DO NOWEJ PODSTAWY PROGRAMOWEJ

Kwalifikacja E.13

Projektowanie lokalnych sieci komputerowych i administrowanie sieciami

Podręcznik do nauki zawodu
technik informatyk

Barbara Halska, Paweł Bensel

Helion Edukacja

Podręcznik dopuszczony do użytku szkolnego przez ministra właściwego
do spraw oświaty i wychowania i wpisany do wykazu podręczników
przeznaczonych do kształcenie w zawodach technik informatyk i technik
teleinformatyk, na podstawie opinii rzeczoznawców: mgr. Marka Muszyńskiego,
mgr. inż. Grzegorza Śmigielskiego oraz dr Ewy Ogłozy.

Nazwa kwalifikacji: Kwalifikacja E.13. Projektowanie lokalnych sieci komputerowych
i administrowanie sieciami
Typ szkoły: technikum, szkoła policealna, kurs kwalifikacyjny
Rok dopuszczenia: 2013

Nr ewidencyjny w wykazie: 58/2013

Redaktor prowadzący: Tomasz Waryszak
Projekt okładki: Maciej Pasek

Materiały graficzne na okładce oraz wewnątrz książki zostały wykorzystane za zgodą
Shutterstock.

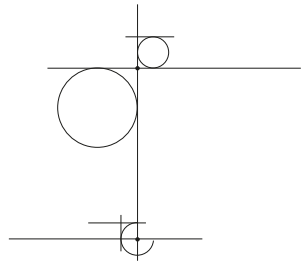
Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/e13men
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-246-7070-3

Printed in Poland.

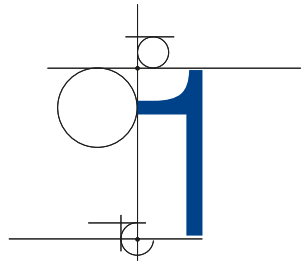
Spis treści



Wstęp

Podręcznik *Kwalifikacja E.13. Projektowanie lokalnych sieci komputerowych i administrowanie sieciami* omawia treści ujęte w nowej podstawie programowej. Jest przeznaczony dla szkół kształcących uczniów i słuchaczy w zawodzie technik informatyk. Treści zawarte w podręczniku mogą być z powodzeniem wykorzystywane również w przypadku innych kierunków kształcenia, a także przez osoby, które samodzielnie poszerzają swoją wiedzę z zakresu systemów operacyjnych z grupy Windows, Linux oraz sieci komputerowych.

W podręczniku duży nacisk został położony na praktyczne stosowanie zdobywanej wiedzy, co przekłada się na dużą liczbę opisanych instrukcji postępowania, które czytelnik może w łatwy sposób wykorzystać, pracując w systemie komputerowym.



Sieć komputerowa

Siecią komputerową nazywa się grupę komputerów lub innych urządzeń połączonych ze sobą za pomocą dowolnego medium transmisyjnego w celu wymiany danych lub współdzielenia zasobów, np.:

- korzystania ze wspólnych urządzeń peryferyjnych i sieciowych (skanera, drukarki),
- korzystania ze wspólnego oprogramowania,
- korzystania z centralnej bazy danych,
- przesyłania danych (jak poczta elektroniczna, pliki itp.).

1.1. Rodzaje sieci

Sieci komputerowe mogą być sklasyfikowane w zależności od sposobu dostępu do zasobów oraz ze względu na obszar działania.

DEFINICJA

W zależności od sposobu dostępu do zasobów rozróżnia się dwa rodzaje sieci:

Klient-serwer — sieć, w której znajduje się jeden centralny serwer udostępniający dane.

Peer-to-peer (sieć równoprawna) — sieć, w której wszystkie urządzenia są równoprawne.

Sieć typu *klient-serwer* jest siecią, w której znajduje się centralny komputer nazywany serwerem (jest to komputer, na którym zainstalowano odpowiednie usługi odpowiadające za udostępnianie zasobów, zarządzanie uprawnieniami czy kontami użytkowników).

Transmisja typu klient-serwer jest wykorzystywana także w przypadku wielu usług w Internecie. Przykładowo strony WWW są umieszczane na serwerach, z których są pobierane za pomocą przeglądarki internetowej.

Komputery pracujące w sieci *peer-to-peer* są równorzędne wobec siebie, tak jak ma to miejsce w przypadku *grupy roboczej* w systemie Windows, a więc nie ma centralnego komputera, który pełni funkcję serwera. Każdy z komputerów w takiej sieci może być

komputerem, który udostępnia usługę, jak i odbiorcą usług udostępnionych przez inne komputery takiej sieci.

DEFINICJA

Ze względu na obszar działania sieci komputerowej rozróżniane są sieci:

LAN (*ang. Local Area Network*) — sieć lokalna działająca na niewielkim, ograniczonym obszarze.

MAN (*ang. Metropolitan Area Network*) — sieć miejska (metropolitalna) działająca na większym obszarze, np. miasta Łódź — LODMAN.

WAN (*ang. Wide Area Network*) — sieć rozległa działająca na dużym obszarze, np. POLPAK-T.

Przykładem sieci lokalnej LAN jest sieć obejmująca swoim zasięgiem budynek szkoły. Najczęściej spotyka się sieci zbudowane z wykorzystaniem technologii *Ethernet*.

Sieciami rozległymi można nazwać sieci dużych firm łączące oddziały na terenie całego kraju. Mianem sieci rozległej określamy również internet, który swoim zasięgiem obejmuje cały świat. Tego rodzaju sieci korzystają z wielu technologii transmisji na dalekie odległości, takich jak *Frame Relay*, *ATM*, *DSL*.

2

Topologie sieci

Topologie sieci lokalnych mogą być opisane zarówno na płaszczyźnie fizycznej, jak i logicznej. **Topologia fizyczna** określa organizację okablowania strukturalnego, **topologia logiczna** opisuje dostęp do medium fizycznego oraz reguły komunikacji, z których korzystają podłączone do sieci urządzenia. Obie płaszczyzny topologii są ściśle ze sobą powiązane.

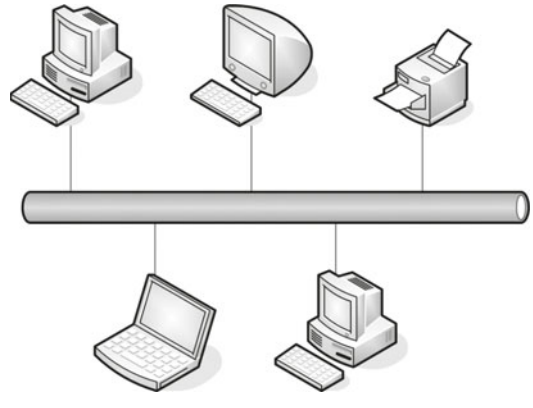
2.1. Topologie fizyczne

2.1.1. Topologia magistrali

DEFINICJA

W sieci zbudowanej w **topologii magistrali** (ang. *bus*) wszystkie elementy podłączone są do jednej wspólnej magistrali (zazwyczaj kabla koncentrycznego). Sieć umożliwia tylko jedną transmisję w danym momencie — sygnał nadany przez jedną ze stacji jest odbierany przez wszystkie pozostałe, lecz tylko adresat go interpretuje (rysunek 2.1).

