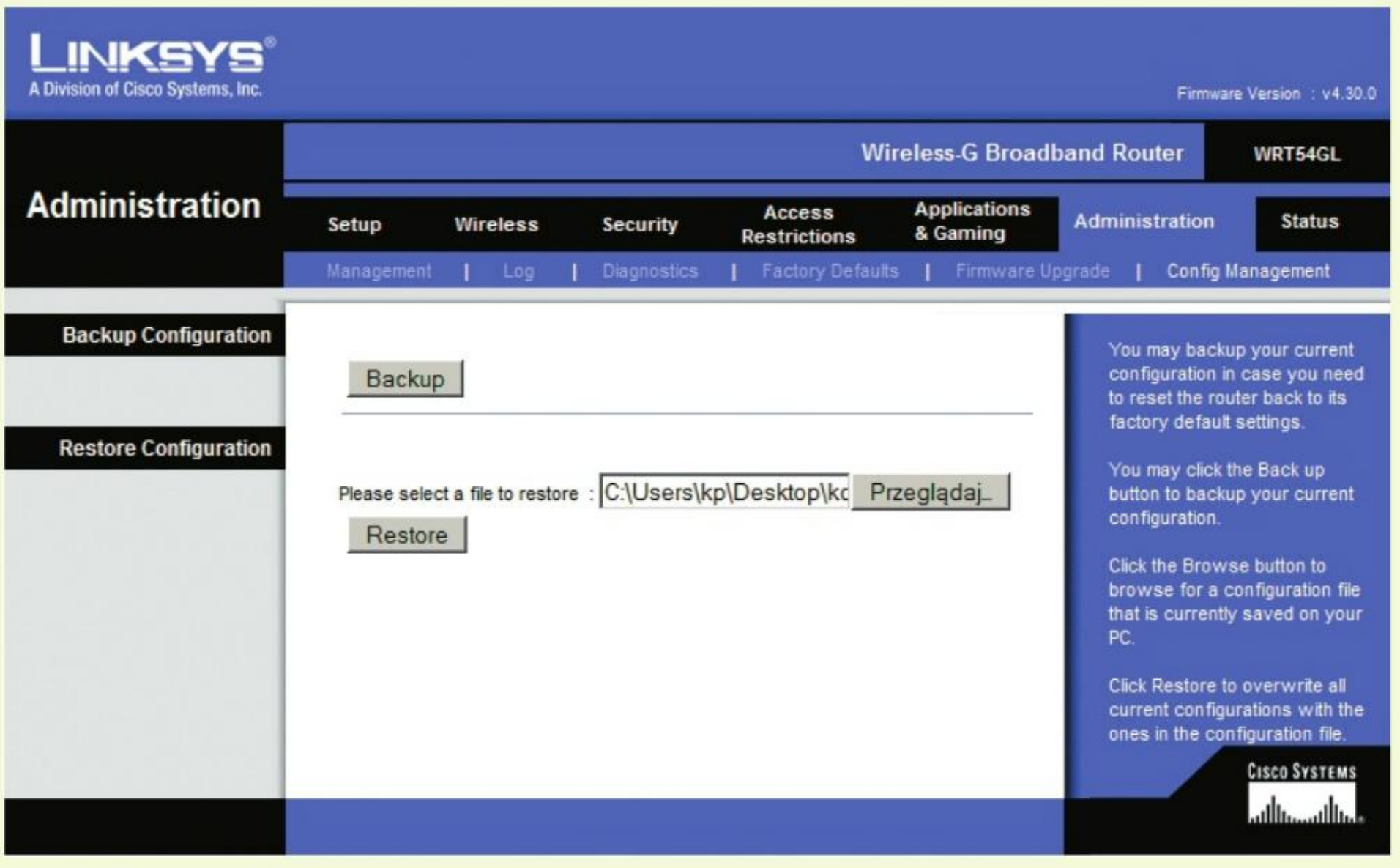
6. Wprowadzić informacje o konfiguracji interfejsu LAN (na rys. 50.13 blok informacji oznaczony 2). O konfiguracji interfejsu LAN decyduje administrator routera. Najczęściej po stronie sieci LAN przydziela się adresy prywatne odpowiadające schematowi adresowania przyjętemu w organizacji (w sieci LAN mogą być używane również adresy publiczne, ale wymaga to przydziału tych adresów od dostawcy). Administrator powinien określić:
- adres IP (ang. *local IP address*) dla interfejsu LAN routera;
- maskę podsieci (ang. *subnet mask*).



Rys. 50.13. **Okno podstawowej konfiguracji routera**

7. Na routerze można uruchomić serwer DHCP, który będzie przydzielał dane konfiguracyjne dla hostów w sieci LAN. Można też wprowadzić informacje o konfiguracji serwera DHCP (na rys. 50.13 blok informacji oznaczony 3):
   - włączyć serwer DHCP – przełącznik **DHCP Server** ustawić na **Enable**;
   - wprowadzić początkowy adres puli adresów przydzielanych klientom (ang. *starting IP address*);
   - wprowadzić maksymalną liczbę adresów przydzielanych klientom (ang. *maximum number of DHCP users*);
   - ustawić czas dzierżawy adresu (ang. *DHCP lease time*);
   - adres serwera WINS (WINS) – usługa WINS w nowych sieciach nie jest wykorzystywana – może pozostać bez zmian.
8. Kliknąć przycisk **Save Settings**, aby zapisać zmiany.

Po zakończeniu konfiguracji routera należy przetestować jego działanie. W tym celu z wiersza poleceń komputera w sieci lokalnej trzeba wydać polecenie **ping**. Jako argument należy podać adres IP interfejsu LAN routera (ping do bramy) i adres IP serwera w internecie, np. serwera DNS (208.67.222.222). Jeżeli oba polecenia zwrócą wynik pozytywny, oznacza to, że konfiguracja została wykonana prawidłowo i można korzystać z dostępu do internetu.
Parametry konfiguracji routera można zapisać w pliku. Utworzona w ten sposób kopia parametrów może być wykorzystana w razie uszkodzenia routera i w obliczu konieczności jego wymiany na taki sam model albo w razie uszkodzenia lub skasowania pliku konfiguracyjnego. Aby utworzyć kopię zapasową konfiguracji routera, należy w zakładce **Administration** wybrać opcję **Config management** (rys. 50.14.) Kliknięcie przycisku **Backup** uruchamia kreatora tworzenia kopii zapasowej, natomiast przycisk **Restore** umożliwia odtworzenie danych z kopii.



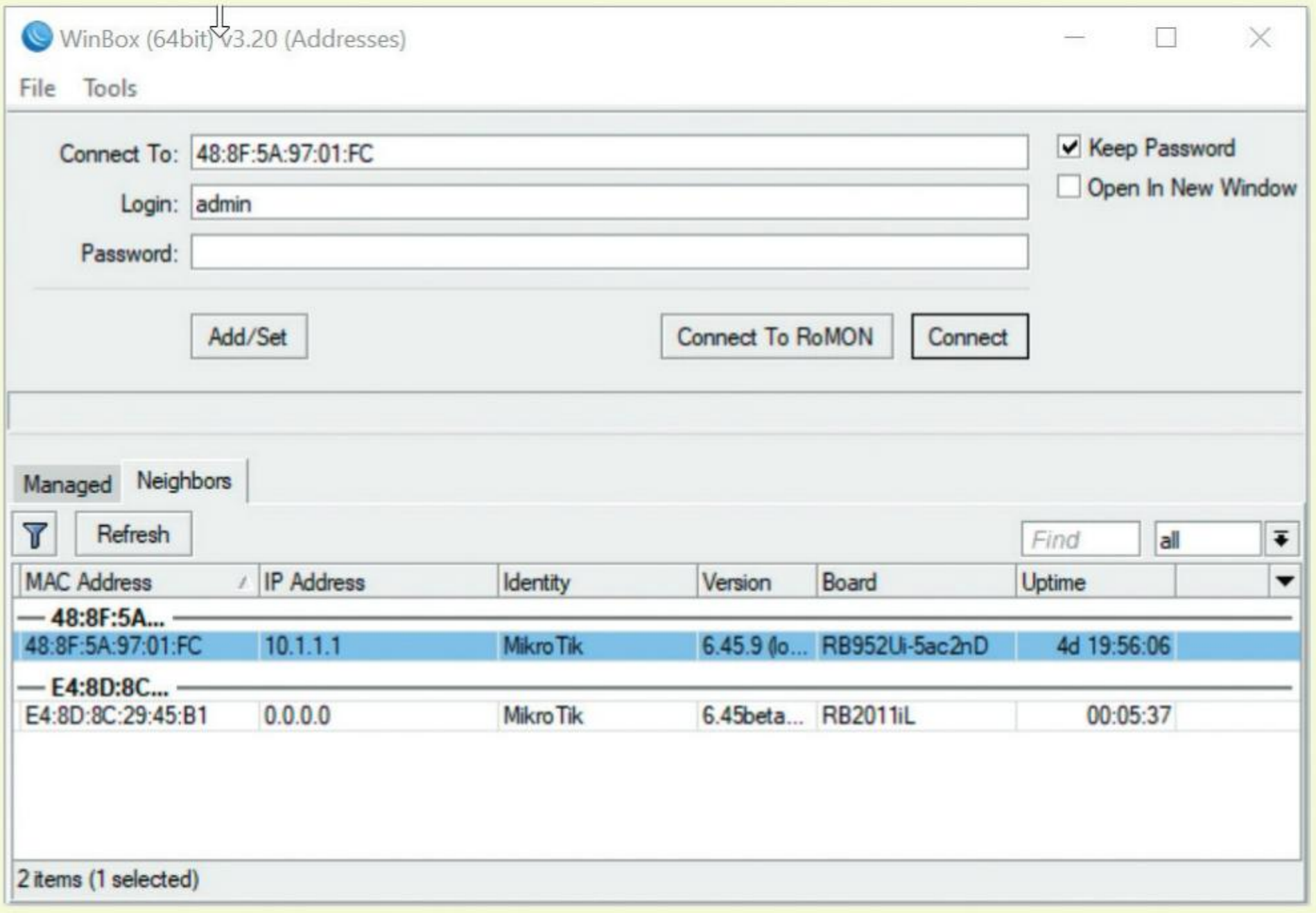
Rys. 50.14. **Okno zarządzania konfiguracją routera**

PRZYKŁAD 50.8

Konfigurowanie sieci w oparciu na routerach firmy Mikrotik

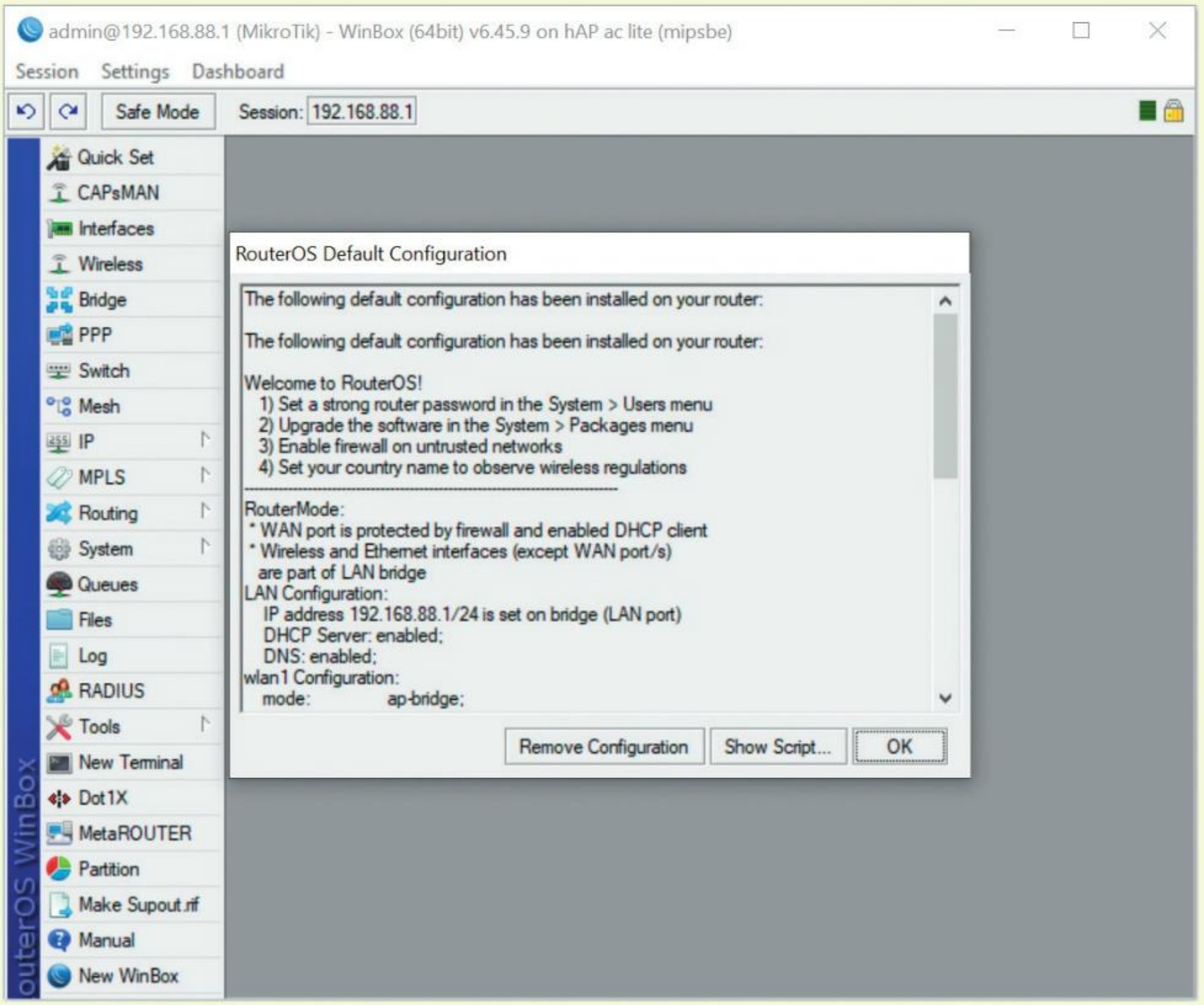
W tym przykładzie zostanie skonfigurowana sieć (jak na rys. 50.1) za pomocą routerów Mikrotik hAP ac lite. Routery zapewnią komunikację między sieciami lokalnymi z adresami 192.168.1.0/24 oraz 192.168.2.0/24, przyłączonymi do portu Ethernet2. Połączenie między routerami za pomocą portu Ethernet1 z adresami z sieci 10.0.0.0/30. Konfiguracja tych routerów może być wykonana za pomocą programu **Winbox** lub przeglądarki internetowej. Konfiguracja innych modeli tego samego producenta przebiega podobnie. Aby skonfigurować router za pomocą programu Winbox, należy:

1. Pobrać Winbox, np. ze strony https://mikrotik.com/download, i go zainstalować.
2. Uruchomić program i nawiązać połącznie z routerem (rys. 50.15). Program automatycznie wyszuka kompatybilne urządzenia w sieci lokalnej. Urządzenia mogą być lokalizowane za pomocą adresów MAC lub IP. Kliknąć odpowiednie urządzenie. Wprowadzić dane logowania (login i password) i kliknąć przycisk **Connect**.

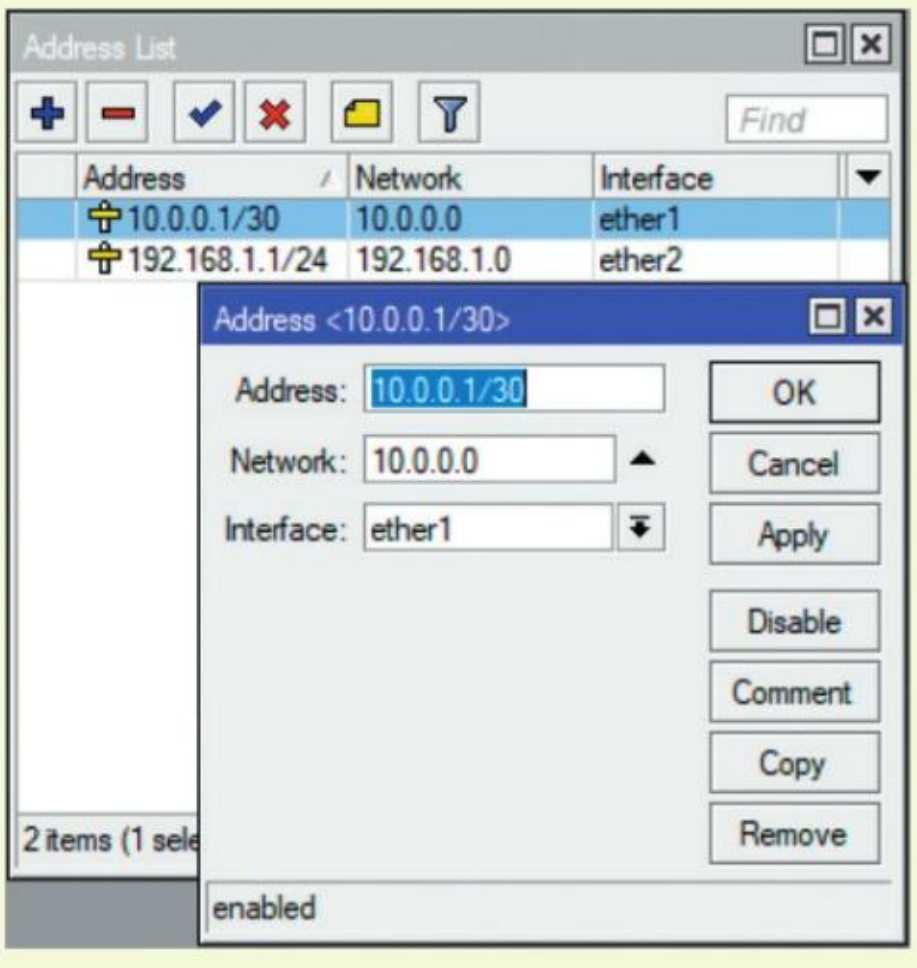


Rys. 50.15. **Nawiązywanie połącznia z routerem Mikrotik**

3. Podczas pierwszego uruchomienia urządzenia (lub po resecie do ustawień fabrycznych) jest tworzona domyślna konfiguracja. Trzeba ją zaakceptować – kliknięciem przycisku **OK** (rys. 50.16).
4. Skonfigurować port Ethernet1, przeznaczony do połączenia między routerami. Aby wprowadzić dane konfiguracyjne interfejsu, należy z menu bocznego wybrać **IP/Addresses**. W oknie **Address List** kliknąć przycisk „**+**”, wprowadzić dane konfiguracyjne interfejsu (rys. 50.17) i kliknąć przycisk **Apply**, a następnie – **OK**.



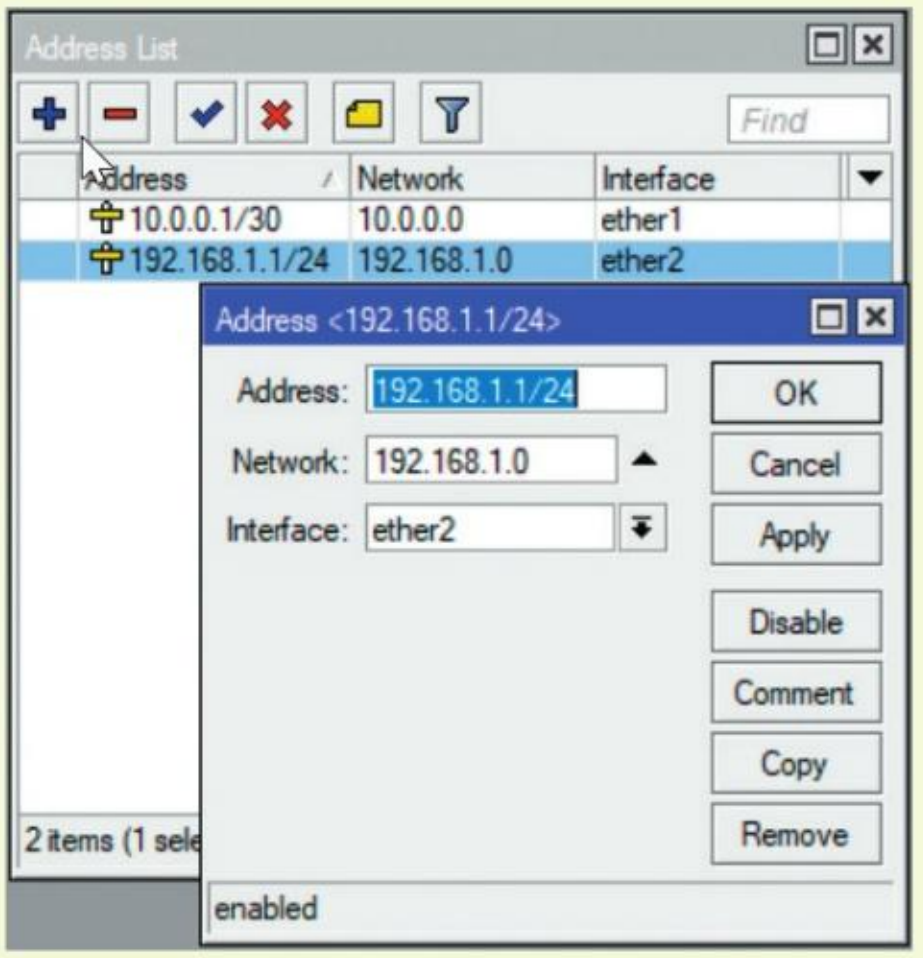
Rys. 50.16. **Domyślna konfiguracja routera Mikrotik**



Rys. 50.17. **Konfiguracja interfejsu Ethernet1 routera Mikrotik**

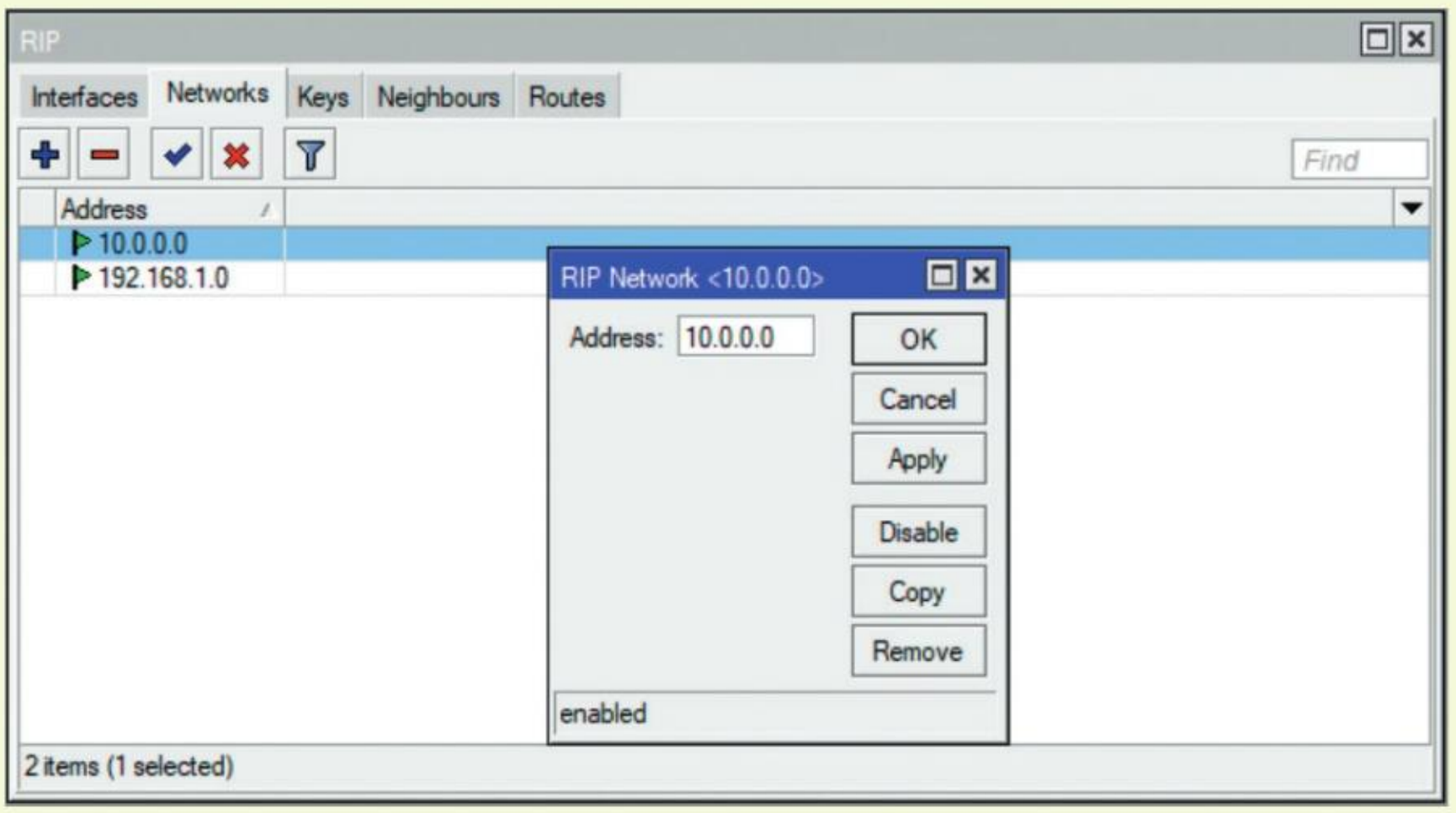
5. Skonfigurować interferjs Ethernet2. Aby wprowadzić dane konfiguracyjne portu, należy z menu bocznego wybrać **`IP/Addresses`**. W oknie **`Address List`** kliknąć

przycisk „**+**”, wprowadzić dane konfiguracyjne interfejsu (rys. 50.18) i kliknąć przycisk **Apply**, a następnie – **OK**.



Rys. 50.18. **Konfiguracja interfejsu Ethernet2 routera Mikrotik**

6. Skonfigurować protokół routingu. Z menu bocznego wybrać **Routing/RIP**. W oknie **RIP** wybrać zakładkę **Networks** i kliknąć przycisk „**+**”, wprowadzić dane sieci 10.0.0.0 i 192.168.1.0 (rys. 50.19). Kliknąć przycisk **Apply**, a następnie – **OK**.



Rys. 50.19. **Konfiguracja protokołu RIP w routerze Mikrotik**

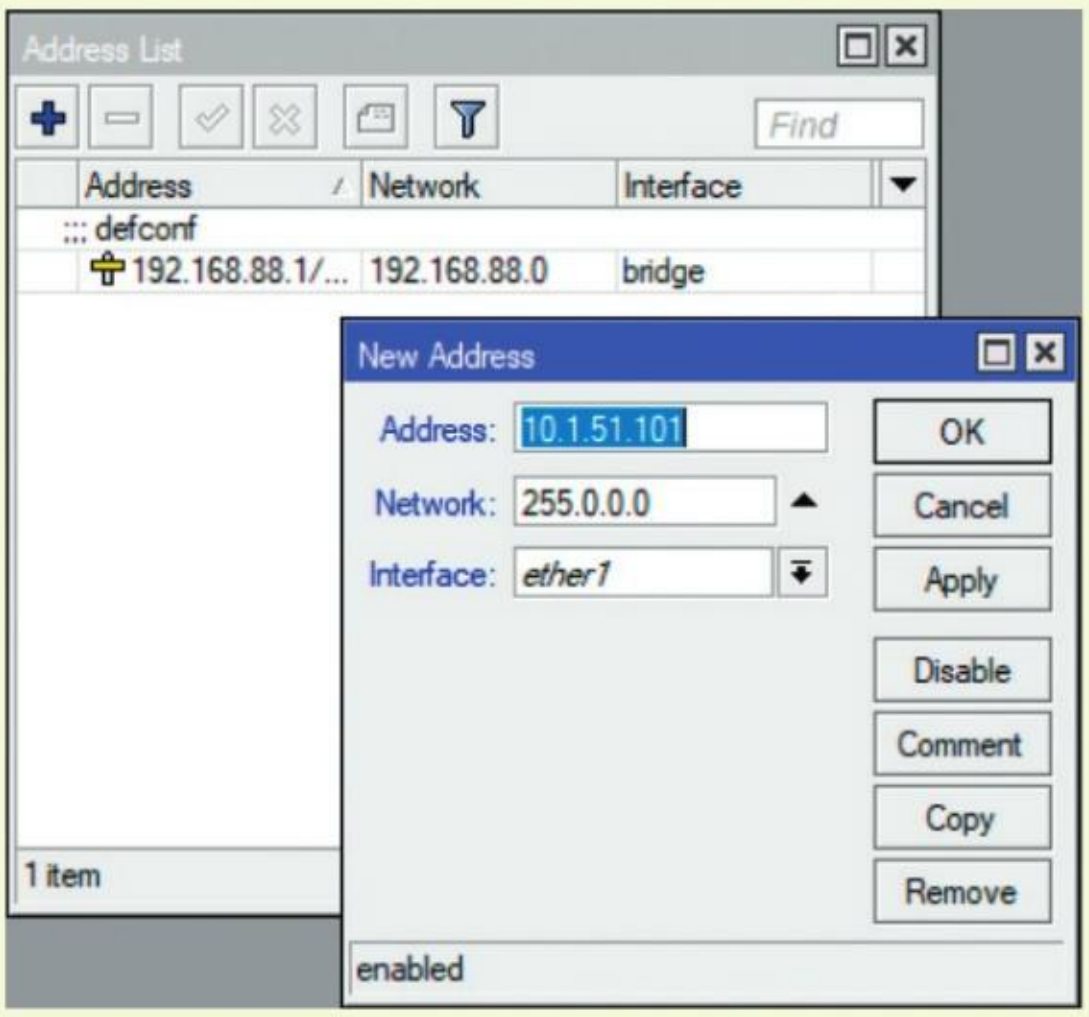
7. Skonfigurować drugi router. Dla interfejsu Ethernet1 przydzielić adres 10.0.0.2/30, a dla interfejsu Ethernet2 przydzielić adres 192.168.2.1/24. Skonfigurować protokół routingu (dodać sieci 10.0.0.0 i 192.168.2.0).
8. Do portów Ethernet2 w obu routerach podłączyć komputery z ustawionymi odpowiednimi adresami IP i sprawdzić możliwość komunikacji między komputerami.

PRZYKŁAD 50.9

Konfigurowanie routera firmy Mikrotik

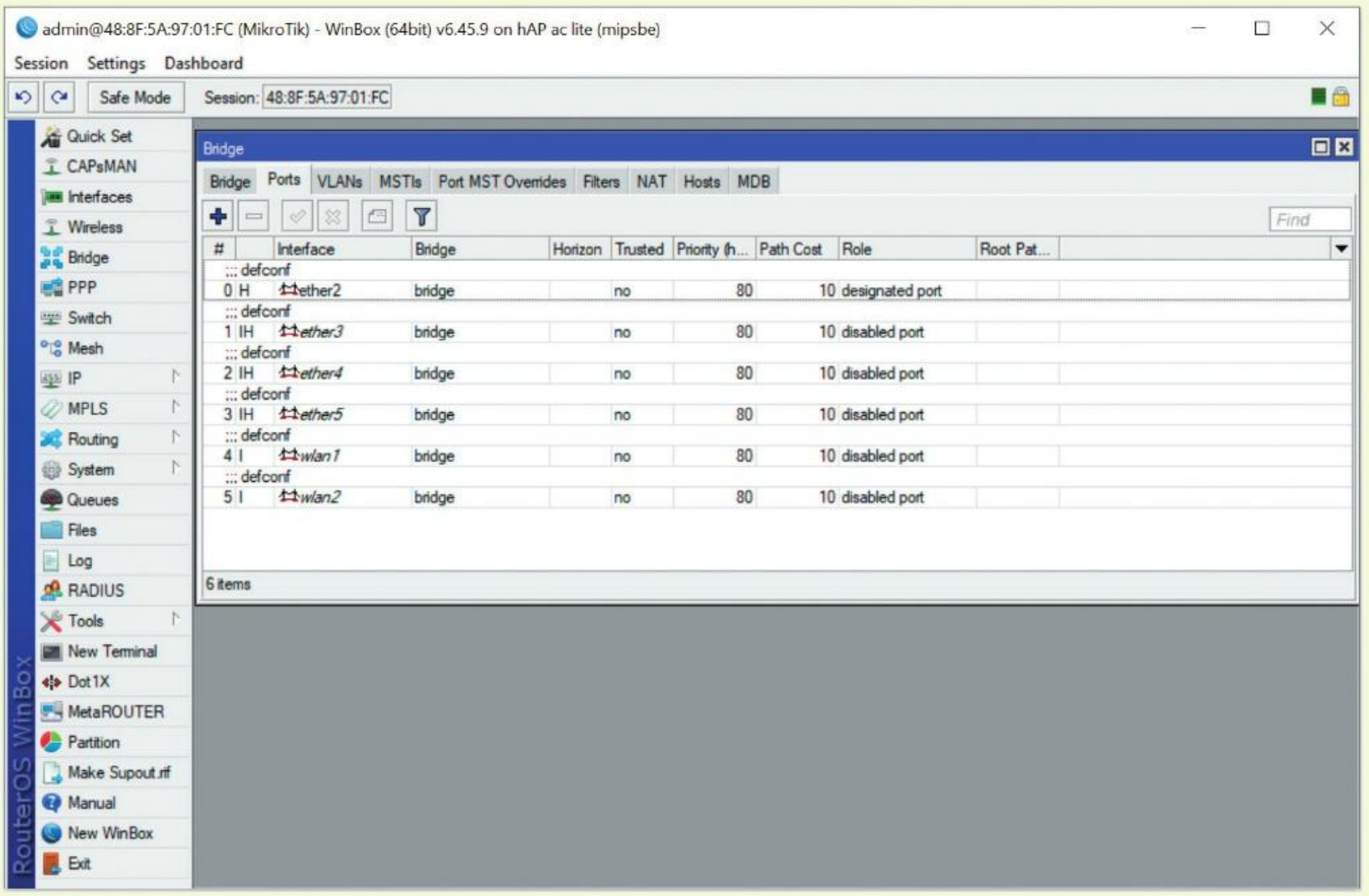
W tym przykładzie zostanie skonfigurowany router Mikrotik hAP ac lite. Router zapewni komunikację między siecią szkolną z adresami 10.0.0.0/8 a siecią lokalną użytkownika, np. 192.168.10.0/24. Konfiguracja innych modeli tego samego producenta przebiega podobnie. Aby skonfigurować router za pomocą programu Winbox, należy:

1. Uruchomić program Winbox i nawiązać połącznie z routerem. Kliknąć odpowiednie urządzenie. Wprowadzić dane logowania (login i password) i kliknąć przycisk **Connect**.
2. Podczas pierwszego uruchomienia urządzenia (lub po resecie do ustawień fabrycznych) jest tworzona domyślna konfiguracja. Trzeba ją zaakceptować kliknięciem przycisku **OK**.
3. Skonfigurować interfejs sieci WAN. Standardowo port Ethernet1 jest przeznaczony do podłączenia dostawcy internetowego. Ten interfejs może być konfigurowany przez protokół DHCP (jeśli dostawca oferuje taką usługę) lub do interfejsu należy przypisać dane konfiguracyjne uzyskane od dostawcy. Aby samodzielnie wprowadzić dane, należy z menu bocznego wybrać **IP/Addresses**. W oknie **Address List** kliknąć przycisk „**+**”, wprowadzić dane konfiguracyjne interfejsu (rys. 50.20) i kliknąć przycisk **Apply**, a następnie – **OK**.

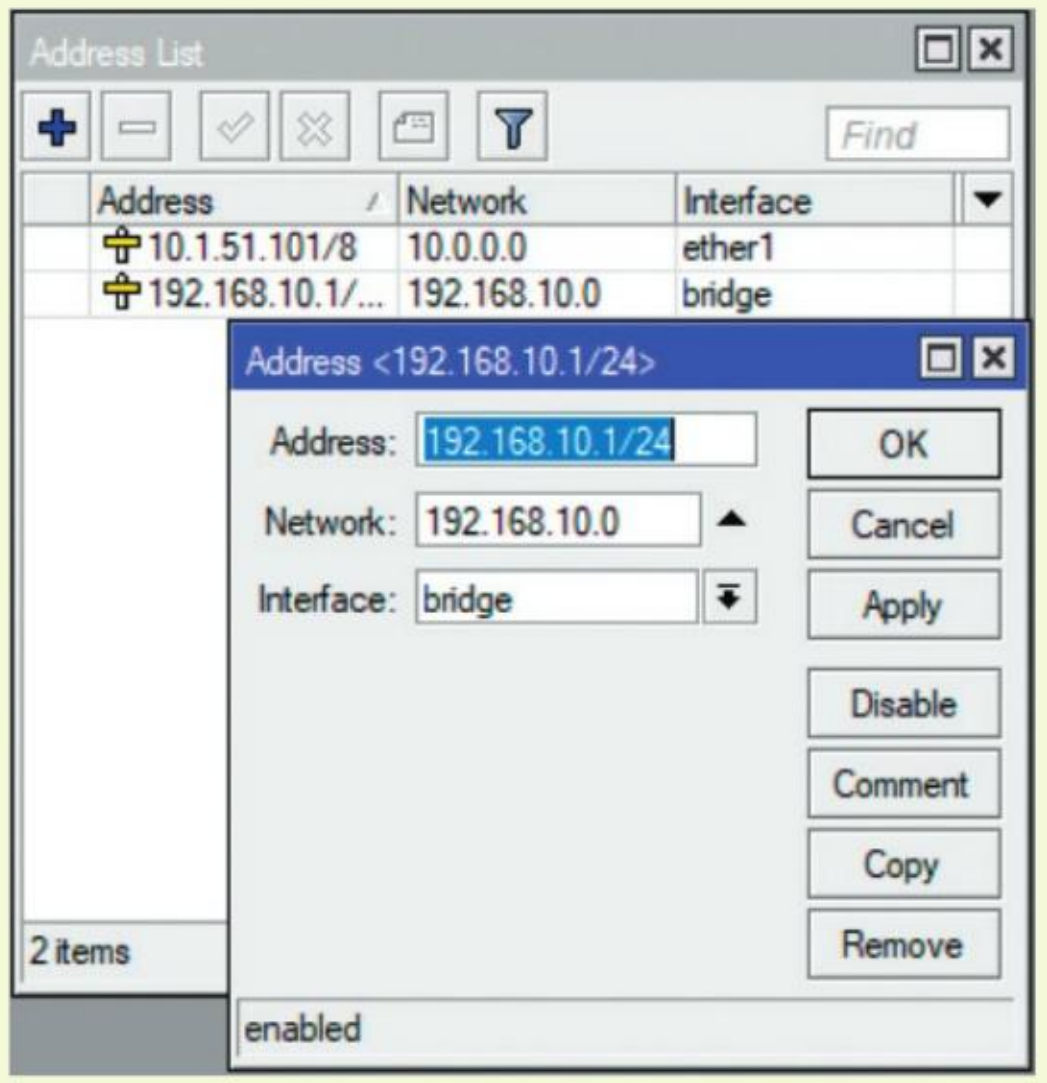


Rys. 50.20. **Konfiguracja interfejsu WAN routera Mikrotik**

4. Skonfigurować interferjs sieci LAN. Standardowo porty Ethernet (z wyjątkiem portu WAN) są połączone **mostem** (ang. *bridge*). Adres IP można przypisać do mostu lub skasować most i przypisać adresy IP do poszczególnych portów. W tym przykładzie adres IP zostanie przypisany do mostu **brigde**. Aby skonfigurować most, należy z menu bocznego wybrać **Bridge**. W zakładce **Ports** kliknąć przycisk „**+**”, wskazać porty należące do mostu (rys. 50.21).
5. Aby wprowadzić adres IP dla mostu, należy z menu bocznego wybrać **IP/Addresses**. W oknie **Address List** kliknąć przycisk „**+**”, wprowadzić dane konfiguracyjne mostu (rys. 50.22) i kliknąć przycisk **Apply**, a następnie – **OK**.



Rys. 50.21. **Konfiguracja mostu w routerze Mikrotik**

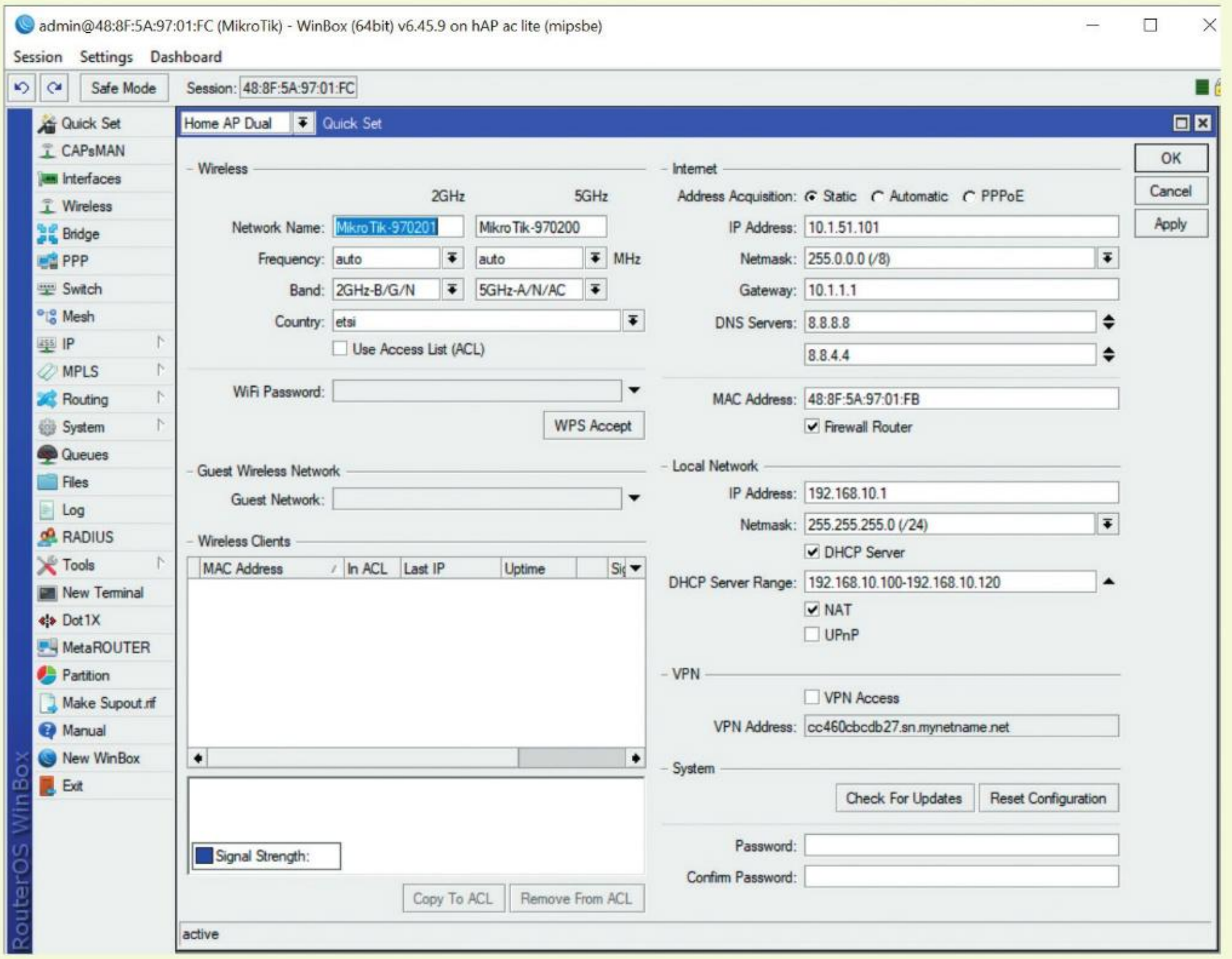


Rys. 50.22. **Konfiguracja adresu IP mostu w routerze Mikrotik**

6. Wprowadzić dodatkowe ustawienia. Z menu bocznego wybrać **`Quick Set`**. W oknie **`Quick Set`** (rys. 50.23) ustawić:
   - adres bramy (ang. *Gateway*), np. **`10.1.1.1`**;
   - adresy serwerów DNS (ang. *DNS Servers*), np. **`8.8.8.8`** i **`8.8.4.4`**;

- włączyć serwer DHCP (ang. *DHCP Server*) i ustawić zakres adresów przydzielanych dla klientów w sieci lokalnej, np. od **`192.168.10.100`** do **`192.168.10.120`**;
- włączyć usługę NAT.

7. Kliknąć przycisk **`Apply`**, a następnie – **`OK`**.
8. Przetestować działanie routera. Podłączyć komputer do portu należącego do mostu i poleceniem **`ping`** sprawdzić możliwość komunikacji z wybranym serwerem w internecie.



Rys. 50.23. **Konfiguracja routera Mikrotik**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sporządź listę wszystkich parametrów konfiguracji routera niezbędnych do uzyskania dostępu do internetu w twojej szkole i w domu. Zapisz dane w bezpiecznym miejscu na wypadek uszkodzenia routera i ponownej konfiguracji.

51 Konfigurowanie urządzeń sieci bezprzewodowych

ZAGADNIENIA

Infrastruktura sieci bezprzewodowych **Tryby pracy sieci bezprzewodowych** **Standardy dotyczące sieci bezprzewodowych** **Skonfigurowanie bezprzewodowej karty sieciowej** **Skonfigurowanie sieci działającej w trybie ad hoc i infrastruktury** **Zabezpieczenie sieci bezprzewodowej przed podsłuchem** **Standardy szyfrowania danych używane w sieciach bezprzewodowych** **Włączanie szyfrowania danych w sieci bezprzewodowej** **Bezpieczne uwierzytelnianie za pomocą protokołu RADIUS** **Sieci Wi-Fi zarządzane przez kontroler sieci** **Anteny używane w telekomunikacji**

Łączność bezprzewodowa zdobywa coraz szersze zastosowanie, również w dziedzinie lokalnych sieci komputerowych. **Bezprzewodowa sieć lokalna WLAN** to sieć, w której połączenia między urządzeniami sieciowymi zrealizowano bez użycia przewodów. Do przesyłania danych między urządzeniami wykorzystuje się fale radiowe. Zakres częstotliwości fal radiowych wykorzystywany w sieciach WLAN nie podlega koncesjonowaniu i dlatego można go używać bez żadnych zezwoleń. Jednak w tym paśmie występują znaczne zakłócenia pochodzące od innych urządzeń, np. kuchenek mikrofalowych bądź telefonów bezprzewodowych. Infrastruktura sieci bezprzewodowych składa się z:

- **kart sieciowych** – najczęściej typu PCI, PCIExpress, ExpressCard, USB, PCMCIA, ale też wbudowanych w urządzenia przenośne, takie jak laptopy, smartfony itp.;
- **punktów dostępowych** – odgrywających rolę bezprzewodowych koncentratorów w sieciach pracujących w trybie infrastruktury;
- **anten**;
- **kabli**, **złączy** itp.

Małe sieci bezprzewodowe mogą być budowane w trybie **ad hoc** – w tym trybie urządzenia komunikują się bezpośrednio. Dla większych sieci przewidziano **tryb infrastruktury**, w którym urządzenia komunikują się za pośrednictwem punktów dostępowych. Istnieje kilka standardów sieci WLAN, różniących się częstotliwościami pracy, prędkościami przesyłania danych i sposobem kodowania sygnału. Te standardy opisano w dokumencie IEEE802.11. Najpopularniejsze standardy sieci bezprzewodowych to:

- **802.11a** (**Wi-Fi 2**) – standard wykorzystuje pasmo częstotliwości w zakresie 5,15–5,35 GHz i 5,725–5,825 GHz. Obejmuje osiem kanałów, przeznaczonych do pracy w budynkach, i cztery do pracy między dwoma punktami (ang. *point-to-point*). Praca na wyższych częstotliwościach powoduje zmniejszenie zasięgu mniej więcej o połowę (w porównaniu z innymi sieciami). Maksymalna prędkość transmisji w tym standardzie wynosi 54 Mb/s. Wadą jest brak zgodności z innymi standardami;
- **802.11b** (**Wi-Fi 1**) – używa pasma w częstotliwości mniej więcej 2,4 GHz (od 2400 MHz do 2485 MHz) i osiąga maksymalną prędkość 11 Mb/s w promieniu 46 m w pomieszczeniach

zamkniętych i 96 m na otwartych przestrzeniach. Pasmo częstotliwości jest podzielone na 14 kanałów o szerokości 22 MHz, częściowo zachodzących na siebie (tylko trzy kanały nie pokrywają się w swoich zakresach). W Polsce można wykorzystywać tylko kanały od 1 do 13;

- **802.11g** (**Wi-Fi 3**) – ten standard używa tego samego pasma częstotliwości co 802.11b. Umożliwia transmisję danych z prędkością do 54 Mb/s. Jest w pełni zgodny z 802.11b;
- **802.11n** (**Wi-Fi 4**) – zależnie od rozwiązania (zastosowanych anten) pozwala na przesyłanie plików z prędkością teoretyczną – od 150 Mb/s do 600 Mb/s. Standard „n" może działać na częstotliwości zarówno 2,4 GHz, jak i 5 GHz (jednak większość urządzeń pracuje tylko w paśmie 2,4 GHz). Standard obsługuje **technologię komunikacji wielostrumieniowej** (ang. *Multiple Input Multiple Output*, MIMO) wykorzystującą wiele anten do nadawania oraz odbioru sygnału (sygnał jest dzielony na kilka strumieni, nadawany jednocześnie z kilku źródeł i odbierany przez kilka odbiorników). Urządzenia 802.11n wykorzystują do czterech kanałów transmisyjnych o przepustowości 150 Mb/s każdy do stworzenia jednego połączenia, co zwiększa dostępną prędkość transmisji. Starsze urządzenia obsługujące jedynie standard „b" lub „g" mogą współpracować z urządzeniem działającym w standardzie „n", jednak w takiej sytuacji następuje przełączenie na wolniejsze tempo standardu „b" lub „g";
- **802.11ac** (**Wi-Fi 5**) – standard o przepustowości przekraczającej 1 Gb/s, pracujący na częstotliwości 5 GHz;
- **802.11ax** (**Wi-Fi 6**) – najnowszy standard pracujący na częstotliwości 2,4 GHz lub 5 GHz i dodatkowo na częstotliwości 6 GHz (Wi-Fi 6E). Stanowi rozszerzenie standardu Wi-Fi 5. Oferuje maksymalną prędkość transmisji 9,6 Gb/s, m.in. dzięki udoskonalonej metodzie kodowania 1024-QAM, obsłudze MIMO 8×8 i zwiększeniu pojemności sieci.

Przed przyłączeniem komputera do sieci bezprzewodowej należy skonfigurować bezprzewodową kartę sieciową. Jeżeli w sieci bezprzewodowej działa serwer DHCP, to karta będzie mogła otrzymać adres IP i inne dane niezbędne do prawidłowej pracy w sieci. Jeżeli w sieci nie ma serwera DHCP, to wszystkie dane należy przypisać karcie ręcznie.

PRZYKŁAD 51.1

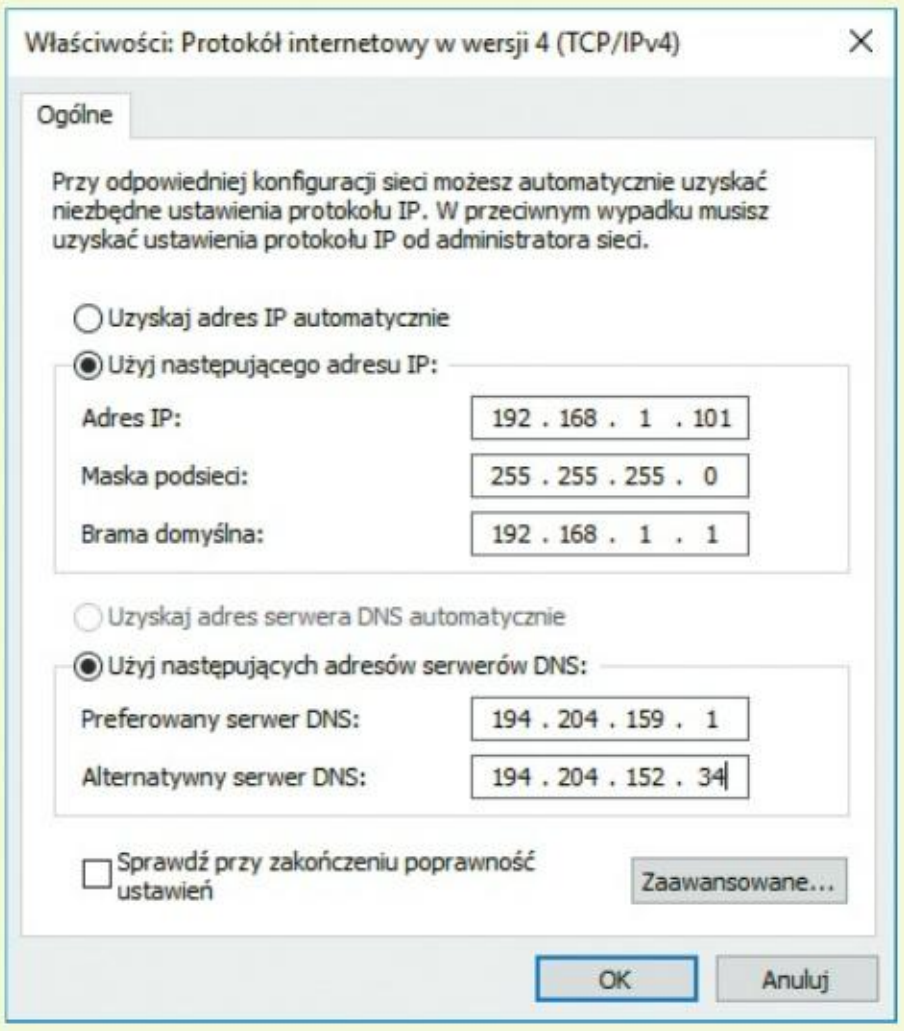
Konfigurowanie bezprzewodowej karty sieciowej

W tym przykładzie zostanie skonfigurowana bezprzewodowa karta sieciowa w systemie Windows 10. Inne systemy, np. Linux i starsze wersje systemu Windows, są wyposażone w inne narzędzia służące do konfigurowania sieci bezprzewodowych. Jeżeli korzystasz z innego systemu niż Windows 10, zapytaj nauczyciela, jak skonfigurować sieć bezprzewodową w takim systemie.

Jeżeli dane konfiguracyjne mają być przypisane do karty w sposób statyczny, należy wykonać następujące czynności:

1. Zainstalować kartę i niezbędne sterowniki lub upewnić się, że zostały one poprawnie zainstalowane.
2. W panelu sterowania wybrać **`Sieć i Internet`**, a następnie – **`Centrum sieci i udostępniania`**.
3. W oknie **`Centrum sieci i udostępniania`** wybrać polecenie **`Zmień ustawienia karty sieciowej`**.
4. W oknie **`Połączenia sieciowe`** kliknąć prawym klawiszem myszy ikonę symbolizującą konfigurowaną kartę i wybrać polecenie **`Właściwości`**.
5. Z rozwijanej listy wybrać **`Protokół internetowy w wersji 4 (TCP/IPv4)`** i kliknąć przycisk **`Właściwości`**.

6. W odpowiednie pola (rys. 51.1) wprowadzić dane konfiguracyjne:
   - adres IP;
   - maskę podsieci;
   - bramę domyślną;
   - adresy serwerów DNS (preferowanego i alternatywnego).
7. Kliknąć przycisk **OK**.
8. Upewnić się za pomocą polecenia **`ipconfig /all`**, że dane konfiguracyjne zostały wprowadzone poprawnie.



Rys. 51.1. Konfigurowanie protokołu IP dla karty bezprzewodowej

Sieć w trybie ad hoc charakteryzuje się zdecentralizowaną strukturą, w której przyłączone urządzenia mogą pełnić funkcje zarówno klientów, jak i serwerów. Do przekazywania danych nie jest wymagana żadna infrastruktura sieciowa, ponieważ pakiety są dostarczane bezpośrednio do odbiorcy. Sieci tego typu buduje się zazwyczaj na krótko i później się je demontuje. Wykorzystuje się je np. do połączenia laptopa ze smartfonem lub tabletem.

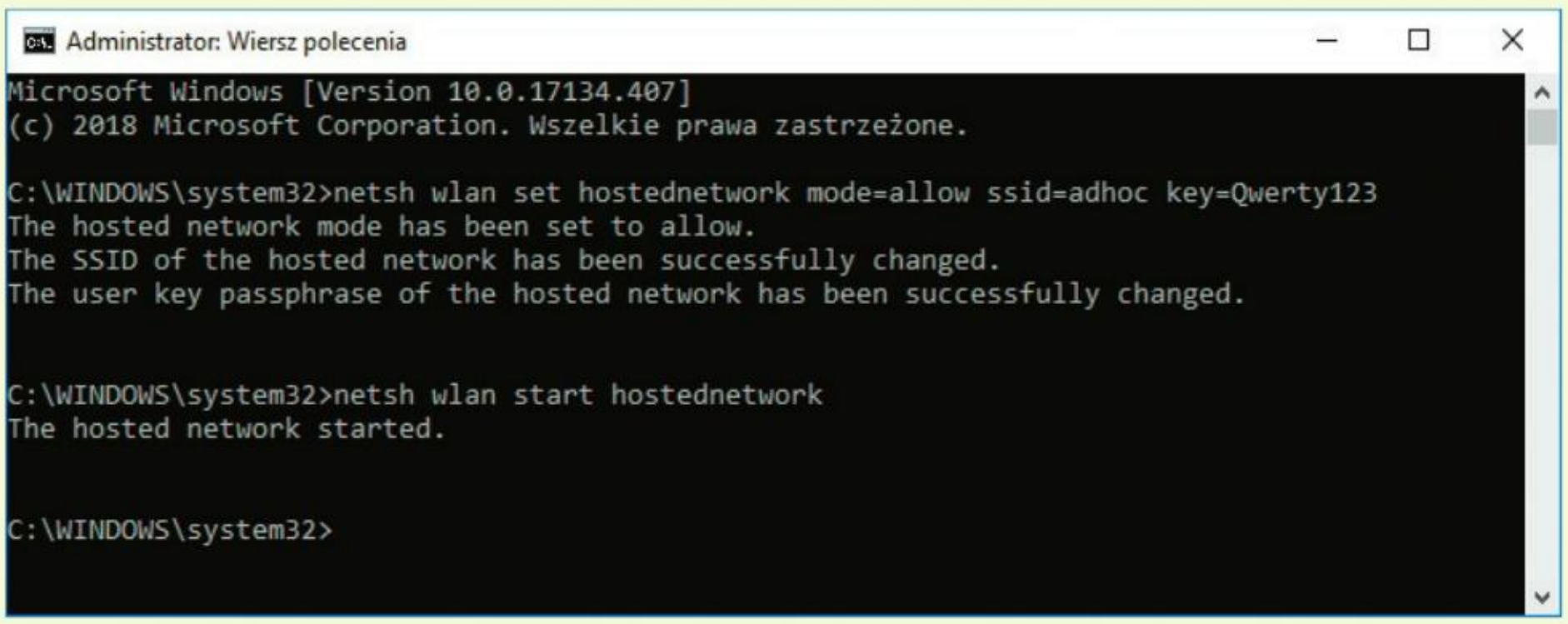
PRZYKŁAD 51.2

Konfigurowanie sieci ad hoc

W tym przykładzie zostanie skonfigurowana sieć ad hoc w systemie Windows 10. Komputer musi mieć również poprawnie skonfigurowane połączenie realizowane za pomocą przewodowej karty sieciowej. Połączenie zostanie udostępnione, dzięki czemu komputer będzie działał jako punkt dostępowy, za którego pośrednictwem inne urządzenia, takie jak smartfony, tablety, będą mogły uzyskać połączenie z internetem. Linux i starsze wersje systemu Windows są wyposażone w inne narzędzia służące do konfigurowania sieci bezprzewodowych. Dlatego jeżeli korzystasz z innego systemu niż Windows 10, zapytaj nauczyciela, jak skonfigurować w nim sieć bezprzewodową.
Sieci ad hoc najczęściej są budowane jako rozwiązania tymczasowe, wykorzystywane do przesyłania plików między dwoma urządzeniami. Ze względu na tymczasowość sieci na ogół tworzy się sieci niezabezpieczone przed dostępem osób nieuprawnionych

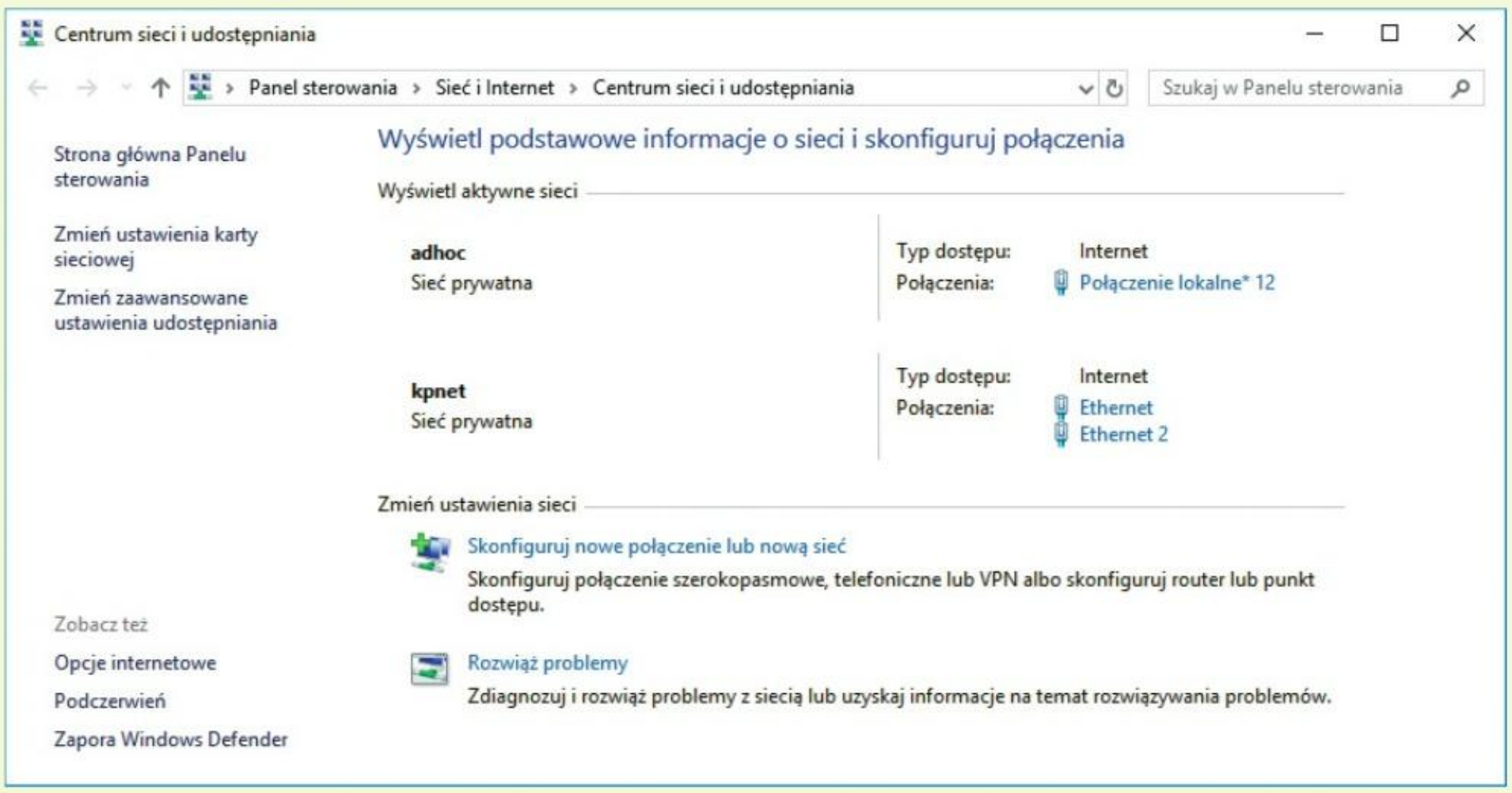
(takie sieci można również zabezpieczyć przed niepożądanym dostępem). W tym ćwiczeniu zostanie zbudowana niezabezpieczona sieć w trybie ad hoc. Należy jednak pamiętać, że to rozwiązanie nie zapewnia bezpieczeństwa i może być stosowane tylko w wyjątkowych przypadkach, gdy przesyłane dane nie wymagają ochrony.
Aby skonfigurować sieć, należy:

1. Uruchomić konsolę z prawami administratora.
2. Wykonać polecenie **`netsh wlan set hostednetwork mode=allow ssid=adhoc key=Qwerty123`**. W rezultacie utworzy się sieć z identyfikatorem SSID **`adhoc`** i hasłem **`Qwerty123`**.
3. Włączyć sieć poleceniem **`netsh wlan start hostednetwork`** (rys. 51.2).



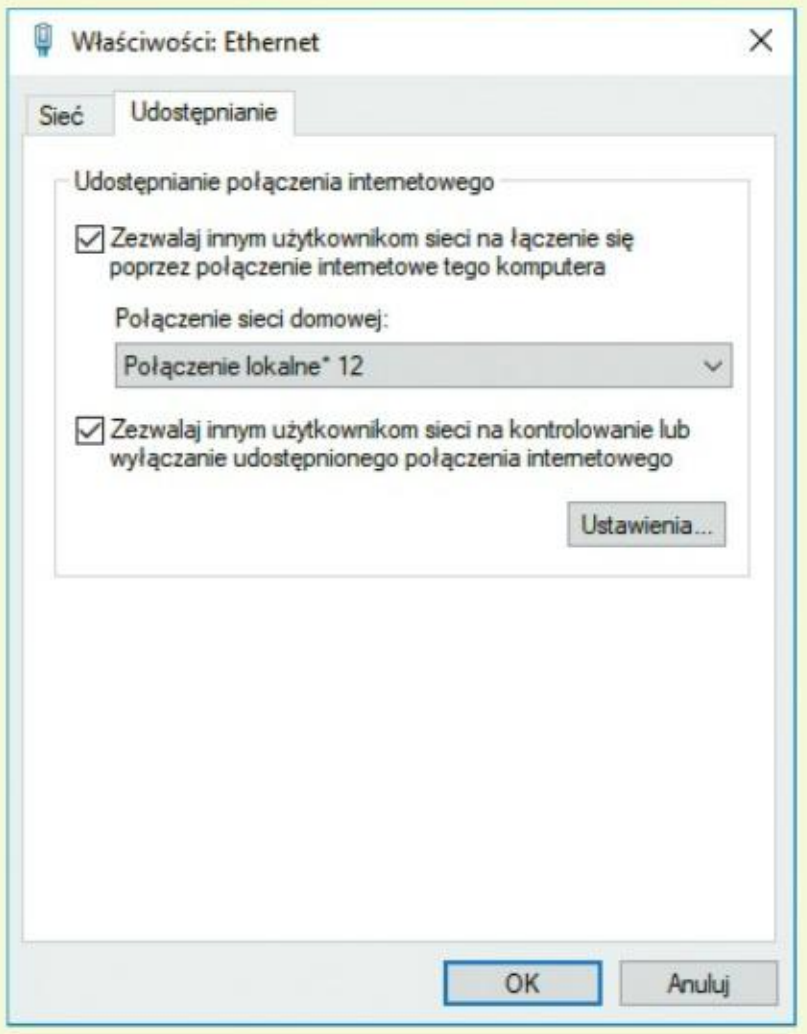
Rys. 51.2. **Tworzenie i włączenie sieci ad hoc**

4. Sprawdzić w oknie **`Centrum sieci i udostępniania`**, czy zostało utworzone nowe połączenie sieciowe (rys. 51.3).



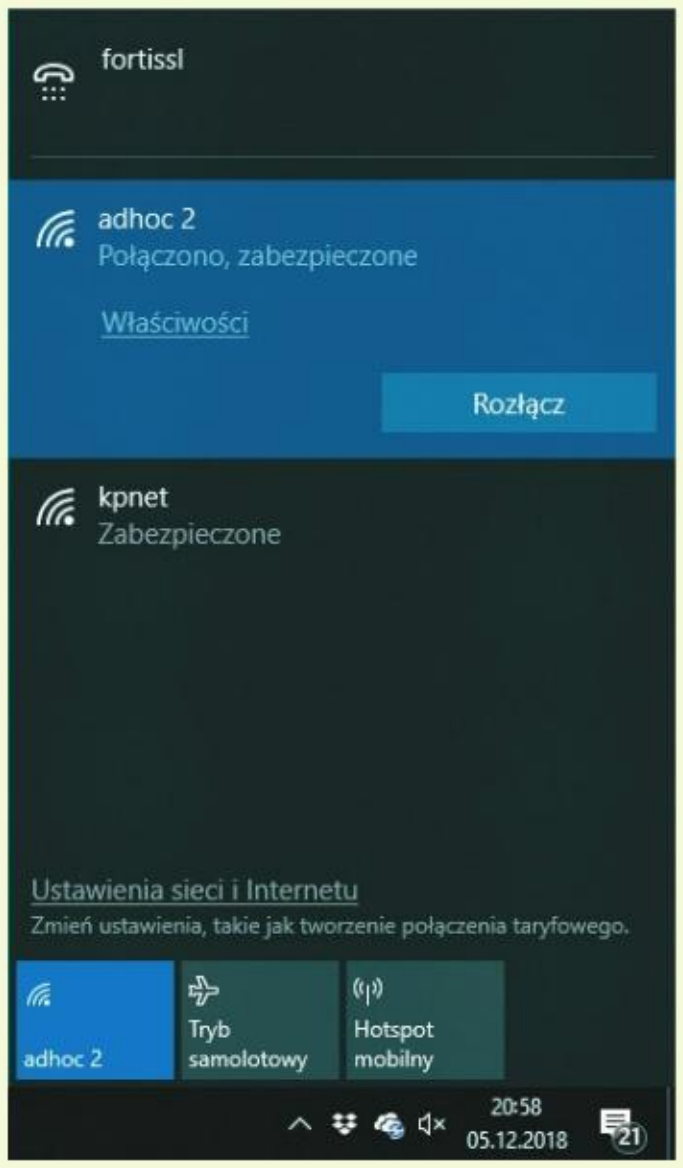
Rys. 51.3. **Weryfikacja sieci ad hoc**

5. W oknie **Połączenia sieciowe** kliknąć prawym przyciskiem myszy ikonę połączenia sieciowego karty przewodowej i wybrać **Właściwości**.
6. Wybrać zakładkę **Udostępnianie**, zaznaczyć opcję **Zezwalaj innym użytkownikom sieci na łączenie się poprzez połączenie internetowe tego komputera**.
7. Z rozwijanej listy wybrać połączenie sieci **ad hoc** i kliknąć przycisk **OK** (rys. 51.4).



Rys. 51.4. **Udostępnianie połączenia przewodowego dla użytkowników sieci ad hoc**

8. Za pomocą innego urządzenia, np. laptopa, połączyć się z siecią ad hoc i sprawdzić możliwość komunikacji z internetem (rys. 51.5).



Rys. 51.5. **Okno dostępnych sieci bezprzewodowych**

Sieci bezprzewodowe są narażone na podsłuch danych w znacznie większym stopniu niż sieci kablowe. Przyczyna tkwi w tym, że fale elektromagnetyczne rozchodzą się w całej przestrzeni, a każdy, kto znajdzie się w ich zasięgu, może je odbierać (pod warunkiem że ma odpowiednie urządzenia). Aby zabezpieczyć sieć przed dostępem osób nieuprawnionych, należy zastosować następujące procedury:

1. **Zmienić domyślny login i hasło punktu dostępowego** – wszystkie inne zabezpieczenia będą nieskuteczne, jeśli każdy będzie mógł zalogować się na routerze lub punkcie dostępowym i przejąć nad nim kontrolę. Listę domyślnych haseł można znaleźć w internecie.
2. **Umożliwić zarządzanie tylko przez kabel** – wyłączenie możliwości logowania się do punktu dostępowego przez sieć bezprzewodową przekłada się na ograniczony dostęp do zarządzania urządzeniem tylko dla użytkowników podłączonych kablem.
3. **Ograniczyć moc nadawania** – pozwoli to na ograniczenie zasięgu sieci tylko do niezbędnego obszaru, np. mieszkania, a sieć będzie niedostępna dla sąsiadów znajdujących się poza zasięgiem.
4. **Dobrać umiejscowienie punktu dostępowego** – punkt dostępowy można w miarę możliwości instalować w środku mieszkania i ograniczyć moc nadawania tak, aby jego zasięg obejmował jedynie mieszkanie. Innym możliwym rozwiązaniem jest zastosowanie specjalnych anten sektorowych o ograniczonym obszarze pokrycia terenu.
5. **Wyłączyć rozgłaszanie identyfikatora sieci** – każda sieć bezprzewodowa ma unikatowy identyfikator **SSID** (ang. *Service Set Identifier*). Identyfikator SSID jest wysyłany przez każde urządzenie, np. punkt dostępowy. Na podstawie tej nazwy urządzenia wykrywają sieci w swoim otoczeniu i mogą rozpocząć procedurę przyłączenia do sieci. Punkty dostępowe i routery standardowo używają jako identyfikatora swojej nazwy, np. linksys. Dobrą praktyką jest zmiana nazwy identyfikatora na inną – jeżeli potencjalny włamywacz wie, jaki jest typ punktu dostępowego, to ma ułatwione zadanie. Można również wyłączyć wysyłanie identyfikatora SSID – sieć stanie się niewidoczna dla typowych narzędzi. Przyłączyć się do sieci będą mogli tylko ci użytkownicy, którzy znają SSID. To zabezpieczenie jest niewystarczające, gdyż istnieje wiele specjalistycznych programów, które mogą odczytać SSID, nawet jeżeli jego wysyłanie jest wyłączone.
6. **Włączyć filtrowanie adresów MAC** – każda karta bezprzewodowa ma unikatowy adres fizyczny MAC. Na jego podstawie punkt dostępowy może rozpoznać, czy jest to legalny użytkownik sieci, czy – intruz. Punkt dostępowy może mieć zdefiniowaną listę adresów MAC urządzeń, które powinny uzyskać dostęp do sieci (**biała lista**), oraz urządzeń, którym należy zabronić dostępu (**czarna lista**). Niestety, metoda filtrowania adresów MAC w obecnych czasach nie spełnia swojego zadania, ponieważ włamywacz bardzo łatwo może obejść to zabezpieczenie przez zamianę adresu MAC. Mimo wszystko warto stosować ten sposób.
7. **Włączyć szyfrowanie danych** – brak szyfrowania sprawia, że nasze dane (loginy, hasła, numery kart) są przesyłane w sieci w sposób umożliwiający ich łatwe przechwycenie i odczytanie przez osoby trzecie.

Spośród wymienionych metod zwiększenia bezpieczeństwa sieci bezprzewodowych największe znaczenie praktyczne ma szyfrowanie danych. Obecnie szyfrowanie uznaje się za jedyną skuteczną metodę ochrony sieci bezprzewodowej. W sieciach bezprzewodowych można spotkać następujące standardy zabezpieczenia danych:

- **WEP** (ang. *Wired Equivalent Privacy*) – do ochrony danych w tym standardzie wykorzystuje się algorytm RC4, który jest symetrycznym szyfrem strumieniowym z kluczem poufnym. Podczas szyfrowania metodą RC4 zostaje wykonana operacja różnicy symetrycznej XOR na bitach klucza i danych, której efektem jest szyfrogram. W celu odkodowania wiadomości

odbiorca musi użyć tego samego klucza, który został wykorzystany do zaszyfrowania wiadomości. W WEP stosuje się klucze o długości 64 bitów lub 128 bitów (klucz składa się z 40 bitów lub 104 bitów klucza i z tzw. wektora inicjalizującego o długości 24 bitów). W standardzie WEP oferuje się klucze poufne o długości 40 bitów, ponieważ w momencie opracowywania standardu prawo Stanów Zjednoczonych nie pozwalało na wykorzystywanie klucza dłuższego niż 40 bitów. Obecnie metoda WEP jest uznawana za niewystarczającą i powinna być stosowana tylko wtedy, gdy urządzenia nie obsługują standardu WPA;

- **WPA** (ang. *Wi-Fi Protected Access*) – wykorzystuje protokoły **TKIP** (ang. *Temporal Key Integrity Protocol*) i uwierzytelnienie **EAP** (ang. *Extensible Authentication Protocol*). Został wprowadzony jako standard przejściowy między WEP a WPA2. Zwiększenie bezpieczeństwa użytkowników sprzętu następuje bez konieczności wymiany sprzętu – wystarczy zmienić sterownik w karcie sieciowej lub firmware w punktach dostępowych. WPA może korzystać z trybu:
  - **Enterprise** – używa serwera RADIUS, który odpowiada za proces uwierzytelniania użytkowników;
  - **Personal** – wszystkie podłączone stacje wykorzystują jeden klucz dzielony, przypisywany ręcznie przez administratora (ang. *Pre-Shared Key*, PSK);
- **WPA2** – zawiera poprawki eliminujące wszystkie znalezione luki w zabezpieczeniach WEP i WPA. W porównaniu z WPA, wykorzystuje dynamiczne klucze o długości 128 bitów i automatycznie je dystrybuuje. Wykorzystuje algorytm szyfrowania AES. Jest zalecany do stosowania w sieciach bezprzewodowych. Podobnie jak WPA, oferuje tryby Enterprise i Personal;
- **WPA3** – w stosunku do WPA2 wymaga silniejszych algorytmów szyfrowania. Zwiększono również bezpieczeństwo wymiany kluczy.

Konfiguracja sieci bezprzewodowej pracującej w trybie infrastruktury składa się z dwóch kroków: z konfiguracji punktu dostępowego i z konfiguracji klienta sieci.

PRZYKŁAD 51.3

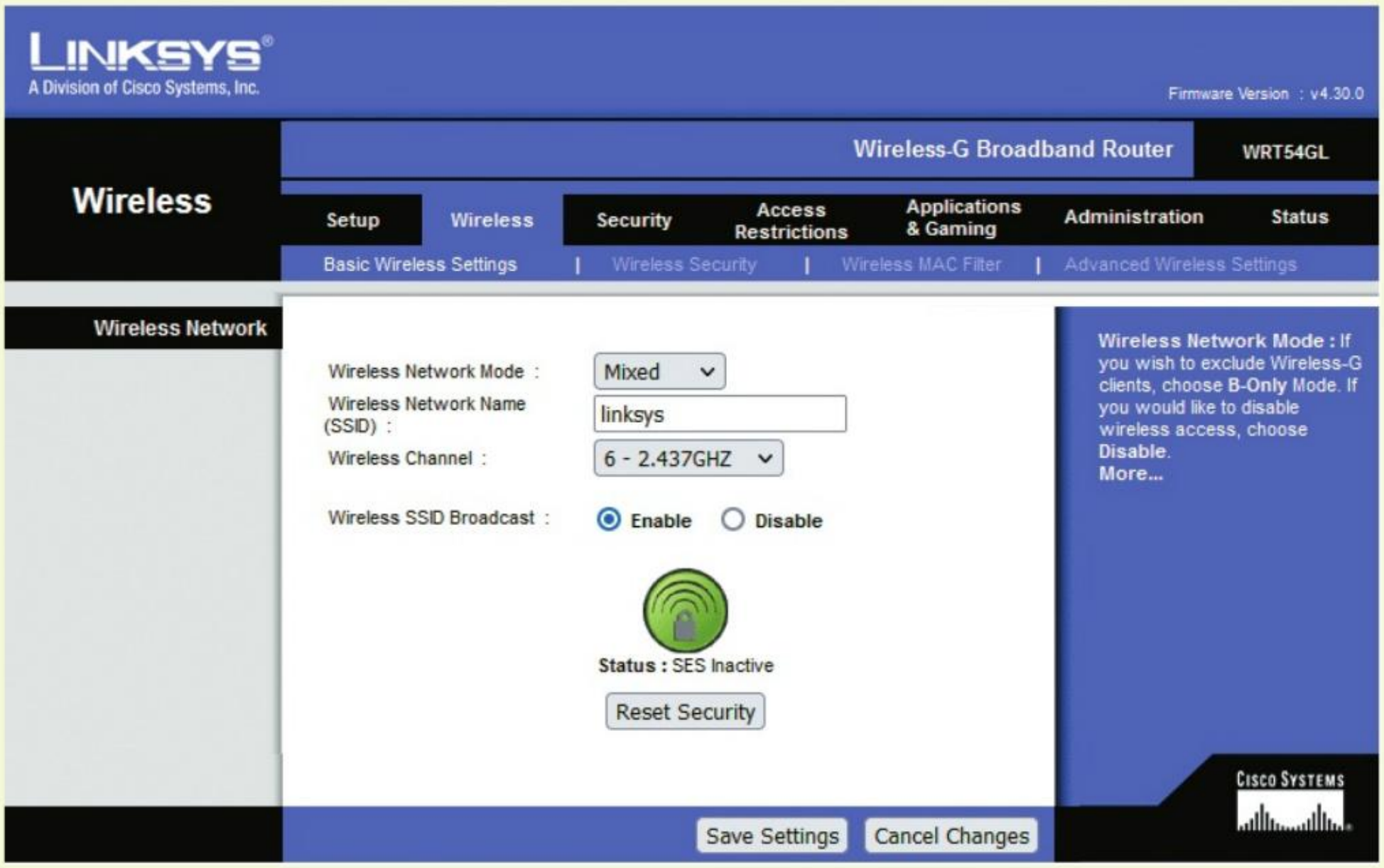
Konfigurowanie punktu dostępowego w routerze

W tym ćwiczeniu zostanie skonfigurowana bezprzewodowa sieć z włączonymi zabezpieczeniami na przykładzie routera Linksys WRT54GL. Konfigurację pokażemy na przykładzie routera z wbudowanym punktem dostępowym. Przed przystąpieniem do konfiguracji należy sprawdzić, jakie sieci bezprzewodowe działają na danym obszarze i jakie kanały są wykorzystywane. Aby kanały nie zakłócały się wzajemnie (zakresy częstotliwości kanałów częściowo zachodzą na siebie), odległości między wykorzystywanymi kanałami powinny wynosić co najmniej 6. Aby skonfigurować punkt dostępowy, należy wykonać następujące czynności:

1. Połączyć kablem kartę sieciową komputera z interfejsem sieciowym punktu dostępowego lub z interfejsem LAN w przypadku routera z wbudowanym punktem dostępowym.
2. Skonfigurować kartę sieciową komputera i interfejs punktu dostępowego albo routera do pracy w tej samej sieci (informacje o standardowej konfiguracji punktu dostępowego albo routera można znaleźć w dokumentacji). Jeżeli hasło konta administratora nie jest znane, to można przywrócić urządzenie do stanu fabrycznego – w tym celu należy nacisnąć i przytrzymać przez 30 s przycisk **`Reset`**. Operacja usunie wszystkie ustawienia konfiguracyjne wprowadzone przez użytkownika.
3. W komputerze w oknie przeglądarki internetowej wpisać adres urządzenia, np. **`192.168.1.1`**, a w wyskakującym okienku podać nazwę konta administratora i hasło.

4. W zakładce **Wireless** wskazać **Basic Wireless Settings**, a następnie z listy rozwijanej wybrać tryb pracy (ang. *wireless network mode*). Dostępne tryby pracy to: tylko B (ang. *B-only*), tylko G (ang. *G-only*), mieszany, czyli wykorzystujący jednocześnie B i G (ang. *mixed*), oraz wyłączony (ang. *disabled*). W pozostałych polach należy wpisać: identyfikator SSID w polu **Wireless Network Name** oraz numer kanału w polu **Wireless Channel**.
5. Za pomocą przycisku radiowego **Wireless SSID Broadcast** można włączyć (ang. *enable*) lub wyłączyć (ang. *disable*) rozgłaszanie identyfikatora SSID.
6. Kliknąć przycisk **Save Settings**.

Na rys. 51.6 przedstawiono sposób konfiguracji punktu dostępowego.



Rys. 51.6. **Okno konfiguracji sieci bezprzewodowej w punkcie dostępowym**

PRZYKŁAD 51.4

Konfigurowanie szyfrowania sieci bezprzewodowej

Aby włączyć szyfrowanie danych przesyłanych w sieci bezprzewodowej, należy wykonać następujące czynności:

1. Połączyć kablem kartę sieciową komputera z interfejsem sieciowym urządzenia, a następnie za pomocą przeglądarki internetowej zalogować się na konto administratora.
2. W zakładce **Wireless** wybrać **Wireless Security**, a potem z listy rozwijanej wybrać tryb szyfrowania, np. **WPA2 Personal**.
3. W polach okna konfiguracji wprowadzić: nazwę wybranego algorytmu szyfrowania, np. **AES** w polu **WPA Algorithms** oraz hasło umożliwiające uzyskanie dostępu do sieci w polu **WPA Shared Key**. Natomiast pole **Group Key Renewal** określa

częstotliwość zmian grupy kluczy – można pozostawić wartość domyślną 3600. Okno konfiguracji szyfrowania przedstawiono na rys. 51.7.

4. Kliknąć przycisk **Save Settings**.



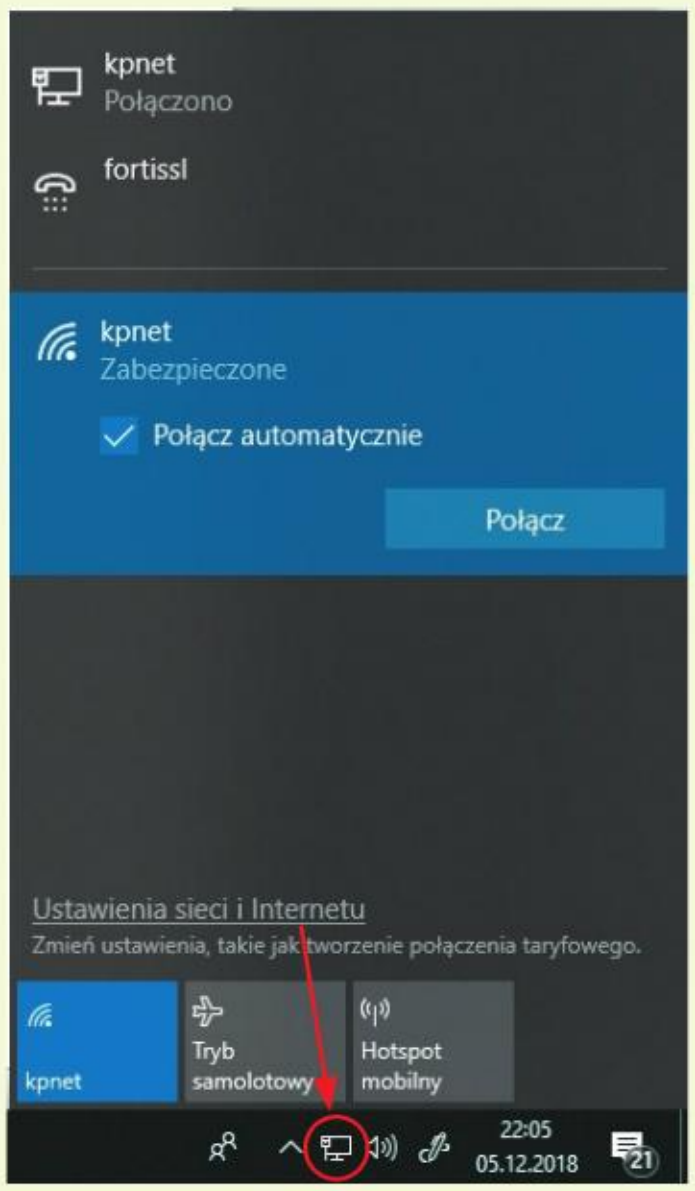
Rys. 51.7. **Okno konfiguracji szyfrowania sieci bezprzewodowej**

PRZYKŁAD 51.5

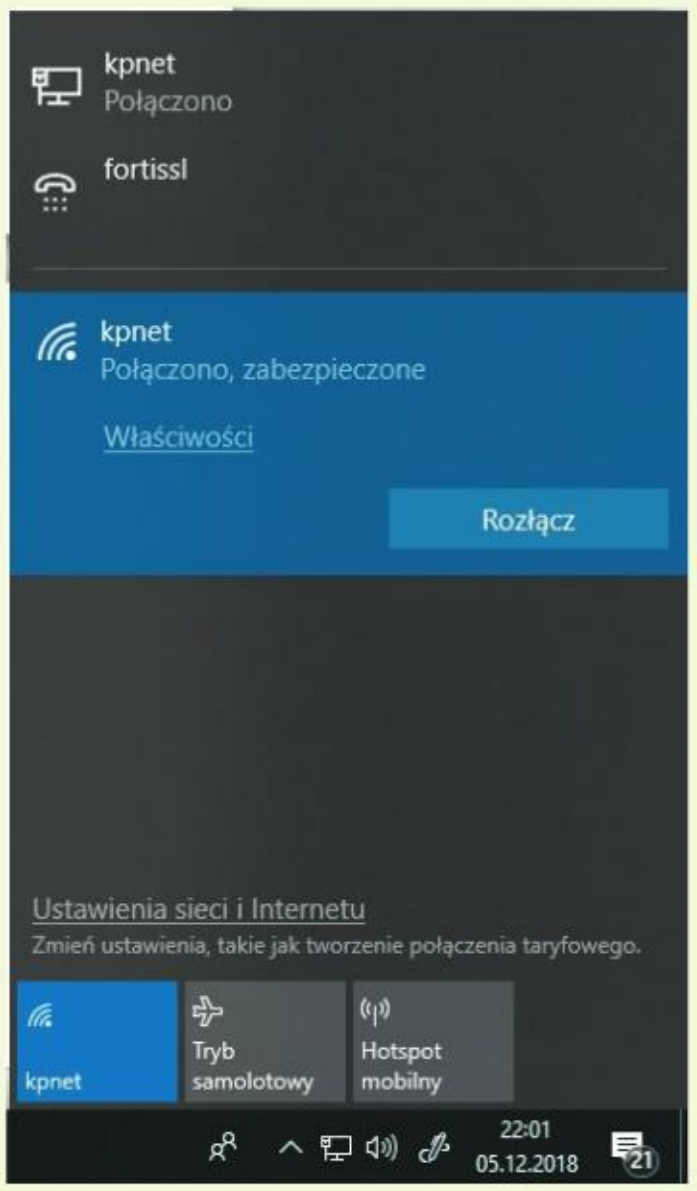
Konfigurowanie klienta sieci bezprzewodowej

W tym przykładzie zostanie wykonana konfiguracja klienta sieci bezprzewodowej w systemie Windows 10. W pozostałych systemach procedura przebiega podobnie, lecz może się różnić drobnymi szczegółami. W przykładzie przyjęto założenie, że rozgłaszanie identyfikatora SSID w punkcie dostępowym jest włączone (takie rozwiązanie sprawia, że wykrycie sieci przez klienta staje się łatwiejsze, ale bezpieczeństwo sieci się obniża). Aby przyłączyć klienta do sieci bezprzewodowej, należy wykonać następujące czynności:

1. W prawym dolnym rogu ekranu kliknąć ikonę sieci komputerowej (na rys. 51.8 zaznaczona strzałką).
2. W oknie dostępnych połączeń kliknąć wybraną sieć, zaznaczyć opcję **Połącz automatycznie**, a następnie kliknąć przycisk **Połącz**.
3. W oknie wprowadzić hasło dostępu do sieci zdefiniowane podczas konfiguracji punktu dostępowego.
4. Rozwinąć ponownie okno **Dostępne połączenia**, aby sprawdzić, czy istnieje połączenie z siecią (rys. 51.9).



Rys. 51.8. **Otwieranie okna z listą dostępnych sieci bezprzewodowych**



Rys. 51.9. **Weryfikacja dostępnych sieci bezprzewodowych**

51.1. Uwierzytelnianie klientów Wi-Fi za pomocą serwera RADIUS

Protokół **RADIUS** (ang. *Remote Authentication Dial in User Service*) został przygotowany i wdrożony przez firmę Livingstone Enterprises. Jest on wykorzystywany jako protokół uwierzytelniania i autoryzacji. **Uwierzytelnianie** (ang. *authentication*) to proces polegający na potwierdzeniu zadeklarowanej tożsamości podmiotu biorącego udział w procesie komunikacji. Podczas **autoryzacji** (ang. *authorization*) podmiotowi są nadawane uprawnienia do danych. Zaletą stosowania uwierzytelniania z wykorzystaniem serwera RADIUS jest jego uniwersalność – RADIUS może zabezpieczać zarówno małe sieci, które składają się tylko z kilku użytkowników, jak i sieci miejskie, zarządzane przez firmy, które oferują usługi z dostępem do sieci. Protokół RADIUS jest protokołem działającym w architekturze klient–serwer.

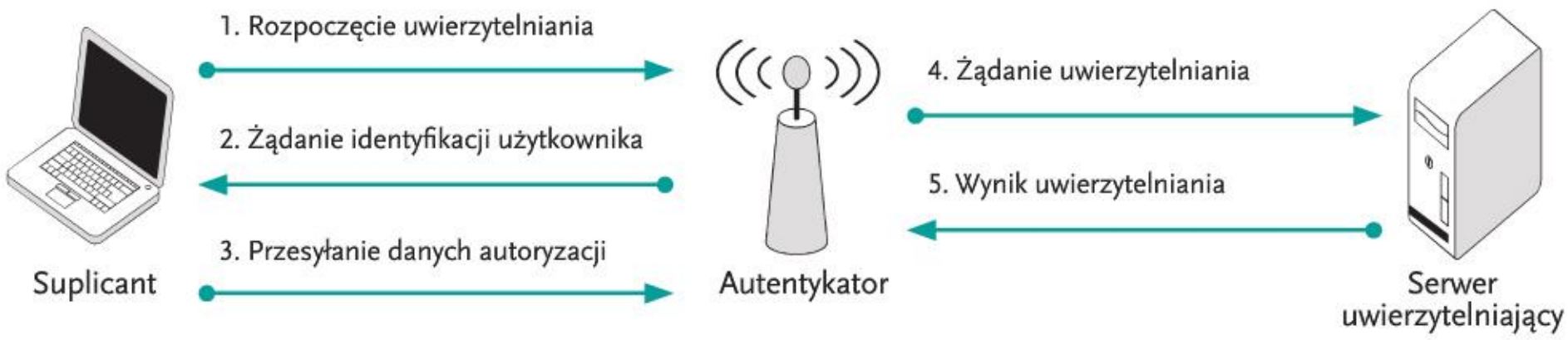
W okresie początkowym serwer RADIUS wykorzystywał porty UDP 1645 (do uwierzytelniania) i UDP 1646 (do autoryzacji). Później RADIUS otrzymał nowe porty 1812 i 1813, jednak starsze numery portów w dalszym ciągu mogą być używane.

Jeżeli **użytkownik sieci Wi-Fi** (**suplikant**) podejmie próbę zalogowania do sieci, to **serwer dostępowy NAS** (**autentykator**) generuje zapytanie o dane użytkownika, w tym – o jego identyfikator i hasło. Punkt dostępowy w tym wypadku odgrywa rolę **klienta RADIUS**. Po otrzymaniu tych danych od użytkownika wysyła jego identyfikator wraz z zakodowanym hasłem do **serwera uwierzytelniającego** (serwera RADIUS), na którym zostaje uruchomione specjalne oprogramowanie. Po sprawdzeniu danych użytkownika we własnej bazie danych serwer RADIUS może odpowiedzieć jednym z następujących komunikatów:

- **ACCEPT** – oznacza sukces uwierzytelniania;
- **REJECT** – użytkownik nie został poprawnie uwierzytelniony, dostęp do zasobów sieci jest zabroniony;

- **CHALLENGE** – prośba o wprowadzenie dodatkowych danych uwierzytelniających.

Schemat komunikacji przedstawiono na rys. 51.10.



Rys. 51.10. Komunikacja podczas uwierzytelniania RADIUS

Komunikacja podczas logowania do sieci Wi-Fi z wykorzystaniem serwera RADIUS przebiega według schematu:

1. Użytkownik (suplikant) wysyła do punktu dostępowego (klient RADIUS) komunikat o próbie nawiązania połączenia.
2. Punkt dostępowy żąda identyfikacji użytkownika.
3. Użytkownik wysyła swój identyfikator i dane niezbędne do autentykacji do punktu dostępowego.
4. Punkt dostępowy przesyła dane otrzymane od użytkownika do serwera RADIUS.
5. Serwer RADIUS przesyła do punktu dostępowego zgodę na przeprowadzenie autentykacji (ang. *ACCEPT*) lub odmowę (ang. *REJECT*).

PRZYKŁAD 51.6

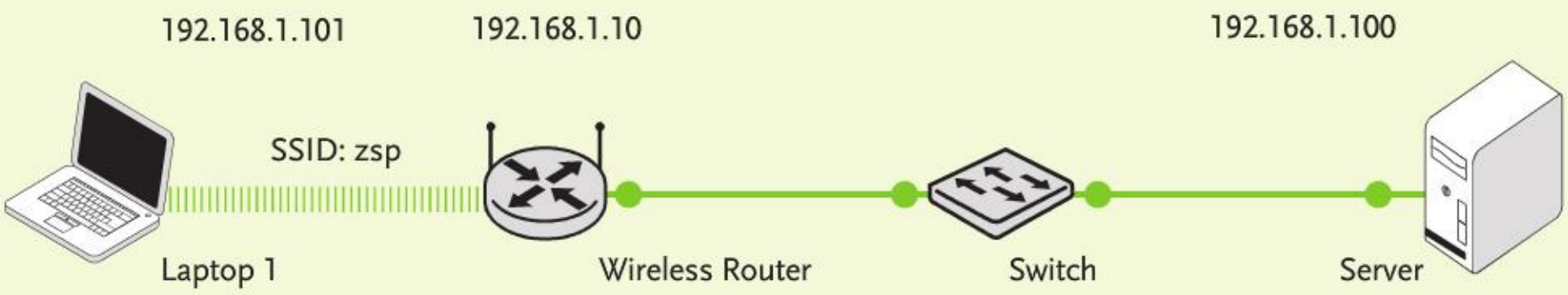
Konfigurowanie uwierzytelniania klientów Wi-Fi za pomocą serwera RADIUS

Konfigurowanie uwierzytelniania klientów Wi-Fi za pomocą serwera RADIUS obejmuje czynności wykonywane na stacji roboczej (laptopie), punkcie dostępowym i serwerze. W tym przykładzie zostanie wykorzystany symulator sieci Cisco Packet Tracer. Aby skonfigurować klienta do sieci bezprzewodowej, należy wykonać następujące czynności:

1. Uruchomić **`Cisco Packet Tracer`**.
2. Zbudować sieć złożoną z: laptopa wyposażonego w kartę Wi-Fi, routera (WRT300N) z wbudowanym punktem dostępowym, przełącznika i serwera (rys. 51.11).

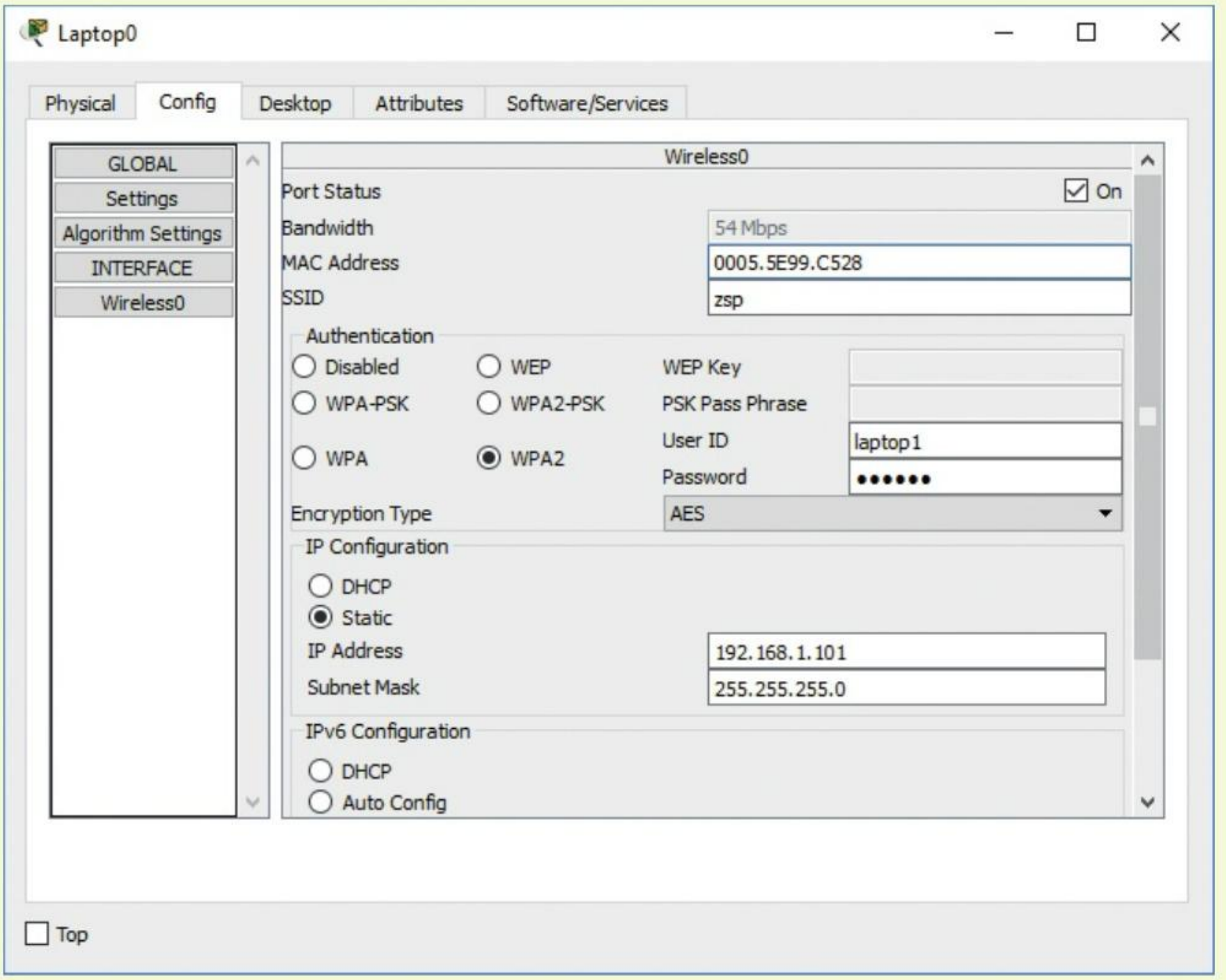
UWAGA

Port przełącznika trzeba połączyć z portem LAN routera.



Rys. 51.11. Schemat sieci z uwierzytelnianiem RADIUS

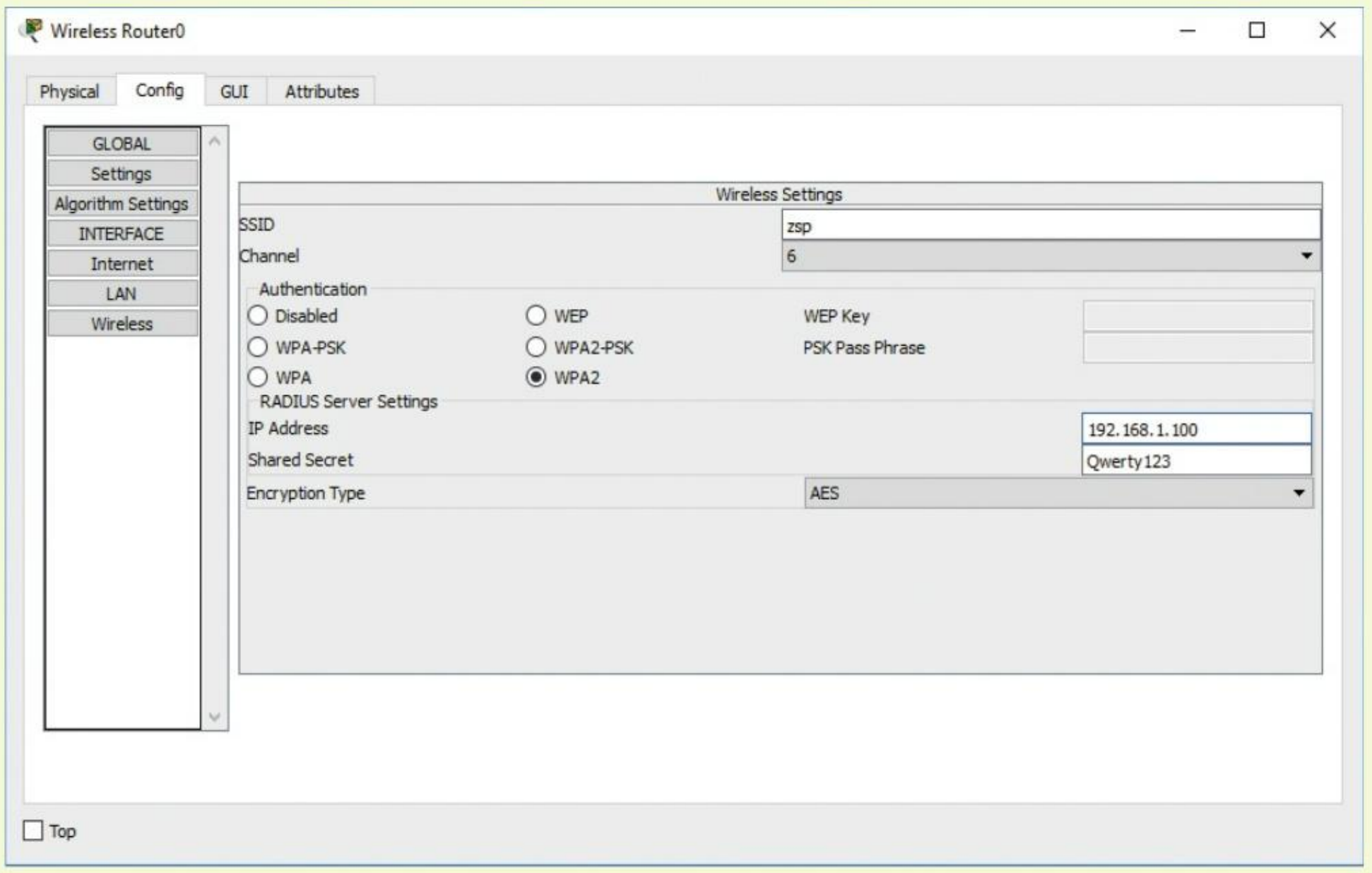
3. Ustawić w laptopie konfigurację IP:
   - adres IP: **192.168.1.101** i maskę podsieci **255.255.255.0**;
   - adres bramy: **192.168.1.1**.
4. Skonfigurować sieć Wi-Fi w laptopie, jak na rys. 51.12:
   - SSID: **zsp**;
   - autentykacja: **WPA2**;
   - User ID: **laptop1**;
   - Password: **Qwerty**;
   - Encryption Type: **AES**.



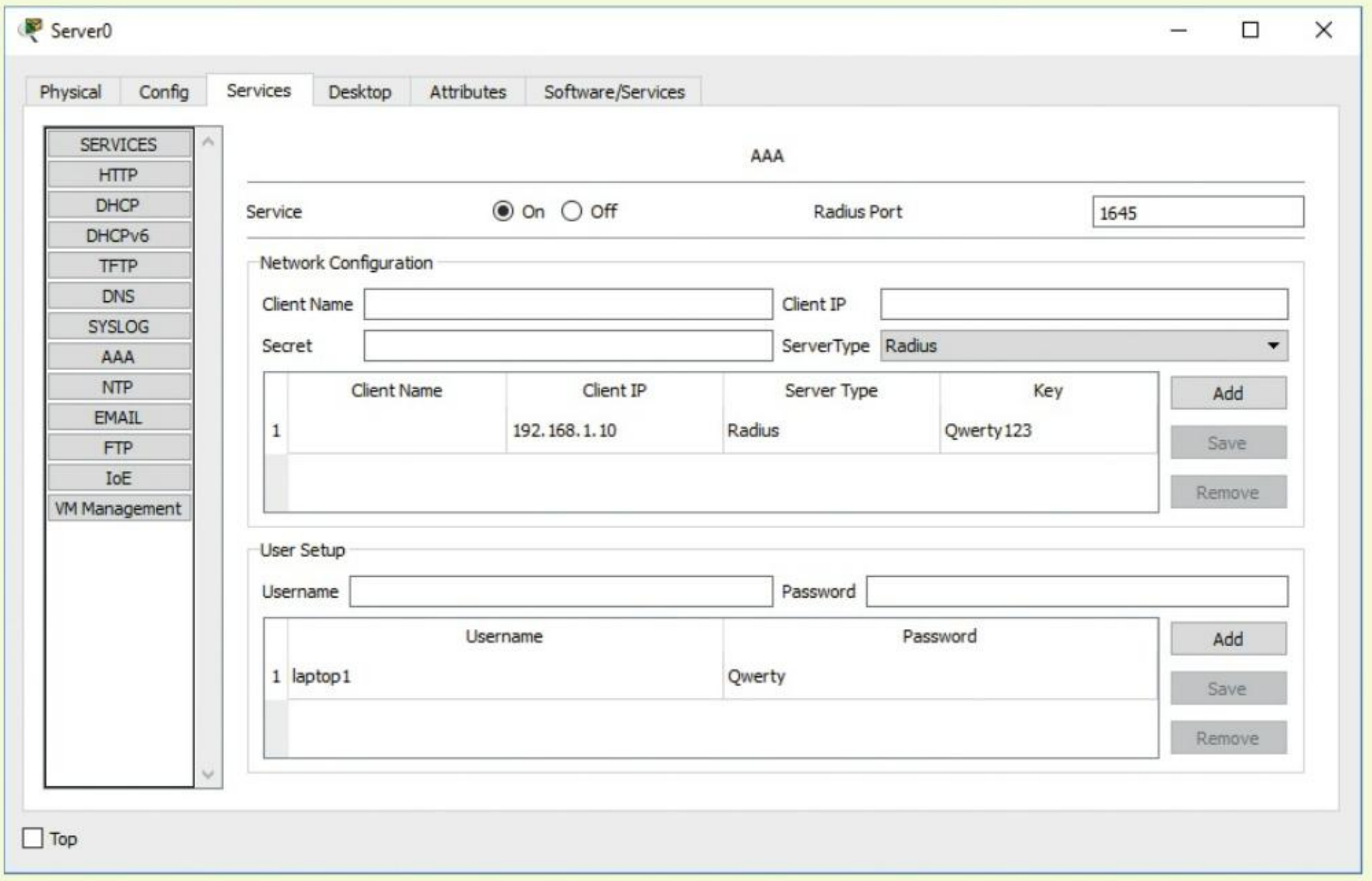
Rys. 51.12. **Konfiguracja sieci Wi-Fi w laptopie**

5. Ustawić w interfejsie LAN routera konfigurację IP:
   - adres IP: **192.168.1.10** i maskę podsieci **255.255.255.0**.
6. Skonfigurować sieć Wi-Fi w routerze, jak na rys. 51.13:
   - SSID: **zsp**;
   - Channel: **6**;
   - autentykacja: **WPA2**;
   - IP Address (w sekcji RADIUS Server Settings): **192.168.1.100**;
   - Shared Secret (w sekcji RADIUS Server Settings): **Qwerty123**;
   - Encryption Type: **AES**.

7. Ustawić w interfejsie serwera konfigurację IP:
   - adres IP: **192.168.1.100** i maskę podsieci **255.255.255.0**;
   - adres bramy: **192.168.1.1**.
8. Skonfigurować usługę autoryzacji w serwerze, jak na rys. 51.14. W tym celu należy wybrać zakładkę **Services/AAA**:
   - w sekcji **Service** – włączyć usługę **On**;
   - w sekcji **Network Configuration** wprowadzić informacje o kliencie RADIUS. Wpisać adres IP routera (**192.168.1.10**) w pole **Client IP**, hasło (**Qwerty123**) w pole **Secret** i kliknąć przycisk **Add**. Sprawdzić, czy klient został dodany do listy klientów;
   - w sekcji **User Setup** wprowadzić informacje o użytkowniku. Wpisać nazwę użytkownika (**laptop1**) w pole **Username**, hasło (**Qwerty**) w pole **Password** i kliknąć przycisk **Add**. Sprawdzić, czy użytkownik został dodany do listy użytkowników.
9. Sprawdzić, czy laptop zostanie przyłączony do sieci Wi-Fi:
   - sprawdzić możliwość komunikacji między laptopem i serwerem, np. za pomocą polecenia **ping**, jak na rys. 51.15.

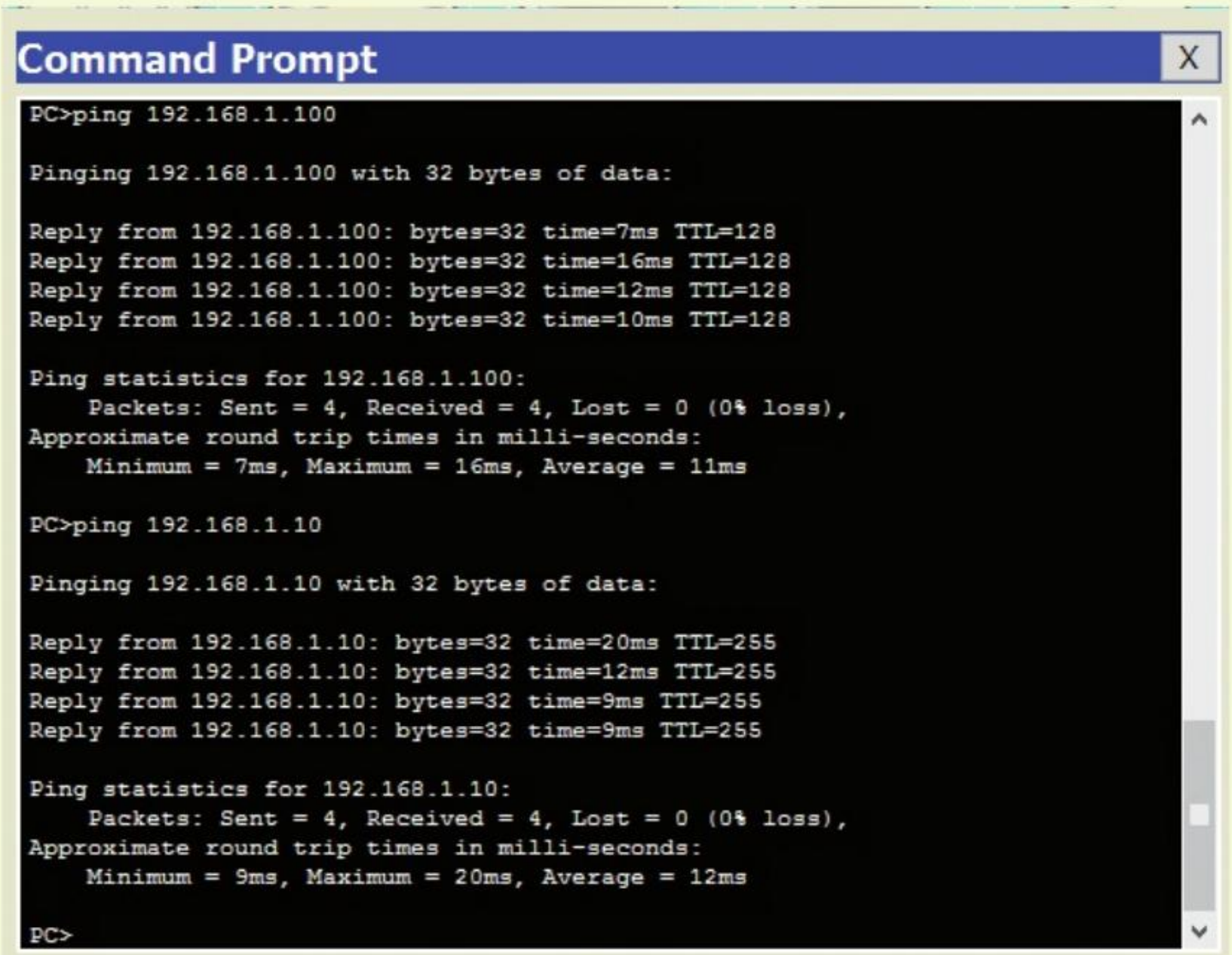


Rys. 51.13. **Konfiguracja sieci Wi-Fi w routerze**



Rys. 51.14. **Konfiguracja serwera RADIUS**

KODY



Rys. 51.15. **Testowanie łączności między laptopem a routerem i serwerem**

51.2. Sieci Wi-Fi zarządzane przez kontroler sieci

Bezprzewodowe sieci lokalne Wi-Fi zyskują coraz większą popularność zarówno w sieciach domowych, w małych firmach, jak i w zastosowaniach biznesowych. W małych sieciach Wi-Fi, tworzonych na potrzeby użytkowników domowych, stosuje się pojedyncze punkty dostępowe i standard szyfrowania typu WPA Personal, w którym klucz szyfrowania jest przypisywany ręcznie przez administratora. To rozwiązanie jest proste, ale mało skalowalne. W małych sieciach firmowych może być używanych wiele punktów dostępowych i protokół RADIUS do uwierzytelniania użytkowników, dzięki czemu administrowanie użytkownikami staje się łatwiejsze. Wymagania stawiane wdrożeniom Wi-Fi w dużych sieciach są odmienne od tych stawianych rozwiązaniom domowym lub w małych firmach, wykorzystujących kilka punktów dostępowych. Technologia komunikacji jest ta sama, ale rozwiązania dla dużych sieci wymagają dodatkowo:

- zapewnienia wydajnej obsługi bardzo wielu klientów jednocześnie;
- obsługi roamingu dla urządzeń mobilnych – możliwie w sposób niezauważalny dla użytkowników;
- zapewnienia bezpieczeństwa użytkowników i własnej infrastruktury (np. wykrywanie obcych punktów dostępowych);
- zapewnienia autoryzacji i rozliczania użytkowników;
- zapewnienia różnego poziomu dostępu dla użytkowników (np. dostęp dla uczniów może być ograniczony czasowo, dla gości – realizowany przy mniejszej prędkości, a dla pracowników – nieograniczony);
- optymalizacji liczby punktów dostępowych oraz ich mocy nadawania;
- centralizacji zarządzania punktami dostępowymi;
- pracy w trudnych warunkach fizycznych (np. na zewnątrz budynków).

W dużych sieciach Wi-Fi za zarządzanie i za udostępnianie sieci są odpowiedzialne specjalne urządzenia – **kontrolery sieci**, współpracujące z punktami dostępowymi. Punkty dostępowe zapewniają łączność Wi-Fi dla klientów w swoim otoczeniu, natomiast kontroler służy do zarządzania siecią i punktami dostępowymi oraz do realizacji funkcji bezpieczeństwa, do autoryzacji użytkowników, do realizacji roamingu itp.

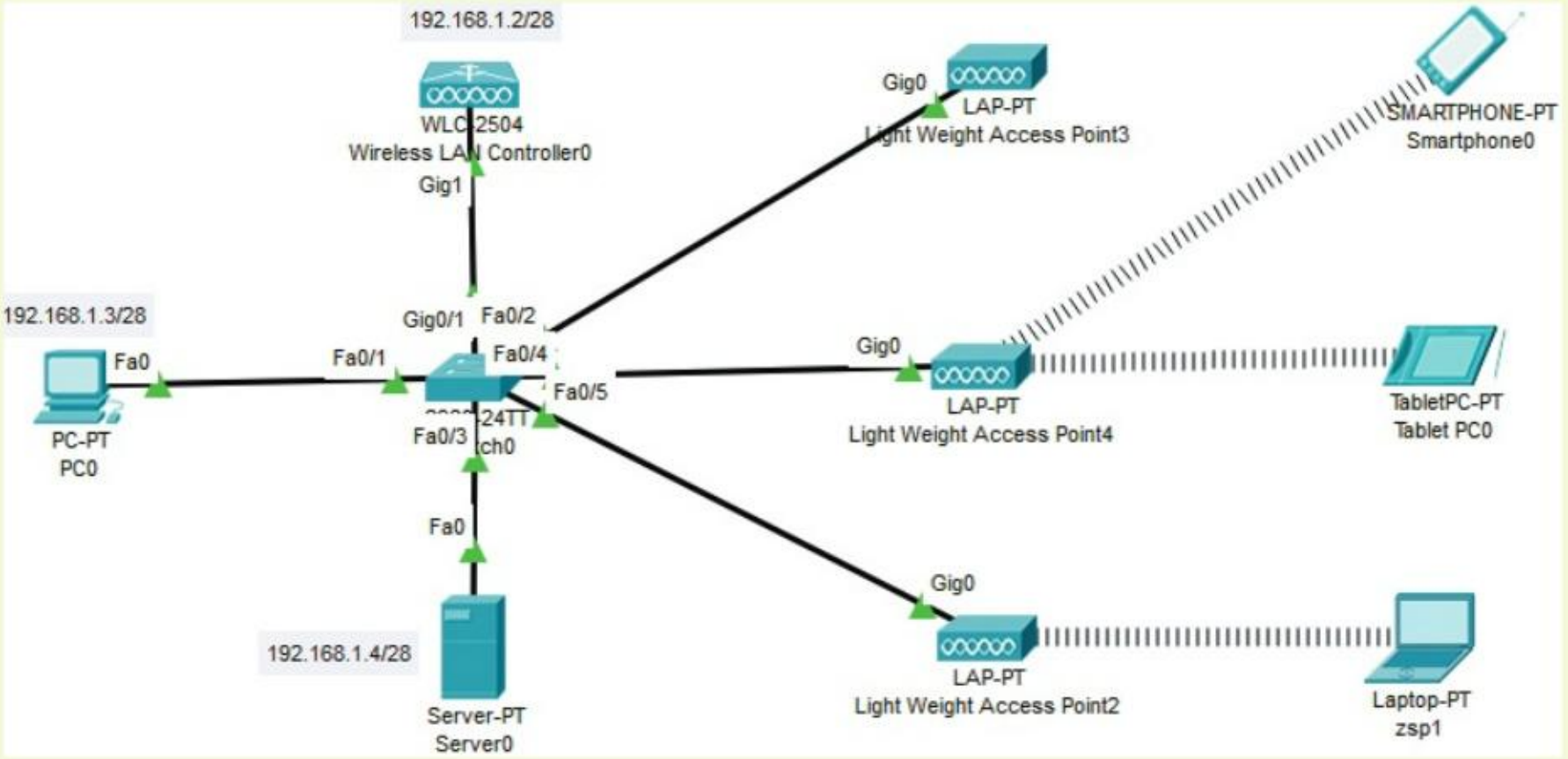
PRZYKŁAD 51.7

Konfigurowanie sieci Wi-Fi zarządzanej za pomocą kontrolera

W tym ćwiczeniu zostanie skonfigurowana sieć Wi-Fi administrowana przez kontroler zarządzający trzema punktami dostępowymi. Każdy z punktów dostępowych ma udostępniać sieci o identyfikatorach **`zsp1`**, **`zsp2`** i **`zsp3`**. Do sieci zostaną podłączone urządzenia bezprzewodowe: laptop, tablet i smartfon. Schemat sieci przedstawiono na rys. 51.16.

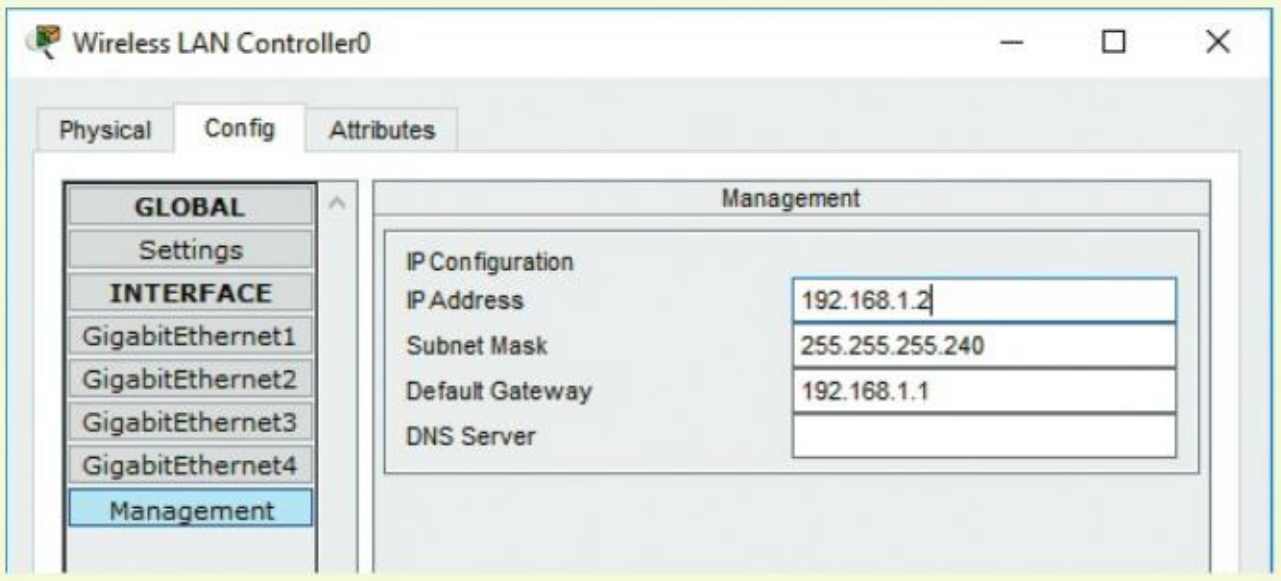
Aby skonfigurować klienta sieci bezprzewodowej, należy wykonać następujące czynności:

1. Uruchomić Cisco Packet Tracer i połączyć urządzenia według schematu z rys. 51.16.
2. Podłączyć zasilanie do punktów dostępowych. Punkty dostępowe mogą być zasilane przez kabel sieciowy (ang. *Power on Ethernet*, PoE) lub przez zewnętrzne zasilacze. W tym ćwiczeniu należy wykorzystać zasilacze.
3. Domyślnie kontroler sieci Cisco WLC 2504 do zarządzania wykorzystuje port GigabitEthernet1, z ustawionym adresem **`192.168.1.1/28`**. Ponieważ zwykle pierwszy adres z puli był przeznaczany na bramę, to adres interfejsu można zmienić, np. na **`192.168.1.2/28`**, jak na rys. 51.17.



Rys. 51.16. **Schemat sieci Wi-Fi zarządzanej przez kontroler**

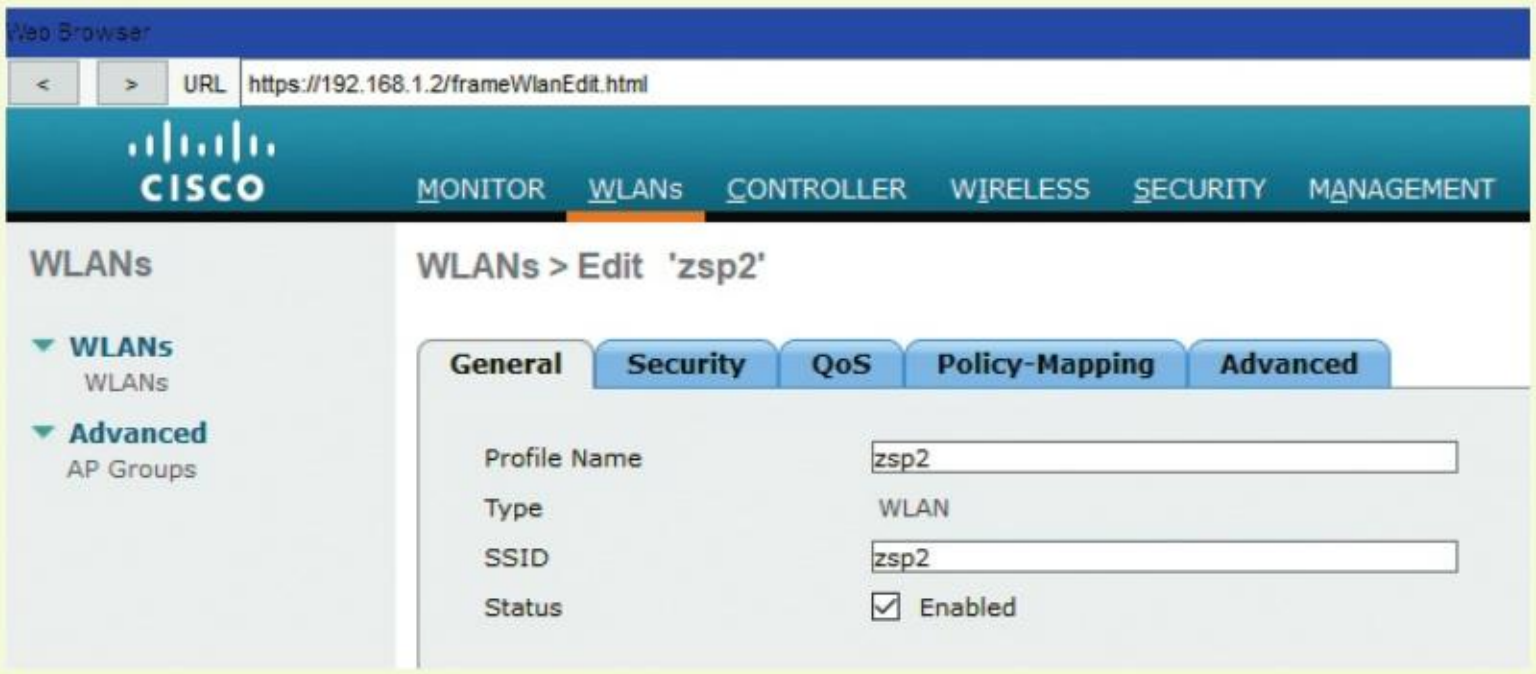
4. Komputerowi PC wykorzystywanemu do zarządzania należy przydzielić adres z tej samej sieci, np. **`192.168.1.3/28`**, i bramę **`192.168.1.1`**.
5. Za pomocą przeglądarki internetowej z komputera połączyć się z kontrolerem (adres **`192.168.1.2`**).
6. Utworzyć konto do zarządzania kontrolerem, np. **`Admin`** z hasłem **`Qwerty123`**, i kliknąć przycisk **`Start`**.



Rys. 51.17. **Konfiguracja adresów IP kontrolera sieci**

7. W sekcji **`Set UP Your Controller`** wprowadzić dane konfiguracyjne kontrolera:
   - nazwę systemu (ang. *System Name*), np. **`zsp`**;
   - adres IP zarządzania (ang. *Management IP Address*), np. **`192.168.1.2`**;
   - maskę podsieci (ang. *Subnet Mask*), np. **`255.255.255.240`**;
   - domyślną bramę (ang. *Default Gateway*), np. **`192.168.1.1`**;
   - identyfikator sieci VLAN zarządzania (ang. *Management VLAN ID*), np. **`1`**.
8. Kliknąć przycisk **`Next`**.
9. W sekcji **`Create Your Wireless Networks`** wprowadzić dane konfiguracyjne sieci Wi-Fi:
   - identyfikator SSID (ang. *Network Name*), np. **`zsp1`**;
   - standard szyfrowania (ang. *Security*), np. **`WPA2 Personal`**;
   - hasło do sieci Wi-Fi (w pola **`Passphrase`** i **`Confirm Passphrase`**), np. **`Qwerty123`**.

10. Kliknąć przycisk **Next**.
11. W sekcji **Advanced Setting** można nie wprowadzać zmian. Kliknąć przycisk **Next**. Po sprawdzeniu ustawień kliknąć przycisk **Apply** i pozwolić na restart urządzenia.
12. Za pomocą przeglądarki internetowej z komputera połączyć się z kontrolerem (adres **192.168.1.2**) za pomocą protokołu **https** i kliknąć przycisk **Login**.
13. Wprowadzić nazwę konta (**Admin**) i hasło (**Qwerty123**).
14. Wybrać zakładkę **WLANs**.
15. Dodać nową sieć Wi-Fi. Wybrać opcję **Create New** i kliknąć **Go**.
16. W zakładce **General** wprowadzić nazwę profilu (ang. *Profile Name*), np. **zsp2**, identyfikator SSID, np. **zsp2**, zaznaczyć opcję **Enabled** i kliknąć przycisk **Apply** (rys. 51.18).



Rys. 51.18. **Dodawanie sieci Wi-Fi**

17. W zakładce **Security** wprowadzić informacje o zabezpieczeniach sieci:
    - standard szyfrowania (Layer 2 Security), np. **WPA+WPA2**;
    - zaznaczyć opcję **WPA2 Policy**;
    - zaznaczyć opcję **PSK**;
    - wprowadzić hasło w polu **PSK Format**, np. **format ASCII**, hasło **Qwerty123**.
18. Kliknąć przycisk **Apply**.
19. Powtórzyć punkty od 15. do 18. dla sieci **zsp3**.
20. Sprawdzić poprawność konfiguracji sieci (rys. 51.19).

KODY



Rys. 51.19. **Sprawdzanie poprawności konfiguracji sieci**

21. Serwerowi przydzielić adres, np. **192.168.1.14/28**, i bramę **192.168.1.1**.
22. Skonfigurować serwer DHCP. Kliknąć w ikonę serwera i wybrać zakładkę **Services**. W lewym panelu wskazać DHCP i wprowadzić ustawienia:
    - Default Gateway: **192.168.1.1**;
    - Start Address: **192.168.1.5**;
    - Maskimum Number of Users: **9**;
    - Włączyć serwer – zaznaczyć **Service ON**.
    - Kliknąć przycisk **Save**.
23. Skonfigurować urządzenia bezprzewodowe: laptop, tablet i smartfon do pracy w różnych sieciach i sprawdzić możliwości komunikacji z serwerem.

Firma Ubiquiti oferuje programowy kontroler sieci Wi-Fi współpracujący z punktami dostępowymi (i innymi urządzeniami) tego producenta. Taki kontroler może być zainstalowany na komputerze z systemem Windows, Linux lub MacOS i zarządzać punktami dostępowymi. Kontroler można pobrać ze strony https://www.ui.com/download-software/. Po pobraniu kontroler należy zainstalować i skonfigurować.

PRZYKŁAD 51.8

Konfigurowanie sieci Wi-Fi zarządzanej za pomocą kontrolera z wykorzystaniem urządzeń firmy Ubiquiti

W tym ćwiczeniu zostanie wykonana konfiguracja sieci Wi-Fi w nowo zainstalowanym kontrolerze. Po instalacji kontrolera należy:

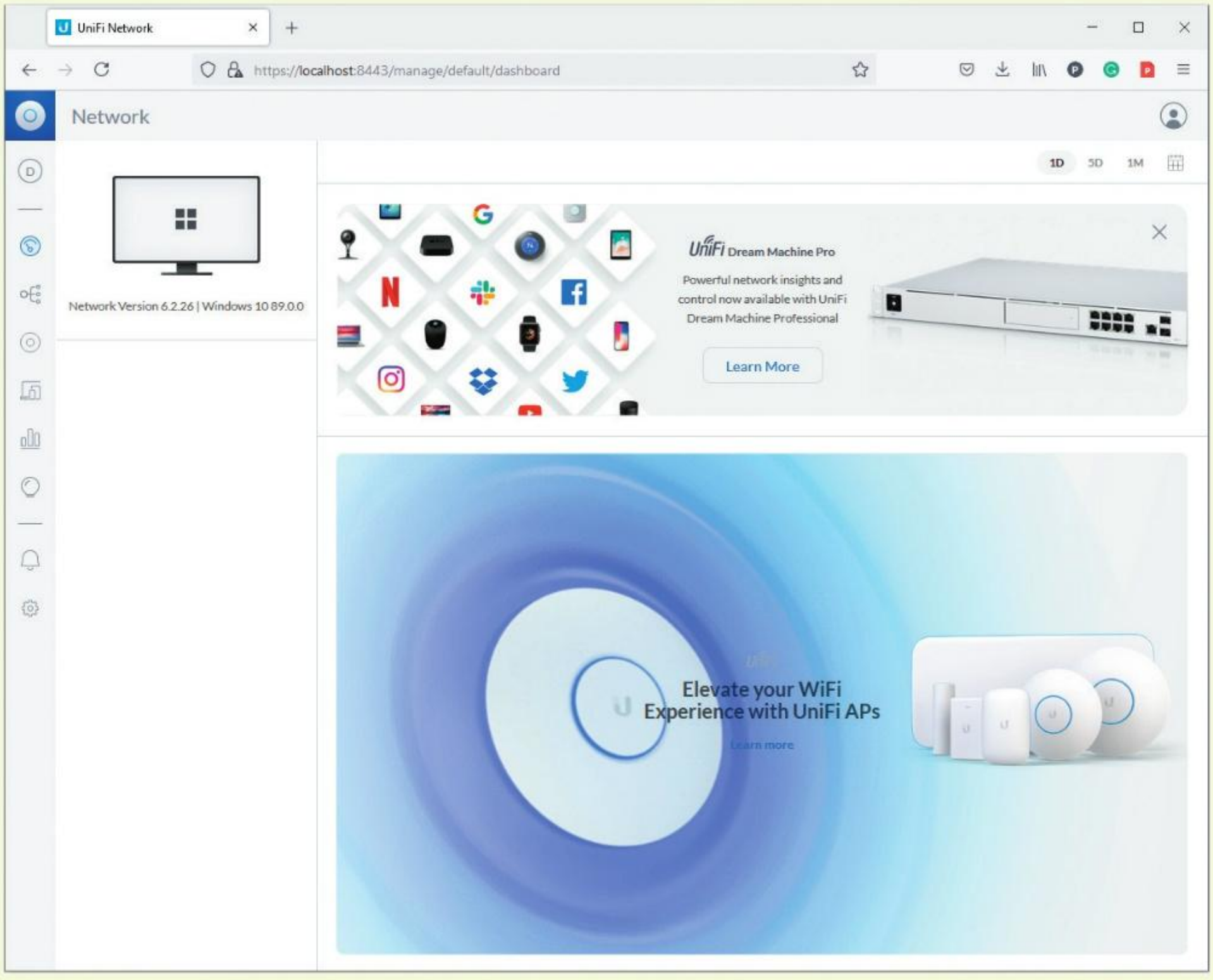
1. Zarejestrować konto w systemie Ubiquiti na stronie https://account.ui.com/register. Aktywować konto przez system e-mail.
2. Uruchomić kontroler (rys. 51.20). Kliknąć przycisk **Launch a Browser to Manage the Network**.



Rys. 51.20. **Uruchomienie kontrolera Wi-Fi**

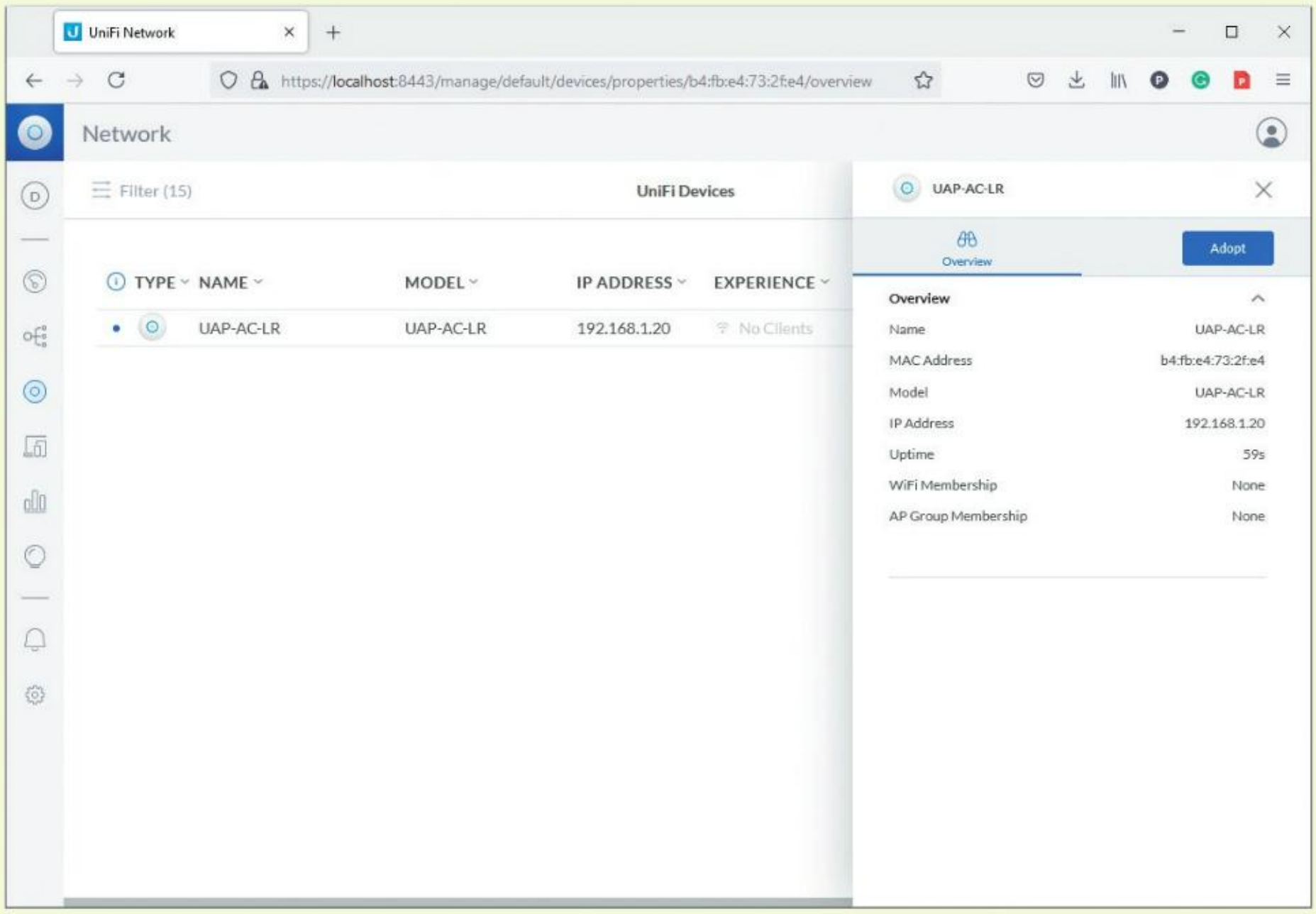
3. W oknie **Name Your Controller** wprowadzić nazwę kontrolera, np. **zsp_sieradz**. Wyrazić zgodę na warunki licencji. Kliknąć przycisk **Next**.

4. W oknie **Sign in with your Ubiquiti Account** wprowadzić nazwę konta i hasło. Kliknąć przycisk **Next**.
5. Zatwierdzić opcje w oknie **UniFi Network Setup**. Kliknąć przycisk **Next**.
6. Jeżeli system wykryje kompatybilne urządzenia w oknie **Device Setup**, to można je wskazać. Jeżeli urządzenia będą podłączone w przyszłości – kliknąć przycisk **Next**.
7. W oknie **WiFi Setup** wprowadzić nazwę sieci Wi-Fi (np. **zsp_sieradz**) i hasło (np. **Qwerty123**). Kliknąć przycisk **Next**.
8. Sprawdzić ustawienia sieci w oknie **Review Configuration**. Kliknąć przycisk **Finish**. Po zakończeniu konfiguracji kontroler jest gotowy do pracy (rys. 51.21).



Rys. 51.21. **Okno kontrolera po zakończeniu konfiguracji**

9. Dodać punkty dostępowe. Kliknąć ikonę **UNIFI DEVICES** w lewym panelu okna. Wskazać punkt dostępowy, który ma być przyłączony do kontrolera, i kliknąć przycisk **Adopt** (rys. 51.22).



Rys. 51.22. **Przyłączanie punktu dostępowego do kontrolera**

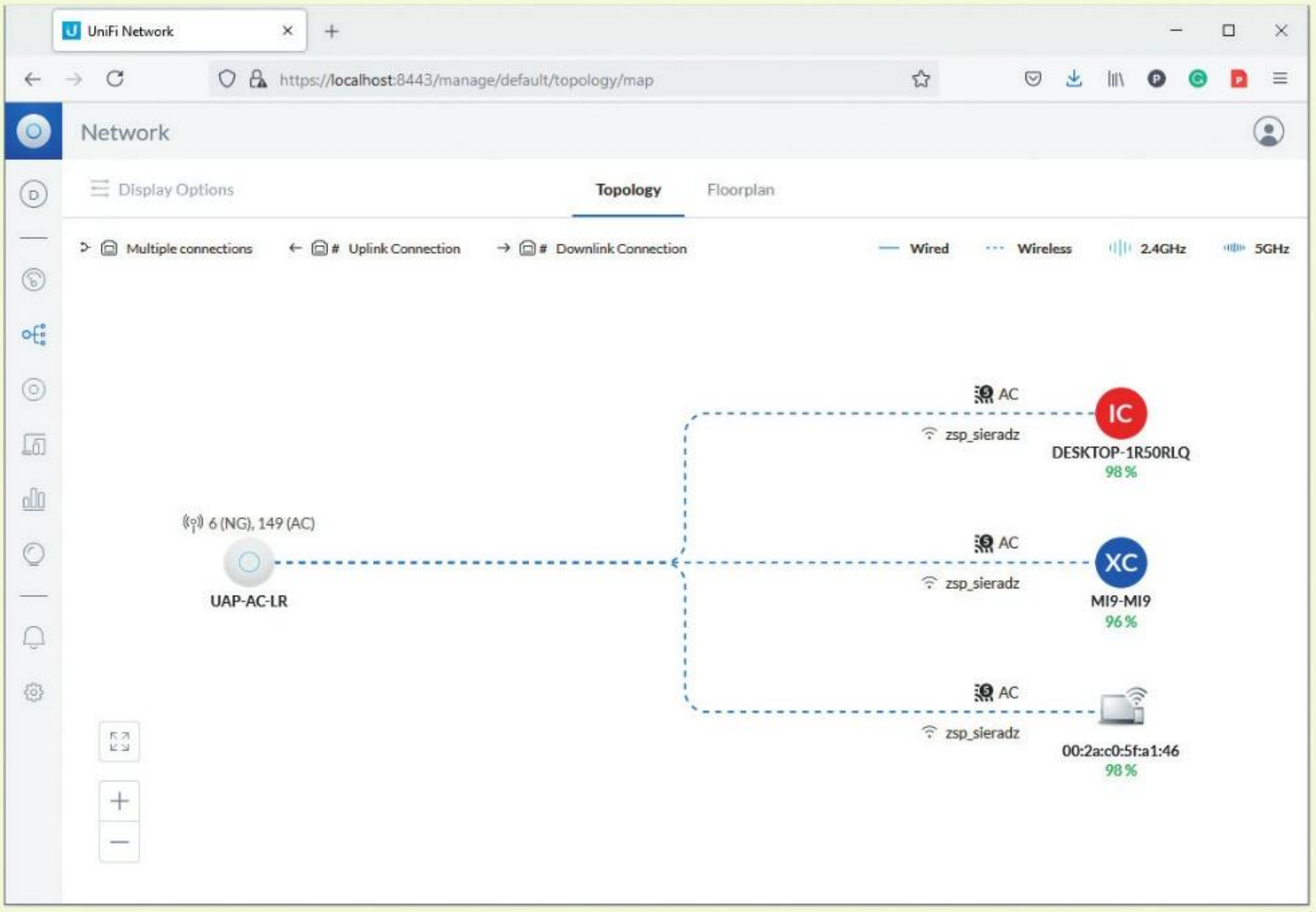
Dzięki kontrolerowi sieci Wi-Fi możliwe staje się scentralizowane zarządzanie urządzeniami i użytkownikami sieci. Wszystkie ustawienia wprowadzane na kontrolerze są kopiowane do punktów dostępowych. Po zakończeniu konfiguracji kontroler może zostać wyłączony, a punkty dostępowe zachowują konfigurację.

PRZYKŁAD 51.9

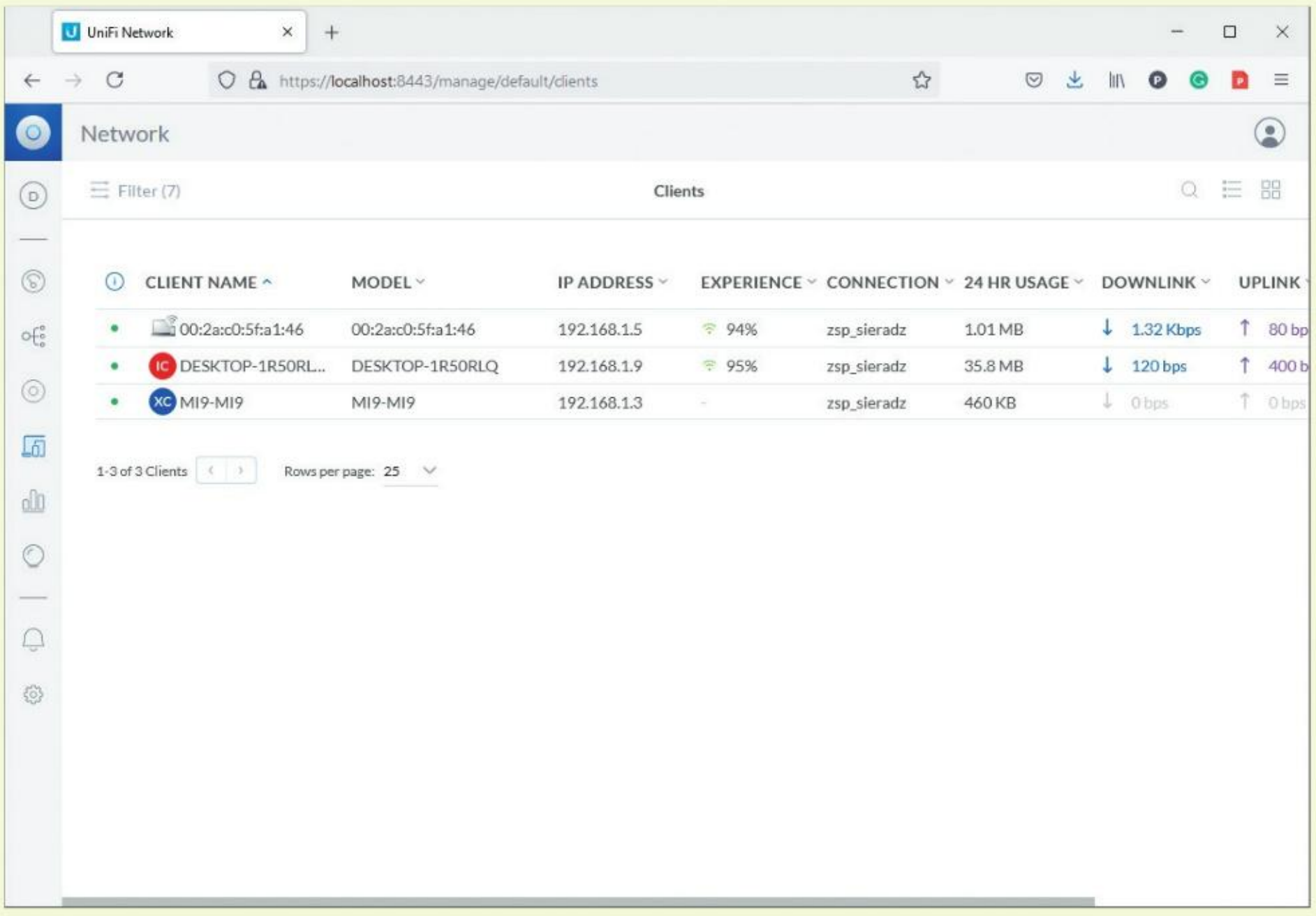
Zarządzanie siecią Wi-Fi z kontrolerem firmy Ubiquiti

W tym ćwiczeniu zobaczymy podstawowe możliwości konfiguracyjne kontrolera.

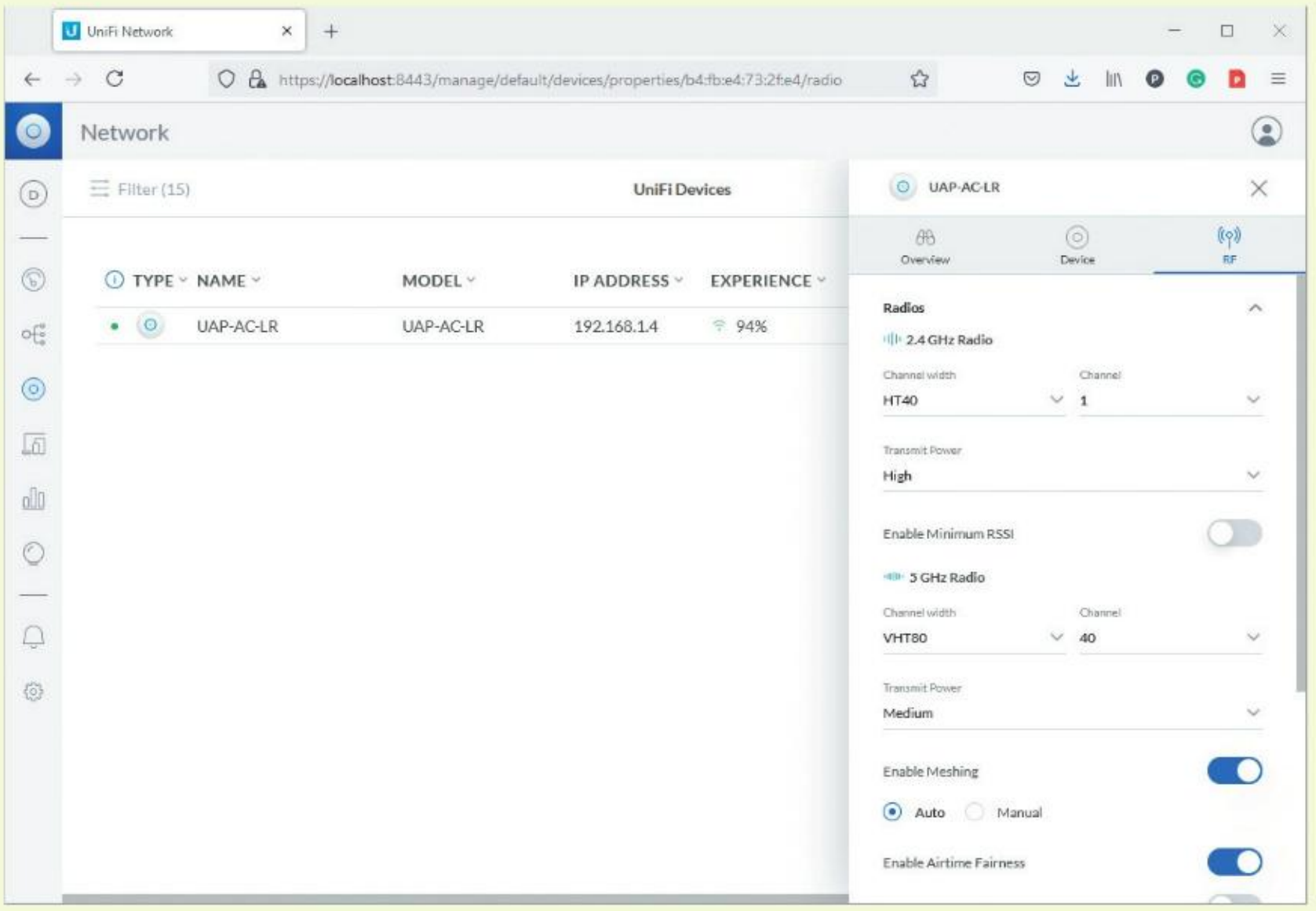
1. Uruchomić kontroler i zalogować się na konto.
2. W lewym panelu okna kliknąć ikonę **`TOPOLOGY`** (rys. 51.23), aby zobaczyć schemat połączeń między punktami dostępowymi a użytkownikami.
3. W lewym panelu okna kliknąć ikonę **`CLIENTS`**, aby zobaczyć listę użytkowników zalogowanych do sieci (rys. 51.24).
4. Zarządzanie punktami dostępowymi możliwe jest po wybraniu ikony **`UNIFI DEVICES`** z lewego panelu bocznego. Po wskazaniu punktu dostępowego pojawi się okno z ustawieniami:
   - **`OverWiew`** – ogólne ustawienia punktu dostępowego, np. nazwa, model, wersja oprogramowania, adres fizyczny i odnośnik **`Apply Upgrade`**, umożliwiający aktualizację oprogramowania;
   - **`Device`** – okno konfiguracji urządzenia, m.in. nazwy, adresu IP;
   - **`RF`** – okno konfiguracji kanału radiowego (rys. 51.25), np. wybór zakresu częstotliwości, kanału, emitowanej mocy.



Rys. 51.23. **Topologia sieci Wi-Fi**

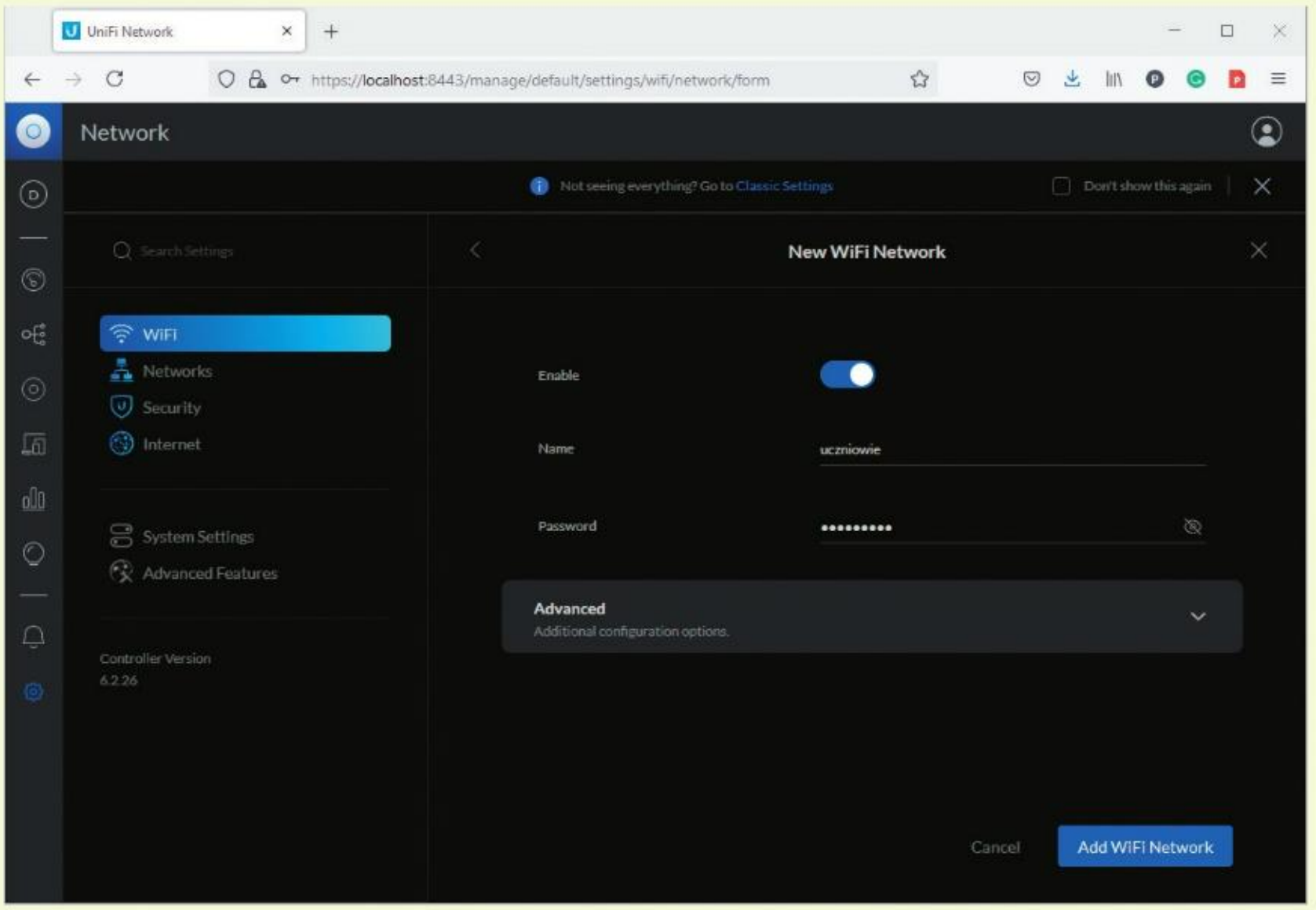


Rys. 51.24. **Lista użytkowników zalogowanych do sieci**



Rys. 51.25. **Okno konfiguracji kanału radiowego w kontrolerze UniFi**

5. W lewym panelu okna kliknąć ikonę **SETTINGS**. W zakładce Wi-Fi można zarządzać sieciami, np. aby utworzyć nową sieć, należy kliknąć odnośnik **Add New WiFi Network** (rys. 51.26), wprowadzić dane nowej sieci i kliknąć przycisk **Add WiFi Network**.



Rys. 51.26. **Tworzenie nowej sieci Wi-Fi**

> **! UWAGA**
> Aby wprowadzić dodatkowe ustawienia, np. wyboru częstotliwości lub bezpieczeństwa, należy rozwinąć zakładkę **Advanced**.

6. W zakładce **`System Settings`** można zmienić ogólne ustawienia kontrolera lub w sekcji **`Maintenance/Backup/Restore`** sporządzić bądź odtworzyć kopię zapasową ustawień konfiguracyjnych kontrolera.

51.3. Anteny

Anteny służą do zamiany fal elektromagnetycznych na sygnał elektryczny i odwrotnie. Stosuje się je we wszystkich systemach radiokomunikacyjnych, np. w komunikacji radiowej i telewizyjnej, a także w sieciach Wi-Fi. Anteny są elementami odwracalnymi. Oznacza to, że antena może dokonywać przemiany energii prądu elektrycznego na falę elektromagnetyczną i fali elektromagnetycznej na prąd (siłę elektromotoryczną).

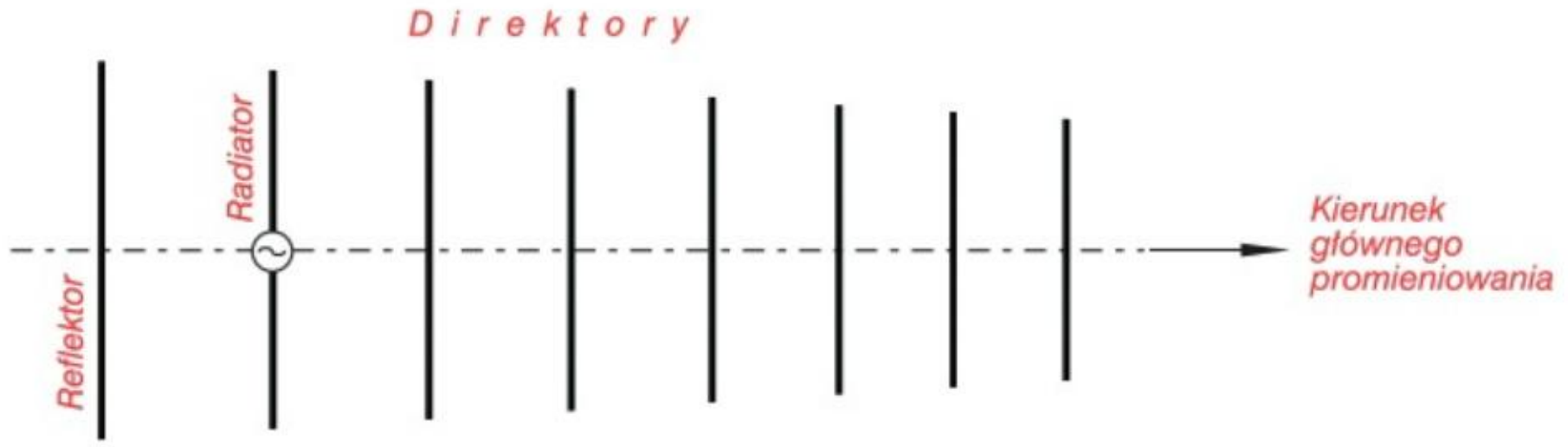
Najważniejszym parametrem anten jest **charakterystyka promieniowania**. Zależnie od potrzeb antena może być przystosowana do emitowania fali elektromagnetycznej z jednakową mocą we wszystkich kierunkach (w określonej płaszczyźnie). W tym przypadku mówimy o **charakterystyce dookólnej anteny**. Taką charakterystykę mają niemal wszystkie anteny standardowo montowane w punktach dostępowych. Niekiedy istnieje potrzeba wyemitowania energii w ściśle określonym kierunku kosztem pozostałych kierunków. Tę własność nazywa się **kierunkowością**, a anteny tego typu – **antenami kierunkowymi**. Parametry rzeczywistych anten są często podawane w odniesieniu do **anteny izotropowej** – teoretycznej idealnej konstrukcji, która promieniuje energię równomiernie we wszystkich kierunkach i charakteryzuje się stuprocentową sprawnością.

Zysk energetyczny anteny (ang. *gain*) to stosunek wypromieniowanej przez nią energii do energii, którą wypromieniowałaby antena wzorcowa (izotropowa), przy założeniu, że do obu anten została doprowadzona taka sama moc. Zysk energetyczny w odniesieniu do anteny izotropowej jest podawany w dBi. Powszechnie używanym parametrem anten jest **zastępcza moc promieniowana izotropowo EIRP** (ang. *Effective Isotropic Radiated Power*). Ten parametr określa moc, którą należałoby zasilać antenę izotropową, aby gęstość mocy w otoczeniu tej anteny była taka sama jak gęstość mocy w kierunku maksymalnego promieniowania rzeczywistej anteny, w której występują straty mocy.

O stratach w antenie, głównie cieplnych, informuje **sprawność energetyczna**. Jest to stosunek mocy promieniowanej przez antenę do mocy na zaciskach wejściowych. **Pasmo anteny** to zakres częstotliwości, w którym antena zachowuje nominalne parametry. **Impedancja anteny** to obciążenie, jakie przedstawia antena dla generatora (źródła sygnału). Impedancja anten zależy od geometrii anteny i od częstotliwości. Najwyższą sprawność układu urządzenie – kabel – antena uzyskuje się wtedy, gdy wszystkie elementy toru transmisyjnego mają taką samą impedancję. W radiokomunikacji zwykle stosuje się urządzenia o impedancji 50 Ω. Drgania fal elektromagnetycznych zachodzą w ściśle określonych płaszczyznach. Jeżeli drgają tylko w jednej płaszczyźnie, występuje **polaryzacja liniowa** – pionowa lub pozioma. Gdy drgają w obu płaszczyznach, występuje **polaryzacja kołowa** lub **eliptyczna** – prawoskrętna lub lewoskrętna.

Najprostszym typem anteny jest **dipol** – składa się zazwyczaj z dwóch symetrycznych ramion -radiatorów wyposażonych w zaciski do doprowadzenia napięcia zasilającego. Najczęściej dipole mają długość zbliżoną do połowy długości fali roboczej.

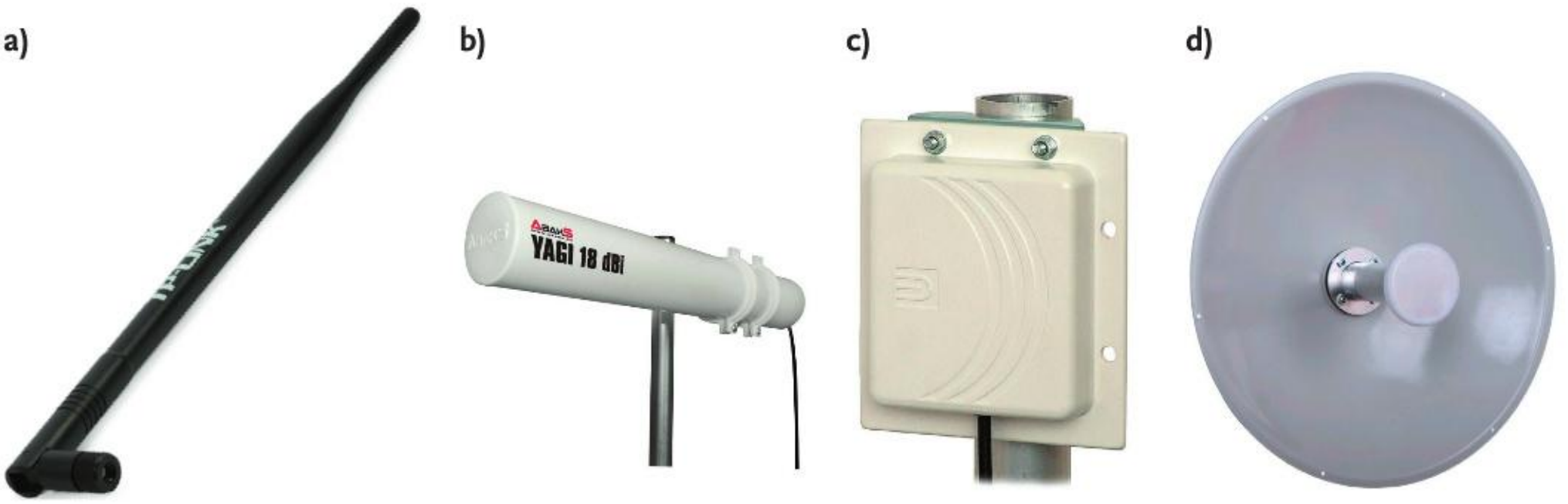
Antena **Yagi-Uda** jest zazwyczaj zbudowana z **elementu czynnego** (radiatora) w postaci dipola pętlowego i szeregu sprzężonych z nim elementów biernych. Elementy bierne umieszczone w kierunku maksymalnego promieniowania nazywa się **direktorami**, a umieszczone w kierunku przeciwnym (promieniowania wstecznego) – **reflektorami**. Zysk energetyczny anteny Yagi-Uda osiąga od kilku do kilkunastu dBi.



Rys. 51.27. **Budowa anteny Yagi-Uda**

Antena panelowa przeważnie jest zbudowana z zespołu dipoli umieszczonych przed płaskim ekranem (reflektorem). Zysk energetyczny anteny panelowej osiąga od kilku do kilkunastu dBi.

Antena paraboliczna ma charakterystykę o silnej kierunkowości i duży zysk (do 30 dBi). Wykorzystuje się ją w transmisjach satelitarnych, ale również do budowy połączeń punkt–punkt na duże odległości.



Rys. 51.28. **Przykłady anten używanych w sieciach komputerowych: a) prętowa, b) Yagi-Uda, c) panelowa, d) paraboliczna**

Zasięg sieci bezprzewodowej zależy od wielu czynników związanych z zastosowanymi urządzeniami, takich jak moc wyjściowa urządzenia nadawczego, tłumienie kabli, zysk anten, czułość odbiornika, jak również od czynników zewnętrznych: tłumienia w przestrzeni między antenami czy wpływu przeszkód oraz zakłóceń.

Moc maksymalna nadajnika jest ograniczona przepisami prawa, np. dla sieci Wi-Fi to:

- dla częstotliwości 2,400–2,4835 GHz moc nieprzekraczająca 100 mW EIRP (20 dBm);
- dla częstotliwości 5,150–5,350 GHz moc nieprzekraczająca 200 mW EIRP (23 dBm) – to pasmo dopuszczono do użytku wyłącznie wewnątrz pomieszczeń;
- dla częstotliwości 5,470–5,725 GHz moc nieprzekraczająca 1000 mW EIRP (30 dBm).

Do podłączenia anten zwykle stosuje się kabel koncentryczny o jak najkrótszej długości i o jak najmniejszym tłumieniu. Czułość odbiornika podaje producent i zależy ona od konkretnego modelu. Urządzenia do budowy łącza radiowego dobiera się w oparciu na bilansie energetycznym łącza, który można zapisać za pomocą wzoru:

$$P_o - L - L_d + G_1 + G_2 = P_{rx},$$

gdzie:

- P_o – moc nadajnika [dBm];
- L – straty rozproszeniowe, np. w przestrzeni między antenami, zależne od odległości, częstotliwości oraz tłumienia w przestrzeni. Straty można obliczyć na podstawie wzoru:

$$L = 20 \cdot \log(x) + 20 \cdot \log(f) + 32{,}4,$$

  gdzie:
  - L – tłumienie [dB];
  - x – długość drogi [km];
  - f – częstotliwość [MHz];
  - 32,4 – wartość stała;
- L_d – straty dodatkowe, np. w złączach, kablach, zależne od długości kabla i jego tłumienia, liczby złączy i ich tłumienia. Straty można obliczyć na podstawie wzoru:

$$L_d = d_1 \cdot t_{w1} + d_2 \cdot t_{w2} + t_{k1} + t_{k2} + 6,$$

  gdzie:
  - L_d – straty dodatkowe [dB];
  - d_1, d_2 – długość kabla do anteny 1 i 2 [m];
  - t_{w1}, t_{w2} – tłumienie właściwe kabla 1 i 2 [dB/m];
  - t_{k1}, t_{k2} – tłumienie złącz konektorowych [dB] (jeśli jest ich więcej niż 2, to zsumować wszystkie);
  - 6 – margines błędu na wypadek nieprzewidzianych okoliczności, np. zakłóceń, przesłonięcia przestrzeni między antenami przez przeszkody;
- G_1, G_2 – zyski energetyczne anten [dBi];
- P_{rx} – czułość odbiornika [dB] (np. –89 dB).

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zaplanuj rozmieszczenie minimalnej liczby punktów dostępowych tak, aby zapewnić pełne pokrycie obszaru twojej szkoły. Dla uproszczenia przyjmij, że każdy punkt dostępowy może pokryć obszar, który jest okręgiem o promieniu zależnym od konkretnego urządzenia. Obszary pokrycia poszczególnych punktów dostępowych powinny zachodzić na siebie na mniej więcej 10 %, aby zapewnić dostęp do sieci w każdym punkcie szkoły.
2. Skorzystaj z dowolnego punktu dostępowego i skonfiguruj listę adresów MAC, które mogą uzyskać dostęp do sieci.

WSKAZÓWKA

Należy skorzystać z zakładki **Wireless MAC Filter** lub innej o podobnym znaczeniu w przypadku innego urządzenia.

3. Wyszukaj w internecie dowolny kalkulator ułatwiający obliczenie bilansu energetycznego łącza. Wykonaj obliczenia dla przykładowych danych, np. dla połączenia ze szkoły do domu. Dobierz urządzenia do budowy łącza.

52 Funkcje przełączników zarządzalnych

ZAGADNIENIA

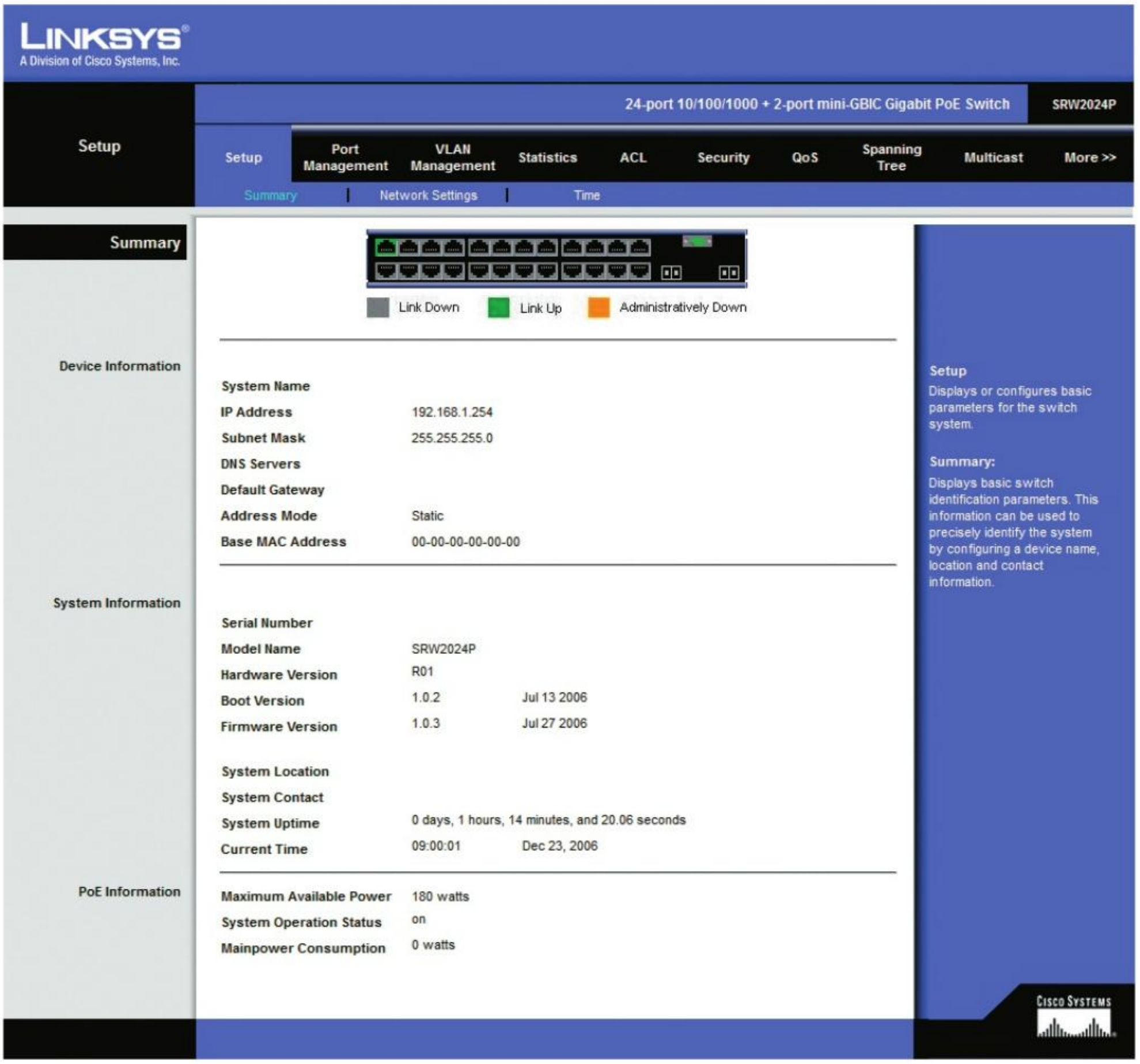
Konfigurowanie przełącznika **Zabezpieczenie konfiguracji przełącznika za pomocą hasła** **Zmiana prędkości i trybu pracy portu przełącznika** **Zarządzanie wpisami do tablicy adresów MAC przełącznika** **Skonfigurowanie funkcji bezpieczeństwa portów w przełączniku** **Funkcja i działanie protokołu Spanning-Tree**

W ofercie różnych producentów sprzętu sieciowego są dostępne przełączniki pracujące w warstwie drugiej i przełączniki trzeciej warstwy modelu ISO/OSI, czyli tzw. przełączniki routujące, a nawet modele pracujące w jeszcze wyższych warstwach modelu OSI (przełączniki zawartości). Najczęściej spotyka się przełączniki warstwy drugiej, odgrywające rolę punktu koncentracji dla podłączonych stacji roboczych, serwerów, routerów, koncentratorów i innych przełączników.

Przełącznik warstwy drugiej jest urządzeniem sieciowym pełniącym funkcję punktu koncentracji dla podłączonych stacji roboczych, serwerów, routerów, koncentratorów i innych przełączników. W przełącznikach są wstępnie zdefiniowane domyślne fabryczne ustawienia parametrów umożliwiające podłączenie przełącznika do sieci bez wprowadzania jakichkolwiek zmian w konfiguracji. Konfigurowanie przełączników i zarządzanie nimi może się odbywać za pomocą **interfejsu wiersza poleceń CLI**.

Przełączniki sieciowe mogą być także konfigurowane i zarządzane za pośrednictwem interfejsu WWW i przeglądarki. Przykład interfejsu przełącznika konfigurowanego za pomocą przeglądarki przedstawiono na rys. 52.1. Przełączniki to wyspecjalizowane komputery z centralną jednostką obliczeniową CPU, pamięcią RAM i systemem operacyjnym. W przełącznikach jest zazwyczaj dostępnych wiele portów, do których mogą zostać podłączone hosty, a także są tam specjalne porty umożliwiające zarządzanie. W dalszej części omówimy funkcje przełączników zarządzalnych na przykładzie urządzeń firmy CISCO. Przełączniki innych producentów są wyposażone w podobne funkcje, lecz mogą różnić się poleceniami i sposobem konfiguracji.

Przełącznik od chwili włączenia wykonuje sekwencję poleceń mającą na celu przygotowanie go do pracy. Jest ona taka sama jak dla routera. Aby skonfigurować przełącznik, należy połączyć port szeregowy komputera (COM) z portem konsoli przełącznika i ustanowić sesję komunikacyjną.



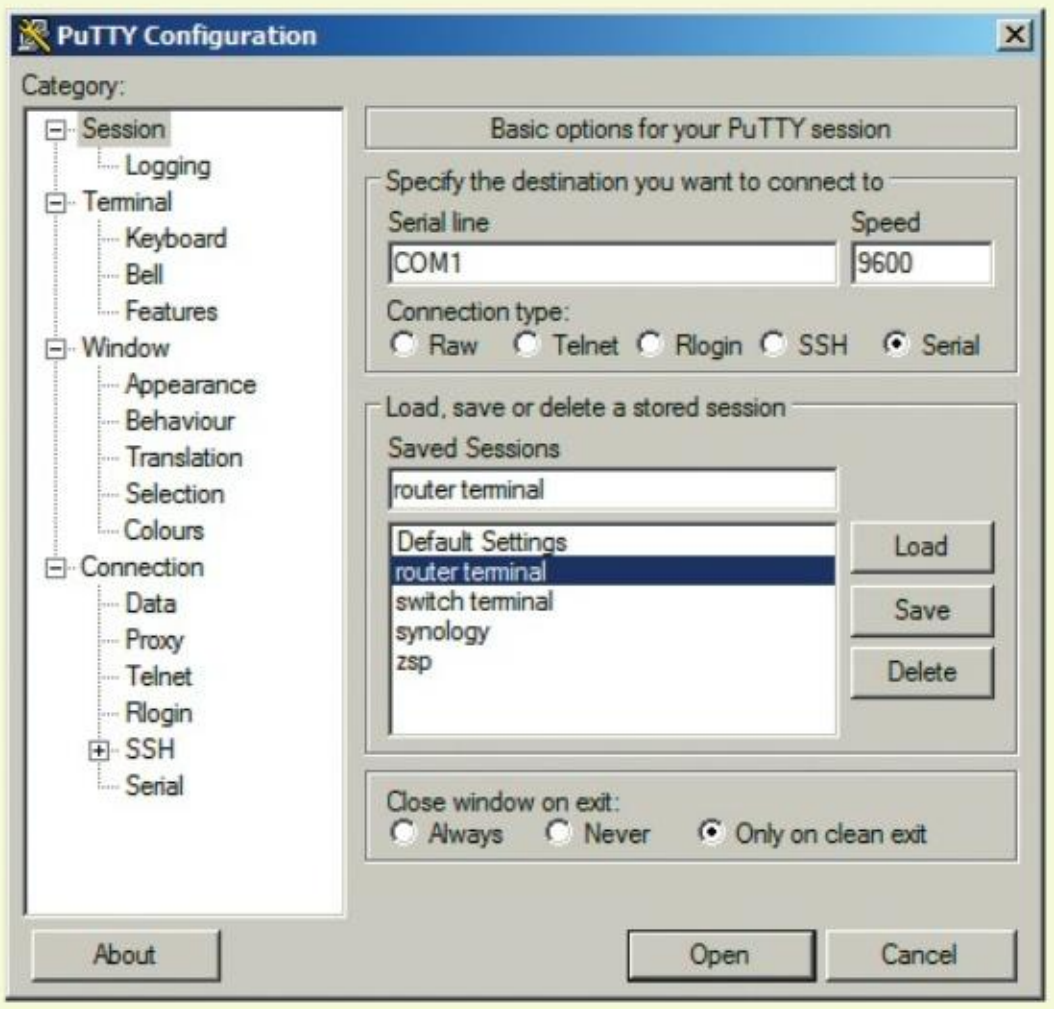
Rys. 52.1. Przykład interfejsu przełącznika konfigurowanego za pomocą przeglądarki

PRZYKŁAD 52.1

Połączenie komputera z portem konsoli w przełączniku

Aby nawiązać połączenie między komputerem a przełącznikiem za pomocą portu konsoli, należy:

1. Za pomocą **kabla konsolowego** (ang. *rollover*) połączyć port konsoli przełącznika z portem COM komputera.
2. Uruchomić na komputerze program Putty. W wyświetlonym oknie dialogowym (rys. 52.2) za pomocą przycisku radiowego należy wybrać typ połączenia **`Serial`** i nazwę portu szeregowego komputera (np. **`COM1`**). Wybrać w sekcji **`Category`** opcję **`Serial`** i ustawić prędkość połączenia (**`Speed: 9600`**) oraz sterowanie przepływem (**`Flow Control: None`**). Pozostałe parametry połączenia, takie jak bit parzystości, ilość bitów danych, bity stopu, można pozostawić jako wartości domyślne. Po kliknięciu przycisku **`Open`** połączenie zostanie nawiązane, co jest sygnalizowane znakiem gotowości przełącznika.



Rys. 52.2. **Konfiguracja programu Putty do połączenia za pomocą portu konsoli**

Trybem domyślnym pracy przełącznika, podobnie jak routera, jest tryb EXEC użytkownika – w symbolu zachęty występuje znak „większe niż" (>). Polecenie **enable** służy do przełączania z trybu EXEC użytkownika do uprzywilejowanego trybu EXEC – w symbolu zachęty występuje znak „#". W zestawie poleceń uprzywilejowanego trybu EXEC, oprócz polecenia **configure**, są także osiągalne wszystkie polecenia dostępne w trybie EXEC użytkownika. Zasady dotyczące pracy w różnych trybach i ich zmiany są takie same jak dla routerów. Polecenia umożliwiające zmianę trybu poleceń w przełączniku przedstawiono na rys. 52.3. Zmianę sygnalizuje znak gotowości przełącznika.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Rys. 52.3. **Polecenia umożliwiające zmianę trybu poleceń w przełączniku**

Przełącznik można zabezpieczyć przed dostępem osób nieuprawnionych za pomocą hasła. Hasło będzie wymagane w momencie uruchamiania trybu użytkownika uprzywilejowanego (po wydaniu polecenia **enable**). Gdy skorzystamy z polecenia **enable password**, będziemy mogli określić hasło przechowywane w formie jawnego tekstu. Szyfrowaną postać hasła wprowadza się za pomocą polecenia **enable secret** – jeśli zostanie skonfigurowane, będzie używane zamiast hasła wprowadzonego za pomocą polecenia **enable password**.

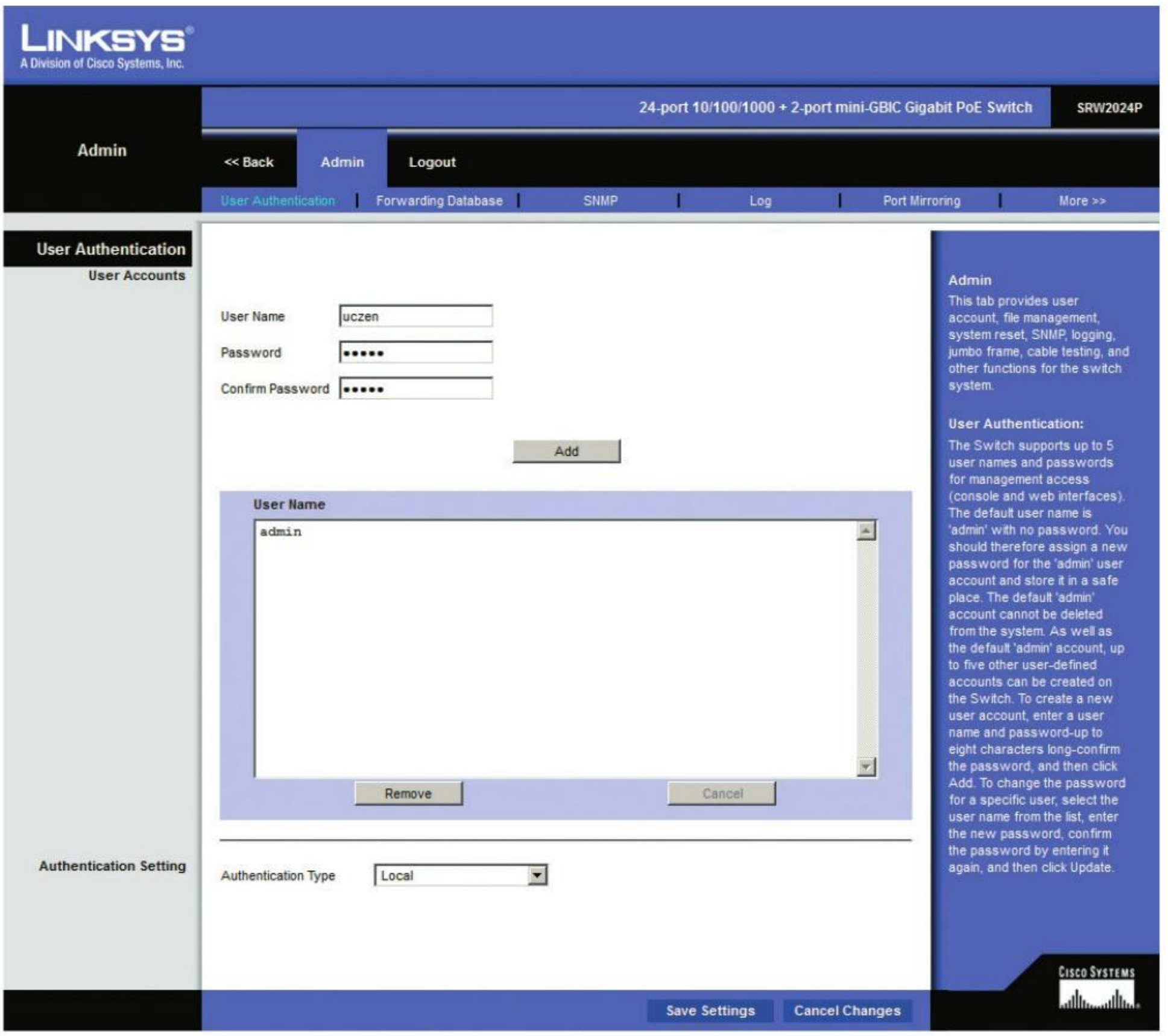
Aby usunąć wymóg podawania hasła przez użytkownika podczas przechodzenia w uprzywilejowany tryb wykonawczy, można użyć poleceń **no enable password** i **no enable secret**, wprowadzanych w trybie konfiguracji globalnej. Przykłady poleceń związanych z obsługą haseł przedstawiono na rys. 52.4.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable password cisco
Switch(config)#enable secret cisco
Switch(config)#no enable password
Switch(config)#no enable secret
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Rys. 52.4. **Polecenia umożliwiające obsługę haseł**

W przełącznikach konfigurowanych za pomocą interfejsu WWW do konfigurowania konta i hasła umożliwiającego dostęp do urządzenia służy zakładka ustawień administracyjnych (**Admin/User Authentication**). Przykład konfigurowania konta i hasła w przełączniku firmy Linksys przedstawiono na rys. 52.5.



Rys. 52.5. **Konfigurowanie hasła przełącznika za pomocą interfejsu WWW**

PRZYKŁAD 52.2

Zabezpieczanie przełącznika za pomocą hasła

Połącz komputer z przełącznikiem i za pomocą programu Putty nawiąż sesję. Wprowadź hasło nieszyfrowane „**haslo1**" i hasło szyfrowane „**haslo2**". Za pomocą polecenia **disable** przejdź do trybu EXEC użytkownika. Za pomocą polecenia **enable** przejdź do trybu użytkownika uprzywilejowanego. Którego hasła należy użyć i dlaczego? Skonfiguruj przełącznik do obsługi hasła nieszyfrowanego i przetestuj jego działanie.

Każdy z portów przełącznika Fast Ethernet ma domyślnie włączone funkcje autonegocjacji szybkości i trybu dupleksu. Umożliwia to interfejsom wynegocjowanie odpowiednich ustawień. W razie potrzeby administratorzy sieci mogą skonfigurować ręcznie szybkość interfejsu i ustawienia dotyczące trybu dupleksu. Na rys. 52.6 przedstawiono polecenia potrzebne do zmiany parametrów interfejsów.

KODY

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#duplex half
Switch(config-if)#speed 10
Switch(config-if)#exit
Switch(config)#interface range fastEthernet 0/4 - 10
Switch(config-if-range)#speed 10
Switch(config-if-range)#duplex full
Switch(config-if-range)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#
```

Rys. 52.6. **Polecenia umożliwiające zmianę parametrów interfejsów**

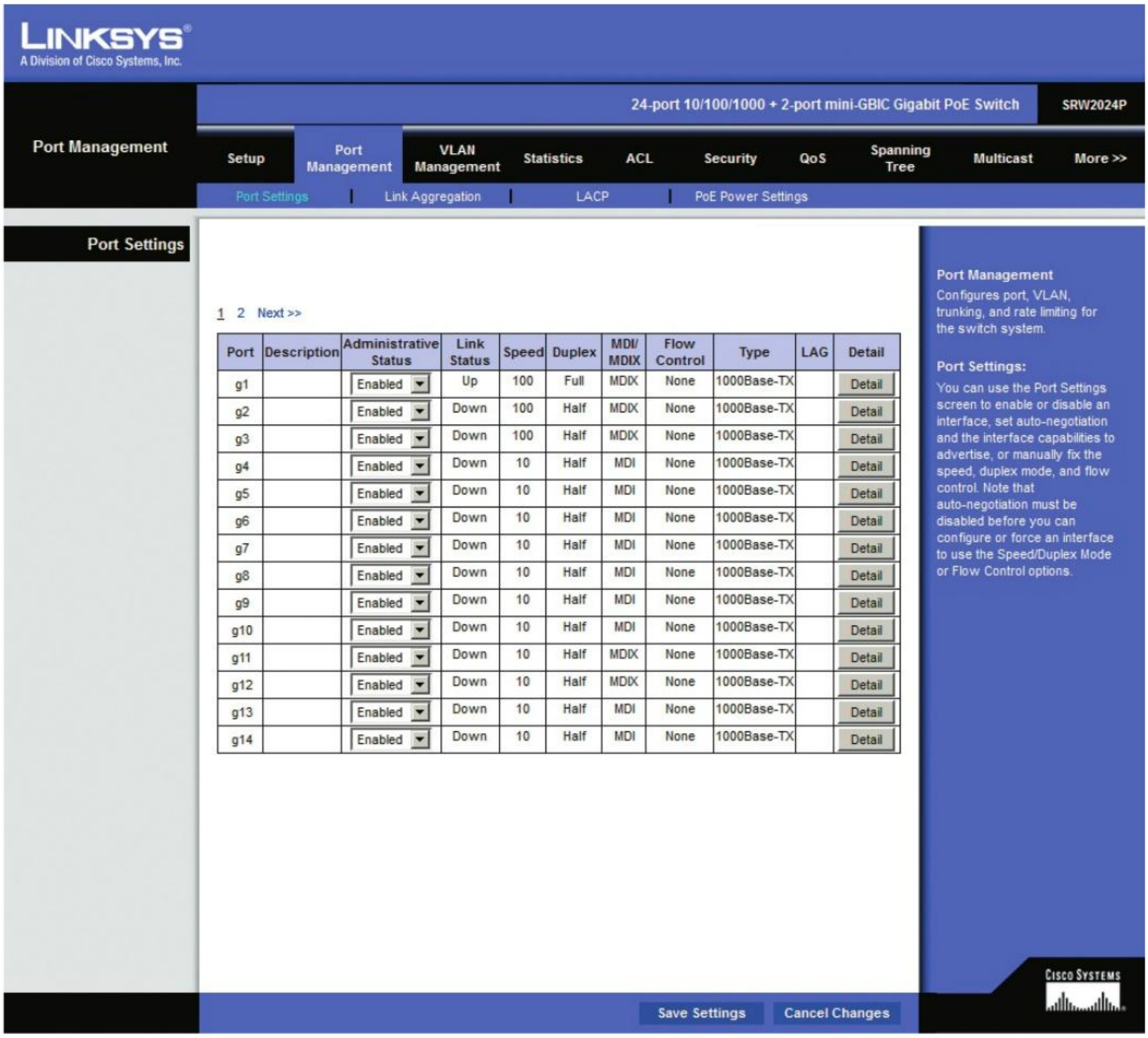
PRZYKŁAD 52.3

Konfigurowanie szybkości i trybu pracy interfejsu

Aby skonfigurować prędkość i tryb pracy interfejsu bez autonegocjacji, należy wykonać następujące czynności:

1. Połączyć komputer z przełącznikiem i nawiązać sesję.
2. W trybie konfiguracji globalnej wybrać interfejs, który będzie konfigurowany, np. za pomocą polecenia **interface fastEthernet 0/1**. Można również wybrać grupę interfejsów za pomocą polecenia **interface range fastEthernet 0/4 - 10** – pozwoli to na jednoczesne konfigurowanie interfejsów od 4 do 10.
3. Wpisać polecenie **duplex half**, aby ustawić tryb pracy interfejsu na „half duplex".
4. Wpisać polecenie **speed 10**, aby ustawić prędkość pracy interfejsu na 10 Mb/s.
5. Podłączyć komputer do interfejsu i sprawdzić, czy połączenie zostanie nawiązane, w jakim trybie i z jaką prędkością.

Tryb pracy portów przełącznika i ich szybkość można konfigurować również za pomocą interfejsu WWW. Na rys. 52.7 przedstawiono okno zarządzania portami w przełączniku firmy Linksys.

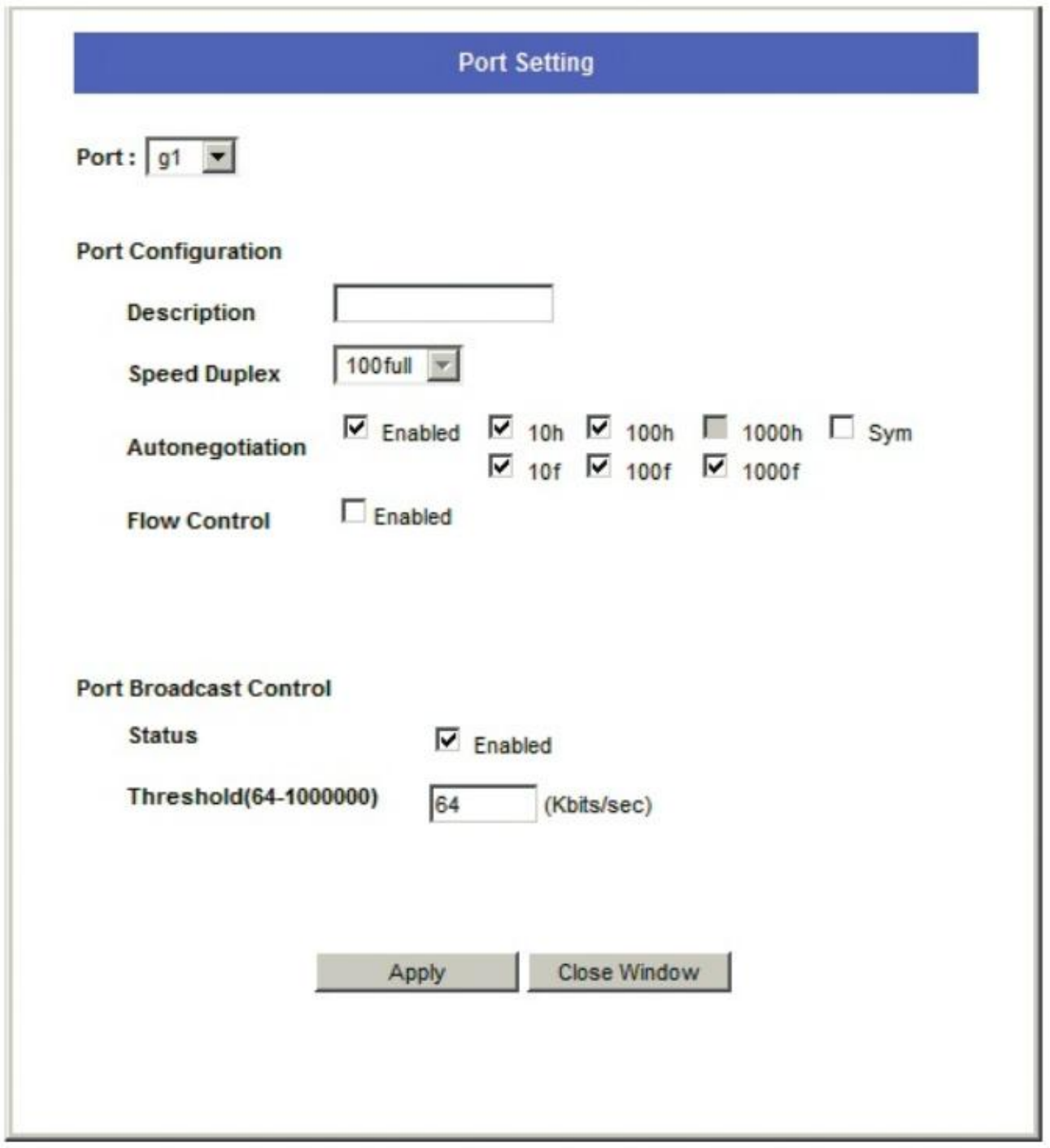


Rys. 52.7. Okno zarządzania portami w przełączniku firmy Linksys

W celu zmiany ustawień portu należy kliknąć przycisk **`Detail`**, a następnie skorzystać z okna konfiguracyjnego i wybrać port oraz jego ustawienia (rys. 52.8).

Każdy przełącznik bada adresy źródłowe ramek odbieranych na portach w celu uzyskania adresów MAC komputerów PC lub stacji roboczych podłączonych do tych portów. Uzyskane w ten sposób adresy MAC (adresy dynamiczne) są zapisywane na tablicach adresów MAC. Ramki zawierające docelowy adres MAC równy adresowi MAC zapisanemu na tablicy mogą zostać przekazane do odpowiedniego interfejsu. W celu wyświetlenia adresów uzyskanych przez przełącznik należy w uprzywilejowanym trybie EXEC użyć polecenia:

```
show mac-address-table
```



Rys. 52.8. Okno konfiguracji parametrów portu w przełączniku firmy Linksys

Aby zachować miejsce w pamięci i zapewnić optymalne działanie przełącznika, uzyskane wpisy zostają automatycznie usunięte z tablicy adresów MAC po upływie określonego czasu. Urządzenia mogą zostać odłączone od portu, wyłączone lub przeniesione do innego portu tego samego lub innego przełącznika. Jeśli w ciągu 300 s nie zostaną odebrane ramki od urządzeń, których adres został uprzednio uzyskany i zapisany na tablicy adresów MAC, wpis dotyczący tego adresu będzie automatycznie usunięty (ulegnie przedawnieniu).

Administratorzy sieci mogą usunąć wpisy za pomocą polecenia:

```
clear mac-address-table
```

Administrator może w sposób trwały przypisać adres MAC do interfejsu. Wtedy:

- określony adres MAC nie ulegnie automatycznie przedawnieniu w przełączniku;
- specyficzny serwer lub określona stacja robocza użytkownika o znanym adresie MAC muszą być podłączone do właściwego portu;
- zostanie podniesiony poziom bezpieczeństwa – przełącznik będzie „wiedział", jakie urządzenie powinno być przyłączone do określonego interfejsu.

Do skonfigurowania statycznego adresu MAC służy polecenie:

```
mac-address-table static <adres mac hosta> interface FastEthernet
<identyfikatorEthernet> vlan <nazwa sieci vlan>
```

Do usunięcia statycznego adresu MAC z przełącznika służy polecenie:

```
no mac-address-table static <adres mac hosta> interface
FastEthernet <identyfikatorEthernet> vlan <nazwa sieci vlan>
```

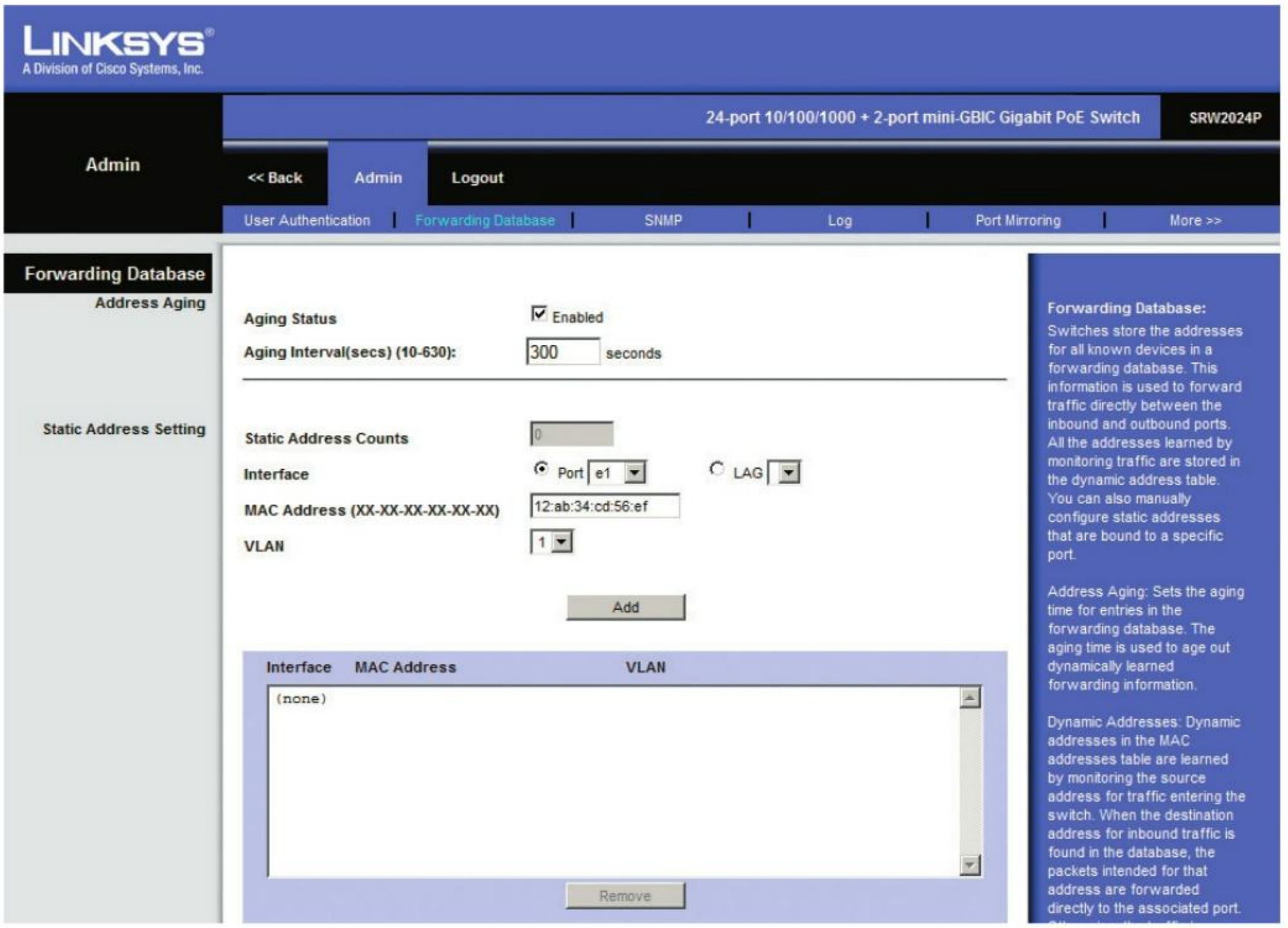
Na rys. 52.9 przedstawiono zawartość tablicy adresów MAC w przełączniku, do którego przyłączono trzy urządzenia (adresy dynamiczne). Następnie wprowadzono adres statyczny dla interfejsu Fa0/1 i ponownie wyświetlono zawartość tablicy. Po wyczyszczeniu tablicy wszystkie wpisy usunięto. Po pewnym czasie, gdy przełącznik otrzyma ramkę od komputera, ponownie umieści odpowiedni wpis dynamiczny na tablicy.

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.c938.7501    DYNAMIC     Fa0/2
   1    0006.2ad5.2801    DYNAMIC     Fa0/1
   1    00d0.bcda.8401    DYNAMIC     Fa0/3
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#mac-address-table static 12.ab.34 vlan 1 interface fast-
Ethernet 0/1
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.c938.7501    DYNAMIC     Fa0/2
   1    0006.2ad5.2801    DYNAMIC     Fa0/1
   1    0012.00ab.0034    STATIC      Fa0/1
   1    00d0.bcda.8401    DYNAMIC     Fa0/3
Switch#clear mac-address-table
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
Switch#
```

Rys. 52.9. Zarządzanie tablicą adresów MAC w przełączniku

Na rys. 52.10. przedstawiono fragment okna, w którym można w sposób statyczny przypisać adresy MAC do poszczególnych portów przełącznika. W przykładzie wykorzystano przełącznik firmy Linksys. Opcje związane z konfiguracją za pomocą interfejsu WWW są dostępne w zakładce **Admin** na podstronie **Forwarding Database**.



Rys. 52.10. Fragment okna konfiguracji statycznych adresów MAC

Każdy użytkownik może podłączyć komputer PC lub laptop do jednego z gniazd okablowania strukturalnego (potencjalny punkt dostępu do sieci, który mogą wykorzystać nieuprawnieni użytkownicy). W przełącznikach można ograniczyć liczbę adresów MAC dla interfejsu. **Bezpieczne adresy MAC** uda się skonfigurować statycznie lub dynamicznie (adres dynamicznie uzyskany przez przełącznik staje się adresem bezpiecznym). Statyczne bezpieczne adresy MAC to adresy skonfigurowane ręcznie za pomocą polecenia:

```
switchport port-security mac-address adres-mac
```

Skonfigurowane w ten sposób adresy MAC są przechowywane na tablicy adresów i dodawane do bieżącej konfiguracji przełącznika. Zabezpieczenia portu ograniczają liczbę adresów MAC obsługiwanych przez port. Jeżeli do zabezpieczonego portu zostaną przypisane bezpieczne adresy MAC, to ten port nie będzie przekazywał pakietów, których adresy źródłowe są spoza grupy zdefiniowanych adresów. Jeśli liczba bezpiecznych adresów MAC zostanie ograniczona do jednego, to podłączona do niego stacja robocza będzie miała zagwarantowaną pełną szerokość pasma właściwą dla tego portu i tylko ta stacja robocza będzie mogła się komunikować za pośrednictwem tego portu przełącznika.