Rysunek 2.1.
Topologia magistrali



Końce magistrali są wyposażone w tzw. terminatory (rysunek 2.2), których zadaniem jest wyeliminowanie odbicia sygnału od końca kabla. Odbicia te zakłócają, a nawet uniemożliwiają komunikację w sieci.

Rysunek 2.2. Terminator (wersja przeznaczona do stosowania z cienkim kablem koncentrycznym)

Maksymalna długość segmentu:

- cienki koncentryk (10Base2) — 185 m,
- gruby koncentryk (10Base5) — 500 m,
- IOBroad36 — 1800 m.

Maksymalna przepustowość łącza to 10 Mb/s.

Do zalet sieci budowanych w topologii magistrali należą: brak dodatkowych urządzeń sieciowych, takich jak koncentratory i przełączniki, spora odległość pomiędzy węzłami oraz użycie niewielkiej ilości kabla i niska cena instalacji sieci (węzły łączy pojedynczy kabel). Wśród wad trzeba wymienić często występujące kolizje, kłopotliwość lokalizacji usterek, możliwość przeprowadzenia tylko jednej transmisji w danym momencie oraz zagrożenie potencjalnym unieruchomieniem całej sieci za sprawą awarii głównego kabla lub nawet rozpięcia dowolnego złącza.

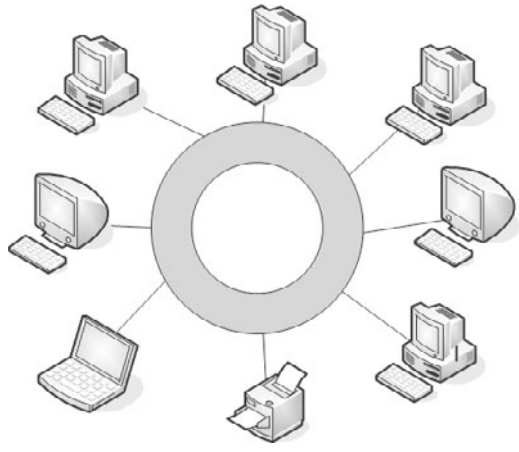
2.1.2. Topologia pierścienia

DEFINICJA

W sieci zbudowanej w **topologii pierścienia** (ang. *ring*) wszystkie węzły lub elementy połączone są za pomocą jednego nośnika w układzie zamkniętym — okablowanie tworzy krąg, nie występują zakończenia okablowania (rysunek 2.3). Stosowane są też metody podwójnych pierścieni (główny i dublujący). Sygnał wędruje w pętli między komputerami. Każdy komputer pełni funkcję wzmacniacza regenerującego sygnał i wysyłającego go dalej. Przykładem topologii podwójnego pierścienia jest **FDDI** (ang. *Fiber Distributed Data Interface*). Sieć w topologii pierścienia tworzona jest za pomocą kabla koncentrycznego lub światłowodu.

Zaletami sieci w topologii pierścienia są: użycie niewielkiej ilości przewodów, elastyczność w zakresie odległości pomiędzy węzłami sieci (w zależności od rodzaju wybranego medium). Wadą jest łatwość uszkodzenia sieci (uszkodzenie jednego węzła powoduje zatrzymanie transmisji w całej sieci), trudności w lokalizacji uszkodzeń, a także utrudniona rozbudowa sieci.

Rysunek 2.3.
Topologia pierścienia

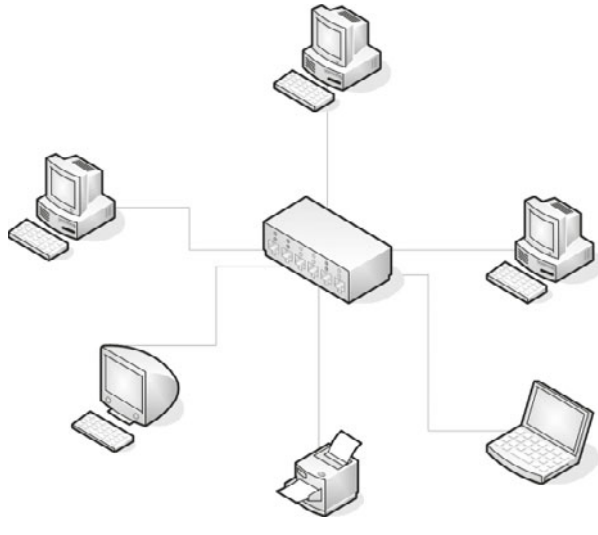


2.1.3. Topologia gwiazdy i gwiazdy rozszerzonej

DEFINICJA

Topologia gwiazdy (ang. *star*) charakteryzuje się tym, że okablowanie sieciowe (skrętka) łączy elementy sieci w centralnym punkcie, którym jest koncentrator lub przełącznik (rysunek 2.4).

Rysunek 2.4.
Topologia gwiazdy



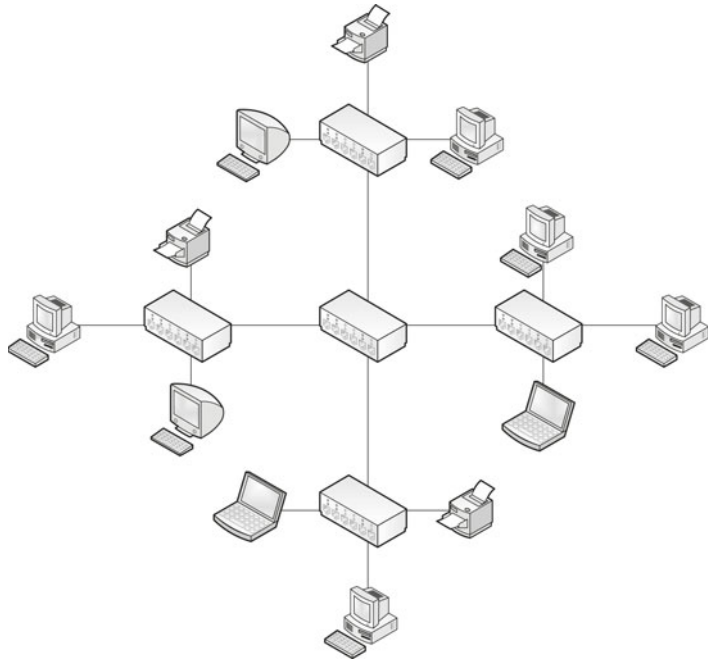
Topologie gwiazdy stały się dominujące we współczesnych sieciach LAN. Są elastyczne, skalowalne i stosunkowo tanie. Główną zaletą topologii gwiazdy jest to, że sieć może działać nawet wtedy, gdy jeden lub kilka komputerów ulegnie awarii, ponieważ każdy komputer jest połączony z centralnym urządzeniem (koncentratorem lub przełącznikiem). Podstawową wadą tego rozwiązania jest to, że w przypadku awarii centralnego

urządzenia cała sieć przestaje działać. Dzieje się tak dlatego, że cały ruch w sieci jest obsługiwany przez koncentrator lub przełącznik.

DEFINICJA

Topologia gwiazdy rozszerzonej (ang. *extended star*) jest oparta na topologii gwiazdy, w której gwiazdy połączone są między sobą za pomocą przełączników lub koncentratorów (rysunek 2.5). Ten rodzaj topologii pozwala na rozszerzenie zasięgu sieci i wzmocnienie sygnału między segmentami. Wadą takiej topologii jest wyższy koszt budowy związany z użyciem dodatkowych elementów sieciowych. Podobnie jak w topologii gwiazdy, wykorzystywana jest tutaj skrętka.

Rysunek 2.5.
Topologia
gwiazdy rozszerzonej



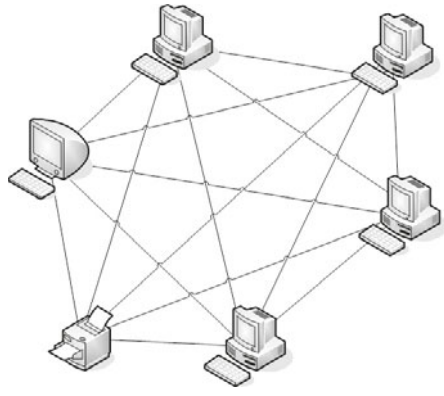
2.1.4. Topologia siatki

DEFINICJA

Topologia siatki (ang. *mesh*) polega na zapewnieniu wszystkim urządzeniom połączeń ze wszystkimi pozostałymi urządzeniami w sieci (rysunek 2.6). Oznacza to, że każdy host ma własne połączenie z pozostałymi.

Rozwiązanie topologii siatki jest bardziej złożone. Projekt takiej sieci polega na łączeniu ze sobą urządzeń w ten sposób, że każde z nich połączone jest z więcej niż jednym urządzeniem sieciowym. Zalety tego rozwiązania to wysoka prędkość transmisji oraz odporność na uszkodzenia. Wadami tego rozwiązania są wysokie koszty urządzeń sieciowych oraz okablowania, a także kłopotliwa rozbudowa.

Rysunek 2.6.
Topologia siatki

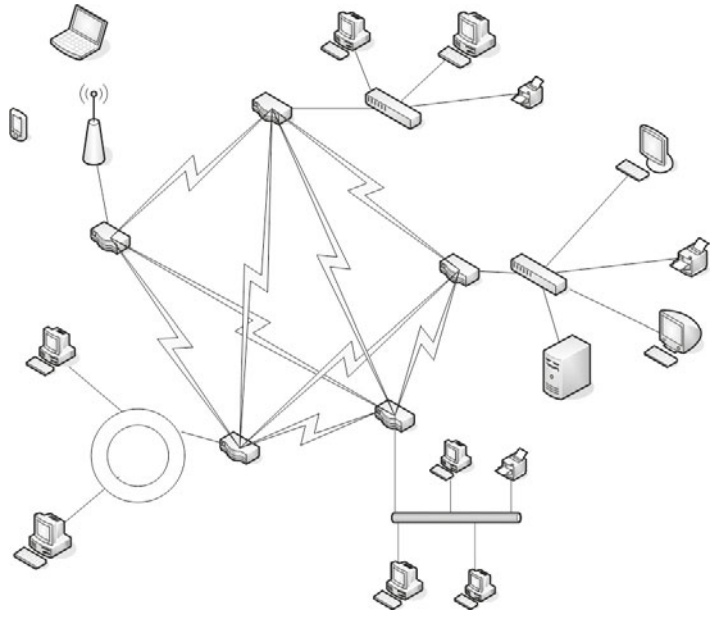


2.1.5. Topologia siatki mieszanej

DEFINICJA

Topologia siatki mieszanej (ang. *mixed mesh*) łączy w sobie różne rozwiązania — jest połączeniem co najmniej dwóch innych topologii z różnym rodzajem medium transmisyjnego (rysunek 2.7). Topologia sieci komputerowej tego typu jest stosowana w sieciach metropolitalnych oraz w sieciach rozległych (WAN).

Rysunek 2.7.
Topologia
siatki mieszanej



2.2. Topologie logiczne

Topologia logiczna opisuje metodę dostępu urządzeń sieciowych do medium transmisyjnego. Generalnie topologie logiczne są podzielone na:

- topologie rozgłaszania,
- topologie przekazywania żetonu (ang. *token*).

2.2.1. CSMA/CD

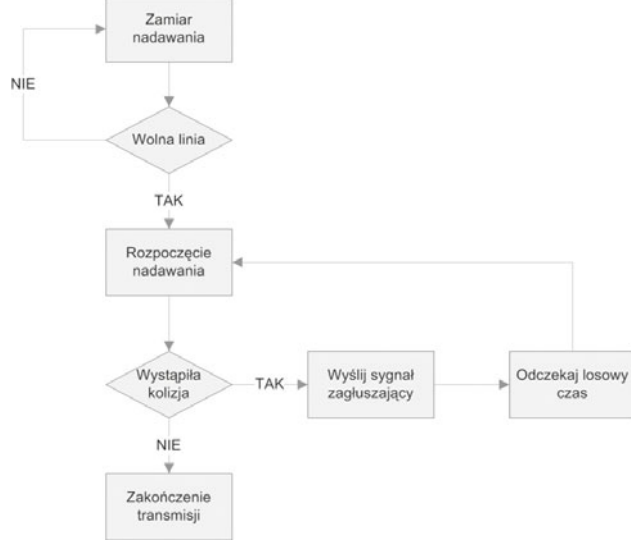
Dostęp do medium transmisyjnego w przypadku sieci Ethernet realizowany jest najczęściej przez protokół CSMA/CD (ang. *Carrier Sense Multiple Access/Collision Detection*), który jest przykładem topologii rozgłaszania. Protokół ten wykrywa, czy łącze jest dostępne, a także reaguje na występujące kolizje.

DEFINICJA

W sieci z protokołem CSMA/CD urządzenia przed nadawaniem sprawdzają, czy medium sieciowe nie jest zajęte. Jeśli węzeł wykryje, że sieć jest zajęta, będzie oczekiwał przez losowo wybrany czas przed ponowieniem próby. Jeśli węzeł wykryje, że medium nie jest zajęte, rozpocznie nadawanie i nasłuchiwanie. Celem nasłuchiwania jest upewnienie się, że żadna inna stacja nie nadaje w tym samym czasie. Po zakończeniu transmisji danych urządzenie powróci do trybu nasłuchiwania.

Jeśli dwa urządzenia rozpoczęły nadawanie w tym samym czasie, występuje kolizja, która jest wykrywana przez urządzenia nadawcze. Transmisja danych zostaje wówczas przerwana. Węzły zatrzymują nadawanie na losowo wybrany czas, po którym jest podejmowana kolejna próba uzyskania dostępu do medium (rysunek 2.8).

Rysunek 2.8. Algorytm blokowy działania mechanizmu CSMA/CD



Ta metoda transmisji jest wykorzystywana w sieciach Ethernet zbudowanych na bazie fizycznej topologii magistrali, gwiazdy, gwiazdy rozszerzonej oraz siatki.