Naruszenie zasad bezpieczeństwa może wystąpić wtedy, gdy do tablicy adresów została dodana maksymalna liczba bezpiecznych adresów MAC, a stacja, której adresu MAC nie ma na tablicy adresów, próbuje uzyskać dostęp do interfejsu. Naruszenie zasad bezpieczeństwa skutkuje zablokowaniem portu – odblokować go może tylko administrator. Odblokowanie portu następuje przez wpisanie polecenia **`shutdown`**, a zaraz po nim – **`no shutdown`** (trzeba je wydać w trybie konfiguracji interfejsu). Procedurę konfiguracji zabezpieczeń portu przedstawiono na rys. 52.11.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 0006.2aca.7235
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#
```

KODY

Rys. 52.11. **Procedura konfiguracji zabezpieczeń portu**

PRZYKŁAD 52.4

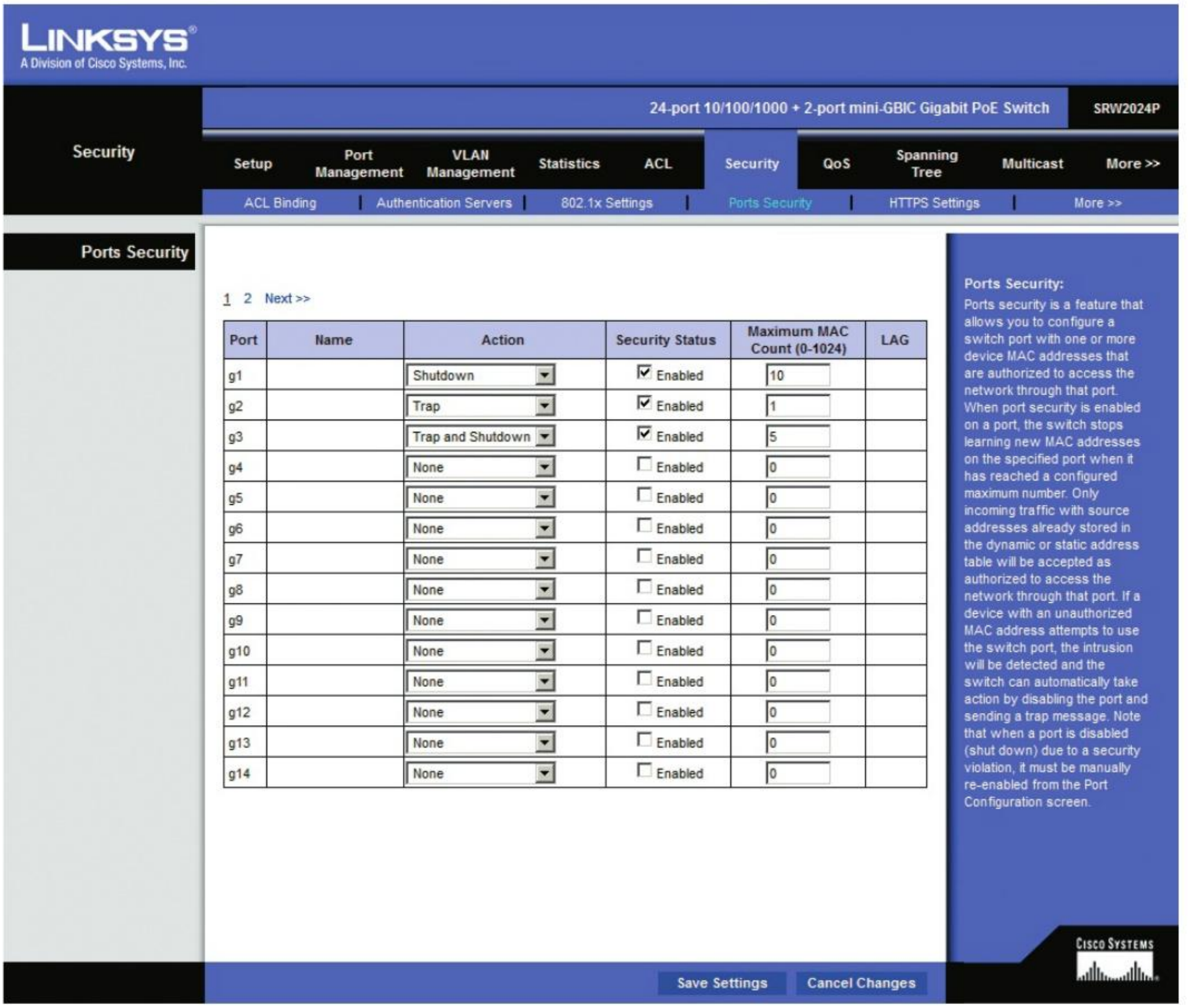
Konfigurowanie bezpieczeństwa portów w przełączniku

Aby skonfigurować możliwość przyłączenia do portu tylko jednego urządzenia, należy wykonać następujące czynności:

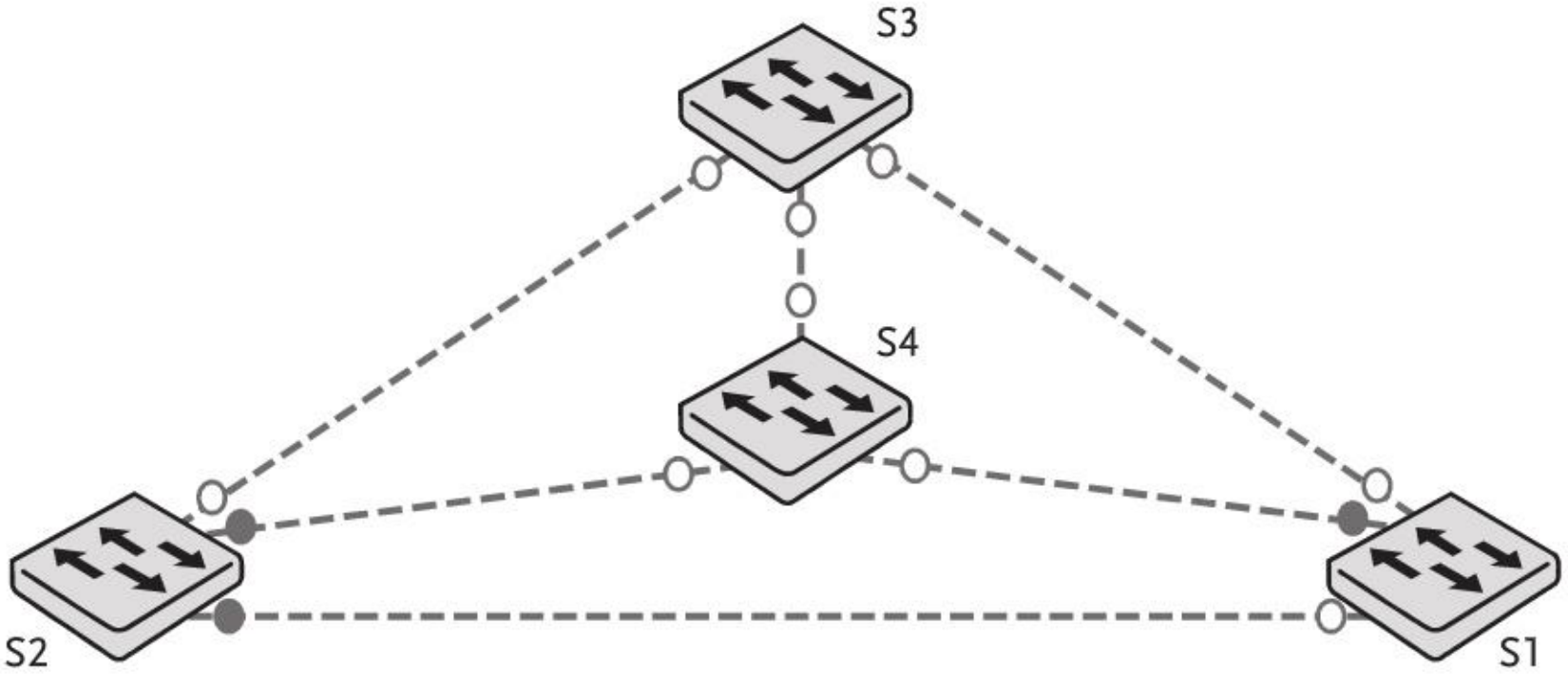
1. Połączyć komputer z przełącznikiem i nawiązać sesję.
2. W trybie konfiguracji globalnej wybrać interfejs, który będzie konfigurowany, np. za pomocą polecenia **`interface fastEthernet 0/2`**.
3. Wpisać polecenie **`switchport mode access`**, aby ustawić tryb pracy interfejsu na dostęp „**`Access`**”.
4. Włączyć funkcję bezpieczeństwa portów poleceniem **`switchport port-security`**.
5. Wpisać polecenie **`switchport port-security mac-address 0006.2aca.7235`**, aby przypisać bezpieczny adres do interfejsu przełącznika (**`0006.2aca.7235`** to MAC adres urządzenia, które może być przyłączone do portu).
6. Wpisać polecenie **`switchport port-security maximum 1`**, aby określić maksymalną liczbę adresów MAC możliwą do zaakceptowania przez przełącznik.
7. Podłączyć inny komputer do interfejsu i sprawdzić, czy procedura bezpieczeństwa zostanie uruchomiona. Informacje o bezpieczeństwie portów można uzyskać po wydaniu polecenia **`show port-security`** w trybie użytkownika uprzywilejowanego.

Przykład konfiguracji bezpieczeństwa portów w przełączniku firmy Linksys za pomocą interfejsu WWW przedstawiono na rys. 52.12. W przykładowym przełączniku opcje bezpieczeństwa portów są dostępne w podstronie **`Security/Port Security`**.

Nadmiarowość jest bardzo ważną i pożądaną cechą sieci. Dzięki niej można uzyskać odporność sieci na awarie. Zapobiega ona utracie dostępu do zasobów w przypadku awarii łącza, portu lub przełącznika. Może jednak powodować problemy związane z występowaniem pętli, które prowadzą do wielokrotnej transmisji ramek i burz rozgłoszeniowych. Załóżmy topologię złożoną z czterech przełączników połączonych „każdy z każdym” przedstawioną na rys. 52.13.



Rys. 52.12. Przykład konfiguracji bezpieczeństwa portów w przełączniku firmy Linksys



Rys. 52.13. Topologia sieci z łączami nadmiarowymi

Załóżmy, że komputer przyłączony do przełącznika S1 wysyła ramkę na adres rozgłoszeniowy. Przełącznik S1 przekaże tę ramkę do wszystkich swoich portów oprócz tego, od którego

ramkę otrzymał. Ramkę otrzymają przełączniki S2, S3 i S4. Teraz każdy z nich zachowa się tak, jak S1 wcześniej, tzn. przekaże ramkę do pozostałych przełączników oprócz tego, od którego ją otrzymał. Ramki będą krążyć w sieci, a ich liczba będzie narastać lawinowo. To spowoduje powstanie burzy rozgłoszeniowej aż do momentu całkowitego zablokowania sieci. Przyczynami burzy rozgłoszeniowej są pętla w topologii i brak na poziomie warstwy drugiej modelu OSI mechanizmu zapobiegającego krążeniu ramki w nieskończoność (w nagłówku pakietu na poziomie warstwy trzeciej znajduje się pole TTL, które zapobiega krążeniu pakietu).

Protokół STP (ang. *Spanning-Tree Protocol*) jest używany w sieciach przełączanych w celu utworzenia topologii logicznej bez pętli, na bazie topologii fizycznej z pętlami. Uzyskuje się to przez blokowanie wybranych portów przełącznika. Po włączeniu przełącznika do sieci protokół STP przez określony czas zbiera informacje o topologii sieci, a następnie wybiera jeden z przełączników, który będzie odgrywał rolę **węzła głównego** (ang. *root*). Właśnie od węzła głównego jest budowane logiczne drzewo, w którym do każdej sieci prowadzi tylko jedna ścieżka. Porty nieleżące na tej ścieżce są blokowane. Na rys. 52.13 za pomocą ciemniejszej kropki zaznaczono porty blokowane przez STP. Informacje o protokole STP można uzyskać za pomocą polecenia **show spanning-tree** w trybie użytkownika uprzywilejowanego. Na rys. 52.14 przedstawiono informacje o protokole STP z przełącznika S2. Strzałką zaznaczono informację o pełnionej funkcji węzła głównego (ang. *root*) i stan portów (FWD – porty otwarte). Na rys. 52.15 pokazano informacje o protokole STP z przełącznika S3. Strzałką zaznaczono informację o adresie MAC węzła głównego (root) i stan portów (FWD – porty otwarte, BLK – porty blokowane).

```
S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.4280.DB3E
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.4280.DB3E
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
S2#
```

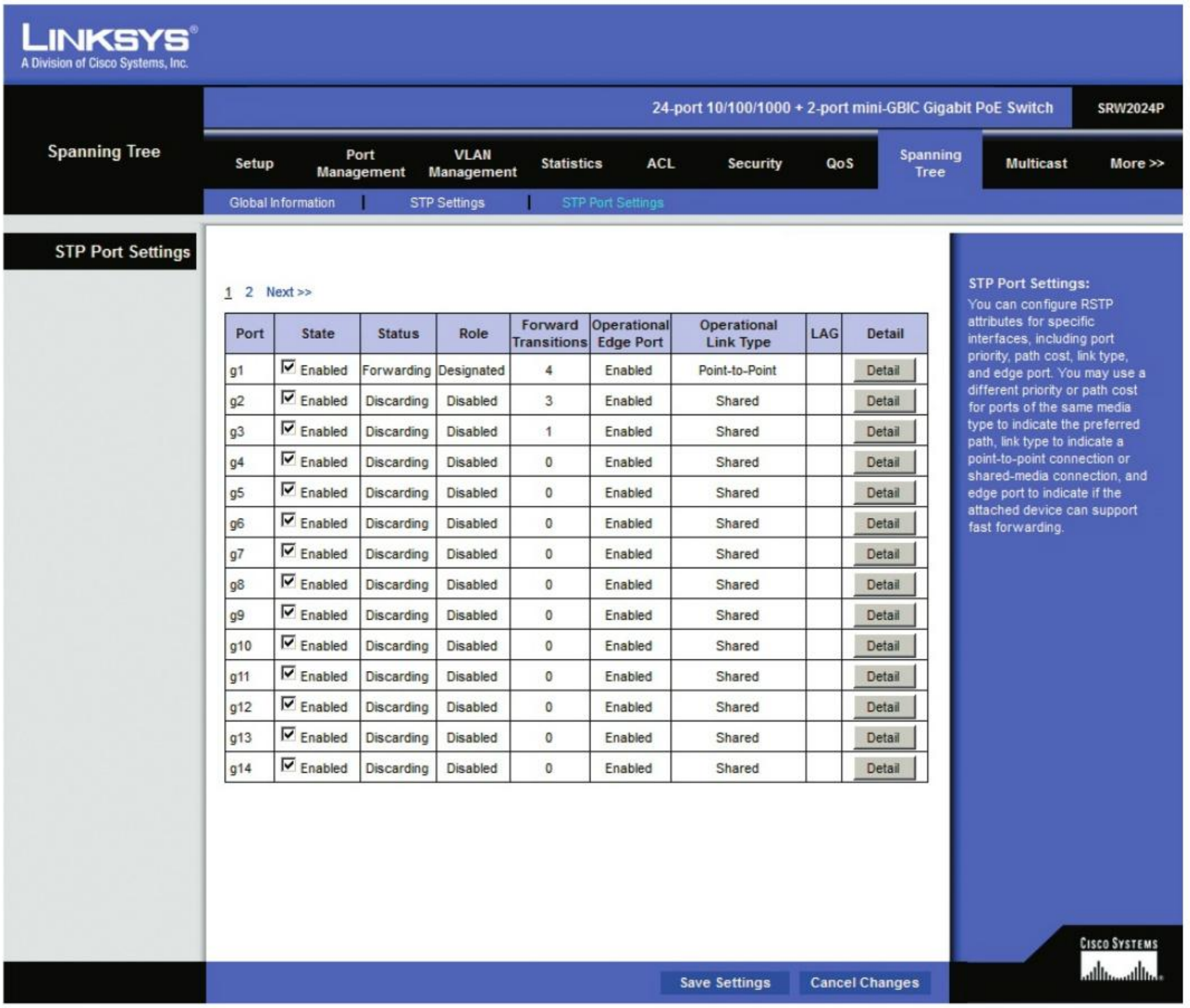
Rys. 52.14. Informacje o protokole STP z przełącznika S2

STP potrzebuje nawet do 50 s na usunięcie pętli, w którym to czasie cały ruch w sieci jest blokowany. Aby wyeliminować tę niedogodność, wprowadzono nowszą odmianę protokołu – **RSTP** (ang. *Rapid Spanning-Tree Protocol*).

> **! UWAGA**
>
> Wprowadzenie łączy nadmiarowych w przełącznikach nieobsługujących protokołu STP spowoduje burzę rozgłoszeniową i niestabilną pracę lub całkowite zablokowanie sieci. Aby przerwać burzę rozgłoszeniową, należy wyłączyć przełącznik lub łącze wprowadzające do topologii pętle.

```
S3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.4280.DB3E
              Cost        19
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.FFE3.5B1B
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Altn BLK 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
S3#
```

Rys. 52.15. Informacje o protokole STP z przełącznika S3



Rys. 52.16. Informacje o protokole STP uzyskane za pomocą interfejsu WWW

Informacje o protokole STP uzyskane za pomocą interfejsu WWW w przykładowym przełączniku firmy Linksys przedstawiono na rys. 52.16. Opcje konfiguracji są dostępne w zakładce **`Spanning-Tree`** w podstronie **`STP Port Settings`**.

Porty w przełączniku mogą przesyłać dane z określoną prędkością. Czasami ta prędkość jest niewystarczająca. Wtedy można połączyć kilka portów fizycznych w jeden port logiczny. Taką opreację nazywa się **agregacją portów**. Przykładowo: zagregowanie 8 portów o przepustowości 1 Gb/s pozwoli na utworzenie łącza logicznego o przepustowości 8 Gb/s. Uzyskuje się dzięki temu **nadmiarowość** (redundancję) połączeń, minimalizującą ryzyko braku komunikacji w razie uszkodzenia jednego z przewodów łączących urządzenia. Algorytm Spanning-Tree traktuje takie zagregowane łącze jak pojedynczy port i nie blokuje poszczególnych portów wchodzących w skład łącza.

Do agregacji można wykorzystać protokół **PAgP** (ang. *Port Aggregation Protocol*) lub **LACP** (ang. *Link Aggregation Control Protocol*). Protokół PAgP należy do CISCO i jest on wspierany tylko na urządzeniach tej firmy, natomiast LACP jest standardem otwartym, z którego mogą korzystać wszystkie urządzenia (w tym również urządzenia CISCO).

Podczas agregowania portów należy pamiętać o następujących zasadach:

- Porty muszą pracować z tą samą szybkością (nie można łączyć ze sobą portów np. 100 Mb/s i 1 Gb/s) i działać w trybie pełnego duplexu.
- Maksymalnie można utworzyć na przełączniku 6 grup portów, przy czym maksymalna liczba portów w grupie wynosi 8 (16 przy zastosowaniu protokołu LACP).
- Ze względu na algorytm rozdzielający obciążenia na poszczególne porty korzystniej jest agregować 2, 4 albo 8 portów.

PRZYKŁAD 52.5

Agregacja portów w przełączniku

Aby skonfigurować zagregowane łącze między przełącznikami, należy wykonać następujące czynności:

1. Połączyć przełączniki za pomocą np. 4 portów, jak na rys. 52.17.



Rys. 52.17. **Połączenie przełączników do agregacji portów**

2. Nawiązać komunikację z pierwszym z przełączników.
3. W trybie konfiguracji globalnej wybrać porty, które mają być zagregowane, np. poleceniem **`interface range fastEthernet 0/1-4`**.
4. Zagregować porty za pomocą polecenia **`channel-group 1 mode active`**. Procedurę konfiguracji przedstawiono na rys. 52.18.
5. Zagregować porty na drugim przełączniku.
6. Sprawdzić, czy zostało ustanowione zagregowane połączenie, np. za pomocą polecenia **`show etherchannel port-channel`**.

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastethernet 0/1 - 4
Switch(config-if-range)#channel-group 1 mode active
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

Switch(config-if-range)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

Switch#
```

Rys. 52.18. **Procedura agregacji portów**

KODY

```
Switch#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:00h:08m:06s
Logical slot/port   = 2/1         Number of ports = 4
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state         No of bits
------+------+------+------------------+-----------
  0     00     Fa0/3    Active              0
  0     00     Fa0/1    Active              0
  0     00     Fa0/2    Active              0
  0     00     Fa0/4    Active              0
Time since last port bundled:    00d:00h:08m:06s    Fa0/4
Switch#
```

Rys. 52.19. **Weryfikacja agregacji portów**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Za pomocą polecenia **`ping`** i protokołu ARP zbierz adresy MAC wszystkich komputerów znajdujących się w pracowni. Zabezpiecz „swój” port w przełączniku tak, aby tylko twój komputer mógł uzyskać połączenie. Przetestuj działanie zabezpieczenia.

53 Wirtualne sieci lokalne

ZAGADNIENIA

Rola wirtualnej sieci lokalnej **Metody przydzielania komputerów do sieci wirtualnych** **Sposoby oznaczania ramek przesyłanych w sieciach wirtualnych** **Łącza trunkowe i sposoby ich konfiguracji**

53.1. Wirtualna sieć lokalna

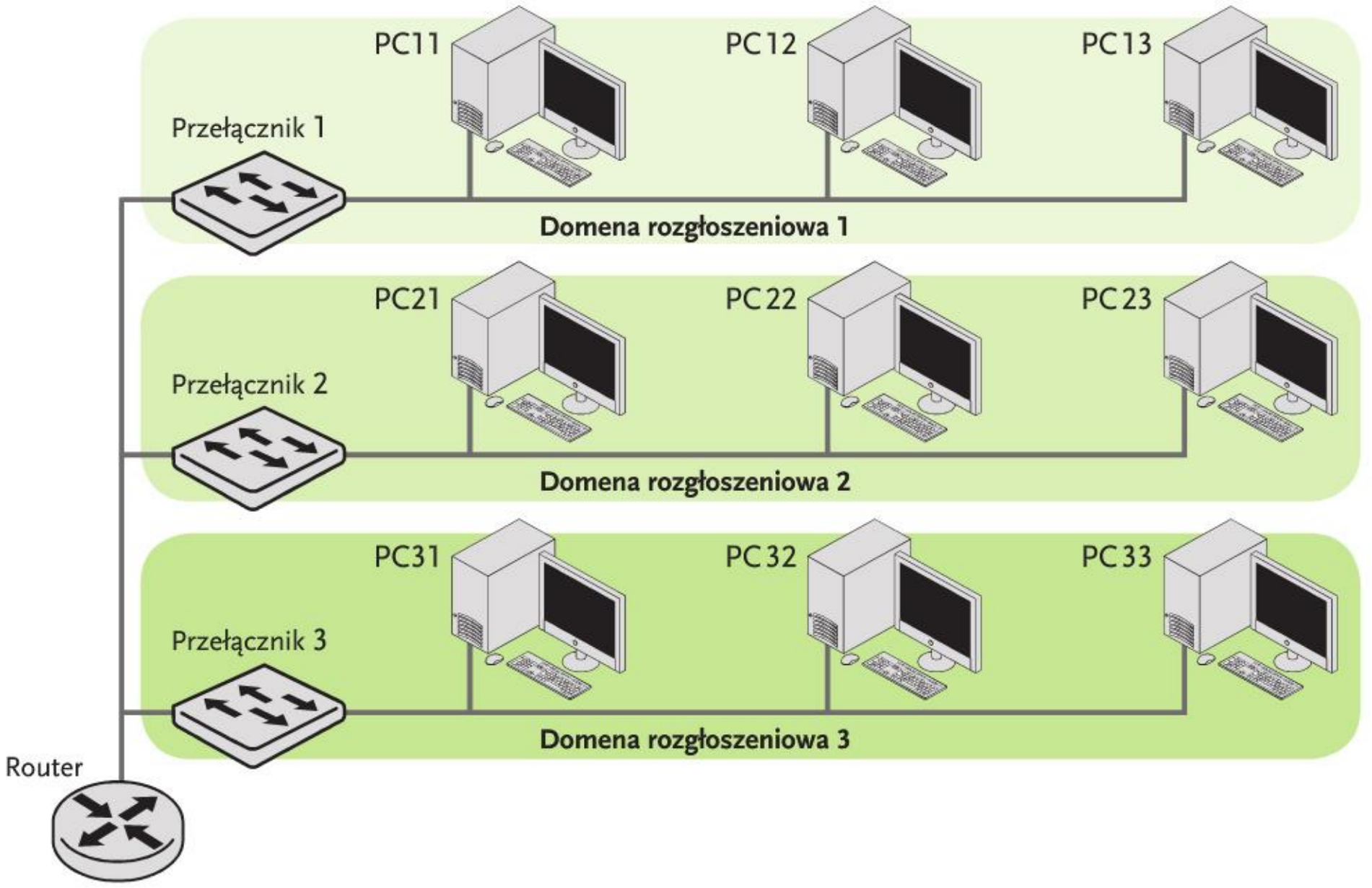
Wirtualna sieć lokalna VLAN (ang. *Virtual Local Area Network*) to sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej. Sieć VLAN jest logiczną grupą stacji roboczych i urządzeń sieciowych. Do tworzenia sieci wirtualnych wykorzystuje się konfigurowalne przełączniki. Komunikacja między VLAN-ami, nawet w tej samej sieci fizycznej, jest możliwa tylko za pośrednictwem routera lub przełącznika warstwy trzeciej.

Sieci VLAN można tworzyć na podstawie stanowisk lub departamentów w firmie, niezależnie od miejsca, w którym fizycznie znajdują się użytkownicy, np. do sieci VLAN o nazwie „Ksiegowosc" mogą należeć pracownicy księgowości niezależnie od miejsca, w którym pracują, i od przełącznika, do którego są przyłączeni. Użytkownicy mogą komunikować się z innymi w tej samej sieci VLAN, lecz ruch między sieciami VLAN jest ograniczony. Przełączniki przekazują ruch **transmisji pojedynczej** (ang. *unicast*), **rozsyłania grupowego** (ang. *multicast*) i **rozgłaszania** (ang. *broadcast*) tylko w tych sieciach VLAN, do których ruch ten należy.

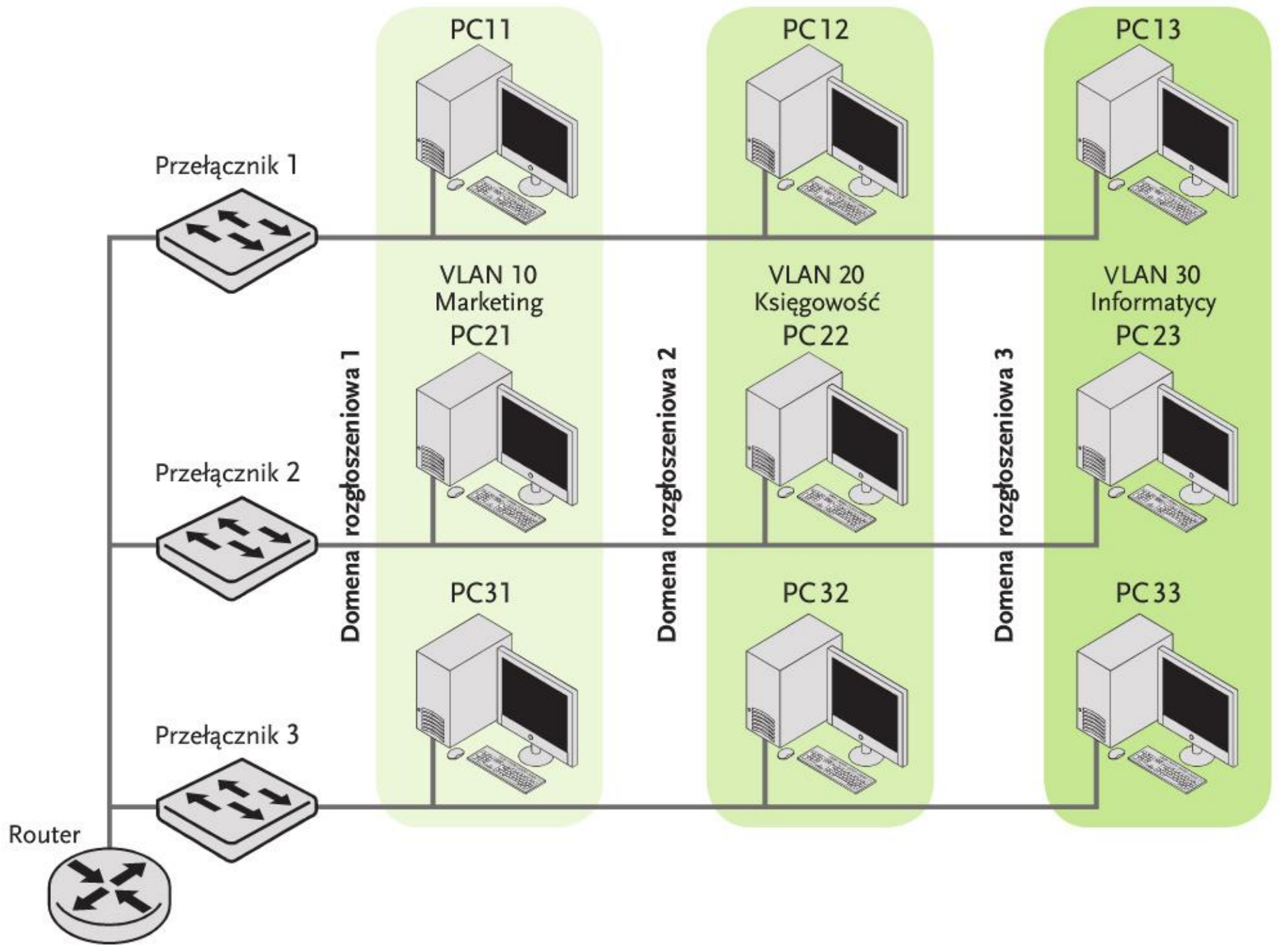
Sieci VLAN zwiększają ogólną wydajność sieci przez logiczne grupowanie zasobów sieci i ograniczenie ruchu rozgłoszeniowego – każda sieć VLAN stanowi odrębną domenę rozgłoszeniową obejmującą jeden lub więcej przełączników. Konfigurowanie sieci VLAN odbywa się na drodze programowej i nie wymaga fizycznego przenoszenia lub podłączania sprzętu sieciowego. Jeżeli w sieci istnieje urządzenie, które nie obsługuje technologii sieci wirtualnych, to dane dla niego są przesyłane przez **VLAN natywny** (ang. *native VLAN*). Z VLAN-u natywnego korzystają również inne protokoły sieciowe wykorzystywane do komunikacji między urządzeniami sieciowymi.

Na rys. 53.1 przedstawiono standardową konfigurację sieci złożonej z trzech domen – urządzenia przyłączone do przełącznika stanowią domenę rozgłoszeniową (ograniczoną przez router). Do danej domeny należą urządzenia przyłączone do konkretnego przełącznika, czyli najczęściej przyłączone do tego samego punktu dystrybucyjnego obsługującego piętro budynku. Jeśli komputer PC11 zamierza wysyłać dane do PC12, to wysyła ramki do przełącznika 1. Przełącznik przekazuje ramkę do PC12.

Na rys. 53.2 przedstawiono konfigurację sieci, w której wydzielono sieci VLAN. W tej konfiguracji do domeny rozgłoszeniowej mogą należeć urządzenia przyłączone do dowolnego przełącznika na dowolnym piętrze. Jeśli komputer PC11 w sieci VLAN 10 „Marketing" zamierza wysyłać dane do PC12 w sieci VLAN 20 „Ksiegowosc", to wysyła ramki przez sieć i VLAN 10 do przełącznika 1. Przełącznik nie może przekazać ramek do innej sieci VLAN (mimo że



Rys. 53.1. **Standardowy podział na domeny rozgłoszeniowe**



Rys. 53.2. **Podział sieci na domeny rozgłoszeniowe realizowany przez sieci VLAN**

PC11 i PC12 są przyłączone do tego samego przełącznika, ale do różnych sieci VLAN), więc wysyła je do routera. Router podejmuje decyzję o przesłaniu danych do innej sieci i przesyła je z powrotem do przełącznika 1 (ale za pośrednictwem sieci VLAN 20). Przełącznik przekazuje ramkę do PC12.

Przynależność stacji roboczych do sieci wirtualnych może być:

- **statyczna** (na podstawie portów) – konfiguracja przełącznika polega na przypisaniu poszczególnych portów do sieci wirtualnych. Gdy urządzenie jest dołączane do sieci, automatycznie przyjmuje ono członkostwo w sieci VLAN tego portu, do którego zostało podłączone. Domyślną siecią VLAN dla każdego portu przełącznika jest sieć VLAN zarządzania (VLAN 1). Tej sieci nie można usunąć. Aby móc zarządzać przełącznikiem, do sieci VLAN 1 musi być przypisany co najmniej jeden port;
- **dynamiczna** – sieci VLAN są tworzone przez specjalne oprogramowanie zarządzające siecią, np. CiscoWorks 2000 lub CiscoWorks for Switched Internetworks. Dynamiczne sieci VLAN mogą przyjmować członkostwo w sieciach VLAN na podstawie adresu MAC. Gdy urządzenie jest podłączane do sieci, przełącznik wysyła zapytanie do oprogramowania zarządzającego i sprawdza w bazie danych, do której sieci VLAN należy to urządzenie przydzielić. Innym, podobnym rozwiązaniem jest przydzielanie urządzeń do sieci VLAN na podstawie adresu IP urządzenia, adresu podsieci lub używanej wersji protokołu.

Wszystkie ramki przesyłane w sieciach wirtualnych są znakowane. Istnieją dwie główne metody znakowania ramek:

- **ISL** (ang. *Inter-Switch Link*) – protokół nie jest obecnie zalecany;
- **802.1Q** – stosuje specjalne oznaczanie ramek (tagowanie) identyfikatorem konkretnej sieci VLAN.

Po odebraniu ramki z dowolnego urządzenia końcowego przełącznik do każdego nagłówka dodaje unikalny identyfikator (informacje określają członkostwo ramki w konkretnej sieci VLAN). Następnie ramka jest przekazywana do kolejnych przełączników lub routerów. W ostatnim przełączniku przed węzłem docelowym identyfikator sieci VLAN jest usuwany i ramka przekazywana do urządzenia.

Sieci VLAN mogą być oznaczane identyfikatorami z zakresu **normalnego** od 1 do 1005 lub **rozszerzonego** od 1006 do 4094. Identyfikatory od 1002 do 1005 są zarezerwowane dla sieci Token Ring i FDDI. Sieci VLAN 1 i te od 1002 do 1005 są tworzone automatycznie i nie mogą być skasowane. Sieci z zakresu normalnego i rozszerzonego są przechowywane w pamięci przełącznika w różny sposób, ponadto nie wszystkie przełączniki obsługują zakres rozszerzony. W niektórych przełącznikach liczba obsługiwanych sieci VLAN jest mniejsza ze względu na ograniczenia pamięci.

PRZYKŁAD 53.1

Zarządzanie sieciami wirtualnymi w przełączniku

W tym ćwiczeniu zostaną utworzone trzy wirtualne sieci: VLAN 10 Uczniowie, VLAN 20 Nauczyciele i VLAN 30 Administracja. Do każdej z sieci zostanie przypisanych po 8 portów. Aby utworzyć w przełączniku sieci wirtualne i przydzielić do nich porty, należy wykonać następujące czynności:

1. Połączyć komputer z przełącznikiem i nawiązać sesję.
2. W globalnym trybie konfiguracyjnym wydać polecenie **`vlan 10`** – zostanie utworzona sieć wirtualna VLAN 10 – a następnie wydać polecenie **`name Uczniowie`**, nadające jej nazwę. Za pomocą polecenia **`exit`** powrócić do trybu konfiguracji globalnej.

3. Powtórzyć operację z punktu 2 dla sieci **`VLAN 20 Nauczyciele i VLAN 30 Administracja`**.
4. Za pomocą polecenia **`interface range fastEthernet 0/1 - 8`** wybrać tryb konfiguracji portów od 1 do 8.
5. Za pomocą polecenia **`switchport mode access`** ustawić porty na pracę w trybie dostępowym.
6. Za pomocą polecenia **`switchport access vlan 10`** przydzielić porty do sieci **`VLAN 10`**.
7. Powtórzyć operację z punktów od 4. do 6. dla sieci **`VLAN 20 Nauczyciele`** i **`VLAN 30 Administracja`**.
8. Za pomocą polecenia **`end`** powrócić do trybu użytkownika uprzywilejowanego.
9. Za pomocą polecenia **`show vlan`** zweryfikować poprawność konfiguracji.

Na rys. 53.3 przedstawiono przebieg konfiguracji sieci VLAN, a na rys. 53.4 – wykaz utworzonych sieci i porty przypisane do tych sieci.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Uczniowie
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Nauczyciele
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Administracja
Switch(config-vlan)#exit
Switch(config)#interface range fastEthernet 0/1 - 8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/9 - 16
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/17 - 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#
```

Rys. 53.3. **Przebieg konfiguracji sieci VLAN**

KODY

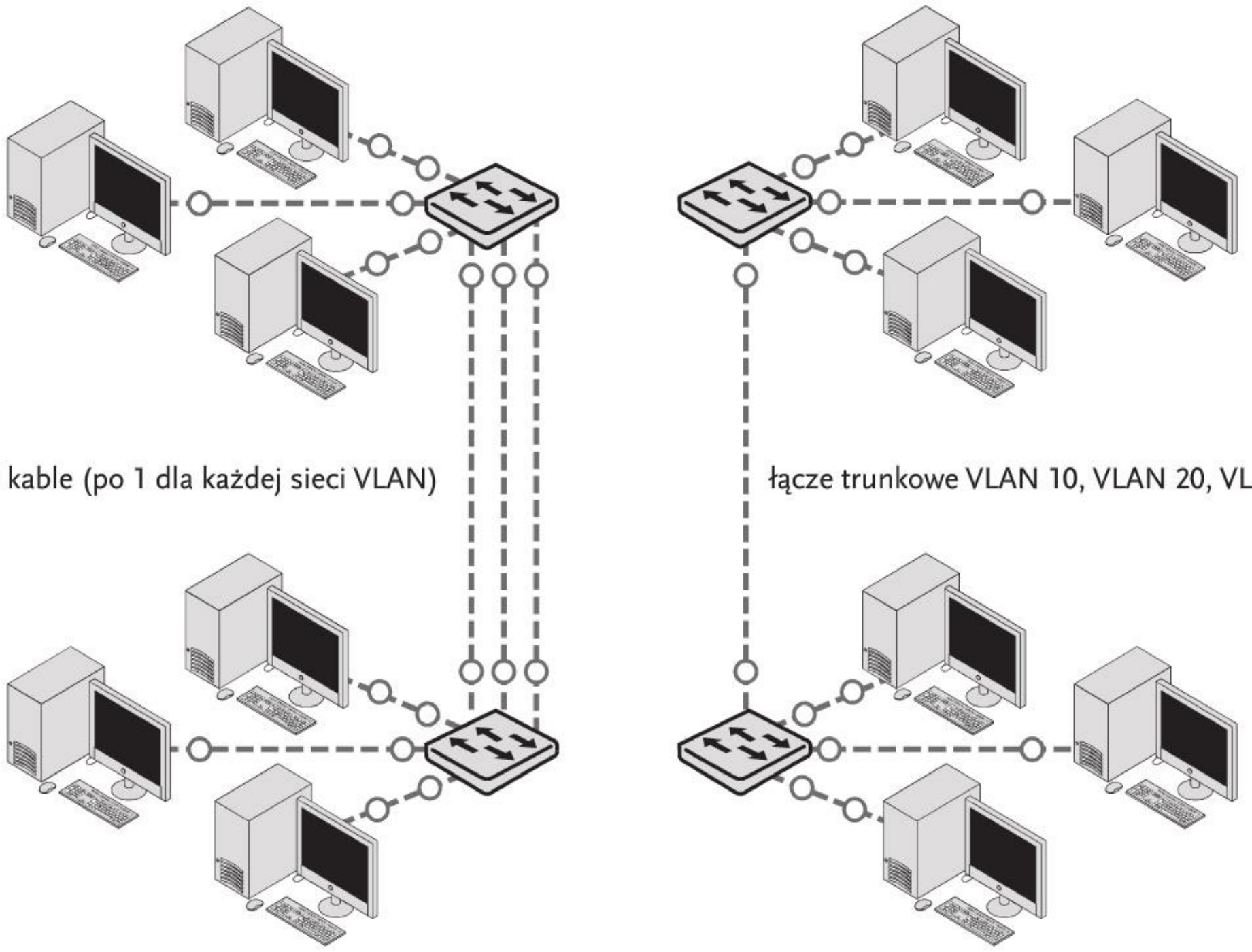
```
Switch#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active
10   Uczniowie                        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
20   Nauczyciele                      active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
30   Administracja                    active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001  1500  -      -      -        -    -        0      0
10   enet  100010  1500  -      -      -        -    -        0      0
20   enet  100020  1500  -      -      -        -    -        0      0
30   enet  100030  1500  -      -      -        -    -        0      0
1002 fddi  101002  1500  -      -      -        -    -        0      0
1003 tr    101003  1500  -      -      -        -    -        0      0
1004 fdnet 101004  1500  -      -      -        ieee -        0      0
1005 trnet 101005  1500  -      -      -        ibm  -        0      0
Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Switch#
```

Rys. 53.4. **Wykaz utworzonych sieci i porty przypisane do tych sieci**

Aby zapewnić możliwość komunikowania się między stacjami przyłączonymi do różnych przełączników, dla każdej sieci wirtualnej należałoby przeznaczyć oddzielny kabel łączący przełączniki. Przykładowo: w sieci, w której zdefiniowano trzy sieci wirtualne, przełączniki należałoby połączyć trzema kablami. Dla większej liczby sieci wirtualnych (a maksymalnie może ich być ponad 4000) zadanie byłoby niewykonalne. Aby temu zapobiec i ograniczyć liczbę portów oraz kabli łączących przełączniki, wprowadzono **połączenia trunkowe**. Pozwalają one na przesyłanie jednym kablem ramek pochodzących od wielu sieci wirtualnych. Na rys. 53.5 przedstawiono przykład łączenia przełączników z wykorzystaniem łączy trunkowych (schemat po prawej stronie) i bez łączy trunkowych (schemat po lewej).



Rys. 53.5. **Porównanie sposobu łączenia przełączników**

PRZYKŁAD 53.2

Tworzenie połączenia trunkowego

Aby utworzyć na porcie 24 połączenie trunkowe obsługujące sieci wirtualne VLAN 10, 20 i 30, należy wykonać następujące czynności:

1. Połączyć komputer z przełącznikiem i nawiązać sesję.
2. Wpisać polecenie **`interface fastEthernet 0/24`**, aby wybrać tryb konfiguracji portu 24.
3. Wpisać polecenie **`switchport mode trunk`**, aby ustawić port na pracę w trybie trunkowym.
4. Wpisać polecenie **`switchport trunk allowed vlan add 10`**, aby dodać sieć VLAN 10 do listy obsługiwanych sieci (opcja **`all`** dodaje wszystkie sieci VLAN). Analogicznie dodać do listy obsługiwanych sieci **`VLAN20`** i **`VLAN30`**.
5. Wpisać polecenie **`end`**, aby powrócić do trybu użytkownika uprzywilejowanego.
6. Wpisać polecenie **`show interfaces trunk`**, aby zweryfikować poprawność konfiguracji.
7. Analogicznie skonfigurować port w drugim przełączniku.

Na rys. 53.6 przedstawiono przebieg konfiguracji łącza trunkowego.

KODY

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet 0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10
Switch(config-if)#switchport trunk allowed vlan add 20
Switch(config-if)#switchport trunk allowed vlan add 30
Switch(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/24      1-1005

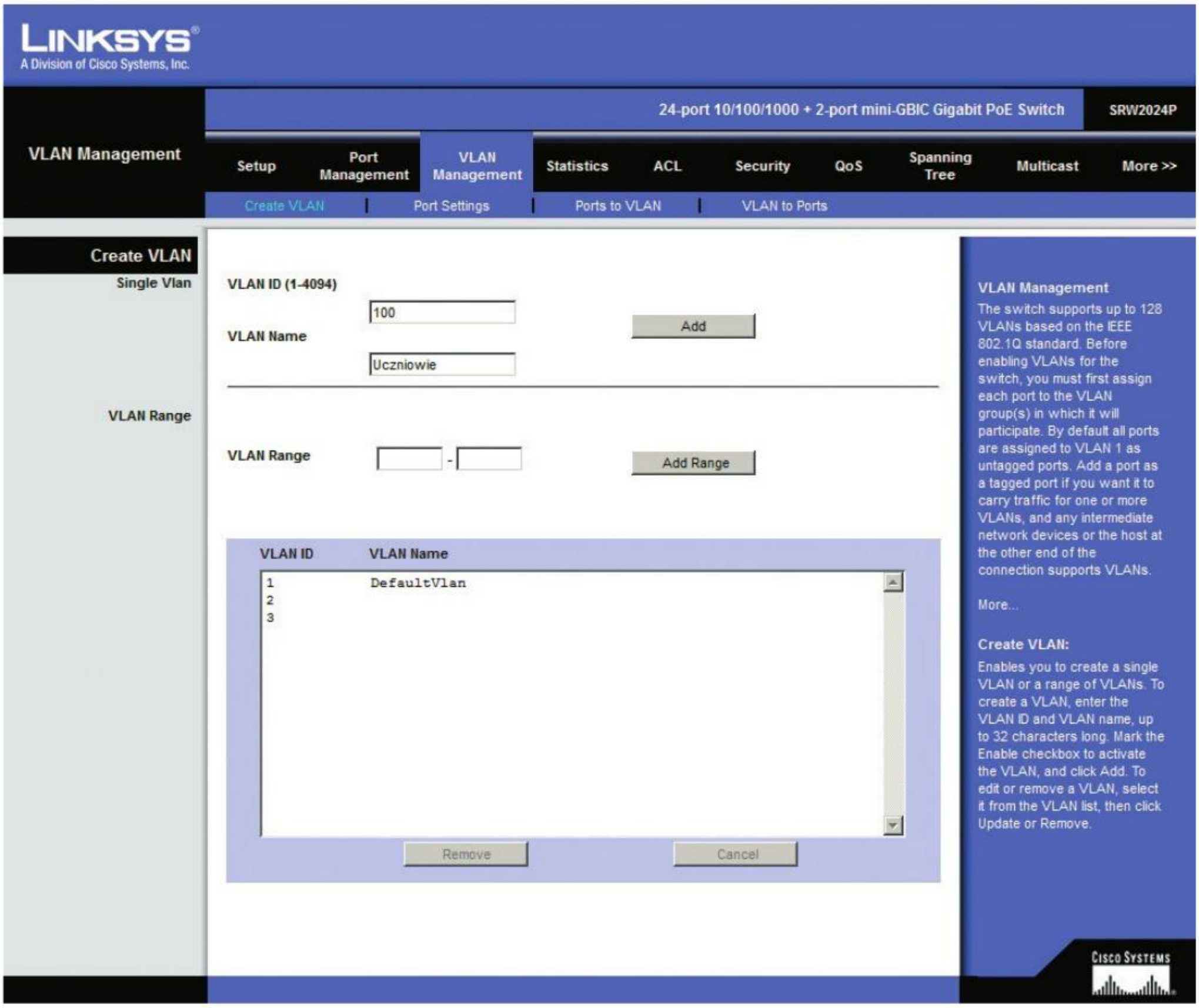
Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1
Switch#
```

Rys. 53.6. Przebieg konfiguracji łącza trunkowego

Na rys. 53.7 przedstawiono okno interfejsu WWW, w którym na przełączniku firmy Linksys można skonfigurować wirtualne sieci. Aby dodać lub usunąć z przełącznika sieć wirtualną, należy wybrać zakładkę **VLAN Management** i w podstronie **Create VLAN** wprowadzić zmiany.

Po utworzeniu sieci wirtualnych na przełączniku można przydzielić porty do poszczególnych sieci. W tym celu w zakładce **VLAN Management** można wybrać podstronę **VLAN to Ports** i dla poszczególnych portów kliknąć przycisk **Join VLAN**, aby przypisać numer sieci VLAN. Porty pracujące w trybie **Access** mogą być przydzielone tylko do jednej sieci wirtualnej, natomiast porty pracujące w trybie **Trunk** mogą obsługiwać wiele sieci wirtualnych. Fragment okna pozwalającego na przypisanie portów do sieci VLAN przedstawiono na rys. 53.8.



Rys. 53.7. Okno interfejsu WWW do zarządzania sieciami wirtualnymi

1 2 Next >>

Port	Mode	Join VLAN	VLANs	LAG
g1	Access	Join VLAN	1U	
g2	Access	Join VLAN	1U	
g3	Access	Join VLAN	1U	
g4	Access	Join VLAN	1U	
g5	Access	Join VLAN	1U	
g6	Access	Join VLAN	1U	
g7	Access	Join VLAN	1U	
g8	Access	Join VLAN	2U	
g9	Access	Join VLAN	2U	
g10	Access	Join VLAN	2U	
g11	Trunk	Join VLAN	1U	
g12	Trunk	Join VLAN	1U	
g13	Access	Join VLAN	2U	
g14	Access	Join VLAN	2U	

Rys. 53.8. Fragment okna pozwalającego na przypisanie portów do sieci VLAN

53.2. Routing między wirtualnymi sieciami lokalnymi

Przełącznik stosuje **oznaczanie – tagowanie** (ang. *tagging*) ramek należących do poszczególnych sieci wirtualnych i kontroluje ich przekazywanie. Urządzenia mogą komunikować się bezpośrednio tylko w tej samej sieci VLAN. Komunikacja między VLAN-ami, nawet w tej samej sieci fizycznej, jest możliwa tylko za pośrednictwem routera lub przełącznika warstwy trzeciej.

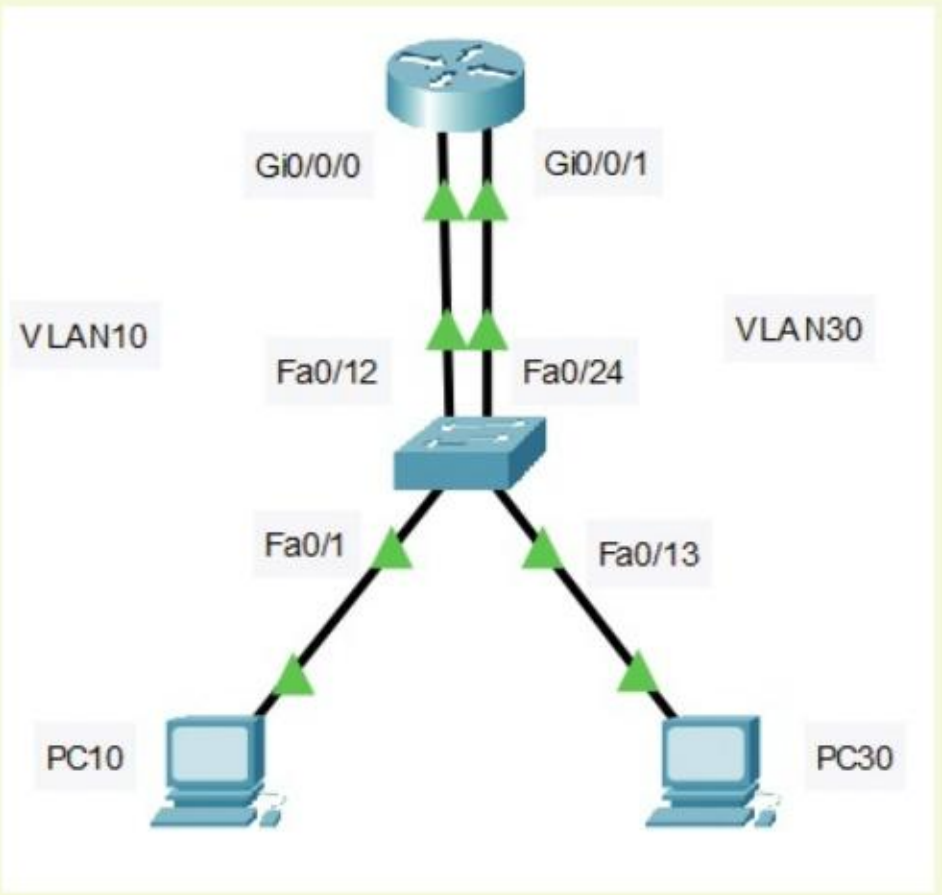
Tradycyjny routing między sieciami VLAN polega na zestawieniu osobnego fizycznego łącza między routerem a przełącznikiem dla każdej z sieci VLAN.

PRZYKŁAD 53.3

Tradycyjny routing między sieciami VLAN

W tym ćwiczeniu zostaną utworzone dwie wirtualne sieci: VLAN10 – Uczniowie i VLAN30 – Nauczyciele. Do sieci VLAN10 na przełączniku zostaną przypisane porty 1–12, a do sieci VLAN30 – porty 13–24. Aby utworzyć w przełączniku sieci wirtualne, przydzielić do nich porty i umożliwić komunikację między sieciami VLAN, należy wykonać następujące czynności:

1. Zbudować sieć według schematu na rys. 53.9. Komputer PC10 przyłączyć do portu należącego do sieci VLAN10, np. do portu 1, komputer PC30 przyłączyć do portu należącego do sieci VLAN30, np. do portu 13. Jeden z portów routera, np. Gi0/0/0, połączyć z portem przełącznika należącym do sieci VLAN10 (np. portem 12), drugi z portów routera, np. Gi0/0/1, połączyć z portem przełącznika należącym do sieci VLAN30 (np. portem 24).



Rys. 53.9. **Tradycyjny routing między sieciami VLAN**

2. Skonfigurować komputer PC10:
   - adres IP: **192.168.10.101**;
   - maska podsieci: **255.255.255.0**;
   - adres bramy: **192.168.10.1**.
3. Skonfigurować komputer PC30:
   - adres IP: **192.168.30.101**;
   - maska podsieci: **255.255.255.0**;
   - adres bramy: **192.168.30.1**.

4. Połączyć komputer z przełącznikiem i nawiązać sesję.
5. Utworzyć sieci wirtualne i przypisać porty.

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name Uczniowie
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Nauczyciele
Switch(config-vlan)#exit
Switch(config)#interface range fastEthernet 0/1 - 12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/13 - 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
```

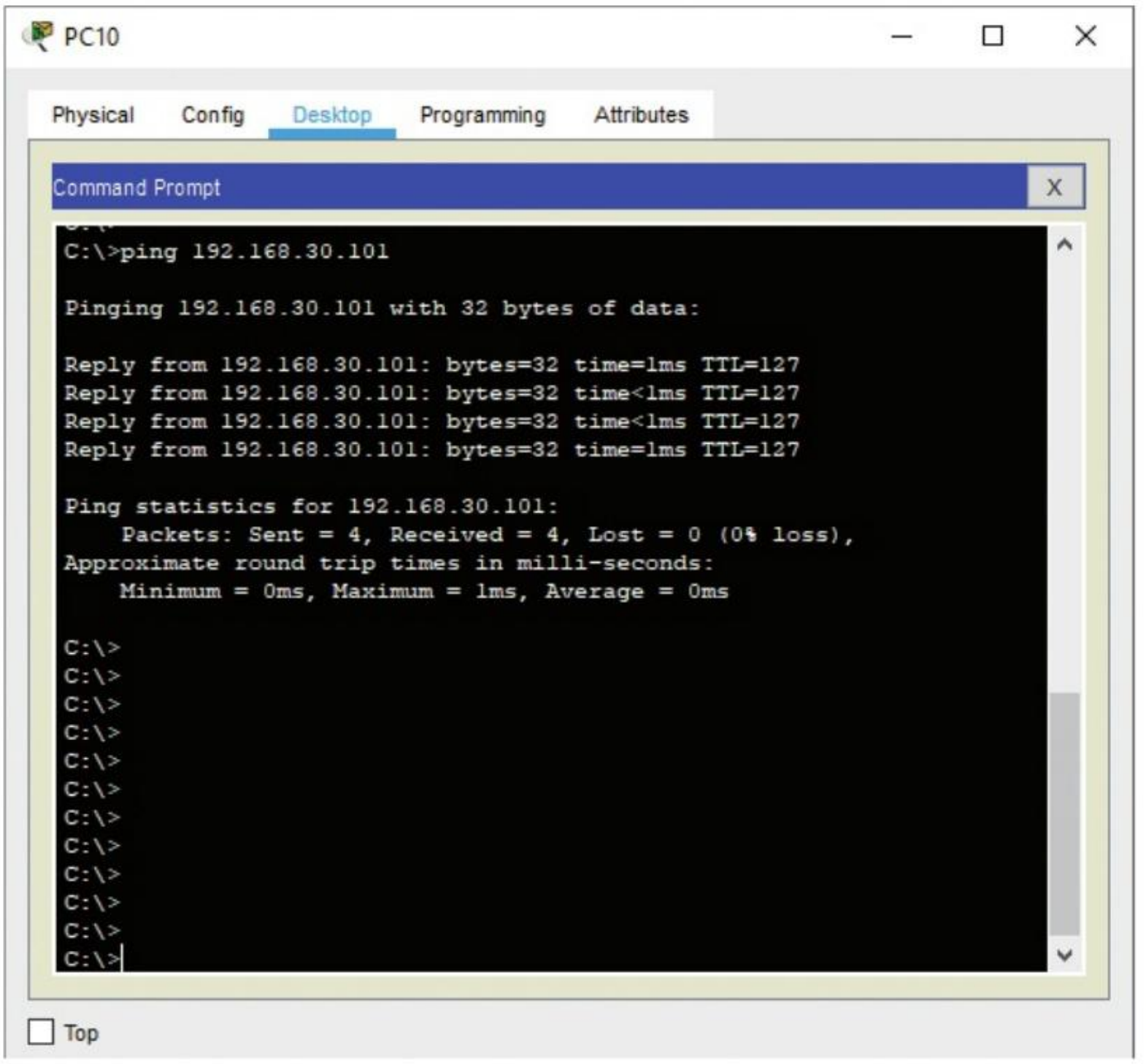
6. Połączyć komputer z routerem i nawiązać sesję.
7. Skonfigurować interfejsy.

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/0/1
Router(config-if)#ip address 192.168.30.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

8. Sprawdzić możliwość komunikacji między komputerami, np. **`ping`** z PC10 do PC30 (rys. 53.10).

Wadą tego rozwiązania jest ograniczona liczba interfejsów routera. Może ono być stosowane tylko wtedy, gdy liczba sieci VLAN nie przekracza liczby interfejsów w routerze. Tego ograniczenia można uniknąć, zestawiając połączenie trunkowe między przełącznikiem a routerem. W takim wypadku na interfejsie routera należy utworzyć **podinterfejsy logiczne** (ang. *subinterfaces*). Każdy z podinterfejsów będzie obsługiwał inną sieć VLAN.

KODY



Rys. 53.10. **Testowanie komunikacji między sieciami VLAN**

PRZYKŁAD 53.4

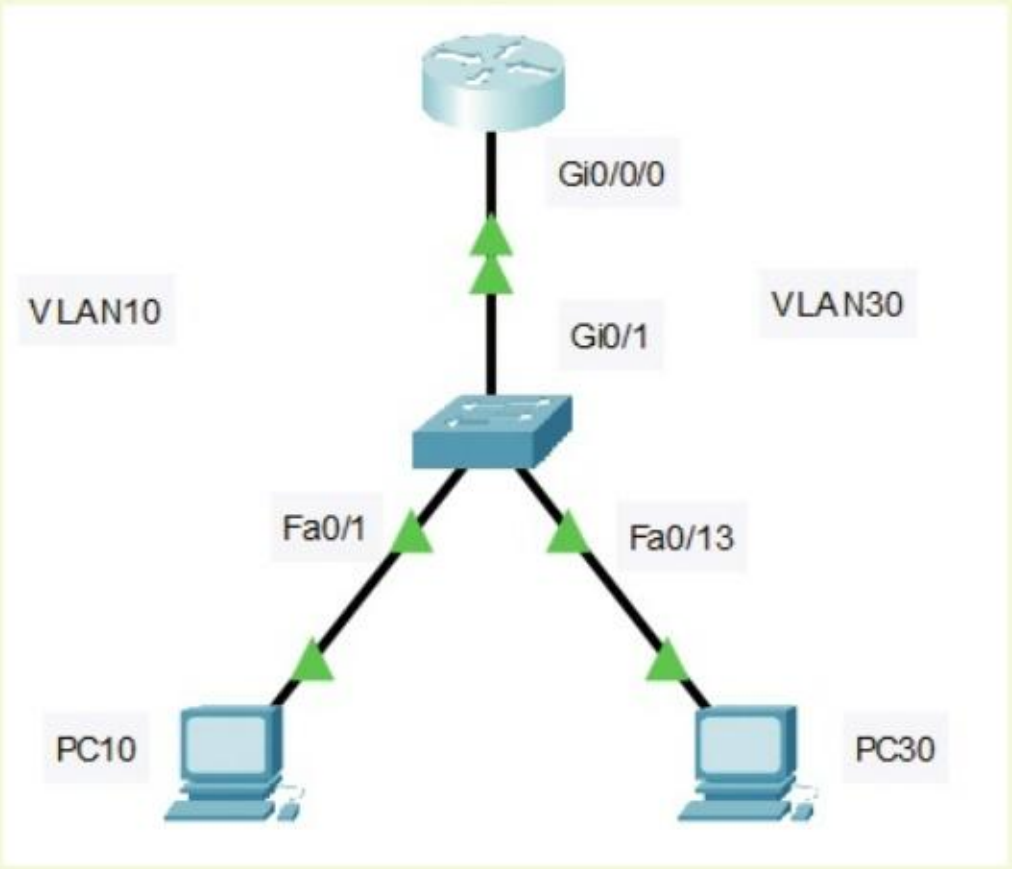
Routing między sieciami VLAN z wykorzystaniem połączenia trunkowego

W tym ćwiczeniu zostaną utworzone dwie wirtualne sieci: VLAN10 – Uczniowie i VLAN30 – Nauczyciele. Do sieci VLAN10 na przełączniku zostaną przypisane porty 1–12, a do sieci VLAN30 – porty 13–24. Aby utworzyć w przełączniku sieci wirtualne, przydzielić do nich porty i umożliwić komunikację między sieciami VLAN, należy wykonać następujące czynności:

1. Zbudować sieć według schematu na rys. 53.11. Komputer PC10 przyłączyć do portu należącego do sieci VLAN10, np. do portu 1, komputer PC30 przyłączyć do portu należącego do sieci VLAN30, np. do portu 13. Port routera, np. Gi0/0/0, połączyć z portem przełącznika nienależącym do sieci VLAN (np. portem GigabitEthernet0/1).
2. Skonfigurować komputery PC10 i PC30, jak w przykładzie 53.3.
3. Połączyć komputer z przełącznikiem i nawiązać sesję. Utworzyć sieci wirtualne i przypisać porty jak w przykładzie 53.3.
4. Skonfigurować interfejs GigabitEthernet0/1 do pracy w trybie trunkowym.

```
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10
Switch(config-if)#switchport trunk allowed vlan add 30
Switch(config-if)#end
```

KODY



Rys. 53.11. **Routing między sieciami VLAN z wykorzystaniem połączenia trunkowego**

5. Połączyć komputer z routerem i nawiązać sesję. Skonfigurować interfejs połączony z przełącznikiem.
   W konfiguracji globalnej wybrać utworzenie podinterfejsu **`gigabitEthernet 0/0/0.10`**, obsługującego sieć VLAN10 (numer podinterfejsu nie musi być taki sam jak numer sieci, ale ułatwia to zarządzanie sieciami).

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0/0.10
```

   Ustawić protokół enkapsulacji ramek na 802.1Q (w skrócie dot1Q) dla sieci VLAN10.

```
Router(config-subif)#encapsulation dot1Q 10
```

   Przypisać adres IP do podinterfejsu.

```
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
```

   Analogicznie skonfigurować podinterfejs dla sieci VLAN30.

```
Router(config)#interface gigabitEthernet 0/0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/0/0
```

   Włączyć interfejs.

```
Router(config-if)#no shutdown
```

6. Sprawdzić możliwość komunikacji między komputerami, np. **`ping`** z PC10 do PC30.

! UWAGA

Jeżeli podinterfejsy są konfigurowane, to interfejs fizyczny nie może mieć przydzielonego adresu IP.

! UWAGA

Włączenie interfejsu fizycznego skutkuje aktywowaniem wszystkich podinterfejsów (nie ma polecenia **`no shutdown`** na podinterfejsach).

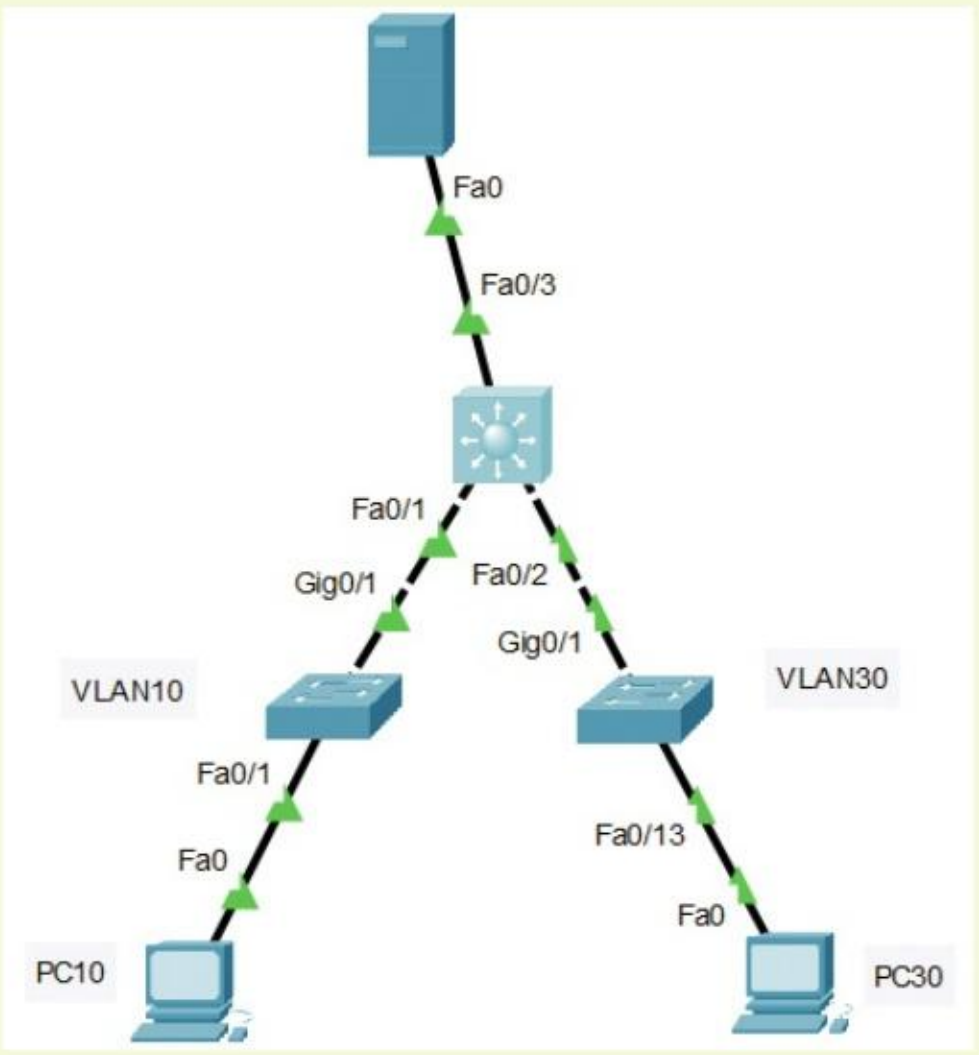
Przełącznik warstwy 3, oprócz funkcji typowego przełącznika warstwy 2, realizuje również funkcję routingu. Ponieważ ma więcej portów niż w typowych routerach, może zapewnić routing między większą liczbą sieci VLAN.

PRZYKŁAD 53.5

Routing między sieciami VLAN z wykorzystaniem przełącznika warstwy 3

W tym ćwiczeniu zostaną utworzone dwie wirtualne sieci: VLAN10 – Uczniowie i VLAN30 – Nauczyciele. Do sieci VLAN10 na przełącznikach warstwy 2 (przełączniki warstwy 2 mają nazwy – odpowiednio – L2_1 i L2_2) zostaną przypisane porty 1–12, a do sieci VLAN30 – porty 13–24. Serwer w sieci **`172.16.0.0/16`** umożliwi testowanie komunikacji. Aby utworzyć w przełączniku sieci wirtualne, przydzielić do nich porty i umożliwić komunikację między sieciami VLAN, należy wykonać następujące czynności:

1. Zbudować sieć według schematu na rys. 53.12. Komputer PC10 przyłączyć do portu należącego do sieci VLAN10, np. do portu 1 w przełączniku L2_1, komputer PC30 przyłączyć do portu należącego do sieci VLAN30, np. do portu 13 w przełączniku L2_2. Port Gi0/1 przełączników warstwy 2 należy przyłączyć do wybranych portów przełącznika L3 (np. do portu 1 i 2). Port 3 przełącznika L3 połączyć z serwerem.



Rys. 53.12. **Routing między sieciami VLAN z wykorzystaniem przełącznika warstwy 3**

2. Skonfigurować komputery PC10 i PC30 jak w przykładzie 53.3.
3. Skonfigurować serwer:
   - adres IP: **`172.16.0.100`**;
   - maska podsieci: **`255.255.0.0`**;
   - adres bramy: **`172.16.0.1`**.

4. Połączyć komputer kolejno z przełącznikami warstwy 2 i nawiązać sesję. Utworzyć sieci wirtualne i przypisać porty (na obu przełącznikach konfiguracja jest taka sama).

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name uczniowie
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name nauczyciele
Switch(config-vlan)#exit
Switch(config)#interface range fastethernet 0/1 - 12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fastethernet 0/13 - 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
```

KODY

5. Skonfigurować interfejs GigabitEthernet0/1 do pracy w trybie trunkowym.

```
Switch(config)#interface GigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10
Switch(config-if)#switchport trunk allowed vlan add 30
Switch(config-if)#end
```

6. Połączyć komputer z przełącznikiem warstwy 3 i nawiązać sesję. Poleceniem **`ip routing`** aktywować funkcje routingu na przełączniku warstwy 3. Utworzyć sieci wirtualne.

```
Switch>enable
Switch#configure terminal
Switch(config)#ip routing
Switch(config)#vlan 10
Switch(config-vlan)#name Uczniowie
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Nauczyciele
Switch(config-vlan)#exit
```

7. Skonfigurować adresy IP dla sieci wirtualnych.

```
Switch(config)#interface Vlan 10
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface Vlan 30
Switch(config-if)#ip address 192.168.30.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

8. Skonfigurować adres IP dla połączenia do serwera. Polecenie **`no switchport`** przełącza port do pracy w warstwie 3.

```
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#no switchport
Switch(config-if)#ip address 172.16.0.1 255.255.0.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

9. Skonfigurować porty 1 i 2 do pracy w trybie trunkowym (połączenie do przełączników L2).

```
Switch(config)#interface range FastEthernet 0/1 - 2
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed vlan add 10
Switch(config-if-range)#switchport trunk allowed vlan add 30
Switch(config-if-range)#exit
```

10. Sprawdzić możliwość komunikacji między komputerami a serwerem, np. **`ping`** z PC10 i PC30 do serwera.

! UWAGA

Niektóre przełączniki warstwy 3, np. serii CISCO C3560CX, mają wszystkie interfejsy w standardzie 1 Gb/s. Jeżeli konfigurujesz taki przełącznik, to w punktach 8. i 9. wybierz odpowiednie oznaczenie interfejsów, np. GigabitEthernet 0/3.

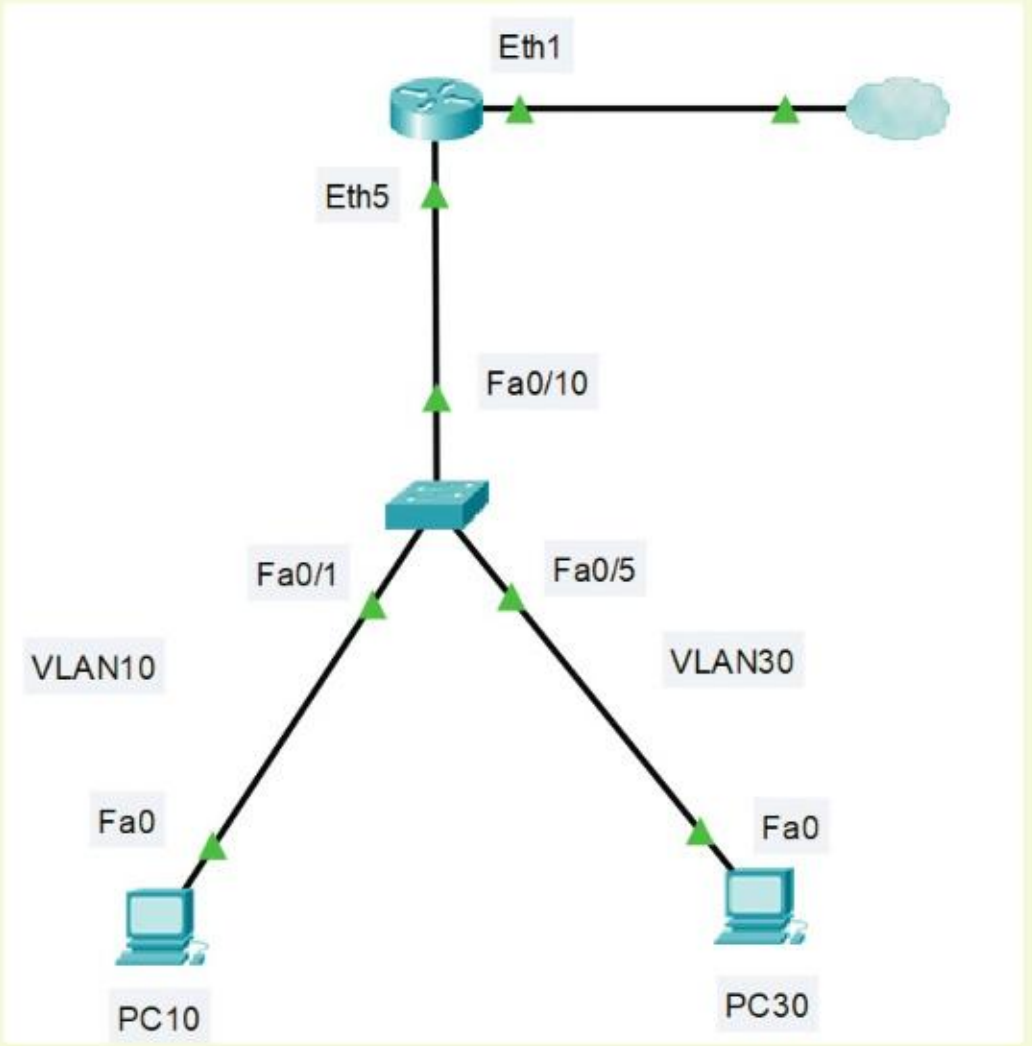
PRZYKŁAD 53.6

Routing między sieciami VLAN z wykorzystaniem routera Mikrotik

W tym ćwiczeniu zostaną utworzone dwie wirtualne sieci: VLAN10 – Uczniowie z adresami **`192.168.10.0/24`** i VLAN30 – Nauczyciele z adresami **`192.168.30.0/24`**. Do sieci VLAN10 na przełączniku zostaną przypisane porty 1–4, a do sieci VLAN30 – porty 5–8. Port 10 zostanie skonfigurowany do pracy w trybie trunkowym i połączony z portem 5 routera Mikrotik hAP ac lite. Port 1 routera służy do uzyskania dostępu do internetu. Schemat połączeń przedstawiono na rys. 53.13. Aby utworzyć w przełączniku sieci wirtualne, przydzielić do nich porty i umożliwić komunikację między sieciami VLAN i z internetem, należy wykonać następujące czynności:

1. Połączyć urządzenia zgodnie ze schematem na rys. 53.13.
2. Skonfigurować komputery PC10 i PC30 jak w przykładzie 53.3.
3. Połączyć komputer z przełącznikiem i nawiązać sesję. Utworzyć sieci wirtualne i przypisać porty.

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name uczniowie
Switch(config-vlan)#exit
```



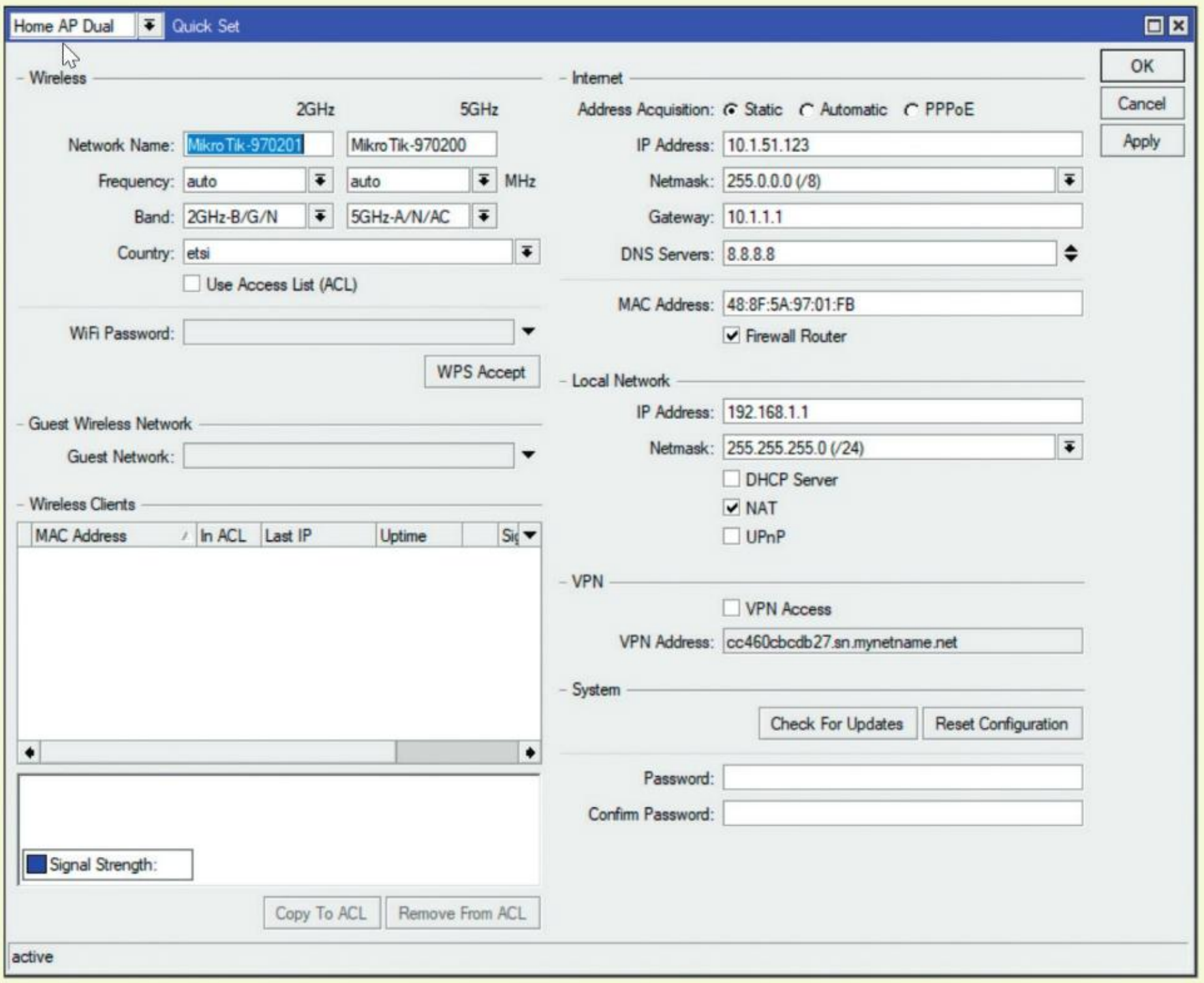
Rys. 53.13. **Schemat połączeń do konfiguracji routingu między sieciami VLAN z wykorzystaniem routera Mikrotik**

```
Switch(config)#vlan 30
Switch(config-vlan)#name nauczyciele
Switch(config-vlan)#exit
Switch(config)#interface range fastethernet 0/1 - 4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fastethernet 0/5 - 8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
```

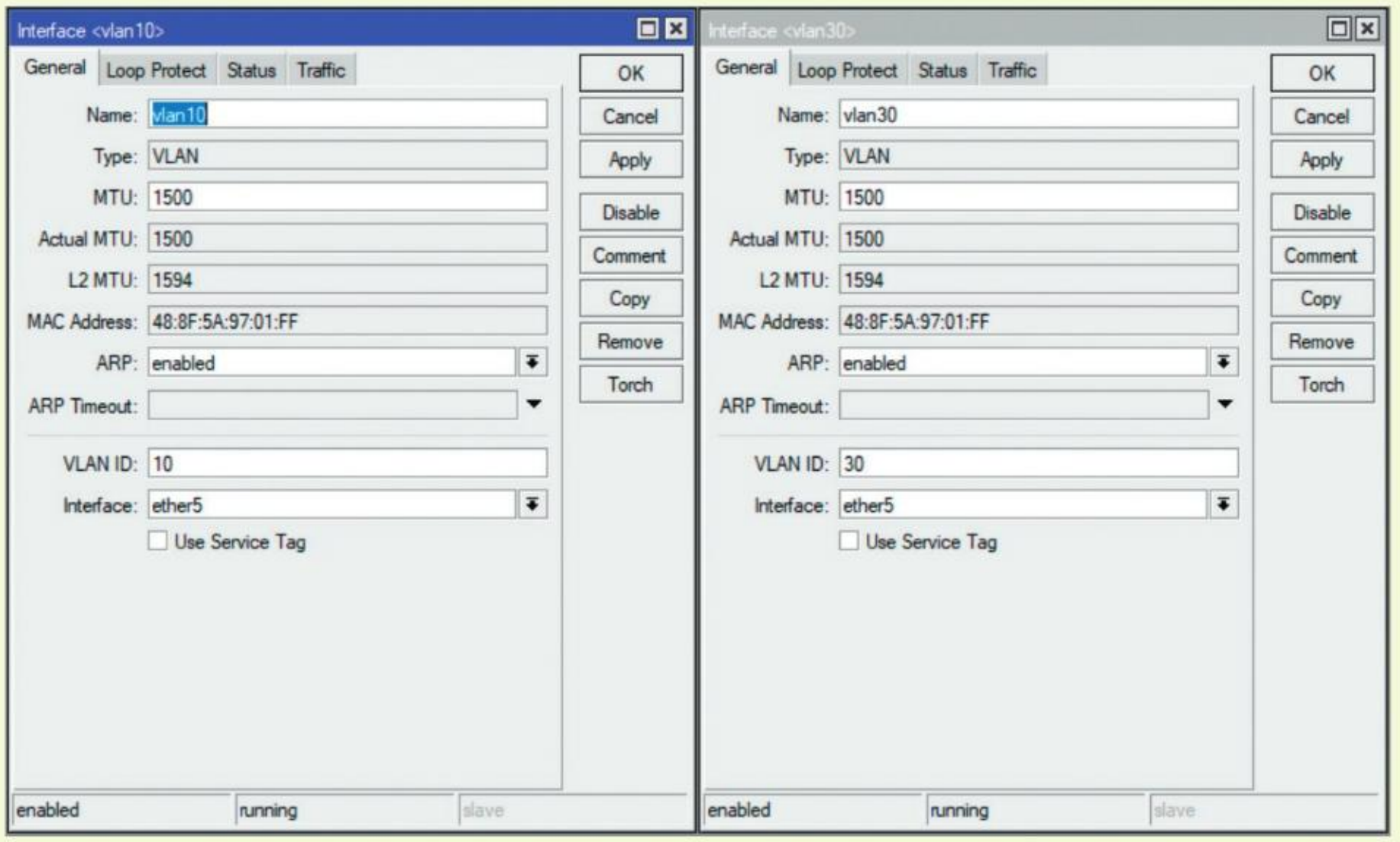
4. Skonfigurować interfejs FastEthernet0/10 do pracy w trybie trunkowym.

```
Switch(config)#interface FastEthernet 0/10
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10
Switch(config-if)#switchport trunk allowed vlan add 30
Switch(config-if)#end
```

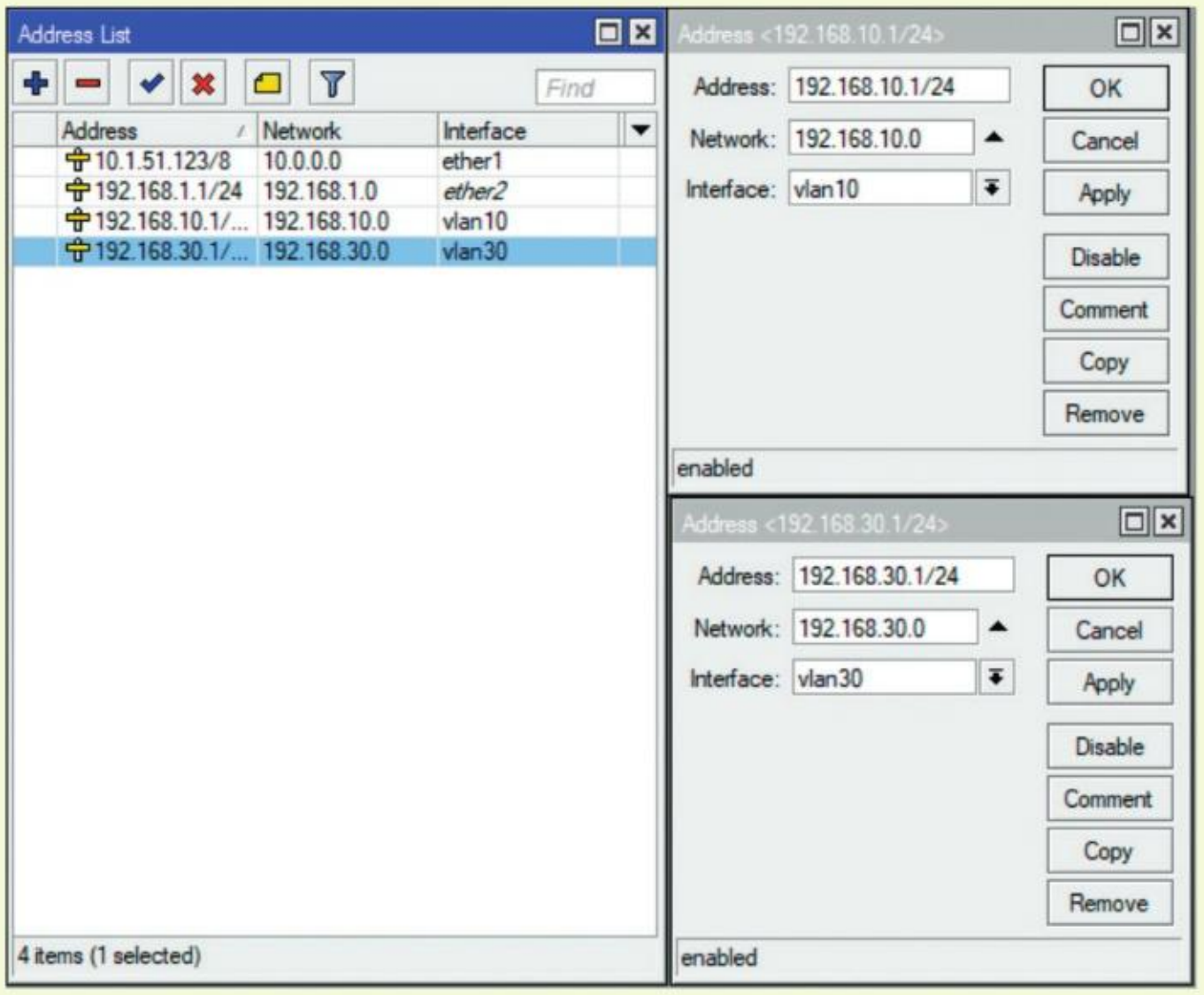
5. Za pomocą programu Winbox połączyć się z routerem.
6. Z lewego panelu wybrać **Quick Set** i skonfigurować dostęp do internetu (rys. 53.14). Kliknąć przycisk **Apply** i **OK**.
7. Skonfigurować sieci VLAN i przypisać je do portu 5. Z lewego panelu wybrać **Interfaces**, a następnie – zakładkę **VLAN**. Kliknąć przycisk dodawania „**+**” i skonfigurować sieć VLAN10 i VLAN30 (rys. 53.15). Kliknąć **Apply** i **OK**.
8. Przypisać adresy IP dla sieci VLAN, jak na rys. 53.16. Kliknąć **Apply** i **OK**.
9. Sprawdzić możliwość komunikacji między komputerami i z internetem (rys. 53.17).



Rys. 53.14. **Konfiguracja dostępu do internetu w routerze Mikrotik**

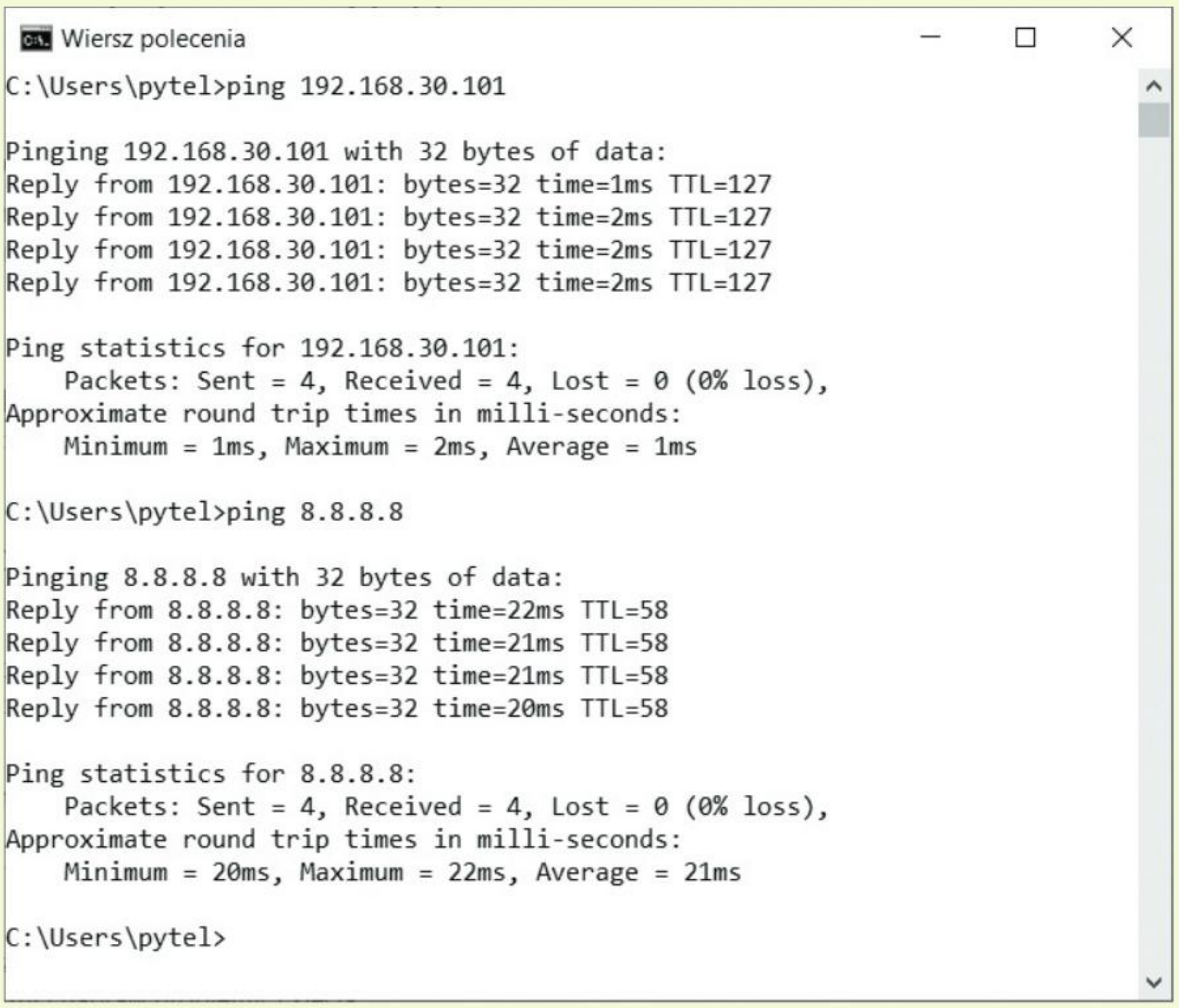


Rys. 53.15. **Konfiguracja sieci wirtualnych w routerze Mikrotik**



KODY

Rys. 53.16. **Konfiguracja adresów IP dla sieci VLAN w routerze Mikrotik**



Rys. 53.17. **Testowanie komunikacji między sieciami VLAN i z internetem**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Przyłącz dwa komputery do przełącznika i sprawdź możliwość komunikacji między portami przydzielonymi do tej samej i do różnych sieci VLAN.
2. Skonfiguruj łącze trunkowe między dwoma przełącznikami. Podłącz dwa komputery do różnych przełączników i sprawdź możliwość komunikacji zarówno w jednej sieci wirtualnej, jak i między różnymi sieciami wirtualnymi.

54 Zasady modernizacji sieci wirtualnych

ZAGADNIENIA

Efektywne zarządzanie sieciami wirtualnymi **Skonfigurowanie przełączników do obsługi protokołu VTP** **Tryby pracy przełączników z zainstalowanym protokołem VTP** **Zarządzanie za pomocą protokołu VTP sieciami wirtualnymi na wszystkich przełącznikach**

Aby zachować spójność sieci, na każdym przełączniku muszą być utworzone takie same sieci wirtualne, niezależnie od tego, czy obecnie w przełączniku jest port skonfigurowany do pracy w danej sieci wirtualnej. Dzięki standardowi IEEE 802.1Q możliwe staje się utworzenie w sieci ponad 4000 sieci wirtualnych. Na ogół liczba sieci wirtualnych jest mniejsza, ale aktualny pozostaje problem efektywnego zarządzania nimi i ich modernizacji. W zarządzaniu sieciami wirtualnymi na przełącznikach pomaga administratorowi **protokół VTP** (ang. *VLAN Trunking Protocol*). VTP został opracowany przez firmę CISCO i stanowi jej własność – działa na przełącznikach CISCO, a korzystanie z niego na sprzęcie innych producentów wymaga wykupienia licencji przez producenta przełącznika. Protokół VTP umożliwia administratorowi sieci skonfigurowanie jednego przełącznika i dystrybucję konfiguracji sieci VLAN do innych przełączników. Protokół VTP w wersjach 1 i 2 rozpoznaje tylko sieci VLAN z przedziału normalnego (identyfikatory od 1 do 1005) i działa wyłącznie na połączeniach trunkowych. Wersja 3 protokołu VTP obsługuje wszystkie sieci wirtualne.

Protokół VTP zmniejsza obciążenie administratora pracą i liczbę błędów konfiguracyjnych, które mogą wystąpić podczas wprowadzania zmian w konfiguracji sieci VLAN na wielu przełącznikach. Ponadto umożliwia zachowanie spójności konfiguracji wszystkich sieci VLAN w całej sieci, monitorowanie zmian w sieci VLAN i dynamiczne zgłaszanie sieci VLAN dodanych lub usuniętych z sieci. Działanie protokołu opiera się na koncepcji domeny VTP.

Domena VTP składa się z jednego przełącznika lub z większej liczby wzajemnie połączonych przełączników, współdzielących szczegóły konfiguracji sieci VLAN i wykorzystujących komunikaty protokołu VTP.

Przełącznik może być skonfigurowany do pracy w trybie:

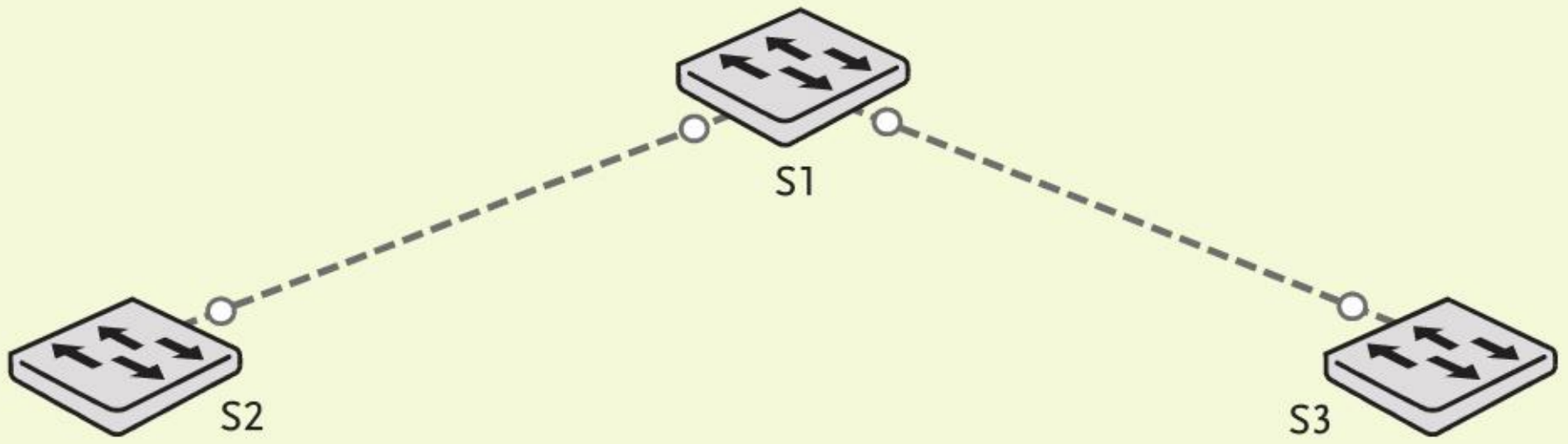
- **serwera VTP** – w tym trybie administrator dodaje lub kasuje sieci wirtualne. W domenie może być wiele serwerów VTP (zapewnienie nadmiarowości). Serwer przechowuje w pamięci NVRAM informacje o sieciach VLAN przeznaczone dla całej domeny i synchronizuje informacje o sieciach VLAN z przełącznikami z całej domeny VTP;
- **klienta VTP** – za pomocą klienta VTP nie można tworzyć, zmieniać ani usuwać sieci VLAN. W tym trybie przełącznik przechowuje informacje o sieciach VLAN dla całej domeny tylko wtedy, gdy jest włączony. Po zresetowaniu przełącznika usuwa się informacje o sieciach VLAN i musi on ponownie uzyskać informacje od serwera;
- **transparentnym** – przełączniki przekazują ogłoszenia VTP do klientów i serwerów VTP, lecz nie są członkami domeny VTP. Sieci VLAN utworzone na przełączniku pracującym w trybie transparentnym mają dla tego przełącznika tylko znaczenie lokalne.

PRZYKŁAD 54.1

Konfigurowanie nazwy domeny VTP

Serwer VTP rozsyła nazwę domeny VTP do wszystkich przełączników w sieci. Przykładowo: jeżeli administrator skonfiguruje na przełączniku S1, będącym serwerem VTP, nazwę domeny VTP jako **`ZSP51`**, to S1 wyśle ogłoszenie VTP z nową nazwą domeny do wszystkich przełączników. Przełączniki S2 i S3, będące serwerami VTP, uaktualniają swoją konfigurację po wprowadzeniu do niej nowej nazwy domeny. Aby skonfigurować nazwę domeny VTP, należy:

1. Połączyć trzy przełączniki jak na rys. 54.1.



Rys. 54.1. **Przykładowa sieć złożona z trzech przełączników**

2. Ustawić między przełącznikami tryb połączeń trunkowy. Procedurę konfiguracji portów gigabitowych na przełączniku S1 przedstawiono na rys. 54.2. Analogicznie należy skonfigurować porty na przełącznikach S2 i S3. Polecenie **`switchport trunk allowed vlan all`** dodaje wszystkie sieci wirtualne do listy obsługiwanych sieci.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range GigabitEthernet 0/1 - 2
Switch(config-if-range)#switchport mode trunk

Switch(config-if-range)#switchport trunk allowed vlan all
Switch(config-if-range)#exit
```

Rys. 54.2. **Procedura konfiguracji trybu trunkowego portów**

3. Skonfigurować na przełączniku S1, będącym serwerem VTP, nazwę domeny VTP jako **`ZSP51`**. W trybie konfiguracji globalnej wydać polecenie **`vtp domain ZSP51`**. Wynik działania polecenia przedstawiono na rys. 54.3.

```
Switch(config)#vtp domain ZSP51
Changing VTP domain name from NULL to ZSP51
Switch(config)#
```

Rys. 54.3. **Zmiana nazwy domeny VTP**

4. Sprawdzić na przełącznikach S2 i S3 (pracujących w trybie serwera VTP) nazwę domeny. W trybie użytkownika uprzywilejowanego wydać polecenie **`show vtp status`**. Na rys. 54.4 nową nazwę domeny zaznaczono strzałką.

```
S2#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : ZSP51
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE9 0x00 0x8E 0x68 0xE6 0xA5 0x3B 0x56
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
S2#
```

Rys. 54.4. **Weryfikacja nazwy domeny VTP**

PRZYKŁAD 54.2

Zarządzanie sieciami VLAN za pomocą protokołu VTP

W tym ćwiczeniu za pomocą protokołu VTP zostaną zaktualizowane sieci VLAN na wszystkich przełącznikach. Na przełączniku S1 zostaną skonfigurowane przykładowe sieci VLAN. Przełącznik S3 zostanie przełączony do trybu klienta.

Aby modyfikować sieci VLAN za pomocą protokołu VTP, należy wykonać następujące czynności:

1. Połączyć trzy przełączniki jak na rys. 54.1.
2. Ustawić między przełącznikami tryb połączeń trunkowy.
3. Skonfigurować przełącznik S3 do pracy w trybie klienta. W globalnym trybie konfiguracyjnym należy wydać polecenie **`vtp mode client`** (rys. 54.5).

```
S3(config)#vtp mode client
Setting device to VTP CLIENT mode.
S3(config)#
```

Rys. 54.5. **Ustawienie trybu klienta VTP**

4. Na przełączniku S1 (pracującym w trybie serwera) skonfigurować dwie nowe sieci wirtualne. W globalnym trybie konfiguracyjnym należy wydać polecenie **`vlan 10`** i **`vlan 20`**, a następnie za pomocą polecenia **`show vtp status`** sprawdzić liczbę sieci wirtualnych. Na rys. 54.6 przedstawiono wyniki działania poleceń, a strzałką zaznaczono aktualną liczbę zdefiniowanych sieci VLAN.

KODY

5. Sprawdzić poprawność konfiguracji na przełącznikach S2 i S3. Na rys. 54.7 strzałką zaznaczono liczbę sieci VLAN, tryb pracy przełącznika S3 i nazwę domeny.
6. Wydać polecenie **show vlan** w trybie użytkownika uprzywilejowanego, aby wyświetlić listę sieci wirtualnych.