2.2.2. Token

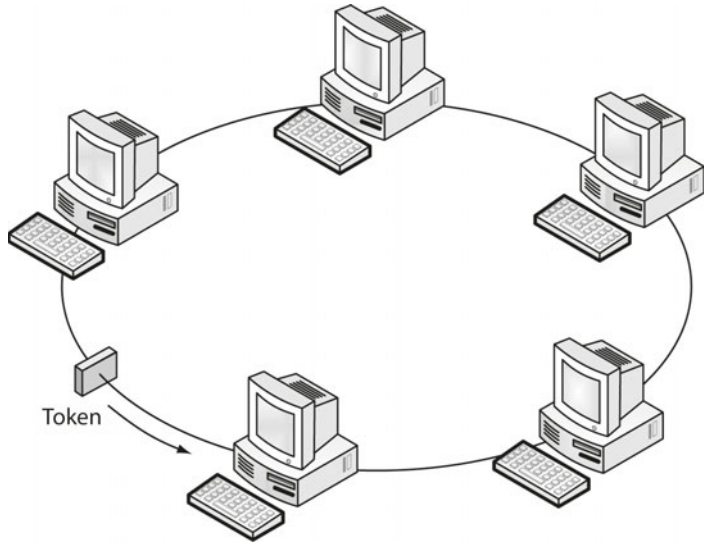
DEFINICJA

Dostęp do medium transmisyjnego jest realizowany przez przekazywanie żetonu. **Żeton** (ang. *token*) dostępu jest określoną sekwencją bitów zawierających informację kontrolną. Przejęcie żetonu przez urządzenie sieciowe zezwala na rozpoczęcie transmisji danych.

Każda sieć ma tylko jeden żeton dostępu przekazywany między kolejnymi węzłami sieci. Jeśli komputer ma dane do wysłania, usuwa żeton z pierścienia i rozpoczyna transmisję.

Dane wędrują po kolejnych węzłach sieci, aż trafią do adresata. Komputer odbierający wysyła do komputera nadającego komunikat o odebraniu danych. Po weryfikacji komputer wysyłający tworzy nowy żeton dostępu i wysyła go do sieci (rysunek 2.9).

Rysunek 2.9. Działanie mechanizmu tokenu



Ta metoda transmisji jest wykorzystywana m.in. w sieciach Token Ring oraz FDDI.

ĆWICZENIA

1. Sprawdź, jaka topologia fizyczna jest zastosowana w pracowni komputerowej.

PYTANIA

1. Opisz topologię magistrali. W jaki sposób uzyskuje się w niej dostęp do medium transmisyjnego?
2. W jakich sieciach wykorzystywany jest mechanizm przekazywania żetonu (tokenu)?
3. Scharakteryzuj topologię gwiazdy.

3

Medium transmisyjne

Medium transmisyjne to nośnik danych w sieciach komputerowych. Rodzaj medium transmisyjnego uzależniony jest od typu sygnałów przekazywanych przez niego. Wyróżnia się media przewodowe i bezprzewodowe.

Przewodowe media transmisyjne to:

- kabel symetryczny (w tym tzw. skrętka),
- kabel współosiowy (koncentryczny),
- kabel światłowodowy (światłowód — jednomodowy, wielomodowy),
- kable energetyczne.

Bezprzewodowe media transmisyjne to:

- fale elektromagnetyczne (fale radiowe),
- promień lasera.

3.1. Media przewodowe

3.1.1. Kabel koncentryczny

Kabel koncentryczny składa się z miedzianego przewodnika (rdzenia) otoczonego warstwą elastycznej izolacji, która z kolei otoczona jest splecioną miedzianą taśmą lub folią metalową działającą jak drugi przewód oraz ekran dla znajdującego się wewnątrz przewodnika. Ta druga warstwa lub ekran zmniejsza także liczbę zewnętrznych zakłóceń elektromagnetycznych (rysunek 3.1).

Rysunek 3.1. Budowa kabla koncentrycznego

Podłączenie urządzeń do sieci komputerowej zbudowanej przy użyciu kabla koncentrycznego umożliwiają łącza typu BNC (rysunek 3.2). Ten rodzaj okablowania jest wykorzystywany w sieciach budowanych w topologii pierścienia lub magistrali. Obecnie praktycznie nie stosuje się go w sieciach komputerowych. Maksymalna prędkość transmisji dla kabla koncentrycznego wynosi 10 Mb/s, a maksymalna długość sieci to 500 m.

Rysunek 3.2.
Wtyk typu BNC

W przypadku sieci komputerowych używane są dwa rodzaje kabli koncentrycznych:

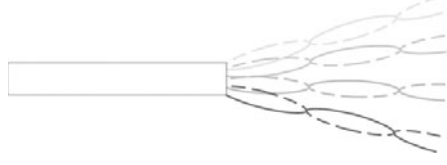
- gruby kabel koncentryczny 10Base5 (maksymalna długość segmentu 500 m),
- cienki kabel koncentryczny 10Base2 (maksymalna długość segmentu 185 m).

3.1.2. Kabel skręcany (Base-T)

Kabel skręcany (skrętka) składa się z zestawu 4 par żył miedzianych skręconych ze sobą. Skręcenie przewodów pozwala na wyeliminowanie zakłóceń elektromagnetycznych. Jest stosowany w topologii gwiazdy.

W skrętce każda żyła oznaczona jest osobnym kolorem: zielonym, pomarańczowym, niebieskim, brązowym oraz biało-zielonym, biało-pomarańczowym, biało-niebieskim, biało-brązowym (rysunek 3.3).

Rysunek 3.3.
Kabel typu skrętka



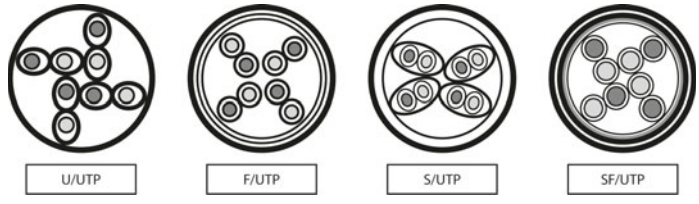
Żyły oznaczone kolorem jednolitym i analogicznym mieszanym (np. zielonym i biało-zielonym) stanowią skręconą parę. Całość skręconych par skręca się ponownie w celu wywołania efektu samoekranowania i w rezultacie zmniejszenia poziomu zakłóceń.

Ze względu na rodzaje stosowanego ekranowania wyróżnia się następujące kable typu skrętka (rysunek 3.4):

- U/UTP (ang. *Unshielded/Unshielded Twisted Pair*) — kabel skręcany nieekranowany. Stanowi najpopularniejszy środek transmisji danych, jest stosowany w pomieszczeniach.
- F/UTP (ang. *Foiled/Unshielded Twisted Pair*) — kabel skręcany ekranowany folią z przewodem uziemiającym. Stosuje się go na korytarzach lub na zewnątrz budynków.

- S/FTP (ang. *Shielded/Foiled Twisted Pair*) — kabel skręcany z ekranem wykonanym w postaci foliowego oplotu każdej pojedynczej pary i dodatkowo zewnętrznej siatki.
- SF/UTP (ang. *Shielded Foil/Unshielded Twisted Pair*) — kabel skręcany z podwójnym zewnętrznym ekranem w postaci foliowego oplotu i siatki.

Rysunek 3.4.
Rodzaje okablowania typu skrętka



Kabel typu skrętka podłączany jest do gniazd i końcówek typu RJ45 (złącze 8P8C, rysunek 3.5). Dodatkowe informacje na temat okablowania strukturalnego znajdują się w rozdziale 9. — „Projektowanie i wykonanie sieci komputerowych".

Rysunek 3.5.
Końcówka RJ45.

Maksymalna długość połączenia za pomocą kabla typu skrętka pomiędzy dwoma urządzeniami wynosi 100 m. Po przekroczeniu tej odległości należy użyć aktywnych urządzeń sieciowych w celu wzmocnienia sygnału.

3.1.3. Światłowód

Coraz większą popularność jako typ okablowania zdobywa **światłowód**. Jest to spowodowane przede wszystkim jego dużą przepustowością, odpornością na zakłócenia, możliwością transmisji na dalekie odległości (dla standardu 100-BaseFX do 2000 m).

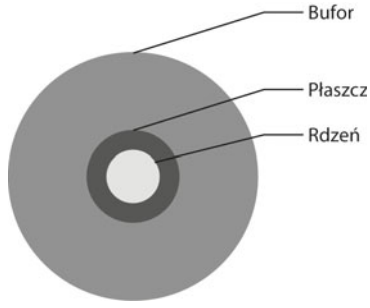
DEFINICJA

Najważniejszym elementem systemu światłowodowej transmisji danych jest światło, które może być emitowane przez:

- diody laserowe (ang. *laser diode* — LD),
- diody elektroluminescencyjne (ang. *light-emitting diode* — LED).

Światłowód składa się z płaszcza zewnętrznego (ochronnego), zbioru włókien, natomiast każde włókno to zbiór trzech elementów (rysunek 3.6):

- bufora,
- płaszcza,
- rdzenia.



Rysunek 3.6. Budowa światłowodu

WAŻNE

Promień świetlny, który trafia do rdzenia pod odpowiednim kątem, jest określany jako mod światłowodowy. Ze względu na liczbę równocześnie transmitowanych modów rozróżnia się światłowody:

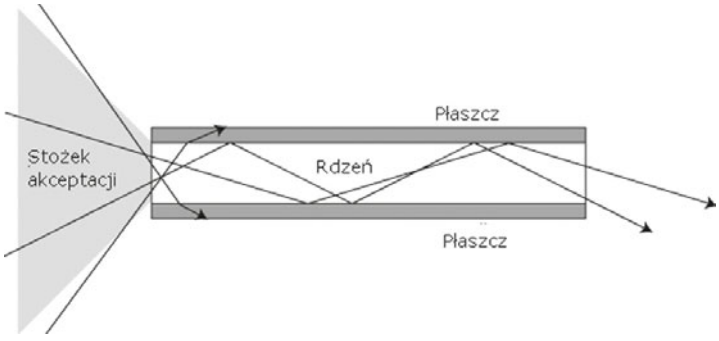
- jednomodowe — transmitujące jeden mod (promień) światła,
- wielomodowe — transmitujące wiele modów (promieni) światła.

Światło przenoszone przez włókna kabla światłowodowego zapewnia największą szybkość transmisji. Realizowana jest ona za pomocą „sygnału świetlnego", który propagowany jest we włóknach światłowodu. Sygnał przesyłany pomiędzy urządzeniami sieciowymi ulega zamianie na impuls świetlny przez nadajnik (ang. *optical transmitter*). Po dotarciu do celu jest odbierany przez odbiornik (ang. *optical receiver*), a następnie przekształcany na impuls elektryczny.

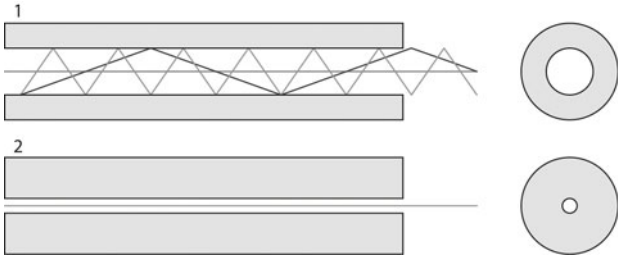
Propagacja sygnału świetlnego (rozchodzenia się) oparta jest na załamaniu (odbiciu). Proces transmisji przez światłowód rozpoczyna się od wprowadzenia pod odpowiednim kątem impulsu świetlnego. Następnie promień rozchodzi się aż do napotkania na swojej drodze punktu odbicia. Odbija się od niego i pokonuje drogę wewnątrz płaszcza, aż napotka kolejny punkt odbicia. Cała transmisja polega na nieustannym (wewnętrznym) odbijaniu się impulsu, dopóki nie osiągnie on celu. Zasadę działania światłowodu przedstawia rysunek 3.7.

Światłowody jednomodowe (ang. *Single Mode* — SM) — transmitują jeden promień (mod) światła. Średnica rdzenia zawiera się w wąskim przedziale 8 – 9 µm, natomiast sam przewód ma standardową średnicę 125 µm.

Światłowody wielomodowe (ang. *Multi Mode* — MM) — transmitują wiele promieni (modów) pod różnymi kątami, dlatego rdzeń włókna ma znacznie większą średnicę (50 – 62,5 µm).



Rysunek 3.7. Zasada działania światłowodu



Rysunek 3.8. 1 — światłowód wielomodowy, 2 — światłowód jednomodowy

Zalety światłowodu jednomodowego:

- ograniczenie zjawiska dyspersji dzięki przesyłowi za pomocą jednego promienia,
- możliwość przesyłania sygnału na długich odcinkach (nawet do 150 km),
- szerokie pasmo przenoszenia i niskie tłumienie.

Zalety światłowodu wielomodowego:

- przesyłanie wielu promieni,
- większa przepustowość na krótkich odległościach (do 2 km).

Sposoby łączenia włókien

Włókna światłowodowe można łączyć na trzy sposoby. Są nimi:

- spawanie (ten sposób łączenia pozwala na uzyskanie najwyższej klasy połączenia),
- klejenie,
- wykorzystanie złączek.

Poniżej prezentowane są przykładowe standardy sieci Ethernet wykorzystującej łącza światłowodowe:

- 100Base-FX — światłowód wielomodowy, maksymalna prędkość transmisji 100 Mb/s, maksymalna długość segmentu — 2000 m,

- 1000Base-LX — światłowód jednomodowy, maksymalna prędkość transmisji 1000 Mb/s, maksymalna długość segmentu — 10 km,
- 1000Base-SX — światłowód wielomodowy, maksymalna prędkość transmisji 1000 Mb/s, maksymalna długość segmentu — 550 m,
- 10GBase-LR — światłowód jednomodowy, maksymalna prędkość transmisji 10 GB/s, maksymalna długość segmentu — 10 km.

3.2. Media bezprzewodowe

W sieciach komputerowych wykorzystuje się dwa rodzaje bezprzewodowego medium transmisyjnego WLAN (ang. *Wireless Local Area Network*):

- fale z zakresu podczerwieni — są stosowane na otwartym terenie bądź wewnątrz budynków. Jako źródła promieniowania fal elektromagnetycznych wykorzystuje się diody elektroluminescencyjne LED (ang. *light-emitting diode*) lub diody laserowe.
- fale radiowe — do transmisji wymagają planowania przydziału częstotliwości z uwzględnieniem maksymalnej dopuszczalnej mocy nadajników, rodzaju modulacji oraz innych zaleceń Międzynarodowej Unii Telekomunikacji (ITU).

Standardy dotyczące sieci bezprzewodowych opisują m.in. prędkość transmisji i pasmo częstotliwości (tabela 3.1).