```
S1(config)#vlan 10
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : ZSP51
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xD6 0x66 0x1A 0xA8 0x4B 0x0F 0x47 0xA1
Configuration last modified by 0.0.0.0 at 3-1-93 00:38:01
Local updater ID is 0.0.0.0 (no valid interface found)
S1#
```

Rys. 54.6. Weryfikacja utworzenia nowych sieci VLAN

```
S3#sh vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : ZSP51
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xD6 0x66 0x1A 0xA8 0x4B 0x0F 0x47 0xA1
Configuration last modified by 0.0.0.0 at 3-1-93 00:38:01
S3#
```

Rys. 54.7. Weryfikacja poprawności konfiguracji sieci VLAN

W sieci może być wiele serwerów VTP i na każdym z nich mogą być wprowadzane zmiany. Każda zmiana powoduje zwiększenie numeru **korekty konfiguracji** (ang. *configuration revision number*). Przyjmuje się, że najbardziej aktualna jest konfiguracja o najwyższym numerze.

Przed włączeniem używanego przełącznika do sieci należy sprawdzić jego numer korekty konfiguracji – jeżeli ma wyższy niż używany w sieci oraz ustawioną taką samą nazwę domeny VTP, to może spowodować usunięcie wszystkich informacji o VLAN z całej sieci i zastąpienie ich własną konfiguracją.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zaproponuj podział sieci w twojej szkole na sieci wirtualne. Zaplanuj przydział portów w przełącznikach do odpowiednich sieci.

55 Korzystanie z wirtualnych sieci prywatnych

ZAGADNIENIA

Wirtualna sieć prywatna VPN **Skonfigurowanie sieci VPN z wykorzystaniem bramki VPN** **Skonfigurowanie klienta sieci VPN**

Wirtualna sieć prywatna VPN (ang. *Virtual Private Network*) pozwala w sposób bezpieczny łączyć sieci i komputery z wykorzystaniem niezaufanego i niebezpiecznego medium, jakim jest np. internet. Transmisja między poszczególnymi sieciami i komputerami odbywa się przez szyfrowane i zabezpieczone wirtualne tunele.

Bezpieczne sieci mogą być budowane na podstawie różnych protokołów, np.:

1. **Protokół IPSec** – pozwala na budowę dwóch typów sieci wirtualnych:
   - sieci typu **site-to-site** – łączące w sposób bezpieczny dwie lub więcej sieci. Tunele między sieciami najczęściej są zakończone specjalnymi urządzeniami, takimi jak routery z funkcją VPN, firewalle lub koncentratory VPN. Ten typ nie wymaga instalacji żadnego oprogramowania na komputerach w sieci;
   - sieci typu **remote-access** – łączące w sposób bezpieczny pojedyncze komputery z sieciami. Ten typ wymaga instalacji na komputerach specjalnego oprogramowania typu **VPN Client**.
2. **Protokół SSL** – najczęściej typu remote-access. Nie wymaga instalacji specjalnego oprogramowania na komputerze, za to ma mniejszą funkcjonalność niż sieci VPN oparte na protokole IPSec. Zwykle wykorzystuje się go do bezpiecznego łączenia się ze stronami internetowymi.
3. Inny protokół (lub technologia), np. **L2TP**, wykorzystywany w systemach Windows.

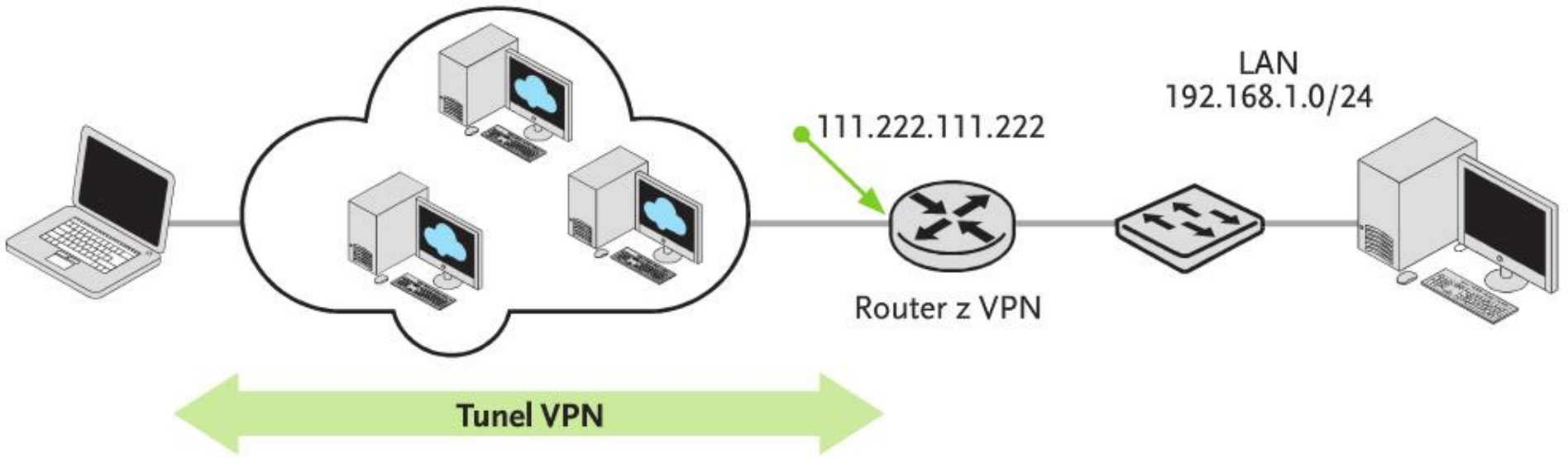
Określenie *wirtualna* oznacza, że sieć istnieje jako struktura logiczna działająca w sieci publicznej. Stacje końcowe mogą korzystać z VPN tak, jak gdyby istniało między nimi łącze fizyczne. Rozwiązania oparte na VPN stosuje się w sieciach korporacyjnych firm, których **zdalni użytkownicy** (telepracownicy) uzyskują bezpieczny dostęp do zasobów sieci firmowej przez niezabezpieczone łącza publiczne. Wykorzystuje się je również w firmach, których pracownicy często podróżują i muszą z dowolnego miejsca uzyskać bezpieczny dostęp do sieci firmy.

W sieciach VPN typu remote-access między komputerem zdalnego klienta a routerem obsługującym VPN tworzy się szyfrowany tunel, którym są przesyłane dane. W sieciach typu site-to-site tunel jest tworzony między specjalnymi urządzeniami, np. routerami. Do szyfrowania danych mogą być wykorzystywane następujące algorytmy:

- **DES** (ang. *Data Encryption Standard*) – szyfruje dane kluczem o długości 56 bitów;
- **3 DES** (ang. *Triple DES*) – potrójne szyfrowanie DES, zapewnia bezpieczniejsze szyfrowanie niż DES;
- **AES** (ang. *Advanced Encryption Standard*) – zapewnia najwyższy poziom bezpieczeństwa.

Za ustalenie wspólnego klucza sesyjnego, niezbędnego do szyfrowania danych, i za późniejsze okresowe jego zmiany odpowiada **algorytm DH** (ang. *Diffie-Hellman*). Istnieją trzy grupy kluczy, oznaczone numerami 1, 2 oraz 5. Im wyższy numer, tym klucze będą bezpieczniejsze, chociaż wymagające większego nakładu obliczeniowego.

Oprócz szyfrowania, IPSec zapewnia również **kontrolę integralności** i **uwierzytelnianie** za pomocą algorytmu **HMAC** (ang. *Hashed Message Authentication Code*). Algorytm HMAC wykorzystuje jedną z dwóch funkcji skrótu **MD5** lub **SHA-1**. Funkcje skrótu na podstawie łańcucha danych, np. wiadomości tekstowej, generują unikatową liczbę. Każda zmiana tekstu oryginalnego powoduje zmianę skrótu. Odtworzenie tekstu na podstawie skrótu nie jest możliwe. Znalezienie innego tekstu, dla którego wartość skrótu byłaby taka sama, jest tak trudne, że uznaje się to za niewykonalne. Ochrona integralności danych jest realizowana w ten sposób, że nadawca dołącza do wiadomości wartość funkcji skrótu, a odbiorca porównuje tę wartość z samodzielnie obliczonym skrótem wiadomości. Jeżeli liczby się zgadzają, to znaczy, że wiadomości wysłana i odebrana są takie same. Schemat sieci VPN w trybie remote-access przedstawiono na rys. 55.1.



Rys. 55.1. Schemat sieci VPN w trybie remote-access

IPSec wykorzystuje szyfrowanie do ochrony informacji przed odczytaniem lub ingerencją w zawartość danych. Oba końce tunelu VPN powinny współdzielić klucz, który jest wykorzystywany do szyfrowania i deszyfrowania informacji. Proces negocjacji parametrów bezpieczeństwa w IPSec przebiega w dwóch fazach:

- **Faza 1** – przeprowadza się negocjację parametrów bezpieczeństwa, wymaganą do ustanowienia bezpiecznego kanału między dwoma końcami tunelu. Faza 1 jest implementowana przez protokół **IKE** (ang. *Internet Key Exchange*).
- **Faza 2** – wykorzystuje się bezpieczny tunel ustanowiony w fazie 1 w celu wymiany parametrów bezpieczeństwa wymaganych do transmisji danych przez użytkownika.

Każdy punkt końcowy korzysta z **asocjacji bezpieczeństwa SA** (ang. *Security Associations*), która opisuje parametry bezpieczeństwa obsługiwane przez urządzenie, takie jak typ uwierzytelniania i szyfrowania. Podczas negocjacji między końcami tunelu jest wybierana asocjacja obsługiwana przez oba końce tunelu. Jeżeli negocjacja zakończy się niepowodzeniem, połączenie zostaje przerwane.

PRZYKŁAD 55.1

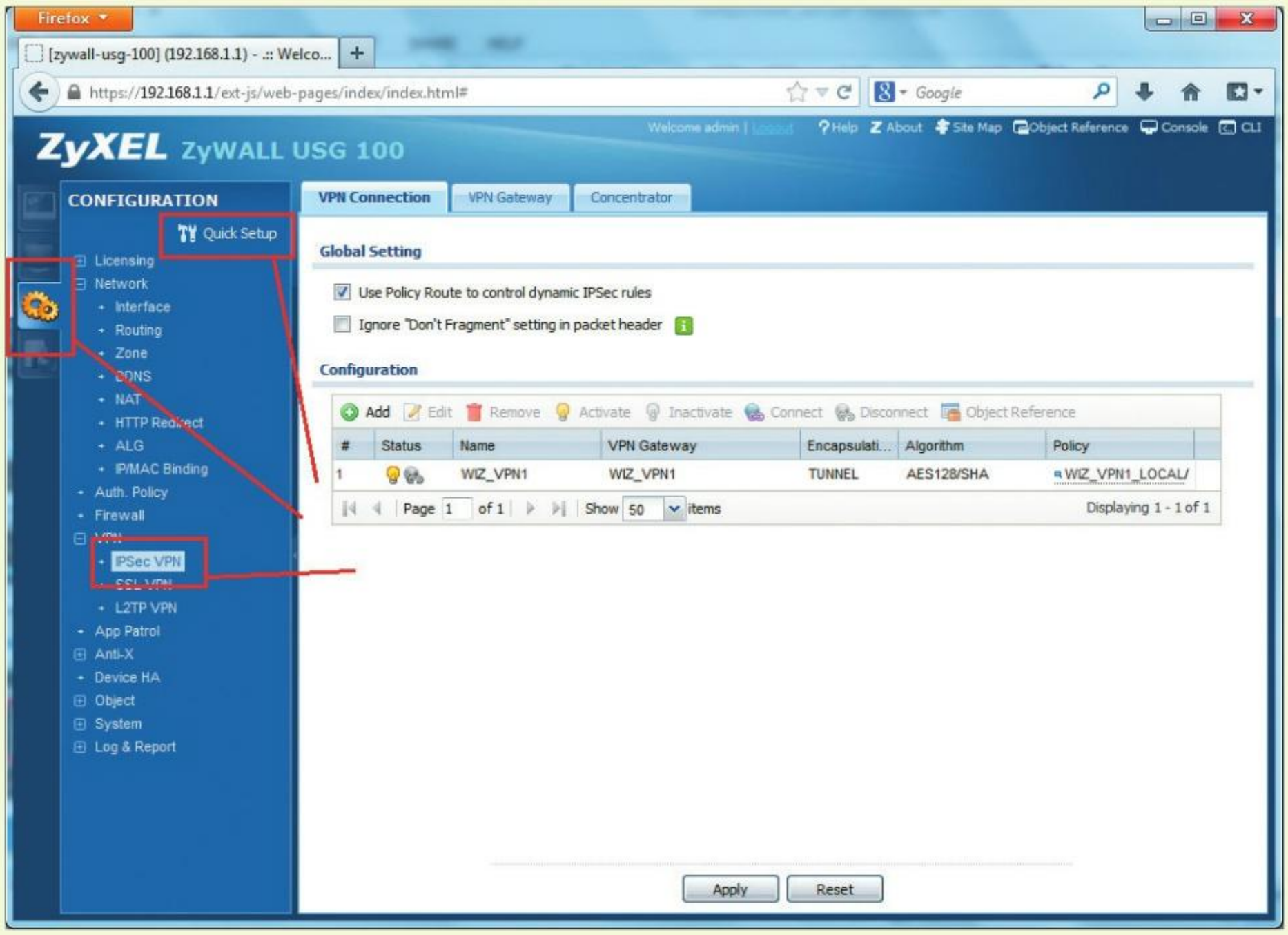
Konfigurowanie sieci VPN w trybie remote-access

W tym ćwiczeniu zostanie skonfigurowana sieć VPN w trybie remote-access.

Do zbudowania sieci posłuży zintegrowana brama internetowa. Brama jest wyposażona w funkcję obsługi sieci VPN. Konfiguracja obejmuje czynności wykonane na komputerze i bramie.

Aby skonfigurować bramę do pracy w sieci VPN w trybie remote-access, należy wykonać następujące czynności:

1. Połączyć komputer z bramą i za pomocą przeglądarki zalogować się do panelu administracyjnego. W oknie głównym kliknąć ikonę konfiguracji, rozwinąć zakładkę VPN i wskazać sieci typu IPSec VPN. Do konfiguracji zostanie wykorzystany kreator, który można uruchomić przyciskiem **`Quick Setup`**. Na rys. 55.2 te elementy zaznaczono czerwonymi ramkami.



Rys. 55.2. **Uruchomienie kreatora sieci VPN**

2. W oknie kreatora wybrać konfigurowanie sieci VPN (ang. *VPN Setup*) (rys. 55.3). Kliknąć przycisk **`Next`**, aby przejść do następnego ekranu.



Rys. 55.3. **Wybór konfigurowania sieci VPN**

3. Wybrać zaawansowany tryb konfigurowania sieci (ang. *Advanced*) (rys. 55.4). Kliknąć przycisk **Next**, aby przejść do następnego ekranu.



Rys. 55.4. **Wybór zaawansowanego trybu konfigurowania sieci**

4. Wybrać typ sieci **Remote Access** (ang. *Server Role*) i w polu **Rule Name:** wprowadzić nazwę dla połączenia (rys. 55.5). Kliknąć przycisk **Next**, aby przejść do następnego ekranu.



Rys. 55.5. **Wybór typu sieci i nazwy**

5. Wprowadzić dane konfiguracyjne dla fazy 1, np. algorytm szyfrowania (ang. *Encryption Algorithm*) **AES128**, algorytm autentykacji (ang. *Authentication Algorithm*) **SHA-1**, algorytm wymiany kluczy (ang. *Key Group*) **DH2** i hasło (ang. *Pre-Shared Key*). Pozostałe wartości pozostawić domyślne. Przykładowy sposób konfiguracji fazy 1 pokazano na rys. 55.6. Kliknąć przycisk **Next**, aby przejść do następnego ekranu.



Rys. 55.6. **Konfiguracja fazy 1 po stronie bramki**

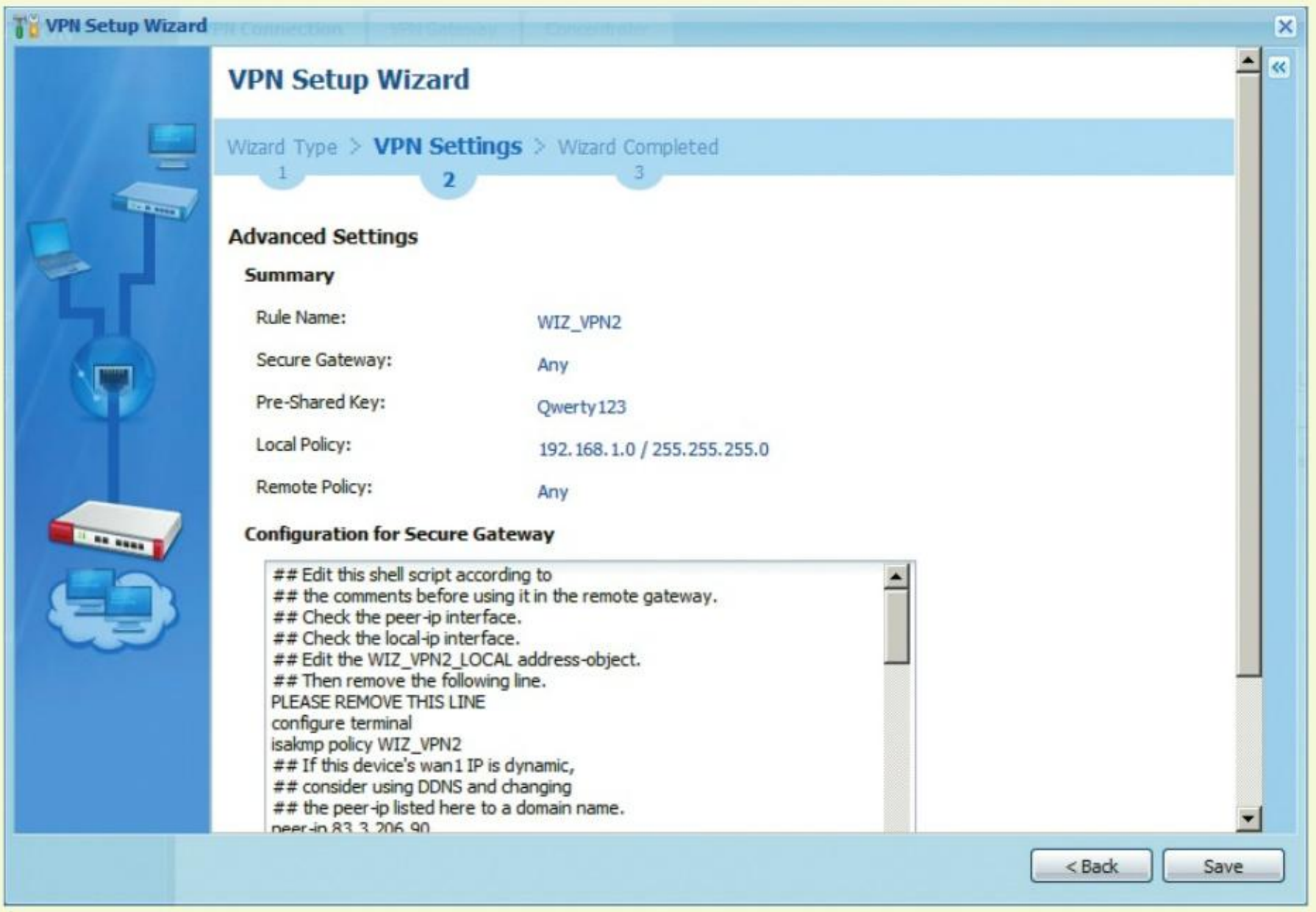


Rys. 55.7. **Konfiguracja fazy 2 po stronie bramki**

6. Wprowadzić dane konfiguracyjne dla fazy 2, np. algorytm szyfrowania (ang. *Encryption Algorithm*) **AES128**, algorytm autentykacji (ang. *Authentication Algorithm*) **SHA-1**,

algorytm wymiany kluczy (ang. *Perfect Forward Secrecy*) **DH1** i adres IP w sieci lokalnej (ang. *Local Policy*). Pozostałe wartości pozostawić domyślne. Przykładowy sposób konfiguracji fazy 2 pokazano na rys. 55.7. Kliknąć przycisk **Next**, aby przejść do następnego ekranu.

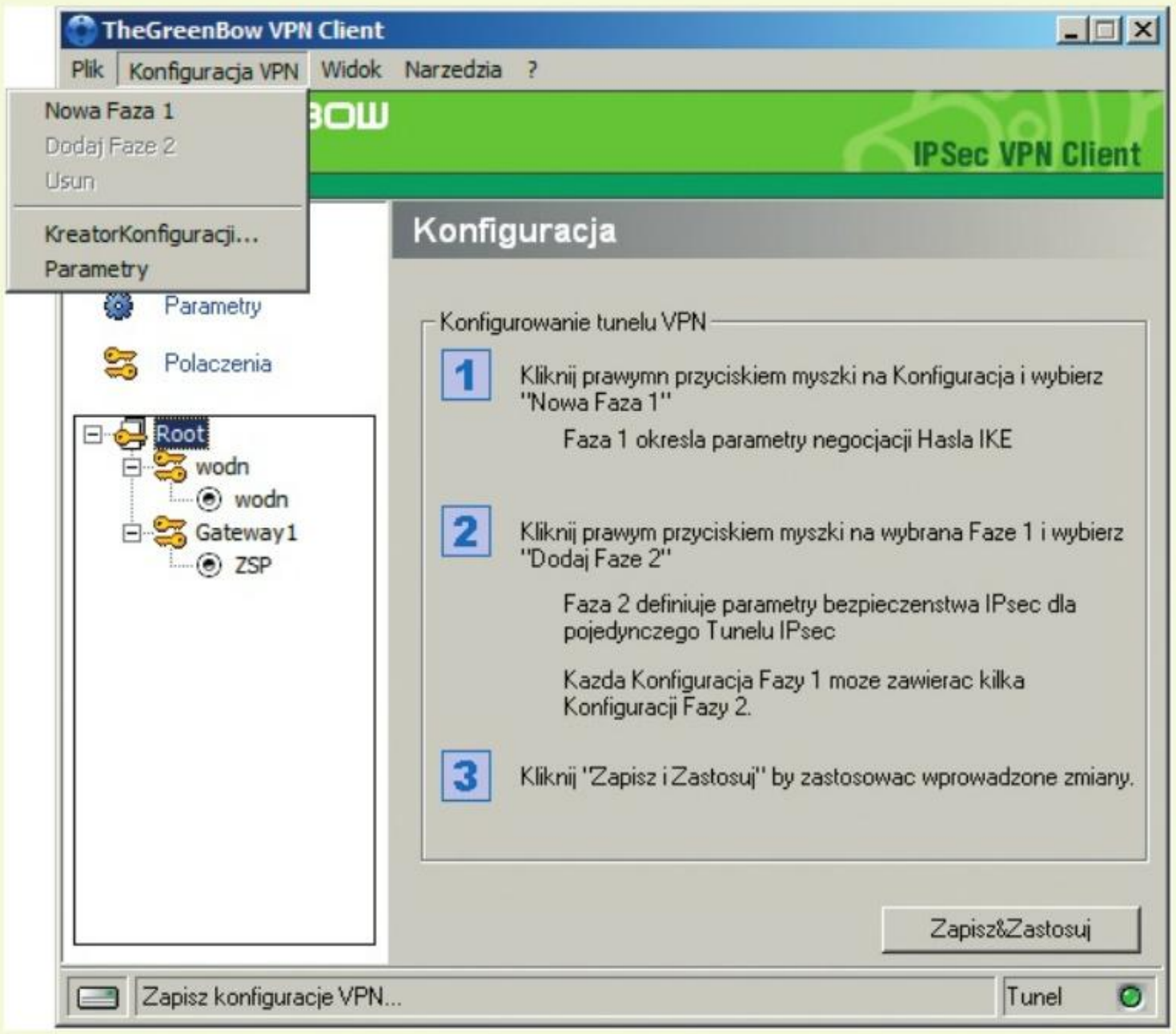
7. Sprawdzić poprawność konfiguracji (rys. 55.8) i kliknąć przycisk **Save**, aby zapisać konfigurację. Po zapisaniu konfiguracji zostanie wyświetlone podsumowanie pracy kreatora. Zamknąć podsumowanie przyciskiem **Close**.



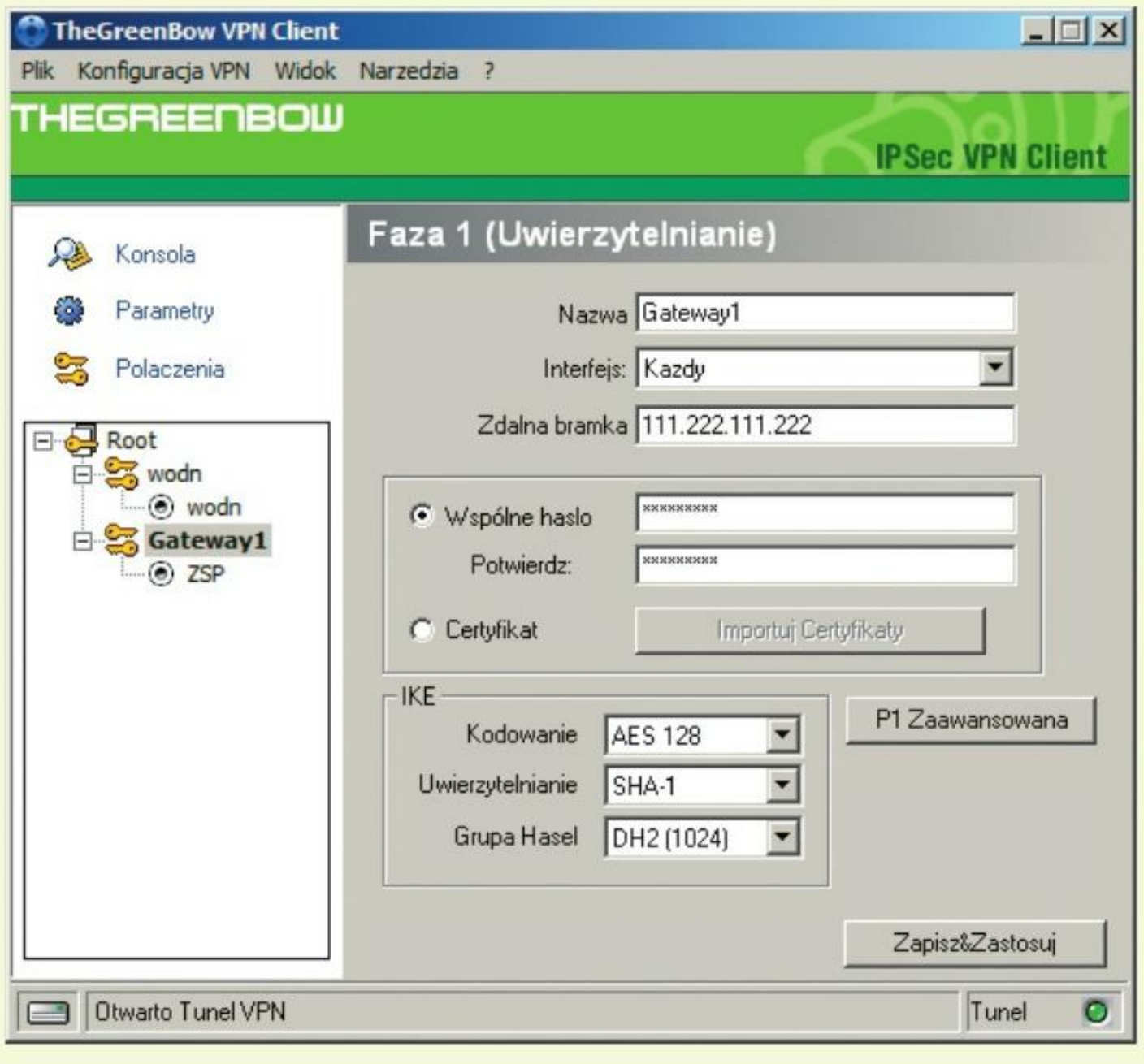
Rys. 55.8. **Podsumowanie konfiguracji fazy 2 po stronie bramki**

Aby skonfigurować komputer do roli klienta sieci VPN, należy wykonać następujące czynności:

1. Zainstalować program – klienta sieci VPN, np. **TheGreenBow VPN Client** (oprogramowanie shareware).
2. Uruchomić program klienta sieci VPN. W menu głównym programu wybrać opcję **Konfiguracja VPN**, a następnie – polecenie **Nowa Faza 1** (rys. 55.9).
3. Wprowadzić dane konfiguracyjne dla fazy 1 jak po stronie bramy: szyfrowanie **AES128**, uwierzytelnianie **SHA-1**, grupa haseł **DH2** i wspólne hasło. W polu **Zdalna bramka** wpisać adres IP interfejsu WAN bramki. Pozostałe wartości pozostawić domyślne. Przykładowy sposób konfiguracji fazy 1 pokazano na rys. 55.10. Kliknąć przycisk **Zapisz&Zastosuj**.
4. Wprowadzić dane konfiguracyjne dla fazy 2 jak po stronie bramy: szyfrowanie **AES128**, uwierzytelnianie **SHA-1**, tryb **Tunnel**, PFS **Grupa DH1**. Wprowadzić nazwę i adres klienta VPN oraz adres i maskę podsieci zdalnej. Przykładowy sposób konfiguracji fazy 2 pokazano na rys. 55.11. Kliknąć przycisk **Zapisz&Zastosuj**.



Rys. 55.9. **Wybór konfiguracji nowej fazy 1 po stronie klienta**

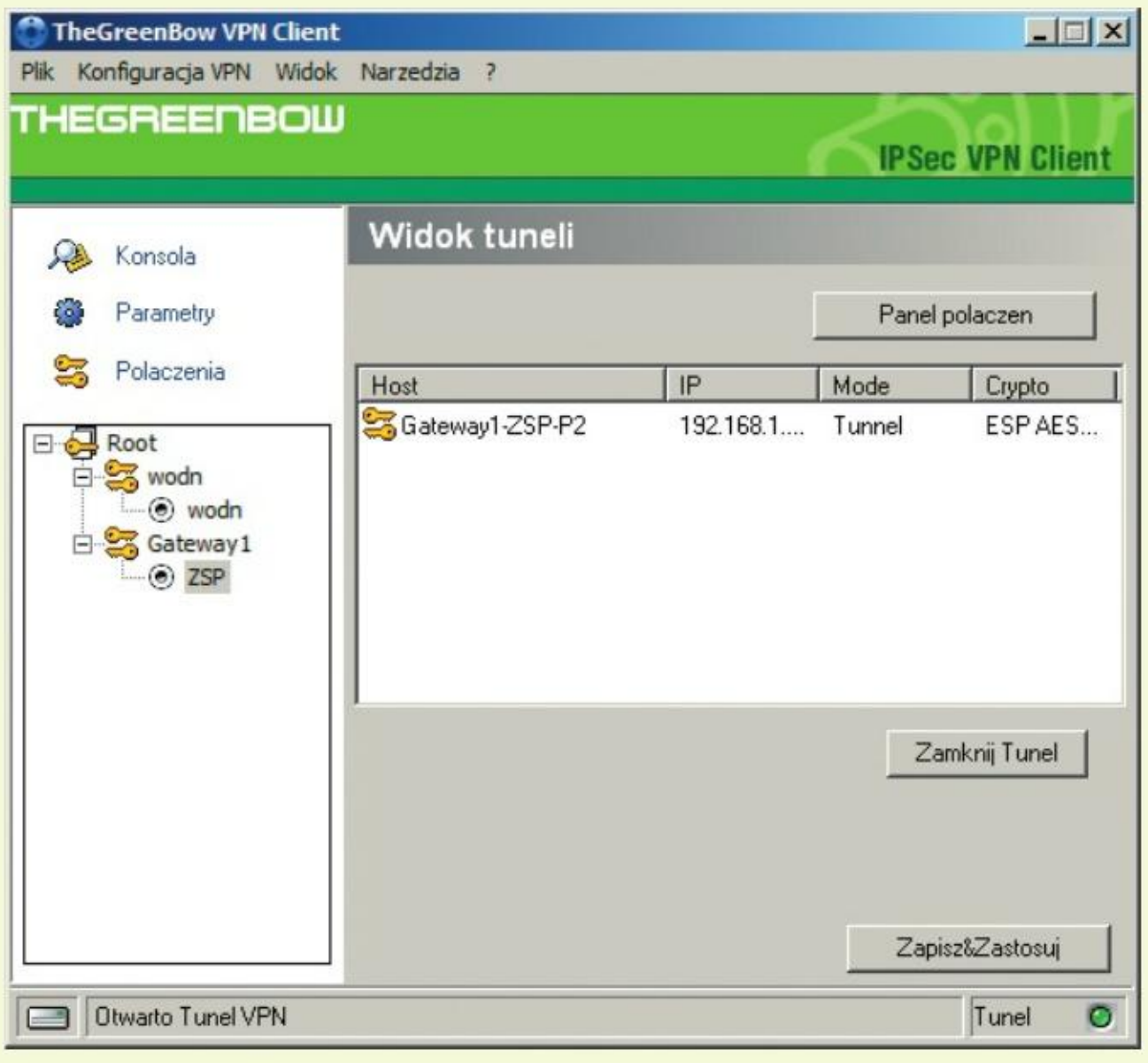


Rys. 55.10. **Konfiguracja fazy 1 po stronie klienta**



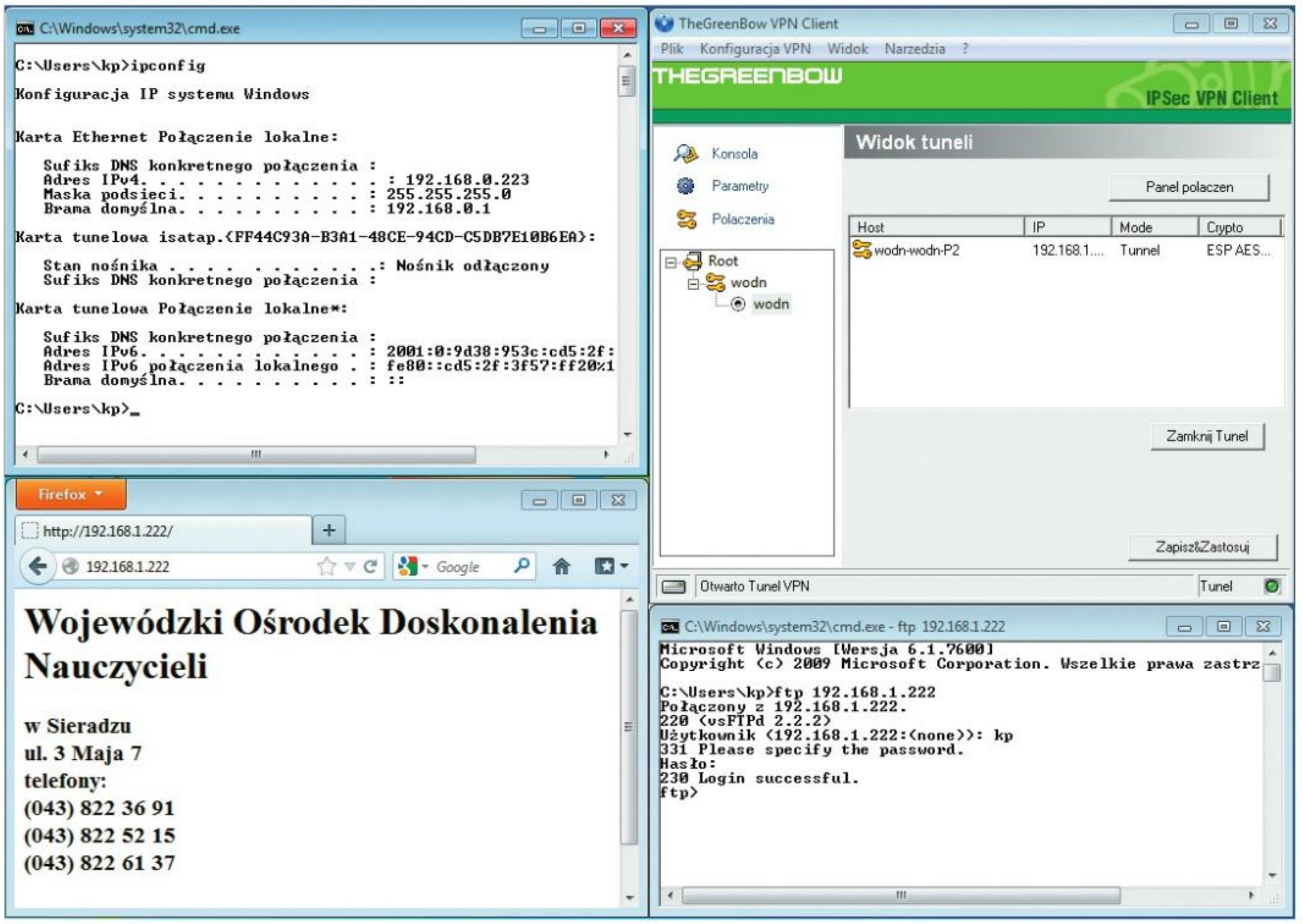
Rys. 55.11. **Konfiguracja fazy 2 po stronie klienta**

5. Kliknąć przycisk **`Otwórz tunel`**. Jeżeli konfiguracja została wykonana poprawnie i uda się nawiązać połączenie, to w oknie **`Połączenia`** (rys. 55.12) pojawi się informacja o nawiązanym połączeniu.



Rys. 55.12. **Okno informacji o aktywnych połączeniach**

Po nawiązaniu połączenia jest ustanawiany bezpieczny (szyfrowany) tunel między komputerem lokalnym a siecią przyłączoną do interfejsu LAN bramy, np. z siecią w szkole. Umożliwia on komunikowanie się komputera z innymi urządzeniami działającymi w tej sieci, np. z serwerem WWW, FTP, tak jakby wszystkie one pracowały w jednej sieci lokalnej. Na rys. 55.13 przedstawiono pobieranie strony z serwera WWW i sesję FTP, realizowane za pomocą sieci VPN.



Rys. 55.13. Korzystanie z serwera WWW i FTP za pomocą sieci VPN

Komputer lokalny ma przydzielony prywatny adres 192.168.0.223, natomiast serwer jest zlokalizowany w sieci lokalnej i świadczy usługi pod adresem 192.168.1.222. Adresy komputera i serwera znajdują się w różnych sieciach i bezpośrednia komunikacja między nimi jest niemożliwa. Komputer lokalny może pobierać dane z serwera WWW i ustanowić sesję FTP z serwerem za pośrednictwem tunelu VPN.

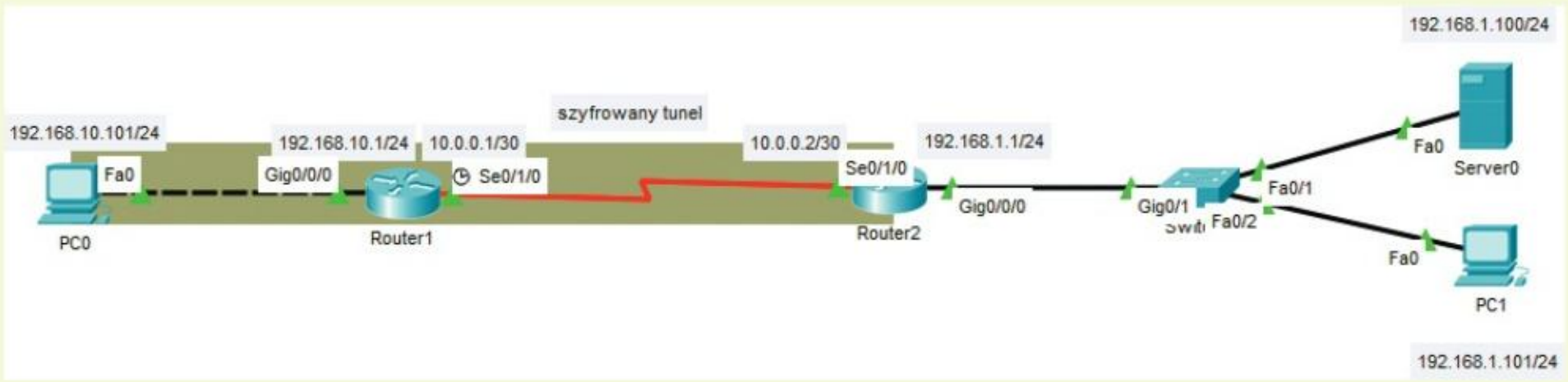
PRZYKŁAD 55.2

Konfigurowanie sieci VPN w trybie remote-access

W tym ćwiczeniu zostanie skonfigurowana sieć VPN w trybie remote-access. Szyfrowany tunel zostanie skonfigurowany między komputerem PC0 i routerem CISCO (Router2). Konfiguracja obejmuje czynności wykonane na routerach i komputerze.

Aby skonfigurować sieć VPN w trybie remote-access, należy wykonać następujące czynności:

1. Połączyć urządzenia zgodnie z rys. 55.14.



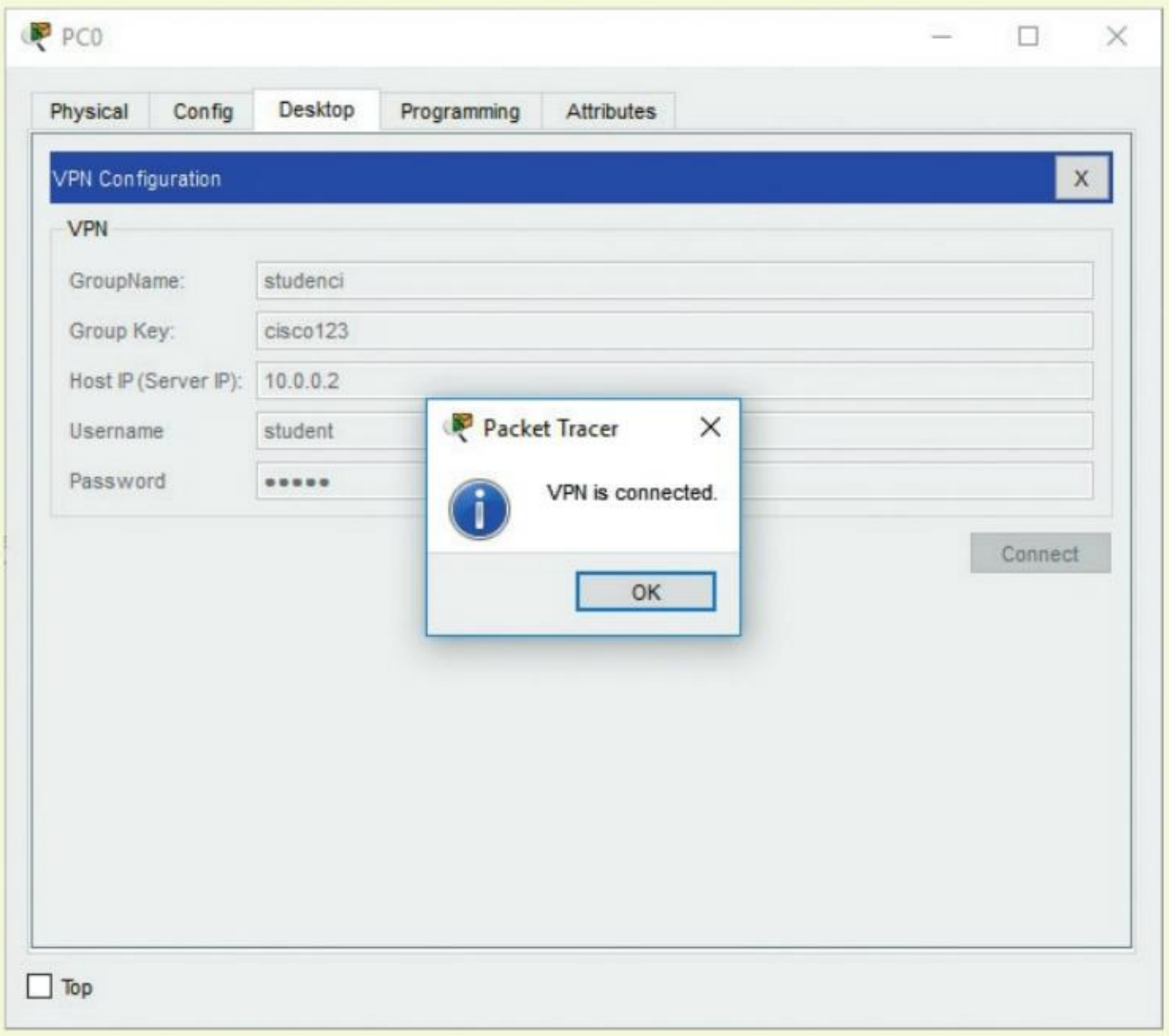
Rys. 55.14. **Schemat sieci VPN w trybie remote-access**

2. Skonfigurować adresy IP komputerów i serwera zgodnie z rys. 55.14.
3. Nawiązać połączenie z routerem Router1. Router będzie wykorzystany tylko do zapewnienia komunikacji między sieciami **192.168.10.0** i **192.168.1.0**. Przejść do trybu konfiguracji globalnej za pomocą poleceń:
```
enable
configure terminal
```
4. Skonfigurować interfejs do sieci lokalnej za pomocą poleceń:
```
interface GigabitEthernet0/0/0
ip address 192.168.10.1 255.255.255.0
no shutdown
exit
```
5. Skonfigurować interfejs szeregowy za pomocą poleceń:
```
interface Serial0/1/0
clock rate 64000
ip address 10.0.0.1 255.255.255.252
no shutdown
exit
```
6. Skonfigurować protokół routingu, np. RIP, za pomocą poleceń:
```
router rip
version 2
network 192.168.10.0
network 10.0.0.0
end
```
7. Nawiązać połączenie z routerem Router2. Router będzie wykorzystany jako zakończenie szyfrowanego tunelu. Przejść do trybu konfiguracji globalnej za pomocą poleceń:
```
enable
configure terminal
```
8. Skonfigurować interfejs do sieci lokalnej za pomocą poleceń:
```
interface GigabitEthernet0/0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
```
9. Skonfigurować interfejs szeregowy za pomocą poleceń:
```
interface Serial0/1/0
ip address 10.0.0.2 255.255.255.252
```

```
no shutdown
exit
```

10. Skonfigurować protokół routingu, np. RIP, za pomocą poleceń:
```
router rip
version 2
network 192.168.1.0
network 10.0.0.0
exit
```
11. Aktywować usługę **uwierzytelniania, autoryzacji i rejestrowania – AAA** (ang. *Authentication, Authorization, Accounting*). Skonfigurować domyślne metody uwierzytelniania i autoryzacji wykorzystujące lokalne bazy użytkowników. Utworzyć lokalne konto użytkownika *student* z hasłem **cisco** za pomocą poleceń:
```
aaa new-model
aaa authentication login VPN local
aaa authorization Network VPN local
username student password cisco
```
12. Skonfigurować politykę bezpieczeństwa i określić jej priorytet, np. **10**. Mniejsza wartość priorytetu oznacza pierwszeństwo, jeżeli zdefiniowano wiele polityk. Ustawić szyfrowanie **3DES**, funkcję kontroli integralności **md5**, algorytm **Diffie-Helmana grupa 2** za pomocą poleceń:
```
crypto isakmp policy 10
encryption 3des
hash md5
group 2
exit
```
13. Zdefiniować pulę adresów przydzielanych dla klientów łączących się przez VPN za pomocą polecenia:
```
ip local pool VPNPOOL 192.168.1.200 192.168.1.220
```
14. Ustalić parametry konfiguracji fazy 1 za pomocą poleceń:
```
crypto isakmp client configuration group studenci
key cisco123
pool VPNPOOL
exit
```
15. Skonfigurować nazwany zbiór danych protokołów bezpieczeństwa (ang. *transform-set*) fazy 2 za pomocą polecenia:
```
crypto ipsec transform-set VPN-SET esp-3des esp-md5-hmac
```
16. Połączyć wszystkie ustawienia w **kryptomapę** (ang. *crypto-map*), która zostanie zaimplementowana na interfejsie za pomocą poleceń:
```
crypto dynamic-map VPN-DMAP 15
set transform-set VPN-SET
reverse-route
exit
crypto map VPN-MAP client configuration address respond
crypto map VPN-MAP client authentication list VPN
crypto map VPN-MAP isakmp authorization list VPN
crypto map VPN-MAP 20 ipsec-isakmp dynamic VPN-DMAP
```

17. Zainstalować kryptomapę na interfejsie, za pomocą którego klienci będą nawiązywać połączenia za pomocą poleceń:
```
interface serial 0/1/0
crypto map VPN-MAP
end
```
18. Skonfigurować klienta sieci VPN w komputerze PC0. W zakładce desktop wybrać VPN (rys. 55.15). Wprowadzić nazwę grupy (ang. *Group Name*) **`studenci`**, klucz grupy (ang. *Group Key*) **`cisco123`**, adres hosta (ang. *Host IP*) **`10.0.0.2`**, nazwę użytkownika (ang. *Username*) **`student`**, hasło (ang. *Password*) **`cisco`**. Kliknąć przycisk **`Connect`**.



KODY

Rys. 55.15. **Konfiguracja klienta sieci VPN**

PRZYKŁAD 55.3[4]

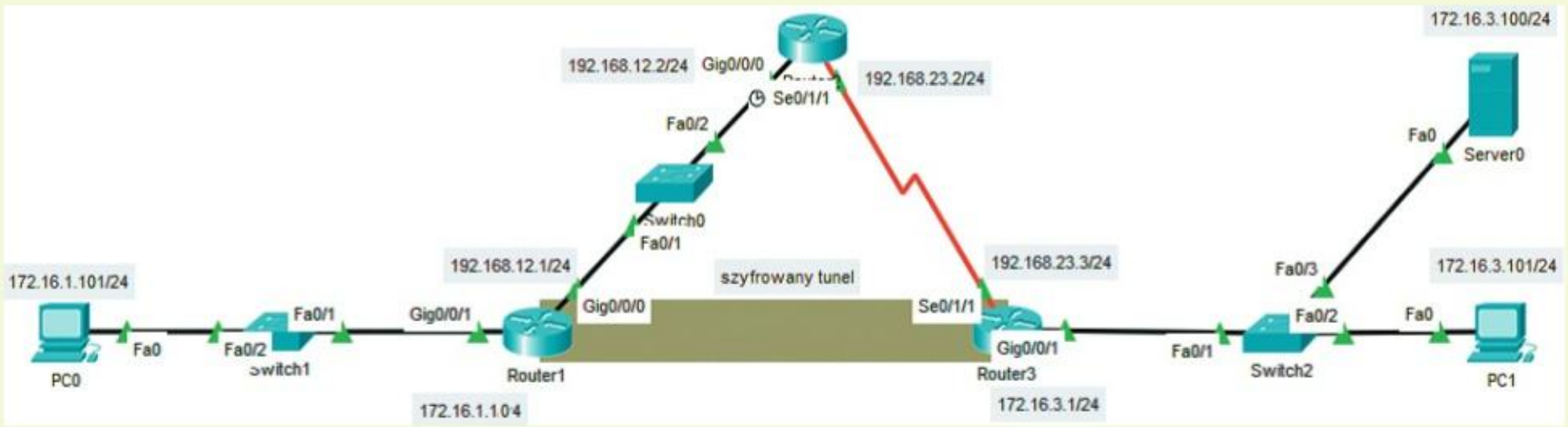
Konfigurowanie sieci VPN w trybie site-to-site

W tym ćwiczeniu zostanie skonfigurowana sieć VPN w trybie site-to-site. Szyfrowany tunel zostanie skonfigurowany między routerami CISCO. Konfiguracja obejmuje czynności wykonane na routerach, komputery nie wymagają żadnych działań poza standardową konfiguracją adresów IP.

[4] Ćwiczenie dla uczniów zaawansowanych lub szczególnie zainteresowanych.

Aby skonfigurować sieć VPN w trybie site-to-site, należy wykonać następujące czynności:

1. Połączyć urządzenia jak na rys. 55.16.



Rys. 55.16. **Schemat sieci VPN w trybie site-to-site**

2. Skonfigurować adresy IP komputerów zgodnie z rys. 55.16.
3. Nawiązać połączenie z routerem Router2. Router będzie wykorzystany tylko w celu zapewnienia komunikacji między sieciami lokalnymi (zastępuje chmurę internetu). Przejść do trybu konfiguracji globalnej za pomocą poleceń:

```
enable
configure terminal
```

4. Skonfigurować interfejs prowadzący do Routera1 za pomocą poleceń:

```
interface gigabitethernet0/0/0
ip address 192.168.12.2 255.255.255.0
no shutdown
exit
```

5. Skonfigurować interfejs prowadzący do Routera3 za pomocą poleceń:

```
interface serial0/1/1
ip address 192.168.23.2 255.255.255.0
clock rate 64000
no shutdown
exit
```

6. Skonfigurować protokół routingu, np. EIGRP, za pomocą poleceń:

```
router eigrp 1
no auto-summary
network 192.168.12.0 0.0.0.255
network 192.168.23.0 0.0.0.255
exit
```

7. Nawiązać połączenie z routerem Router1. Router będzie wykorzystany jako zakończenie szyfrowanego tunelu. Przejść do trybu konfiguracji globalnej za pomocą poleceń:

```
enable
configure terminal
```

8. Skonfigurować interfejs prowadzący do Routera2 za pomocą poleceń:

```
interface gigabitethernet0/0/0
ip address 192.168.12.1 255.255.255.0
no shutdown
exit
```

9. Skonfigurować interfejs do sieci lokalnej za pomocą poleceń:
```
interface gigabitethernet0/0/1
ip address 172.16.1.1 255.255.255.0
no shutdown
exit
```
10. Skonfigurować protokół routingu, np. EIGRP, za pomocą poleceń:
```
router eigrp 1
no auto-summary
network 172.16.1.0 0.0.0.255
network 192.168.12.0 0.0.0.255
exit
```
11. Włączyć protokół IKE odpowiedzialny za przeprowadzanie negocjacji parametrów połączenia między stronami komunikacji za pomocą poleceń:
```
crypto isakmp enable
```
12. Skonfigurować politykę bezpieczeństwa i określić jej priorytet, np. **10**. Mniejsza wartość priorytetu oznacza pierwszeństwo, jeżeli zdefiniowano wiele polityk. Ustawić uwierzytelnienie za pomocą klucza tajnego, wprowadzanego ręcznie, szyfrowanie **AES**, funkcję kontroli integralności **sha**, algorytm **Diffie-Helmana grupa 5**, czas dostępności tunelu 3600 s. Wykonać polecenia:
```
crypto isakmp policy 10
authentication pre-share
encryption aes 256
hash sha
group 5
lifetime 3600
end
```
13. Sprawdzić poprawność konfiguracji (rys. 55.17) za pomocą polecenia:
```
show crypto isakmp policy
```

```
Router#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #5 (1536 bit)
        lifetime:                3600 seconds, no volume limit
Router#
```

Rys. 55.17. **Konfiguracja polityki bezpieczeństwa**

14. Ustalić klucz i adres IP sąsiada za pomocą poleceń:
```
configure terminal
crypto isakmp key cisco address 192.168.23.3
```
15. Skonfigurować nazwany zbiór danych protokołów bezpieczeństwa (ang. *transform-set*) fazy 2:
```
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 1800
```

16. Skonfigurować listę ACL, określającą ruch, który zostanie zaszyfrowany (cała komunikacja między siecią **172.16.1.0** a siecią **172.16.3.0** korzystająca z protokołów IP i icmp). Wykonać polecenia:
```
access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.3.0
0.0.0.255
access-list 101 permit icmp 172.16.1.0 0.0.0.255 172.16.3.0
0.0.0.255
```
17. Połączyć wszystkie ustawienia w kryptomapę, która zostanie zaimplementowana na interfejsie. Kryptomapie nadać nazwę, np. **MYMAP**, i numer sekwencyjny, np. **10**. Wykonać polecenia:
```
crypto map MYMAP 10 ipsec-isakmp
match address 101
set peer 192.168.23.3
set pfs group5
set transform-set 50
set security-association lifetime seconds 900
exit
```
18. Zainstalować kryptomapę na interfejsie, za pomocą którego routery będą nawiązywać połączenia:
```
interface gigabitethernet0/0/0
crypto map MYMAP
end
```
19. Nawiązać połączenie z routerem Router3. Router będzie wykorzystany jako zakończenie szyfrowanego tunelu. Przejść do trybu konfiguracji globalnej za pomocą poleceń:
```
enable
configure terminal
```
20. Skonfigurować interfejs prowadzący do Routera2:
```
interface serial0/1/1
ip address 192.168.23.3 255.255.255.0
no shutdown
exit
```
21. Skonfigurować interfejs do sieci lokalnej:
```
interface gigabitethernet0/0/1
ip address 172.16.3.1 255.255.255.0
no shutdown
exit
```
22. Skonfigurować protokół routingu, np. EIGRP, za pomocą poleceń:
```
router eigrp 1
no auto-summary
network 172.16.3.0 0.0.0.255
network 192.168.23.0 0.0.0.255
exit
```
23. Włączyć protokół IKE odpowiedzialny za przeprowadzanie negocjacji parametrów połączenia między stronami komunikacji:
```
crypto isakmp enable
```

24. Skonfigurować politykę bezpieczeństwa, tak jak w routerze Routerl. Wykonać polecenia:
```
crypto isakmp policy 10
authentication pre-share
encryption aes 256
hash sha
group 5
lifetime 3600
end
```
25. Sprawdzić poprawność konfiguracji za pomocą polecenia:
```
show crypto isakmp policy
```
26. Ustalić klucz i adres IP sąsiada za pomocą poleceń:
```
configure terminal
crypto isakmp key cisco address 192.168.12.1
```
27. Skonfigurować nazwany zbiór danych protokołów bezpieczeństwa (ang. *transform-set*) fazy 2:
```
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 1800
```
28. Skonfigurować listę ACL, określającą ruch, który zostanie zaszyfrowany (cała komunikacja między siecią **172.16.3.0** a siecią **172.16.1.0** korzystająca z protokołów IP i icmp). Wykonać polecenia:
```
access-list 101 permit ip 172.16.3.0 0.0.0.255 172.16.1.0
0.0.0.255
access-list 101 permit icmp 172.16.3.0 0.0.0.255 172.16.1.0
0.0.0.255
```
29. Połączyć wszystkie ustawienia w kryptomapę, która zostanie zaimplementowana na interfejsie. Kryptomapie nadać nazwę, np. **MYMAP**, i numer sekwencyjny, np. **10**. Wykonać polecenia:
```
crypto map MYMAP 10 ipsec-isakmp
match address 101
set peer 192.168.12.1
set pfs group5
set transform-set 50
set security-association lifetime seconds 900
exit
```
30. Zainstalować kryptomapę na interfejsie, za pomocą którego routery będą nawiązywać połączenia:
```
interface serial 0/1/1
crypto map MYMAP
end
```
31. Przetestować połączenie. Za pomocą polecenia **ping** wysłać pakiety testowe z komputera w sieci LAN1 do serwera w sieci LAN2. W przeglądarce internetowej komputera w sieci LAN1 otworzyć stronę z serwera w sieci LAN2.
Na rys. 55.18 pokazano wynik działania polecenia **show crypto isakmp sa**, wydanego przed testowaniem połączenia (pierwsze uruchomienie) i po testowaniu (drugie uruchomienie). Potwierdza to utworzenie tunelu między routerami.

KODY

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state      conn-id   slot     status

IPv6 Crypto ISAKMP SA


Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state      conn-id   slot     status
192.168.23.3    192.168.12.1    QM_IDLE    1038      0        ACTIVE


IPv6 Crypto ISAKMP SA

Router#
```

Rys. 55.18. **Wyświetlanie informacji o tunelu między routerami**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zaplanuj sieć rozproszoną między kilkoma miastami w Polsce. Zaplanuj łącza VPN między miastami. Narysuj schemat sieci i zaznacz adresy IP używane w poszczególnych sieciach. Dla poszczególnych tuneli wybierz polityki bezpieczeństwa, np. algorytmy szyfrowania, funkcje haszujące.

56 Rodzaje i sposób obsługi urządzeń telefonii internetowej

ZAGADNIENIA

Konwergencja sieci **Telefonia VoIP** **Korzystanie z VoIP**

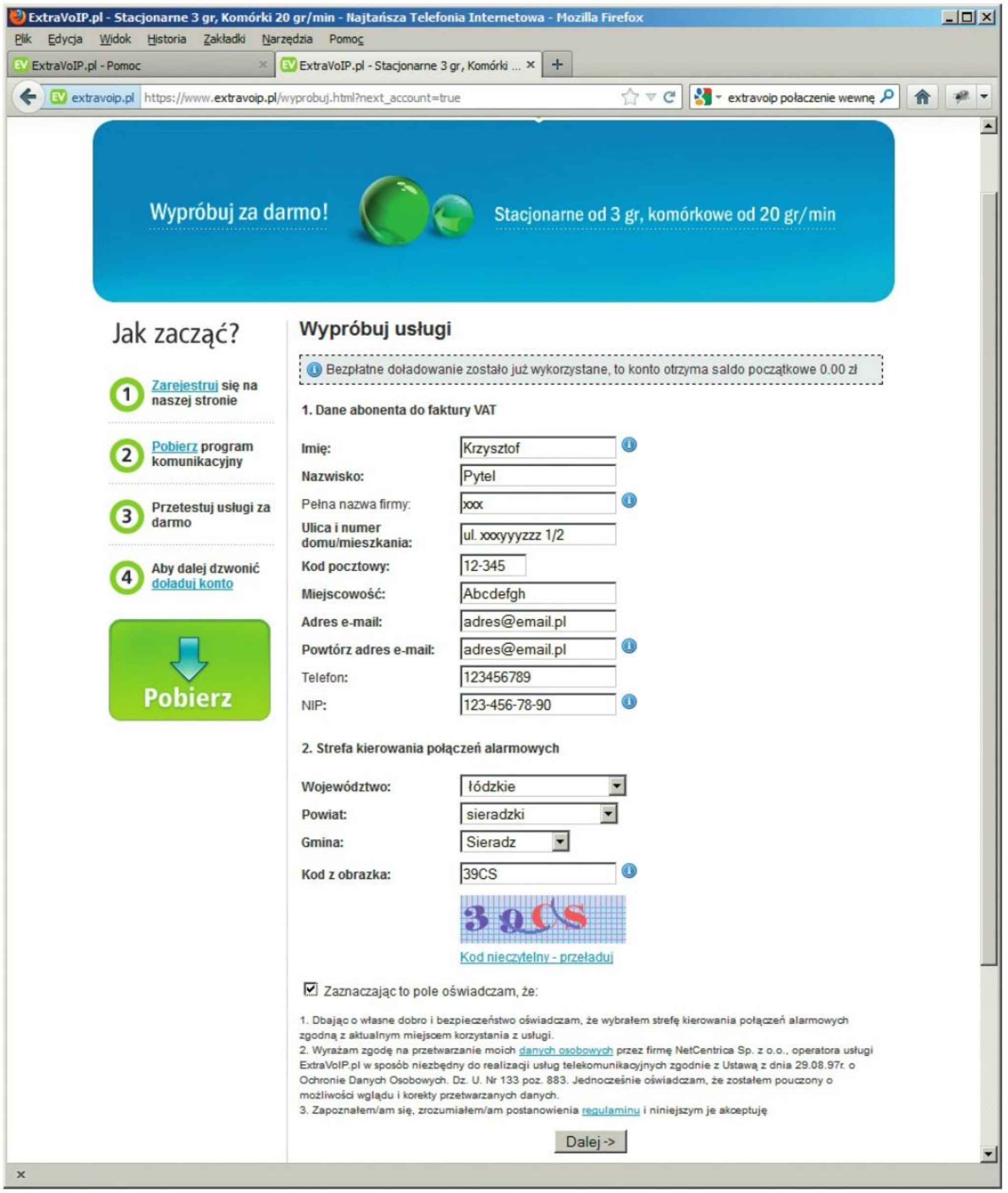
Sieci komputerowe można wykorzystać do przesyłania danych między komputerami a innymi urządzeniami. Przykładowo: przez sieć komputerową można przesyłać audycje radiowe i telewizyjne, rozmowy głosowe i dane z monitoringu. To zjawisko nazywa się **konwergencją** sieci i polega na dążeniu sieci do ujednolicenia standardów i wykorzystania jednego typu sieci do przesyłania wszystkich rodzajów danych. Wszystkie dane są zamieniane na postać cyfrową i przesyłane za pomocą sieci komputerowej korzystającej z protokołu IP.

Coraz większą popularność zyskuje usługa udostępniania rozmów głosowych przesyłanych za pośrednictwem sieci **VoIP** (ang. *Voice over Internet Protocol*). Jest to technologia cyfrowa umożliwiająca prowadzenie rozmów głosowych za pomocą łączy internetowych lub sieci wykorzystujących protokół IP, popularnie nazywana telefonią internetową. Dominującym protokołem służącym do zestawiania sesji między klientami VoIP jest **SIP** (ang. *Session Initiation Protocol*). Innym bardzo popularnym protokołem jest **H.323**. SIP dostarcza funkcje obsługi połączenia takie jak w stacjonarnej telefonii: wybieranie numeru, dzwonek w telefonie, sygnał zajętości itp.

Aby korzystać z usług telefonii internetowej, trzeba mieć stałe szerokopasmowe łącze internetowe o przepustowości co najmniej 128 kb/s. Rozmowy można prowadzić za pomocą komputera z zainstalowanym programem telekomunikacyjnym i zestawem słuchawkowym lub tradycyjnego aparatu telefonicznego podłączonego do **adaptera VoIP** (bramki VoIP).

Bramka VoIP umożliwia prowadzenie rozmów bez konieczności uruchamiania komputera. Aby korzystać z VoIP, należy zarejestrować się w firmie świadczącej usługi i opłacić abonament lub doładować konto. W zamian można prowadzić rozmowy z telefonami stacjonarnymi i komórkowymi oraz uzyskać publiczny numer telefonu (może to być związane z dodatkowymi opłatami). Rozmowy z innymi abonentami prowadzone wewnątrz sieci są zazwyczaj bezpłatne, ale zależy to od oferty dostawcy.

Aby uzyskać konto w usłudze VoIP, należy wypełnić odpowiedni formularz na stronie wybranego operatora. Przykład formularza przedstawiono na rys. 56.1.



Rys. 56.1. Przykładowy formularz rejestracyjny konta VoIP

Po zarejestrowaniu konta zostanie wyświetlone potwierdzenie rejestracji zawierające informacje (rys. 56.2) niezbędne do konfiguracji usługi programu komunikacyjnego lub bramki VoIP. Należy je wydrukować i przechowywać w bezpiecznym miejscu. Ze względu na bezpieczeństwo część informacji z rys. 56.2 usunięto.

Dziękujemy za rejestrację konta w naszej sieci.

Prosimy zanotować i przechowywać w bezpiecznym miejscu poniższe dane autoryzacyjne, służą one zarówno do zalogowania do panelu klienta, jak i do konfiguracji oprogramowania i sprzętu. Kopia informacji zawartych na tej stronie została wysłana pod wskazany podczas rejestracji adres e-mail.

Dane logowania

Nazwa użytkownika (login): extravoip_
Hasło:
Uwaga: wielkość liter w haśle ma znaczenie
Serwer SIP/Proxy/Registrar: sip.extravoip.pl
Zalecane kodeki: G.711 ulaw i G.711 alaw (oba powinny być zawsze aktywne), opcjonalnie G.729

Wykonywanie połączeń

Numery krajowe: (bez zera) + numer telefonu, np. 022123456
Numery zagraniczne: 00 + kierunkowy kraju + numer abonenta
Bezpłatny numer testowy: 600
Sprawdzenie stanu konta pod numerem: 500

Program komunikacyjny (softphone)

Pobierz program ZoIPer

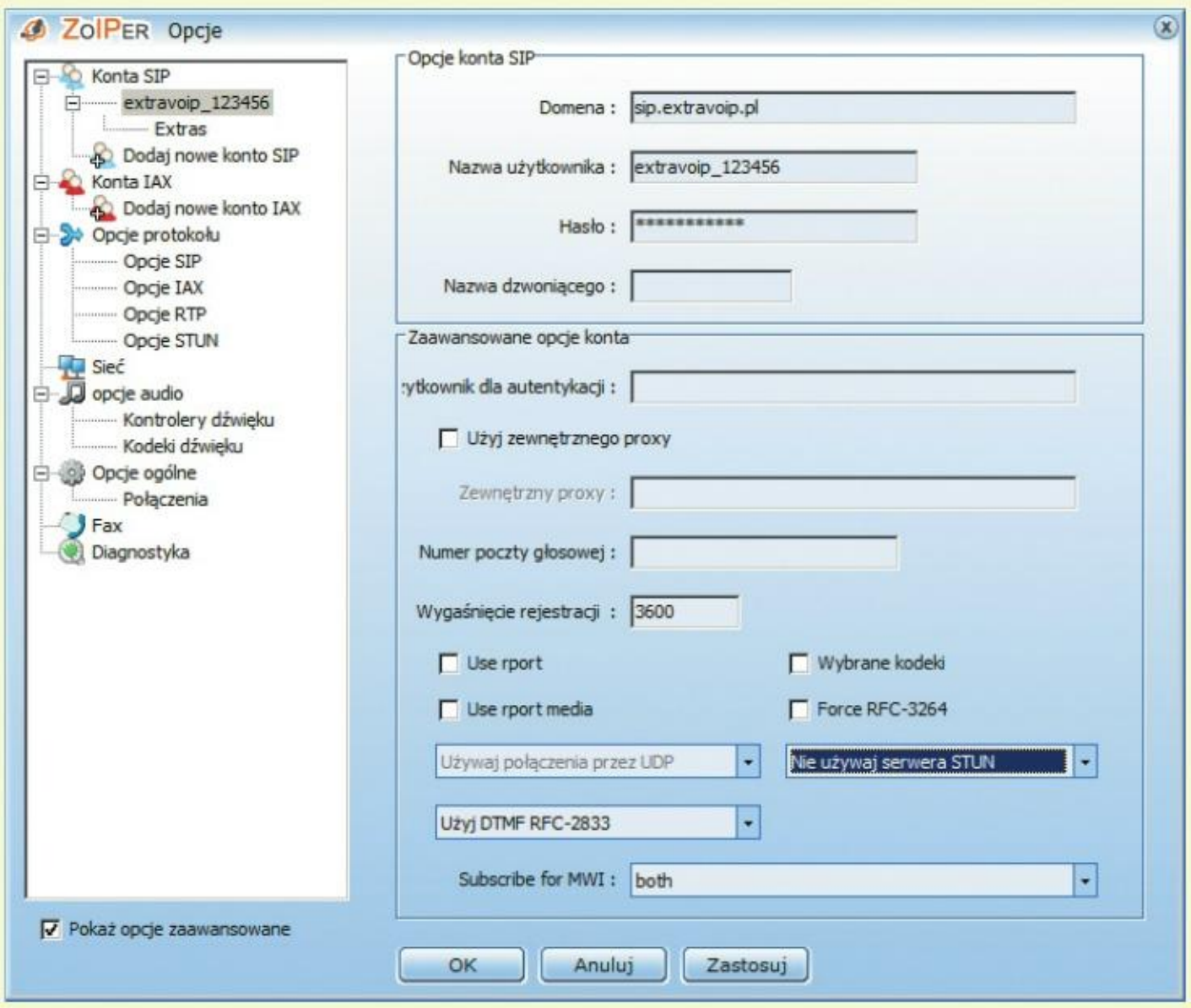
Rys. 56.2. Potwierdzenie rejestracji konta VoIP

PRZYKŁAD 56.1

Konfiguracja programu komunikacyjnego VoIP

Aby skonfigurować program komunikacyjny umożliwiający prowadzenie rozmów VoIP za pomocą zestawu słuchawkowego, należy wykonać następujące czynności:

1. Uzyskać konto u operatora i niezbędne dane do konfiguracji programu.
2. Pobrać program komunikacyjny. Można wybrać dowolny program, ale najbezpieczniejszy jest program polecany przez danego operatora. Uzyskujemy pewność, że został on dokładnie przetestowany i nie będzie sprawiał problemów, a operator zapewni nam wsparcie podczas instalacji, konfiguracji i użytkowania.



Rys. 56.3. Konfiguracja konta SIP

3. Zainstalować program zgodnie ze wskazówkami operatora.
4. Skonfigurować program: wprowadzić dane uzyskane podczas rejestracji i uwzględnić wskazówki operatora (rys. 56.3). Wprowadzić nazwę domeny operatora, nazwę użytkownika i jego hasło. Wybrać opcję **Nie używaj serwera STUN**.
5. Kliknąć przycisk **Zastosuj**. Jeżeli wszystkie dane zostały wprowadzone poprawnie, to program powinien zostać zarejestrowany. Od tego momentu można nawiązywać i odbierać połączenia.
6. Opcjonalnie można uzyskać od operatora publiczny numer telefonu – umożliwi wybieranie numerów telefonów stacjonarnych lub komórkowych tak jak w tradycyjnej telefonii.

Aby nawiązać połączenie z telefonem stacjonarnym lub komórkowym, w pole **Połączenie do wykonania** trzeba wpisać numer telefonu w sposób identyczny jak w tradycyjnym telefonie i nacisnąć przycisk [ENTER] lub kliknąć ikonkę niebieskiej słuchawki (na rys. 56.4 zaznaczona strzałką).



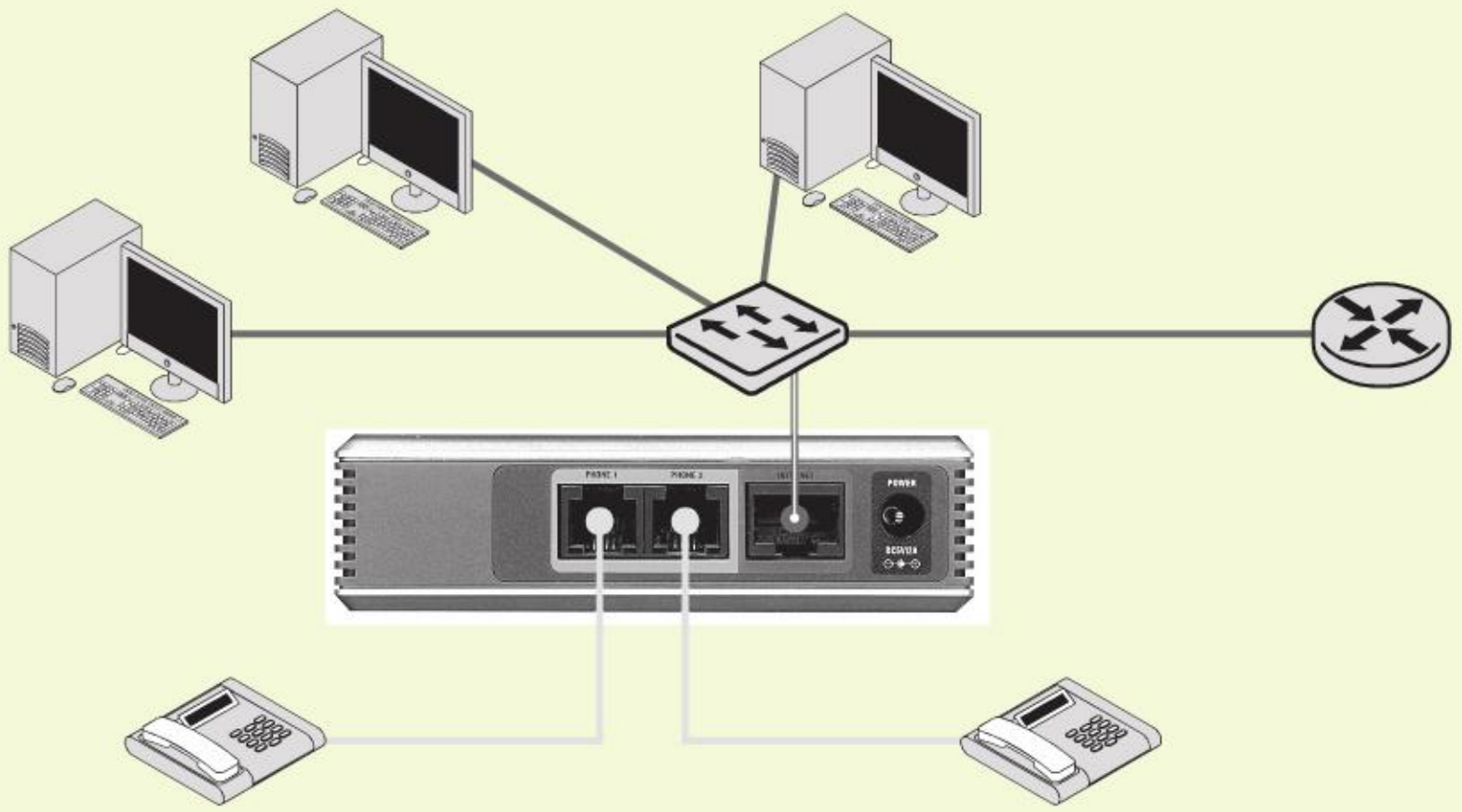
Rys. 56.4. **Nawiązywanie połączenia za pomocą programu ZoIPer**

PRZYKŁAD 56.2

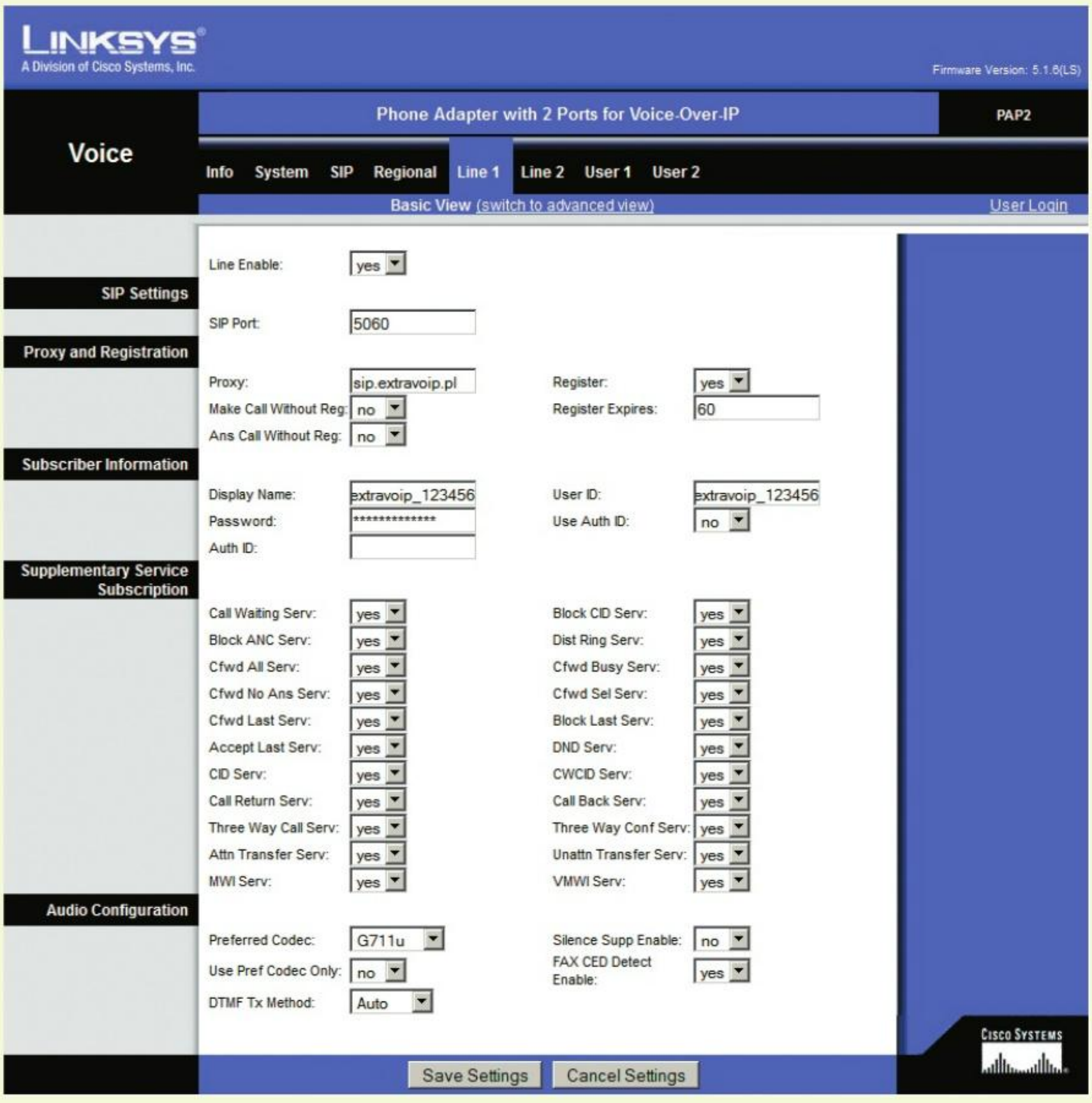
Konfiguracja bramki VoIP

W tym ćwiczeniu zostanie pokazany proces konfigurowania bramki VoIP na przykładzie Linksys PAP2. Aby umożliwić prowadzenie rozmów głosowych za pośrednictwem bramki, należy:

1. Połączyć port **INTERNET** bramki z przełącznikiem (rys. 56.5). Do portu **PHONE 1** przyłączyć telefon stacjonarny, do portu **PHONE 2** można przyłączyć drugi telefon lub faks (jeżeli użytkownik ma dwa konta u operatora).
2. Wybrać za pomocą klawiatury telefonu tonowo ********, a następnie **110#** – bramka odpowie za pomocą syntezatora głosu – poda adres IP.
3. Za pomocą przeglądarki internetowej zalogować się do panelu konfiguracyjnego bramki przez wpisanie w przeglądarce uzyskanego w punkcie 2. adresu IP.
4. Kliknąć w prawym górnym rogu **Admin Login**.



Rys. 56.5. **Schemat połączeń bramki VoIP**



Rys. 56.6. **Konfiguracja bramki VoIP**

5. Wybrać linię, do której jest przyłączony telefon (**`Line 1`** lub **`Line 2`**).
6. Podać parametry niezbędne do działania bramki według zaleceń operatora, np.:
   - Display name: login otrzymany podczas rejestracji;
   - Password: hasło;
   - User ID: login otrzymany podczas rejestracji.

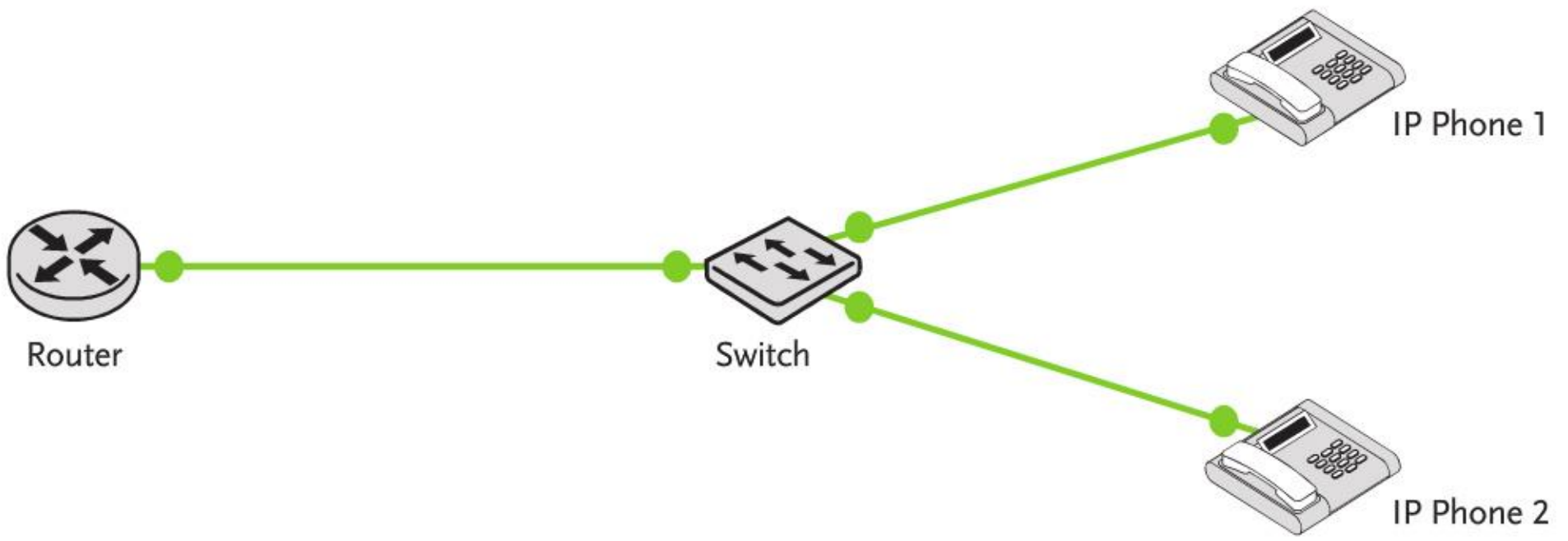
   Pozostałe opcje – według zaleceń operatora.
7. Kliknąć przycisk **`Save Settings`** w celu zapisania ustawień.

Okno z wprowadzonymi przykładowymi danymi pokazano na rys. 56.6.

56.1. Konfigurowanie usługi VoIP w sieci lokalnej

Usługa VoIP może być używana w sieciach lokalnych do wykonywania połączeń głosowych i telekonferencyjnych. Rozmowy głosowe i połączenia telekonferencyjne są wrażliwe na opóźnienia w przesyłaniu danych. Aby zapewnić odpowiednią jakość połączeń, zwykle na potrzeby VoIP tworzy się oddzielną sieć VLAN. Dane przesyłane w sieci Voice VLAN mają zwykle wyższy priorytet niż inne dane, przesyłane za pośrednictwem pozostałych sieci VLAN.

Użytkownicy sieci mają specjalne telefony IP. Taki telefon odgrywa rolę trzyportowego przełącznika: jeden port do podłączenia do sieci lokalnej, jeden port do podłączenia komputera, a z ostatniego portu korzysta telefon. Pozwala to na podłączenie telefonu IP i komputera do pojedynczego gniazda sieciowego. W routerze działającym w sieci lokalnej dodatkowo należy skonfigurować usługę **Call Manager**, dzięki której może on pełnić funkcję centralki telefonicznej (nie każdy router nadaje się do tego). Schemat przykładowej sieci przystosowanej do obsługi VoIP przedstawiono na rys. 56.7.



Rys. 56.7. **Schemat przykładowej sieci przystosowanej do obsługi VoIP**

PRZYKŁAD 56.3

Konfiguracja sieci do obsługi VoIP

W tym przykładzie zostanie pokazana konfiguracja sieci komputerowej, w której są obsługiwane telefony VoIP. W sieci będą umieszczone dwa telefony, które otrzymają dane konfiguracyjne z serwera DHCP i Call Managera routera Cisco 2811. Do zbudowania sieci wykorzystamy Cisco Packet Tracer. Ze względu na funkcję Call Manager do wykonania ćwiczenia należy wybrać router 2811.

! UWAGA

Zasilanie telefonów IP może być realizowane za pomocą technologii PoE lub za pomocą zasilacza sieciowego. Nie zapomnij podłączyć zasilacza telefonu.

Aby skonfigurować sieć, należy:

1. Uruchomić Cisco Packet Tracer, wybrać odpowiednie urządzenia i połączyć je według schematu pokazanego na rys. 56.7.
2. Nawiązać połączenie z routerem i przejść do trybu konfiguracji globalnej za pomocą poleceń:
   ```
   enable
   configure terminal
   ```
3. Skonfigurować interfejs F0/0 za pomocą poleceń:
   ```
   interface FastEthernet0/0
   ip address 192.168.1.1 255.255.255.0
   no shutdown
   exit
   ```
4. Skonfigurować serwer DHCP:
   - z puli przydzielanych dynamicznie adresów wykluczyć adresy wykorzystywane przez urządzenia sieciowe, np. adresy od **192.168.10.1** do **192.168.10.10**. Wydać polecenie:
     ```
     ip dhcp excluded-address 192.168.10.1 192.168.10.10
     ```
   - utworzyć pulę adresów przydzielanych dynamicznie za pomocą polecenia:
     ```
     ip dhcp pool VOICE
     ```
   - określić zakres przydzielanych dynamicznie adresów za pomocą polecenia:
     ```
     network 192.168.1.0 255.255.255.0
     ```
   - określić adres bramy za pomocą polecenia:
     ```
     default-router 192.168.1.1
     ```
   - zdefiniować adres serwera TFTP, z którego telefony będą pobierały dane konfiguracyjne, za pomocą polecenia:
     ```
     option 150 ip 192.168.1.1
     ```
   - zakończyć konfigurację puli adresów za pomocą polecenia:
     ```
     exit
     ```
5. Skonfigurować usługę Call Manager Express:
   - włączyć usługę Call Manager Express za pomocą polecenia:
     ```
     telephony-service
     ```
   - określić maksymalną liczbę numerów za pomocą polecenia:
     ```
     max-dn 5
     ```
   - określić maksymalną liczbę telefonów za pomocą polecenia:
     ```
     max-ephones 5
     ```
   - określić adres IP i numer portu źródła plików konfiguracyjnych za pomocą polecenia:
     ```
     ip source-address 192.168.1.1 port 2000
     ```
   - włączyć automatyczne przypisywanie numerów do przycisków za pomocą poleceń:
     ```
     auto assign 4 to 6
     auto assign 1 to 5
     ```

- zakończyć konfigurację Call Managera za pomocą polecenia:
  exit

6. Przypisać numer 12345 do telefonu 1 i 12346 do telefonu 2 za pomocą poleceń:
   ```
   ephone-dn 1
   number 12345
   ephone-dn 2
   number 12346
   ```
7. Nawiązać połączenie z przełącznikiem i przejść do trybu konfiguracji globalnej za pomocą poleceń:
   ```
   enable
   configure terminal
   ```
8. Wybrać zakres interfejsów, np. od 1 do 5, i skonfigurować do pracy w sieci VLAN 1 za pomocą poleceń:
   ```
   interface range fa0/1 - 5
   switchport mode access
   switchport voice vlan 1
   ```
9. Przetestować działanie telefonów:
   - kliknąć telefon i wybrać zakładkę GUI;
   - podnieść (kliknąć) słuchawkę telefonu 1;
   - wybrać numer telefonu 2;
   - sprawdzić, czy zacznie pulsować czerwona dioda w telefonie, którego numer wybrano.

Na rys. 56.8 przedstawiono sposób testowania telefonów IP.

KODY

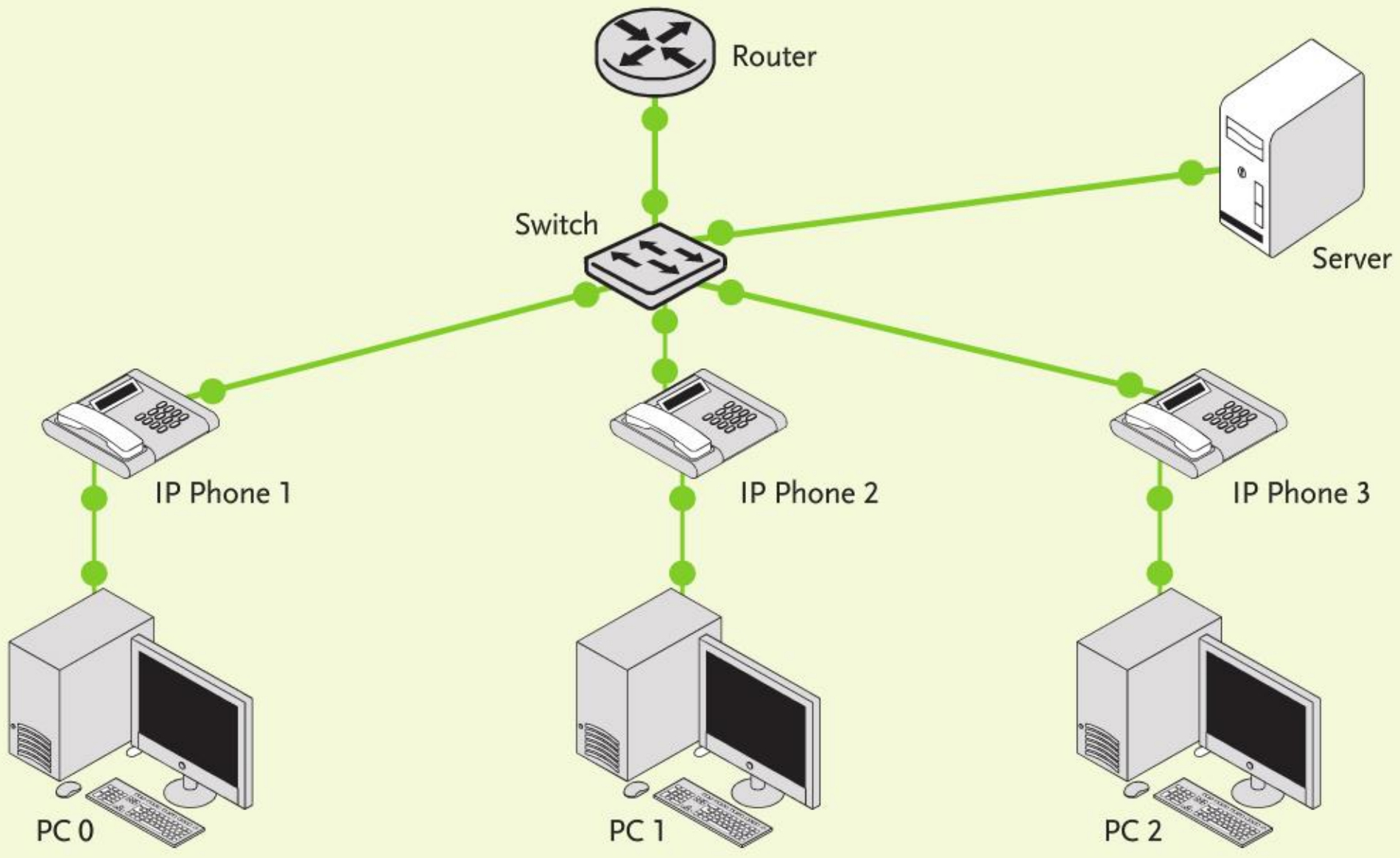


Rys. 56.8. Testowanie telefonów IP

PRZYKŁAD 56.4[5]

Konfiguracja sieci do przesyłania danych i VoIP

W tym przykładzie zostanie pokazana konfiguracja sieci komputerowej, w której wydzielono dwie sieci wirtualne: **`VLAN 50`** do przesyłania danych i **`VLAN 10`** do obsługi komunikacji VoIP. W sieci **`DATA`** będą wykorzystywane adresy **`192.168.50.0/24`**, natomiast w sieci **`VOICE`** adresy z sieci **`192.168.10.0/24`**, przydzielane przez serwer DHCP, skonfigurowany na routerze. Do zbudowania sieci zostanie wykorzystany Cisco Packet Tracer. Ze względu na funkcję Call Manager należy wybrać router 2811. Schemat przykładowej sieci pokazano na rys. 56.9.



Rys. 56.9. **Schemat przykładowej sieci przystosowanej do obsługi VoIP i danych**

UWAGA

Zasilanie telefonów IP może być realizowane za pomocą technologii PoE lub za pomocą zasilacza sieciowego. Nie zapomnij podłączyć zasilacza telefonu.

Aby skonfigurować sieć, należy:

1. Uruchomić Cisco Packet Tracer, wybrać odpowiednie urządzenia i połączyć je według schematu z rys. 56.9.
2. Utworzyć sieci VLAN na przełączniku:
   - nawiązać połączenie z przełącznikiem i przejść do trybu konfiguracji globalnej za pomocą poleceń:

```
enable
configure terminal
```

KODY

[5] Dla uczniów zaawansowanych lub szczególnie zainteresowanych.

- utworzyć sieci VLAN 10 i VLAN 50:

```
vlan 10
name VOICE
exit
vlan 50
name DATA
exit
```

3. Skonfigurować porty przełącznika. Do każdego portu będą przyłączone dwie sieci VLAN – porty muszą pracować w trybie trunk. Wydać polecenia:

```
interface range fastEthernet 0/1 - 24
switchport mode trunk
switchport trunk allowed vlan all
switchport voice vlan 10
switchport trunk native vlan 50
exit
```

4. Skonfigurować serwer DHCP na routerze. Adresy IP dla telefonów i komputerów mogą być przydzielane dynamicznie lub statycznie. Aby skonfigurować router do pełnienia funkcji serwera DHCP, należy:
   - nawiązać połączenie z routerem i przejść do trybu konfiguracji globalnej za pomocą poleceń:
     ```
     enable
     configure terminal
     ```
   - z puli przydzielanych dynamicznie adresów wykluczyć adresy wykorzystywane przez urządzenia sieciowe, np. adresy od **192.168.10.1** do **192.168.10.10**. Wydać polecenie:
     ```
     ip dhcp excluded-address 192.168.10.1 192.168.10.10
     ```
   - zdefiniować pulę adresów dla sieci VOICE. Wykonać polecenia:
     - zdefiniować pulę o nazwie VOICE:
       ```
       ip dhcp pool VOICE
       ```
     - określić zakres przydzielanych dynamicznie adresów:
       ```
       network 192.168.10.0 255.255.255.0
       ```
     - określić adres bramy:
       ```
       default-router 192.168.10.1
       ```
     - zdefiniować adres serwera TFTP, z którego telefony będą pobierały dane konfiguracyjne:
       ```
       option 150 ip 192.168.10.1
       ```
     - zakończyć konfigurację puli adresów:
       ```
       exit
       ```
   - zdefiniować pulę adresów dla sieci DATA. Konfiguracja przebiega analogicznie jak dla sieci VOICE, ale nie jest konieczne definiowanie adresu serwera TFTP. Wykonać polecenia:

```
ip dhcp excluded-address 192.168.50.1 192.168.50.10
ip dhcp pool DATA
network 192.168.50.0 255.255.255.0
default-router 192.168.50.1
exit
```

5. Skonfigurować interfejs sieci lokalnej w routerze. W interfejsie fizycznym fastEthernet0/0 zostaną wydzielone dwa podinterfejsy (ang. *subinterfaces*) do obsługi sieci VLAN. Wykonać polecenia:
   - wybrać podinterfejs do obsługi sieci VOICE:
     `interface fastEthernet 0/0.10`
     – określić protokół znakowania ramek i numer sieci VLAN:
       `encapsulation dot1Q 10`
     – przydzielić adres IP dla podinterfejsu:
       `ip address 192.168.10.1 255.255.255.0`
     – zakończyć konfigurację podinterfejsu:
       `exit`
   - w analogiczny sposób skonfigurować podinterfejs dla sieci DATA („native" oznacza, że w tej sieci będą przesyłane również ramki nieoznakowane):
     `interface fastEthernet 0/0.50`
     `encapsulation dot1Q 50 native`
     `ip address 192.168.50.1 255.255.255.0`
     `exit`
   - włączyć interfejs – włączenie interfejsu fizycznego skutkuje włączeniem wszystkich jego podinterfejsów:
     `interface fastEthernet 0/0`
     `no shutdown`
     `exit`
6. Włączyć usługę centralki telefonicznej (Call Manager):
   - włączyć usługę Call Manager:
     `telephony-service`
   - określić maksymalną liczbę telefonów:
     `max-ephones 10`
   - określić maksymalną liczbę numerów:
     `max-dn 10`
   - określić adres i numer portu Call Managera:
     `ip source-address 192.168.10.1 port 2000`
   - utworzyć pliki konfiguracyjne dla telefonów:
     `create cnf-files`
   - zakończyć konfigurację Call Managera:
     `exit`
7. Zdefiniować telefony:
   - telefon 1:
     – wybrać telefon:
       `ephone 1`
     – określić adres MAC telefonu (wpisać właściwy adres MAC telefonu):
       `mac-address 0007.ecc7.4d0a`
     – określić typ telefonu:
       `type 7960`
     – zakończyć konfigurację telefonu:
       `exit`
   - w analogiczny sposób skonfigurować telefony 2 i 3:

```
ephone 2
mac-address 00d0.bcba.da13
type 7960
exit
ephone 3
mac-address 00d0.ff27.444b
type 7960
exit
```

8. Przydzielić telefonom numery:
   - telefon 1:
     - przypisanie numeru 1:
       `ephone-dn 1`
     - przypisywany numer:
       `number 12345`
     - koniec konfiguracji numeru:
       `exit`
   - w analogiczny sposób skonfigurować telefony 2 i 3:

```
ephone-dn 2
number 12346
exit
ephone-dn 3
number 12347
exit
```

9. Zdefiniować przyciski szybkiego wybierania (w Cisco Packet Tracer przyciski nie są dostępne):

```
ephone 1
button 1:1
exit
ephone 2
button 1:2
exit
ephone 3
button 1:3
exit
```

10. Skonfigurować adres serwera:
    Adres IP: **`192.168.50.5`**
    Maska podsieci: **`255.255.255.0`**
    Brama domyślna: **`192.168.50.1`**
11. Skonfigurować komputery PC do pobierania adresów z serwera DHCP.
12. Przetestować działanie telefonów. Kliknąć telefon i wybrać zakładkę GUI. Podnieść (kliknąć) słuchawkę telefonu. Wybrać numer telefonu. Sprawdzić, czy zacznie pulsować czerwona dioda w telefonie, którego numer wybrano.
13. Przetestować możliwość komunikacji między komputerem a serwerem, np. poleceniem **`ping`**.

! UWAGA

Usługę telefonii VoIP można również skonfigurować w sieci rozległej, w której telefony są zlokalizowane w różnych sieciach lokalnych.

56.2. Konfigurowanie telefonów VoIP i protokołu SIP

SIP to protokół do zestawiania sesji między jednym lub wieloma klientami. SIP dostarcza funkcje obsługi połączenia i inne cechy oraz operacje dostępne w publicznej sieci telefonicznej, takie jak: wybieranie numeru, dzwonek w telefonie, sygnał zajętości. Obecnie jest najczęściej używany w VoIP.

PRZYKŁAD 56.5

Konfiguracja sieci do obsługi VoIP i protokołu SIP

W tym przykładzie zostanie pokazana konfiguracja sieci komputerowej, w której są obsługiwane telefony VoIP wspierające protokół SIP. W sieci będą umieszczone dwa telefony Cisco IP Phone 7821, które otrzymają dane konfiguracyjne z serwera DHCP i Call Managera routera Cisco. Do zbudowania sieci należy wykorzystać router, który obsługuje funkcje VoIP.

! UWAGA

Cisco Packet Tracert nie ma funkcji pozwalających na konfigurowanie protokołu SIP.

W ćwiczeniu przyjęto, że zasilanie telefonów IP będzie odbywać się za pomocą technologii PoE, a do zasilania zostaną wykorzystane indywidualne zasilacze. Zwróć uwagę na prawidłowe podłączenie zasilacza. Aby skonfigurować sieć, należy:

1. Połączyć urządzenia według schematu pokazanego na rys. 56.7.
2. Nawiązać połączenie z routerem i przejść do trybu konfiguracji globalnej za pomocą poleceń:
```
enable
configure terminal
```
3. Skonfigurować adres IP na interfejsie przyłączonym do przełącznika:
```
interface GigabitEthernet 0/0/0
ip address 192.168.10.1 255.255.255.0
no shutdown
exit
```
4. Skonfigurować serwer DHCP, przydzielający adresy IP dla telefonów:
```
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp pool voice
network 192.168.10.0 255.255.255.0
option 150 ip 192.168.10.1
default-router 192.168.10.1
exit
```

5. Telefony mogą pobierać obrazy, system i pliki konfiguracyjne z pamięci FLASH routera za pomocą protokołu TFTP. Trzeba określić nazwy plików odpowiednie dla firmware'u telefonów, np. dla telefonów serii 78xx:
```
tftp-server flash:sip78xx.12-5-1SR3-74.loads
tftp-server flash:kern2.78xx.12-5-1SR3-74.sbn
tftp-server flash:kern78xx.12-5-1SR3-74.sbn
tftp-server flash:rootfs2.78xx.12-5-1SR3-74.sbn
tftp-server flash:rootfs78xx.12-5-1SR3-74.sbn
tftp-server flash:sboot2.78xx.12-5-1SR3-74.sbn
tftp-server flash:sboot78xx.12-5-1SR3-74.sbn
```
6. Aktywować usługę VoIP, zezwolić na zestawianie połączeń SIP do SIP i ustawić parametry globalne konfiguracji:
   - wybrać tryb konfiguracji VoIP:
     `voice service voip`
   - zezwolić na zestawianie połączeń SIP do SIP:
     `allow-connections sip to sip`
   - wybrać tryb konfiguracji protokołu SIP:
     `sip`
   - włączyć funkcję rejestratora SIP:
     `registrar server expires max 600 min 60`
   - wejść w tryb konfiguracji globalnej rejestru:
     `voice register global`
   - wybrać tryb Cisco Unified CME:
     `mode cme`
   - wskazać adres IP i numer portu Call Managera:
     `source-address 192.168.10.1 port 5060`
7. Wybrać liczbę obsługiwanych numerów, typ aparatu i domyślnie pobierany obraz systemu oraz wygenerować pliki konfiguracyjne dla telefonów:
   - maksymalna liczba obsługiwanych numerów kierunkowych:
     `max-dn 10`
   - maksymalna liczba obsługiwanych telefonów:
     `max-pool 10`
   - typ aparatu i domyślnie pobierany obraz systemu:
     `load 7821 sip78xx.12-5-1SR3-74`
   - lokalizacja plików obrazu:
     `tftp-path flash:`
   - tworzenie profili telefonów:
     `create profile`
     `exit`
8. Dla każdego telefonu zdefiniować ustawienia: nazwy, numeru, adresu MAC (ustawić rzeczywisty adres telefonu), typ i używany kodek dźwięku.
   Przykładowo dla telefonu 1:
   - wybór trybu konfiguracji telefonu:
     `voice register dn 1`
   - nazwa telefonu wyświetlana na panelu:
     `name Phone1`

- numer przydzielony dla telefonu:
  number 101
- wybór trybu konfiguracji parametrów telefonu:
  voice register pool 1
- adres MAC telefonu:
  id mac 00AA.6E21.2BB0
- typ telefonu:
  type 7821
- rejestrowany numer telefonu:
  number 1 dn 1
- preferowany kodek dźwięku:
  codec g711ulaw

KODY

Dla telefonu 2:

```
voice register dn 2
name Phone2
number 102
voice register pool 2
id mac 700B.4F91.73F5
type 7821
number 1 dn 2
codec g711ulaw
end
```

9. Przetestować działanie telefonu.

UWAGA

W ćwiczeniu skonfigurowano tylko podstawowe funkcje i usługi wymagane do nawiązywania połączeń w sieci lokalnej.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyszukaj w internecie ofertę operatora VoIP.
2. Uzyskaj bezpłatne konto testowe u operatora (uwaga: osoby niepełnoletnie muszą mieć zgodę rodziców lub opiekunów). Po skonfigurowaniu programu komunikacyjnego i bramki spróbuj nawiązać połączenie z wybranym telefonem stacjonarnym.

57 Programy do administrowania lokalnymi sieciami komputerowymi

ZAGADNIENIA

Funkcja i działanie protokołu SNMP **Baza MIB i zawarte w niej informacje** **Typy komunikatów wymieniane między menedżerem a agentem SNMP**

Administrowanie sieciami komputerowymi jest zadaniem skomplikowanym i wymaga od administratora dobrego przygotowania zawodowego i systematyczności w pracy. Ponadto administrator musi dysponować wiedzą i programami umożliwiającymi wykonywanie zadań zawodowych. Podstawowym protokołem wykorzystywanym do administrowania urządzeniami sieciowymi jest **SNMP** (ang. *Simple Network Management Protocol*).

SNMP jest protokołem warstwy aplikacji, opracowanym w celu ułatwienia wymiany informacji związanych z zarządzaniem między urządzeniami sieciowymi. SNMP ułatwia administratorom sieci zarządzanie działaniem sieci oraz wyszukiwanie i rozwiązywanie problemów. To prosty protokół, ale o możliwościach wystarczających w obliczu poważniejszych problemów wynikających z zarządzania złożonymi sieciami.

Protokół SNMP zakłada istnienie w zarządzanej sieci dwóch rodzajów urządzeń – zarządzających i zarządzanych. **Urządzenie zarządzające** (ang. *Network Management Station*, NMS) ma uruchomiony odpowiedni program – **zarządcę SNMP** (ang. *manager SNMP*). Z kolei na **urządzeniu zarządzanym** jest uruchamiany **agent SNMP**. Dane dotyczące zarządzanej sieci są przechowywane w bazie **MIB** (ang. *Management Information Base*). Zarządca SNMP, zależnie od uprawnień, może odczytać lub zmienić dane z bazy MIB. W tym celu menedżer SNMP kontaktuje się z agentem na zarządzanym urządzeniu. Po odczytaniu wybranej zmiennej menedżer może się zapoznać z informacją o stanie urządzenia, natomiast zapis do zmiennej pozwala sterować zachowaniem się urządzenia w sieci. Agent może sam poinformować menedżera o zmianie swojego stanu w razie zajścia określonego zdarzenia (np. błędu lub uszkodzenia) za pomocą wysyłanego komunikatu **pułapki** (ang. *trap*).

Agent to funkcja oprogramowania umieszczona w każdym urządzeniu sieciowym, np. w routerach, przełącznikach, koncentratorach, drukarkach, serwerach. Baza MIB tego agenta przechowuje całą informację dotyczącą zarządzanego urządzenia. Agent może przechowywać informacje dotyczące zagadnień takich jak:

- liczba i stan obwodów wirtualnych;
- liczba otrzymywanych komunikatów o błędach określonego typu;
- liczba bajtów i pakietów wchodzących i wychodzących z urządzenia;
- maksymalna długość kolejki (dla routerów i innych urządzeń pośredniczących);
- wysłane i otrzymane komunikaty rozgłoszeniowe;
- interfejsy sieci, które przestają działać i które wznawiają pracę.

Dane w bazach MIB są zgrupowane w strukturze hierarchicznej (strukturze drzewa) i zawierają informacje na temat danego urządzenia. Istnieją **standardowe MIB** i **MIB specyficzne**, przeznaczone do zarządzania różnymi urządzeniami konkretnych dostawców. Obiekty liści

drzewa reprezentują określone zasoby, działania lub informacje, które mogą być zarządzane. Każdy zarządzany obiekt ma przypisany unikatowy identyfikator zapisywany w postaci ciągu liczb, np. **`OID=.1.3.6.1.2.1.1.4.0`**. SNMP używa tych identyfikatorów obiektów do identyfikacji zmiennych MIB, które mają być uzyskane lub zmodyfikowane.