Tabela 3.1. Standardy najczęściej występujących sieci bezprzewodowych

Nazwa	Szybkości (Mb/s)	Pasmo częstotliwości (GHz)
802.11	1; 2	2,4
802.11a	6; 9; 12; 18; 24; 36; 48; 54	5
802.11b	1; 2; 5,5; 11	2,4
802.11g	1; 2; 5,5; 6; 9; 11; 12; 18; 24; 36; 48; 54	2,4
802.11n	100; 150; 300; 450; 600	2,4 lub 5
802.11ac	433; 867; 1300; 1733;... 6928	5
802.15.1 (bluetooth)	0,021; 0,124; 0,328; 2,1; 3,1; 24; 40	2,4

Podstawową zaletą sieci bezprzewodowej jest mobilność rozwiązania — aby podłączyć urządzenie sieciowe, nie trzeba prowadzić przewodów, wystarczy jedynie umieścić urządzenie w zasięgu działania sieci i odpowiednio skonfigurować. Pozwala to na szybką i łatwą rozbudowę sieci.

Do wad sieci bezprzewodowych należy zaliczyć możliwość zakłócenia fal radiowych przez przeszkody znajdujące się na drodze fali niosącej sygnał lub przez warunki atmosferyczne, a także mniejsze niż w przypadku sieci kablowych bezpieczeństwo transmitowanych danych (brak kontroli nad dostępem do medium transmisyjnego).

Na infrastrukturę sieci bezprzewodowej składają się:

- karty sieciowe,
- punkty dostępowe,
- anteny.

Sieci WLAN mogą pracować w dwóch trybach:

- ad hoc, w którym urządzenia łączą się bezpośrednio ze sobą,
- w trybie infrastruktury z wykorzystaniem punktów dostępowych (ang. *access point*).

Punkt dostępowy to centralny punkt sieci bezprzewodowej. Przekazuje dane pomiędzy urządzeniami, pozwala także na podłączenie sieci bezprzewodowej do sieci kablowej. Punkty dostępowe mają dwa interfejsy sieciowe: interfejs bezprzewodowy (gniazdo do podłączenia anteny lub wbudowaną antenę) oraz interfejs sieci kablowej (najczęściej gniazdo RJ45 do podłączenia sieci Ethernet).

Punkty dostępowe mogą komunikować się między sobą, co pozwala na budowę złożonej infrastruktury łączącej urządzenia znacznie od siebie oddalone.

Punkty dostępowe pozwalają na budowę dwóch rodzajów sieci:

- BSS (ang. *Basic Service Set* — podstawowy zestaw usługowy) — cała transmisja w danej sieci przeprowadzana jest z wykorzystaniem jednego punktu dostępowego.
- ESS (ang. *Extended Service Set* — rozszerzony zestaw usług) — sieć zbudowana z kilku punktów dostępowych, które komunikują się ze sobą za pomocą protokołu IAPP (ang. *Inter-Access Point Protocol*), tworząc sieć szkieletową. W tego rodzaju sieci urządzenia podłączane są do dowolnego z punktów dostępowych i mogą przemieszczać się między nimi. Tego rodzaju sieci są stosowane m.in. przy budowie hotspotów — publicznych punktów dostępu do internetu.

W przypadku sieci bezprzewodowych ogromne znaczenie ma bezpieczeństwo danych. Ogólnodostępne medium transmisyjne powoduje, że każde urządzenie znajdujące się w zasięgu sieci mogłoby korzystać z jej zasobów. Punkty dostępowe pozwalają na implementację procedur bezpieczeństwa polegających na filtrowaniu adresów MAC lub IP, a także na zabezpieczenie dostępu do sieci kluczem szyfrującym.

Urządzenia bezprzewodowe mogą pracować bez szyfrowania danych (tryb niezalecany ze względów bezpieczeństwa) lub w jednym z następujących trybów szyfrowania danych:

- WEP (ang. *Wired Equivalent Privacy*) — pozwalający na używanie kluczy 64-bitowych lub 128-bitowych. Szyfrowanie WEP zostało złamane i nie jest uznawane za bezpieczne.
- WPA (ang. *WiFi Protected Access*) — zabezpieczenie wykorzystujące cykliczne zmiany klucza szyfrującego podczas transmisji, może działać w dwóch trybach: *Enterprise* (klucze przydzielane są przez serwer Radius dla każdego użytkownika sieci) lub *Personal* (wszyscy użytkownicy sieci korzystają z dzielonego klucza — ang. *Pre-Shared Key* — PSK).

- WPA2 — poprawiona wersja protokołu WPA, zalecana do zabezpieczeń sieci bezprzewodowych.

Konfiguracja urządzeń bezprzewodowych zostanie omówiona w rozdziale 8. — „Konfigurowanie urządzeń sieciowych".

ĆWICZENIA

1. Z jakiego medium transmisyjnego korzystasz? W jakiej topologii jest zbudowana Twoja sieć w domu/szkole?

PYTANIA

1. Omów budowę kabla koncentrycznego.
2. Omów budowę kabla światłowodowego.
3. Dlaczego żyły w kablu UTP są skręcone?
4. Wymień rodzaje bezprzewodowego medium transmisyjnego.

4

Protokoły sieciowe

Protokoły sieciowe to zestaw reguł, które umożliwiają komunikację w sieci komputerowej.

4.1. Model ISO/OSI

DEFINICJA

Model odniesienia OSI (ang. *Open System Interconnection Reference Model*) to wzorcowy model transmisji danych w sieciach komputerowych. Model składa się z 7 warstw (ang. *layers*) współpracujących ze sobą w określony sposób (rysunek 4.1). Został on przyjęty przez Międzynarodową Organizację Standaryzacji ISO w 1984 roku.

Rysunek 4.1.
Warstwy w modelu OSI

Model odniesienia OSI jest wzorcem używanym do reprezentowania mechanizmów przesyłania informacji w sieci. Pozwala wyjaśnić, w jaki sposób dane pokonują różne warstwy w drodze do innego urządzenia w sieci, nawet jeśli nadawca i odbiorca

dysponują różnymi typami medium sieciowego. Podział sieci na warstwy przynosi następujące korzyści:

- dzieli proces komunikacji sieciowej na mniejsze, łatwiejsze do zarządzania procesy składowe,
- tworzy standardy składników sieci, dzięki czemu składniki te mogą być rozwijane niezależnie i obsługiwane przez różnych producentów,
- umożliwia wzajemną komunikację sprzętu i oprogramowania sieciowego różnych rodzajów,
- zmiany wprowadzone w jednej warstwie nie dotyczą innych warstw.

Trzy górne warstwy, czyli warstwa aplikacji, prezentacji i sesji, zajmują się współpracą z oprogramowaniem wykonującym zadania zlecane przez użytkownika systemu komputerowego. Tworzą one interfejs, który pozwala na komunikację z warstwami niższymi.

Warstwa aplikacji (ang. *application layer*) zajmuje się zapewnieniem dostępu do sieci aplikacjom użytkownika. W warstwie tej są zdefiniowane protokoły usług sieciowych, takich jak HTTP, FTP, SMTP.

Warstwa prezentacji (ang. *presentation layer*) odpowiada za reprezentację danych — obsługę znaków narodowych, formatów graficznych oraz kompresję i szyfrowanie.