Urządzenie zarządzające NMS jest zwykle oddzielną stacją roboczą, na której zainstalowano aplikację zarządzania. Aplikacja zarządzania obejmuje interfejs, np. tekstowy lub graficzny, pozwalający zarządzać siecią autoryzowanym zarządcom. Odpowiada na polecenia użytkownika i na polecenia wydawane agentom zarządzania w całej sieci. Agent zarządzania odpowiada na żądania informacji i na żądania działań pochodzące z NMS. Komunikacja między menedżerem a agentem opiera się na wymianie informacji. Podstawą są trzy typy komunikatów:

- **Get** – ustawia stację zarządzania do otrzymania wartości obiektów MIB od agenta;
- **Set** – umożliwia stacji zarządzania ustawienie wartości obiektów MIB w agencie;
- **Trap** – umożliwia agentowi powiadamianie stacji zarządzającej o ważnych zdarzeniach.

Aplikacje zarządzania mogą być prostymi programami działającymi z wiersza poleceń, np.:

- **SnmpWalk** – do przeglądania całego drzewa MIB;
- **SnmpSet** – do wprowadzania wartości do bazy MIB;
- **SnmpGet** – do odczytywania pojedynczych wartości z drzewa MIB.

Wspomniane narzędzia nie są częścią wielu systemów operacyjnych. W związku z tym wymagają instalacji lub konfiguracji. Można je pobrać z internetu, np. ze strony projektu http://www.net-snmp.org/download.html.

PRZYKŁAD 57.1

Zarządzanie routerem za pomocą protokołu SNMP

W ćwiczeniu zademonstrujemy działanie protokołu SNMP na przykładzie aplikacji zarządzania działającej w wierszu polecenia na routerze firmy CISCO. Zostanie wyświetlony fragment drzewa MIB. Zostanie również wprowadzona i wyświetlona pojedyncza wartość parametru.

Aby zarządzać routerem lub innym urządzeniem za pomocą protokołu SNMP, należy:

1. Połączyć komputer z routerem i nawiązać sesję.
2. Uaktywnić protokół SNMP – skonfigurować hasło i opcjonalnie tryb dostępu.
   W tym celu w globalnym trybie konfiguracyjnym trzeba wydać polecenie:
   `snmp-server community zsprw rw`
   W tym poleceniu zdefiniowano grupę **`zsprw`** i tryb pracy **`rw`** – do odczytu i zapisu (rys. 57.1).

```
R1(config)#snmp-server community zsprw rw
R1(config)#
```

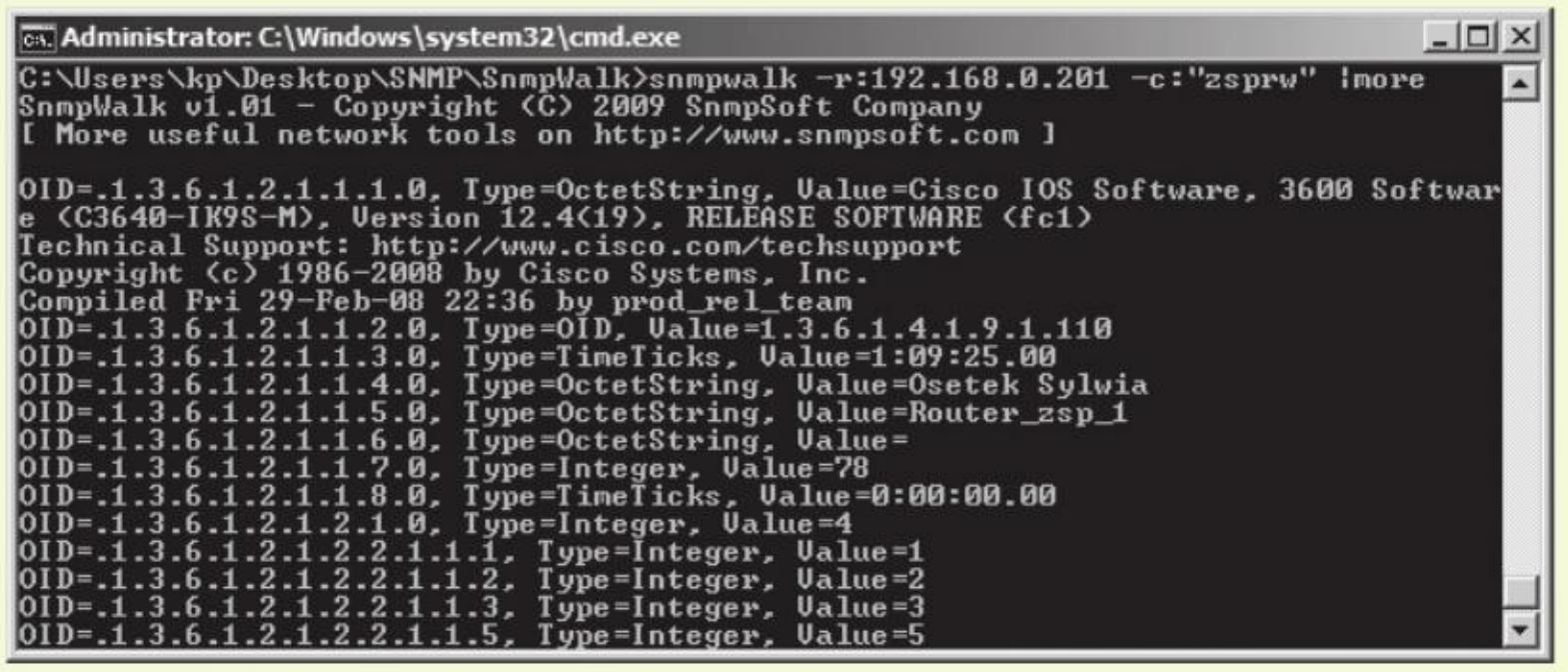
Rys. 57.1. **Uaktywnianie protokołu SNMP**

3. W celu sprawdzenia, czy polecenie zostało wykonane prawidłowo, można wyświetlić listę grup dostępu. Na rys. 57.2 można zweryfikować, czy została utworzona grupa o nazwie **`zsprw`**.

```
R1#show snmp group
groupname: ILMI                                 security model:v1
readview : *ilmi                                writeview: *ilmi
notifyview: <no notifyview specified>
row status: active
groupname: ILMI                                 security model:v2c
readview : *ilmi                                writeview: *ilmi
notifyview: <no notifyview specified>
row status: active
groupname: zsprw                                security model:v1
readview : v1default                            writeview: v1default
notifyview: <no notifyview specified>
row status: active
groupname: zsprw                                security model:v2c
readview : v1default                            writeview: v1default
notifyview: <no notifyview specified>
row status: active
R1#
```

Rys. 57.2. **Wyświetlanie listy grup dostępu protokołu SNMP**

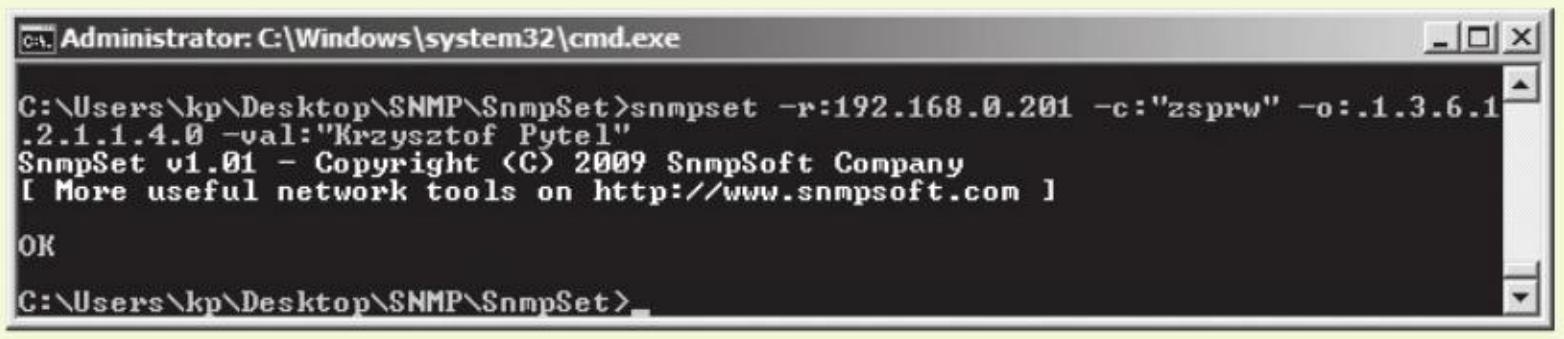
4. Wyświetlić pełne drzewo informacji z bazy MIB routera (każda linijka rozpoczyna się od identyfikatora OID obiektu). W tym celu w wierszu polecenia komputera należy wydać polecenie:
   `SnmpWalk -r:192.168.0.201 -c:"zsprw" |more`
   Uruchomi ono program narzędziowy SnmpWalk.exe (musi on się znajdować w aktualnym katalogu). Program skorzysta z grupy **`zsprw`** i pobierze z urządzenia o adresie **`192.168.0.201`** całą bazę MIB. Ponieważ baza jest bardzo duża, za pomocą **`|more`** zostanie wykonane stronicowanie wyników. Pomoc do programu można uzyskać po wydaniu polecenia:
   `SnmpWalk /?`
   Na rys. 57.3 przedstawiono fragment wyniku działania polecenia.



Rys. 57.3. **Wyświetlanie pełnej bazy MIB agenta**

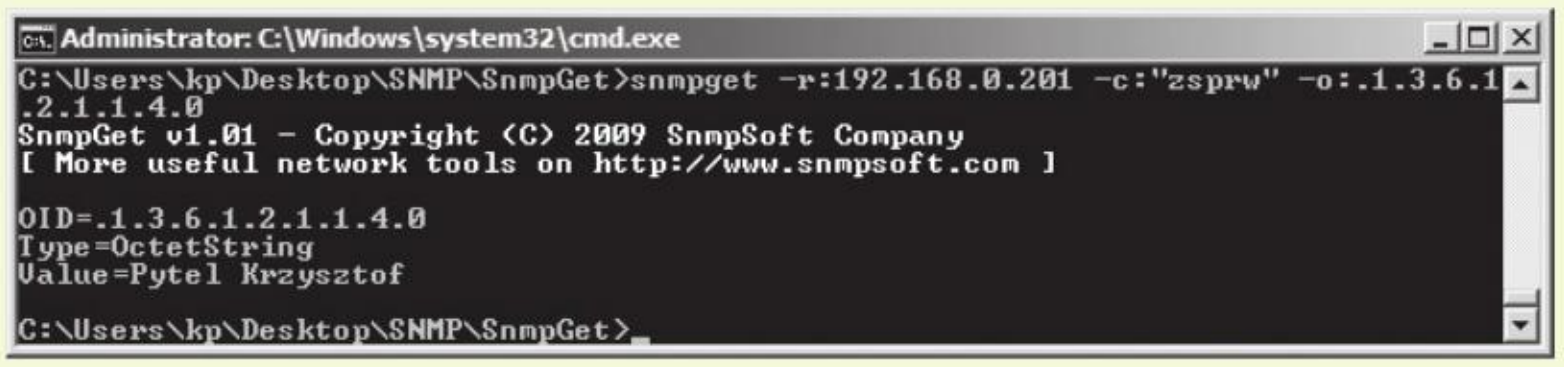
5. Przykładowo: informacja **`OID=.1.3.6.1.2.1.1.4.0`** określa osobę odpowiedzialną za zarządzanie urządzeniem, a **`OID=.1.3.6.1.2.1.1.5.0`** – nazwę urządzenia.

Za pomocą polecenia: **`SnmpSet -r: 192.168.0.201 -c:"zsprw" -o:.1.3.6.1.2.1.1.4.0 -val:"Krzysztof Pytel"`** można zmienić nazwisko osoby odpowiedzialnej za router na własne (rys. 57.4).



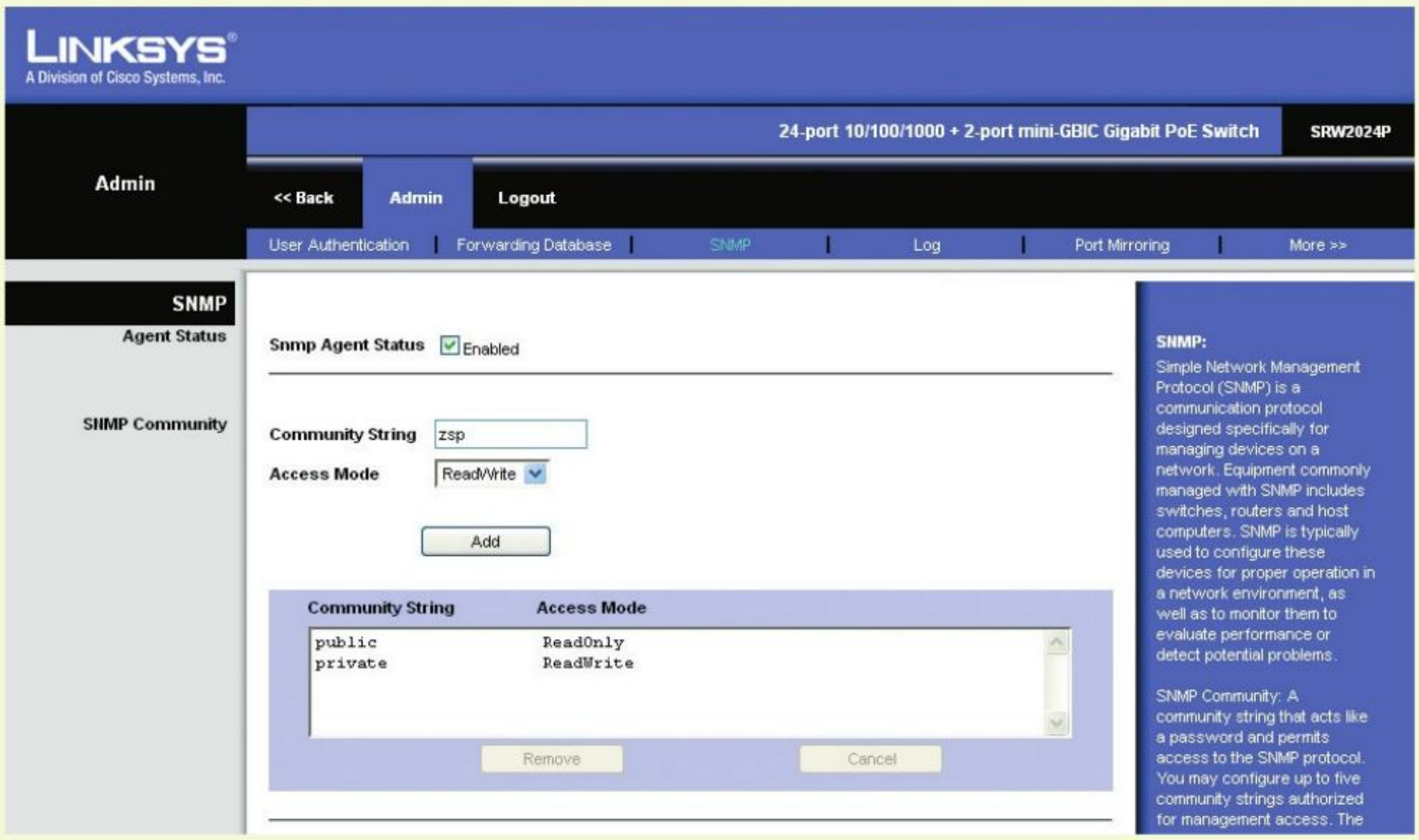
Rys. 57.4. **Modyfikowanie informacji w bazie MIB**

6. Wyświetlenie wartości pojedynczej informacji z bazy MIB można wykonać po wydaniu polecenia:
`SnmpGet -r:192.168.0.201 -c:"zsprw" -o:.1.3.6.1.2.1.1.4.0`
Jak widać na rys. 57.5, nazwisko operatora zostało zmienione na „Pytel Krzysztof".



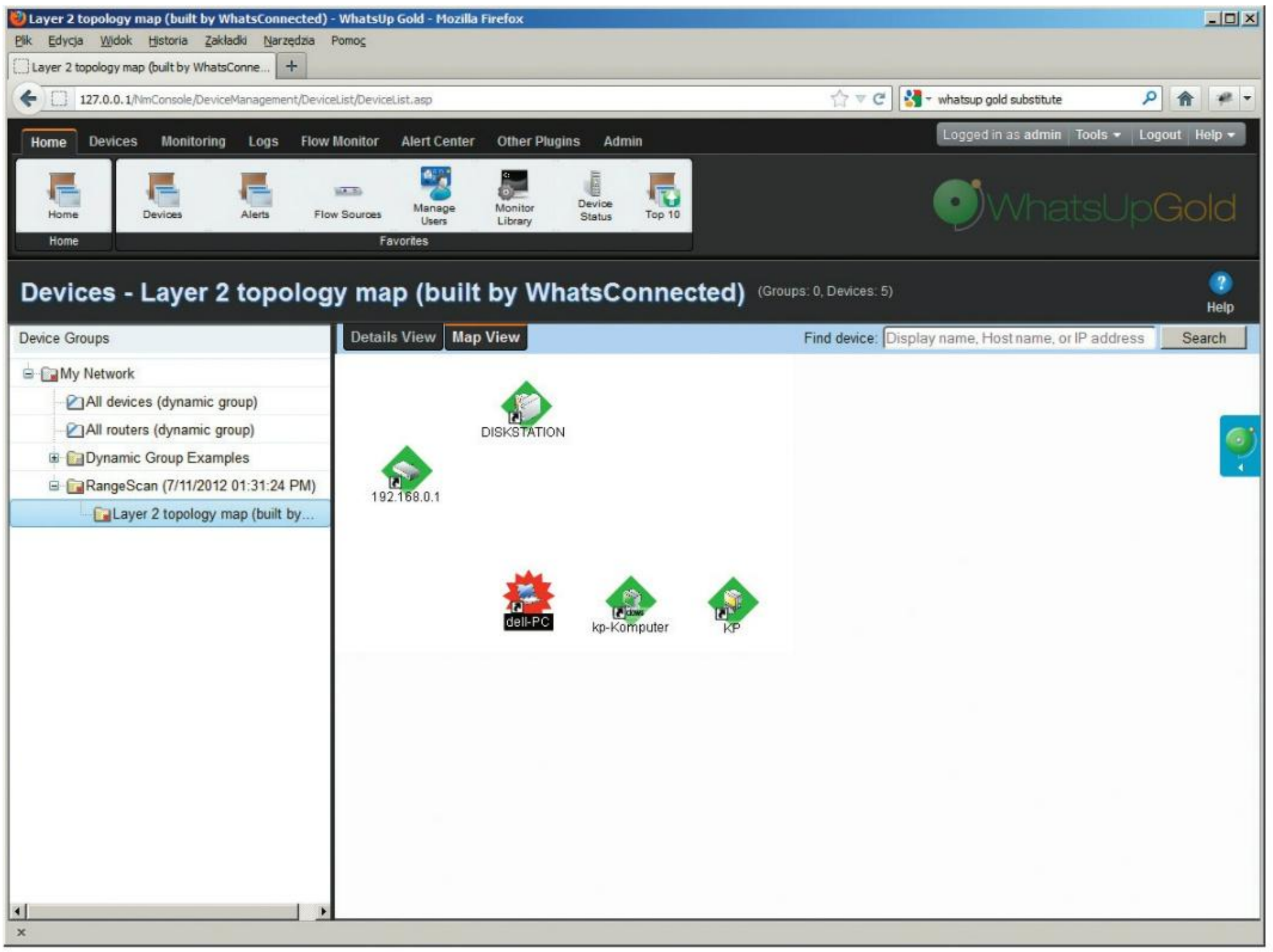
Rys. 57.5. **Wyświetlanie pojedynczej informacji z bazy MIB**

Na rys. 57.6 przedstawiono fragment okna konfiguracji agenta SNMP w przełączniku firmy Linksys. Konfiguracja jest wykonywana w zakładce **`Admin`** na podstronie **`SNMP`**.



Rys. 57.6. **Fragment okna konfiguracji agenta SNMP w przełączniku firmy Linksys**

Do administrowania sieciami komputerowymi można wykorzystać również aplikacje pracujące w środowisku graficznym. Wielu producentów sprzętu sieciowego oferuje własne bardzo zaawansowane rozwiązania, lecz zwykle są to programy komercyjne. Przykładem programu do administrowania sieciami komputerowymi pracującym w środowisku Windows jest **WhatsUpGold**. Jest on dostępny w wersji testowej, lecz wymaga rejestracji. Na rys. 57.7 przedstawiono przykładową sieć, w której jeden z komputerów utracił łączność z siecią.



Rys. 57.7. Graficzna aplikacja do administrowania siecią

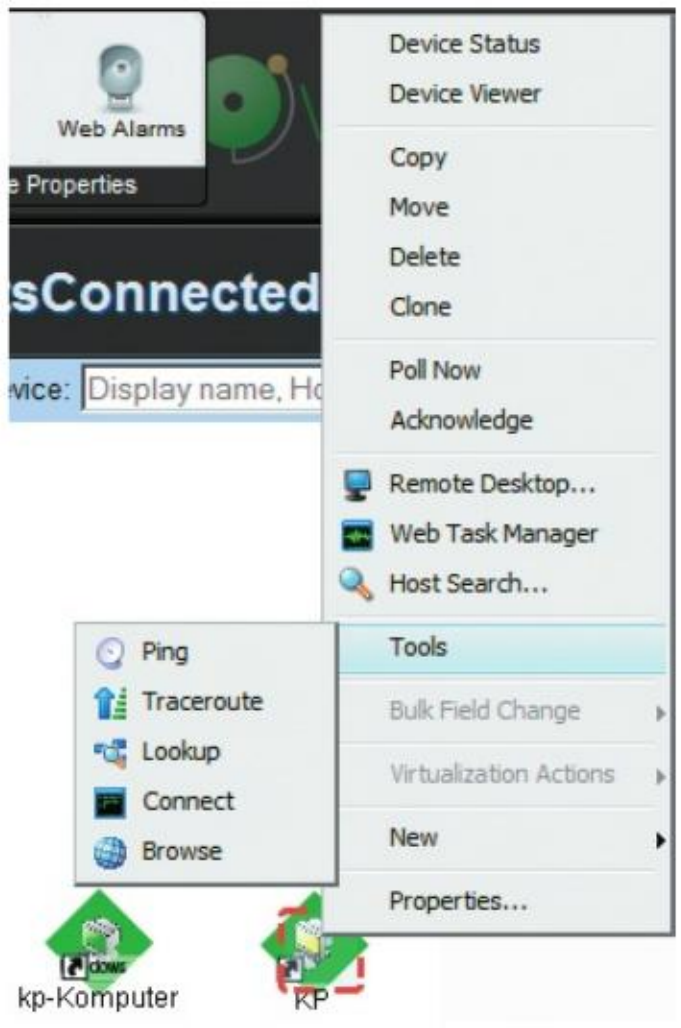
Administrator korzystający z takiego programu otrzymuje informacje w postaci graficznej, dysponuje zaawansowanymi programami diagnostycznymi, raportami i statystykami, które ułatwiają i usprawniają proces administrowania siecią. Aby uruchomić narzędzia, wystarczy kliknąć prawym przyciskiem myszy ikonę komputera, a następnie z menu kontekstowego wybrać polecenie **`Tools`** i odpowiednie narzędzie (rys. 57.8).

Innym bardzo rozbudowanym systemem ułatwiającym administrowanie siecią jest **nVision** firmy Axence. Program składa się z modułów, z których tylko **Network** jest bezpłatny:

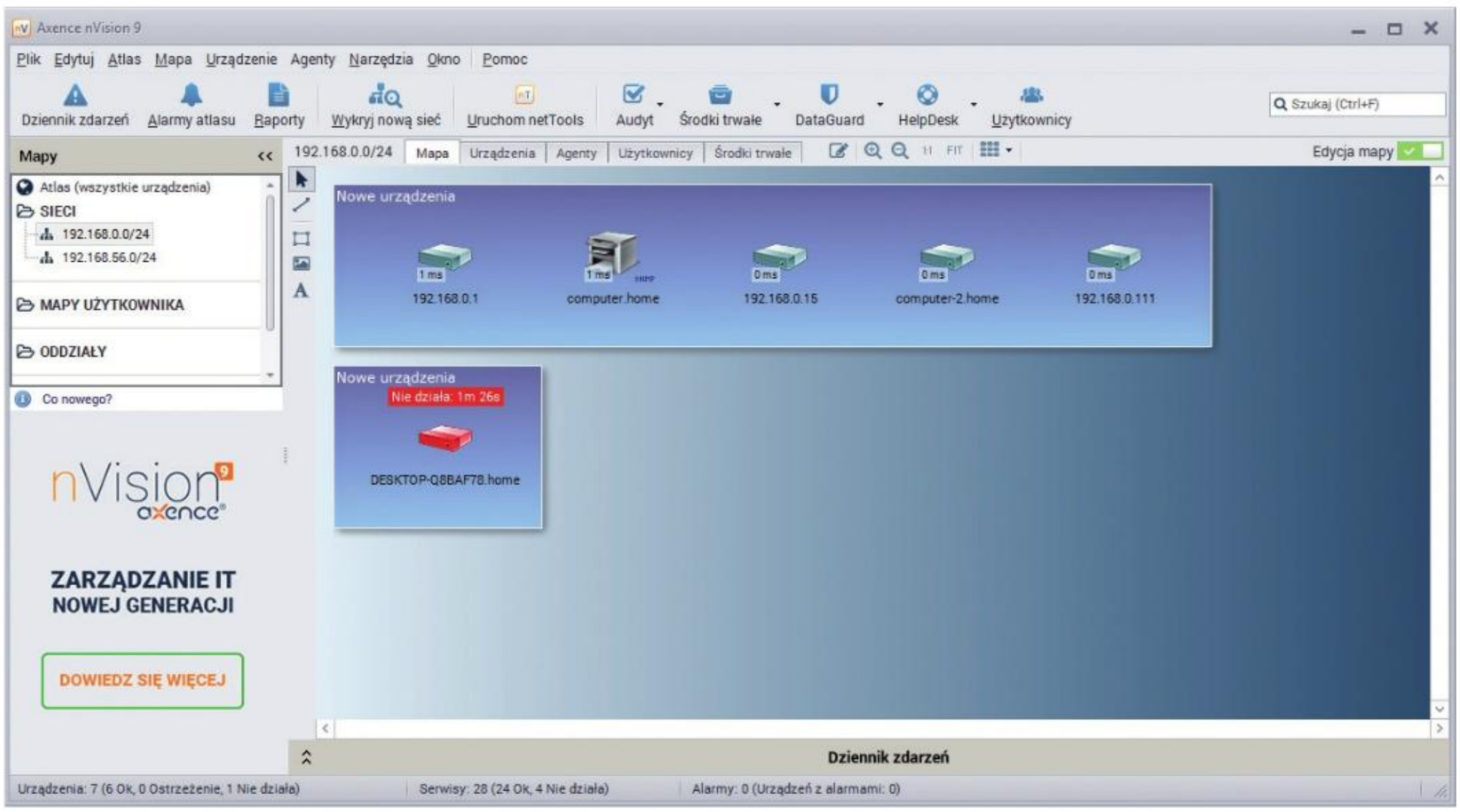
- **Network** – moduł umożliwiający monitorowanie sieci, np. wykrywanie urządzeń, tworzenie map urządzeń;
- **Inventory** – moduł inwentaryzacji i zarządzania zasobami IT, np. oprogramowaniem i sprzętem, przeprowadzanie audytu;
- **Users** – monitorowanie i ochrona pracowników, np. przed atakami sieciowymi, szkodliwymi treściami w sieci;

- **Helpdesk** – moduł świadczenia pomocy użytkownikom i tworzenia dokumentacji tej pomocy;
- **Dataguard** – monitorowanie urządzeń przenośnych podłączanych do sieci.

System składa się z konsoli centralnej i agentów instalowanych na monitorowanych urządzeniach. Okno główne konsoli zarządzania przedstawiono na rys. 57.9.



Rys. 57.8. Uruchamianie narzędzi w programie WhatsUpGold



Rys. 57.9. Okno główne konsoli zarządzania nVision

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyszukaj w dokumentacji dowolnego urządzenia w szkole, obsługującego protokół SNMP (np. drukarki, przełącznika, routera), informacje dotyczące obsługiwanej bazy MIB. Za pomocą protokołu SNMP zmień nazwę urządzenia lub dowolny inny parametr (przed zmianą zapisz poprzednie ustawienia, aby je przywrócić po wykonaniu ćwiczenia).

58 Zdalne zarządzanie stacjami roboczymi

ZAGADNIENIA

Co to jest zdalne zarządzanie stacjami roboczymi **Programy i systemy do zdalnego zarządzania stacjami roboczymi** **Zalety i wady zdalnego zarządzania stacjami roboczymi**

Zadaniami administratora w przedsiębiorstwie są m.in. instalowanie poprawek i aktualizacji systemów, dystrybucja oprogramowania, zarządzanie zasobami IT, zarządzanie licencjami oprogramowania, monitorowanie wykorzystania oprogramowania, zarządzanie korzystaniem z urządzeń USB. W niewielkich środowiskach IT wykonywanie tych zadań nie jest specjalnie kłopotliwe. Instalację aktualizacji i aplikacji bądź inwentaryzację można wykonać bezpośrednio przy każdym urządzeniu klienckim. W dużych organizacjach dysponowanie odpowiednimi narzędziami do przejmowania kontroli nad pulpitami i do zdalnego zarządzania stacjami roboczymi pozwala zautomatyzować typowe czynności obsługi komputerów i znacznie ułatwia wykonywanie tych zadań. Umożliwia również udzielanie wsparcia użytkownikom przez usługi typu czat, przesyłanie plików lub zdalne uruchamianie prezentacji.

Istnieje wiele systemów zarządzania stacjami roboczymi, np. system nVision, wspomniany w poprzednim rozdziale. W większości są to jednak systemy komercyjne. Zapewniają one funkcjonalności, takie jak:

- dystrybucja oprogramowania – uproszczenie dystrybucji oprogramowania przez zdalne instalowanie i odinstalowywanie oprogramowania;
- zarządzanie poprawkami – automatyczna dystrybucja poprawek systemów operacyjnych i aplikacji firm trzecich;
- zarządzanie urządzeniami mobilnymi – umożliwienie konfigurowania, zarządzania i zabezpieczania urządzeń mobilnych z centralnej lokalizacji;
- zarządzanie zasobami – zliczanie oprogramowania, zarządzanie licencjami oprogramowania, zakazanym oprogramowaniem itp.;
- zdalna kontrola – zdalne rozwiązywanie problemów dotyczące stanowisk roboczych za pomocą połączeń zdalnych i współpracy z użytkownikami, przesyłania plików, nagrywania wideo itp.;
- kontrola zużycia energii – zarządzanie energią przez stosowanie schematów zasilania, wyłączanie nieużywanych komputerów i sporządzanie raportów dotyczących czasu pracy systemów;
- zarządzanie urządzeniami USB – ograniczanie i kontrola korzystania z urządzeń USB w sieci zarówno na poziomie użytkowników, jak i na poziomie komputerów.

Podstawowe korzyści wynikające ze stosowania tych systemów to:

- zwiększenie produktywności administratorów sieci i zmniejszenie ich obciążenia;
- zmniejszenie wydatków na utrzymanie i wsparcie użytkowników, związane z ręcznym zarządzaniem stacjami roboczymi;
- poprawa bezpieczeństwa;
- automatyzacja procesów konfiguracji i dystrybucji oprogramowania zarówno dla komputerów, jak i dla urządzeń mobilnych;
- zmniejszenie liczby zgłoszeń do działu help desk i skrócenie czasu usunięcia usterki.

Podstawowe wady zdalnego zarządzania to zmniejszenie poziomu bezpieczeństwa systemu i narażenie systemu na zdalne ataki innych użytkowników sieci.

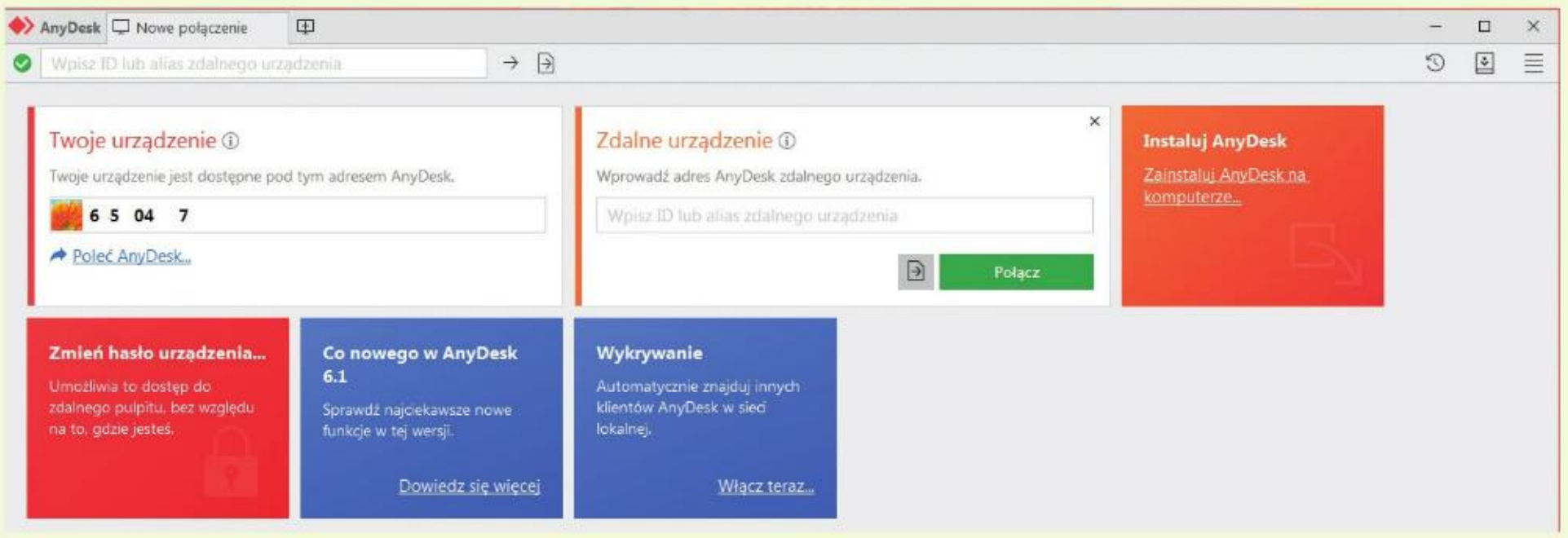
Wiele narzędzi do zdalnego zarządzania stacjami roboczymi standardowo jest dostępnych w sieciowych systemach operacyjnych, np. Windows Server (niektóre z nich omówiono w części dotyczącej administrowania systemem Windows Server). Istnieje również wiele programów i systemów dostępnych bezpłatnie. Jednym z nich jest **AnyDesk**, umożliwiający zdalne przejęcie kontroli i udzielanie zdalnego wsparcia użytkownikom systemów Windows, Linux, iOS i Android. Użytkownik za pomocą programu może m.in.: przenosić dane, prowadzić czaty, wirtualne szkolenia. Aplikacja jest dostępna bezpłatnie dla użytkowników indywidualnych, niekomercyjnych. Użytkownicy komercyjni muszą wykupić licencję, aby legalnie korzystać z programu.

PRZYKŁAD 58.1

Instalacja i konfiguracja aplikacji AnyDesk

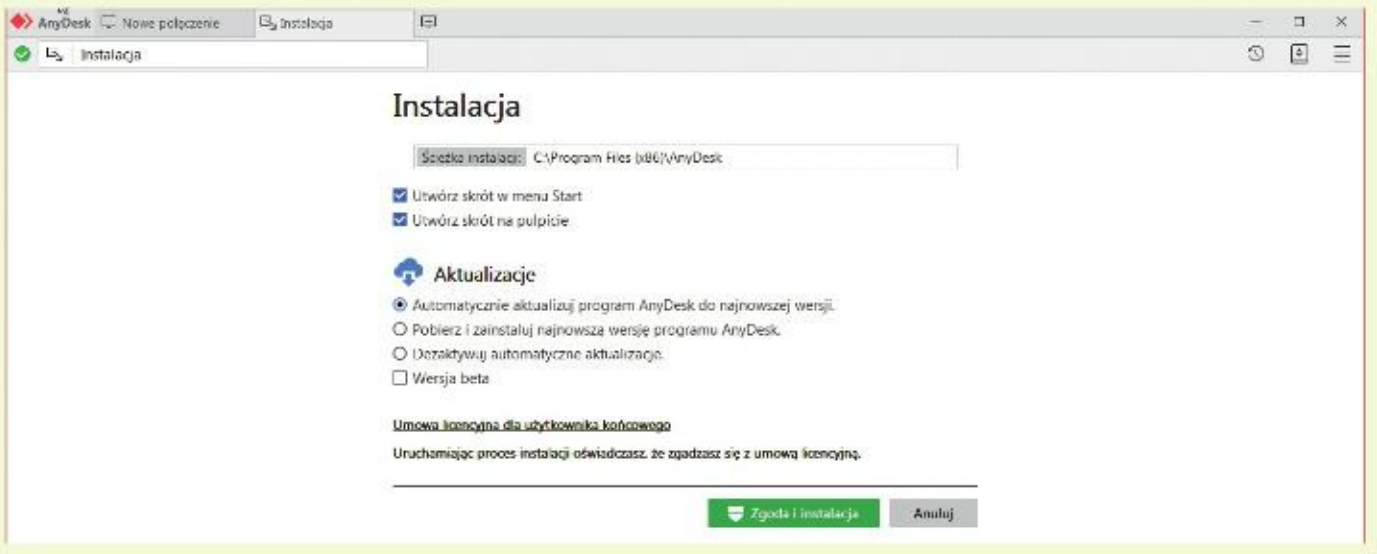
W ćwiczeniu zostanie zademonstrowana procedura instalacji i konfiguracji aplikacji AnyDesk. Aby zainstalować i skonfigurować AnyDesk, należy:

1. Pobrać plik **`AnyDesk.exe`** ze strony https://anydesk.com/pl.
2. Uruchomić plik i postępować zgodnie ze wskazówkami kreatora instalacji. W oknie kreatora (rys. 58.1) wybrać opcje konfiguracji. Aplikację można tylko uruchomić lub zainstalować (umożliwi to zarządzanie zdalnymi systemami). Zaznaczyć opcję **`Zainstaluj AnyDesk na komputerze`**. Umożliwi to zarządzanie zdalnymi komputerami, jak również udostępni innym możliwość zarządzania tym komputerem.



Rys. 58.1. **Okno wyboru instalacji AnyDesk**

3. Następnie wybrać miejsce instalacji (rys. 58.2).



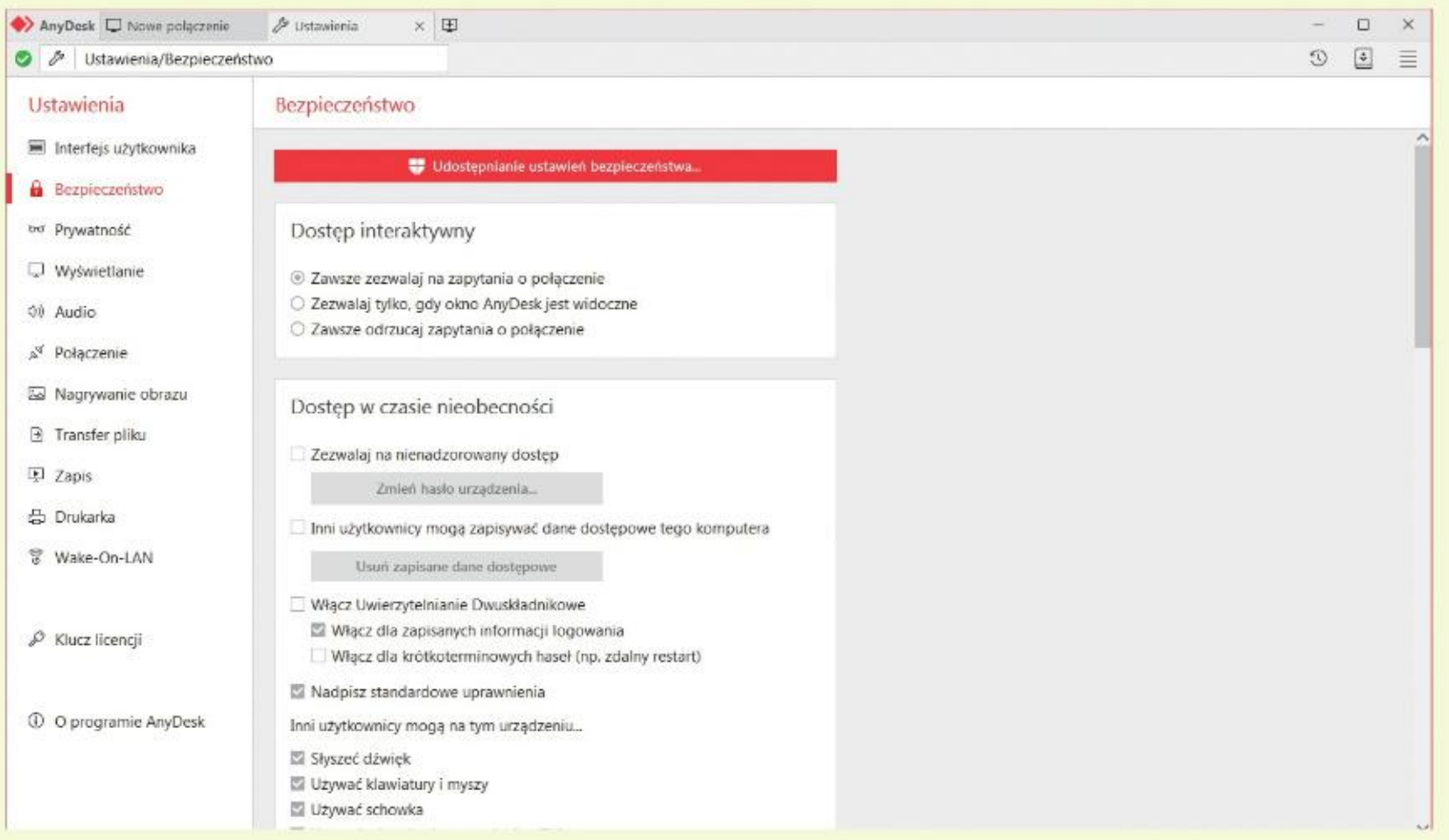
Rys. 58.2. **Okno wyboru miejsca instalacji AnyDesk**

4. Po zapoznaniu się z warunkami umowy kliknąć przycisk **`Zgoda i Instalacja`**. Na rys. 58.3 przedstawiono okno programu po instalacji.



Rys. 58.3. **Okno programu AnyDesk po instalacji**

5. Użytkownik może dostosować ustawienia programu, jeżeli wybierze w prawym górnym rogu opcję **`Ustawienia`** (rys. 58.4).



Rys. 58.4. **Okno ustawień i dostosowań AnyDesk**

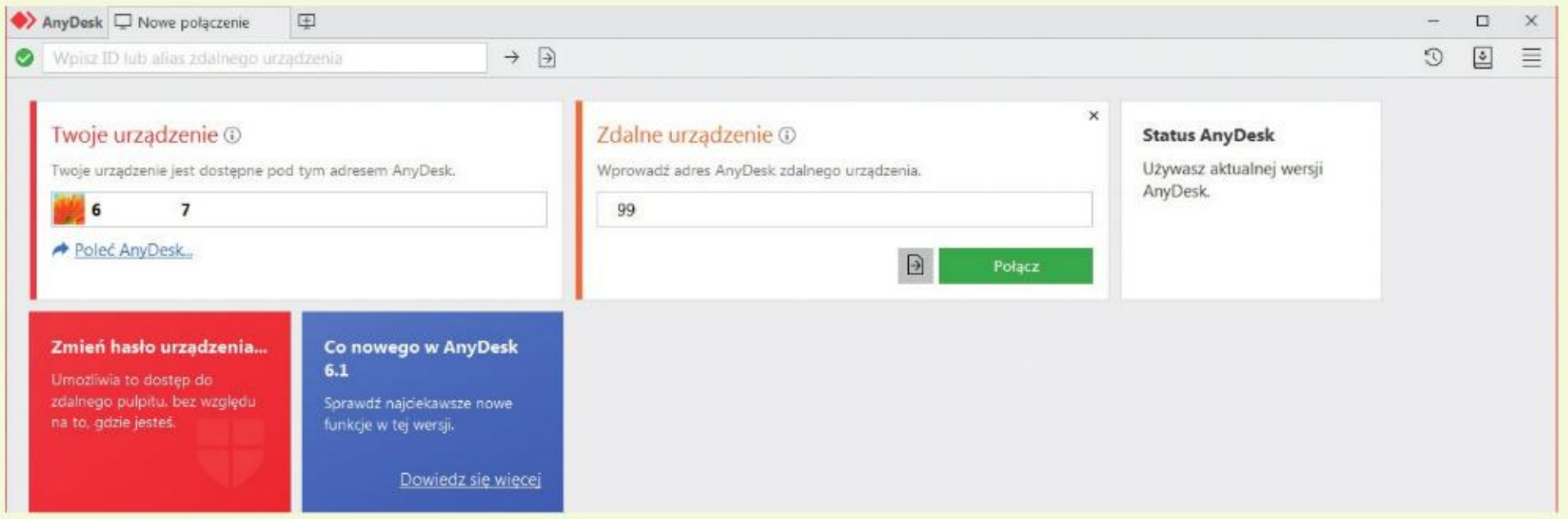
Po instalacji aplikacji i skonfigurowaniu dostępu możliwe staje się nawiązywanie połączenia ze zdalnymi systemami.

PRZYKŁAD 58.2

Nawiązywanie komunikacji ze zdalnym systemem za pomocą aplikacji AnyDesk

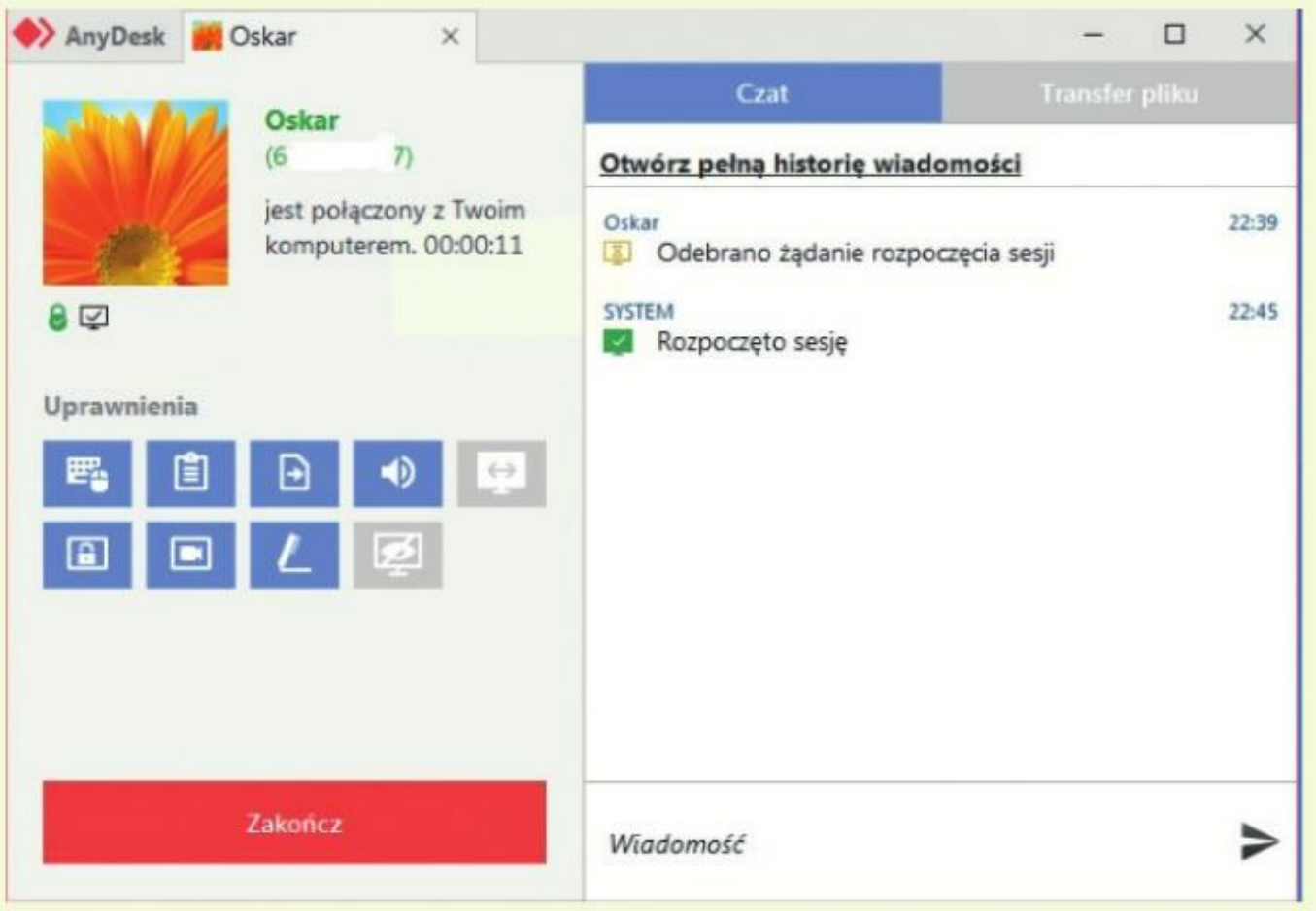
Aby nawiązać połączenie ze zdalnym systemem, należy:

1. Uruchomić aplikację AnyDesk.
2. Aby połączyć się z drugim komputerem, AnyDesk musi być na nim uruchomiony. Należy wpisać ID drugiego komputera. Znajduje się on na głównym ekranie aplikacji w oknie **`Twoje urządzenie`**.
3. Wpisać adres drugiego urządzenia (rys. 58.5) w polu **`Zdalne urządzenie`** i kliknąć **`Połącz`**. Zaczekać na zaakceptowanie połączenia przez właściciela drugiego urządzenia (opcja **`Zezwalaj na nienadzorowany dostęp`** w ustawieniach pozwala ominąć konieczność oczekiwania na akceptację połączenia).

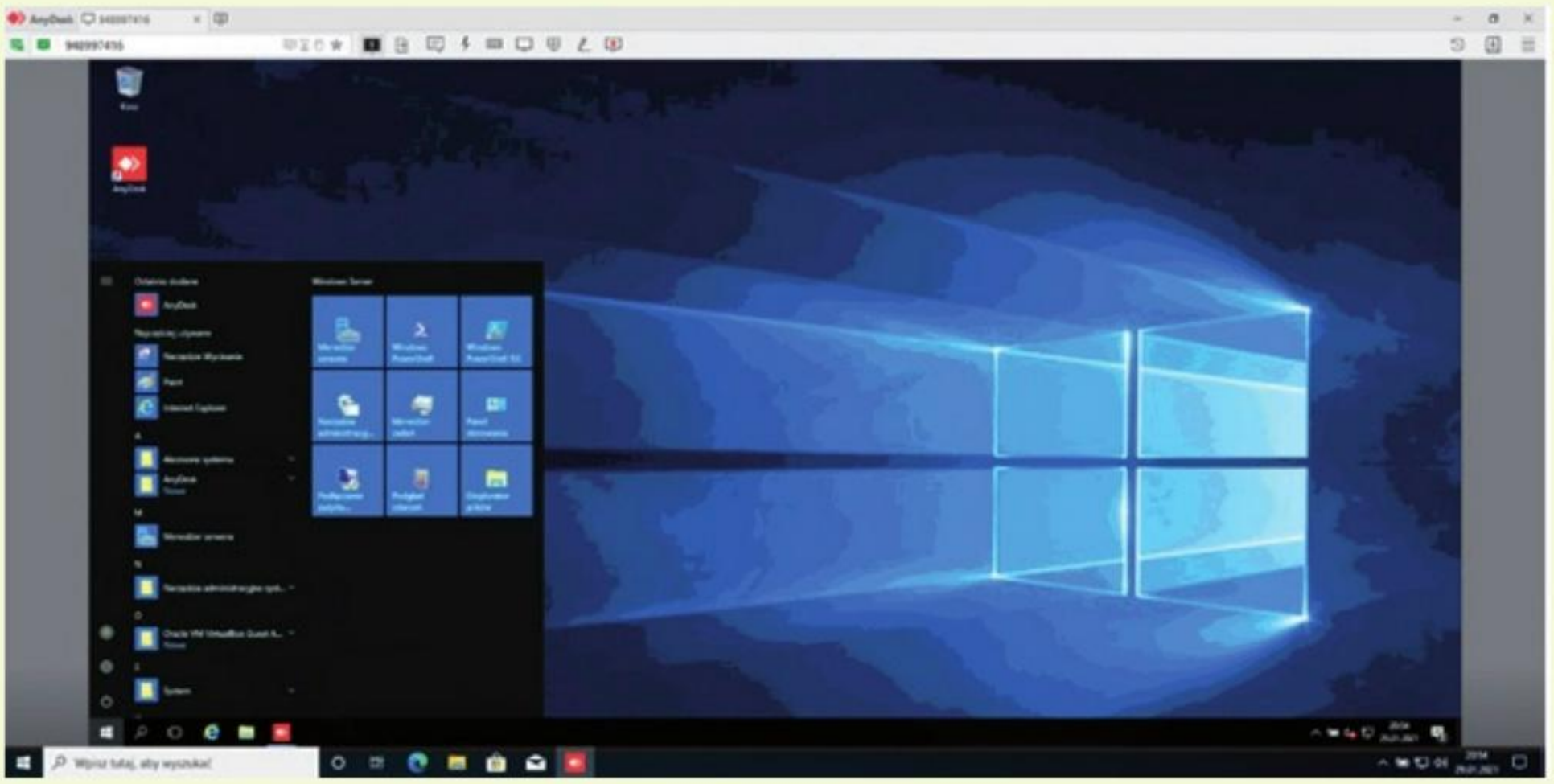


Rys. 58.5. **Okno nawiązywania połączenia**

4. Po zaakceptowaniu połączenia pojawi się okno aplikacji z widokiem na zdalny pulpit AnyDesk drugiego urządzenia (rys. 58.7). Na pasku widocznym u góry okna połączenia znajdują się narzędzia, takie jak: czat, przesyłanie plików, ustawienia połączenia (rys. 58.6).

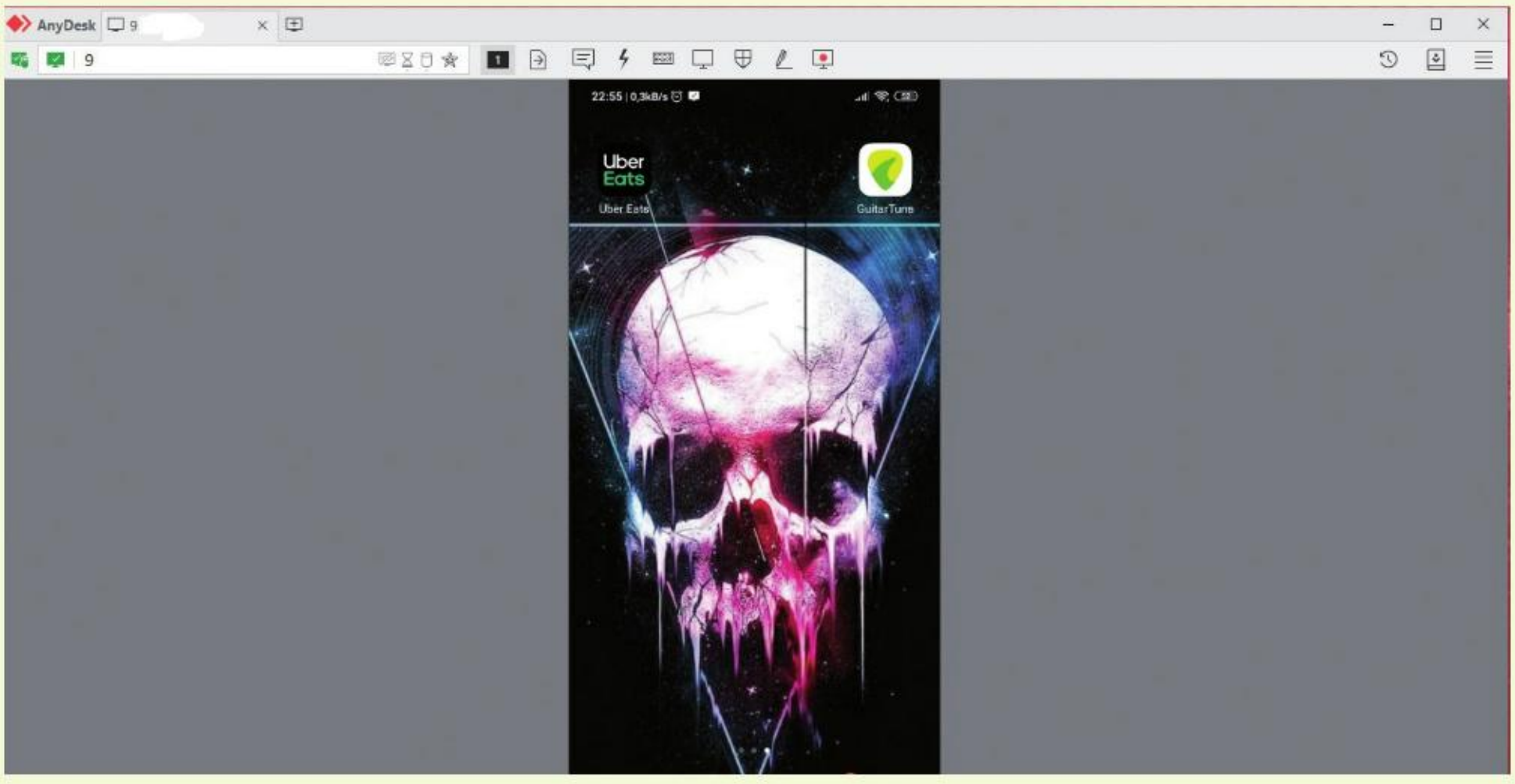


Rys. 58.6. **Okno nawiązanego połączenia**



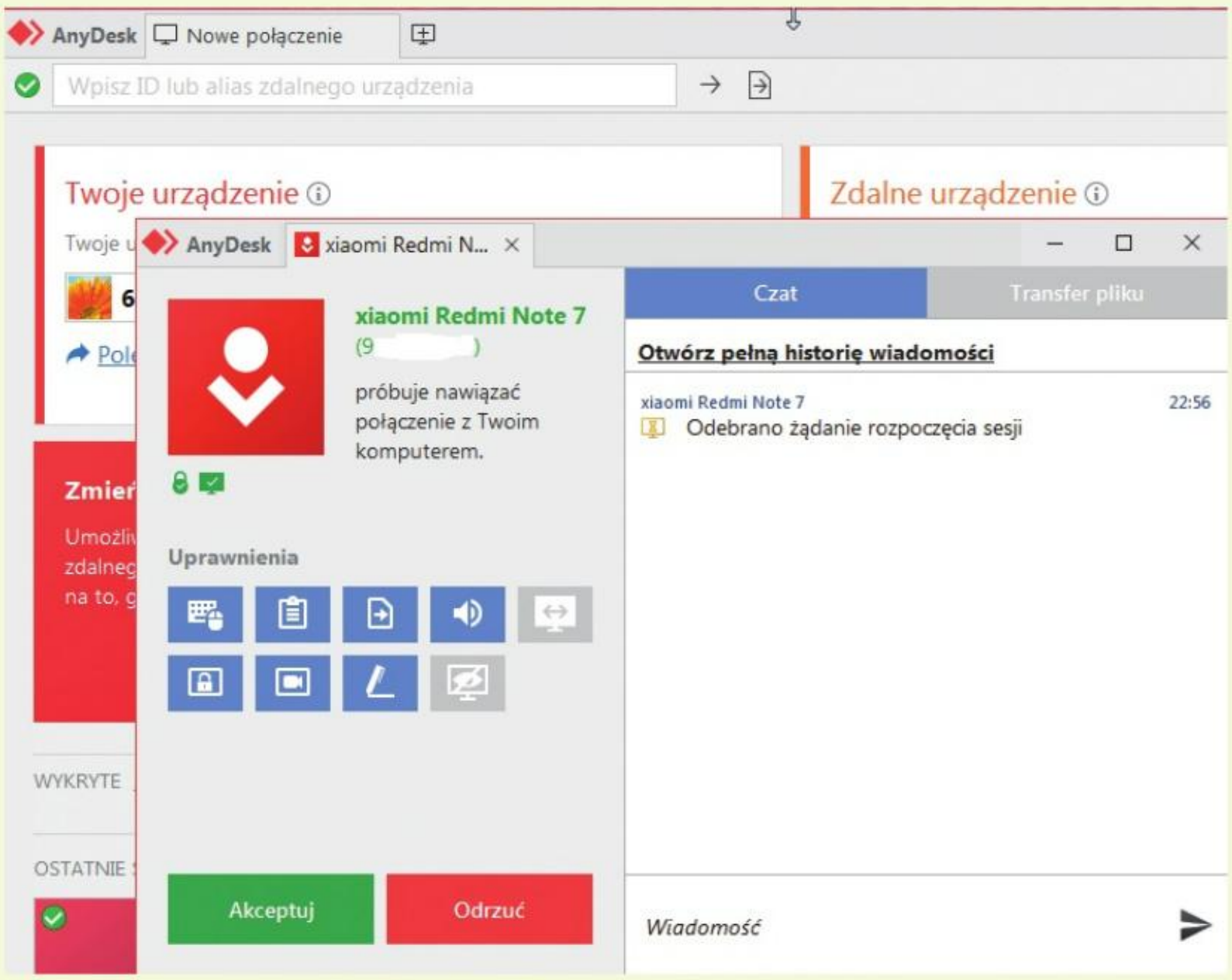
Rys. 58.7. **Okno zdalnego logowania do systemu Windows Serwer**

5. Z wykorzystaniem AnyDesk można również wykonywać połączenia i łączyć się z urządzeniami mobilnymi (rys. 58.8). Proces łączenia się na urządzeniu mobilnym jest identyczny do tego na komputerze. Aby rozpocząć sesję, w polu **`Adres urządzenia zdalnego`**, z którym chcemy się połączyć, wprowadza się adres tego urządzenia.



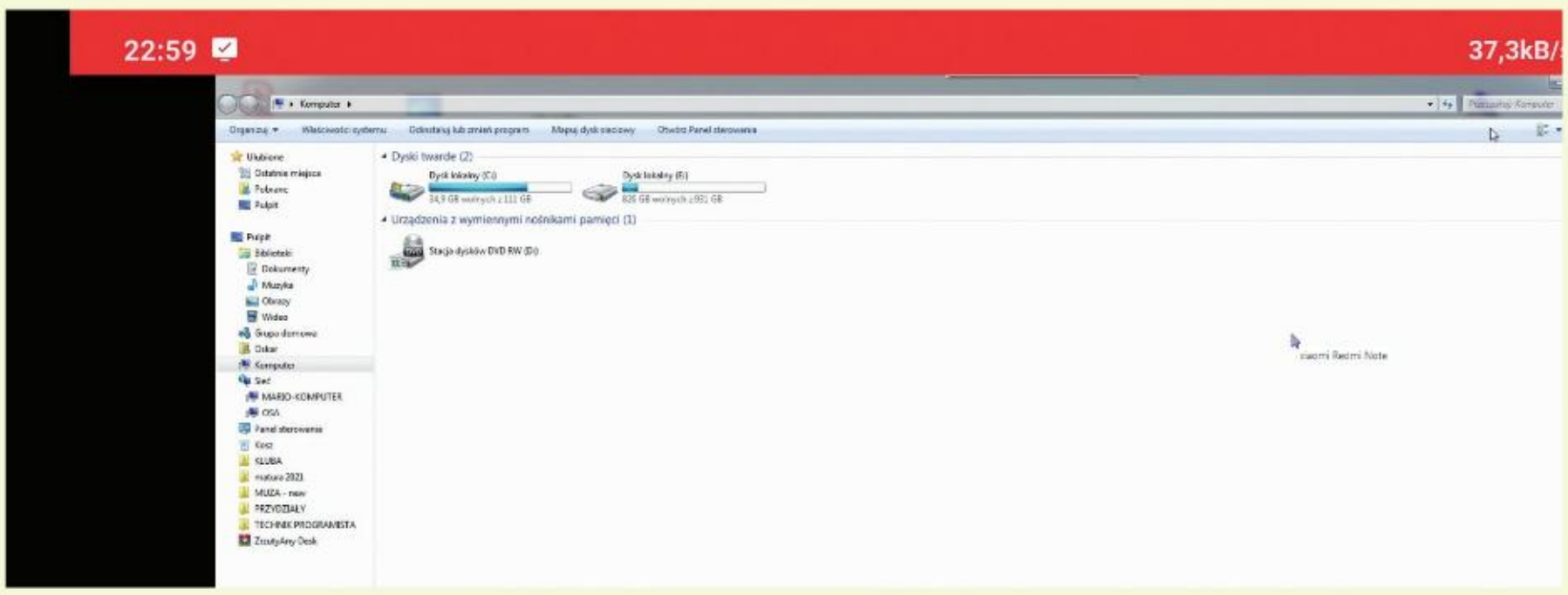
Rys. 58.8. **Okno zdalnego logowania do urządzenia mobilnego**

Możliwa jest również operacja odwrotna. Dzięki AnyDesk można także wykonywać połączenia i łączyć się z urządzenia mobilnego z komputerem (rys. 58.9).



Rys. 58.9. **Okno zdalnego logowania z urządzenia mobilnego na komputer**

6. Proces łączenia się jest identyczny do tego na komputerze. Wprowadza się adres komputera, z którym chcemy się połączyć w polu **`Adresu zdalnego`**, by rozpocząć sesję (rys. 58.10).



Rys. 58.10. **Okno zdalnego zarządzania z urządzenia mobilnego**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj dostęp zdalny do komputera z systemami Windows i Linux.
2. Nawiąż połączenie ze zdalnymi systemami Windows i Linux.
3. Nawiąż połączenie za pomocą urządzenia mobilnego z systemem Windows.

59 Zasady aktualizowania oprogramowania urządzeń sieciowych

ZAGADNIENIA

Protokół wykorzystywany do sporządzania kopii zapasowych plików konfiguracyjnych i systemów operacyjnych urządzeń sieciowych **Uruchomienie i skonfigurowanie serwera TFTP** **Kopia zapasowa pliku konfiguracyjnego i systemu operacyjnego** **Odtworzenie danych z kopii zapasowej pliku konfiguracyjnego i systemu operacyjnego**

Urządzenia sieciowe, takie jak zarządzalne przełączniki i routery, można traktować jako wyspecjalizowane komputery wyposażone w systemy operacyjne i pliki konfiguracyjne. Pliki obrazu systemu są przechowywane w pamięci **flash** urządzenia, natomiast pliki konfiguracyjne – w pamięci nieulotnej **NVRAM**. Dla celów bezpieczeństwa należy wykonać kopię zapasową systemu operacyjnego urządzenia i plików konfiguracyjnych – w razie uszkodzenia pamięci będzie można odtworzyć system i konfigurację urządzenia.

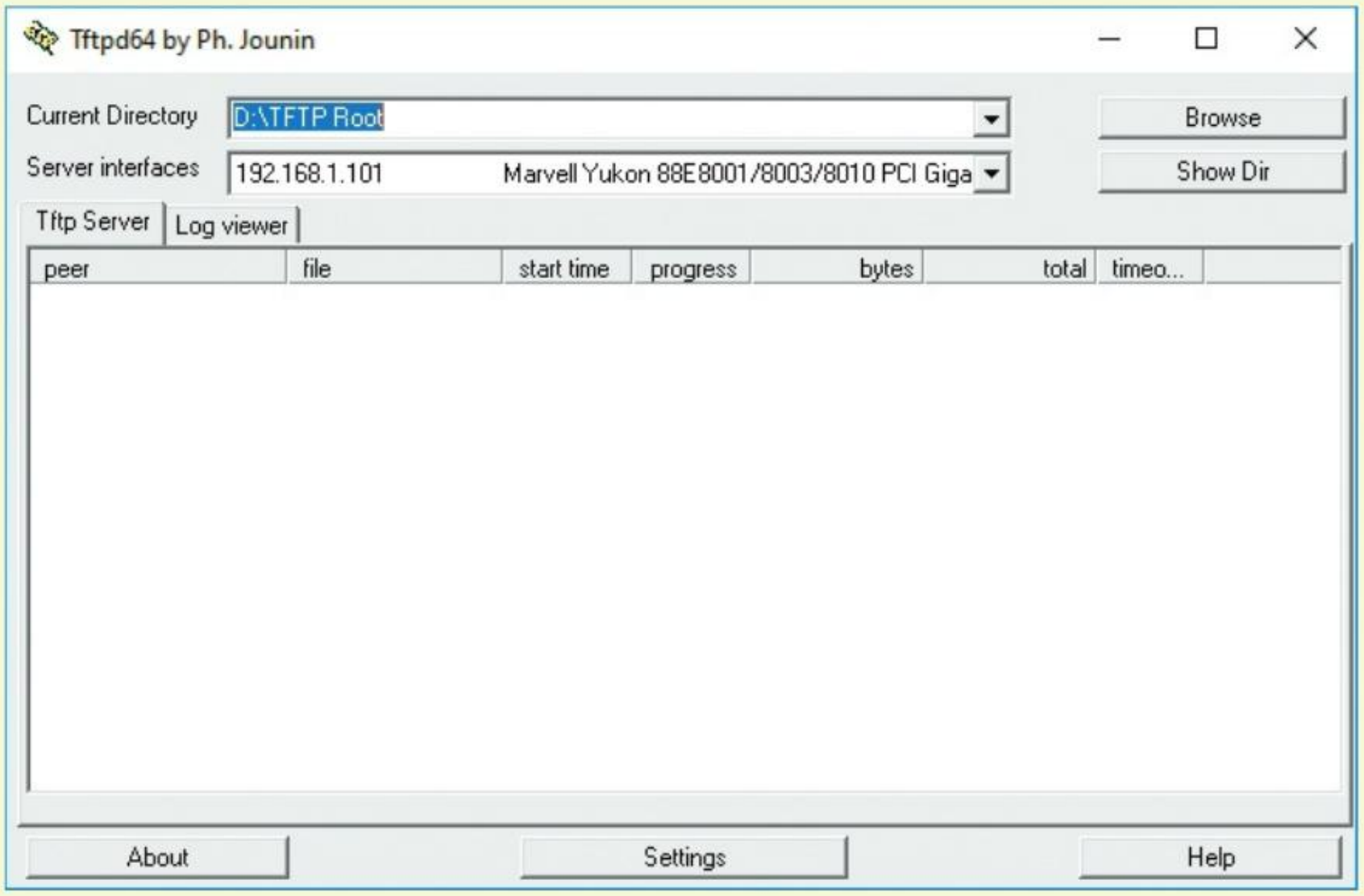
Do kopiowania plików między urządzeniem a komputerem służy protokół **TFTP**. Jest to prosty protokół wykorzystywany do przesyłania plików. Korzysta z 69. portu protokołu UDP, a jego jedynym zadaniem jest odczytywanie plików z komputera zdalnego i transmitowanie do niego plików. Działa w architekturze klient–serwer.

PRZYKŁAD 59.1

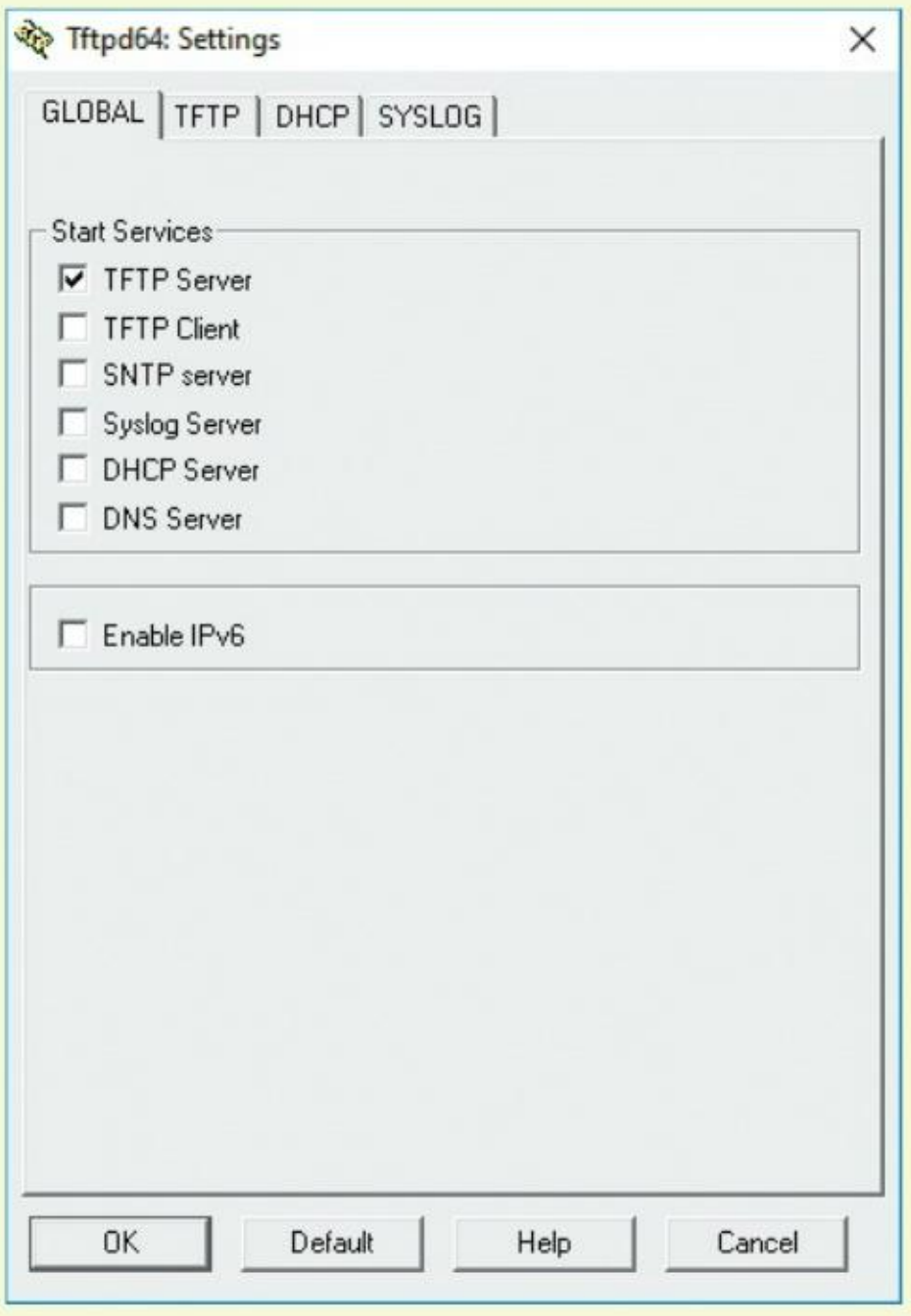
Instalowanie i konfiguracja serwera TFTP

W tym ćwiczeniu zostanie zainstalowany przykładowy serwer TFTP. Do wykonania ćwiczenia będzie potrzebny dowolny serwer TFTP, np. **`TFTPd64`** dostępny w wersji bezpłatnej do pobrania na stronie http://tftpd32.jounin.net/tftpd32_download.html. Aby go zainstalować, należy:

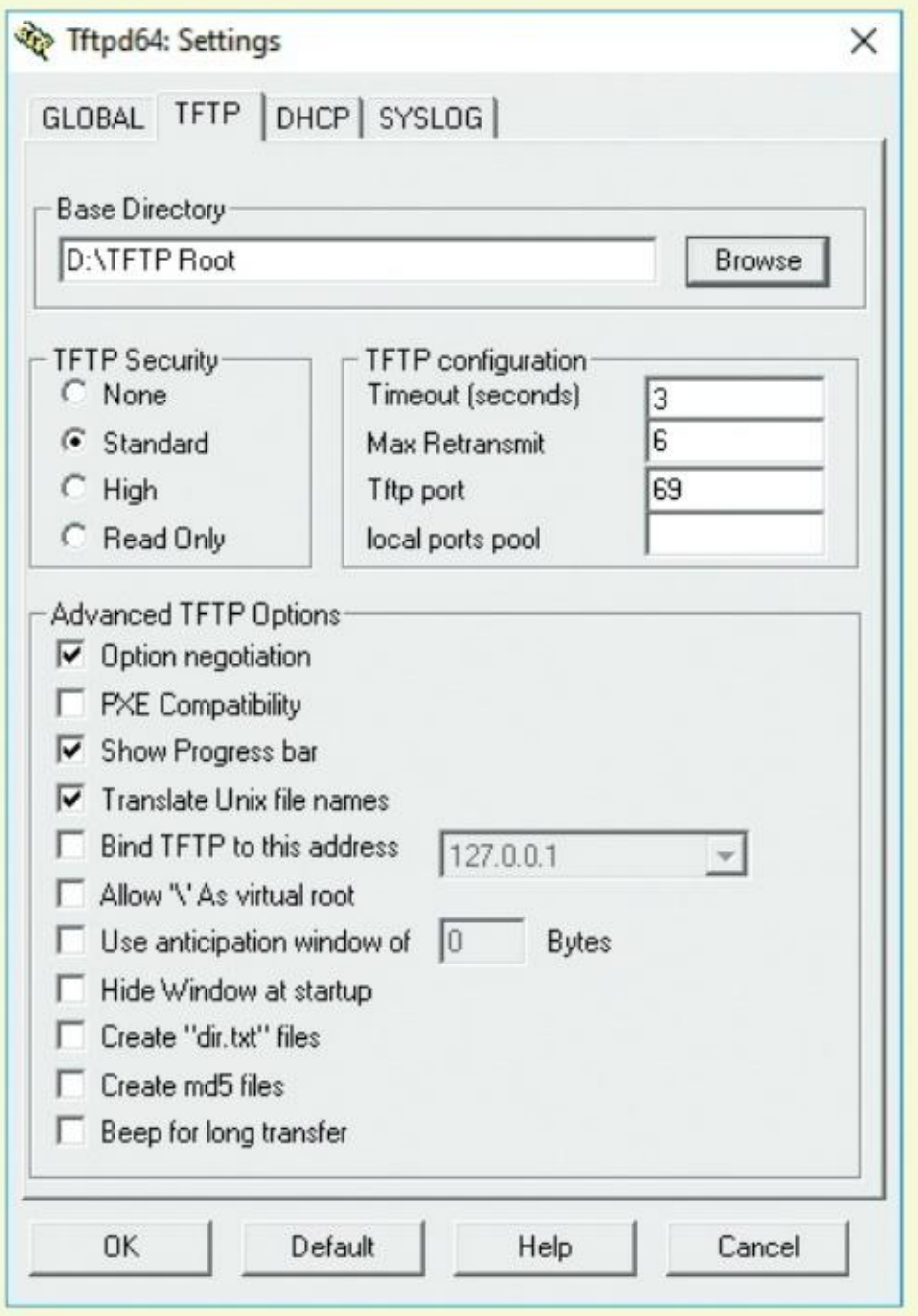
1. Odszukać w internecie i pobrać plik instalacyjny serwera TFTP, np.: **`Tftpd64-4.62-setup.exe`**
2. Zainstalować serwer – uruchomić plik **`Tftpd64-4.62-setup.exe`** i postępować zgodnie z poleceniami kreatora.
3. Po instalacji trzeba uruchomić program (rys. 59.1) i wybrać interfejs (ang. *Server interfaces*), na którym serwer będzie nasłuchiwał.
4. Kliknąć przycisk **`Settings`**.
5. W zakładce **`GLOBAL`** zaznaczyć usługi świadczone przez serwer – pozostawić tylko TFTP (rys. 59.2).
6. W zakładce **`TFTP`** (rys. 59.3) wskazać katalog główny usługi (do tego katalogu będą kopiowane pliki). W pozostałych opcjach pozostawić wartości domyślne.
7. Po wykonaniu tych czynności serwer jest uruchomiony i gotowy do pracy.



Rys. 59.1. **Okno główne serwera Tftpd64**



Rys. 59.2. **Wybór usług serwera Tftpd64**



Rys. 59.3. **Okno konfiguracji serwera Tftpd64**

PRZYKŁAD 59.2

Zapisywanie na serwerze kopii zapasowej pliku konfiguracyjnego

W tym ćwiczeniu za pomocą protokołu TFTP zostanie utworzona kopia zapasowa pliku konfiguracyjnego routera. W urządzeniach innych producentów procedura przebiega podobnie, chociaż mogą występować drobne różnice, np. w nazwach lub lokalizacji pliku. Plik konfiguracyjny routera CISCO nosi nazwę **`running-config`** i jest przechowywany w pamięci RAM. Aby zapisać na serwerze kopię pliku konfiguracyjnego routera, należy wykonać następujące czynności:

1. Połączyć komputer z routerem i nawiązać sesję.
2. W trybie użytkownika uprzywilejowanego wydać polecenie kopiowania pliku: **`copy running-config tftp:`**
3. Wprowadzić adres serwera TFTP (ang. *Address or name of remote host*).
4. Wprowadzić nazwę dla pliku na serwerze (ang. *Destination filename*) – domyślnie jest to **`nazwa_routera-confg`**. Przebieg kopiowania przedstawiono na rys. 59.4.

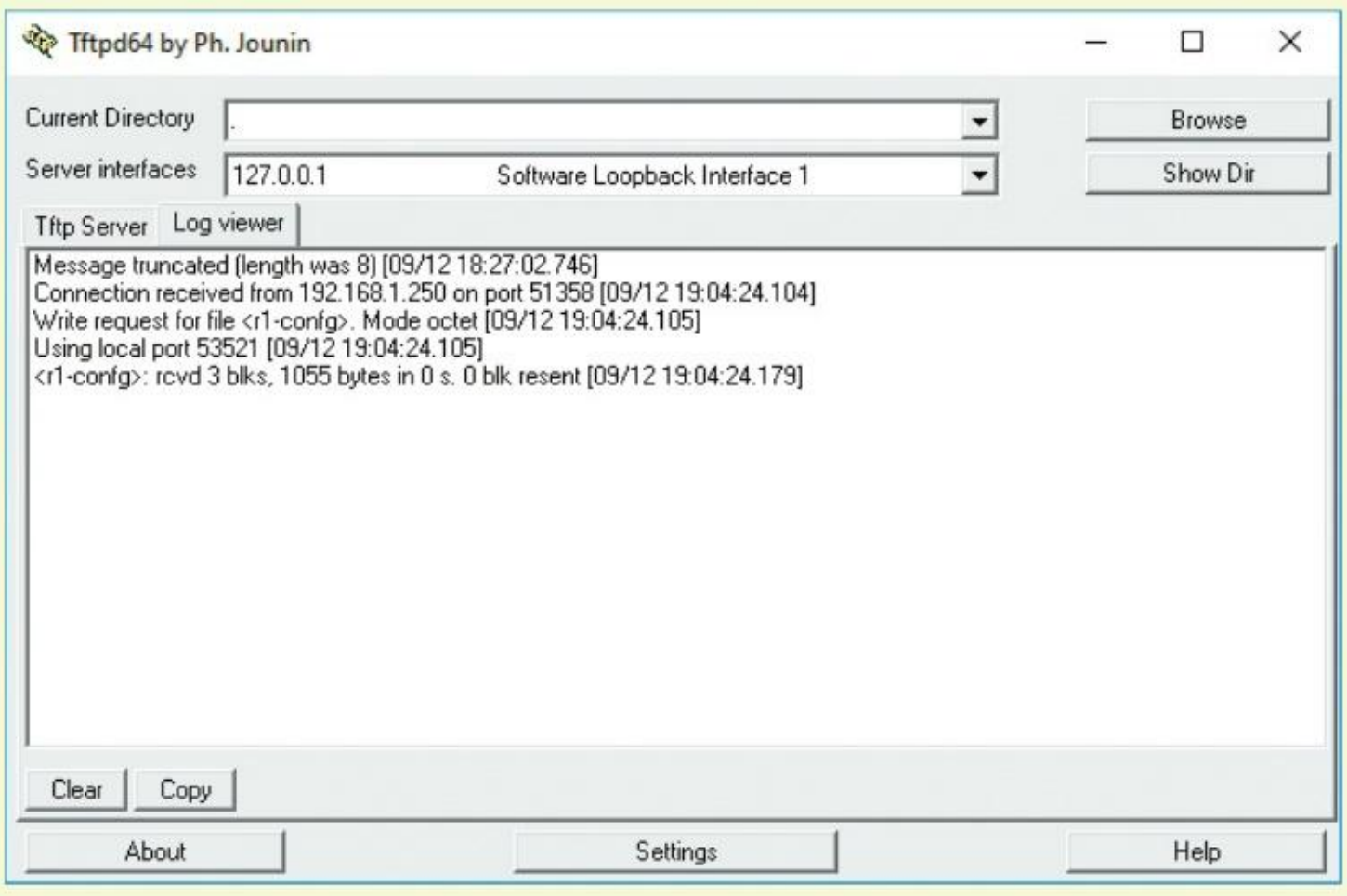
```
R1#copy running-config tftp:
Address or name of remote host []? 192.168.1.101
Destination filename [R1-confg]?

Writing running-config....!!
[OK - 564 bytes]

564 bytes copied in 3.014 secs (187 bytes/sec)
R1#
```

Rys. 59.4. **Procedura kopiowania pliku konfiguracyjnego na serwer TFTP**

5. Sprawdzić w komunikatach serwera TFTP, czy kopiowanie przebiegło bez błędów (rys. 59.5).



Rys. 59.5. **Komunikaty serwera TFTP dotyczące kopiowania pliku**

! UWAGA

W razie błędu z dostępem do serwera TFTP na niektórych routerach, np. Cisco 4321, należy określić interfejs źródłowy routera za pomocą polecenia:

```
ip tftp source-interface GigabitEthernet 0/0/0
```

PRZYKŁAD 59.3

Odtwarzanie na routerze kopii zapasowej pliku konfiguracyjnego

W tym ćwiczeniu za pomocą protokołu TFTP zostanie odtworzona kopia zapasowa pliku konfiguracyjnego routera CISCO. W urządzeniach innych producentów procedura przebiega podobnie, chociaż mogą występować drobne różnice, np. w nazwach lub lokalizacji plików. Plik konfiguracyjny routera CISCO nosi nazwę **`running-config`** i jest przechowywany w pamięci RAM.

Aby odtworzyć na routerze kopię pliku konfiguracyjnego, należy wykonać następujące czynności:

1. Połączyć komputer z routerem i nawiązać sesję.
2. W trybie użytkownika uprzywilejowanego wydać polecenie kopiowania pliku:
   `copy tftp: running-config`
3. Wprowadzić adres serwera TFTP.
4. Wprowadzić nazwę pliku na serwerze – plik musi zawierać poprawną konfigurację urządzenia.
5. Wprowadzić nazwę pliku na routerze. Przebieg kopiowania przedstawiono na rys. 59.6.
6. Po prawidłowym skopiowaniu pliku następuje automatyczne skonfigurowanie routera zgodnie z informacjami zapisanymi w kopiowanym pliku.

```
R1#copy tftp: running-config
Address or name of remote host []? 192.168.1.101
Source filename []? R1-confg
Destination filename [running-config]?

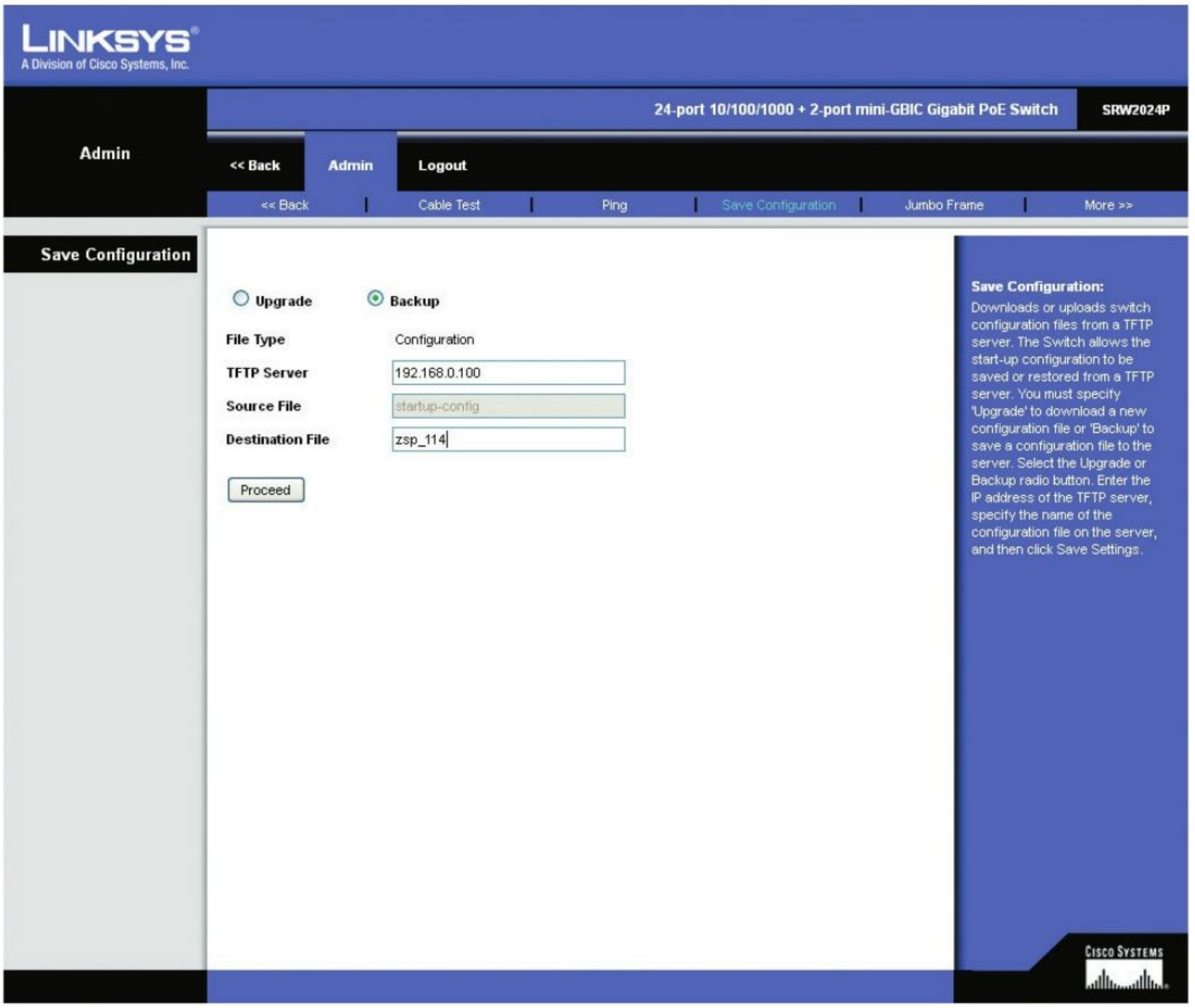
Accessing tftp://192.168.1.101/R1-confg...
Loading R1-confg from 192.168.1.101: !
[OK - 564 bytes]

564 bytes copied in 0.001 secs (564000 bytes/sec)
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Rys. 59.6. **Procedura kopiowania pliku konfiguracyjnego z serwera TFTP**

W urządzeniach zarządzanych przez interfejs WWW również istnieje możliwość zapisania i odtworzenia zawartości pliku konfiguracyjnego urządzenia. Funkcja zapisu i odczytu danych pliku konfiguracyjnego przełącznika Linksys jest dostępna w zakładce **`Admin`**, na podstronie **`Save Configuration`** (rys. 59.7).



Rys. 59.7. Okno zapisywania i odtwarzania pliku konfiguracyjnego w przełączniku Linksys

Podobnie jak w przypadku komputerów, w kolejnych wersjach systemów operacyjnych są wprowadzane poprawki i usuwane pojawiające się błędy. Oprogramowanie systemowe urządzeń sieciowych powinno być aktualizowane. Do dobrych praktyk należy wykonanie kopii zapasowej systemu przed rozpoczęciem konfiguracji.

PRZYKŁAD 59.4

Zapisywanie na serwerze kopii zapasowej systemu operacyjnego

W tym ćwiczeniu za pomocą protokołu TFTP zostanie utworzona kopia zapasowa systemu operacyjnego routera. System operacyjny routera jest zapisany w jednym pliku. Nazwę tego pliku można odczytać po wydaniu na routerze polecenia **`show version`** (na rys. 59.8 nazwę pliku zaznaczono strzałką).

Aby zapisać na serwerze kopię pliku zawierającego system operacyjny routera, należy wykonać następujące czynności:

1. Połączyć komputer z routerem i nawiązać sesję.
2. W trybie użytkownika uprzywilejowanego wydać polecenie kopiowania pliku
   `copy flash: tftp:`

3. Wprowadzić nazwę dla pliku na routerze (ang. *Source filename*). Ponieważ w pamięci flash routera może być zapisanych wiele plików, należy podać nazwę pliku do kopiowania.

```
Router#show version
Cisco IOS XE Software, Version 03.16.05.S - Extended Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version Version 15.5 (3)S5, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Thu 19-Jan-17 11:24 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 37 seconds
Uptime for this control processor is 37 seconds
System returned to ROM by power-on
System image file is "bootflash:/isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin"
Last reload reason: PowerOn


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
```

Rys. 59.8. **Wyświetlenie nazwy pliku zawierającego system operacyjny**

4. Wprowadzić adres serwera TFTP.
5. Wprowadzić nazwę dla pliku na serwerze – domyślnie jest to ta sama nazwa co na routerze. Przebieg kopiowania przedstawiono na rys. 59.9.

```
R1#copy flash: tftp:
Source filename []? isr4300-universalk9.03.16.05.S.155-3.S5.ext.SPA.bin
Address or name of remote host []? 192.168.1.101
Destination filename [isr4300-universalk9.03.16.05.S.155-3.S5.ext.SPA.bin]?

Writing isr4300-universalk9.03.16.05.S.
155-3.S5.ext.SPA.bin...!!!
```

PRZYKŁAD 59.5

Odtwarzanie na routerze kopii zapasowej pliku zawierającego system operacyjny

W tym ćwiczeniu za pomocą protokołu TFTP zostanie odtworzona kopia zapasowa pliku zawierającego system operacyjny routera. Aby odtworzyć na routerze kopię pliku, należy wykonać następujące czynności:

1. Połączyć komputer z routerem i nawiązać sesję.
2. W trybie użytkownika uprzywilejowanego wydać polecenie kopiowania pliku:
   `copy tftp: flash:`
3. Wprowadzić adres serwera TFTP.
4. Wprowadzić nazwę pliku źródłowego na serwerze.
5. Wprowadzić nazwę pliku na routerze. Ponieważ kopiowanie pliku może skutkować czyszczeniem pamięci flash, system ostrzega użytkownika i żąda potwierdzenia wykonania tej operacji. Przebieg kopiowania przedstawiono na rys. 59.10.

```
R1#copy tftp: flash:
Address or name of remote host []? 192.168.1.101
Source filename []? isr4300-universalk9.03.16.05.S.155-3.S5.ext.SPA.bin
Destination filename [isr4300-universalk9.03.16.05.S.155-3.S5.ext.SPA.bin]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]

Accessing tftp://192.168.1.101/isr4300-universalk9.03.16.05.S.155-3.S5.ext.SPA.bin...
Loading isr4300-universalk9.03.16.05.S.155-3.S5.ext.SPA.bin from 192.168.1.101:
!!!
```

60 Gwarantowanie jakości usług QoS

ZAGADNIENIA

Przeciążenie i kolejkowanie sieci **Algorytmy kolejkowania** **Klasyfikacja ruchu**

Dane w sieci lokalnej przesyła się za pomocą łączy o różnej prędkości, np. Fast Ethernet lub Gigabit Ethernet. Połączenie sieci lokalnej z internetem najczęściej odbywa się z mniejszą prędkością. Ponadto poszczególne łącza są obciążone w różnym stopniu. Jeśli łącze będzie przeciążone, mogą występować zatory, powodujące obniżenie wydajności sieci. Najlepszym rozwiązaniem okazałoby się wtedy zwiększenie prędkości przesyłania danych w przeciążonym łączu, lecz nie zawsze jest to możliwe. Przeciążenia mogą występować również tylko okresowo.

W razie przeciążenia łącza część danych może zostać dostarczona z opóźnieniem lub całkowicie utracona. Celem **gwarantowania jakości usług w sieciach QoS** jest ograniczenie problemów związanych z chwilowym przeciążeniem łącza przez zapewnienie nierównego traktowania ruchu sieciowego. Dzięki uwzględnieniu mechanizmów działania QoS można opisać modele usług zintegrowanych i usług zróżnicowanych.

Architektura **usług zintegrowanych IntServ** (ang. *Integrated Services*) jest przeznaczona do transmisji danych wymagających określonej przepustowości łącza. Polega na gwarantowaniu jakości usług dla indywidualnych strumieni, mających jedno źródło i jedno miejsce docelowe. Urządzenia sieciowe, np. routery, muszą rozpoznawać i obsługiwać protokoły związane z rezerwacją zasobów, a aplikacja – mieć zdolność do określania i przekazywania do sieci wymagań dotyczących jakości usługi. W modelu określono trzy typy usług:

- usługi ściśle gwarantujące parametry połączenia (ang. *Guaranteed Quality of Service*), np. górną granicę wartości opóźnień, wymaganą przepływność i dopuszczalny procent utraty pakietów; przeznaczone dla aplikacji wymagających reżimu czasu rzeczywistego;
- usługi zapewniające pewną jakość obsługi, np. potrzebną przepustowość całego połączenia i jakość przekazu. Jeżeli na trasie występuje łącze, które nie spełnia wymagań żądania, jest wyszukiwana inna trasa, a jeśli takiej nie ma, jest wysyłany komunikat zwrotny i operacja zostaje anulowana;
- usługi bez zapewnienia parametrów transmisji (ang. *Best Effort*), w których transmisja danych odbywa się z możliwie najwyższą przepustowością, bez gwarancji parametrów przesyłu danych.

Architektura IntServ wymaga rezerwacji zasobów, np. za pomocą protokołu sygnalizacyjnego dla zestawienia połączenia w sieci **RSVP** (ang. *Resource Reservation Protocol*). Nadawca inicjuje żądanie rezerwacji zasobów i wysyła do sieci komunikat z informacją o wymaganej przepustowości. Każdy router na trasie przesyłu danych rezerwuje zasoby, dzięki czemu zapewnia potrzebną przepustowość całego połączenia oraz jakość przekazu. Jeżeli na trasie występuje łącze, które nie spełnia wymagań żądania, jest wyszukiwana inna trasa, a jeśli takiej nie ma, jest wysyłany komunikat zwrotny i operacja zostaje anulowana.

W architekturze **usług zróżnicowanych DiffServ** (ang. *Differentiated Services*) zapewnianie jakości usług odbywa się dla klasy połączeń. W nagłówku IP pole **usług zróżnicowanych** jest

zdefiniowane jako część pola TOS (ang. *Type of Service*). Składa się z sześciu bitów, które przenoszą informacje o priorytecie aplikacji będącej źródłem pakietu. Klasyfikacja pakietów do poszczególnych klas odbywa się wyłącznie w routerach brzegowych. Pozostałe routery odczytują to pole i wykorzystują jego wartości do zróżnicowania sposobu traktowania ruchu w sieci, zgodnie z regułami przekazywania pakietów, np. zaimplementowanych za pomocą kolejek. Przykładami kolejek są:

- **FIFO** (ang. *First In First Out*) – jest najpowszechniej stosowanym kolejkowaniem. Ta metoda nie korzysta z klasyfikowania, ponieważ wszystkie pakiety należą do tej samej klasy. Pakiety, które wchodzą do bufora, opuszczają go w takiej kolejności, w jakiej do niego weszły. Działanie tego algorytmu na przepływ danych jest związane z ograniczoną objętością bufora, który w momencie zapełnienia odrzuca przychodzące pakiety do czasu, aż zwolni się miejsce;
- **PQ** (ang. *Priority Queuing*) – polega na tym, że każdemu z pakietów jest przydzielany priorytet. Pakiety są ustawiane w hierarchii kolejek bazujących na ustawionych priorytetach (np. czterech kolejek: wysokiego, średniego, zwykłego i niskiego priorytetu). Jeśli nie ma żadnych pakietów w najwyższej kolejce, wtedy jest obsługiwana ta niżej położona. W następnej kolejności jest sprawdzana kolejka wyższa – jeśli są w niej jakieś pakiety, są one obsługiwane, jeśli nie ma, są obsługiwane pakiety znajdujące się w najwyższej kolejce w danym momencie. Proces trwa do momentu opróżnienia wszystkich kolejek. Główną wadą mechanizmu kolejkowania PQ jest częste przywłaszczanie pasma przez kolejkę o najwyższym priorytecie. Powoduje to, że pakiety o niższym priorytecie czekające w kolejce mogą nigdy nie zostać obsłużone;
- **PFPQ** (ang. *Per Flow Priority Queuing*) – jest zmodyfikowanym mechanizmem PQ. Usunięto z niego główną wadę PQ, czyli przywłaszczanie kolejek przez jeden przepływ. Utworzono tu wiele kolejek, które są przeznaczone na pakiety należące do jednego przepływu. Tak samo jak w kolejkowaniu PQ, istnieje podział kolejek według priorytetów (wysoki, średni, zwykły i niski). Kolejki o tym samym priorytecie są obsługiwane według wcześniej ustalonego algorytmu, co zapewnia równoprawne dzielenie wszystkich przepływów tego samego poziomu;
- **CQ** (ang. *Custom Queuing*) – pozwala na skonfigurowanie szesnastu niezależnych kolejek. Umożliwia określenie: potrzebnej liczby kolejek, aplikacji, które będą korzystały z tych kolejek, oraz sposobu, w jaki będą obsługiwane te kolejki. W każdym cyklu router pobiera z każdej kolejki wstępnie ustaloną liczbę danych, którą konfiguruje się jako liczbę bajtów. Dzięki temu można w przybliżeniu określić, jaką część pasma otrzyma każda kolejka;
- **WFQ** (ang. *Weighted Fair Queuing*) – jest automatycznym trybem kolejkowania, obsługującym klasy na podstawie list dostępu. Mechanizm dzieli pamięć buforową na tysiące niezależnych kolejek. WFQ polega głównie na przydzielaniu kolejkom wag. Są one przydzielane na podstawie liczby i długości pakietów – im większe i dłuższe, tym większa waga przyznawana kolejkom. Dzięki temu przepływy o wyższych wagach są obsługiwane rzadziej niż pozostałe, a to powoduje, że pasmo jest dzielone równo między przepływami.

Podczas kolejkowania część pakietów jest odrzucana, na co aplikacje reagują retransmisją. Powstaje wtedy przeciążenie, ponieważ przy pełnej kolejce są odrzucane wszystkie pakiety, przez co następuje wiele retransmisji. Jednym z głównych mechanizmów zapobiegania zatorom jest algorytm **RED** (ang. *Random Early Detection*), przeznaczony do protokołów reagujących na odrzucanie pakietów. Aby zapobiec gubieniu pakietów, są one odrzucane jeszcze przed umieszczeniem ich w kolejce. Podczas wypełniania kolejki przez pakiety do pewnego poziomu algorytm RED zaczyna losowo odrzucać pakiety. Aplikacje korzystające z protokołu TCP zmniejszają prędkość wysyłania, gdy zaczynają gubić pakiety, dzięki czemu nie dochodzi ani do przeciążenia kolejki, ani do gubienia pakietów.

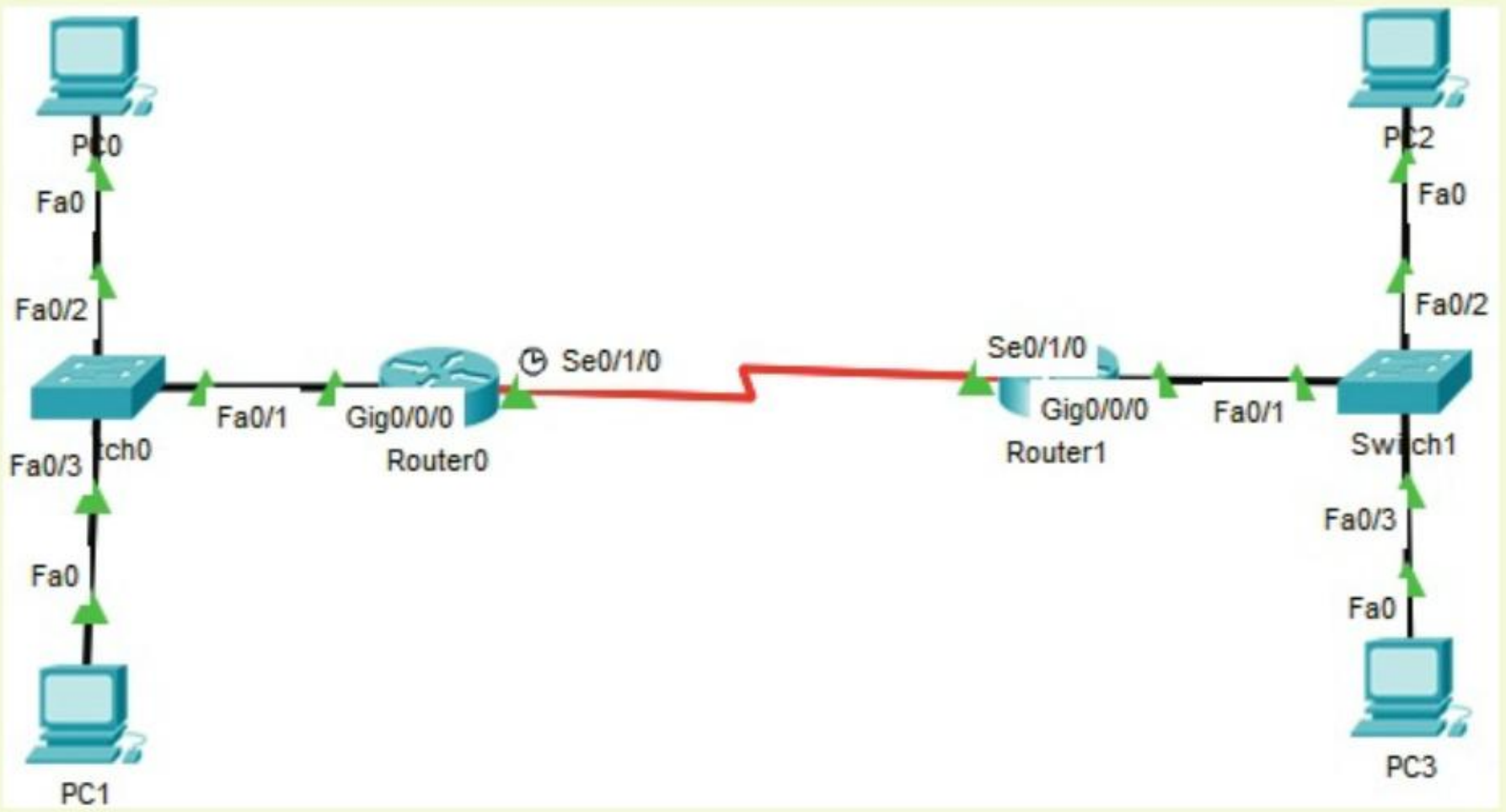
PRZYKŁAD 60.1

Konfigurowanie kolejki PQ w routerze

Komputery mogą wysyłać dane do routera za pomocą interfejsów fastethernetowych (100 Mb/s). Prędkość portu szeregowego jest zbyt mała, aby stało się możliwe przesłanie całego ruchu generowanego przez komputery do drugiej sieci lokalnej – co może powodować zatory. W tym ćwiczeniu na porcie szeregowym routera zostanie skonfigurowana kolejka priorytetowa PQ. Ruch związany z usługami WWW (port 80) i FTP (porty 20 i 21) zostanie przypisany do kolejki o wysokim (ang. *high*) priorytecie, ruch związany z usługami SSH (port 22) i TELNET (port 23) – do kolejki o średnim (ang. *medium*) priorytecie. Do kolejki o normalnym (ang. *normal*) priorytecie zostanie przydzielony ruch związany z pocztą elektroniczną (protokoły: SMTP – port 25, POP3 – port 110, IMAP – port 143). Reszta ruchu trafi do domyślnej kolejki o niskim (ang. *low*) priorytecie.

Aby skonfigurować kolejki na porcie routera, należy wykonać następujące czynności:

1. Połączyć urządzenia jak na na rys. 60.1.



Rys. 60.1. **Schemat sieci do testowania kolejki PQ**

2. Skonfigurować adresy komputerów i urządzeń. Można przypisać adresy z sieci `192.168.1.0/24` i `192.168.2.0/24` dla sieci lokalnych i adresy z sieci `10.0.0.0/30` dla portów szeregowych routerów.
3. Skonfigurować protokół routingu, np. RIP.
4. Przejść do trybu konfiguracji globalnej za pomocą poleceń:
   ```
   enable
   configure terminal
   ```
5. Przejść do trybu konfiguracji portu szeregowego:
   ```
   interface serial 0/1/0
   ```
6. Do interfejsu szeregowego przypisać grupę priorytetów o identyfikatorze 10:
   ```
   priority-group 10
   ```
7. Powrócić do trybu konfiguracji globalnej poleceniem:
   ```
   exit
   ```

8. Skonfigurować grupę priorytetów. Pakiety do kolejki o wysokim, średnim i niskim priorytecie będą wybierane za pomocą listy ACL o numerach (odpowiednio) 100, 110 i 120. Pozostałe pakiety zostaną umieszczone w kolejce o niskim priorytecie:
```
priority-list 10 protocol ip high list 100
priority-list 10 protocol ip medium list 110
priority-list 10 protocol ip normal list 120
priority-list 10 default low
```
9. Zdefiniować listę ACL dla priorytetu wysokiego. Do skonfigurowania listy 100 można użyć poleceń:
```
ip access-list extended 100
permit tcp any any eq 80
permit tcp any any eq 20
permit tcp any any eq 21
exit
```
10. Zdefiniować listę ACL dla priorytetu średniego. Do skonfigurowania listy 110 można użyć poleceń:
```
ip access-list extended 110
permit tcp any any eq 23
permit tcp any any eq 22
exit
```
11. Zdefiniować listę ACL dla priorytetu normalnego. Do skonfigurowania listy 110 można użyć poleceń:
```
ip access-list extended 120
permit tcp any any eq 25
permit tcp any any eq 110
permit tcp any any eq 143
end
```
12. Sprawdzić poprawność konfiguracji kolejki np. za pomocą polecenia:
```
show queueing
```

KODY

```
Router#show queueing
Current fair queue configuration

   Interface       Discrd      Dynamic   Reserved  Link      Priority
                   threshold   queues    queues    queues    queues
   Serial10/1/1    64          256       0         8         1

Current DLCI priority queue configuration
Current priority queue configuration:

List    Queue    Args
10      high     protocol ip          list 100
10      medium   protocol ip          list 110
10      normal   protocol ip          list 120
10      low      default
Current custom queue configuration:
Current random-detect configuration:
Current per-SID queue configuration:
Router#
```

Rys. 60.2. **Sprawdzanie konfiguracji kolejki w routerze**

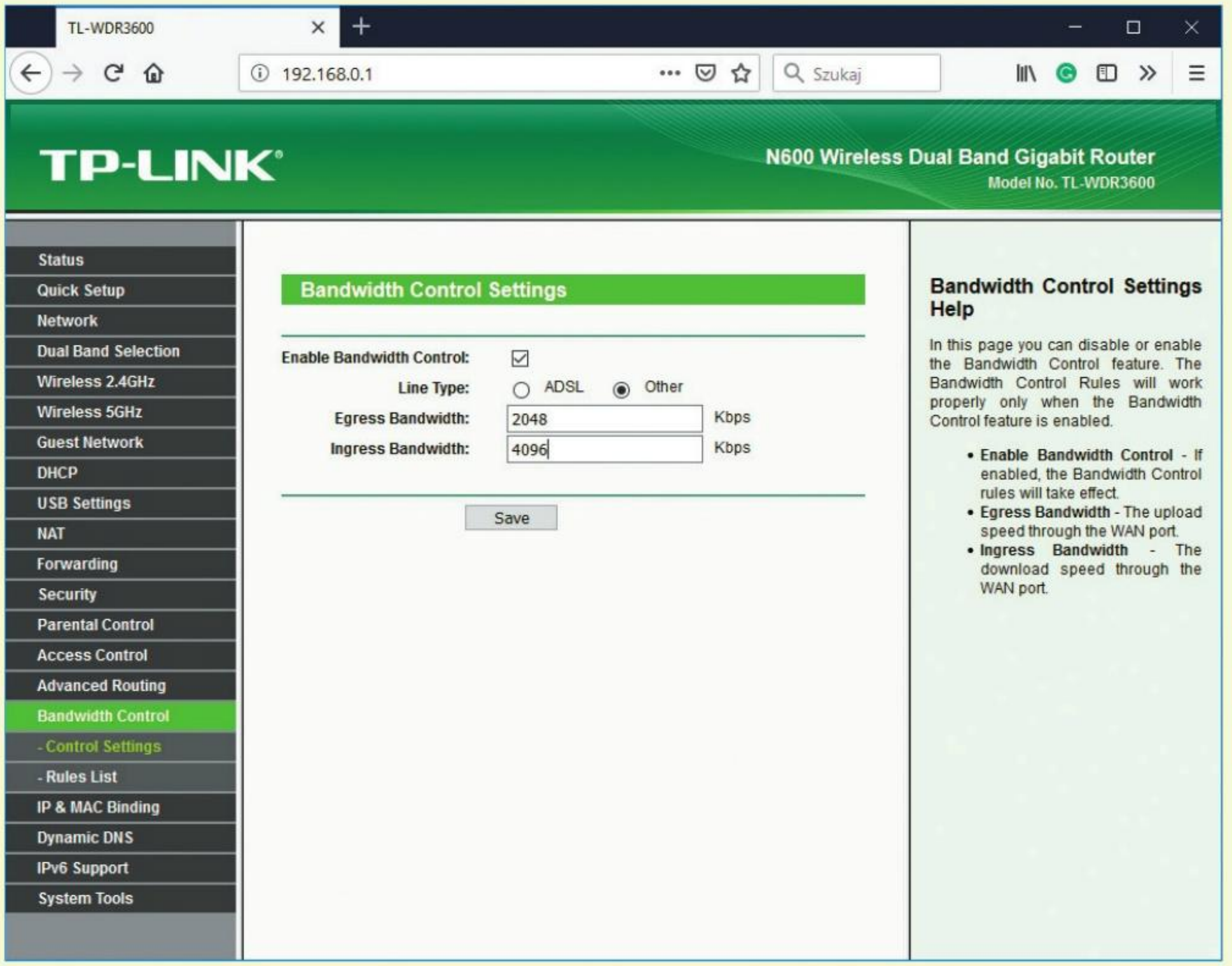
W sieci komputerowej w domu lub małej firmie łącze internetowe jest zwykle współdzielone przez komputery i inne urządzenia, np. tablety, smartfony. Stacja robocza intensywnie korzystająca z usług wymagających dużej przepustowości może wpływać na jakość połączenia, dostępną dla innych urządzeń, i wydajność całej sieci. W routerach przeznaczonych do zastosowań domowych może być zaimplementowana funkcja kontroli przepustowości (ang. *Bandwidth Control* lub IP QoS). Pozwala ona określić minimalną lub maksymalną przepustowość łączy dla poszczególnych stacji roboczych, identyfikowanych za pomocą adresów IP.

PRZYKŁAD 60.2

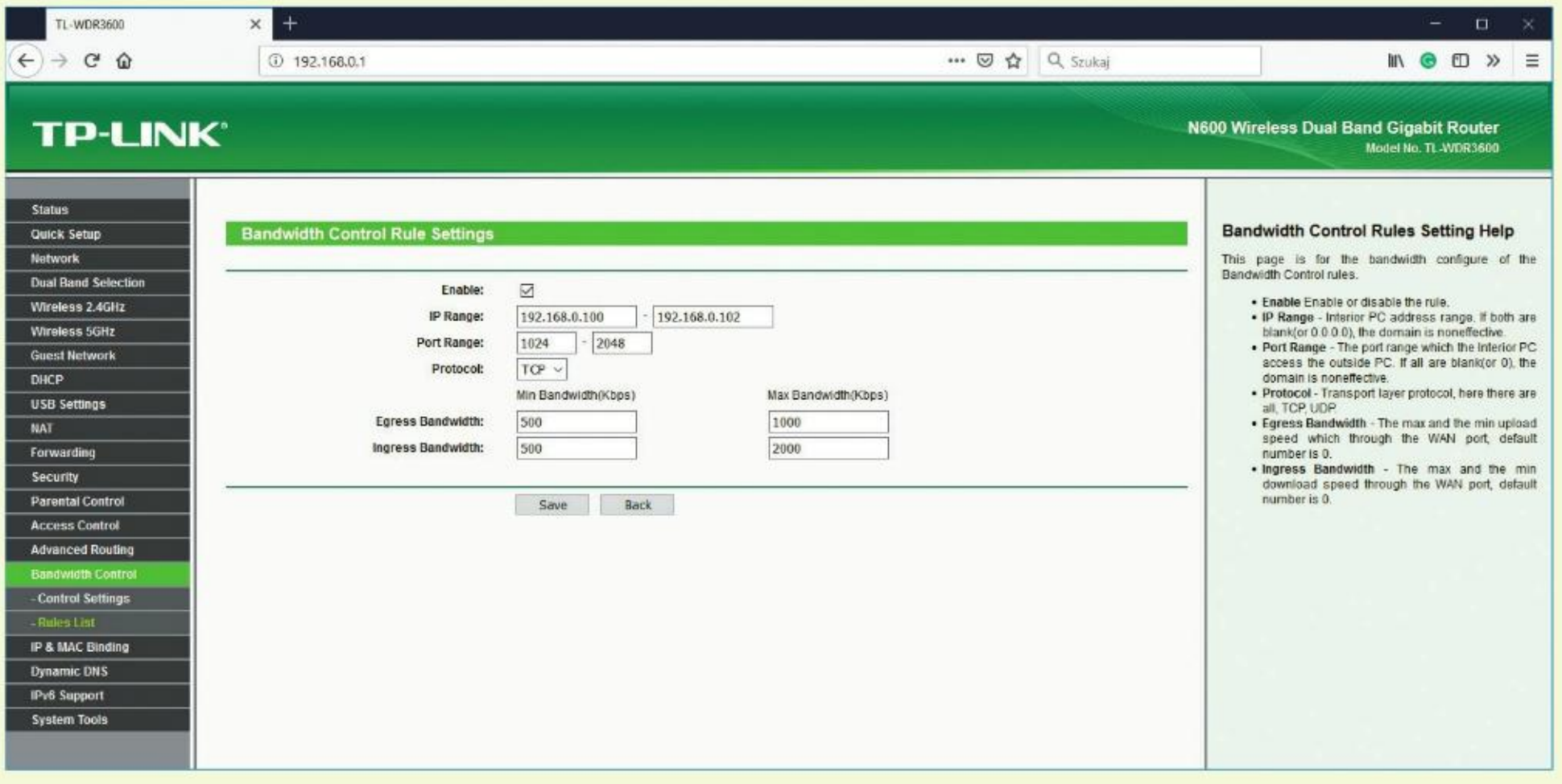
Konfigurowanie kontroli przepustowości w routerze

W tym ćwiczeniu zostanie skonfigurowana funkcja kontroli przepustowości, która pozwoli na określenie minimalnej i maksymalnej przepustowości dostępnej dla poszczególnych urządzeń (adresów IP). Aby skonfigurować funkcję kontroli przepustowości na routerze TP-Link TL-WDR-3600, należy wykonać następujące czynności:

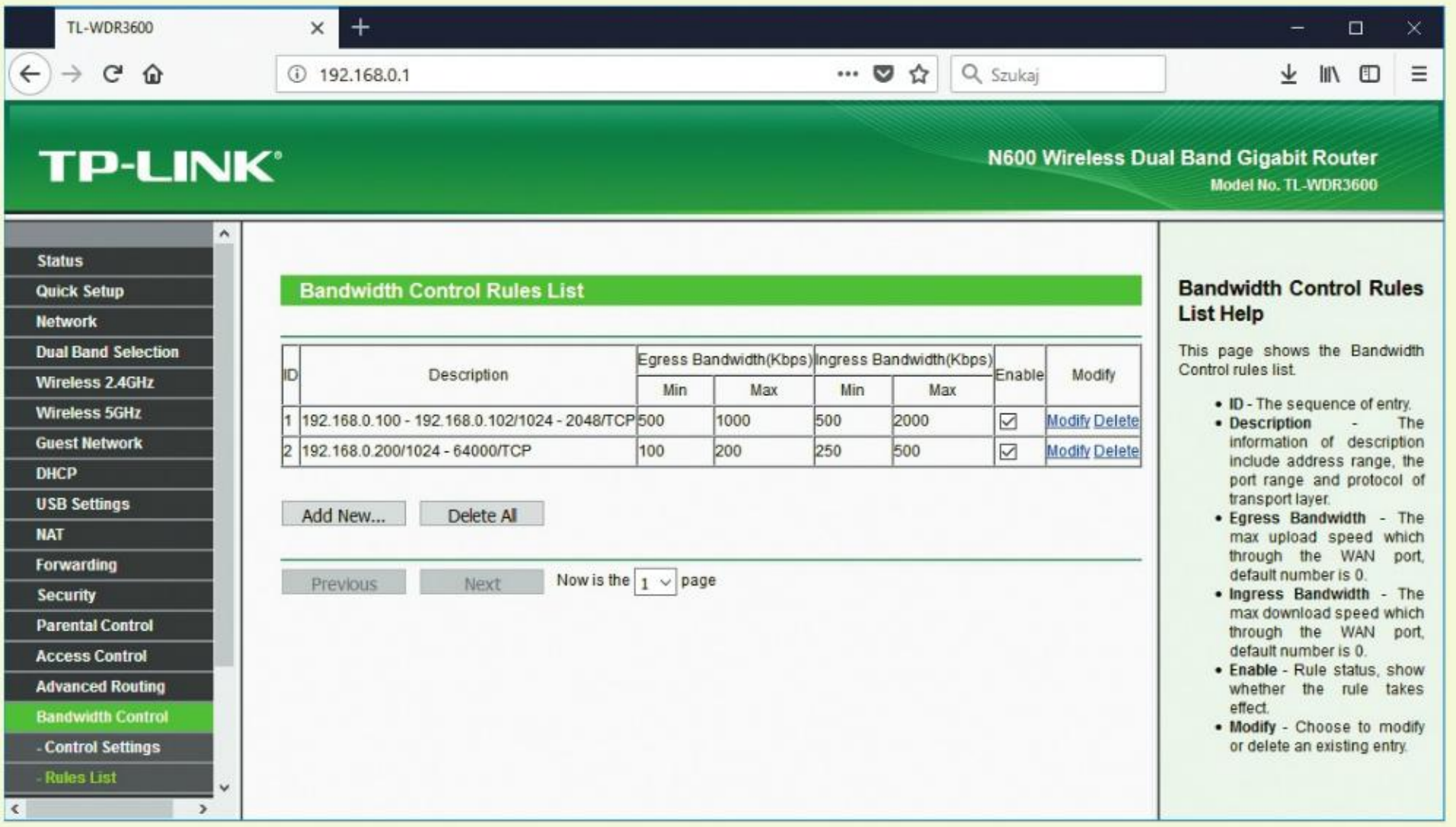
1. Połączyć router z komputerem, skonfigurować adresy IP i upewnić się, że urządzenia mają adresy z tej samej sieci.
2. W przeglądarce internetowej komputera w pole adres wpisać adres interfejsu LAN routera (domyślnie adres IP routera to **`192.168.0.1`**, konto: *admin*, hasło: **`admin`**). Nacisnąć klawisz [Enter], a następnie zalogować się na konto administratora.
3. Z menu po lewej stronie okna wybrać opcję **`Bandwidth Control/Control Settings`** i aktywować funkcję – zaznaczyć opcję **`Enable Bandwidth Control`** (rys. 60.3). Jeżeli połączenie internetowe jest dostępne przez usługę ADSL, należy wybrać opcję **`Line Type ADSL`**, w innym przypadku – **`Other`**. Wprowadzić informacje o przepustowości łącza (w kilobitach na sekundę) podczas wysyłania danych (ang. *Egress Bandwidth*) i pobierania danych (ang. *Ingress Bandwidth*).
4. Z menu po lewej stronie okna wybrać opcję **`Rules List`**, a następnie kliknąć przycisk **`Add New...`** (rys. 60.4).
5. W pole **`IP Range`** wprowadzić adres IP lub zakres adresów IP komputerów lokalnych, których reguła będzie dotyczyć. Jeżeli zostanie wprowadzony pojedynczy adres IP, to zostanie mu przydzielone wybrane pasmo transmisji. Jeżeli zostanie wprowadzony zakres adresów IP, to wszystkie komputery o adresach IP należących do wprowadzonego zakresu będą dzieliły dostęp do pasma transmisji.
6. W pole **`Port Range`** wprowadzić numer portu lub zakres numerów portów, których reguła będzie dotyczyć.
7. W polu **`Protocol`** zaznaczyć wykorzystywany protokół warstwy 4 modelu OSI.
8. W polu **`Egress Bandwidth`** ustawić minimalną i maksymalną przepustowość podczas wysyłania danych. Wartość minimalna oznacza gwarantowaną przepustowość łącza; nawet w przypadku dużego ruchu w sieci. Wartość maksymalna określa górną granicę przepustowości dostępną dla użytkownika.
9. W polu **`Ingress Bandwidth`** ustawić minimalną i maksymalną przepustowość podczas pobierania danych.
10. Zapisać regułę za pomocą przycisku **`Save`**.
11. Sprawdzić poprawność reguł (rys. 60.5). Suma wartości **`Minimum Bandwidth`** nie powinna być większa niż wartość przepustowości łącza. Poszczególne wartości **`Maximum Bandwidth`** nie powinny być większe niż wartość przepustowości łącza.



Rys. 60.3. **Aktywowanie funkcji kontroli przepustowości**



Rys. 60.4. **Wprowadzanie nowej reguły kontroli przepustowości**



Rys. 60.5. **Sprawdzanie poprawności reguł kontroli przepustowości**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj funkcję kontroli przepustowości dla szkolnego routera.
2. Skonfiguruj funkcję kontroli przepustowości dla domowego routera.

61 Konfiguracja sprzętowej zapory sieciowej

ZAGADNIENIA

- **Funkcje sprzętowej zapory sieciowej**
- **Sposób działania sprzętowej zapory sieciowej**
- **Sposoby konfigurowania sprzętowej zapory sieciowej**
- **Strefa zdemilitaryzowana**

Zapora sieciowa (ang. *firewall*) to jeden ze sposobów zabezpieczania sieci i pojedynczych komputerów przed zagrożeniami zewnętrznymi, np. atakami hakerów, a także wewnętrznymi, np. niekontrolowanym wyciekiem danych do sieci. Zapora sieciowa może pracować na styku sieci z internetem lub inną siecią. W takim przypadku służy do oddzielania od siebie ważnych podsieci LAN. Pozwala na kontrolowanie całego ruchu odbywającego się między sieciami. Może blokować ataki, ale również informować administratora o podejrzanych zdarzeniach. Nie jest jednak w stanie zabezpieczyć komputerów przed atakami pochodzącymi z komputerów w tej samej sieci. Zapora działająca na komputerze chroni tylko pojedyncze urządzenie, na którym jest zainstalowana. W celu zapewnienia bezpieczeństwa należy stosować oba typu zapór.

Dostępne są **zapory sprzętowe** (dedykowany sprzęt komputerowy wraz ze specjalnym oprogramowaniem) i **programowe**, instalowane lub umieszczane standardowo we wszystkich współczesnych systemach operacyjnych. Zapory sprzętowe są z reguły łatwiejsze do wdrożenia, oferują wiele funkcji, ale są droższe od rozwiązań programowych. Zapory programowe są trudniejsze w instalacji i konfiguracji, ponadto mogą dodatkowo obciążać komputery, na których pracują.

Zapora sieciowa może pracować jako **filtr pakietów** (ang. *packetfilters* / *stateless filter*). Filtr ma zdefiniowany zestaw **reguł filtrowania**. Jeżeli pakiet pasuje do reguły filtrowania odrzucającej pakiet, to jest on odrzucany (filtr może generować powiadomienie o odrzuceniu lub odrzucać bez powiadomienia). Pakiet, który pasuje do zaprogramowanych reguł filtrowania przepuszczających ruch, jest przepuszczany przez filtr. Filtry pakietów sprawdzają adres źródłowy i docelowy pakietu, protokół oraz porty źródłowe i docelowe.

Zapory sieciowe stanowe (ang. *stateful filters*) odgrywają rolę filtrów pakietów. Dodatkowo rejestrują wszystkie połączenia przechodzące przez zaporę. Na tej podstawie mogą ocenić, czy pakiet jest początkiem nowego połączenia, częścią istniejącego połączenia, czy nie jest częścią żadnego połączenia. Filtr stanowy może więc odrzucić pakiety, jeżeli użytkownik z internetu próbuje nawiązać połączenie z komputerem w sieci lokalnej, albo zezwolić temu samemu użytkownikowi na przesłanie danych, jeżeli komunikację zainicjował komputer z sieci lokalnej.

PRZYKŁAD 61.1

Konfigurowanie sprzętowej zapory sieciowej pracującej w trybie bezstanowym (filtru pakietów)

W tym ćwiczeniu zostanie skonfigurowana sprzętowa zapora sieciowa CISCO ASA 5506.

UWAGA

To ćwiczenie można wykonać, jeżeli dysponuje się sprzętową zaporą (w symulatorze Cisco Packet Tracer konfiguracja poniżej opisana nie zadziała).

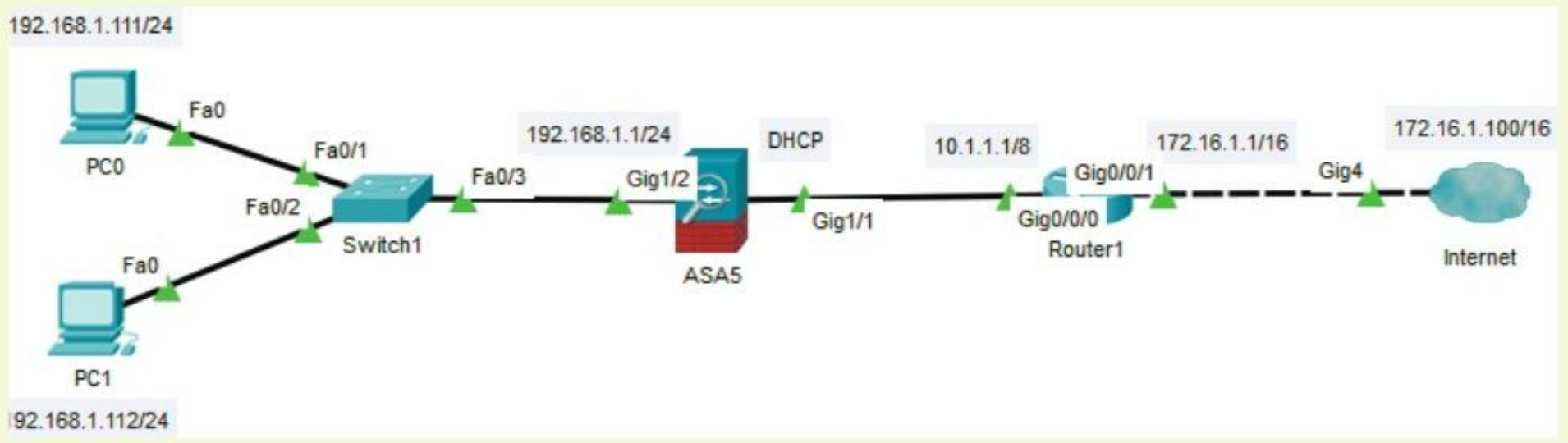
Domyślnie urządzenie zostało skonfigurowane następująco:

- sieć wewnętrzna LAN (ang. *inside*): **`192.168.1.0/24`**;
- sieć wewnętrzna LAN może komunikować się z internetem;
- interfejs (GE1/1) sieci zewnętrznej WAN (ang. *outside*) jest skonfigurowany do uzyskiwania adresu IP w sposób automatyczny z serwera DHCP;
- interfejs (GE1/2) sieci wewnętrznej LAN ma przydzielony adres **`192.168.1.1`**;
- serwer DHCP jest włączony do przydzielania adresów dla hostów w sieci lokalnej.

Zadaniem zapory jest filtrowanie ruchu między siecią lokalną a internetem.

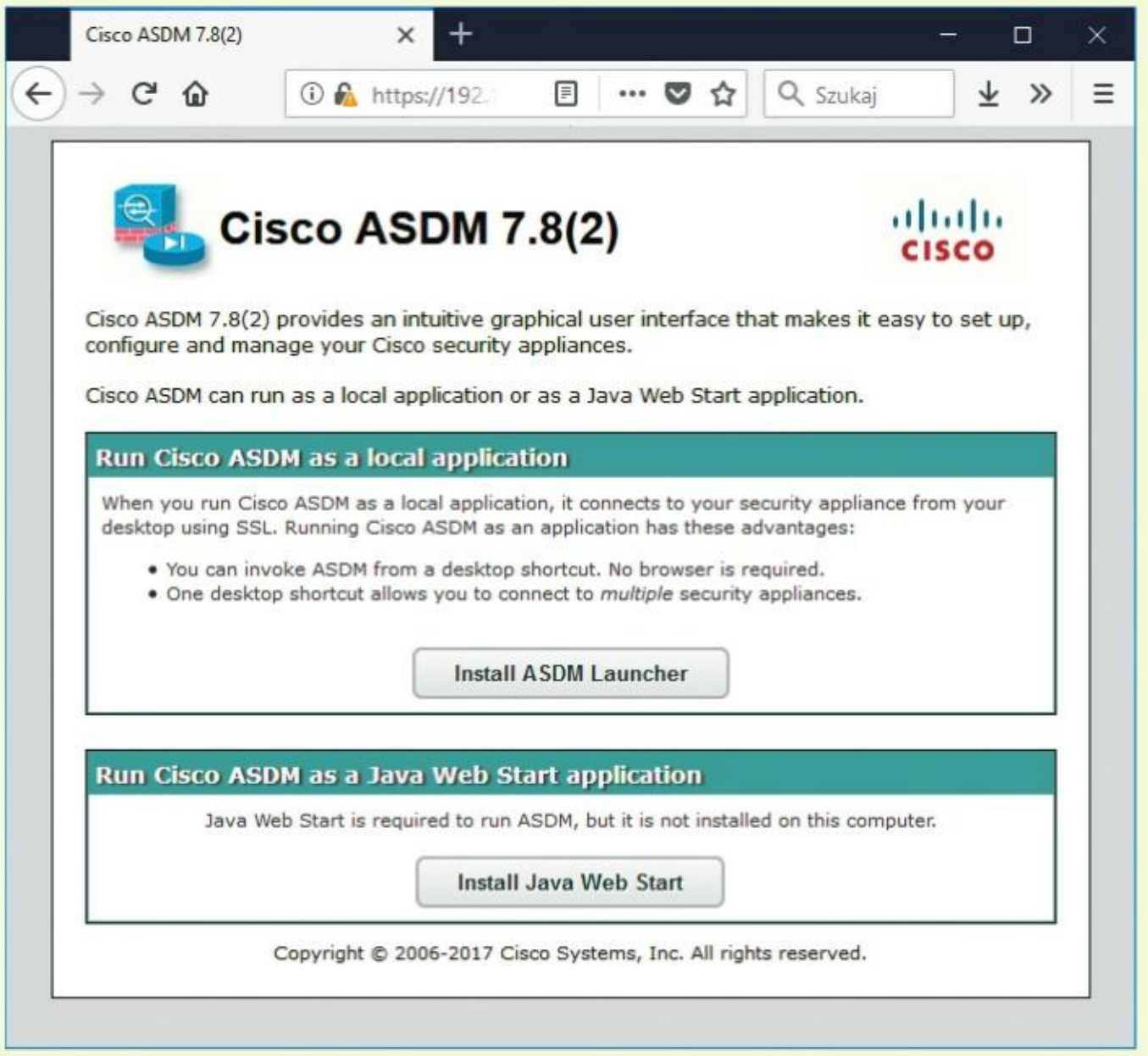
Aby skonfigurować sprzętową zaporę sieciową, należy wykonać następujące czynności:

1. Połączyć urządzenia jak na rys. 61.1 i przypisać adresy IP dla komputerów.

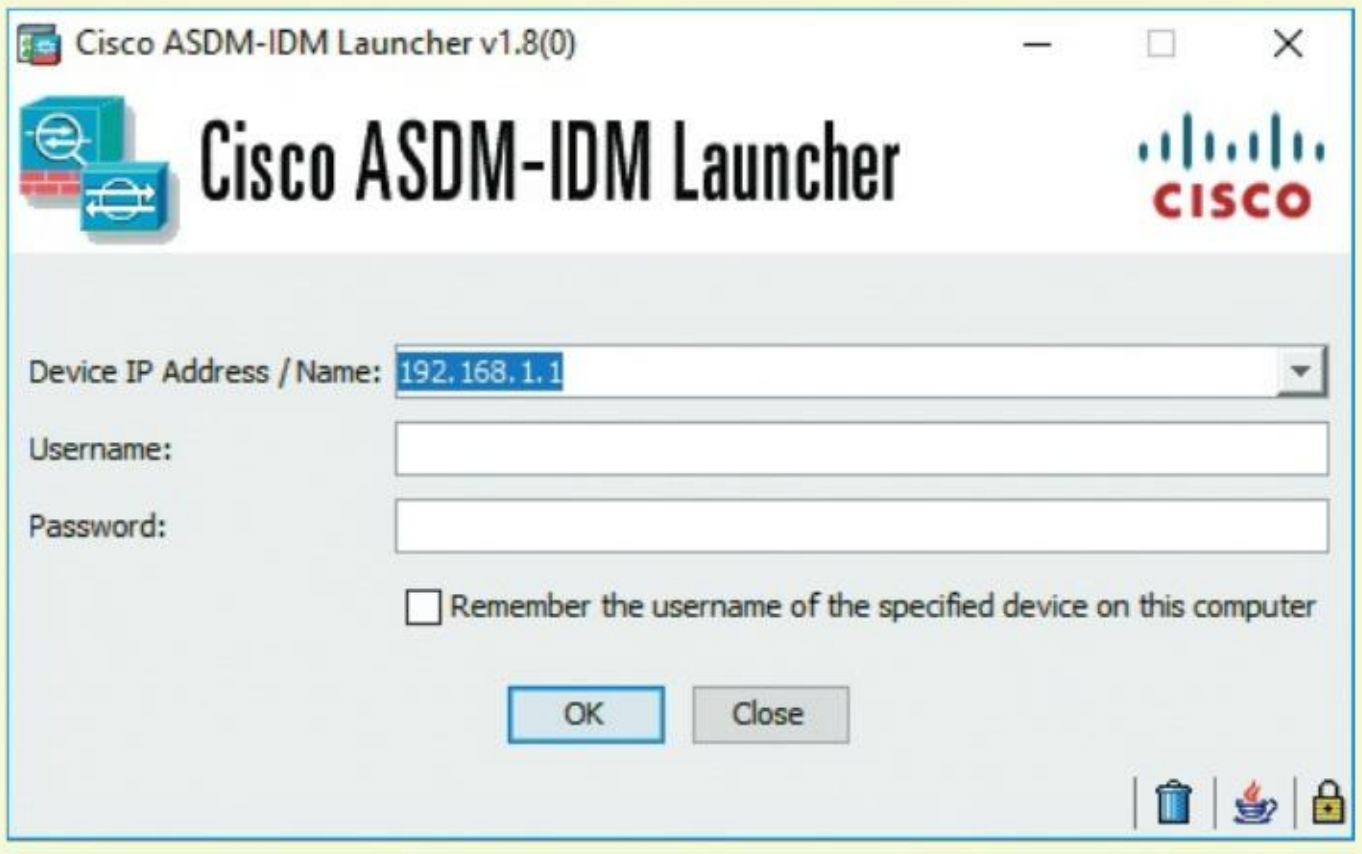


Rys. 61.1. **Schemat sieci z zaporą sieciową**

2. Skonfigurować adresy IP interfejsów routera. Włączyć serwer DHCP, przydzielający adres IP dla interfejsu WAN zapory.
3. Za pomocą przeglądarki internetowej komputera połączyć się z zaporą, z wykorzystaniem adresu **`https://192.168.1.1`** (rys. 61.2). Zainstalować program ASDM (ang. *Install ASDM Launcher*), umożliwiający administrowanie zaporą w środowisku graficznym. Jeśli podczas nawiązywania połączenia pojawią się komunikaty o naruszeniu reguł bezpieczeństwa, to należy dodać stronę do listy stron zaufanych w przeglądarce.
4. Uruchomić program ASDM. W polu **`Device IP Address`** wpisać adres zapory (**`192.168.1.1`**). Pola **`Username`** i **`Password`** pozostawić puste i kliknąć przycisk **`OK`** (rys. 61.3).

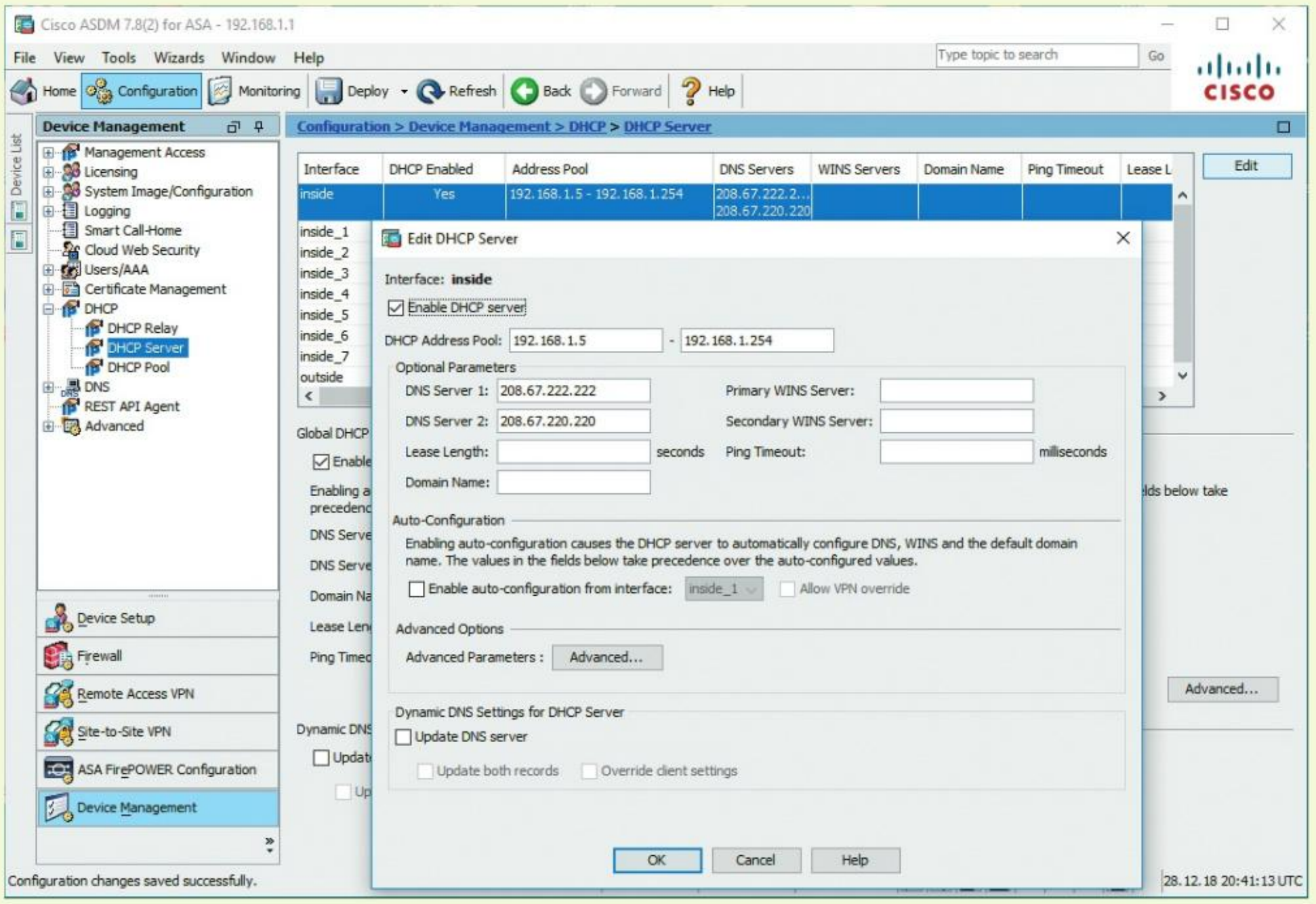


Rys. 61.2. **Uruchomienie instalatora ASDM**



Rys. 61.3. **Logowanie do zapory sieciowej**

5. Skonfigurować serwer DHCP, przydzielający adresy dla hostów w sieci lokalnej (rys. 61.4).W zakładce **`Configuration`** wybrać opcję **`Device Management`**. W sekcji **`Device Management`** rozwinąć gałęzie **`DHCP/DHCP Server`**. Wybrać interfejs **`inside`**, a potem kliknąć przycisk **`Edit`**. Zaznaczyć opcję **`Enable DHCP Server`**, następnie wprowadzić zakres adresów przydzielanych dla hostów (ang. *DHCP Address Pool*) i adresy serwerów DNS (ang. *DNS Server 1* i *DNS Server 2*). Kliknąć przycisk **`OK`**, a na końcu zastosować zmiany – przycisk **`Apply`**.



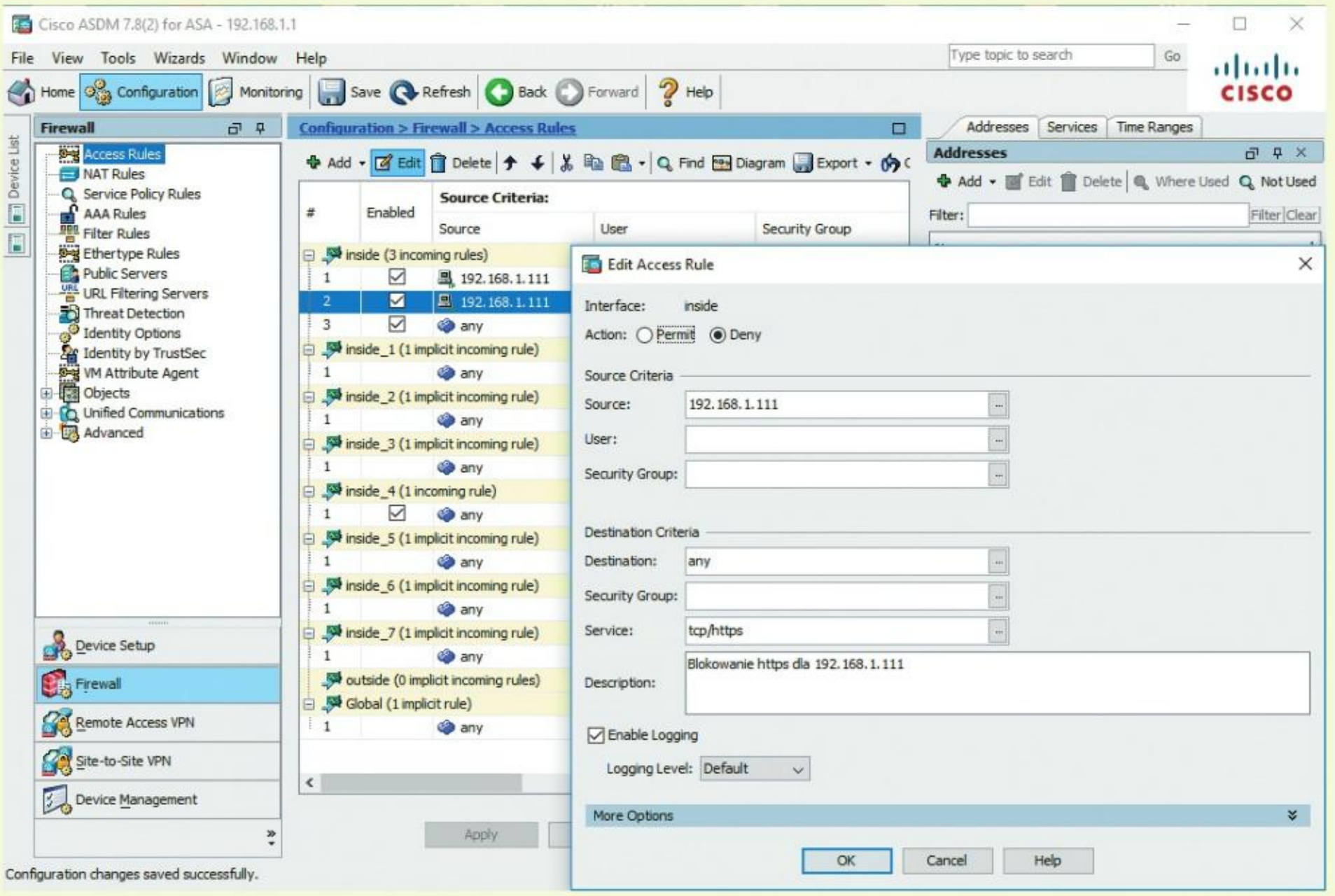
Rys. 61.4. **Konfigurowanie serwera DHCP w zaporze sieciowej**

6. Skonfigurować reguły dostępu (rys. 61.5). W zakładce **Configuration** wybrać opcję **Firewall**, a następnie – **Access Rules**. Dla wybranego interfejsu, np. inside, wprowadzić nową regułę. Kliknąć przycisk **Add** i skonfigurować regułę, np. **blokowanie** (ang. *Deny*), adres źródłowy (ang. *Source*) **192.168.1.111**, adres docelowy (ang. *Destination*) **any**, usługa (ang. *Service*) **tcp/https** i opis reguły (ang. *Description*) **Blokowanie https dla 192.168.1.111**. Kliknąć przycisk **OK**, a na końcu zastosować zmiany – przycisk **Apply**. Podobne reguły można wprowadzić dla innych hostów lub usług. Wprowadzane reguły muszą znajdować się powyżej domyślnej reguły przepuszczającej ruch z całej sieci lokalnej.

! UWAGA

Wprowadzona reguła blokuje ruch tyko protokołu HTTPS. Jeśli ma być blokowany ruch z protokołu http, to należy dodać kolejną regułę.

7. Przetestować działanie zapory. Korzystanie z usługi https z komputera **192.168.1.111** powinno zostać zablokowane, ale możliwe jest korzystanie z innych usług z tego komputera, np. z FTP. Dla pozostałych komputerów z sieci lokalnej obowiązuje domyślna reguła przepuszczająca cały ruch.



Rys. 61.5. **Konfigurowanie reguł dostępu w zaporze sieciowej**

Strefa zdemilitaryzowana to obszar sieci między siecią lokalną (LAN) a siecią globalną (WAN), w którym zwykle są umieszczane serwery, dostępne dla użytkowników z obu sieci. Dla stref w zaporze są przypisywane priorytety, na których podstawie są określane dopuszczalne przepływy danych. Najwyższy priorytet (100) przypisuje się do strefy sieci lokalnej (LAN), do strefy sieci globalnej (WAN) – najniższy (0), a do strefy zdemilitaryzowanej – 50. Dane ze strefy o wyższym priorytecie są domyślnie przesyłane do strefy o niższym priorytecie, np. z sieci LAN (100) do sieci WAN (0) i z sieci LAN (100) do DMZ (50). Przesyłanie danych ze strefy o niższym priorytecie do strefy o wyższym priorytecie jest domyślnie blokowane, np. z sieci WAN (0) do LAN (100) i z sieci WAN (0) do DMZ (50). Domyślnie klienci z sieci LAN mogą nawiązywać połączenia ze strefą DMZ, natomiast próby nawiązania połączenia z sieci WAN do DMZ są blokowane. Należy więc utworzyć specjalną regułę, która pozwoli na nawiązywanie połączeń z sieci WAN do strefy DMZ, ale tylko na adres serwera WWW i port 80. Jeżeli w strefie DMZ mają być dostępne inne usługi, to należy utworzyć dodatkowe reguły zezwalające na połączenia.

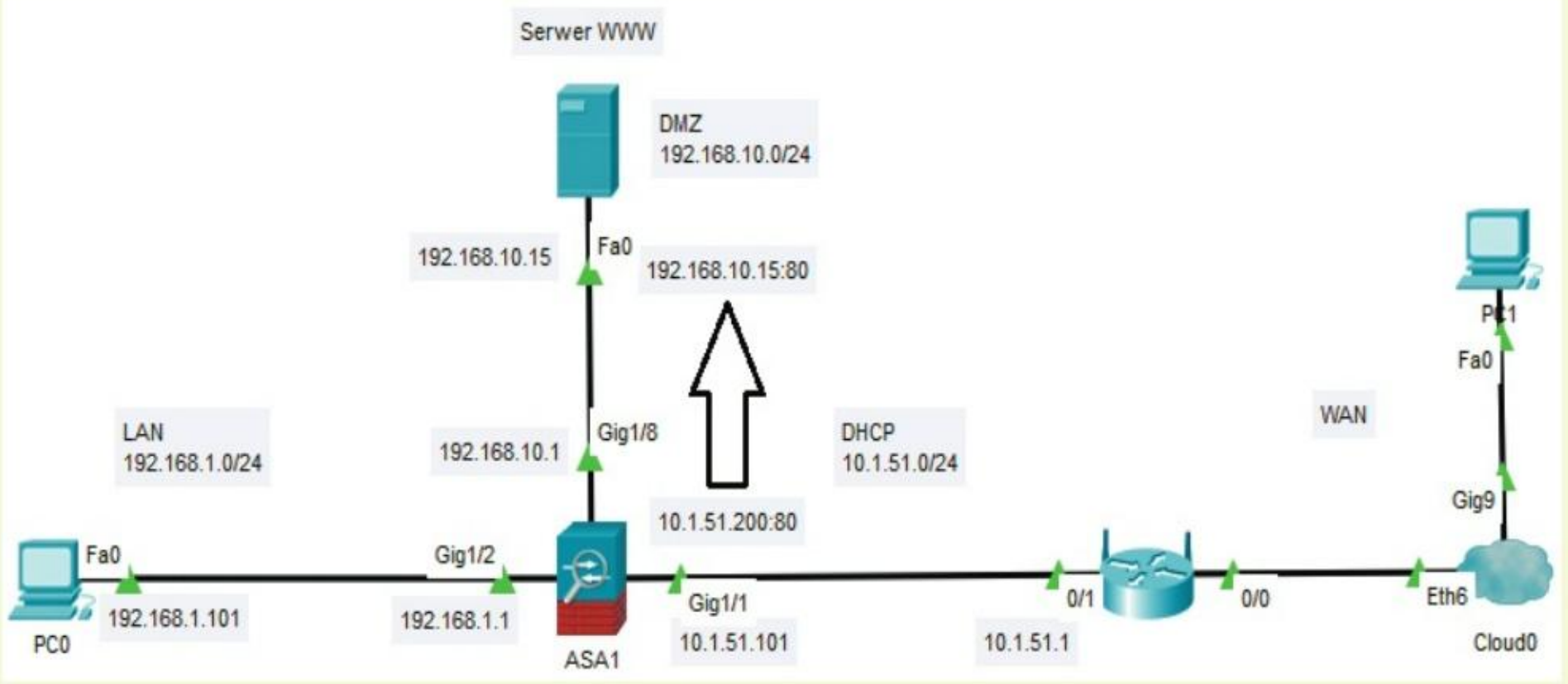
PRZYKŁAD 61.2

Konfigurowanie sprzętowej zapory sieciowej ze strefą zdemilitaryzowaną (DMZ)
W tym ćwiczeniu zostanie skonfigurowana sprzętowa zapora sieciowa CISCO ASA 5506 ze strefą DMZ, w której zostanie umieszczony serwer WWW.

UWAGA

To ćwiczenie można wykonać, jeżeli dysponuje się sprzętową zaporą (w symulatorze Cisco Packet Tracer konfiguracja poniżej opisana nie zadziała).

W zaporze interfejs GigabitEthernet 1/1 zostanie przeznaczony na dostęp do sieci WAN (sieć **10.1.51.0/24** – konfiguracja przez DHCP z routera), interfejs GigabitEthernet 1/2 zostanie przeznaczony do sieci LAN (**192.168.1.0/24**), natomiast interfejs GigabitEthernet 1/8 zostanie przeznaczony do strefy zdemilitaryzowanej (**192.168.10.0/24**). Schemat sieci przedstawiono na rys. 61.6.



Rys. 61.6. **Schemat sieci ze strefą DMZ**

Aby skonfigurować sprzętową zaporę sieciową, należy wykonać następujące czynności:

1. Połączyć urządzenia jak na rys. 61.6 i przypisać adresy IP dla komputerów i serwera.
2. Skonfigurować adresy IP interfejsów routera. Włączyć serwer DHCP, przydzielający adres IP dla interfejsu WAN zapory (**10.1.51.0/24**).
3. Przywrócić ustawienia fabryczne zapory. Skonfigurować interfejs GigabitEthernet 1/8 do pracy w sieci DMZ za pomocą poleceń:

```
enable
configure terminal
interface GigabitEthernet 1/8
no nameif
no bridge-group 1
nameif dmz
security-level 50
ip address 192.168.10.1 255.255.255.0
```

   Standardowo interfejsy GigabitEthernet 1/2-8 zapory są przyłączone do logicznego interfejsu (mostu) BVI1 o adresie **192.168.1.1** i nie można przypisać im adresów IP. Aby przydzielić interfejsowi GigabitEthernet 1/8 adres IP, należy najpierw usunąć nazwę interfejsu (polecenie **no nameif**), a następnie usunąć interfejs z mostu (polecenie **no brigde-group 1**). Poleceniem **nameif dmz** należy nadać nową nazwę interfejsowi, przypisać priorytet (polecenie **security-level 50**) i przydzielić adres IP (polecenie **ip address 192.168.10.1 255.255.255.0**).
4. Utworzyć trasę domyślną dla zapory. Trasa informuje zaporę, za pomocą którego adresu powinna ona wysyłać dane do internetu. Trasę tworzy się za pomocą polecenia:

```
route outside 0.0.0.0 0.0.0.0 10.1.51.1
```

5. Utworzyć obiekt reprezentujący sieć lokalną (inside-subnet) i skonfigurować translację adresów źródłowych (ang. *dynamic*) między interfejsem GigabitEthernet 1/2 (inside_1) i interfejsem GigabitEthernet 1/1 (outside) za pomocą poleceń:
```
object network inside-subnet
subnet 192.168.1.0 255.255.255.0
nat (inside_1,outside) dynamic interface
exit
```
6. Utworzyć obiekt reprezentujący sieć DMZ (dmz-subnet) i skonfigurować translację adresów źródłowych między interfejsem GigabitEthernet 1/8 (dmz) i interfejsem GigabitEthernet 1/1 (outside) za pomocą poleceń:
```
object network dmz-subnet
subnet 192.168.10.0 255.255.255.0
nat (dmz,outside) dynamic interface
exit
```
7. Utworzyć obiekt reprezentujący serwer WWW w sieci WAN (webserver-external-ip) i przypisać mu adres IP, np. **10.1.51.200**. Jeżeli użytkownik z sieci WAN zażąda połączenia z tym adresem, to jego żądanie zostanie przekierowane na adres serwera WWW (webserver) w strefie DMZ (przekierowanie ilustruje strzałka na rys. 61.6).
```
object network webserver-external-ip
host 10.1.51.200
exit
```
8. Utworzyć obiekt reprezentujący serwer WWW w strefie DMZ (webserver) i przypisać mu adres IP, np. **192.168.10.15**. Jeżeli użytkownik z sieci WAN zażąda połączenia z adresem (webserver-external-ip), to jego żądanie zostanie przekierowane na adres serwera WWW (webserver) w strefie DMZ. Skonfigurować translację adresów docelowych (ang. *static*) między interfejsem GigabitEthernet 1/8 (dmz) i interfejsem GigabitEthernet 1/1 (outside). Translacja dotyczy protokołu tcp i domyślnego portu usługi WWW:
```
object network webserver
host 192.168.10.15
nat (dmz,outside) static webserver-external-ip service tcp www
www
exit
```
9. Utworzyć listę kontroli dostępu (outside_acl), która zezwoli na przekazywanie ruchu protokołu tcp z dowolnego miejsca do serwera WWW w sieci DMZ (obiekt webserwer) na port usługi WWW. Umieścić listę na interfejsie outside na kierunku wejściowym.
```
access-list outside_acl extended permit tcp any object
webserver eq www
access-group outside_acl in interface outside
```
10. Przetestować działanie zapory sieciowej. W pole adres przeglądarki internetowej komputera w sieci WAN (PC1) wpisać adres **10.1.51.200**. Przetestować możliwości komunikacji między wszystkimi strefami.

KODY

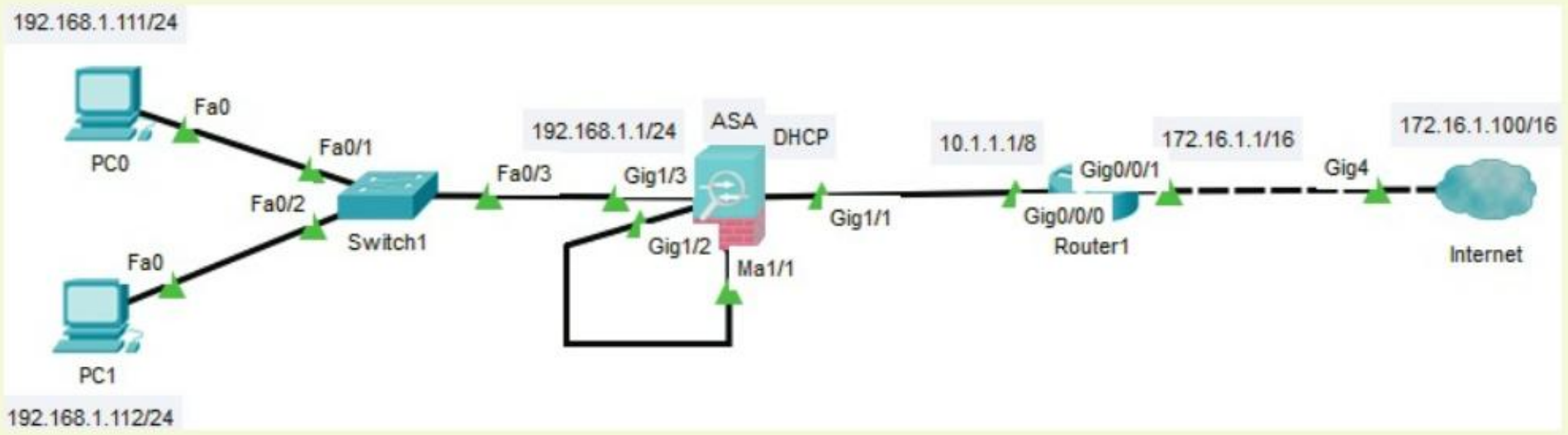
PRZYKŁAD 61.3

Konfigurowanie sprzętowej zapory sieciowej pracującej w trybie stanowym
W tym ćwiczeniu zostanie skonfigurowana sprzętowa zapora sieciowa CISCO ASA 5506 pracująca w trybie stanowym.

UWAGA

To ćwiczenie można wykonać, jeżeli dysponuje się sprzętową zaporą (w symulatorze Cisco Packet Tracer konfiguracja poniżej opisana nie zadziała). Ponadto konieczne jest nabycie odpowiednich licencji na użytkowanie modułu FirePOWER.

Za analizę ruchu jest odpowiedzialny dodatkowy moduł zapory o nazwie FirePOWER. Aby umożliwić jego działanie, należy połączyć port zarządzania (ang. *Management 1/1*) z portem GigabitEthernet 1/2 (jeśli masz starszą wersję ASA, np. z systemem poniżej 9.7, zapytaj nauczyciela, jak wykonać połączenie). Konfiguracja obejmuje dwa zadania: skonfigurowanie polityki bezpieczeństwa (reguł dostępu) i określenie, który ruch powinien być kierowany do dodatkowej analizy.



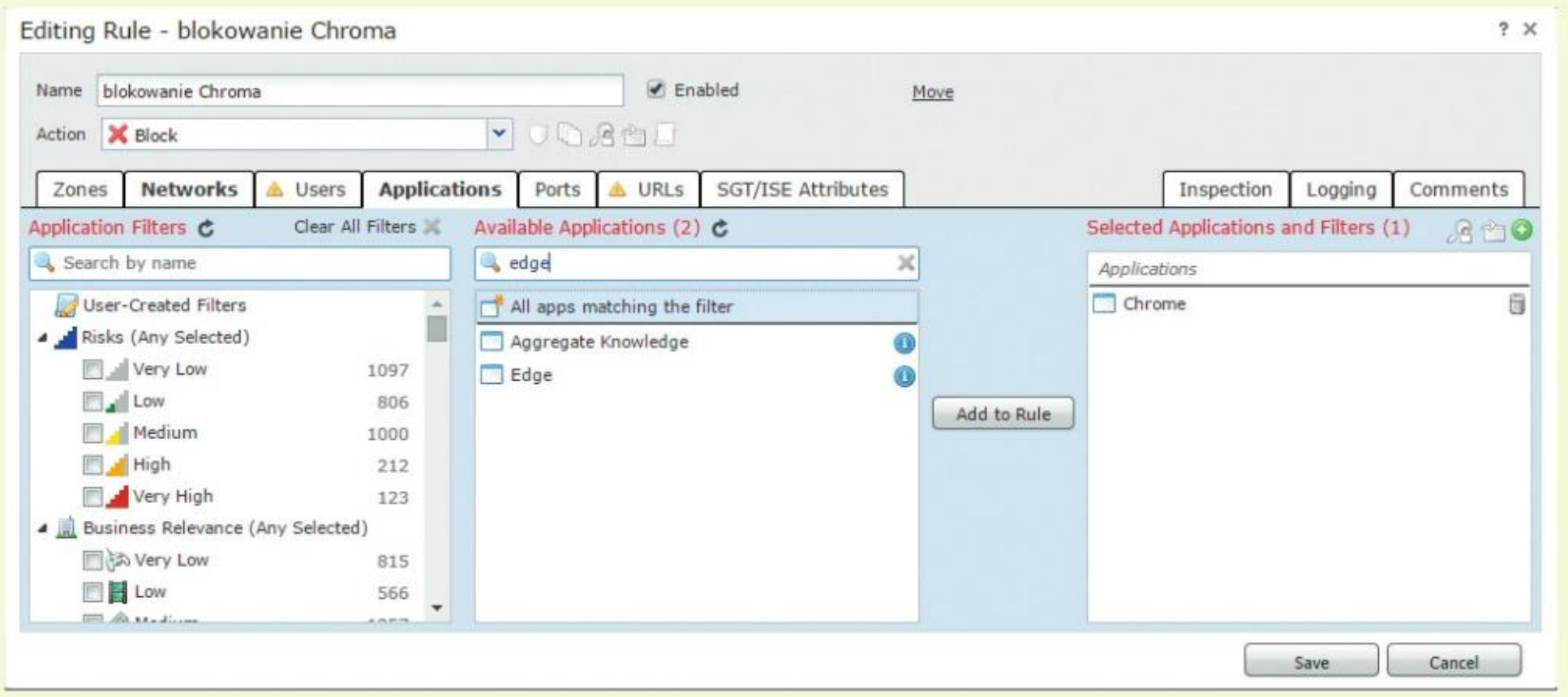
Rys. 61.7. **Schemat sieci z zaporą sieciową połączoną z modułem FirePOWER**

1. Uruchomić program ASDM. W polu **`Device IP Address`** wpisać adres zapory (**`192.168.1.1`**). Pola **`Username`** i **`Password`** pozostawić puste i kliknąć przycisk **`OK`**.
2. Uruchomić kreator konfiguracji początkowej **`Wizards/Startup Wizard`**.
3. W pierwszym oknie kreatora konfiguracji wybrać opcję modyfikowania istniejącej konfiguracji (ang. *Modify existing configuration*).
4. Skonfigurować ustawienia zapory w krokach od 2. do 8., np. nazwę, hasło, serwer DHCP, lub pozostawić konfigurację bez zmian.
5. W kroku 9. skonfigurować ustawienia modułu FirePOWER, np. maskę podsieci (ang. *Subnet Mask*) **`255.255.255.0`** i bramę (ang. *Gateway*) **`192.168.1.1`** (rys. 61.8). W pozostałych krokach nie wprowadzać zmian. Kliknąć przycisk **`Finish`**.
6. Skonfigurować reguły dostępu. W zakładce **`Configuration`** wybrać opcję konfiguracji modułu **`FirePOWER`** (ang. *ASA FirePOWER Configuration*), a następnie w gałęzi polityki (ang. *Policies*) – polityki kontroli dostępu (ang. *Access Control Policy*).
7. Wprowadzić nową regułę. Kliknąć przycisk dodaj regułę (ang. *Add Rule*) i skonfigurować regułę, np. **`blokowanie aplikacji Google Chrome`**. W polu nazwy (ang. *Name*) wprowadzić nazwę reguły, np. **`blokowanie Chroma`**, w polu akcji (ang. *Action*) wybrać **`blokowanie`** (ang. *Block*).



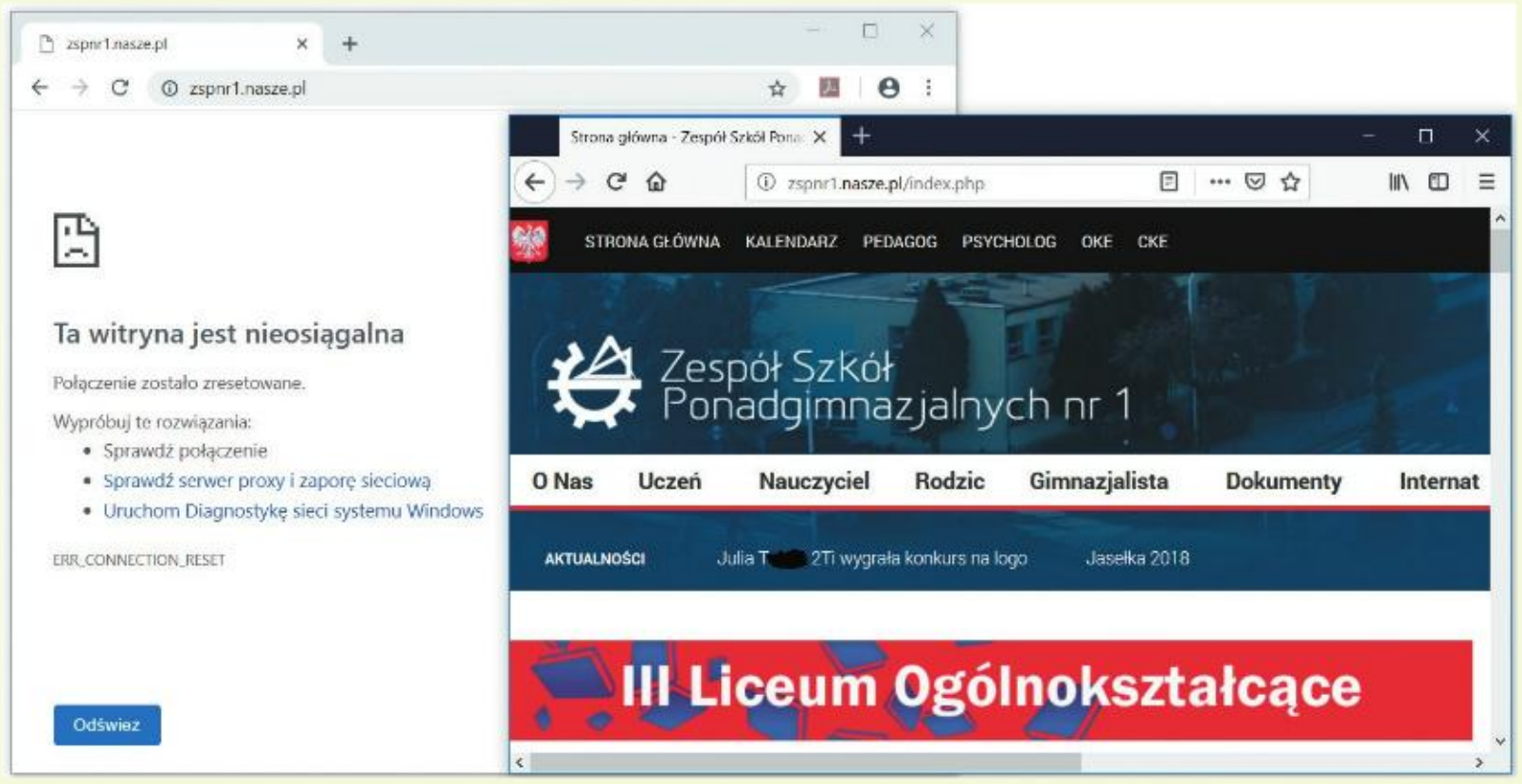
Rys. 61.8. **Konfiguracja modułu FirePOWER**

8. W zakładce sieci (ang. *Networks*) wskazać adres źródłowy hosta lub sieci (ang. *Source Networks*), np. **`192.168.1.5`**.
9. W zakładce aplikacji (ang. *Applications*) odszukać aplikację, która ma zostać zablokowana, np. w sekcji dostępnych aplikacji (ang. *Available Applications*) w oknie wyszukiwania można wpisać nazwę aplikacji. Dodać aplikację do listy wybranych (ang. *Seleted applications and filters*). Kliknąć przycisk **`Save`** (rys. 61.9).
10. Kliknąć przycisk **`Store ASA FirePOWER Changes`**.



Rys. 61.9. **Konfiguracja nowej reguły filtrowania aplikacji**

11. Określić, które dane mają być przesyłane do analizy w module FirePOWER. W zakładce **Configuration** wybrać opcję konfiguracji modułu zapory sieciowej, a następnie w gałęzi reguł polityki usług (ang. *Service Policy Rules*) kliknąć przycisk dodawania (ang. *Add*) i wskazać dodawanie reguły polityki usług (ang. *Add Servce Policy Rule*).
12. W oknie **Edit Service Policy Rule** w zakładce **Traffic Classification** wskazać, który ruch ma być kierowany do modułu FirePOWER, np. **Cały ruch** (ang. *Any traffic*). Można również wybrać precyzyjniej, np. za pomocą list kontroli dostępu (ACL) lub innej metody spośród dostępnych w oknie konfiguracyjnym.
13. W zakładce **Rule Actions** wybrać zakładkę **ASA FirePOWER Inspection** i zaznaczyć opcję **Enable ASA FirePOWER for this traffic flow**. Dodatkowo można wybrać, czy w razie awarii modułu FirePOWER ruch ma być przepuszczany (ang. *Permit traffic*), czy blokowany (ang. *Close traffic*). Kliknąć przycisk **OK**.
14. Kliknąć przycisk **Apply**.
15. Z menu wybrać polecenie **Deploy/Deploy FirePOWER Changes**.
16. Sprawdzić działanie zapory. Jeżeli reguła działa poprawnie, to ze wskazanego adresu, np. **192.168.1.5**, możliwe będzie połączenie z serwerem WWW realizowane za pomocą dowolnej przeglądarki internetowej z wyjątkiem **Google Chrome** (rys. 61.10).



Rys. 61.10. **Testowanie zapory sieciowej**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Przeanalizuj polecenia służące do konfiguracji zapory ze strefą DMZ. Za pomocą aplikacji ASDM otwórz wszystkie obiekty niezbędne do takiej konfiguracji. Sprawdź działanie sieci.
2. Sporządź listę aplikacji, które twoim zdaniem powinny być blokowane w szkole. Uzasadnij wybór.
3. Skorzystaj z oferty wybranego producenta sprzętowych zapór sieciowych i dobierz urządzenie o wydajności wystarczającej w twojej szkole.

- Urządzenia pomiarowe i diagnostyczne
- Oprogramowanie monitorujące lokalne sieci komputerowe
- Rodzaje awarii sieciowych i ich przyczyny
- Procedury serwisowe dotyczące urządzeń sieciowych
- Sposoby naprawy okablowania strukturalnego

Diagnostyka i naprawa lokalnych sieci komputerowych

VI

62 Urządzenia pomiarowe i diagnostyczne

ZAGADNIENIA

Urządzenia wykorzystywane do pomiarów i diagnostyki sieci **Przeprowadzanie procedury pomiarów różnego typu urządzeniami** **Dobór urządzeń pomiarowych**

Urządzenia diagnostyczne i pomiarowe wykorzystuje się zarówno podczas budowy i odbioru wykonania okablowania sieci, jak i w czasie jej normalnej eksploatacji. Cele pomiarów i rodzaje stosowanych do tego urządzeń mogą być jednak różne. Podczas wykonywania okablowania instalator wykorzystuje proste urządzenia, dzięki którym może sprawdzić instalację pod względem zgodności montażu i ciągłości kabli. Do tego celu używa się prostego testera okablowania (rys. 62.1). Tester pozwala wykryć usterki, takie jak niewłaściwe połączenia czy brak przejść.



Rys. 62.1. **Tester okablowania**

Podczas odbioru instalacji okablowania należy wykonać bardziej szczegółowe testy mające na celu sprawdzenie dodatkowych parametrów okablowania zgodnie z przyjętymi standardami i normami, odpowiednio dla danego typu sieci. Aby sieć została dopuszczona do użytku, powinna otrzymać certyfikat zgodności z wymaganiami. Sprawdzeniu podlega każdy tor transmisyjny. Do sprawdzania wykorzystuje się specjalne urządzenia diagnostyczne (rys. 62.2), wykonujące wszystkie niezbędne pomiary i sporządzające raporty. Wydruki z raportów należy dołączyć do dokumentacji powykonawczej sieci. Przykład wydruków przedstawiono na rys. 62.3 i 62.4.



Rys. 62.2. **Urządzenie diagnostyczne do certyfikowania sieci**

Job Name:
Company:

Report Date: Monday, November 09, 2009 10:20 AM
Version: 1.0.1.7

Summary:

All Cables	Twisted Pair	Coax/Twinax	Fiber
Total: 2	Total: 2	Total: 0	Total: 0
Pass: 2	Pass: 2	Pass: 0	Pass: 0
Fail: 0	Fail: 0	Fail: 0	Fail: 0
Tot. Length: 131,0m	Tot. Length: 131,0m	Tot. Length: 0m	Tot. Length: 0m

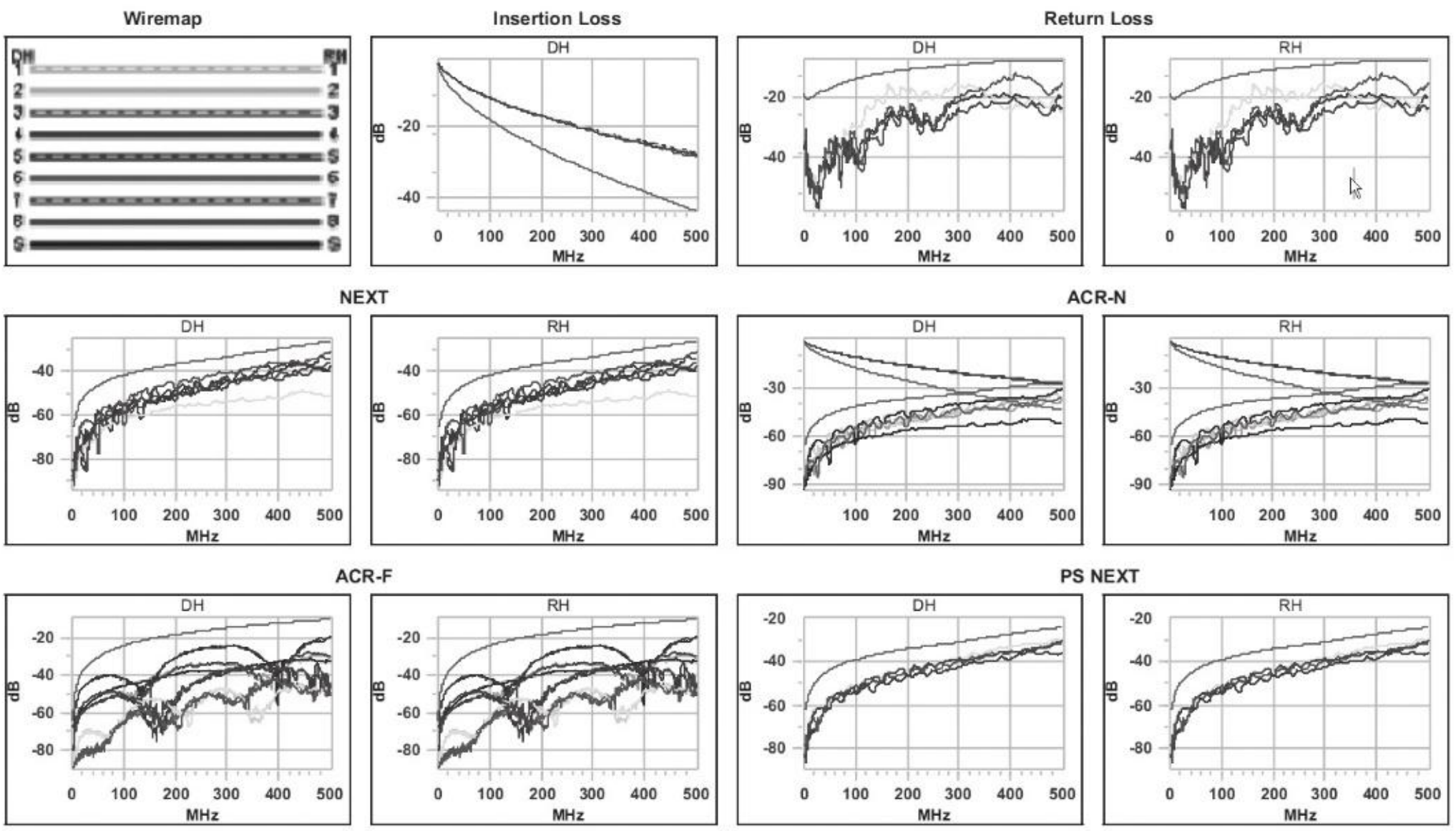
Pass

Test Name: K10014
Test Limit: Cat 6a 500 STP Perm
Test Date: 11/3/2009
Test Time: 18:12:21
Adapter ID: 6004
User Notes: Kabel poziomy I pietro, pokój 1

Standard: TIA 568-B.2-10
Frequency Range: 1 - 500MHz
Operator:
Contractor:
Company:

	Result	Worst Case Value	DH/RH	Pairs	Limit	Margin	Worst Overall Value	Limit	Margin
Wiremap	Pass	N/A		N/A	N/A	N/A			
Length	Pass	65,5 m.		5,4	90,0 m.	24,5 m.			
DC Resistance	Pass	8,5 ohms		7,8	20,0 ohms	11,5 ohms			
Propagation Delay	Pass	309,5 ns		7,8	498,0 ns	188,5 ns			
Delay Skew	Pass	5,9 ns		7,8	498,0 ns	492,1 ns			
Insertion Loss	Pass	2,3 dB @ 3,1MHz	DH	7,8	< 3,1 dB	0,8 dB	28,3 dB @ 499,0MHz	< 43,9 dB	15,6 dB
Return Loss	Pass	12,1 dB @ 410,0MHz	DH	3,6	> 8,0 dB	4,1 dB	20,1 dB @ 408,0MHz	> 8,0 dB	12,1 dB
NEXT	Pass	30,9 dB @ 500,0MHz	DH	7,8-5,4	> 26,7 dB	4,2 dB	49,4 dB @ 439,0MHz	> 28,5 dB	20,9 dB
ACR-N	Pass	50,6 dB @ 58,8MHz	DH	3,6-1,2	>= 32,0 dB	18,6 dB	23,4 dB @ 439,0MHz	>= -12,2 dB	35,6 dB
ACR-F	Pass	67,6 dB @ 1,0MHz	DH	3,6-5,4	> 64,2 dB	3,4 dB	45,9 dB @ 441,0MHz	> 11,3 dB	34,6 dB
Headroom	Pass	43,8 dB		N/A	N/A	N/A			
PS NEXT	Pass	29,3 dB @ 496,0MHz	RH	3,6	> 23,8 dB	5,5 dB	35,3 dB @ 500,0MHz	> 23,7 dB	11,6 dB
PS ACR-N	Pass	48,3 dB @ 58,8MHz	DH	1,2	> 29,0 dB	19,3 dB	8,2 dB @ 500,0MHz	> -20,2 dB	28,4 dB
PS ACR-F	Pass	66,9 dB @ 1,0MHz	DH	3,6	> 61,2 dB	5,7 dB	34,6 dB @ 367,0MHz	> 9,9 dB	24,7 dB

Rys. 62.3. Przykładowy wydruk pomiarów testera okablowania



Rys. 62.4. Wykresy generowane w raporcie testera okablowania

Podczas normalnej eksploatacji sieci może dochodzić do awarii okablowania, np. przerwania kabla. W przypadku kabla umieszczonego w rynienkach lub zakopanego w ziemi ustalenie miejsca wystąpienia uszkodzenia jest bardzo trudne, ale konieczne. Do tego celu można wykorzystać **reflektometr TDR** (ang. *Time-Domain Reflectometer*), przedstawiony na rys. 62.5. Działanie przyrządu polega na porównaniu parametrów impulsu pomiarowego wysyłanego w kierunku

przewodu badanego z impulsem powrotnym odbitym od końca przewodu (lub od jego niejednorodności, występujących np. w punktach łączenia poszczególnych odcinków). Na podstawie pomiaru czasu potrzebnego na powrót sygnału i charakteru jego zniekształceń można precyzyjnie ocenić długość przewodu, tłumienność i charakter uszkodzenia, np. czy jest to przerwa, zwarcie lub zmiana tłumienności spowodowana dostaniem się do przewodu wody bądź jego zawilgoceniem. W funkcję reflektometru są zaopatrzone również niektóre zaawansowane testery okablowania.

Testowanie okablowania światłowodowego polega na sprawdzeniu tłumienia okablowania w oknach transmisyjnych. Przed przystąpieniem do testowania należy sprawdzić, z jakiego typu włókna jest wykonana instalacja i jakich złączy użyto do zakończenia kabli. Pomiar tłumienia można wykonać **miernikiem tłumienia optycznego**. Składa się on z dwóch części: źródła światła generującego sygnał o określonej częstotliwości i **miernika tłumienia optycznego** (rys. 62.6). Miernik optyczny wyposażono w przyciski umożliwiające ustawienie poziomu odniesienia na podstawie wstępnie mierzonego kabla krosowego i innych parametrów pomiaru, np. długości fali świetlnej, rodzaju pomiaru (tłumienia lub mocy optycznej).

Przed przyłączeniem miernika do toru optycznego należy przetrzeć złącza chusteczką nawilżoną spirytusem. Pomiar powinno się poprzedzić ustaleniem poziomu odniesienia. W tym celu miernik i źródło światła łączy się za pomocą dwóch kabli krosowych i adaptera. Kable krosowe muszą być wykonane z takiego samego typu włókna jak mierzony tor transmisyjny i mieć z jednej strony typ złącza, w które jest wyposażony miernik, a z drugiej strony – typ złącza, którym jest zakończony tor. Wynik pomiaru jest poziomem odniesienia (tłumieniem kabli, które posłużą do przyłączenia mierzonego toru transmisyjnego do miernika i źródła światła). Następnie za pomocą tych samych kabli krosowych należy przyłączyć miernik do mierzonego toru optycznego. Wartość tłumienia mierzonego toru światłowodowego uzyskuje się po odjęciu poziomu odniesienia od odczytanej wartości. Testowanie światłowodów można również wykonać **reflektometrem optycznym** (**OTDR** – rys. 62.7).



Rys. 62.5. Reflektometr do okablowania miedzianego

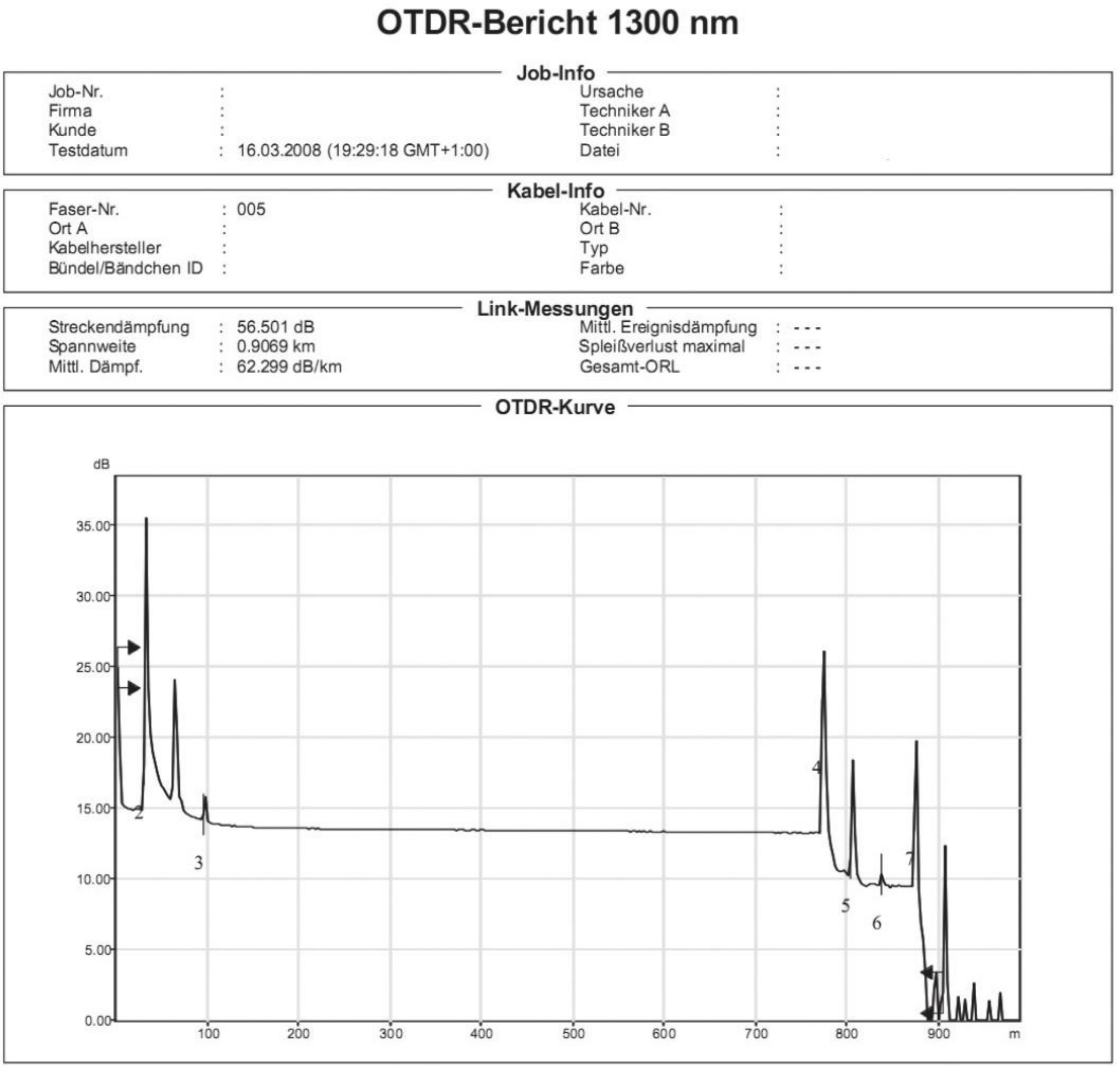


Rys. 62.6. Miernik tłumienia optycznego



Rys. 62.7. Reflektometr optyczny

Jest to urządzenie umożliwiające pomiar lub certyfikację światłowodów, przeprowadzanie testów PASS/FAIL oraz pomiar odległości i tłumienia. Przykład raportu z testera przedstawiono na rys. 62.8.



Rys. 62.8. **Raport z reflektometru OTDR**

Najbardziej zaawansowane urządzenia, nazywane **sprzętowymi analizatorami sieci,** wykonują wszystkie testy, zarówno pasywne, jak i aktywne. Przykład takiego urządzenia pokazano na rys. 62.9.

Analizator ma następujące cechy i pełni funkcje wymienione poniżej:

- testy sieci miedzianych i światłowodowych:
  - identyfikacja urządzeń aktywnych sieci za pomocą funkcji Network Discovery;
  - porównanie aktualnie występujących urządzeń w sieci z wcześniej zarejestrowanymi danymi za pomocą funkcji Network Verify;
  - wsparcie dla usług: klient DHCP, Ping i TraceRoute z VLAN (śledzenie trasy);



Rys. 62.9. **Analizator sieci**

  - tester pełnej przepustowości, 1, 2 i 3 warstwy sieci;
  - statystyki diagnostyczne obejmujące ostatnich dziesięciu nadawców, protokoły, generatory błędów i rozmiary rozesłanych pakietów;
- kable miedziane:
  - test mapy połączeń – testy każdej żyły kabla włącznie z pomiarem długości i wykryciem złego rozszycia par;
  - funkcja śledzenia przewodu w połączeniu z sondą indukcyjną;
  - wykrycie PoE i PoE+, możliwość sprawdzenia aktualnego zasilania i napięcia w konfiguracji In-Line lub endpoint;
  - monitoring sieci w konfiguracji In-Line i funkcja diagnostyki komputera;
  - monitoring i pomiar jakości telefonii VoIP włącznie z pomiarem RTP Jitter;
- kable światłowodowe:
  - obsługa modułów światłowodowych SFP jedno- i wielomodowych;
  - wsparcie aplikacji 1000 BASE-SX, LX i ZX;
  - funkcja Hub blink;
- Wi-Fi:
  - identyfikacja urządzeń aktywnych sieci za pomocą funkcji Network Discovery;
  - porównanie aktualnie występujących urządzeń w sieci z wcześniej zarejestrowanymi danymi za pomocą funkcji Network Verify;
  - wsparcie dla usług: klient DHCP, Ping i TraceRoute z VLAN (śledzenie trasy);
  - wsparcie dla wszystkich standardów 802.11;
  - identyfikacja access pointów, informacje o SSID, o kanałach w użyciu, o sile sygnału i o poziomie zabezpieczeń;
  - detekcja konfliktu kanałów.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sprawdź, czy kabel, którym twój komputer jest przyłączony do sieci, spełnia wymagania określone standardem lub normą. Jaka jest maksymalna prędkość, przy której kabel może działać?

63 Oprogramowanie monitorujące lokalne sieci

ZAGADNIENIA

Działanie skanera IP i wykorzystanie go do monitorowania sieci **Działanie skanera portów i wykorzystanie go do monitorowania sieci** **Działanie analizatora ruchu i wykorzystanie go do monitorowania sieci** **Monitorowanie sieci przez standardowe narzędzie systemu Windows** **Monitorowanie danych przesyłanych przez przełącznik**

Administrator powinien na bieżąco monitorować działanie sieci i rozwiązywać pojawiające się problemy. Istnieje wiele programów ułatwiających te zadania. Administrator powinien mieć przygotowany zestaw narzędzi gotowych do użycia, gdy pojawią się problemy. Pozwala to na skrócenie czasu reakcji na awarię. W dalszej części tego tematu przedstawimy kilka programów do monitorowania funkcjonowania sieci.

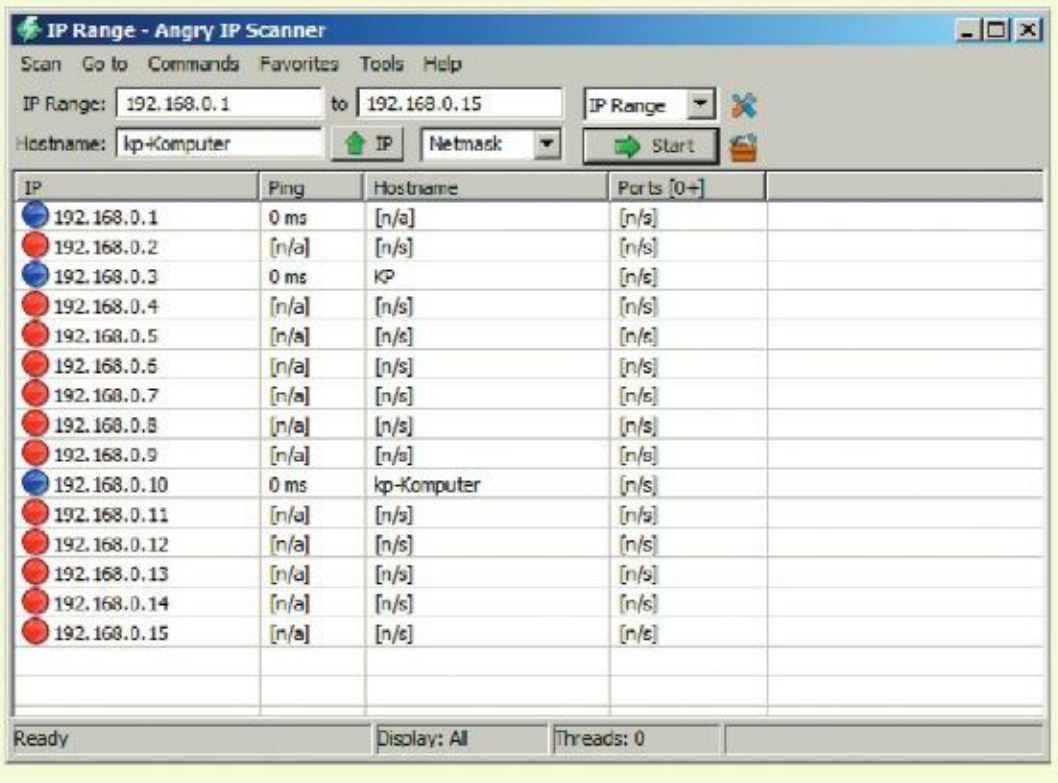
Wszystkie komputery w sieci muszą mieć unikatowe adresy IP. Zdarza się jednak, że użytkownicy, np. uczniowie, zmieniają adresy swoich komputerów. Jeżeli zdarzy się sytuacja, w której dwa komputery będą miały przypisany ten sam adres, to wystąpi **konflikt adresów** i żaden z nich nie będzie mógł korzystać z dostępu do sieci. Program nazywany **skanerem IP** pozwala na sprawdzenie, które adresy w danej sieci są aktualnie używane. Przykładem takiego programu jest **Angry IP Scanner**. Jest to program typu open-source, dostępny bezpłatnie na licencji GPLv2. Istnieją wersje programu dla systemów Windows, Linux i MacOS X.

PRZYKŁAD 63.1

Skanowanie adresów IP w sieci

Aby sprawdzić, jakie adresy IP są używane w sieci, należy wykonać następujące czynności:

1. Pobrać i uruchomić program **`Angry IP Scanner`**. Okno główne programu przedstawiono na rys. 63.1.

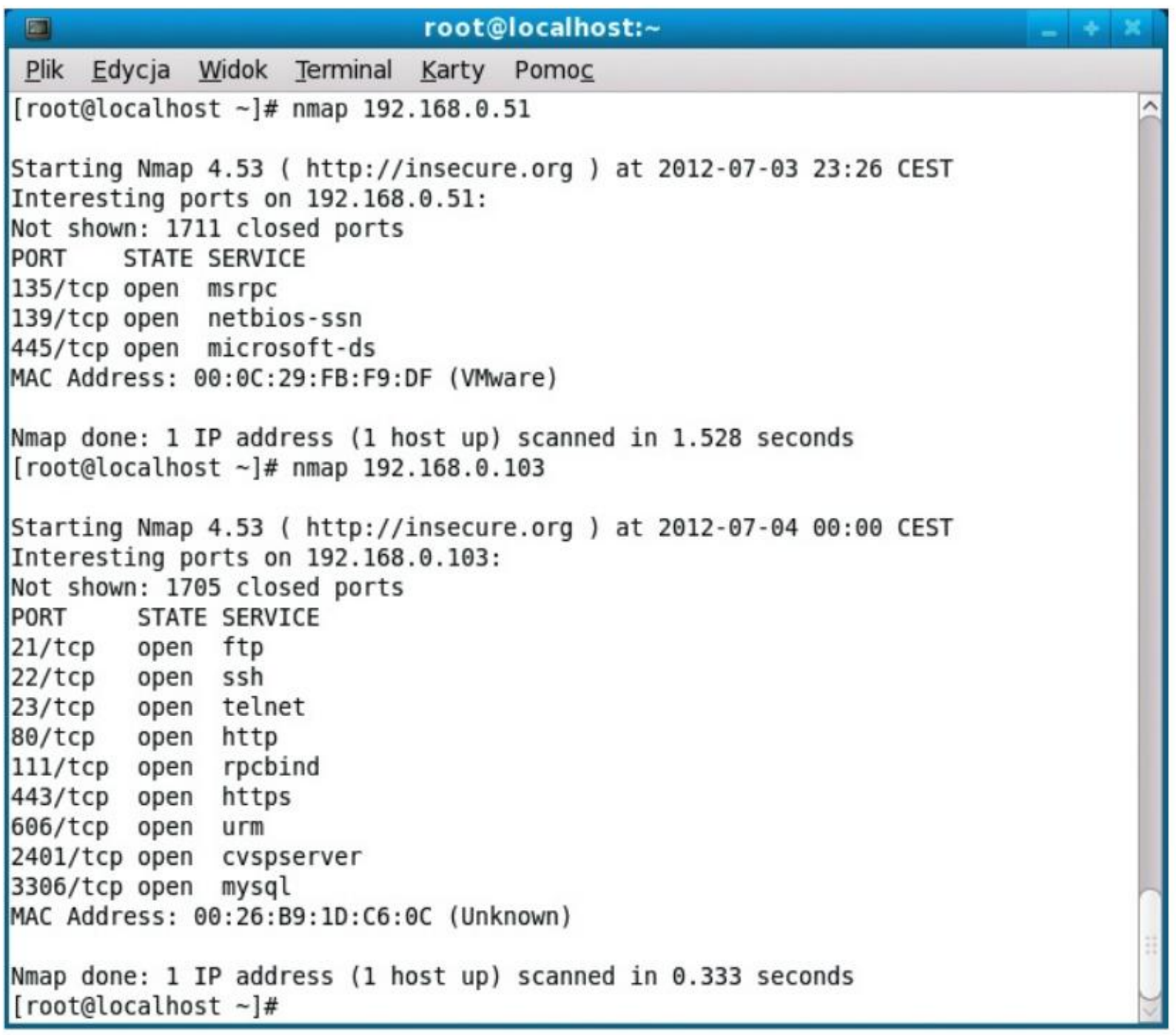


Rys. 63.1. **Okno główne programu Angry IP Scanner**

2. W polu **IP Range** podać początkowy adres przeszukiwanego zakresu, w polu **to** podać końcowy adres zakresu.
3. Kliknąć przycisk **Start**.
4. Po pewnym czasie (zależnym od wielkości przeszukiwanego zakresu) w oknie pojawi się lista adresów z przeszukiwanego zakresu. Adresy wykorzystywane w sieci zaznaczono ciemniejszym kolorem, dodatkowo – jeżeli jest to możliwe – jest wyświetlana nazwa komputera.

Jednym z najpopularniejszych programów, uważanych też za najlepsze narzędzie do skanowania w sieciach opartych na stosie TCP/IP, okazuje się program **Nmap** (ang. *Network Mapper*). Jest to darmowe i działające na licencji open-source narzędzie do eksploracji sieci i audytów bezpieczeństwa. Nmap zaprojektowano do szybkiego skanowania dużych sieci, ale ten program sprawdza się również dla pojedynczych adresów. Nmap działa na większości systemów operacyjnych Linux, Windows i MacOS X. Pakiet Nmap w wersji dla systemu Windows wyposażono nie tylko w klasyczny wiersz poleceń, lecz także w interfejs graficzny **Zenmap**. Wynikiem działania Nmap jest lista przeskanowanych adresów z dodatkowymi informacjami, np. lista interesujących portów. Zawiera ona numery portów wraz z protokołami, nazwami usługi i wykrytym stanem (np. otwarty, filtrowany, zamknięty lub niefiltrowany). Oprócz listy interesujących portów, Nmap może dostarczyć dodatkowych informacji na temat badanych adresów, takich jak prawdopodobne systemy operacyjne, typy urządzeń i adresy sprzętowe MAC.

Na rys. 63.2 przedstawiono wynik skanowania portów komputera z zainstalowanym systemem Windows (komputer o adresie 192.168.0.51) i serwera z zainstalowanym systemem Linux (adres 192.168.0.103).

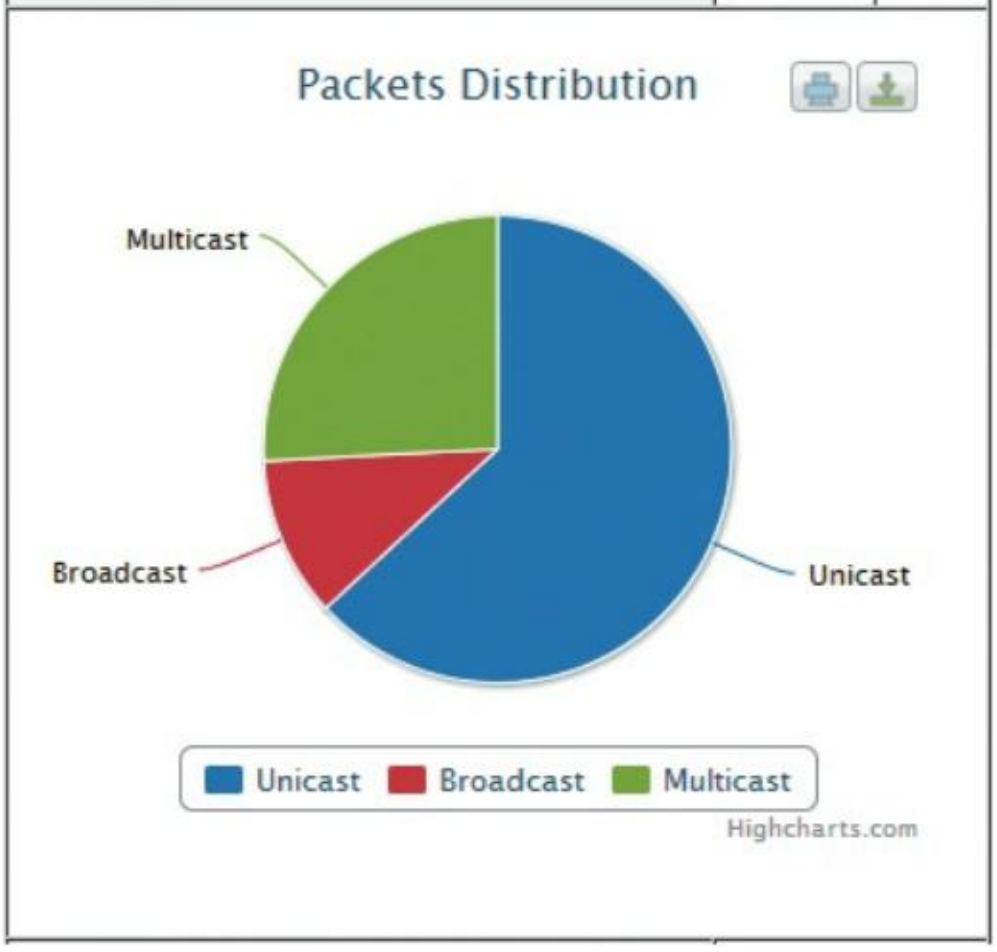


Rys. 63.2. Wynik skanowania komputera programem Nmap

Do zbierania informacji statystycznych dotyczących natężenia ruchu sieciowego w czasie rzeczywistym można wykorzystać program typu **analizator sieci**, np. program **Ntop**. Zaletą tego narzędzia jest możliwość użycia przeglądarki internetowej do zarządzania i nawigowania informacjami o ruchu w sieci. Ntop pozwala na posortowanie ruchu sieciowego, np. według protokołów. Można również dzięki niemu podejrzeć rozkład ruchu IP w różnych protokołach i zidentyfikować adresy e-mailowe użytkowników komputerów. Przykłady analizy ruchu w sieci wykonane za pomocą programu Ntop przedstawiono na rysunkach od 63.3 do 63.6. Na rys. 63.3 pokazano analizę ruchu zależnie od typu transmisji. W analizowanym ruchu dominuje komunikacja typu unicast.

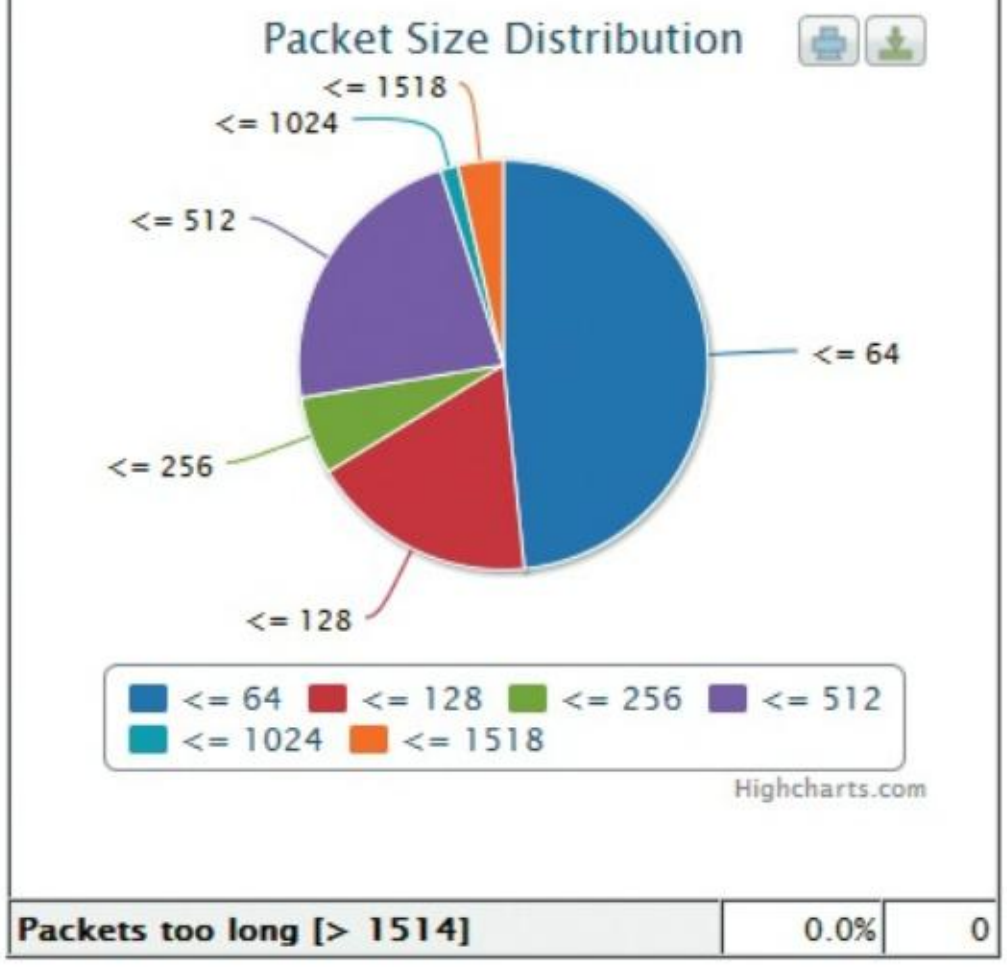
Na rys. 63.4 przedstawiono analizę ruchu zależnie od wielkości transmitowanych pakietów. W analizowanym ruchu 80 % pakietów ma rozmiar mniejszy niż 64 bajty – duża liczba małych pakietów nie jest dobra ze względu na wydajność sieci.

Dropped (libpcap)	0.0%	0
Dropped (ntop)	0.0%	0
Total Received (ntop)		1,503
Total Packets Processed		905
Unicast	62.9%	569
Broadcast	11.2%	101
Multicast	26.0%	235



Rys. 63.3. **Analiza ruchu zależnie od typu transmisji**

Shortest		42 bytes
Average Size		287 bytes
Longest		1,484 bytes
Size <= 64 bytes	80.0%	724
64 < Size <= 128 bytes	31.4%	284
128 < Size <= 256 bytes	10.4%	94
256 < Size <= 512 bytes	35.2%	319
512 < Size <= 1024 bytes	2.5%	23
1024 < Size <= 1518 bytes	6.5%	59
Size > 1518 bytes	0.0%	0

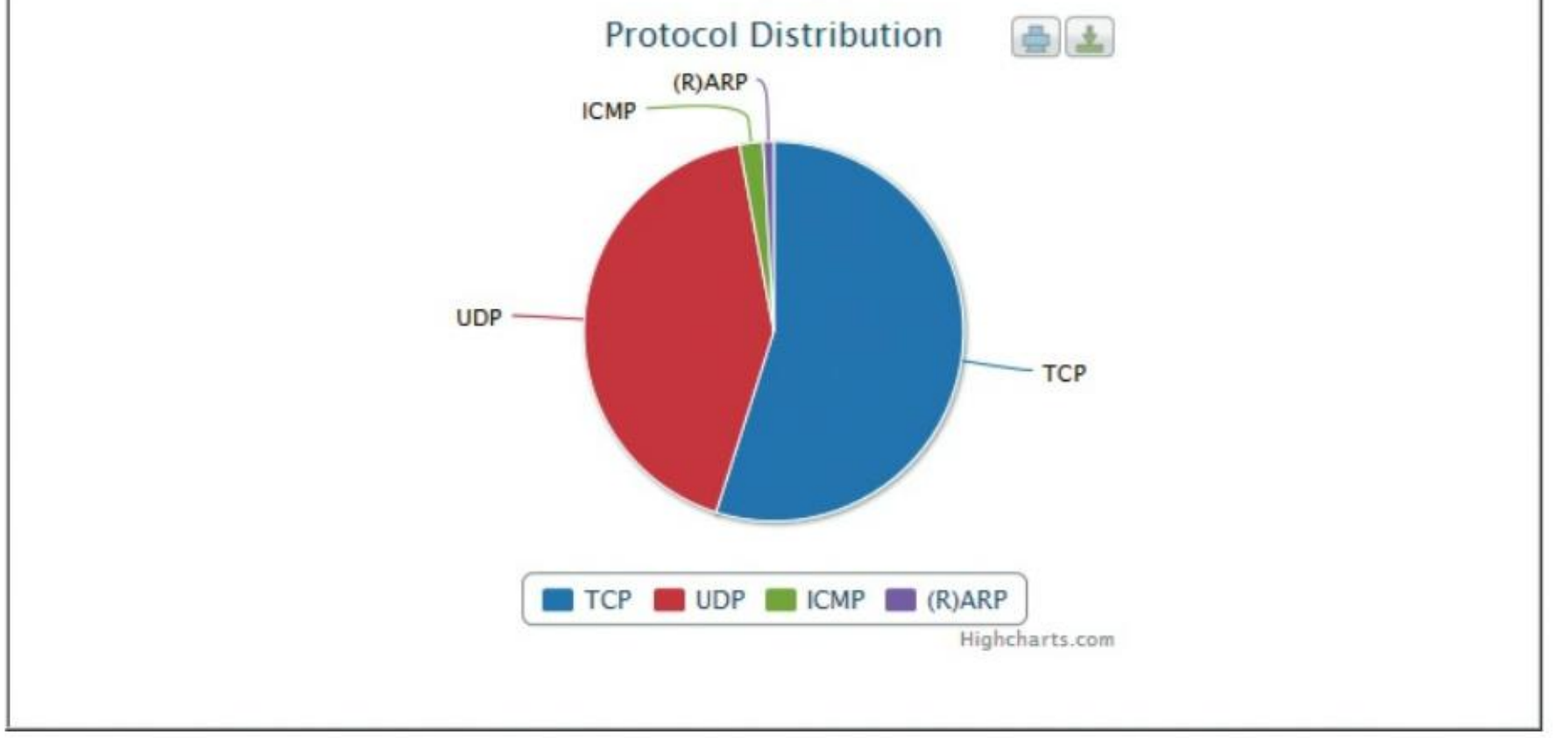


Packets too long [> 1514]	0.0%	0

Rys. 63.4. **Analiza ruchu zależnie od wielkości pakietu**

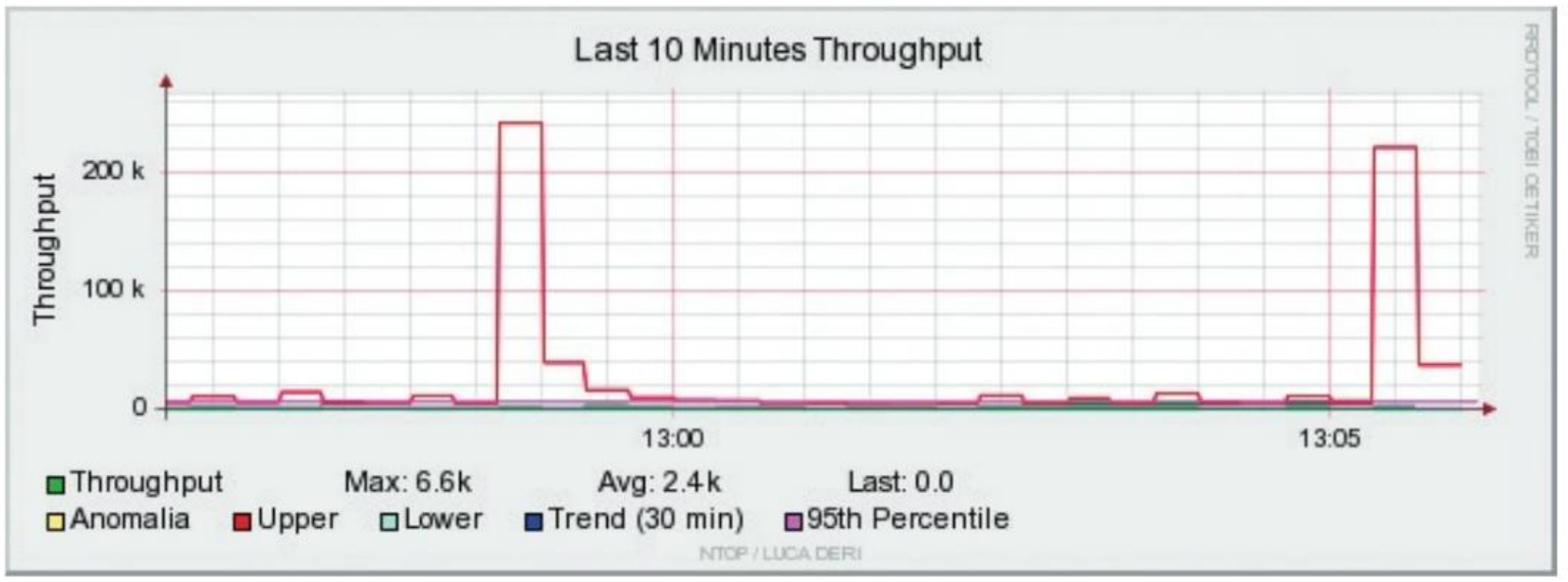
Na rys. 63.5 przedstawiono analizę ruchu zależnie od typu protokołu. W analizowanej sieci najczęściej jest wykorzystywany protokół TCP, ale udział procentowy protokołu UDP jest zbyt duży, co może oznaczać, że ktoś w sieci korzysta z usługi VoIP.

L2/L3 Protocol	Data	Percentage				
IP	314.5 KBytes	98.9%	TCP	174.2 KBytes	55.4%	
			UDP	133.8 KBytes	42.5%	
			ICMP	6.5 KBytes	2.1%	
(R)ARP	2.7 KBytes	0.9%				



Rys. 63.5. **Analiza ruchu w zależności od typu transmisji**

Na poniższym wykresie (rys. 63.6) przedstawiono wykorzystanie łącza sieciowego.



Rys. 63.6. **Analiza wykorzystania łącza sieciowego**

W systemie Windows standardowo są zaimplementowane narzędzia umożliwiające monitorowanie komputera i sieci. Do wyświetlenia statystyki interfejsu można użyć polecenia **`netstat`**. Polecenie z opcją **`-e`** wyświetla (rys. 63.7) liczbę pakietów wysłanych (ang. *Received*) i odebranych (ang. *Sent*).

Polecenie **`netstat -n`** pozwala na wyświetlenie informacji o aktywnych połączeniach komputera (rys. 63.8). Polecenie **`nbtstat`** wyświetla statystykę protokołu NetBIOS, tabele nazw NetBIOS (zarówno dla komputera lokalnego, jak i komputerów zdalnych) i pamięć podręczną nazw NetBIOS. Tabela nazw NetBIOS jest listą nazw NetBIOS odpowiadających aplikacjom NetBIOS uruchomionym na danym komputerze (rys. 63.9).