Warstwa sesji (ang. *session layer*) zapewnia aplikacjom komunikację między różnymi systemami. Zarządza sesjami transmisyjnymi poprzez nawiązywanie i zrywanie połączeń między aplikacjami.

Warstwa transportowa (ang. *transport layer*) zapewnia połączenie między aplikacjami w różnych systemach komputerowych, dba o kontrolę poprawności przesyłanych danych. Tutaj następuje podział danych na segmenty, które są kolejno numerowane i wysyłane do stacji docelowej. Stacja docelowa po odebraniu segmentu może wysłać potwierdzenie odbioru, co pozwala zapewnić prawidłowość transmisji.

Warstwa sieciowa (ang. *network layer*) zapewnia metody łączności. W tej warstwie obsługiwane są routing i adresacja logiczna.

Warstwa łącza danych (ang. *data link layer*) odpowiada za poprawną transmisję danych przez konkretne media transmisyjne. Warstwa ta operuje na fizycznych adresach interfejsów sieciowych (MAC), zapewniając łączność między dwoma bezpośrednio połączonymi urządzeniami.

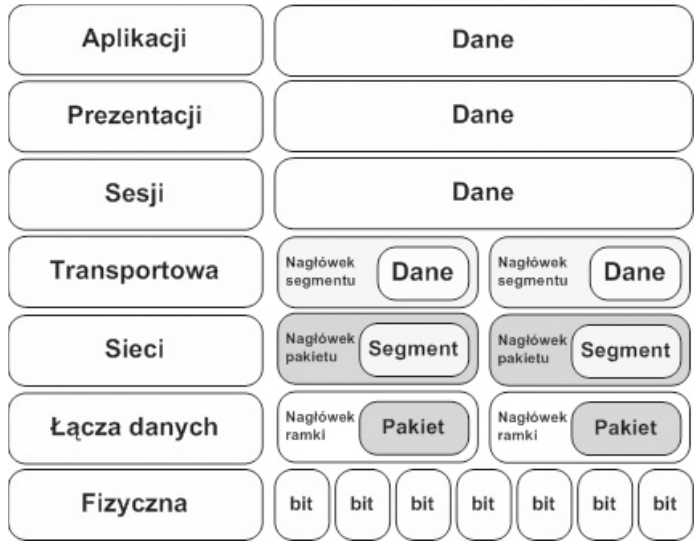
Warstwa fizyczna (ang. *physical layer*) odbiera dane z warstwy łącza danych i przesyła je w medium transmisyjnym jako bity reprezentowane w konkretny sposób (sygnały elektryczne, impulsy świetlne).

Model OSI opisuje drogę danych przesyłanych między aplikacjami, które zostały uruchomione w różnych systemach komputerowych. W przypadku większości usług w internecie transmisja między systemami jest realizowana według modelu klient-serwer, a komunikują się aplikacje klienckie (np. przeglądarka internetowa) z aplikacją serwerową (np. serwer stron WWW).

DEFINICJA

Transmisja w modelu OSI jest przeprowadzana w dół kolejnych warstw (na urządzeniu źródłowym), a następnie w górę (na serwerze lub urządzeniu docelowym). Proces przekazywania danych między warstwami protokołu jest nazywany **enkapsulacją** lub kapsułkowaniem (rysunek 4.2).

Rysunek 4.2.
Model enkapsulacji



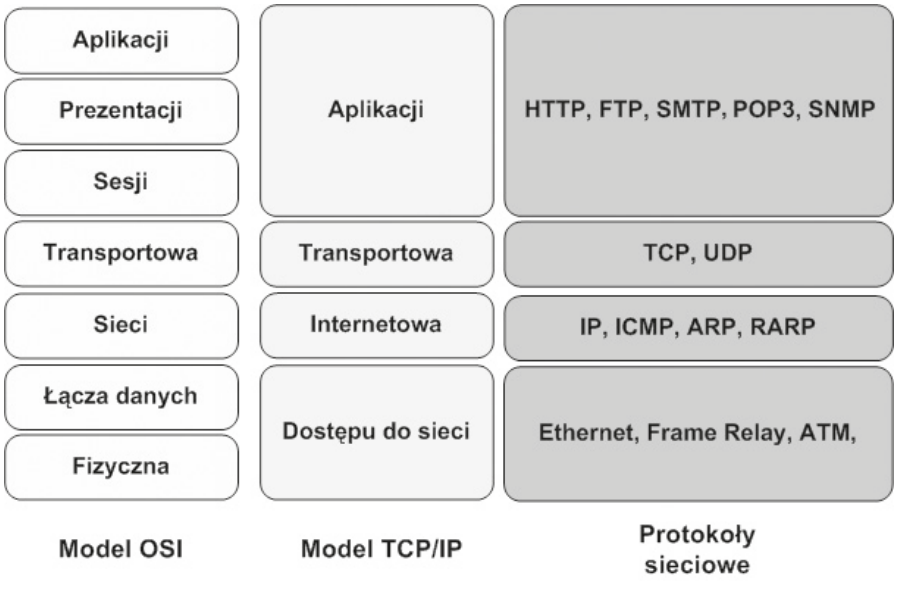
W procesie enkapsulacji dane użytkownika (z warstwy aplikacji) są dzielone w warstwie transportu na **segmenty** i opatrywane nagłówkiem zawierającym m.in. numery portów. Tak przygotowane porcje danych wędrują do warstwy trzeciej, gdzie jest dodawany nagłówek zawierający adresy logiczne nadawcy i odbiorcy. Powstaje **pakiet**. Do pakietów w warstwie łącza danych są dodawane adresy fizyczne — tworzona jest **ramka**. Ostatnia warstwa — fizyczna — przekształca ramkę z poprzedniej warstwy do postaci pozwalającej przesłać informację medium transmisyjnym. Dane wędrują do stacji docelowej i tam są ponownie przekształcane, najpierw z bitów na ramki, następnie na pakiety i segmenty, po czym zostają zinterpretowane przez aplikację na komputerze docelowym.

4.2. Model TCP/IP

Warstwa aplikacji (ang. *application layer*) to najwyższy poziom, w którym pracują aplikacje, na przykład serwer WWW czy przeglądarka internetowa. Warstwa ta obejmuje zestaw gotowych protokołów, które są wykorzystywane przez aplikacje do przesyłania w sieci różnego typu informacji.

DEFINICJA

Model TCP/IP (ang. *Transmission Control Protocol/Internet Protocol*) to teoretyczny model warstwowej struktury komunikacji sieciowej. Opiera się on na szeregu współpracujących ze sobą warstw (ang. *layers*). Założenia modelu TCP/IP są pod względem organizacji warstw zbliżone do założeń modelu OSI, jednak liczba warstw jest mniejsza i lepiej odzwierciedla prawdziwą strukturę internetu (rysunek 4.3).



Rysunek 4.3. Porównanie modeli OSI i TCP/IP

Warstwa transportowa (ang. *transport layer*) odpowiada za przesyłanie danych i kieruje właściwe informacje do odpowiednich aplikacji, wykorzystując porty określane dla każdego połączenia. Warstwa transportowa nawiązuje i zrywa połączenia między komputerami. W tej warstwie działa protokół TCP (przesyłający potwierdzenia odbioru porcji danych, co gwarantuje pewność transmisji) oraz protokół UDP (bez potwierdzeń odbioru).