```
Wiersz polecenia
Microsoft Windows [Version 10.0.17134.471]
(c) 2018 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\kp>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    3372369392       359145409
Unicast packets             3179722         2176643
Non-unicast packets          242200           71841
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

C:\Users\kp>
```

Rys. 63.7. **Wyświetlenie statystyki interfejsu**

```
Wiersz polecenia
C:\Users\kp>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1026         127.0.0.1:16396        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16397        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16398        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16399        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16400        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16401        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16402        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16403        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16404        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16406        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16407        TIME_WAIT
  TCP    127.0.0.1:1026         127.0.0.1:16408        TIME_WAIT
```

Rys. 63.8. **Wyświetlenie listy aktywnych połączeń**

```
Wiersz polecenia
C:\Users\kp>nbtstat -n

Ethernet 5:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

VirtualBox Host-Only Network:
Node IpAddress: [192.168.56.1] Scope Id: []

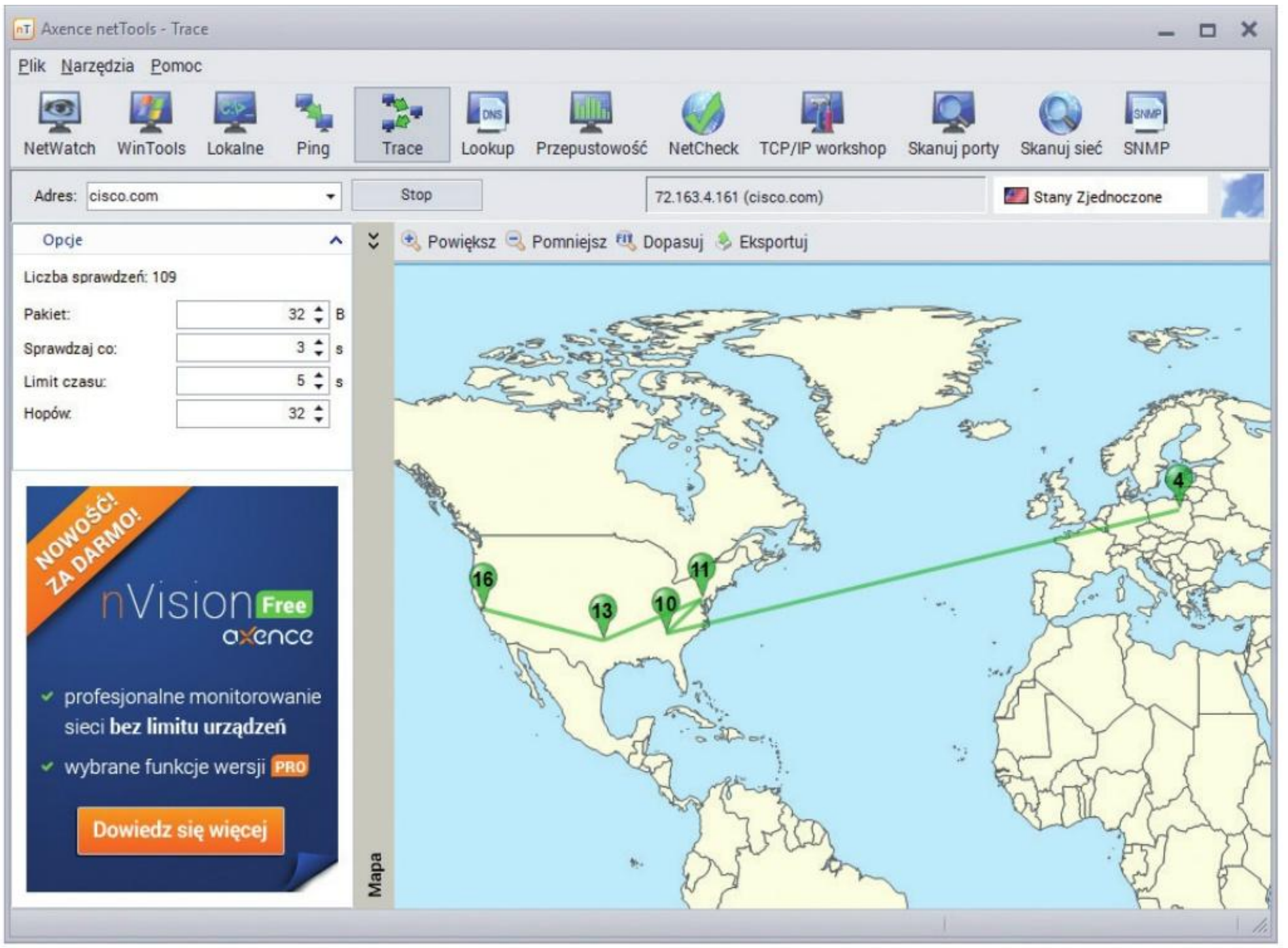
                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    DESKTOP-60DATQ7<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    DESKTOP-60DATQ7<20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered

Ethernet 3:
Node IpAddress: [0.0.0.0] Scope Id: []
```

Rys. 63.9. **Wyświetlenie statystyki protokołu NetBIOS**

NetTools to zestaw narzędzi firmy Axence, umożliwiający monitorowanie i diagnozowanie sieci komputerowych. Program jest bezpłatny, ale wymaga rejestracji na stronie producenta. Można go pobrać ze strony http://axence.net/pl/axencenettools. W programie jest dostępnych wiele narzędzi do testowania sieci, np. ping, trace, lookup, przepustowość, netcheck, skaner portów, skaner sieci, przeglądarka obiektów OID protokołu SNMP. Działanie przykładowego narzędzia Trace przedstawiono na rys. 63.10.



Rys. 63.10. **Narzędzie Trace z pakietu NetTools**

63.1. Monitorowanie danych przesyłanych przez przełącznik sieciowy

Przełącznik sieciowy, po otrzymaniu ramki na dowolnym porcie, analizuje nagłówek ramki i zawarty w nim adres MAC miejsca docelowego. Następnie porównuje ten adres z tablicą adresów MAC przechowywaną w pamięci i na tej podstawie decyduje, do którego portu wysłać ramkę. Unika w ten sposób wysyłania zbędnych ramek do urządzeń, które ich nie potrzebują.

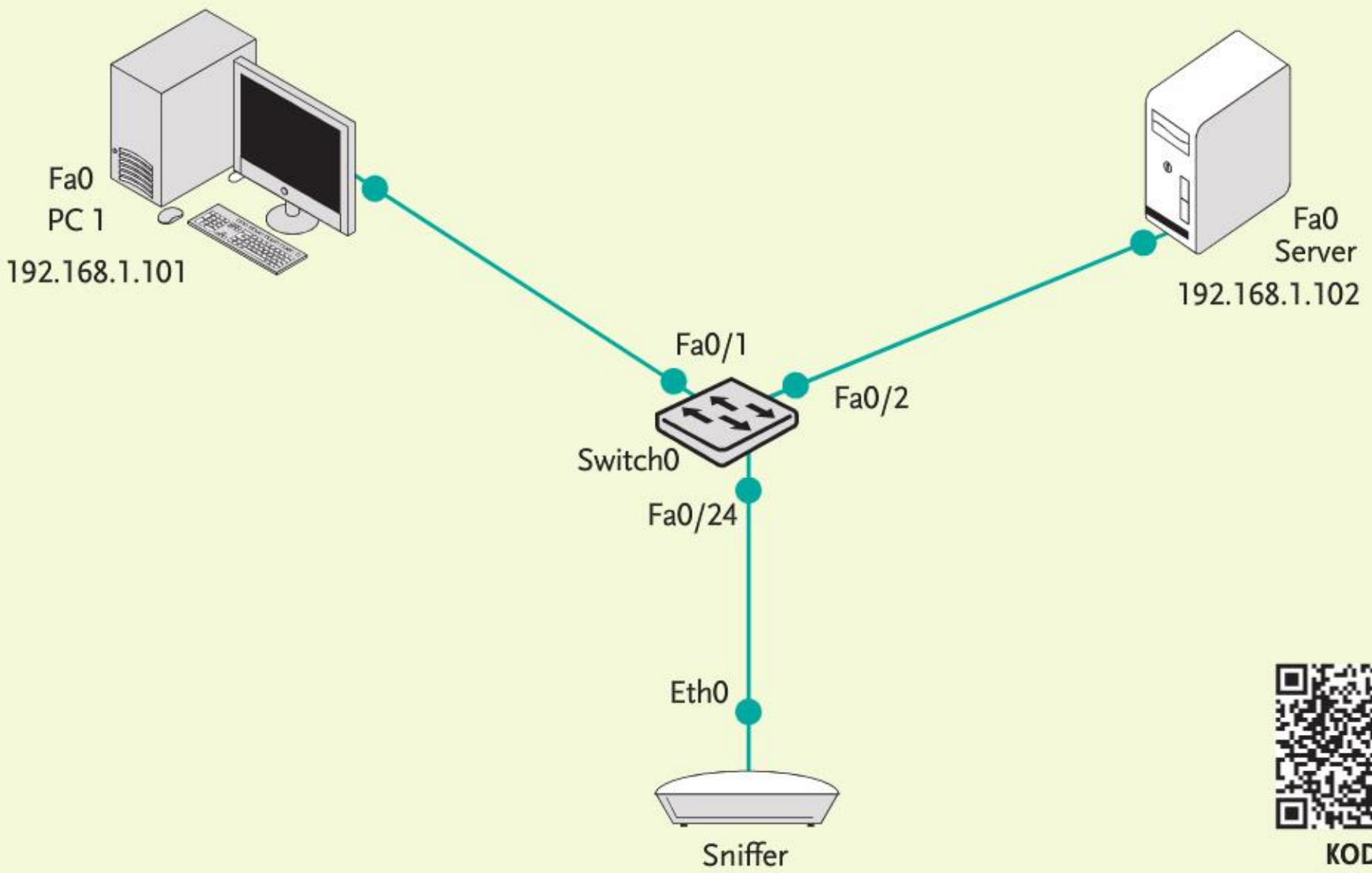
Zdarzają się jednak sytuacje, w których administrator chciałby monitorować cały ruch w sieci (również ten skierowany do innych urządzeń). Wtedy może na przełączniku skonfigurować usługę **monitorowania ruchu sieciowego** (ang. *port mirroring*). Monitorowanie może dotyczyć wybranych portów przełącznika lub wybranych sieci wirtualnych. W przełączniku można skonfigurować port, do którego będą dodatkowo wysyłane wszystkie ramki danych wpływające do monitorowanego portu lub do monitorowanej sieci wirtualnej. Podczas monitorowania dane mogą być zbierane i analizowane za pomocą programowych lub sprzętowych snifferów lub innych programów służących do analizy danych.

PRZYKŁAD 63.2

Monitorowanie portów przełącznika

W tym przykładzie zostanie skonfigurowane monitorowanie wybranych portów przełącznika CISCO. Wszystkie ramki przesyłane na wskazane porty przełącznika będą również przesyłane do wybranego (w tym przykładzie – do 24) portu przełącznika. Ramki zostaną przechwycone przez sprzętowy sniffer przyłączony do portu 24.
Aby skonfigurować monitorowanie portu, należy:

1. Uruchomić Cisco Packet Tracer, wybrać odpowiednie urządzenia i połączyć je według schematu przedstawionego na rys. 63.11.



Rys. 63.11. **Schemat sieci do monitorowania portów**

2. Skonfigurować adres IP komputera: **`192.168.1.101`**, maska podsieci **`255.255.255.0`**, adres bramy **`192.168.1.1`**.
3. Skonfigurować adres IP serwera: **`192.168.1.102`**, maska podsieci **`255.255.255.0`**, adres bramy **`192.168.1.1`**.
4. Nawiązać połączenie z przełącznikiem.
5. Wybrać tryb konfiguracji globalnej za pomocą poleceń:
   ```
   enable
   configure terminal
   ```
6. Wyłączyć sesję monitorowania (jeśli wcześniej była włączona) za pomocą polecenia:
   ```
   no monitor session 1
   ```
7. Skonfigurować port monitorowany dla obu kierunków ruchu (ang. *both*) za pomocą polecenia:
   ```
   monitor session 1 source interface fastEthernet 0/1 both
   ```
8. Skonfigurować port monitorujący za pomocą polecenia:
   ```
   monitor session 1 destination interface fastEthernet 0/24
   ```

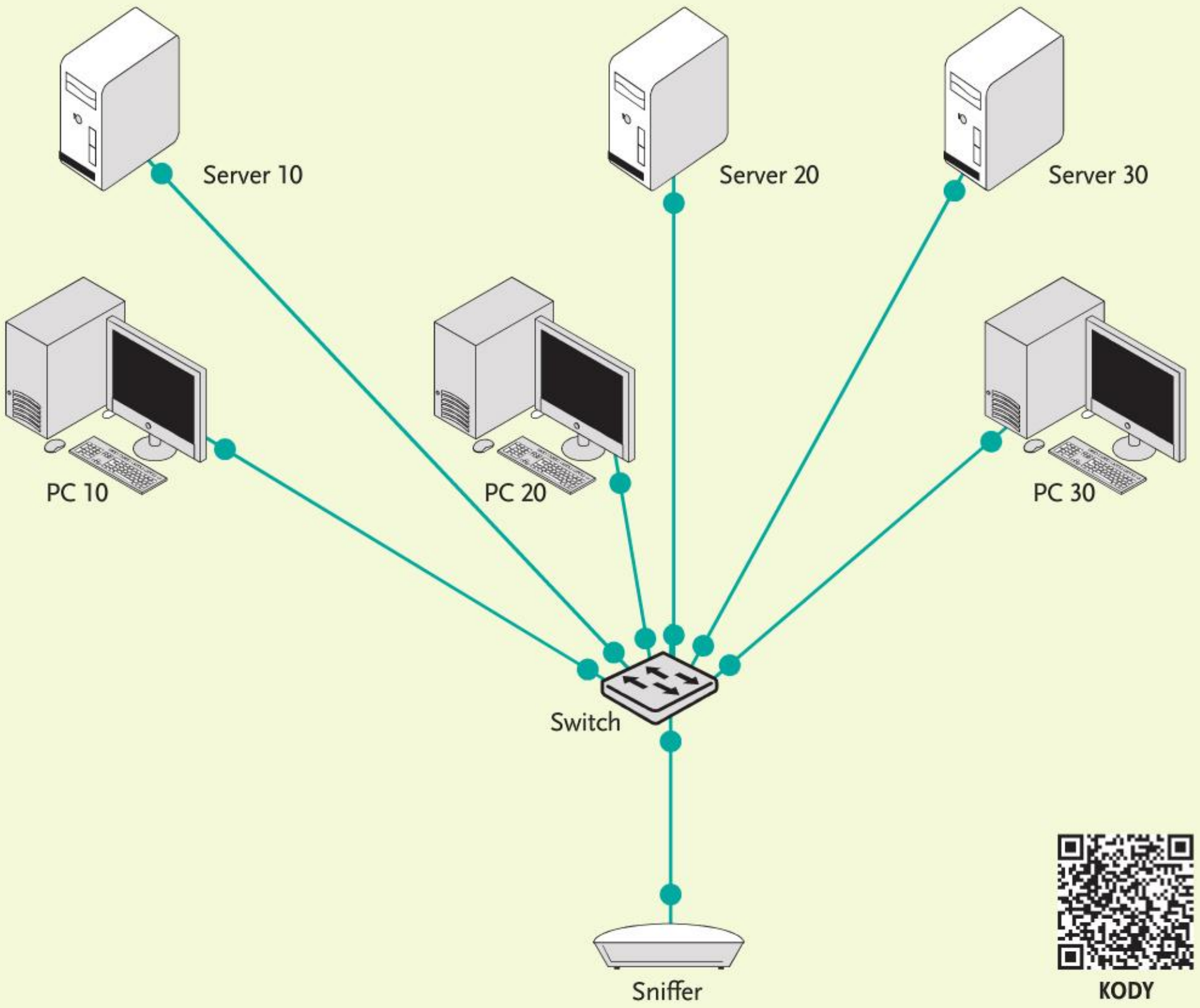
9. Zakończyć konfigurację:
   `end`
10. Sprawdzić poprawność konfiguracji za pomocą polecenia:
    `show monitor`
11. Z komputera wysłać pakiety testowe (ping) do serwera i sprawdzić, czy są one odbierane przez sniffer.

PRZYKŁAD 63.3

Monitorowanie sieci wirtualnych

W tym przykładzie zostanie skonfigurowane monitorowanie sieci wirtualnej na przełączniku CISCO. Wszystkie ramki przesyłane w monitorowanej sieci wirtualnej będą również przesyłane do wybranego (w tym przykładzie – do 24) portu przełącznika. Ramki zostaną przechwycone przez sprzętowy sniffer, przyłączony do portu 24. Aby skonfigurować monitorowanie portu, należy:

1. Uruchomić Cisco Packet Tracer, wybrać odpowiednie urządzenia i połączyć je według schematu przedstawionego na rys. 63.12. Komputery PC10 i Serwer10 pracują w sieci VLAN10 – można je przyłączyć do portów od 1 do 8. Komputery PC20 i Serwer20 pracują w sieci VLAN20 – można je przyłączyć do portów od 9 do 16. Komputery PC30 i Serwer30 pracują w sieci VLAN30 – można je przyłączyć do portów od 17 do 23. Do portu 24 należy przyłączyć sprzętowy sniffer (rys. 63.12).
2. Skonfigurować adresy IP komputerów i serwerów, np.:
   PC10: **`192.168.10.101`**, maska podsieci **`255.255.255.0`**, adres bramy **`192.168.10.1`**;
   Serwer10: **`192.168.10.102`**, maska podsieci **`255.255.255.0`**, adres bramy **`192.168.10.1`**;
   PC20: **`192.168.20.101`**, maska podsieci **`255.255.255.0`**, adres bramy **`192.168.20.1`**;
   Serwer20: **`192.168.20.102`**, maska podsieci **`255.255.255.0`**, adres bramy **`192.168.20.1`**;
   PC10: **`192.168.30.101`**, maska podsieci **`255.255.255.0`**, adres bramy **`192.168.30.1`**;
   Serwer30: **`192.168.30.102`**, maska podsieci **`255.255.255.0`**, adres bramy **`192.168.30.1`**.
3. Nawiązać połączenie z przełącznikiem.
4. Wybrać tryb konfiguracji globalnej za pomocą poleceń:
   ```
   enable
   configure terminal
   ```
5. Utworzyć trzy sieci VLAN, np. VLAN 10 – uczniowie, VLAN 20 – nauczyciele, VLAN 30 – goscie, za pomocą poleceń:
   ```
   vlan 10
   name uczniowie
   exit
   vlan 20
   name nauczyciele
   exit
   ```



KODY

Rys. 63.12. **Schemat sieci do monitorowania sieci wirtualnych**

```
vlan 30
name goscie
exit
```

6. Przypisać porty do sieci VLAN za pomocą poleceń:

```
interface range fastEthernet 0/1 - 8
switchport mode access
switchport access vlan 10
exit
interface range fastEthernet 0/9 - 16
switchport mode access
switchport access vlan 20
exit
interface range fastEthernet 0/17 - 23
switchport mode access
switchport access vlan 30
exit
```

7. Wyłączyć sesję monitorowania (jeśli wcześniej była włączona) za pomocą polecenia:
   `no monitor session 2`
8. Wybrać sieci VLAN do monitorowania za pomocą poleceń:
   `monitor session 2 source vlan 10`
   `monitor session 2 source vlan 20`
9. Skonfigurować port monitorujący za pomocą polecenia:
   `monitor session 2 destination interface fastethernet 0/24`
10. Zakończyć konfigurację:
    `end`
11. Sprawdzić poprawność konfiguracji za pomocą polecenia:
    `show monitor`
12. Z komputerów wysłać pakiety testowe (ping) do serwerów i sprawdzić, czy są one odbierane przez sniffer.

PRZYKŁAD 63.4

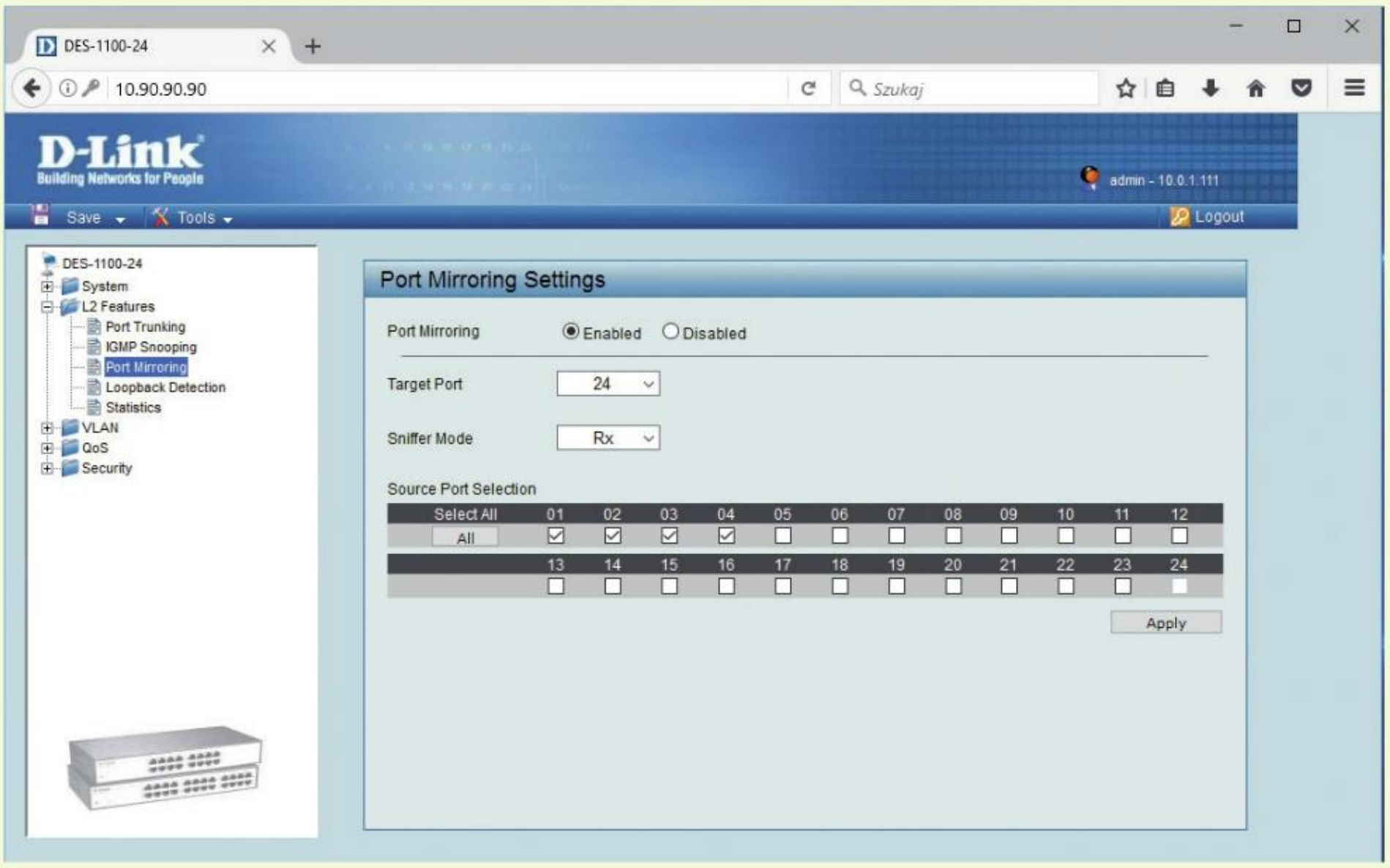
Monitorowanie portów przełącznika w interfejsie graficznym

W tym przykładzie zostanie skonfigurowane monitorowanie wybranych portów przełącznika D-Link. Wszystkie ramki przesyłane na wskazane porty przełącznika będą również przesyłane do wybranego (w tym przykładzie – do portu 24) portu przełącznika. Konfiguracja zostanie przeprowadzona w środowisku graficznym za pomocą przeglądarki WWW.

Aby skonfigurować monitorowanie portu w środowisku graficznym, należy:

1. Połączyć kablem sieciowym komputer z dowolnym portem przełącznika i zalogować się na konto administratora. W przypadku przełączników D-Link zwykle są to adres **`10.90.90.90`** z maską **`255.255.255.0`** i hasło **`admin`**.
2. W lewym panelu rozwinąć gałąź **`L2 Features/Port Mirroring`**.
3. Włączyć monitorowanie portów – ustawić **`Port Mirroring Enabled`**.
4. Wybrać port docelowy, np. **`Target Port 24`**.
5. W sekcji **`Source Port Selection`** wskazać monitorowane porty i kliknąć **`Apply`**.
6. Sprawdzić, czy ramki wysyłane na monitorowany port są przesyłane również na port 24.

Ekran konfiguracji ustawień monitorowania portu przełącznika przedstawiono na rys. 63.13.



Rys. 63.13. **Ekran konfiguracji ustawień monitorowania portu przełącznika**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zainstaluj program Nmap. Wykonaj skanowanie portów komputera z zainstalowanymi systemami Windows i Linux. Ile portów jest otwartych na każdym z komputerów?
2. Zainstaluj na komputerze lub serwerze program Ntop. Zbierz dane i odpowiedz na pytania:
   - Ile procent transmisji wykorzystuje protokół TCP?
   - Ile procent ruchu w sieci używa transmisji w trybie broadcast?
   - Jaka była maksymalna prędkość pobierania danych (dane z ostatnich 10 minut)?

64 Rodzaje awarii sieciowych i ich przyczyny

ZAGADNIENIA

Najczęstsze przyczyny awarii w sieci komputerowej **Przyczyny awarii** **Punkt demarkacyjny i jego znaczenie**

Sieć informatyczna jest narażona na wystąpienie różnego rodzaju awarii. Prawidłowe funkcjonowanie sieci jest ponadto uzależnione od sprawnego działania innych systemów, takich jak sieć energetyczna, systemy klimatyzacji i wentylacji, systemy alarmowe i kontroli dostępu. Ze względu na stopień skomplikowania można przyjąć, że wcześniej bądź później nastąpi awaria. Należy więc odpowiednio się przygotować, tak aby usuwanie awarii i jej skutków okazało się jak najkrótsze, a straty spowodowane awarią – jak najmniejsze.

Zakres awarii i jej następstw zależy od typu i miejsca jej wystąpienia oraz od przyczyn, które ją spowodowały. Najogólniej przyczyny można podzielić na **wewnętrzne** (spowodowane w samej sieci) i **zewnętrzne** (spowodowane czynnikami niezależnymi od sieci, np. awaria zasilania). Z punktu widzenia administratora istotne jest precyzyjne zdefiniowanie położenia tzw. **punktu demarkacyjnego**, czyli punktu oddzielającego sieć lokalną od sieci globalnej (internetu). Jeżeli awaria wystąpi w sieci lokalnej (np. awaria przełącznika), to za jej usunięcie odpowiada administrator sieci lokalnej. Jeżeli natomiast awaria wystąpi za punktem demarkacyjnym, np. uszkodzenie w centrali telekomunikacyjnej, to za jej usunięcie odpowiada dostawca usług internetowych. Po zlokalizowaniu miejsca awarii administrator powinien podjąć decyzję, kto odpowiada za jej usunięcie, i w razie potrzeby skontaktować się z dostawcą internetu.

Zależnie od miejsca wystąpienia awarii można wyróżnić awarie:

- systemu okablowania;
- urządzeń aktywnych;
- systemu zasilania;
- systemu chłodzenia i wentylacji;
- innych systemów współpracujących z siecią.

Awaria systemu okablowania sieci lokalnej może wystąpić w różnych miejscach. Niezależnie od miejsca jej wystąpienia administrator powinien dysponować zapasowymi materiałami (kable, gniazda, złącza) i narzędziami umożliwiającymi usunięcie awarii. Najmniejszy problem sprawiają awarie okablowania poziomego. Wtedy zakres awarii jest ograniczony do pojedynczego punktu abonenckiego lub pewnego obszaru sieci, który łatwo zdiagnozować. Uszkodzenie kabla pionowego powoduje awarie o większym zasięgu. Do typowych awarii okablowania zalicza się również uszkodzenia kabli krosowych w szafach dystrybucyjnych, kabli stacyjnych oraz gniazd i wtyczek. Najczęstszymi przyczynami uszkodzeń okablowania są:

- niska jakość elementów pasywnych – po pewnym czasie powstaje luz między wtyczką i gniazdem;
- niewłaściwy montaż kabla w panelu krosowniczym i wtyczce;
- nadmierne zgięcie kabla;

- fizyczne uszkodzenie kabla – najczęściej dotyczy to kabli prowadzonych poza korytkami ochronnymi, np. kabli stacyjnych, które są deptane, rozjeżdżane kółkami od foteli lub wyrywane z gniazd. Częstą przyczyną uszkodzeń okablowania są prace remontowe i modernizacyjne wykonywane w kanałach kablowych lub inne prace budowlano-remontowe.

Przyczyną wystąpienia awarii mogą być również urządzenia aktywne. Można je podzielić na dwie grupy: **awarie wynikające z uszkodzenia sprzętu** i **awarie spowodowane niewłaściwą konfiguracją**. Awarie wynikające z uszkodzenia sprzętu najczęściej wymagają interwencji specjalistycznego serwisu danego producenta. Na czas naprawy sprzętu należy prowizorycznie podłączyć inne urządzenie, np. przełącznik. W przypadku urządzeń w warstwie dostępu zamiana urządzenia jest łatwa, trudniejsza sytuacja występuje podczas awarii urządzeń szkieletowych. Koszt takiego urządzenia okazuje się bardzo wysoki, a samego sprzętu nie uda się na ogół zastąpić innym. Rozwiązaniem tego problemu jest stosowanie nadmiarowości podczas projektowania sieci i preferowanie wysokiej jakości sprzętu, a także wybieranie firm, które oferują serwis z krótkim czasem reakcji na awarie.

Przyczyną niewłaściwej konfiguracji urządzeń może być brak odpowiednich mechanizmów bezpieczeństwa, które chronią urządzenia przed dostępem osób nieupoważnionych, np. modyfikacje konfiguracji routera lub przełącznika wykonywane przez pracowników, aby ominąć zabezpieczenia sieci. Niewłaściwe funkcjonowanie sieci mogą powodować również inne urządzenia obce podłączane do sieci, np. użytkownik przynosi do pracy własny laptop, na którym działa serwer DHCP. Po podłączeniu laptopa do sieci komputery mogą otrzymać niewłaściwe adresy.

Ze względu na bezpieczeństwo użytkownicy nie mają prawa podłączać do sieci żadnego sprzętu. Przykładowo: access point wpięty do sieci zamiast komputera może ułatwić pracownikom przyłączenie urządzeń bezprzewodowych, ale jeżeli nie jest on poprawnie skonfigurowany, może stanowić lukę w systemie bezpieczeństwa, przez którą włamywacz uzyska dostęp do zasobów sieci.

Przyczynami awarii mogą również okazać się błędy w oprogramowaniu lub nieprawidłowa konfiguracja serwerów, powodujące spadek wydajności lub całkowite wyłączenie usług bądź serwisów. Bardzo ważne okazuje się także instalowanie aktualizacji oprogramowania usuwającego wykryte błędy i luki w systemie bezpieczeństwa oraz wprowadzającego nowsze rozwiązania dotyczące bezpieczeństwa.

Awaria systemu zasilania uniemożliwia działanie urządzeń aktywnych sieci. Zanik lub pogorszenie jakości zasilania z sieci energetycznej mogą być chwilowe lub długotrwałe. Zazwyczaj chwilowe zaniki są spowodowane awarią sieci energetycznej w budynku, np. przeciążeniem sieci i zadziałaniem bezpieczników.

Podczas wykonywania różnego rodzaju prac konserwatorskich i modernizacyjnych sieci energetycznej może dochodzić do zamierzonego lub niezamierzonego tymczasowego wyłączenia obwodu. Przyczyną długotrwałych awarii jest najczęściej uszkodzenie trakcji energetycznej po stronie dostawcy energii. Zwykle ma to związek ze zdarzeniami losowymi, np. powodzią, burzą, uszkodzeniem trakcji spowodowanym upadającymi drzewami.

Obronę przed krótkotrwałymi awariami sieci stanowią urządzenia UPS, których zadaniem jest podtrzymanie napięcia do momentu włączenia agregatów prądotwórczych. W razie dłuższych awarii agregaty prądotwórcze są uruchamiane automatycznie. Proces uruchomienia i ustabilizowania agregatu zajmuje trochę czasu, dlatego nie powinno się ich uruchamiać w razie krótkotrwałych awarii. Usunięciem awarii sieci energetycznej może zajmować się tylko wykwalifikowany pracownik mający odpowiednie uprawnienia. W firmach i instytucjach szczególnie wrażliwych na awarie instalacji elektrycznych wskazane staje się pełnienie ciągłego dyżuru przez takiego pracownika lub zawarcie umowy z firmą zewnętrzną świadczącą usługi tego typu.

Urządzenia aktywne podczas eksploatacji wydzielają ciepło, które musi być odprowadzone na zewnątrz za pośrednictwem systemu wentylacji lub klimatyzacji. Rola systemu klimatyzacji polega na zapewnieniu stabilnych warunków pracy (temperatury, wilgotności), do których są przystosowane urządzenia aktywne. Awaria tego systemu będzie odczuwalna dopiero po pewnym czasie i może spowodować wzrost temperatury w pomieszczeniach, a w konsekwencji – przegrzanie się urządzeń i ich awarię.

Większość urządzeń sieciowych aktywnych jest wyposażona we własne systemy wentylacji. Wentylatory w nich wykorzystywane są urządzeniami mechanicznymi i jako takie stanowią najczęstsze źródło awarii. W niektórych urządzeniach zamontowano nadmiarowe wentylatory, pracujące w trybie „hot-swap", z możliwością wymiany bez wyłączania urządzenia. Podczas planowania rozmieszczenia urządzeń aktywnych należy pamiętać, że brak swobodnego przepływu powietrza wokół urządzeń może również być przyczyną ich przegrzania.

Na funkcjonowanie sieci wpływają także inne systemy, takie jak system kontroli dostępu do pomieszczeń i monitoringu, np. do serwerowni. Jego awaria może całkowicie zablokować dostęp do urządzeń. Awaria systemu przeciwpożarowego może częściowo lub całkowicie pozbawić urządzenia ochrony i narazić je na zniszczenie.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Opracuj przykładową procedurę postępowania na wypadek awarii, np. przerwy w dostawie energii elektrycznej do twojej szkoły lub uszkodzenia kabla w instalacji pionowej.

65 Procedury serwisowe dotyczące urządzeń sieciowych

ZAGADNIENIA

Procedury serwisowe do samodzielnego wykonania **Wykonanie aktualizacji oprogramowania systemowego urządzenia** **Wyczyszczenie hasła na routerze CISCO**

Jeżeli urządzenie funkcjonuje niezgodnie z oczekiwaniami użytkownika lub działa nieprawidłowo, należy przeprowadzić tzw. **procedury serwisowe**. Powinny one być wykonywane ściśle według zaleceń producenta danego urządzenia. Te procedury pozwalają użytkownikowi na zebranie informacji, np. przez uruchomienie programu diagnostycznego na urządzeniu i ocenę, czy działa ono prawidłowo, a jeśli – nie, to jakie są tego przyczyny i objawy. Niektóre usterki można usunąć samodzielnie, w przypadku innych niezbędna staje się interwencja wykwalifikowanego serwisu producenta. Procedura szczegółowo określa sposób komunikowania się z serwisem, dostarczenia urządzenia do serwisu oraz wymagane dokumenty i sposób opisu usterki.

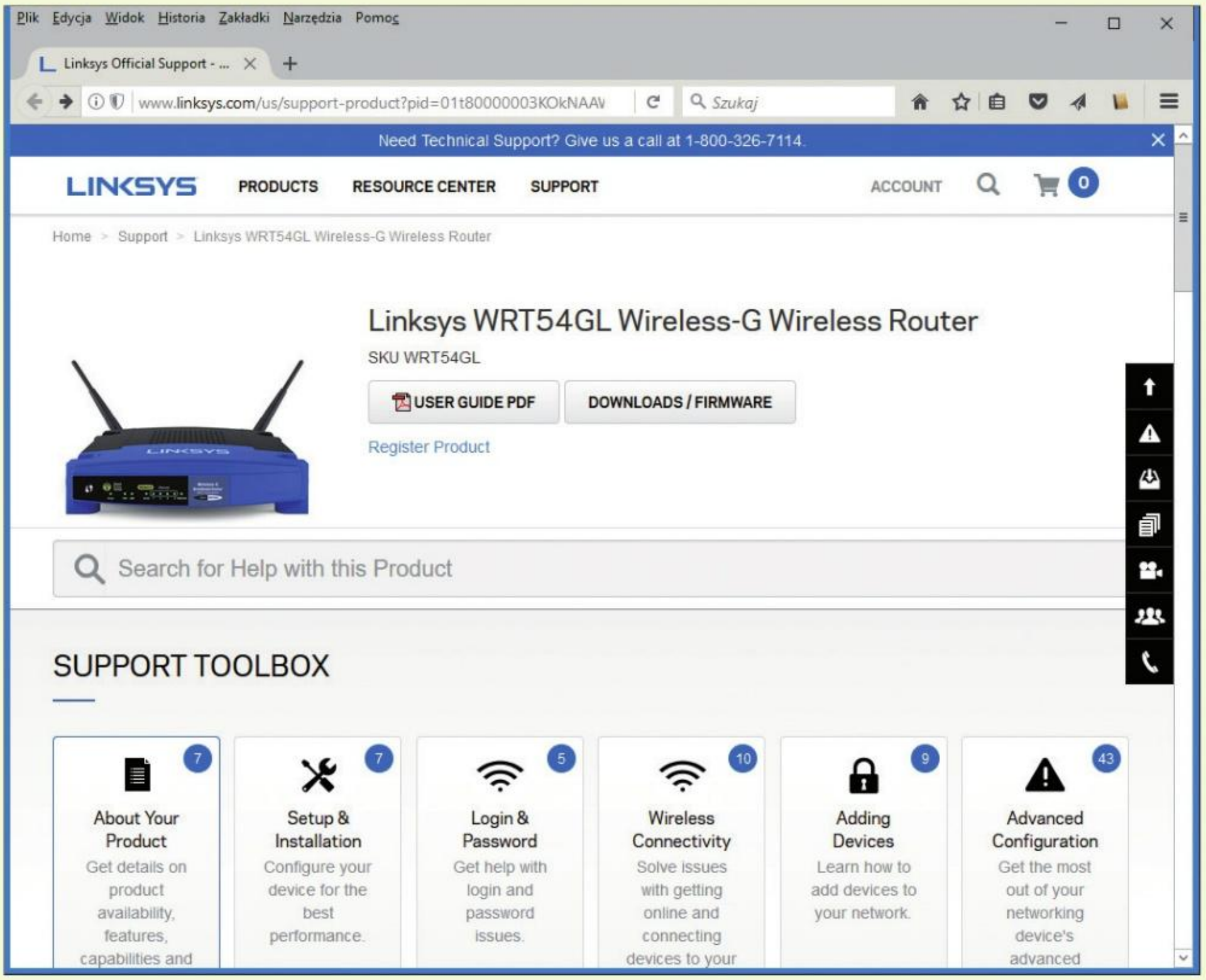
Nie wszystkie usterki sprzętu wymagają interwencji serwisu producenta. W niektórych sytuacjach można samodzielnie usunąć usterkę lub przywrócić sprzęt do stanu fabrycznego. Najczęściej stosowaną procedurą wykonywaną przez użytkownika jest **aktualizacja oprogramowania systemowego urządzenia** (ang. *firmware*). Procedura powinna być wykonana starannie, ponieważ jej niewłaściwa realizacja może doprowadzić do poważniejszej awarii lub do utraty gwarancji.

PRZYKŁAD 65.1

Aktualizacja oprogramowania systemowego routera

W tym ćwiczeniu zostanie pokazana realizacja procedury aktualizacji oprogramowania systemowego na przykładzie routera WRT54GL. Aby przeprowadzić aktualizację, należy wykonać następujące czynności:

1. Pobrać ze strony producenta wersję oprogramowania odpowiednią dla danego urządzenia. Z myślą o produktach firmy Linksys można skorzystać ze strony http://www.linksys.com/us/support-product?pid=01t80000003KOkNAAW. Na stronie należy się upewnić, że jest pobierane właściwe oprogramowanie dla urządzenia, i za pomocą przycisku **`DOWNLOAD/FIRMWARE`** pobrać oprogramowanie (rys. 65.1).
2. Połączyć komputer z routerem za pomocą kabla sieciowego i zalogować się do panelu administracyjnego routera. Router Linksys WRT54GL standardowo ma przypisany adres: **`192.168.1.1`**, maskę podsieci: **`255.255.255.0`**, konto administratora: admin i hasło: admin.
3. Wybrać zakładkę **`Administration`**, a w niej zakładkę **`Firmware Upgrade`** (rys. 65.2).



Rys. 65.1. **Pobieranie oprogramowania systemowego ze strony producenta**



Rys. 65.2. **Wybór okna aktualizacji oprogramowania systemowego**

4. Kliknąć przycisk **Przeglądaj** i w oknie wyboru wskazać pobrany wcześniej plik zawierający oprogramowania systemowe.
5. Kliknąć przycisk **Upgrade** i poczekać na zakończenie kopiowania pliku.Po zakończeniu kopiowania należy kliknąć przycisk **Continue** i ponownie uruchomić router.
6. Jeżeli wszystko przebiegło prawidłowo, to po restarcie routera uruchomi się już nowa wersja oprogramowania.

Czasami dochodzi do utraty hasła do panelu administracyjnego urządzenia. Jeżeli router jest prosty, wystarczy nacisnąć i przytrzymać przez czas określony w dokumentacji wciśnięty przycisk **Reset**. Oprócz hasła zostaną wyczyszczone również wszystkie parametry skonfigurowane przez użytkownika. Dla urządzeń profesjonalnych istnieje procedura pozwalająca na odzyskanie kontroli nad panelem administracyjnym bez konieczności usuwania konfiguracji. Wymaga ona jednak fizycznego dostępu do urządzenia.

PRZYKŁAD 65.2

Procedura odzyskiwania hasła z routera CISCO

Procedura odzyskiwania hasła jest podobna na wszystkich routerach CISCO. W ćwiczeniu przedstawimy ją na przykładzie CISCO 2811. Aby odzyskać hasło z routera, należy wykonać następujące czynności:

1. Połączyć komputer z portem konsolowym routera i nawiązać sesję.
2. Wyłączyć router przełącznikiem **ON/OFF**.
3. Nacisnąć na klawiaturze klawisz [Break] (podczas korzystania z aplikacji Hyper terminal lub PuTTy – [Ctrl] + [Break]), aby uruchomić router w trybie **rommon**. Tryb rommon to specjalny tryb pracy routera, umożliwiający resetowanie hasła lub instalację nowego systemu operacyjnego.
4. Wprowadzić polecenie **confreg 0x2142**. Powoduje ono pominięcie interpretacji pliku **startup-config** zawierającego konfigurację podczas uruchamiania routera. Hasło jest przechowywane w pliku **startup-config** – jeżeli plik zostanie pominięty, to router uruchomi się bez konieczności wprowadzania hasła.
5. Uruchomić ponownie router za pomocą polecenia **reset**. Początek procedury resetowania hasła routera przedstawiono na rys. 65.3.

```
Self decompressing the image :
####################################System Bootstrap, Version 12.1(3r)T2,
RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes
of memory
Self decompressing the image :
###################
monitor: command „boot" aborted due to user interrupt
rommon 1 > confreg 0x2142
rommon 2 > reset
```

Rys. 65.3. **Początek procedury resetowania hasła routera**

6. Router uruchomi się ponownie, z pominięciem interpretacji pliku **startup-config** – będzie możliwe przejście do trybu użytkownika uprzywilejowanego bez konieczności podawania hasła.

7. Pominąć dialog konfiguracyjny (opcja: **no**).
8. Wydać polecenie **enable**, aby przejść do trybu użytkownika uprzywilejowanego.
9. Wprowadzić polecenie **copy startup-config running-config**, aby skopiować plik konfiguracyjny do pamięci RAM. Spowoduje ono wczytanie zawartości pliku konfiguracyjnego i przywrócenie konfiguracji routera.
10. Wprowadzić polecenie **configure terminal**.
11. Wprowadzić polecenia **enable password <password>** i **enable secret <password>**, aby zmienić hasła nieszyfrowane i szyfrowane.
12. Wprowadzić polecenie **no shutdown** na każdym interfejsie, który ma być włączony.
13. Poleceniem **config-register 0x2102** przywrócić domyślne ustawienia (interpretowanie plików konfiguracyjnych podczas uruchamiania routera).
14. Wprowadzić polecenie end lub wybrać kombinację klawiszy [Ctrl] + z, aby przejść do trybu użytkownika uprzywilejowanego.
15. Wprowadzić polecenie **copy running-config startup-config**, aby w pliku konfiguracyjnym zapisać wszystkie zmiany. Ciąg dalszy procedury resetowania hasła routera przedstawiono na rys. 65.4.

```
         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable
Router#copy startup-config running-config
Destination filename [running-config]?

450 bytes copied in 0.416 secs (1081 bytes/sec)
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable password cisco
Router(config)#enable secret cisco
Router(config)#config-register 0x2102
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

Rys. 65.4. **Ciąg dalszy procedury resetowania hasła routera**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Odszukaj w internecie najnowsze oprogramowanie dla routera używanego w twojej szkole.
2. Zaktualizuj oprogramowanie systemowe w routerze.

66 Sposoby naprawy okablowania strukturalnego

ZAGADNIENIA

- **Usuwanie awarii w okablowaniach poziomym i pionowym**
- **Usuwanie awarii w okablowaniu światłowodowym**

Awarie występujące w okablowaniu strukturalnym powinno się szybko usuwać, aby ograniczyć skutki awarii i zminimalizować straty. Skutki awarii zależą od miejsca awarii i od typu kabla, który uległ uszkodzeniu.

Uszkodzenie w okablowaniu poziomym na ogół wpływa tylko na gniazdo, które jest bezpośrednio przyłączone tym kablem. Może wystąpić całkowite przerwanie kabla lub częściowe jego uszkodzenie. Całkowite przerwanie kabla wymaga jego ponownego ułożenia – nie wolno łączyć odcinków kabla. Do każdego punktu abonenckiego sygnał jest doprowadzony przez oddzielny kabel – najczęściej przez skrętkę.

Punkt abonencki zwykle składa się z dwóch gniazd RJ-45. Jedno z nich służy do przyłączenia komputera, a drugie – telefonu. Jeżeli zostanie uszkodzony tylko jeden kabel, to administrator – w porozumieniu z użytkownikiem – może podjąć decyzję, czy na czas potrzebny do usunięcia awarii sprawnym kablem podłączyć komputer, czy telefon. Po naprawie należy niezwłocznie przywrócić połączenia do stanu pierwotnego. Jeżeli nastąpiło częściowe uszkodzenie kabla, a jego wymiana jest trudna lub w danym momencie niemożliwa, to warto wówczas użyć kabla do podłączenia telefonu, który wykorzystuje tylko jedną parę przewodów. Jeżeli doszło do całkowitego uszkodzenia kabla, a trzeba podłączyć komputer i telefon, można skorzystać z zapasowego gniazda (o ile przewidziano je w instalacji). Tymczasowo można zastosować dodatkowy przełącznik, do podłączenia urządzeń. Jest to jednak rozwiązanie tymczasowe i należy jak najszybciej przywrócić normalne funkcjonowanie sieci.

Do budowy sieci w okablowaniu pionowym najczęściej wykorzystuje się światłowody. Uszkodzenie światłowodu może skutkować odcięciem od sieci piętra lub całego budynku. Uszkodzenie pojedynczych włókien można ominąć dzięki wykorzystaniu nadmiarowych włókien w tym samym kablu (o ile przewidziano je podczas projektowania).

W szczególnym przypadku warto spróbować połączyć włókna światłowodu za pomocą spawania lub innych technik, np. **mechanicznych złączy Fibrolok** (rys. 66.1). Złącza Fibrolok mogą być używane we wszystkich zastosowaniach złączy spawanych. Eliminują skomplikowane i kosztowne spawanie włókien. Pozwoli to na tymczasowe zapewnienie łączności do czasu ułożenia nowego kabla.

W przypadku uszkodzenia całego kabla światłowodowego komunikacja może odbywać się tylko dzięki redundancji okablowania. Jeżeli podczas projektowania sieci nie przewidziano redundancji kabli, to jedynym rozwiązaniem jest ułożenie



Rys. 66.1. **Mechaniczne złącze światłowodowe Fibrolok**

nowego kabla. Największe problemy sprawiają awarie okablowania międzybudynkowego ze względu na duże odległości i ułożenie kabla w gruncie. Do lokalizowania miejsca awarii wykorzystuje się reflektometry optyczne OTDR.

Częstymi przyczynami awarii są uszkodzone kable krosowe i stacyjne. W odróżnieniu od innych nie układa się ich w ochronnych kanałach kablowych i przez to są one szczególnie narażone na uszkodzenia mechaniczne. Należy je prowadzić tak, aby maksymalnie chronić przed możliwością uszkodzenia, zgniecenia lub nadmiernego zagięcia. Uszkodzone kable należy wymienić na nowe. Niedopuszczalne jest używanie kabli zakończonych wtykami z wyłamanymi zatrzaskami.

Po wykonaniu napraw instalacji trzeba przeprowadzić testy potwierdzające, że naprawione okablowanie spełnia wymogi określone normą. Wszystkie zmiany muszą być wprowadzone do dokumentacji sieci.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Znajdź w internecie ofertę firmy zlokalizowanej najbliżej twojej szkoły, a świadczącej usługę spawania światłowodów. Jaki jest koszt wykonania naprawy pojedynczego włókna?

- Współpraca Windows z serwerem sieci lokalnej
- Typy sieci komputerowych
- Korzystanie z usług sieciowych – serwis stron WWW
- Korzystanie z usług transferu plików
- Korzystanie z poczty elektronicznej i grup dyskusyjnych
- Korzystanie z usługi telnet
- Korzystanie z usługi bezpiecznego terminala
- Korzystanie z usługi bezpiecznego kopiowania plików

Korzystanie z wybranych usług oferowanych przez sieciowe systemy operacyjne

VII

67 Współpraca systemu Windows z serwerem sieci lokalnej

ZAGADNIENIA

Zadania wykonywane przez sieciowy system operacyjny **Rola serwera w sieci komputerowej**

Sieciowy system operacyjny jest podstawowym oprogramowaniem sieci komputerowej: tworzy środowisko współpracy dla wielu urządzeń i decyduje o charakterze sieci oraz o zakresie oferowanych usług. Koordynuje też pracę sieci, zapewnia efektywne gospodarowanie zasobami i udostępnianie ich użytkownikom według określonych reguł i zasad.

Serwer – jako komputer centralny, na którym znajduje się całość oprogramowania – jest najważniejszym elementem systemu sieciowego. Ponieważ obsługuje wiele stacji roboczych, musi być komputerem o dużej mocy obliczeniowej i o dużej ilości pamięci dyskowej.

Systemy operacyjne współczesnych komputerów umożliwiają przyłączenie ich do sieci. Może to być sieć globalna, jak internet, lub sieć lokalna, np. w szkole. W latach dziewięćdziesiątych ubiegłego wieku w dziedzinie sieci komputerowych dominowała firma Novell z jej podstawowym systemem **NetWare**. Obecnie dużą popularnością cieszą się sieci oparte na systemach operacyjnych z rodziny **Windows Server** firmy Microsoft. Coraz większe grono zwolenników zdobywają różne wersje systemów **Unix** i **Linuks**.

Jednym z systemów operacyjnych pozwalających na współpracę z sieciami, niezależnie od ich producenta, typu i architektury, jest Windows, zainstalowany w różnych wersjach na większości komputerów osobistych.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skorzystaj z dostępnych źródeł (literatura, czasopisma, internet) i wyszukaj informacje o sieciowych systemach operacyjnych. Wskaż adresy w internecie, pod którymi można odszukać te systemy oraz oferowane przez nie usługi i obszar ich zastosowań.
2. Jakie wymagania musi spełniać komputer, aby można było zainstalować na nim sieciowy system operacyjny? Wyszukaj w dowolnym źródle ofertę wybranego producenta lub dystrybutora serwerów i dobierz konfigurację spełniającą wymagania systemu operacyjnego. Jaka jest cena zaproponowanego serwera?

68 Typy sieci komputerowych

ZAGADNIENIA

Cel tworzenia sieci komputerowych **Typy sieci komputerowych** **Rola i uprawnienia administratora** **Funkcja usługi katalogowej**

Sieć komputerowa to grupa komputerów, drukarek i innych urządzeń połączonych za pomocą kabla sieciowego lub innego medium transmisyjnego w celu wspólnego korzystania z zasobów. Podstawowym celem budowy sieci jest stworzenie możliwości współdzielenia zasobów w postaci danych, m.in. plików i folderów, sprzętu (np. modemu) lub usług i umożliwienie pracy grupowej. Typ sieci określa, w jaki sposób będą udostępniane współdzielone zasoby. Sieci mogą być równorzędne lub pracować w architekturze klient–serwer. W sieciach **równorzędnych** (ang. *peer -to-peer*) każdy komputer może być **klientem** (korzystać z usług oferowanych przez inne urządzenia), **serwerem** (udostępniać usługi) lub jednocześnie klientem i serwerem. Takie rozwiązanie stosuje się w małych sieciach. Każdy z użytkowników zarządza swoim komputerem i podejmuje decyzje, jakie zasoby udostępnić i komu. Informacje o udostępnionych zasobach są przechowywane na lokalnym komputerze.

W sieciach pracujących w architekturze **klient–serwer** urządzenia dzielą się na oferujące usługi (serwery) i korzystające z tych usług (klienci). Takie rozwiązanie stosuje się w większych sieciach. Taka sieć jest zarządzana przez specjalnego użytkownika – **administratora**. Wszystkie informacje o składnikach sieci, jej użytkownikach i zasobach przechowuje się na serwerze i udostępnia wszystkim użytkownikom sieci.

Zadaniem administratora jest umożliwienie korzystania z sieci użytkownikom, a w szczególności:

- administrowanie użytkownikami;
- zarządzanie systemem plików;
- realizowanie polityki kopii bezpieczeństwa i archiwizacji danych;
- prowadzenie audytu zdarzeń w systemie.

Przykładami sieci opartych na architekturze klient–serwer są sieci korzystające z usług serwerów z zainstalowanym systemem Novell NetWare lub Windows Server. W każdej z tych sieci do przechowywania informacji o obiektach, np. użytkownikach, udostępnianych zasobach, uprawnieniach, służy **usługa katalogowa**. W odniesieniu do sieci NetWare usługa ta nazywa się **eDirectory**, a we wcześniejszych wersjach – **Novell Directory Services** (NDS). Usługa katalogowa w środowisku Windows nosi nazwę **Active Directory**.

Usługi katalogowe są wyspecjalizowanym typem baz danych, przeznaczonym przede wszystkim do szybkiego czytania, przeglądania i przeszukiwania. Są one wykorzystywane jako mechanizmy zarządzania w środowiskach sieciowych. Usługi katalogowe umożliwiają przeszukiwanie wszystkich zasobów sieci zorganizowanej w strukturze drzewa. Mogą realizować również przeszukiwanie według właściwości, np. wyszukać wszystkie obiekty typu drukarka niezależnie od tego, w którym miejscu w sieci są zlokalizowane.

PRZYKŁAD 68.1

W ćwiczeniu na bazie systemu Windows 10 zostanie zbudowana prosta sieć peer-to-peer. Można ją wykorzystać do wymiany plików między komputerami. Do budowy sieci złożonej z dwóch komputerów można wykorzystać kabel skrosowany. Aby ją zbudować, należy:

1. Połączyć karty sieciowe komputerów za pomocą kabla skrosowanego.
2. Przydzielić komputerom unikatowe adresy IP należące do tej samej podsieci, np. **`192.168.0.1`** i **`192.168.0.2`** z maską **`255.255.255.0`**. W tym celu wybiera się **`Start/Panel sterowania/Sieć i Internet/Centrum sieci i udostępniania/Zmień ustawienia karty sieciowej`**. W oknie trzeba kliknąć prawym klawiszem myszy ikonę połączenia i z menu kontekstowego wybrać **`Właściwości`**. Następnie – zaznaczyć **`Protokół internetowy w wersji 4 (TCP/ IPv4)`** i kliknąć przycisk **`Właściwości`**. Na koniec – wpisać adres komputera i maski podsieci (pozostałe pola mogą pozostać puste) i kliknąć przycisk **`OK`**.
3. Przetestować możliwość komunikacji między komputerami – wpisać polecenie **`ping <adres IP sąsiada>`**, np. **`ping 192.168.0.1`**.

UWAGA

Przez systemowy firewall może być blokowane polecenie **`ping`**. Zapytaj nauczyciela, jak go wyłączyć na czas testów.

PRZYKŁAD 68.2

W tym ćwiczeniu zostanie na bazie systemu Windows 10 zbudowana prosta sieć peer-to-peer. Jeżeli w sieci mają być więcej niż dwa komputery, to do ich połączenia można wykorzystać przełącznik lub kilka przełączników. Aby zbudować sieć, należy:

1. Połączyć karty sieciowe komputerów z przełącznikiem za pomocą kabla prostego.
2. Przydzielić komputerom unikatowe adresy IP należące do tej samej podsieci, np. **`192.168.0.1`**, **`192.168.0.2`** ... **`192.168.0.x`**, gdzie x jest kolejnym numerem komputera (maksymalnie 254), z maską **`255.255.255.0`**. Sposób przydziału adresów jest taki sam jak opisany w przykładzie 68.1.
3. Przetestować możliwość komunikacji między komputerami – za pomocą polecenia **`ping`** przetestować komunikację ze wszystkimi komputerami w sieci.

UWAGA

Przez systemowy firewall może być blokowane polecenie **`ping`**. Zapytaj nauczyciela, jak go wyłączyć na czas testów. Jeżeli komputery mają karty sieciowe korzystające z innego medium transmisyjnego niż skrętka, to zapytaj nauczyciela, jak je połączyć.

SPRAWDŹ SWOJE WIADOMOŚCI

1. Jaką architekturę sieci wykorzystuje się w twojej szkole?
2. Kto jest administratorem sieci?
3. Czym różni się sieć równorzędna od sieci klient–serwer?
4. Kiedy komputer w sieci partnerskiej pełni funkcję klienta, a kiedy serwera?
5. Podaj definicję sieci komputerowej.
6. Podaj definicję stacji roboczej.
7. Narysuj schemat i opisz typ sieci klient–serwer.
8. Narysuj schemat i opisz typ sieci peer-to-peer.

69 Korzystanie z usług sieciowych – serwis stron WWW

ZAGADNIENIA

Wykorzystanie serwisu WWW **Działanie przeglądarki internetowej** **Zapisanie strony WWW do przeglądania w trybie offline**

Sieć internet pracuje w architekturze klient–serwer. Oznacza to, że przez serwery świadczy się usługi, z których korzystają klienci. W internecie funkcjonuje wiele usług, pełniących różne funkcje, np. serwis stron WWW, FTP, poczta elektroniczna, serwery news (grupy dyskusyjne), telnet, ssh.

Serwis WWW (ang. *World Wide Web*) jest usługą internetową opartą na protokole **HTTP** lub szyfrowanej wersji tego protokołu **HTTPS**. Jest to publicznie dostępny system informacyjny oparty na otwartych standardach. Jego podstawowym zadaniem jest udostępnianie informacji w formie **hipertekstu**. Użytkownik przeglądający dokumenty może się przemieszczać między dokumentami za pomocą **odnośników** (ang. *link*), które przenoszą go do dokumentów udostępnianych na tym samym lub dowolnym innym serwerze dostępnym w sieci.

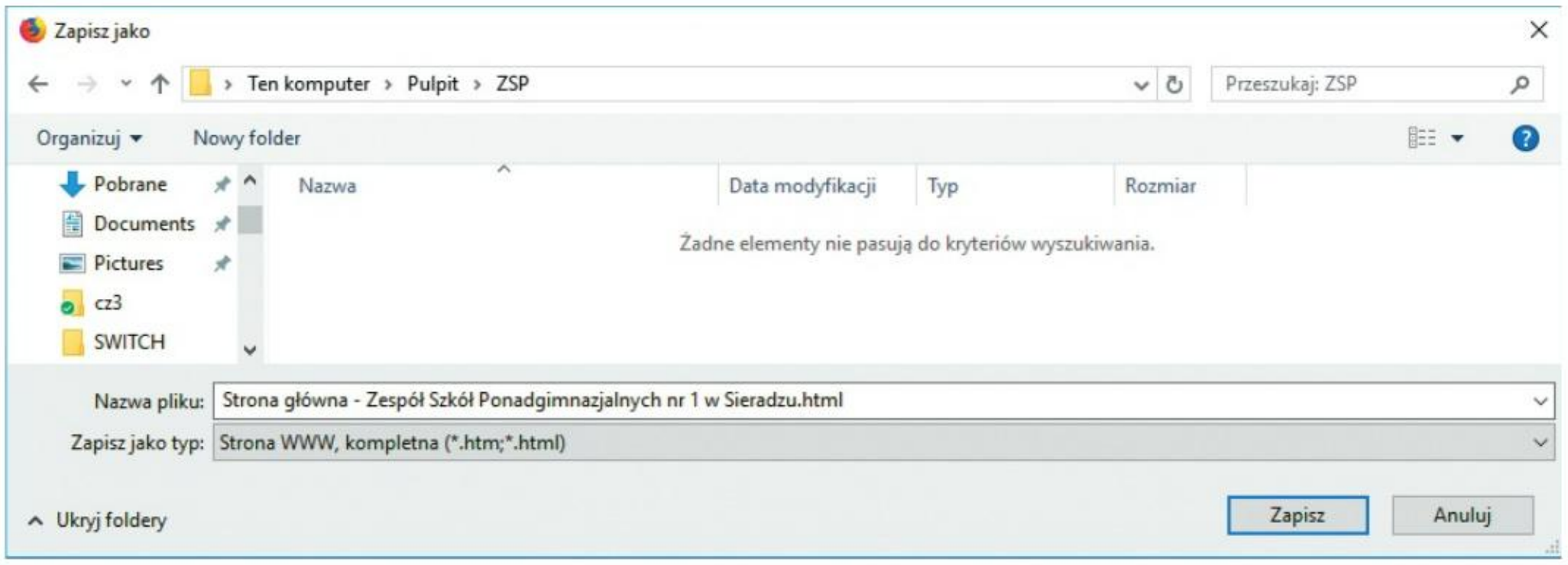
Aby uzyskać dostęp do informacji udostępnianej na serwerze WWW, należy posłużyć się programem komputerowym nazywanym **przeglądarką internetową**. Przeglądarka łączy się z serwerem WWW i pobiera zbiór informacji nazywany **stroną internetową** lub **witryną internetową**. Przeglądarka interpretuje kod strony zapisany w języku **HTML** (ang. *Hyper-Text Markup Language*) i wyświetla stronę. Serwer WWW przechowuje i udostępnia pliki tekstowe, graficzne, dźwiękowe, wideo i innych typów. Poprzez strony internetowe mogą być również uruchamiane skrypty programów, np. PHP lub JavaScript. Sposób wykorzystania plików i rodzaje akceptowanych formatów plików zależą od oprogramowania i od wyposażenia komputera lokalnego.

Do poprawnego odtwarzania niektórych formatów plików konieczne jest zainstalowanie w przeglądarce **wtyczki** (ang. *plug-in*) obsługującej dany format. Współczesne przeglądarki internetowe również mogą oferować obsługę wielu usług i funkcji. Przykładami przeglądarek internetowych są Microsoft Edge, Opera, Mozilla Firefox, Chrome.

Serwis WWW stanowi źródło olbrzymiej ilości informacji. Do ich pozyskiwania służą **wyszukiwarki internetowe**, czyli programy lub strony internetowe, których zadaniem jest ułatwienie użytkownikom wyszukiwania informacji w sieci. Przykładem wyszukiwarki może być www.google.pl.

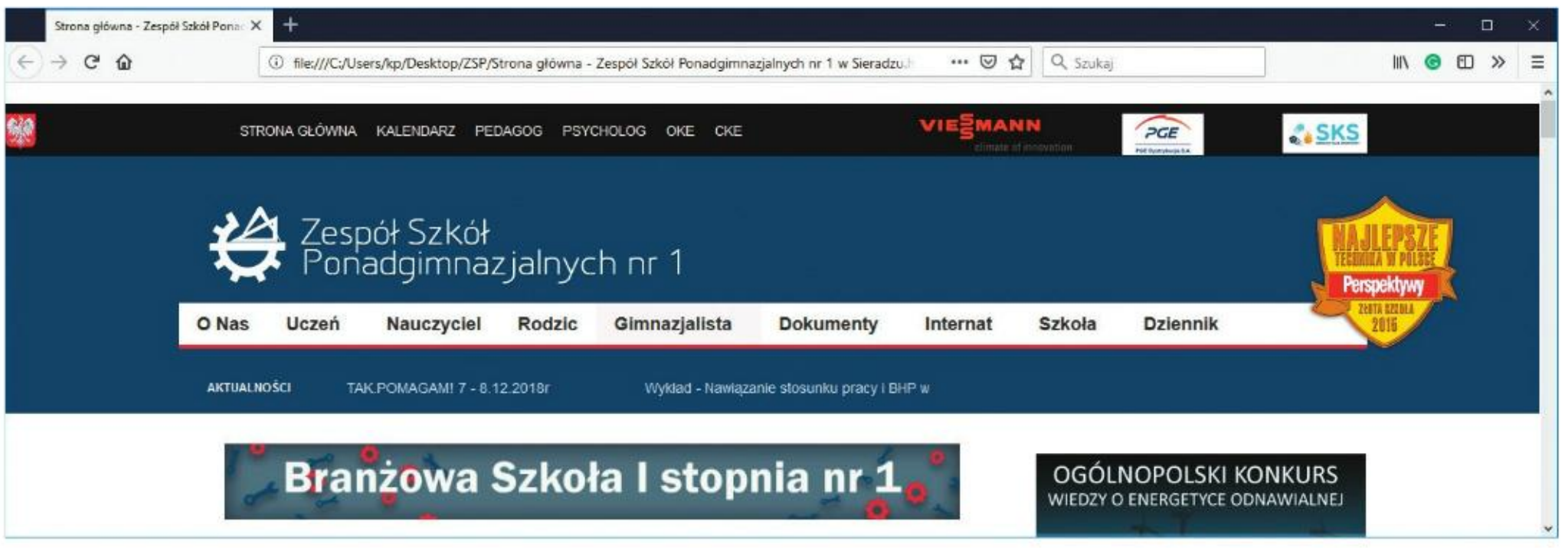
Przeglądarki internetowe oferują możliwość pracy w trybie **bez połączenia z siecią** (ang. *off-line*). Aby przeglądanie stron było możliwe, stronę internetową należy wcześniej pobrać i zapisać na dysku. Takie rozwiązanie może być przydatne, gdy przepustowość łącza jest niewielka lub gdy komputer, na którym będziemy przeglądać stronę, nie ma łączności z internetem. Do pobierania stron internetowych możemy wykorzystać specjalistyczny program, np. teleport (program komercyjny), lub odpowiednią funkcję przeglądarki. Rozwiązaniem alternatywnym dla programu teleport może być linuksowy program wget lub HTTrack Website Copier – bezpłatny program umożliwiający pobieranie i zapisywanie w całości wybranej strony internetowej w postaci statycznych plików HTML.

Zawartość strony można zapisać na dysku również za pomocą przeglądarki internetowej, np. Mozilla Firefox. W tym celu należy otworzyć stronę, którą zamierzamy zapisać, a następnie wybrać polecenie **Zapisz stronę jako**. W oknie zapisywania strony (rys. 69.1) wskazujemy folder, w którym ma być zapisana strona, i jako typ zapisu wybieramy **Strona WWW, kompletna (*.htm, *.html)**.



Rys. 69.1. Zapisywanie strony za pomocą przeglądarki internetowej

Po zapisaniu strony są tworzone plik w formacie .html i folder zawierający wszystkie pozostałe pliki, z których składa się strona. Aby otworzyć stronę w trybie offline, należy dwukrotnie kliknąć plik strony (rys. 69.2).



Rys. 69.2. Przeglądanie strony w trybie offline

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zapisz stronę internetową twojej szkoły w wersji offline. Przetestuj możliwość odczytania jej bez połączenia z internetem.

70 Korzystanie z usługi transferu plików

ZAGADNIENIA

Funkcje protokołu FTP **Korzystanie z klienta FTP** **Korzystanie z programu FileZilla**

FTP jest protokołem służącym do transmisji plików w sieci. Działa na bazie protokołu TCP i zazwyczaj wykorzystuje do transmisji danych port 20, a do kontroli transmisji – port 21. Podstawową zaletą FTP jest to, że rozpoczęty, lecz niezakończony pomyślnie, transfer danych może zostać wznowiony aż do uzupełnienia brakujących części pliku (należy jednak wspomnieć, że nie wszystkie serwery oferują tę usługę). Głównymi wadami tego protokołu są brak możliwości szyfrowania transmisji i problemy z implementacją filtrów pakietów na routerach. Mimo tych wad FTP jest nadal jednym z najpopularniejszych w internecie protokołów przesyłania plików.

Protokół działa z wykorzystaniem architektury klient–serwer. Użytkownik (klient) łączy się z **serwerem FTP** za pomocą specjalnego programu, nazywanego **klientem FTP**. W większości systemów operacyjnych jest wbudowany klient FTP pracujący w trybie tekstowym. Aby wykonać jakąś operację, należy wpisać odpowiednie polecenie. Nie jest to metoda wygodna, wymaga znajomości poleceń i protokołu, ale działa zawsze i we wszystkich systemach operacyjnych. Funkcję klienta FTP mogą pełnić także przeglądarki internetowe, choć pod względem możliwości ustępują one specjalnie utworzonym klientom FTP. Klient FTP jest wbudowany także do wielu menedżerów plików, np. do **Total Commandera**.

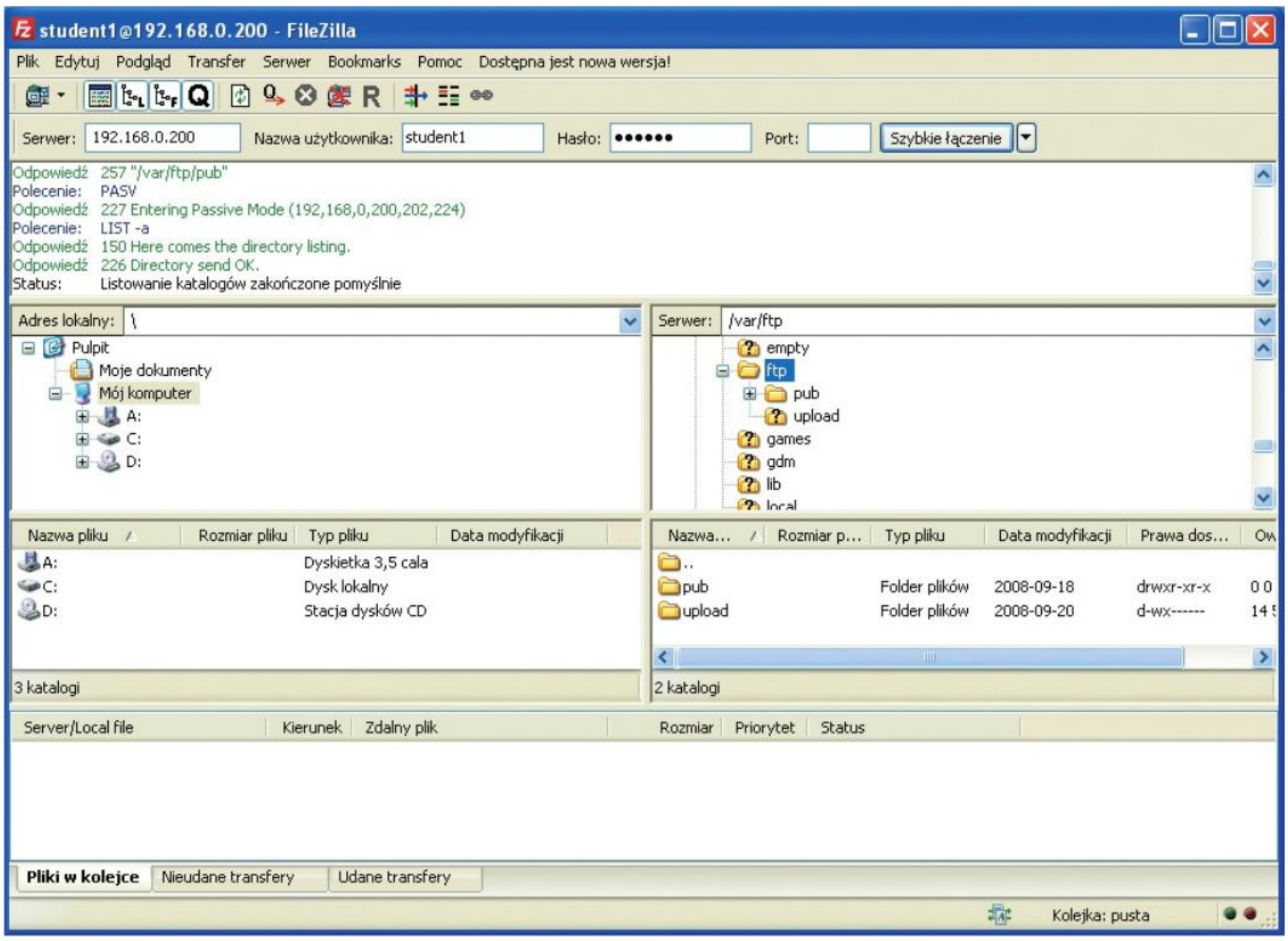
Sesja FTP składa się z trzech części. Pierwsza z nich to zalogowanie się na odległy komputer: należy podać nazwę użytkownika i hasło. Na ich podstawie serwer FTP identyfikuje użytkownika i przydziela mu na czas sesji określone prawa dostępu do swoich zasobów. Posiadanie konta i związanych z nim odpowiednich uprawnień na komputerze docelowym jest warunkiem koniecznym do rozpoczęcia transmisji jakichkolwiek danych. Takie konto jest przydzielane przez administratora systemu. Podczas drugiej części są wykonywane operacje na odległych plikach i folderach – kopiowanie, przenoszenie, zmiana nazwy itp. Ostatni etap to zamknięcie sesji. Niektóre serwery wysyłają na zakończenie krótką statystykę, w której są zawarte m.in. informacje o czasie trwania sesji i liczbie przesłanych danych.

Jak każdy komputer dostępny w internecie, serwer FTP ma indywidualny adres pozwalający jednoznacznie go zidentyfikować. Aby połączyć się z serwerem FTP, możemy się posłużyć jego adresem IP, np. 10.1.51.31. Z tego typu adresów korzystamy najczęściej, gdy nasz serwer znajduje się w sieci lokalnej, której nie obsługuje serwer DNS. Jeżeli w sieci działa serwer DNS lub korzystamy z internetu, to zamiast adresu IP możemy posługiwać się nazwami domenowymi, np. **`ftp.task.gda.pl`**. Pełny adres internetowy (URL) wymaga prefiksu „**`ftp://`**”, np.: **`ftp://ftp.task.gda.pl`**. Jeżeli dostęp do serwera wymaga podania nazwy użytkownika i hasła, należy dołączyć te dane do adresu w następujący sposób:

```
ftp://uzytkownik:haslo@ftp.task.gda.pl.
```

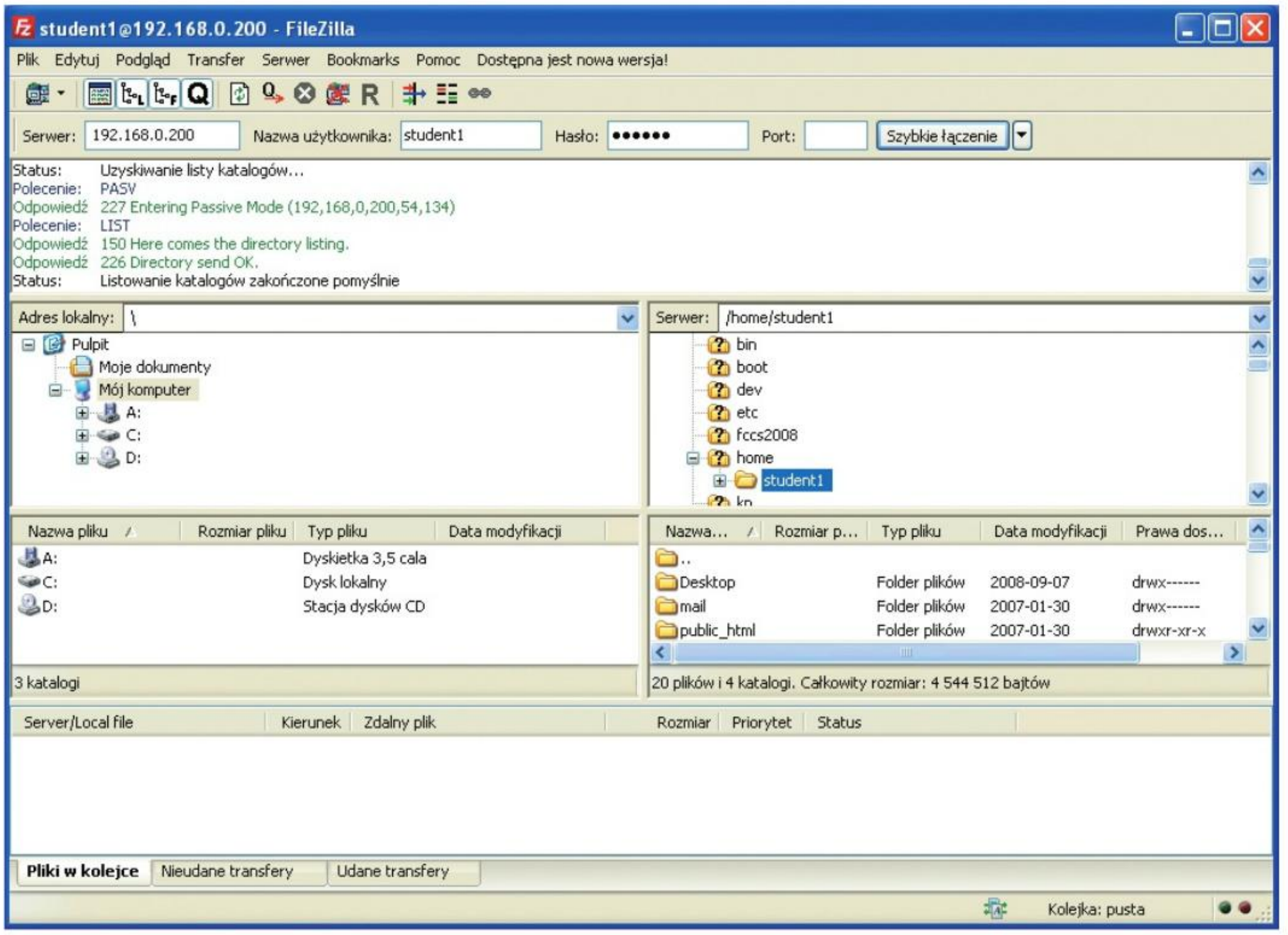
Często stosowaną praktyką jest wydzielanie części publicznej serwera i udostępnianie jej zawartości każdemu zainteresowanemu internaucie. Te serwery nazywa się **publicznymi** lub **anonimowymi**, ponieważ osoba z nich korzystająca podaje podczas procedury logowania nazwę konta „anonymous", a jako hasło – własny adres e-mail.

W standardowej konfiguracji uprawnienia anonimowego użytkownika pozwalają jedynie na pobieranie plików (i to tylko z wydzielonych, publicznych folderów) i nie dają możliwości ich wysyłania na serwer. Najczęściej do dyspozycji anonimowych użytkowników jest przeznaczony folder **pub**, w którym są gromadzone zbiory dostępne dla każdego użytkownika (prawa tylko do pobierania danych z serwera). Administrator serwera FTP może udostępnić oddzielne foldery przeznaczone na pliki do przesyłania na serwer przez użytkowników anonimowych. Jest to najczęściej pojedynczy folder o nazwie **upload** lub **incoming**, w którym można umieścić ciekawy program lub dokument. Po sprawdzeniu jego zawartości administrator może skopiować go do folderu **pub**, tak aby był dostępny dla innych użytkowników. Po zalogowaniu się na konto anonimowe zostajemy przeniesieni do folderu głównego usługi FTP. Ten folder w Linuksie jest zlokalizowany w **/var/ftp** (rys. 70.1). W folderze na ogół dysponujemy uprawnieniami umożliwiającymi tylko pobieranie plików.



Rys. 70.1. Ścieżka dostępu dla udostępnianych folderów dla konta anonimowego

Po zalogowaniu się na konto lokalne na serwerze jesteśmy przenoszeni do folderu domowego użytkownika. Standardowo w Linuksie jest to **/home/użytkownik** (rys. 70.2).



Rys. 70.2. Ścieżka dostępu dla udostępnianych folderów dla konta lokalnego

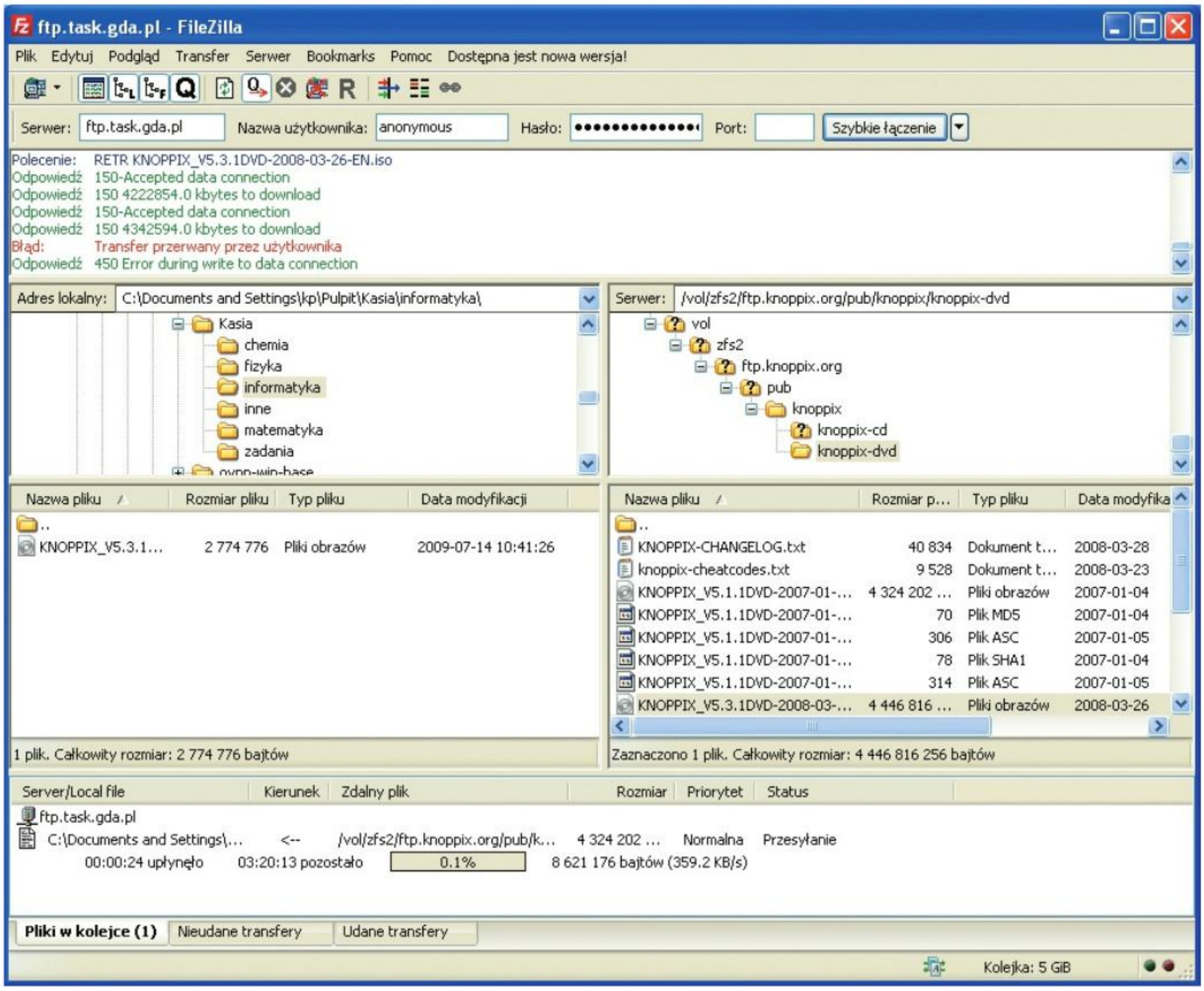
W tym folderze dysponujemy pełnymi uprawnieniami (możemy pliki pobierać z serwera, przenosić na serwer, kasować i zarządzać folderami). Przesyłanie plików przez FTP może odbywać się w dwóch trybach:

- **ASCII** (ang. *American Standard Code for Information*) – przeznaczony tylko do plików zapisanych w standardzie ASCII (takie pliki zawierają tylko tekst, np. pliki wsadowe, dokumenty HTML, dokumenty tekstowe z rozszerzeniem *.txt);
- **binarnym** – przeznaczony do przesyłania wszystkich pozostałych typów plików.

Dokumenty popularnych programów biurowych, np. MS Word, nie są plikami ASCII – oprócz tekstu zawierają wiele dodatkowych informacji i nie mogą być przesyłane w trybie ASCII. Plik binarny (program, grafika, archiwum ZIP) przesłany w trybie ASCII zostałby uszkodzony. Klient FTP i przeglądarka internetowa na ogół automatycznie rozpoznają typ przesyłanego pliku i uruchamiają odpowiedni tryb przesyłania.

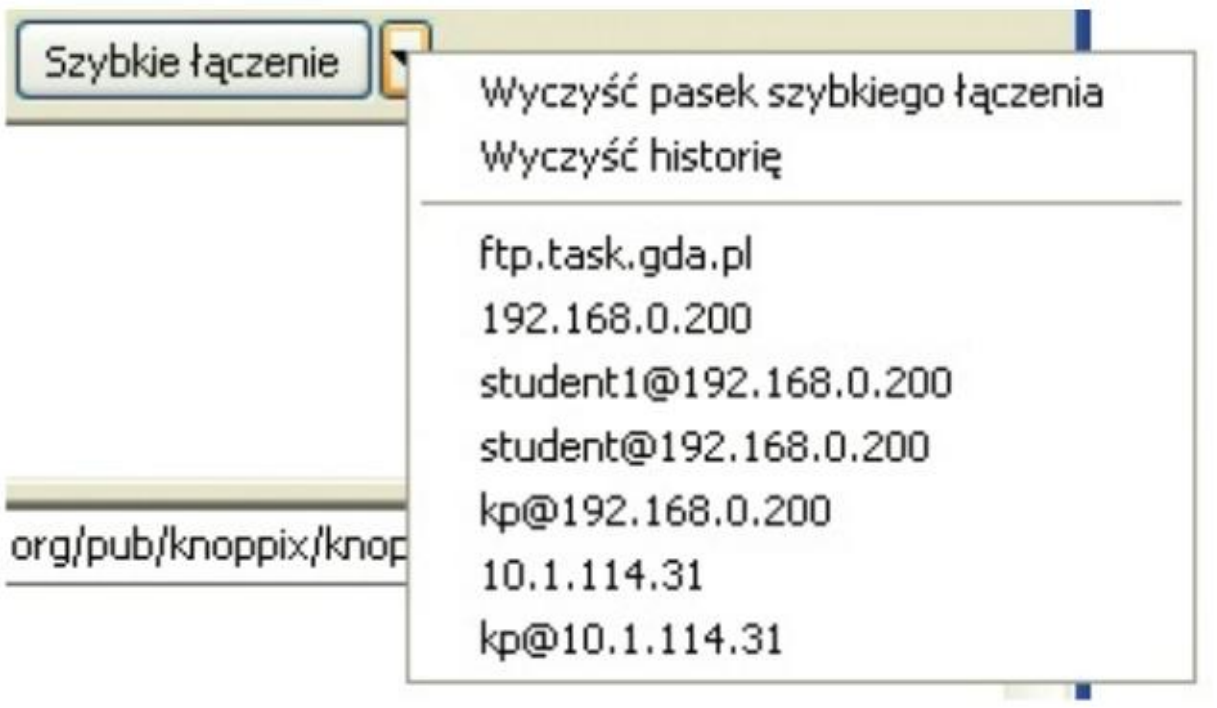
Jednym z bezpłatnych klientów FTP, przeznaczonych dla systemu Windows, jest **FileZilla**. Jak większość klientów FTP, ma klasyczny interfejs składający się z dwóch paneli. Po lewej stronie (rys. 70.3) umieszczono folder komputera lokalnego. Po prawej stronie wyświetla się zawartość folderu na serwerze.

Dodatkowo w górnej części okna znajduje się lista poleceń i komunikatów przesyłanych między komputerami. W dolnej części okna umieszczono kolejkę zadań do wykonywania. Połączenie z serwerem (rys. 70.3) nawiązujemy przez wpisanie w odpowiednie okna nazwy lub adresu IP serwera, nazwy użytkownika, hasła i numeru portu (domyślnie 21).



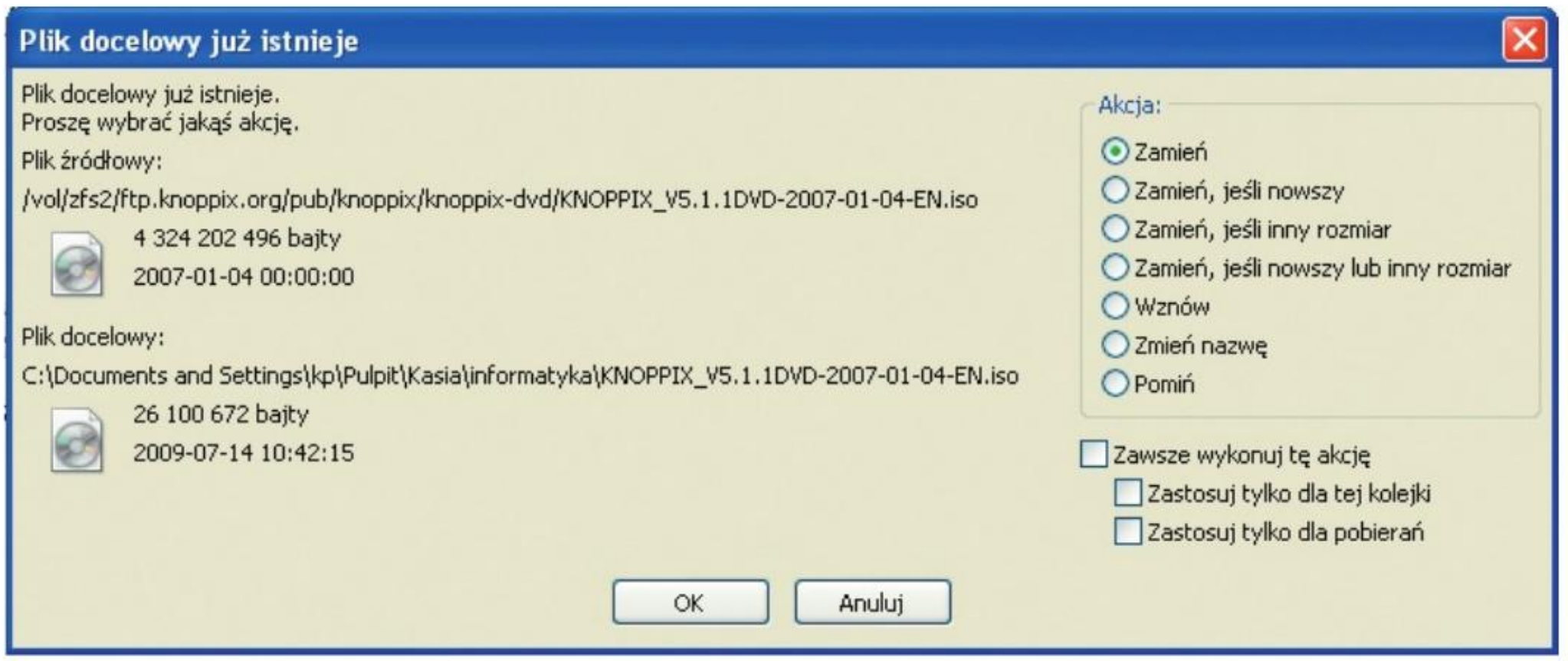
Rys. 70.3. **Interfejs programu FilleZilla**

Wszelkie operacje na plikach wykonuje się **metodą przeciągnij i upuść**. Jeżeli połączenie zostanie zerwane, możemy je przywrócić, gdy wybierzemy przycisk **Szybkie łączenie**. W oknie dialogowym (rys. 70.4) pojawi się lista połączeń, spośród których wybieramy to, które chcemy przywrócić.



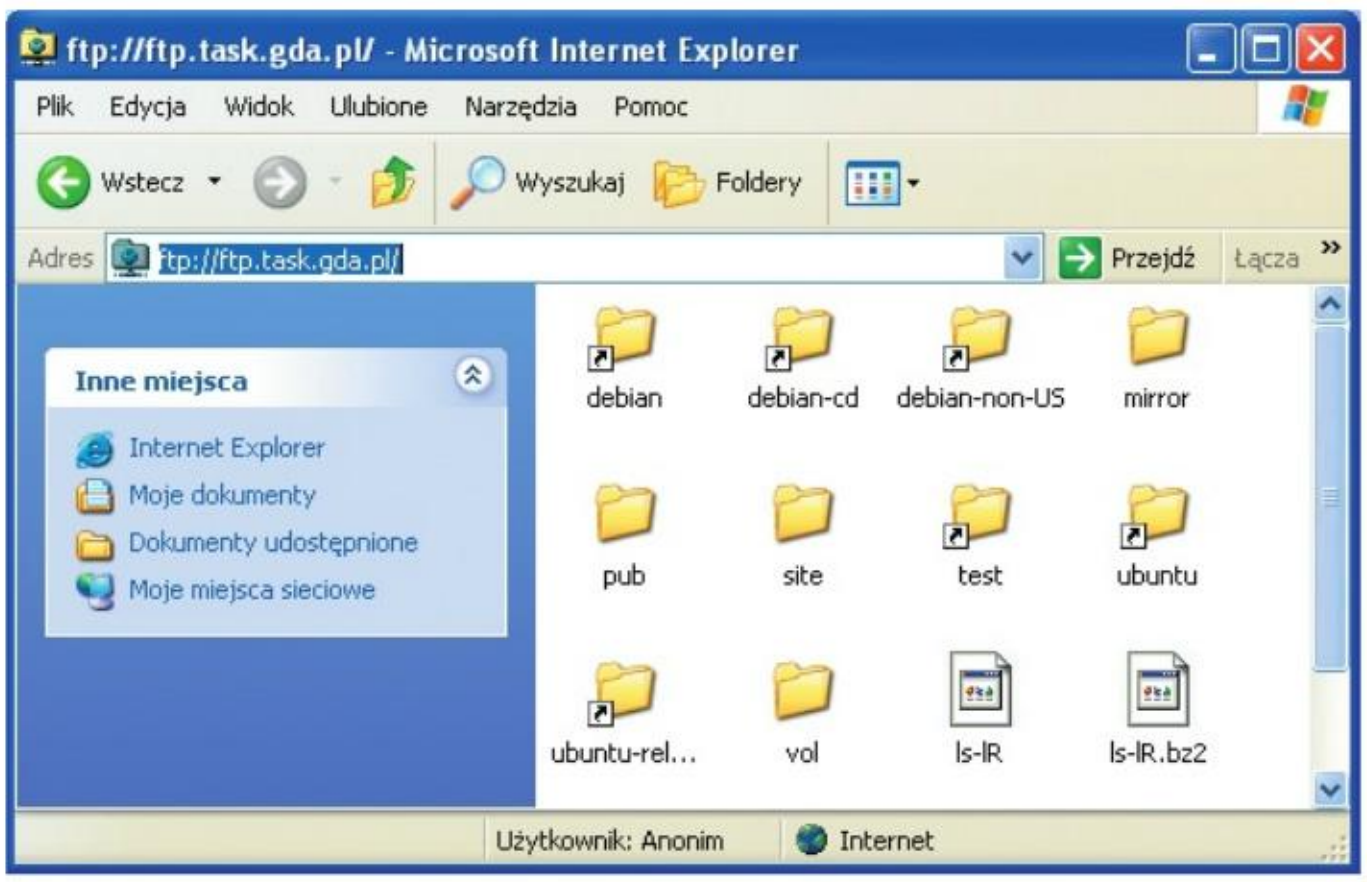
Rys. 70.4. **Szybkie łączenie z serwerem FTP**

Jeżeli połączenie zostanie przerwane w czasie transmisji danych, możemy kontynuować transfer danych od miejsca, w którym transmisja została przerwana (niestety, nie wszystkie serwery oferują tę usługę). W otwartym oknie dialogowym (rys. 70.5) możemy wybrać nadpisanie istniejącego pliku (rozpoczęcie transmisji od początku) lub wznowienie transmisji.



Rys. 70.5. **Wznowienie sesji FTP**

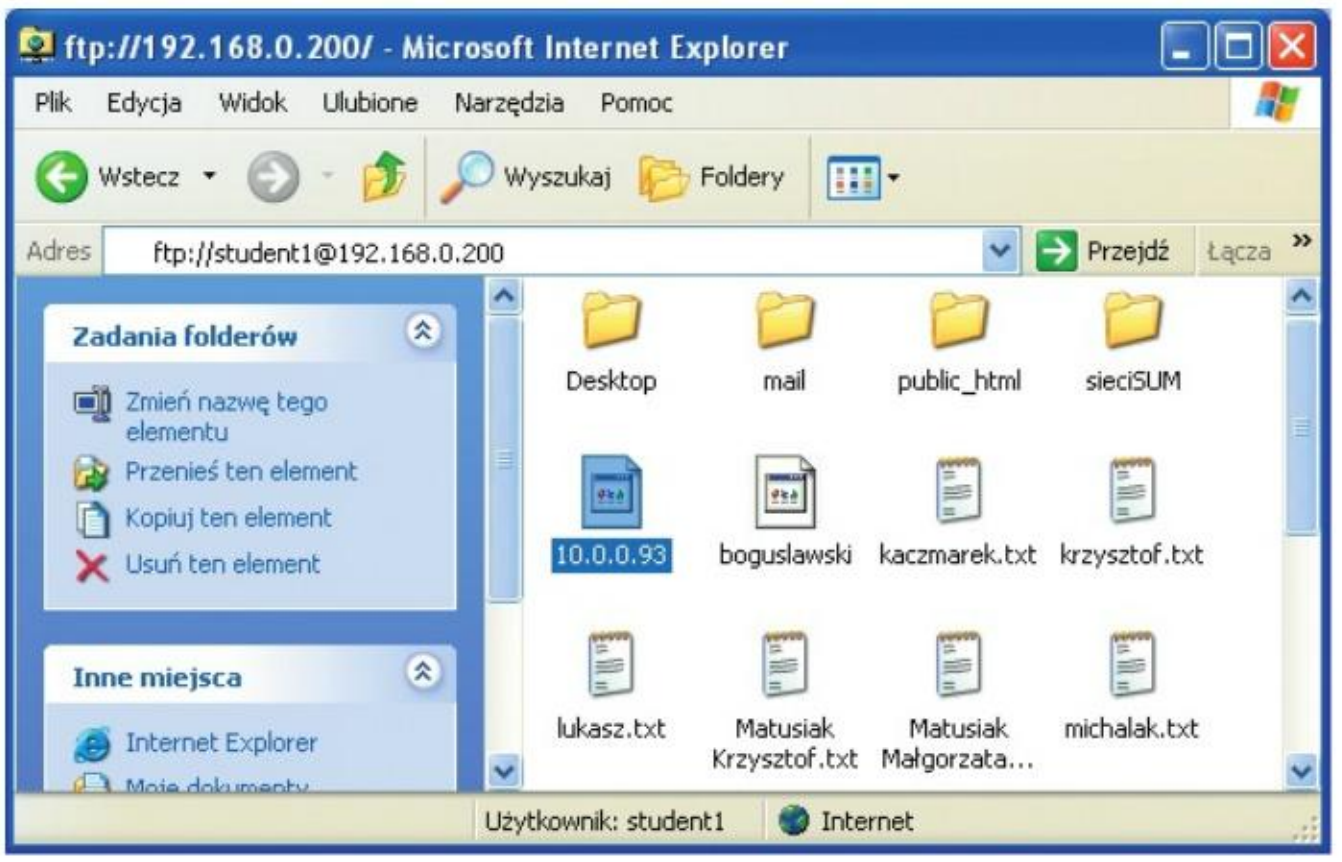
Przeglądarka internetowa standardowo jest tak skonfigurowana, aby obsługiwać przeglądanie stron internetowych za pomocą protokołu HTTP. Większość współczesnych przeglądarek ma wbudowanego klienta FTP. Aby jednak połączyć się z serwerem FTP, należy w jawny sposób poinformować serwer o zamiarze korzystania z protokołu FTP. W tym celu w polu **`Adres przeglądarki`** wpisujemy pełny adres URL (rys. 70.6).



Rys. 70.6. **Anonimowy dostęp do FTP**

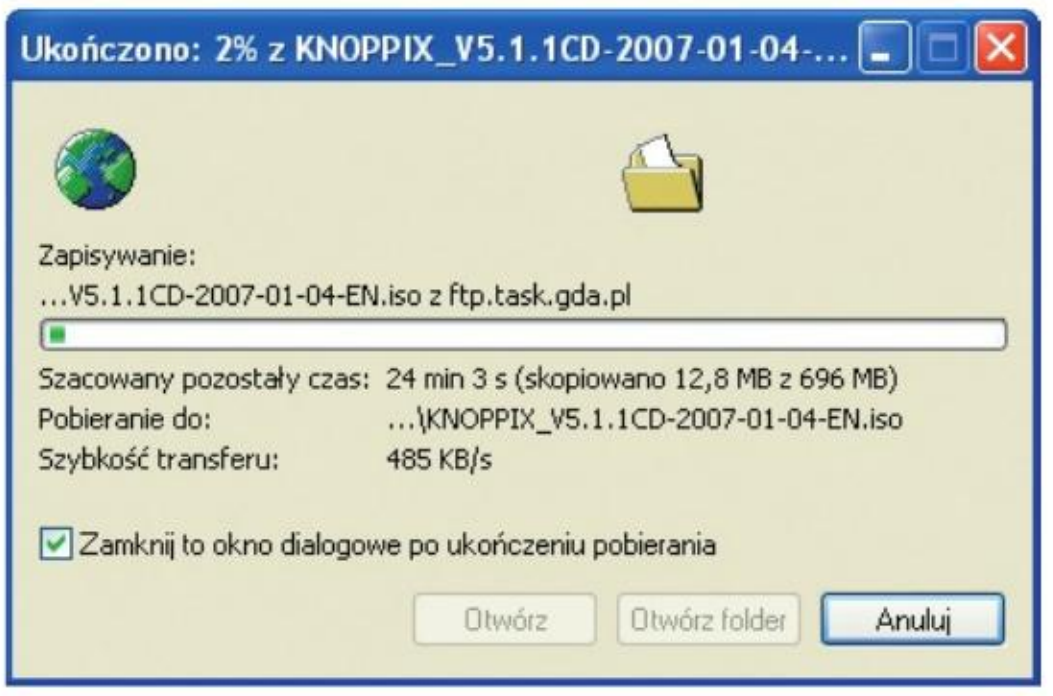
Klient w przeglądarce internetowej jest skonfigurowany w taki sposób, aby automatycznie był logowany użytkownik anonimowy. Serwery mogą mieć – ale nie muszą – skonfigurowane konta anonimowe, niewymagające podania hasła. Dzięki temu bezpośrednio po wpisaniu adresu jesteśmy przenoszeni do folderu **`pub`** (bez konieczności wpisywania hasła). Operacje na plikach możemy wykonywać za pomocą myszy, tak jak w oknie **Eksploratora Windows**. Mała strzałka

po lewej stronie ikony folderu oznacza, że tak naprawdę jest to nie folder, ale tylko skrót do niego. Po kliknięciu system automatycznie przeniesie nas w miejsce wskazane za pomocą skrótu. Podczas korzystania z konta anonimowego nasze uprawnienia na ogół są ograniczone tylko do pobierania danych z folderu **pub**. Próba przejścia do folderu nadrzędnego powoduje zakończenie sesji FTP i rozłączenie z serwerem. Jeżeli na serwerze FTP mamy konto lokalne, to podczas logowania w polu **Adres** przeglądarki wpisujemy nazwę konta i adres serwera oddzielone znakiem @ (rys. 70.7).



Rys. 70.7. Logowanie do serwera FTP na konto lokalne

W czasie kopiowania pliku na bieżąco jest wyświetlana statystyka połączenia pozwalająca na zorientowanie się w szacunkowym terminie zakończenia operacji (rys. 70.8).



Rys. 70.8. Statystyka połączeń FTP

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skorzystaj z dowolnej metody i pobierz dane ze szkolnego serwera FTP.
2. Wyślij plik **nazwisko.txt** do twojego katalogu domowego na szkolnym serwerze FTP.
3. Z serwera **ftp.task.gda.pl** pobierz na własny komputer plik **Sieciowy_Savoir-vivre.txt**. Plik ten znajduje się w folderze **/pub/doc**.

71 Korzystanie z usług poczty elektronicznej

ZAGADNIENIA

Funkcje poczty elektronicznej **Skonfigurowanie poczty elektronicznej do pobierania i wysyłania wiadomości** **Wykorzystanie grup dyskusyjnych**

Usługa poczty elektronicznej (ang. *e-mail*) pozwala na wymianę wiadomości tekstowych i załączników w postaci plików innych formatów, zawierających np. zdjęcia, muzykę. Z poczty elektronicznej można korzystać nie tylko za pomocą komputera, lecz także za pośrednictwem innych urządzeń, np. tabletu lub telefonu komórkowego. Program, dzięki któremu funkcjonuje poczta elektroniczna, składa się z dwóch części – **klienta** i **serwera**. Aby korzystać z poczty, trzeba zainstalować odpowiedniego klienta i mieć konto (skrzynkę pocztową) na serwerze poczty elektronicznej. Adres składa się z nazwy skrzynki (musi być unikatowa na danym serwerze), znaku rozdzielającego @ i unikatowego adresu serwera usługodawcy na serwerze, na którym założyliśmy konto. Obecnie większość dostawców usług poczty elektronicznej oferuje dostęp do skrzynki e-mail przez WWW.

Do wysyłania e-maili służy protokół **SMTP**. Wiadomość jest wysyłana na skrzynkę pocztową adresata i tam czeka na jej odebranie lub skasowanie. Do odbioru poczty stosuje się protokoły **POP3** i **IMAP**. POP3 jest znacznie prostszy i powszechnie używany. Program korzystający z POP3 do obsługi poczty, zainstalowany na komputerze, może po uzyskaniu połączenia pobrać wszystkie wiadomości do naszego lokalnego komputera i usunąć je z serwera (ustawienie można zmienić w konfiguracji programu pocztowego). Wiadomości możemy odczytywać w dowolnej chwili bez konieczności ponownego połączenia się z serwerem.

IMAP po nawiązaniu połączenia z serwerem poczty pobiera do naszego komputera wyłącznie nagłówki wiadomości. Dopiero po kliknięciu nagłówka jest pobierana cała wiadomość. Wiadomości przesyłane za pomocą poczty elektronicznej powinny być szyfrowane w celu zapewnienia poufności, np. za pomocą programu PGP.

Za pomocą poczty elektronicznej można:

- wysyłać teksty do dowolnego użytkownika internetu na całym świecie;
- dołączać do listu załączniki, które nie są tekstem, np. programy komputerowe, obrazy, dźwięk;
- wysyłać wiadomości do wielu adresatów jednocześnie za pomocą list e-mailowych;
- odpowiadać na listy lub przekazywać je dalej.

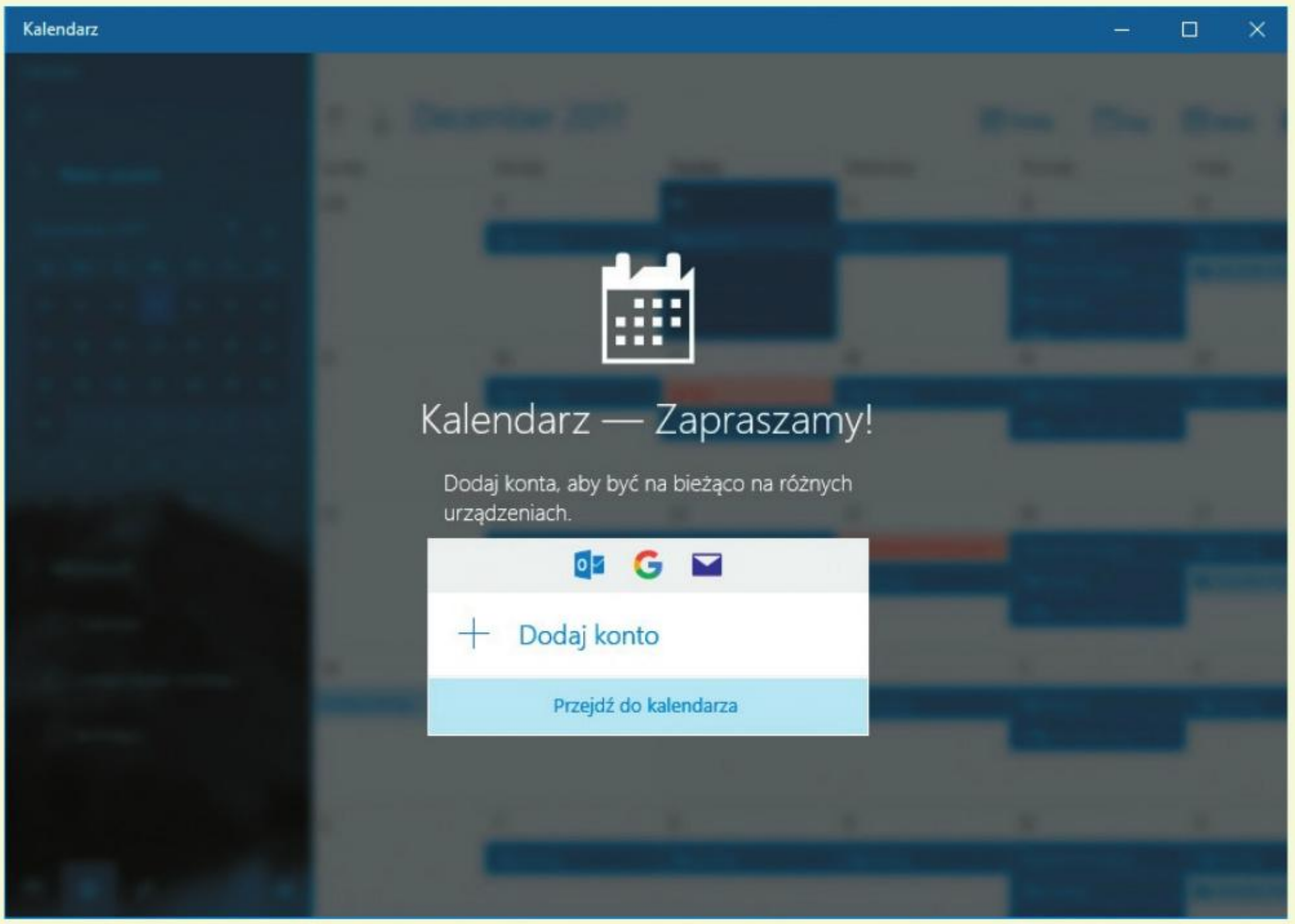
Dysponowanie kontem poczty elektronicznej pozwala użytkownikowi na korzystanie z innych usług dostępnych w internecie, np. z anonimowego dostępu do serwerów FTP lub grup dyskusyjnych.

W systemie Windows 10 pocztę elektroniczną można obsługiwać za pomocą aplikacji **`Poczta i kalendarz`**.

PRZYKŁAD 71.1

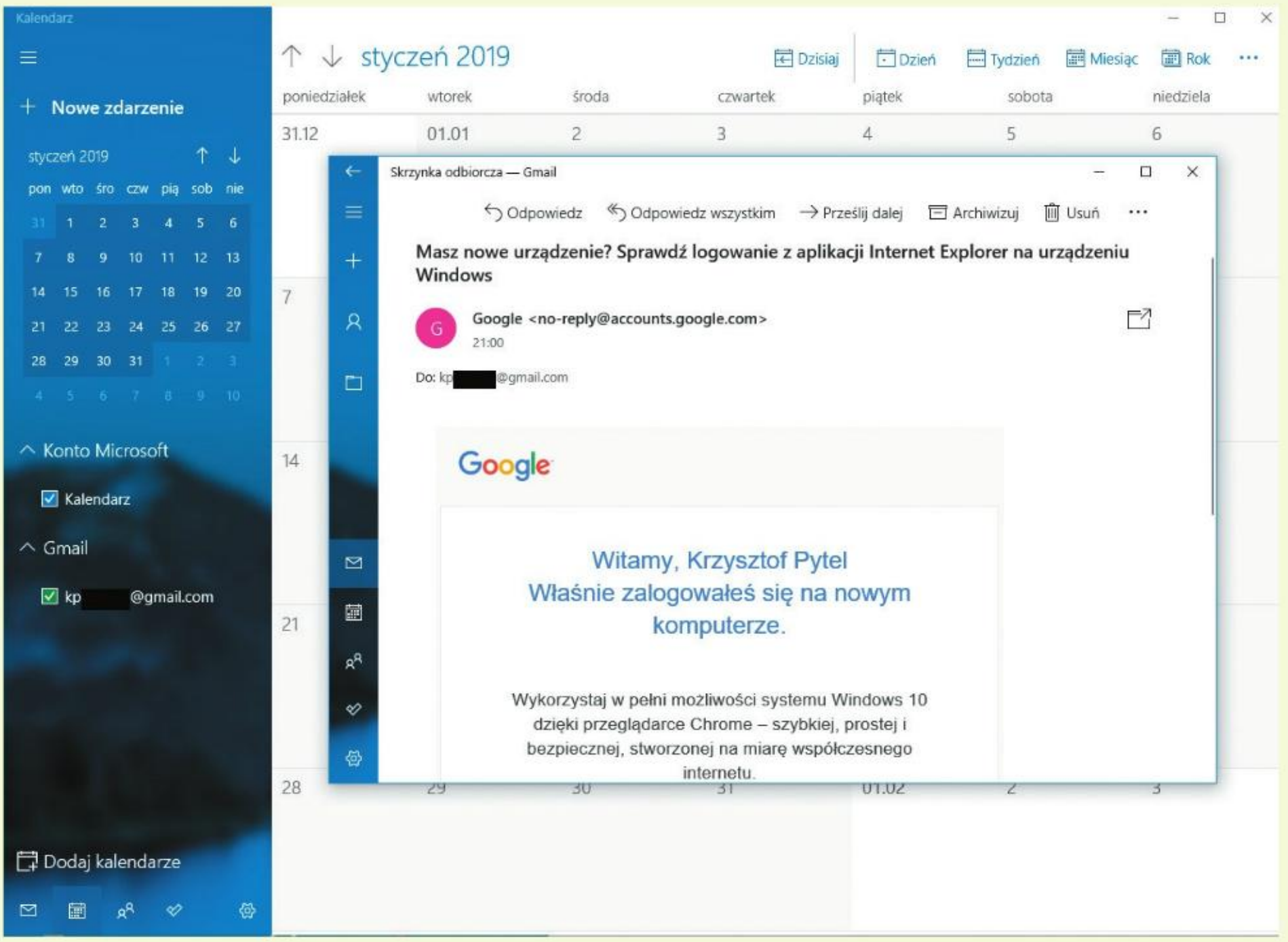
W tym ćwiczeniu zostanie wykonana konfiguracja programu pocztowego dla Windows 10. Aby skonfigurować program, należy:

1. Uruchomić aplikację kalendarz **Start/Kalendarz**.
2. Jeżeli jest to pierwsze uruchomienie programu, kliknąć odnośnik **Dodaj konto** (rys. 71.1).



Rys. 71.1. **Uruchomienie kreatora konfiguracji konta**

3. Wybrać dostawcę usługi, np. **Google**.
4. Jeżeli użytkownik ma już konto, wpisać jego adres i kliknąć przycisk **Dalej**. Jeżeli użytkownik nie ma konta, kliknąć odnośnik **Utwórz konto** i postępować zgodnie ze wskazówkami kreatora. Po utworzeniu konta powrócić do ekranu i wpisać adres konta.
5. Wpisać hasło do konta i kliknąć przycisk **Dalej**.
6. Zezwolić aplikacji na dostęp do konta – kliknąć przycisk **Zezwól**.
7. Po zakończeniu pracy kreatora i wyświetleniu komunikatu o pomyślnym skonfigurowaniu konta kliknąć przycisk **Gotowe**.
8. W oknie aplikacji **Kalendarz** kliknąć ikonę koperty w lewym dolnym rogu, wskazać konto i wprowadzić hasło.
9. Wybrać wiadomość do czytania lub zarządzania wiadomościami.



Rys. 71.2. **Przeglądanie wiadomości w skrzynce odbiorczej**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zapisz w swoim zeszycie przedmiotowym adresy serwerów SMTP i POP3 lub IMAP skrzynki pocztowej, której używasz.
2. Wyślij do koleżanki / kolegi wiadomość z załącznikiem (dowolny plik graficzny).

72 Korzystanie z usługi telnet

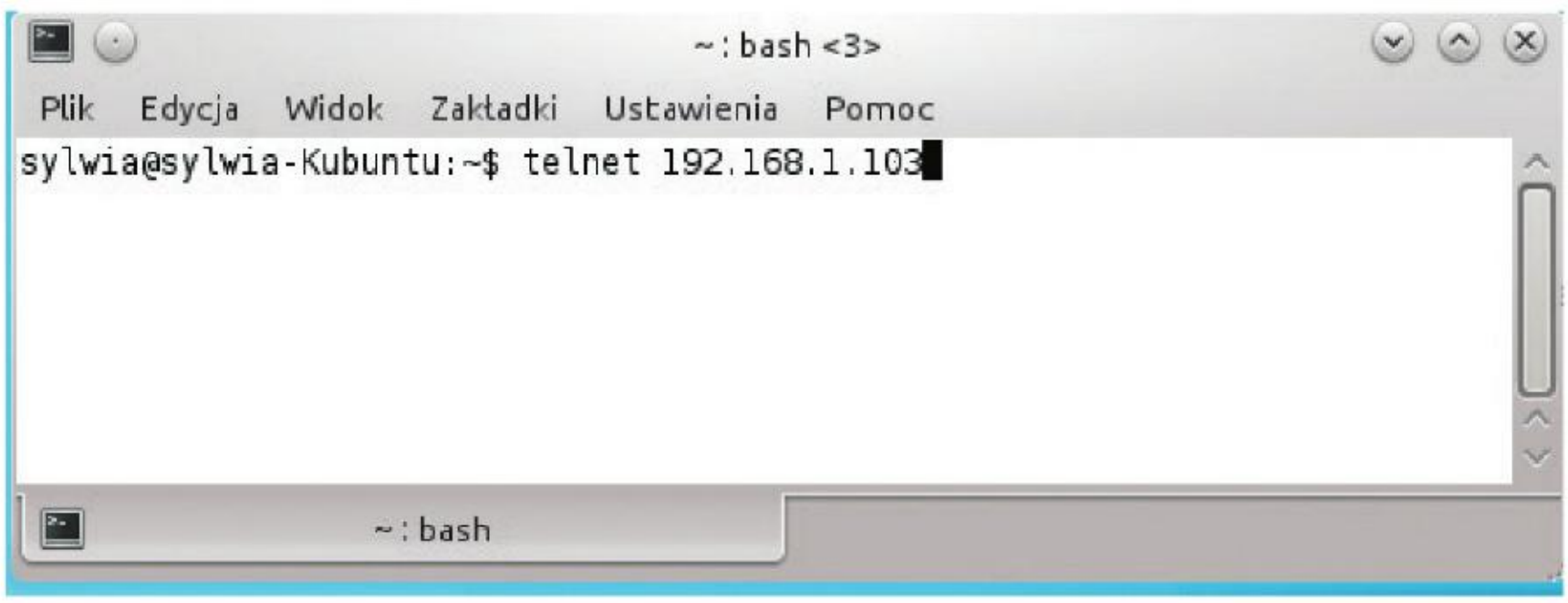
ZAGADNIENIA

Funkcja usługi telnet **Uruchomienie sesji telnetu** **Korzystanie z telnetu**

Telnet jest protokołem umożliwiającym wykonywanie poleceń na odległym komputerze. Umożliwia on użytkownikowi interakcyjną pracę w środowisku tekstowym na odległych komputerach, uruchamianie programów, dostęp do baz danych itp. Pozwala korzystać z usług oferowanych przez komputer niezależnie od tego, czy znajduje się on w sąsiednim pokoju, czy – na innym kontynencie. Lokalny komputer działa tak, że emuluje – czyli naśladuje – terminal odległego komputera, co stwarza wrażenie pracy w systemie, z którym nawiązano połączenie. Klient telnetu musi emulować terminal właściwy dla zdalnego systemu, ponieważ korzystanie z niewłaściwego typu terminalu mogłoby skutkować błędnym interpretowaniem poszczególnych klawiszy lub znaków.

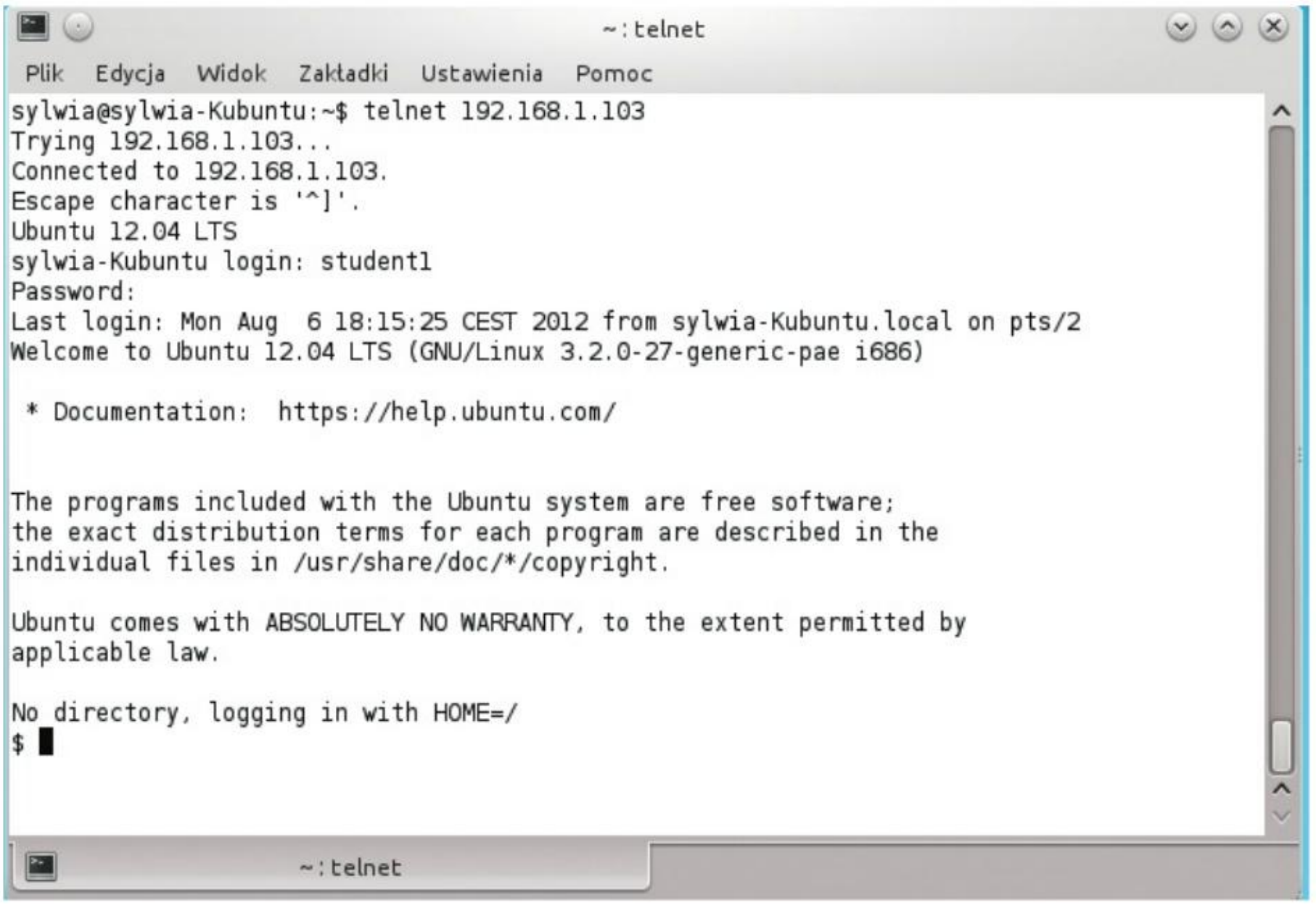
Aby połączenie było możliwe, na zdalnym systemie należy uruchomić **serwer usługi telnet**. Standardowo telnet korzysta z portu 23. Klient telnetu jest wbudowany w większość systemów operacyjnych, np. Linux, Windows XP. Nie jest natomiast wbudowany w Windows 7 i w wersje nowsze. W systemie Windows 10 należy pobrać i zainstalować dodatkowy program, np. **PuTTY**.

Aby uruchomić sesję telnetu, np. w Ubuntu, uruchamiamy **Konsolę** (Terminal). W oknie (rys. 72.1) wpisujemy polecenie **`telnet`** i wprowadzamy adres IP lub nazwę komputera, z którym nawiązujemy połączenie.



Rys. 72.1. Uruchamianie sesji telnetu

Po nawiązaniu połączenia należy zalogować się na konto w serwerze odległym (rys. 72.2). Podaje się nazwę konta (ang. *login*) i hasło (ang. *password*). Zalogowanie na serwerze pozwala na rozpoczęcie pracy w terminalu. W celu zapewnienia bezpieczeństwa w niektórych systemach logowanie na konto administratora może być zablokowane.



Rys. 72.2. **Logowanie zdalne w sesji telnetu**

Telnet umożliwia logowanie się na zdalnych komputerach i wykonywanie poleceń systemowych. Usługa nie jest bezpieczna, gdyż wszystkie dane, takie jak nazwa użytkownika i hasło, są przesyłane przez sieć w nieszyfrowanej postaci. Z tego powodu dostęp przez telnet jest blokowany lub wyłączany przez wielu administratorów. Tam, gdzie jest to możliwe, powinno się go unikać, a w zamian – korzystać z usługi SSH o podobnych możliwościach, co jest bezpieczniejsze ze względu na szyfrowanie danych.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Za pomocą usługi telnet zaloguj się na szkolnym serwerze. Skorzystaj z indywidualnego konta, przydzielonego przez administratora.
2. Wymień zalety, wady i zastosowanie telnetu.
3. Wyszukaj w internecie, np. skorzystaj z portalu www.dobreprogramy.pl, informacje o nazwach i charakterystyce programów – klientów usługi telnet.

73 Korzystanie z usługi bezpiecznego terminala

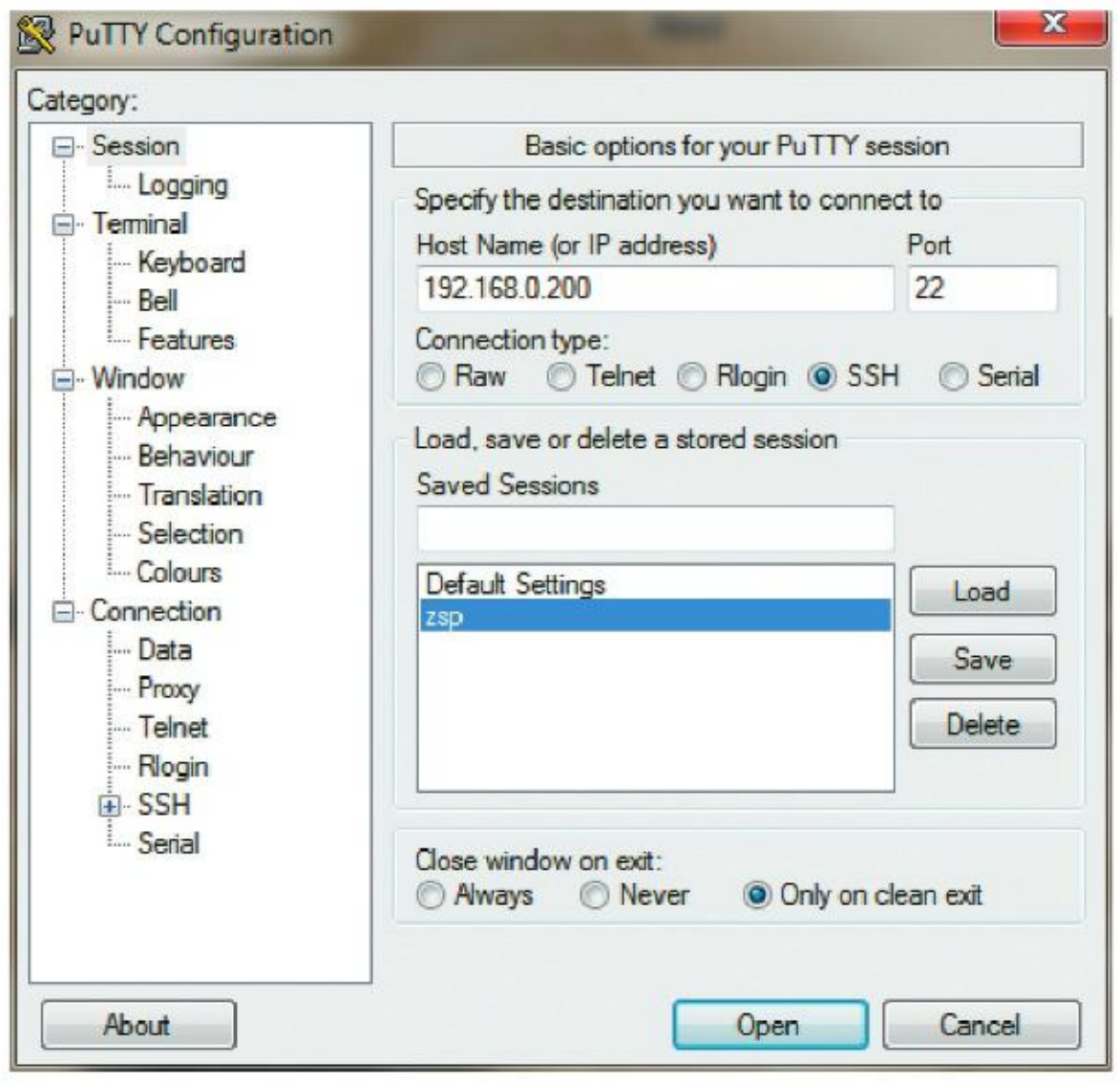
ZAGADNIENIA

- **Funkcje usługi SSH**
- **Korzystanie z usługi SSH**
- **Funkcje programu PuTTY**

Usługa SSH (ang. *Secure Shell*) jest następcą protokołu telnet i również służy do terminalowego łączenia się ze zdalnymi komputerami. Inaczej niż w usłudze telnet, transfer danych jest szyfrowany. Najczęściej stosuje się szyfrowanie algorytmem **AES**. Każdy komputer podczas pierwszego nawiązania połączenia z serwerem generuje dwa klucze. Jeden z nich (**publiczny**) jest dostępny dla wszystkich, drugi (**prywatny**) musi być starannie ukryty. Te klucze wykorzystuje się do szyfrowania transmisji. Identyfikacja użytkownika może polegać na weryfikacji konta i hasła lub za pomocą klucza wygenerowanego dzięki poleceniu **`ssh-keygen`**.

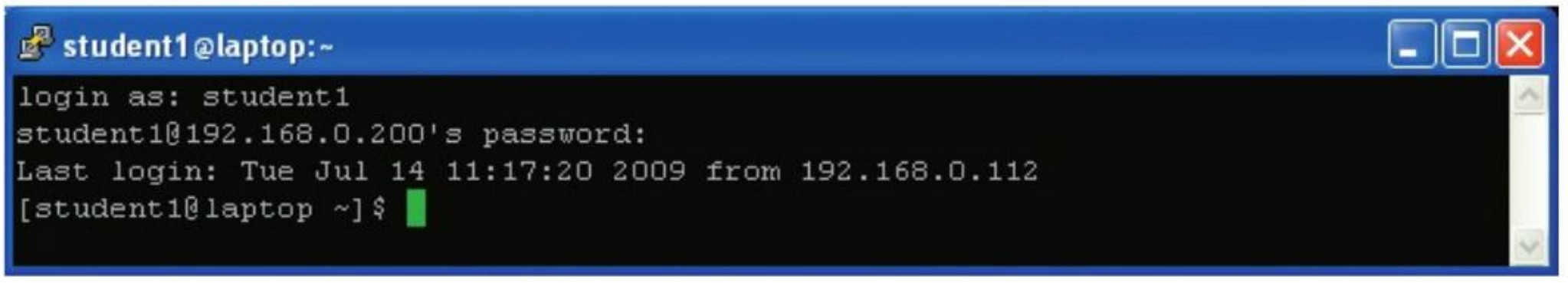
SSH pracuje w architekturze klient–serwer. Klient będzie mógł nawiązać połączenie z serwerem tylko wtedy, gdy administrator uruchomi na serwerze usługę dostępu przez SSH. Oprogramowanie serwera standardowo nasłuchuje przychodzących połączeń od klientów w porcie 22 protokołu TCP. Klientem SSH może być program **PuTTY**, umożliwiający bezpieczny dostęp do powłoki (ang. *shell*) systemu operacyjnego.

Po uruchomieniu programu w oknie dialogowym wprowadza się dane serwera, z którym zamierza się nawiązać połączenie. W polu **`Host Name`** (rys. 73.1) wpisuje się nazwę komputera lub jego adres IP (np. **`192.168.0.200`**) i zaznacza wybór protokołu **`SSH`** (oraz sprawdza numer portu – powinien wskazywać 22). Po wpisaniu danych można wybrać przycisk **`Open`**.



Rys. 73.1. Okno konfiguracji programu PuTTY

Jeżeli wcześniej między komputerami nie nawiązano połączenia za pomocą PuTTY, to zostanie wygenerowana para kluczy służących do szyfrowania połączenia. W oknie informującym o tworzeniu kluczy należy wybrać przycisk **Tak**. W oknie (rys. 73.2) można się zalogować – trzeba podać identyfikator konta użytkownika, np. *student1*, i nacisnąć [Enter]. Po wpisaniu hasła użytkownika ponownie należy nacisnąć [Enter]. W czasie pisania hasła komputer nie wyświetla żadnych znaków – nawet gwiazdek (nie można policzyć wprowadzonych znaków).



Rys. 73.2. Logowanie za pomocą PuTTY

Po zalogowaniu można uzyskać dostęp do wszystkich usług dostępnych za pośrednictwem terminalu dla użytkownika, którego konto jest wykorzystywane.

Usługa SSH umożliwia funkcjonowanie innych usług pozwalających np. na bezpieczne przesyłanie danych. W systemach Unix/Linux do bezpiecznego kopiowania plików jest wykorzystywane polecenie **scp**. Dla systemu Windows została stworzona aplikacja **WinSCP**.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

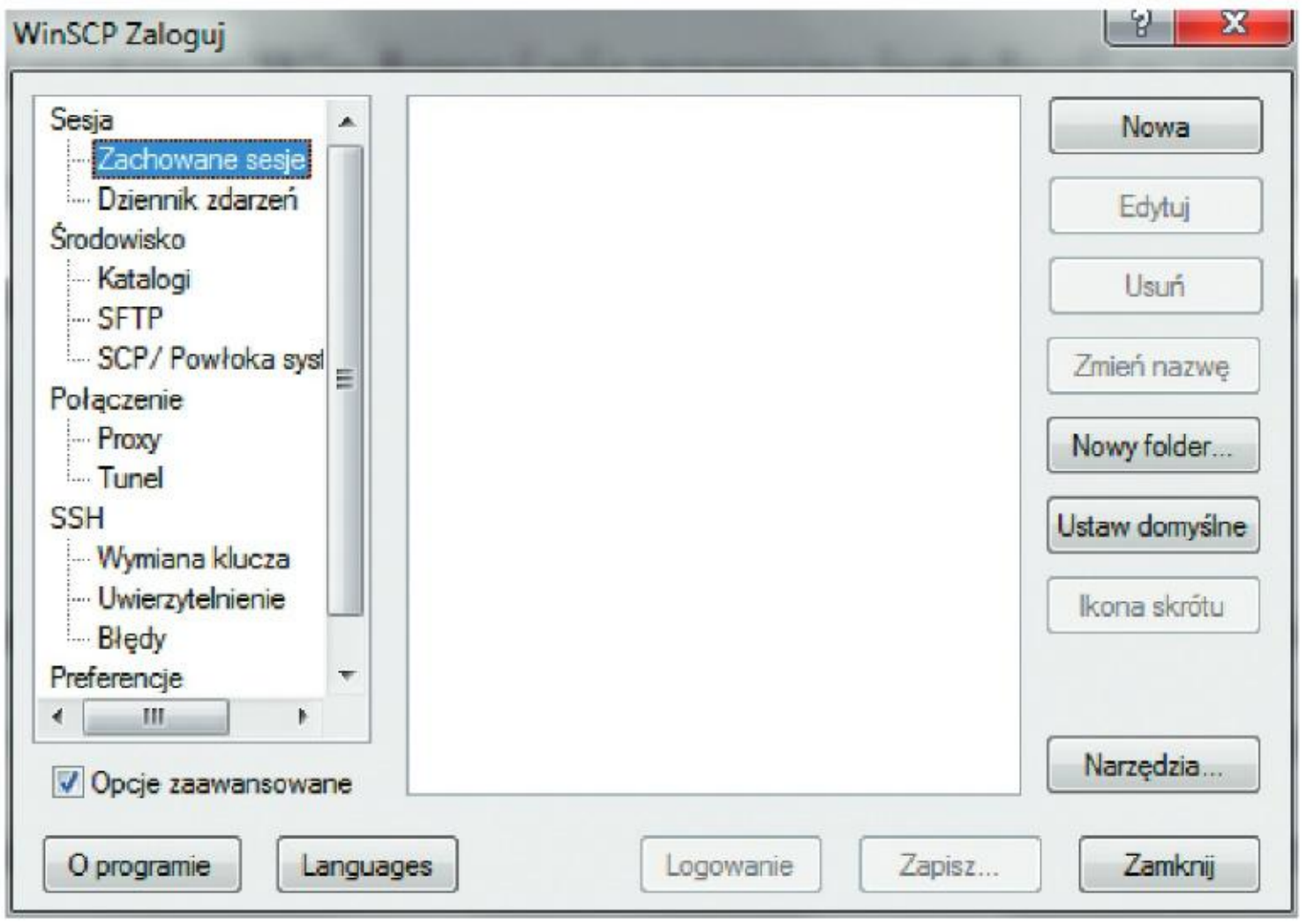
1. Za pomocą usługi SSH zaloguj się na szkolnym serwerze. Skorzystaj z indywidualnego konta, przydzielonego przez administratora.
2. Wyjaśnij, dlaczego korzystanie z SSH jest bezpieczniejsze niż korzystanie z telnetu.
3. Wyszukaj w internecie, np. na stronie www.download.net.pl w sekcji „Internet i komunikacja", informacje o programach – klientach usługi SSH.

74 Korzystanie z usługi bezpiecznego kopiowania plików

ZAGADNIENIA

- **Funkcja programu WinSCP**
- **Skonfigurowanie połączenia za pomocą programu WinSCP**
- **Zarządzanie plikami i folderami za pomocą WinSCP**

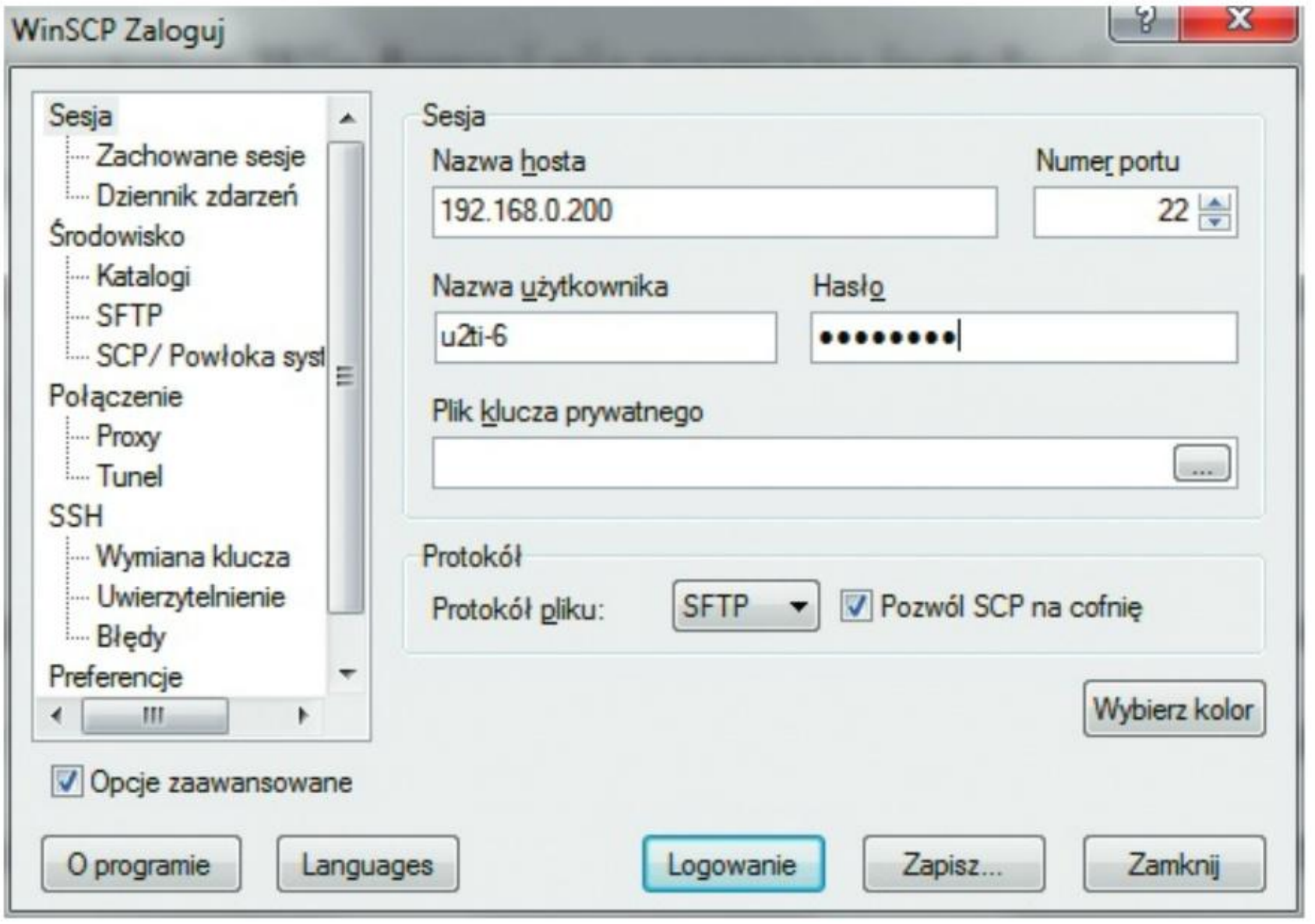
WinSCP jest programem umożliwiającym nawiązanie bezpiecznego połączenia z serwerem, zarządzanie plikami i folderami oraz ich przesyłanie między klientem a serwerem. Program WinSCP jest przeznaczony do systemu Windows i dostępny zarówno w wersji wymagającej instalacji w systemie, jak i w wersji bez konieczności instalacji (wersja portable). Program można bezpłatnie pobrać z internetu. Po skopiowaniu pliku należy go uruchomić. Po uruchomieniu programu wybieramy przycisk **Nowa**, aby utworzyć nową sesję połączenia (rys. 74.1).



Rys. 74.1. Otwieranie nowej sesji w programie WinSCP

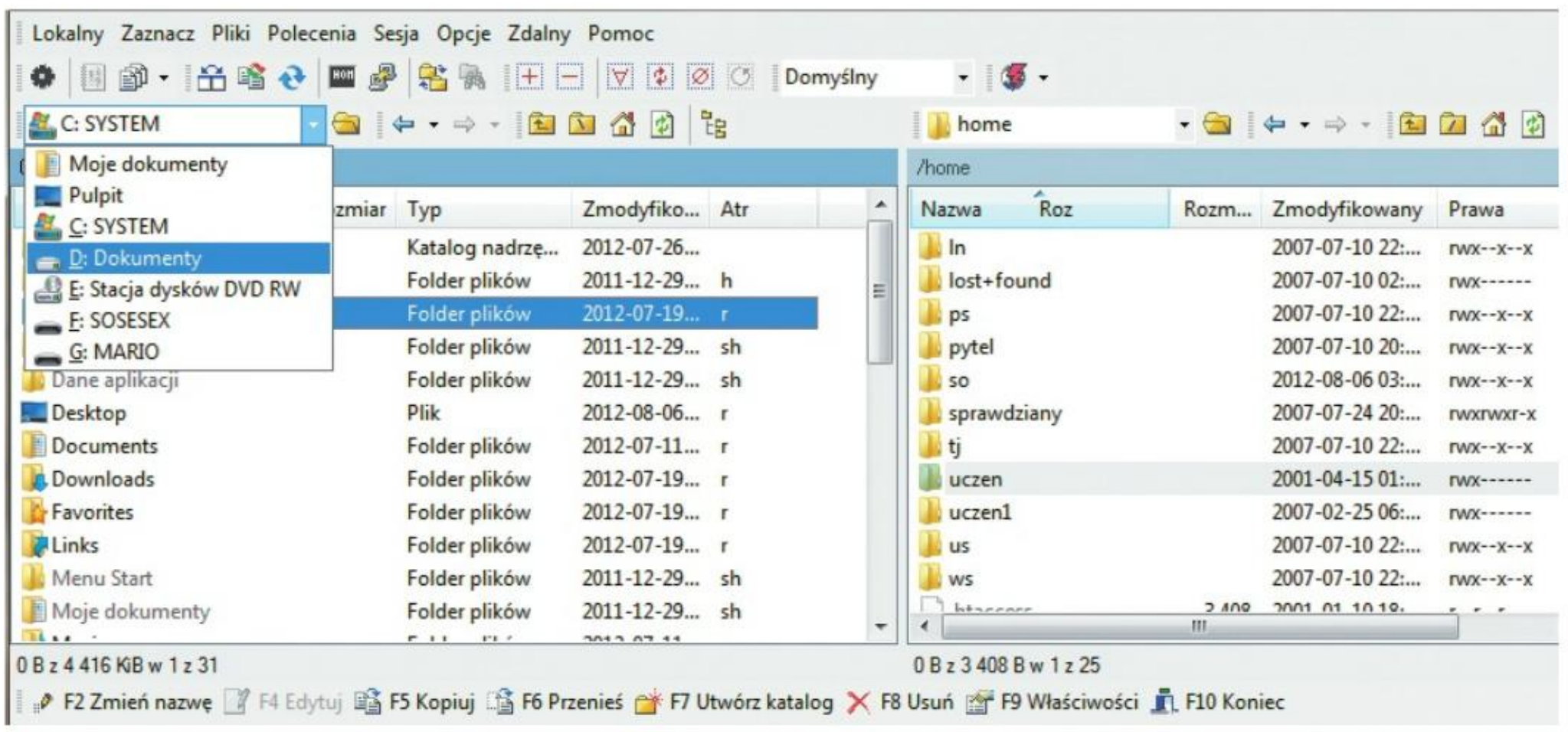
W oknie logowania (rys. 74.2) w polu **Nazwa hosta** wpisuje się adres lub nazwę serwera, w polu **Nazwa użytkownika** – nazwę konta użytkownika, a w polu **Hasło** – hasło odpowiednie dla nazwy konta użytkownika. Po naciśnięciu przycisku **Logowanie** nastąpi połączenie z serwerem.

Jeżeli połączenie jest nawiązywane po raz pierwszy, zostanie automatycznie wygenerowana para kluczy służąca do szyfrowania połączenia – jesteśmy informowani o tym za pomocą komunikatu. Wybranie opcji **Tak** spowoduje, że podczas kolejnych prób połączenia klucze nie będą generowane.



Rys. 74.2. **Konfiguracja połączenia w programie WinSCP**

Po nawiązaniu połączenia zostanie w lewym panelu pokazana zawartość dysku lokalnego, a w prawym – zawartość folderu domowego użytkownika. Operacje na plikach i folderach wykonujemy myszą, metodą „przeciągnij i upuść", lub za pomocą klawiszy funkcyjnych (ich znaczenie opisano w dolnej części ekranu). W celu zmiany dysku lokalnego należy wybrać pole wyboru dysku (rys. 74.3) i wskazać nowy dysk, którego zawartość ma być wyświetlona w lewym panelu.



Rys. 74.3. **Okno główne programu WinSCP**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Za pomocą programu WinSCP skopiuj na serwer dowolny plik.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Na czym polega praca przeglądarki internetowej w trybie offline?
2. Wymień zalety i wady anonimowego dostępu do FTP.
3. Wymień zalety i wady korzystania z klienta poczty elektronicznej

75 Sieć peer-to-peer, grupy robocze, udostępnianie folderów w grupie roboczej

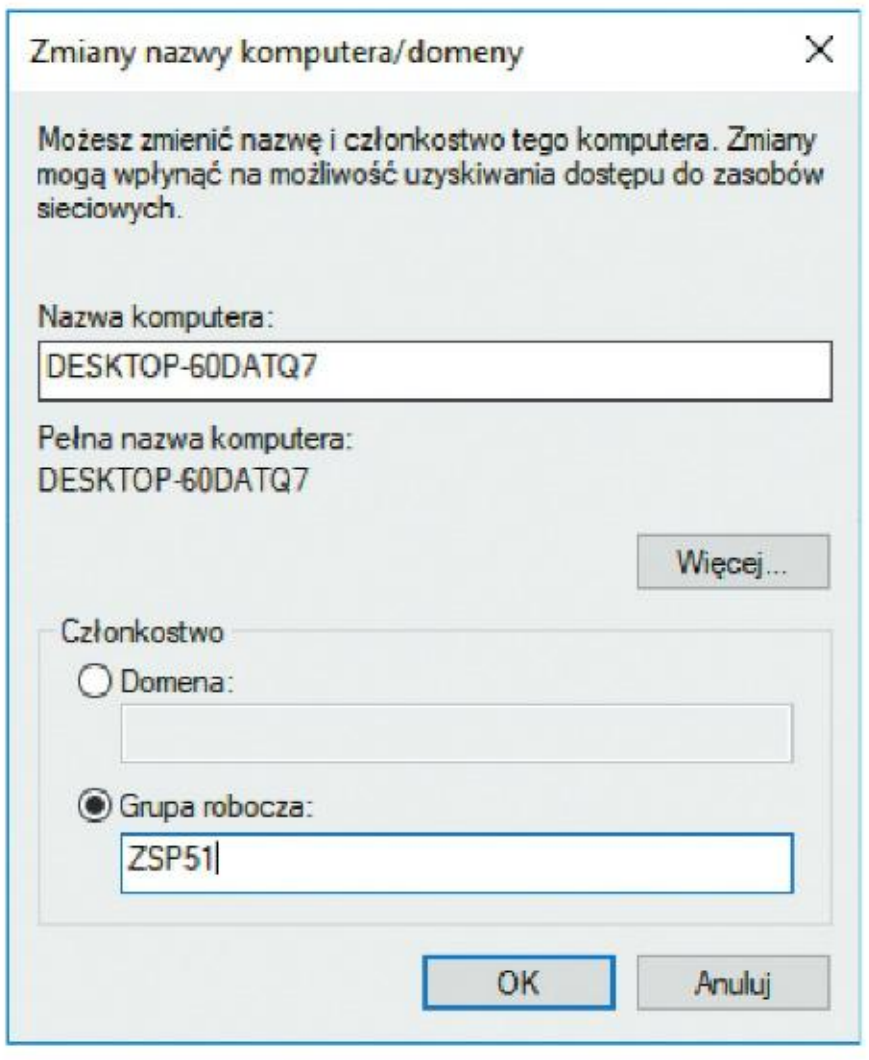
ZAGADNIENIA

- **Skonfigurowanie sieci peer-to-peer w oparciu na Windows 10**
- **Pojęcie grupy roboczej**
- **Udostępnianie zasobów komputera w grupie roboczej**

W **sieciach równorzędnych** (ang. *peer-to-peer*) każdy komputer pełni taką samą funkcję: może być klientem (korzystać z usług oferowanych przez inne urządzenia), serwerem (udostępniać usługi) lub jednocześnie klientem i serwerem. Komputery, które pracują w sieci niezapewniającej centralnej administracji zasobami, są zorganizowane w **grupy robocze**. Każdy komputer w grupie roboczej ma przechowywaną lokalnie własną bazę kont **SAM** (ang. *Security Account Manager*). W grupie roboczej nie obowiązuje zasada pojedynczego konta i pojedynczego logowania. Użytkownik musi mieć stworzone konto na każdym komputerze, do którego chce się zalogować.

Aby zmienić grupę roboczą, należy w oknie **`Start/Panel sterowania/System i zabezpieczenia/System`** wybrać odnośnik **`Zmień ustawienia`**. Następnie w zakładce **`Nazwa komputera`** w oknie **`Właściwości systemu`** – wybrać **`Zmień`** (rys. 75.1). Na koniec – zaznaczyć opcję **`Grupa robocza`**, wpisać nazwę grupy roboczej, np. **`ZSP51`**, i kliknąć przycisk **`OK`**. Zmiana grupy roboczej wymaga ponownego uruchomienia komputera.

Użytkownicy zarządzają swoimi komputerami i podejmują decyzje, które zasoby udostępnić i komu. Informacje o udostępnionych zasobach są przechowywane na lokalnym komputerze. Dzięki udostępnianiu zasobów użytkownicy tej samej sieci, mimo że pracują przy różnych komputerach, mogą uzyskać dostęp do zasobów, np. plików, folderów lub drukarek, jeżeli mają odpowiednie uprawnienia. Takie rozwiązanie stosuje się w małych sieciach.

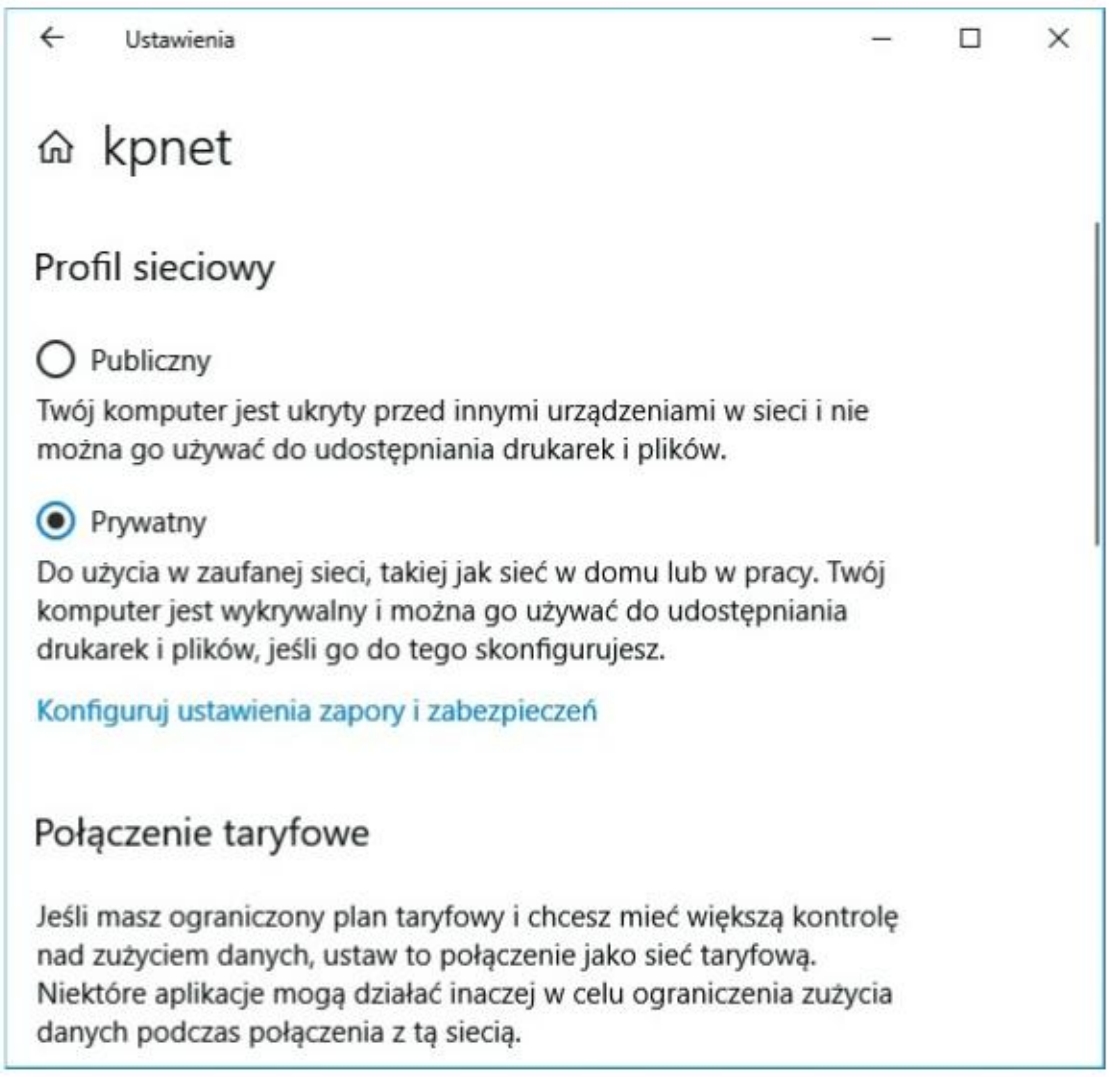


Rys. 75.1. **Zmiana grupy roboczej**

Udostępnianie zasobów, np. plików lub folderów to – potencjalnie – jedno z zagrożeń w sieci. Dlatego w systemach Windows stosuje się profile pozwalające na zapewnienie wymaganego poziomu zaufania do innych użytkowników:

- profil publiczny to zestaw ustawień komputera – głównie zapory sieciowej oraz mechanizmów wykrywania i udostępniania zasobów, tak aby zapewnić bezpieczeństwo komputera w miejscach publicznych;
- profil prywatny to zestaw ustawień komputera – głównie zapory sieciowej oraz mechanizmów wykrywania i udostępniania zasobów, tak aby komputer był bardziej dostępny w sieci prywatnej lub domowej.

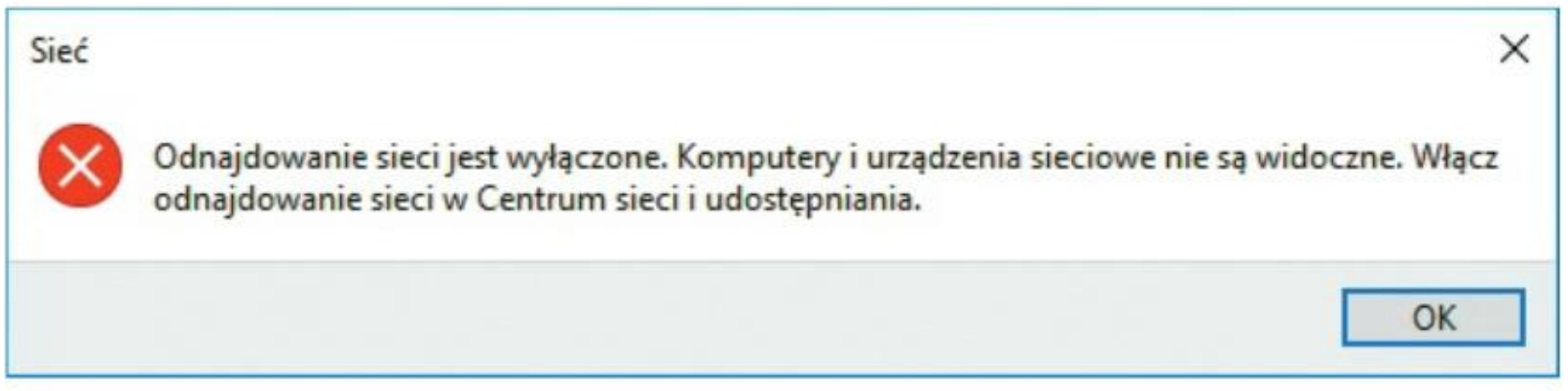
Ustawienia profilu sieciowego można zmienić dla poszczególnych połączeń sieciowych, np. dla zmiany profilu przewodowej karty sieciowej należy wybrać polecenia **Start/Ustawienia/Sieć i Internet/Ethernet/Połączenie sieciowe**. W oknie **Ustawienia** (rys. 75.2) trzeba zaznaczyć odpowiedni profil.



Rys. 75.2. **Wybór profilu sieciowego**

> **! UWAGA**
>
> Przed rozpoczęciem przeglądania zawartości sieci należy się upewnić, że komputery mają unikatowe adresy IP z tej samej podsieci, są połączone za pomocą medium komunikacyjnego i jest możliwa komunikacja między nimi, np. poleceniem **ping**. Komunikację między komputerami może blokować zapora sieciowa (jeżeli są problemy, należy ją skonfigurować lub wyłączyć na czas ćwiczeń, a po ich zakończeniu – ponownie włączyć).

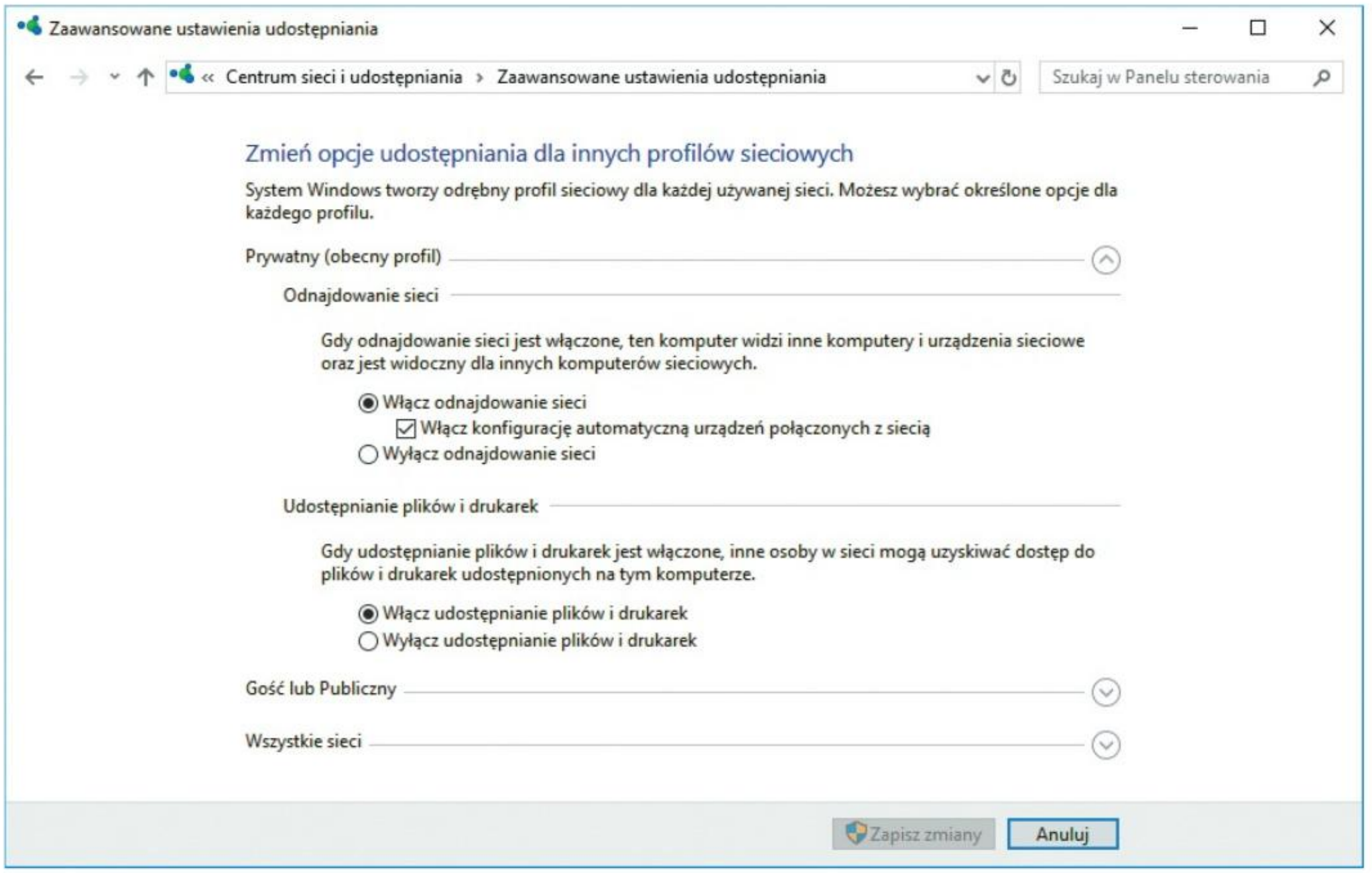
Przeglądanie zasobów udostępnionych w sieci peer-to-peer w systemie Windows jest realizowane za pomocą apletu **Sieć**, uruchamianego przez **Start/Ten komputer/Sieć**. Standardowo odnajdowanie sieci jest wyłączone, co uniemożliwia przeglądanie zawartości innych komputerów i blokuje innym użytkownikom możliwość przeglądania zawartości własnego komputera. Jeżeli po otwarciu apletu **Sieć** jest wyświetlany komunikat przedstawiony na rys. 75.3, należy włączyć odnajdowanie sieci.



Rys. 75.3. **Komunikat o wyłączeniu odnajdowania sieci**

Włączenie odnajdowania sieci staje się możliwe w oknie **Start/Panel sterowania/Sieć i Internet/Centrum sieci i udostępniania/Zaawansowane ustawienia udostępniania**, przedstawionym na rys. 75.4. W tym oknie należy wybrać odpowiedni profil

(obecny profil) i zaznaczyć opcję **Włącz odnajdowanie sieci**. Dodatkowo, jeżeli w sieci mają być udostępniane zasoby tego komputera, np. foldery i drukarki, należy zaznaczyć opcję **Włącz udostępnianie plików i drukarek**.



Rys. 75.4. Włączenie odnajdowania sieci i udostępniania zasobów

Do udostępnionego zasobu można przypisać uprawnienia:

- Odczyt;
- Zmiana;
- Pełna kontrola.

Jeśli partycja jest sformatowana w systemie plików z możliwością przydzielania uprawnień, np. NTFS, to do udostępnianego zasobu należy również nadać uprawnienia w systemie plików – dla wybranego użytkownika.

! UWAGA

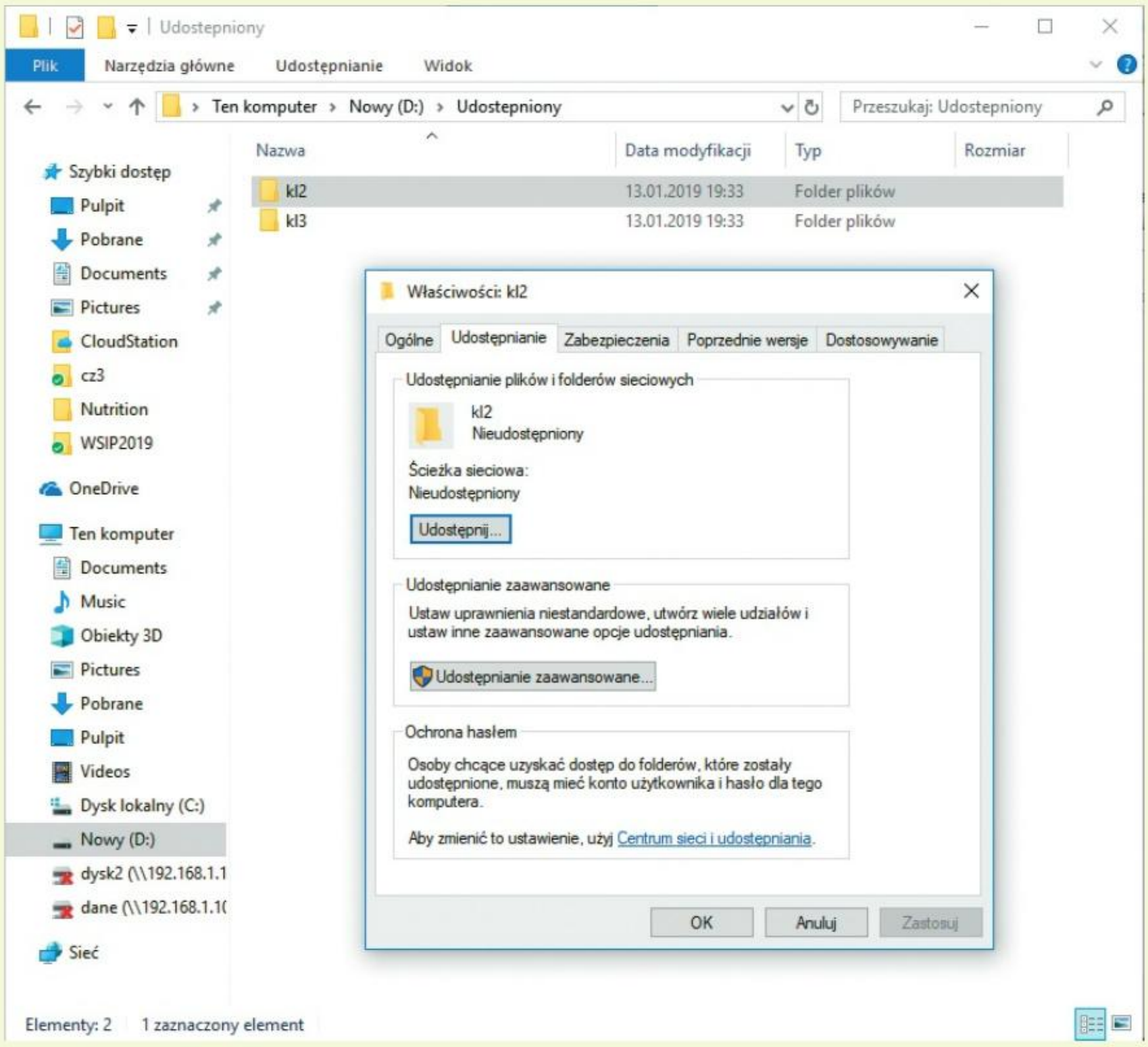
Uprawnienia efektywne użytkownika do udostępnianego w sieci zasobu wynikają z nałożenia się uprawnień udostępniania i uprawnień w systemie plików.

PRZYKŁAD 75.1

Udostępnianie folderu w sieci peer-to-peer

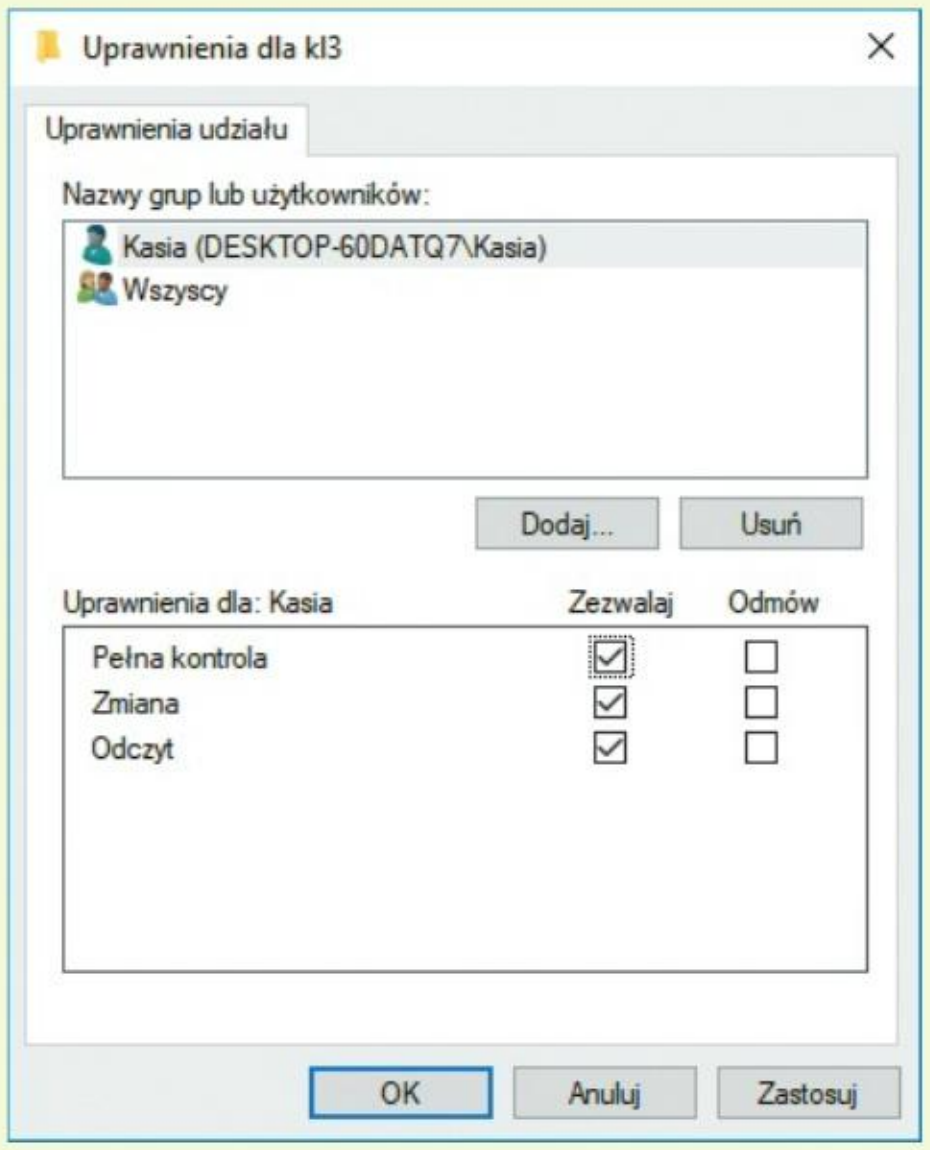
W tym ćwiczeniu zostaną udostępniony folder i skonfigurowane uprawnienia do tego folderu dla wybranego użytkownika. Przed rozpoczęciem udostępniania należy się upewnić, że komputery mogą się ze sobą komunikować. W celu udostępnienia folderu dla użytkownika należy:

1. Utworzyć użytkownika, np. *Kasia*, i podać hasło, np. **123**, w komputerze udostępniającym folder.
2. Utworzyć udostępniany folder, np. **kl2**.
3. Kliknąć prawym klawiszem ikonę folderu i z menu podręcznego wybrać **Właściwości**.
4. Wybrać zakładkę **Udostępnianie** i kliknąć przycisk **Udostępnianie zaawansowane** (rys. 75.5).

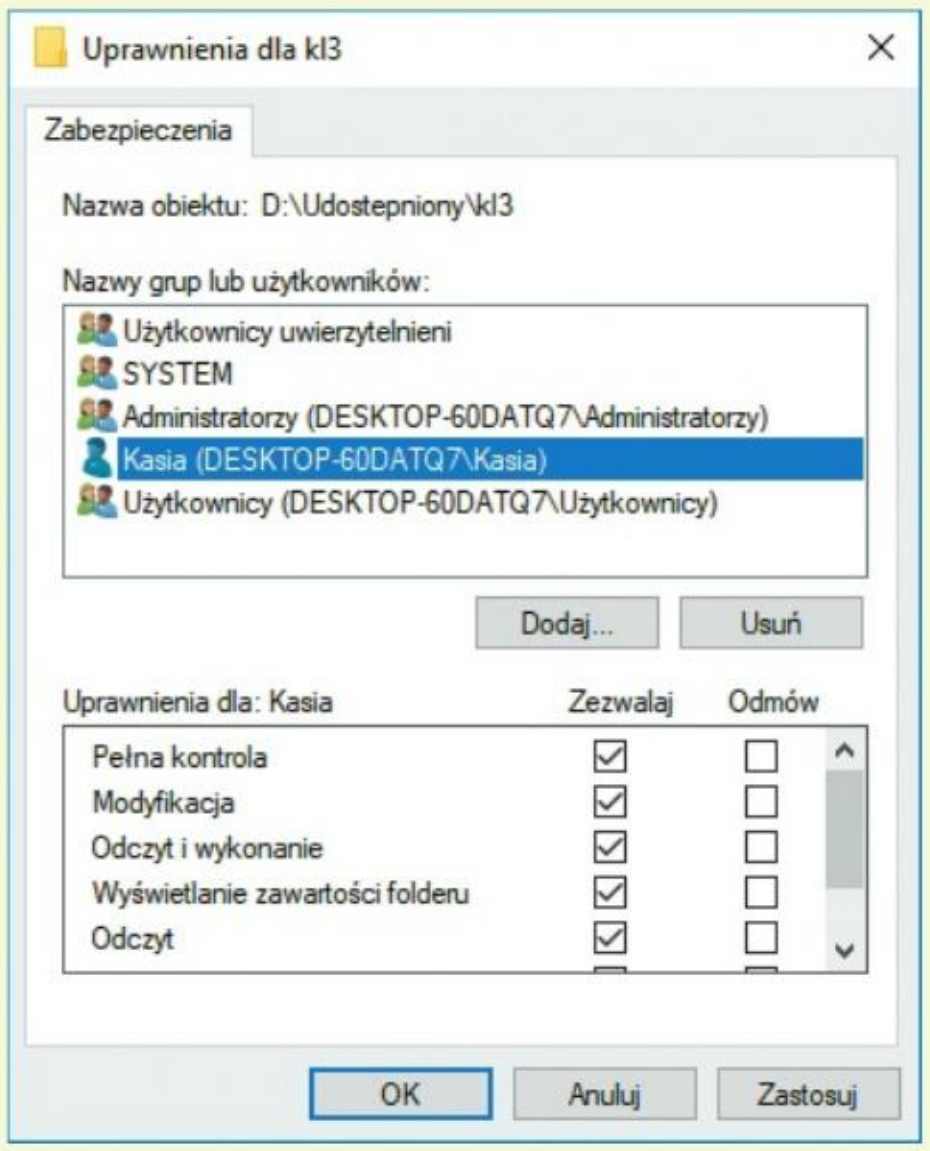


Rys. 75.5. **Wybór opcji udostępniania zaawansowanego**

5. W oknie **Udostępnianie zaawansowane** zaznaczyć opcję **Udostępnij ten folder** i kliknąć przycisk **Uprawnienia**.
6. Wybrać użytkownika, np. *Kasia*, i przydzielane uprawnienia, np. **Pełna kontrola** (rys. 75.6). Kliknąć przyciski **Zastosuj** i **OK**, aby zamknąć okno **Uprawnienia**, i ponownie przyciski **Zastosuj** i **OK**, aby zamknąć okno **Udostępnianie zaawansowane**.
7. Wybrać zakładkę **Zabezpieczenia**, a następnie kliknąć przycisk **Edytuj**... i wskazać użytkownika, np. *Kasia*, w oknie **Uprawnienia** (rys. 75.7). Przydzielić w systemie plików uprawnienia, np. **Pełna kontrola**. Kliknąć przyciski **Zastosuj** i **OK**, aby zamknąć okno **Uprawnienia**, i ponownie przyciski **Zastosuj** i **OK**, aby zamknąć okno **Właściwości**.



Rys. 75.6. **Nadanie użytkownikowi uprawnień do folderu udostępnianego**



Rys. 75.7. **Nadanie użytkownikowi uprawnień do folderu w systemie plików**

! UWAGA

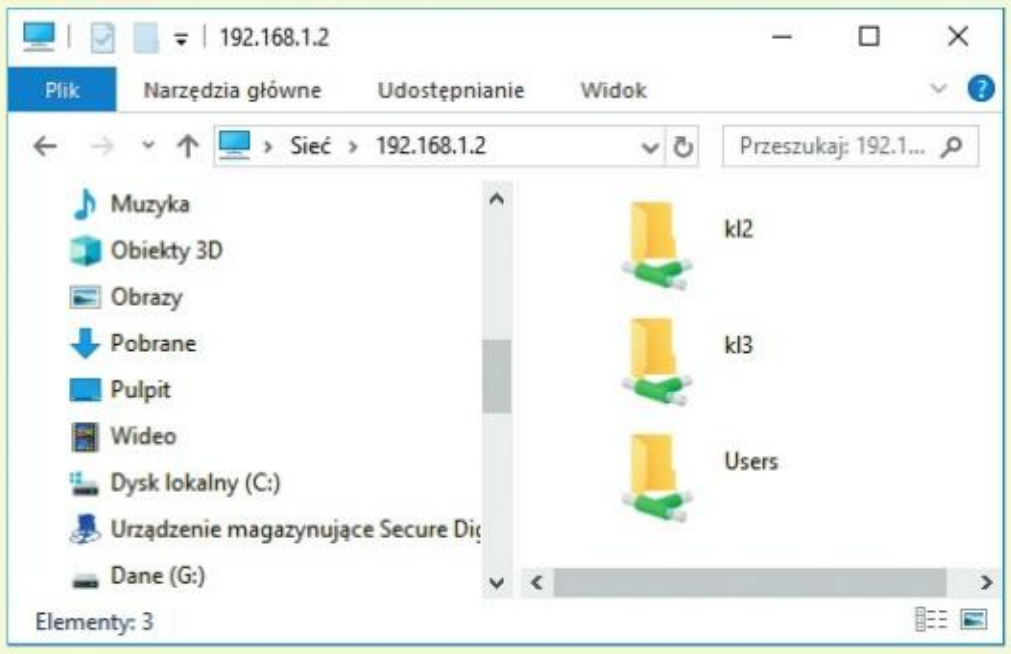
Nie jest to jedyna metoda udostępniania folderu, ale ta procedura oferuje najwyższy stopień kontroli parametrów udostępniania.

PRZYKŁAD 75.2

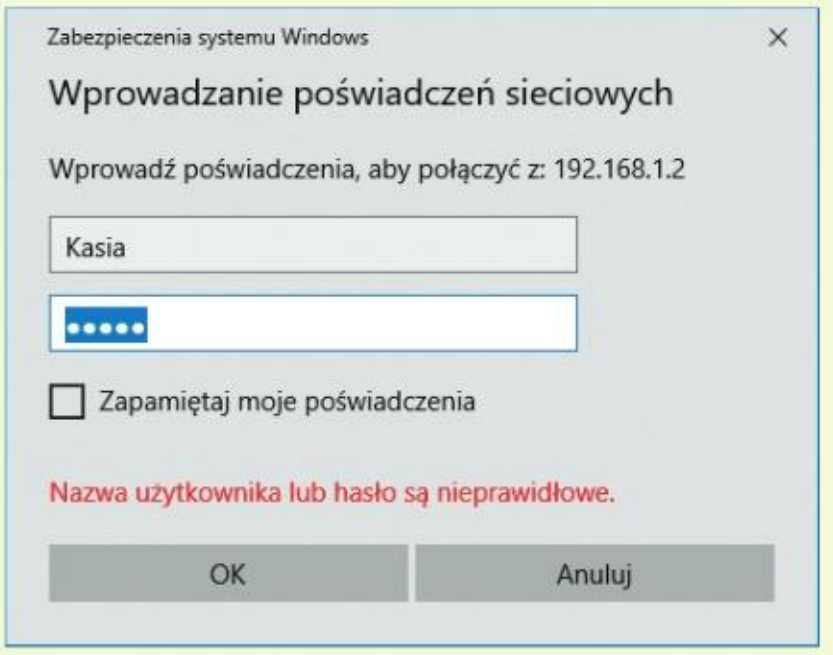
Uzyskiwanie dostępu do udostępnianego folderu w sieci peer-to-peer

W tym ćwiczeniu uzyskamy dostęp do folderu udostępnionego w innym komputerze. Przed rozpoczęciem udostępniania należy się upewnić, że nasz komputer i tamten mogą się komunikować. W celu uzyskania dostępu do udostępnionego folderu należy:

1. Uruchomić **`Eksplorator plików`** poleceniem **`Start/Eksplorator plików`**.
2. W polu ścieżki do zasobu wpisać **`\\adres IP\`**, np. **`\\192.168.1.2\`**. Inną możliwością jest przeglądanie udostępnianych zasobów po kliknięciu w kolejne obiekty w oknie **`Sieć`**.
3. Jeżeli system tego zażąda – wprowadzić nazwę konta użytkownika posiadającego uprawnienia do zasobu i hasło (rys. 75.9).



Rys. 75.8. **Przeglądanie udostępnionych zasobów**



Rys. 75.9. **Wprowadzanie danych uwierzytelniania użytkownika folderu udostępnianego**

4. Zaznaczyć opcję **`Zapamiętaj moje poświadczenia`**, co pozwoli na zapamiętanie w systemie danych i podczas ponownego podłączania do folderu nie trzeba będzie ich ponownie wprowadzać.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zaplanuj system współdzielonych folderów wykorzystywanych w twojej szkole do wymiany plików między nauczycielami a uczniami.
2. Zaimplementuj rozwiązanie zaproponowane w zadaniu 1. Sprawdź, czy wszyscy użytkownicy mogą korzystać z właściwych folderów i czy mają właściwe uprawnienia.

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 address	die Sendeadresse
adres sieci	IP – Internet Protocol Address	IP-Adresse
aktualizacja	update	die Aktualiesierung
architektura klient–serwer	client-server model	das Klient-Server-Modell
architektura równorzędna	peer-to-peer model	das Parallele Model
archiwizacja	data archiving	die Datenversicherung / die Archivierung
ataki aktywne	active attacks	die aktive Angriffe
ataki pasywne	passive attacks	die passive Angriffe
bezprzewodowa sieć lokalna, WLAN	Wireless Local Area Network	Wireless Local Area Network
bezprzewodowy	wireless / cordless	drahtlos / schnurlos
bit	bit	der Bit
brama sieciowa	network gateway	das Gateway
bramka VoIP	Voice over IP gate	das Voice over IP – Tor
chłodzenie	cooling	die Kühlung
częstotliwość	frequency	die Frequenz / die Häufigkeit
czytnik książek elektronicznych	electronic book reader	Ebook-Reader
defragmentacja	defragmentation	die Defragmentierung
dekapsulacja	decapsulation	die Dekapsulation
demon	daemon	der Dämon
diagnostyka	diagnostics / diagnostic testing	die technische Überprüfung
domena	domain	das Domäne
dokumentacja	documentation	die Dokumentation
dokumentacja techniczna	technical documentation	die technische Dokumentation
domena kolizyjna	collision domain	die Kollisionsdomäin
domena rozgłoszeniowa	broadcast domain	die Übertragungsdomäne
domeny najwyższego poziomu	top-level domains	die Domäne oberster Stufe
dostawca usługi internetu, ISP	Internet Service Provider	der Internet-Dienstanbieter

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
drukarka	printer	der Drucker
drukarka lokalna	local printer	der Lokaler Drucker
drukarka sieciowa	network printer	die Netzwerkdrucker
dysponent	network administrator, trustee	der Anweisungsbefugte / der Netwerk administrator
dysk sieciowy	network drive	das Netzlaufwerk
dysk twardy	hard disk	die Festplatte
eksploatacja	operation / utilization / exploitation	der Betrieb / die Nutzung
enkapsulacja	encapsulation	die Ummantelung / die Kapselung
ergonomia	ergonomics	die Ergonomie
formatowanie	formatting	die Formatierung
fragmentacja	fragmentation	die Frarmentierung
głośnik	speaker	der Lautsprecher
główne serwery nazw	DNS – Domain Name System	das Domänennamesystem
główny punkt dystrybucyjny, MDF	Main Distribution Facility	das Hauptabsatzkanal
gniazdo	socket	die Buchse / die Steckdose
gospodarowanie odpadami	waste management	die Abfallwirtschaft
grupa robocza	work group	die Arbeitsgruppe
grupy dyskusyjne	discussion groups	die Diskusionsgruppe
host	host	der Host
instalacja	installation	die Installation
interfejs równoległy	parallel interface	die parallele Schnittstelle / das parallele Interface
interfejs szeregowy	serial interface	die serielle Schnittstelle / das serielle Interface
jasność	brightness	die Helligkeit
jednostka centralna	CPU – Central Processing Unit	die Zentraleinheit
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
karta graficzna	graphics card / GFX	die Grafikkarte
karta sieciowa	network interface controller / adapter / card	die Netzkarte
karta muzyczna	sound card	die Musikkarte
karta pamięci	memory card	die Speicherkarte
karta rozszerzeń	expansion card	die Erweiterungskarte / die Stedkarte

WYKAZ PODSTAWOWYCH POJĘĆ W JĘZYKACH: POLSKIM, ANGIELSKIM I NIEMIECKIM

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
katalog nakładów rzeczowych	unit pricing / material outlays catalog	der Sachaufwendungskatalog
klawiatura	keyboard	die Tastatur
klient	client	der Kunde / der Benutzer
klucz rejestru	registry key	der Registrierungsschlüssel
komputerowy system sieciowy	network computer system	das Netzwerk – Computer – System
kolejka drukowania	print queue	die Druckerwarteschlange
koncentrator	hub	der Hub
kondensator	condenser	der Kondensator
konto użytkownika	user account	das Benutzerkonto
kontroler	controller	der Controller / das Stenergerät
kontroler domeny	domain controller	der Domänen-controller
kopia pełna	full copy	die volständige Sicherung
kopia przyrostowa	incremental copy	die volständige Sicherung
kopia różnicowa	differential copy	die inkrementelle Sicherung
kopia zapasowa	backup copy	die Sicherungsdatei / die Sicherheits-kopie / die Datensichenng
kosztorys	estimated budget / cost estimation	die Berechnung / der Kostenvoranschlag
lista kontroli dostępu, ACL	Access Control List	die ACL (Zugriffsstenerungsliste)
lista zgodności sprzętu, HCL	Hardware Compatibility List	die Hardware Kompatibilitätsliste
logowanie	login	die Anmeldung
lokacja	location	der Standort / die Lokation
łącze komunikacyjne	communication link	die Kommunikationsverbindung / der Kommunikationslink
łączność bezprzewodowa	Wi-Fi	Wi-Fi (Drahtlose Übermittlung)
macierz	matrix / array	die Matrix
magistrala	main / bus	der Bus
mapowanie dysków	disk mapping / drive mapping	die Laufwerkzuordnung
maska podsieci	subnet mask / IPv4 subnetting reference	die Subnetzmaske
materiał eksploatacyjny	operation material / consumable	das Betriebsmaterial
matryca	matrix	die Matrize
mechanizm PnP	Plug and Play mechanism	der PnP Mechanismus
medium transmisyjne	transmission medium	das Übertragungsmedium
mikser	mixer	der Mixer
moc	power	die Stärke
model hierarchiczny sieci	hierarchical network model	das hierarchische Netzwerkmodell
modem	modem	das Modem

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
modernizacja	modernization	die Modernisierung
moduł	module	das Modul
monitor	monitor / screen	der Bildschirm
montaż	assembly	die Montage
most	bridge	die Brücke / der Bus
mostek północny	northbridge	die Northbridge
mostek południowy	southbridge	die Southbridge
mysz	mouse	die Maus
nadmiarowość	redundancy	die Redundanz
nagłówek IP	IP header	IP-Überschrift
napięcie	voltage	die Spannung
napęd optyczny	optical drive	das optische Laufwerk
natężenie	intensity	die Stärke
netykieta	netiquette	die Netiquette
nośnik	medium	der Träger
obciążenie	load / encumbrance / overload	die Belastung
obiekt	object	das Objekt
obudowa	case / tower	das Gehäuse
odległość ogniskowa	focal length	die Brennweite
odzyskiwanie danych	data recovery	die Datenwiederherstellung
okablowanie pionowe (wewnątrz budynku)	vertical cabling	die Vertikale Verkabelung
okablowanie poziome	horizontal cabling	die Horizontale Verkabelung
okablowanie strukturalne	structural cabling	Struktivere / die gegliederte Verkabelun
oprogramowanie biurowe	office software	die Bürosoftware
oprogramowanie diagnostyczne	diagnostic software	die Diagnose-Software
oprogramowanie komunikacyjne	communication software	die Kommunikationssoftware
oprogramowanie monitorujące	monitoring software	die Überwachungssoftware
oprogramowanie narzędziowe	utility software	die Gebrauchssoftware
oprogramowanie użytkowe	application software	die Anwendungssoftware
opóźnienie urządzenia sieciowego	propagation delay	die Netzwerkgeraet-Verzögerung
pakiet	packet / suite (e.g. office suite)	das Paket
pamięć	memory	der Speicher
pamięć masowa	mass storage	der Massenspeicher
pamięć operacyjna	RAM – Random Access Memory	der Arbeitsspeicher RAM
pamięć ROM	Read-Only Memory	der ROM – Speicher
papier elektroniczny	electronic paper	elektronisches Papier

WYKAZ PODSTAWOWYCH POJĘĆ W JĘZYKACH: POLSKIM, ANGIELSKIM I NIEMIECKIM

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
partycja	partition	die Partition
partycja podstawowa	primary partition	primäre Partition
partycja rozszerzona	extended partition	erweitere Partition
plik stronicowania	paging file	die Auslagerungsdatei
planista	planner	der Planer
poczta elektroniczna	e-mail	elektronische Post
polityka bezpieczeństwa	information security policy	die Sicherheitspolitik
płyta główna	mainboard / motherboard	die Hauptplatine
pobór mocy	power consumption	die Leistungsaufnahme
pojemność	capacity	die Kapazität
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
podpis cyfrowy	digital signature	digitale Signatur
pośredni punkt dystrybucyjny, IDF	Intermediate Distribution Facility	der Indirekte Verteilungspunkt
prąd elektryczny	electric current	der elektrische Strom
priorytet	priority	das Priorität
proces	process	der Prozess
procesor	processor / CPU	der Prozessor
procesor graficzny	graphics processing unit	der Grafikprozessor
profil użytkownika	user profile	das Benutzerprofil
program antywirusowy	antivirus	das Antivirenprogramm
program szpiegujący	spyware	die Spyware
projekt	project	das Projekt
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
protokoły routingu	routing protocol	das Routingprotokoll
protokół IP	Internet Protocol	das IP – Internet Protokoll
protokół UDP	User Datagram Protocol	das UPD – Benutzer Datagramm Protokoll
protokół SNMP	Simple Network Management Protocol	das Simple Network Management Protokoll
protokół STP	Spanning Tree Protocol	das STP Protokoll

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
protokół TCP	Transmission Control Protocol	das Transmission Control Protokoll / das Übertragungssteue rungsprotokoll
protokół TFTP	Trivial File Transfer Protocol	das Transmission Control Protokoll
przekazywanie żetonu	token passing	die Token-Übermittlung
przełącznik	switch	der Umschalter
przewodowy	wired	Leitungs – drahtgebunden verd rahtet verkabelt
pulpit	desktop	die Arbeitsumgebung
punkt demarkacyjny	demarcation point	der Demarkationspunkt / der Grenzpunkt
punkt dostępowy	AP – Access Point	der Anschlusspunkt / die Anschlussstelle
punkt montowania	mount point	der Mount-Punkt / der Einhängepunkt
punkty rozdzielcze	distribution points	die Ausgabestellen
radiator	radiator	der Radiator / der Heizkörper
ramka	frame	der Rahmen
rejestr	registry	das Register; das Verzeichnis
rezystor	resistor	der Widerstand
router	router	der Router
rozdzielczość	resolution	die Auflösung
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	Personal Area Network	das Personale Netz
sieci lokalne LAN	Local Area Network	das Lokale Netz
sieci miejskie MAN	Metropolitan Area Network / Municipal Area Network	das Metropolraumnetz
sieci rozległe WAN	Wide Area Network	das Weitverkehrsnetz
skalowalność	scalability	die Skalierbarkeit
skaner	scanner	der Scanner
skrętka	twisted-pair cable	die Litze
sniffer	sniffer	der Sniffer / das Suchgerat
stanowisko pracy	workstation / workplace	der Arbeitsplatz
sterownik	driver	der Treiber

WYKAZ PODSTAWOWYCH POJĘĆ W JĘZYKACH: POLSKIM, ANGIELSKIM I NIEMIECKIM

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
styki	points / joints	die Verbindungsstellen
superdemon	super demon	der Superdämon
synchronizacja	synchronization	die Synchronisation
system informatyczny	IT system	das IT System (das Informations-technologische System)
system komputerowy	computer system	das Computersystem
system operacyjny	data bus	der Datenbus
system plików	file system	das Dateisystem
szum	noise	die Geräusche / das Gerausch
szyna danych	data bus	der Datenbus
ścieżka dostępu	path	der Pfad
ścieżka krytyczna	CPM – Critical Path Method	der kritische Pfad
średnica sieci komputerowej	network diameter	der Netzwerkdiameter
światłowód	fiber-optic cable / optical fibre	der Lichtleiter / die Lichtleitfaser
toner	toner	der Toner
Token Ring	Token Ring	der Token Ring
topologia sieci	network topology	die Netzwerktopologie
topologia fizyczna sieci	physical network topology	die Physikalische Topologie des Netzwerks
topologia logiczna sieci	logical network topology	die Logische Topologie des Netzwerks
tusz	ink	die Tinte
transmisja	transmission / broadcasting	die Übertragung
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-Ubertragung
transmisja w paśmie podstawowym	baseband transmission	Übermittlung im Basisfrequenzband / die Grundfrequenzband
transformator	transformer	der Transformator
układ sterujący	control system	das Steuerwerk; das Leitwerk
urządzenia dostępu	access device	die Zugangsgeräte
urządzenia transmisji	DCE – Data Communications Equipment	die Übertragungseinrichtung
urządzenia wzmacniania przesłanych sygnałów	signal booster device	das Signalverstärkungsgerät
urządzenie peryferyjne	peripheral (device)	das Peripheriegerät

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
urządzenie wielofunkcyjne	multifunction device	das Multifunktionsgerat
usługa APIPA	Automatic Private IP Addressing	die Automatische private IP Adresseirung
usługa DEP	Data Execution Prevention service	DEP-Dienst (Data Execution Prevention service)
usługa NAT	Network Address Translation	die NAT-Netzwerkadresseübersetzung
usługa SSH	Secure Shell Service	SS – Dienst (Secure Shell Service)
usługi katalogowe	directory service	der Katalogdienst
usterka	malfunction	die Panne, die; Funktionsstörung
wejście	input	der Eingang
węzeł sieci	node network	der Netzknoten
wentylator	fan / ventilator	der Lüfter / der Ventilator
wielodostępność	multi-user	das Mehrbenutzersystem
wielozadaniowość	multitasking	der Multitasking
wirtualna sieć lokalna, VLAN	Virtual Local Area Network	das Virtuelle Lokalnetzwerk
wirus komputerowy	virus	das Computervirus
współczynnik kompresji	compression rate	der Kompressionswert
wtyczka	plugin	das Modul
wyjście	output	der Ausgang
wykres Gantta	Gannt chart	das Gannt-Diagramm
wyświetlacz	display	das Display / die Anzeige
wzmacniacz	amplifier / booster	der Verstärker
wzmacniak, regenerator	repeater	der Repeater / der Verstärker
zapora sieciowa	firewall	die Firewall
zadanie drukowania	print job	der Druckerauftrag
zasilacz	feeder / power supply (unit)	das Netzteil / die Stromversorgung
zasilacz awaryjny UPS	Uninterruptible Power Supply	UPS – ungestörte / die ununterbrochene Stromversorgung
zasoby projektu	project resources	die Projekt-Ressourcen
zdalny	remote access	der Fernzugriff
złącze	joint / junction / socket	die Schnittstelle
znaki globalne	global signs	die Globalzeichen

Źródła ilustracji i fotografii

Okładka: (lokalne sieci komputerowe) Andrey Suslov/Shutterstock.com
Tekst główny: s. 10 (szafa stojąca) Signal, (szafa wisząca) Signati; s. 19 (kabel koncentryczny) Krzysztof Pytel/WSiP, (skrętka ekranowana) Krzysztof Pytel/WSiP, (skrętka nieekranowana) Krzysztof Pytel/WSiP, (kabel światłowodowy) Krzysztof Pytel/WSiP; s. 22 (modem) Netgear, (karta sieciowa) TP-Link, (router z punktem dostępowym) TP-Link, (bramka VoIP) GRANDSTREAM; s. 48 (wtyczka RJ-45) Eurokomp; s. 90 (gniazdo RJ-45) NEKU, (organizer kabli) NEKU, (panel krosowy) SLICAN, (kanał kablowy z zainstalowanymi gniazdami) AKS ZIELONKA; s. 108 (tablet graficzny) HUION; s. 132 (narzędzie uderzeniowe do montażu kabli) Delta, (narzędzie zaciskowe do wtyków RJ-45) Knipex; s. 133 (narzędzie do zdejmowania izolacji) Smart-Tel, (końcówka kabla SC) ULTIMODE, (końcówka kabla LC) RS PRO, (końcówka kabla ST) (RS PRO); s. 134 (pigtail) Delta, (spawarka do światłowodów) Fujikura; s. 218 (antena prętowa) Edimax, (antena Yagi-Uda) Abaks, (antena panelowa) Dipol, (antena paraboliczna) MaxLink; s. 330 (tester okablowania) Dipol, (urządzenie diagnostyczne do certyfikowania sieci) Keysight; s. 332 (reflektometr do okablowania miedzianego) BST Caltek Industrial Ltd., (miernik tłumienia optycznego) Dipol, (reflektometr optyczny) Exfo Universal; s. 334 (analizator sieci) IDEAL AnyWARE; s. 354 (mechaniczne złącze światłowodowe Fibrolok) 3M

Ilustracje: Roman Kirilenko, Dominik Krajewski/WSiP

Wydawnictwa Szkolne i Pedagogiczne oświadczają, że podjęły starania mające na celu dotarcie do właścicieli i dysponentów praw autorskich zamieszczonych utworów. Wydawnictwa Szkolne i Pedagogiczne, przytaczając w celach dydaktycznych utwory lub fragmenty, postępują zgodnie z art. 27^1 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.