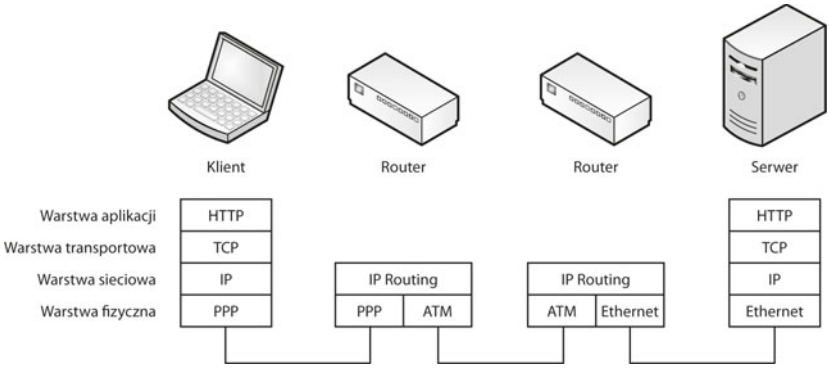
Warstwa internetowa (ang. *internet layer*) ma za zadanie podzielenie segmentów na pakiety i przesłanie ich dowolną siecią. Pakiety trafiają do sieci docelowej niezależnie od przebytej drogi. Tą warstwą zarządza protokół IP. Tutaj jest określana najlepsza ścieżka i następuje przełączanie pakietów.

UWAGA

Związek między protokołem IP i protokołem TCP jest bardzo istotny. Protokół IP określa drogę dla pakietów, a protokół TCP zapewnia niezawodny transport.

Warstwa dostępu do sieci (ang. *network access layer*) zajmuje się przekazywaniem danych przez fizyczne połączenia między urządzeniami sieciowymi (np. karty sieciowe lub modemy). Dodatkowo warstwa ta jest wyposażona w protokoły służące do dynamicznego określania adresów IP.

Przykład komunikacji z wykorzystaniem protokołu TCP/IP (rysunek 4.4).



Rysunek 4.4. Przykład transmisji w TCP/IP

4.2.1. Protokoły w warstwie dostępu do sieci

Warstwa dostępu do sieci jest odpowiedzialna za wszystkie zagadnienia związane z zestawieniem łącza fizycznego służącego do przekazywania pakietu IP do medium transmisyjnego. Odpowiada między innymi za odwzorowywanie adresów IP na adresy sprzętowe i za enkapsulację pakietów IP w ramki. Określa połączenie z fizycznym medium sieci w zależności od rodzaju sprzętu i interfejsu sieciowego.

Warstwa dostępu do sieci w modelu TCP/IP definiuje funkcje umożliwiające korzystanie ze sprzętu sieciowego i dostęp do medium transmisyjnego. W sieciach lokalnych protokołem dostępu do sieci jest Ethernet, w sieciach rozległych są to m.in. protokoły ATM i Frame Relay.

Ethernet

DEFINICJA

Standard Ethernet został opublikowany w latach 80. ubiegłego wieku. Transmisja osiągała szybkość do 10 Mb/s i była realizowana przez gruby kabel koncentryczny na odległościach do 500 m. Pierwotny standard technologii Ethernet był wielokrotnie poprawiany w celu dostosowania go do potrzeb nowych mediów transmisyjnych i większych prędkości transmisji. Obecnie rodzina technologii Ethernet obejmuje następujące standardy: Ethernet (prędkość 10 Mb/s), Fast Ethernet (100 Mb/s), Gigabit Ethernet (1000 Mb/s), 10 Gigabit Ethernet (10 Gb/s), 40 Gigabit Ethernet (40 Gb/s) oraz 100 Gigabit Ethernet (100 Gb/s).

Ethernet jest najpopularniejszą technologią sieci LAN. Specyfikacje sieci Ethernet obejmują różne media transmisyjne, szerokości pasma oraz inne elementy warstw 1 i 2 modelu ISO. Niemniej jednak podstawowy format ramki oraz schemat adresowania są takie same dla wszystkich odmian standardu Ethernet.

Technologie Ethernet określają sposoby ustalania przepustowości łącza sieciowego nazywane **autonegocjacją**. Interfejsy sieciowe mogą pracować w wielu trybach, w zależności od rodzaju wykorzystywanego w sieci medium (tabela 4.1). Celem autonegocjacji jest umożliwienie współpracy różnych urządzeń w trybie o najwyższej prędkości akceptowalnej przez wszystkie urządzenia w sieci.

Format ramki przyjmuje postać przedstawioną na rysunku 4.5.

Rysunek 4.5. Ramka Ethernet

Poszczególne elementy oznaczają:

- **Preambuła** — składa się z 7 bajtów złożonych z naprzemiennych jedynek i zer.
- **SFD** (ang. *Start Frame Delimiter*), czyli znacznik początkowy ramki w postaci sekwencji 8 bitów (1 bajt).
- **Adres MAC odbiorcy** (6 bajtów).
- **Adres MAC nadawcy** (6 bajtów).
- **Typ ramki** (2 bajty).
- **Dane** (46 – 1500 bajtów) — jeżeli dane są mniejsze niż 46 bajtów, to są uzupełniane zerami.
- **Suma kontrolna** (4 bajty).

Tabela 4.1. Najczęściej występujące standardy sieci Ethernet

IEEE 802.3	standard protokołu CSMA/CD
IEEE 802.3u	Fast Ethernet 100BASE-T
IEEE 802.3z	Gigabit Ethernet (światłowód)
IEEE 802.3ab	Gigabit Ethernet, 1000BASE-T
IEEE 802.11	bezprzewodowy Ethernet
IEEE 802.3ae	10 Gigabit Ethernet (światłowód)
IEEE 802.3bg	40 Gigabit Ethernet (światłowód)
IEEE 802.3bj	100 Gigabit Ethernet (kabel miedziany)

Frame Relay

DEFINICJA

Frame Relay to protokół oraz szybka sieć pakietowa, która pozwala na łączenie odległych sieci LAN w celu transmisji danych i głosu oraz przeprowadzania wideo- i telekonferencji. W tej technice informacja jest dzielona na ramki o zmiennej długości, które przenoszą dane między sieciami LAN, co pozwala na przekazywanie informacji między urządzeniami końcowymi sieci rozległych (WAN). Frame Relay zapewnia komunikację połączeniową o przepływności do 45 Mb/s. Funkcjonuje na wysokiej jakości łączach telekomunikacyjnych odznaczających się niskim wskaźnikiem błędów.

Sieć Frame Relay składa się z wielu urządzeń sieciowych połączonych kanałami fizycznymi, na których są tworzone połączenia wirtualne (logiczne). Mogą być one zestawiane na stałe (ang. *Permanent Virtual Circuits* — PVC) i tymczasowo (ang. *Switched Virtual Circuits* — SVC). Grupowe połączenia wirtualne (Multicast) są zestawiane na dłuższy czas i zapewniają dostęp wielu użytkownikom jednocześnie do tych samych zasobów sieci.

Frame Relay zapewnia gwarantowaną szybkość transmisji (ang. *Committed Information Rate — CIR*).

ATM

DEFINICJA

ATM (ang. *Asynchronous Transfer Mode*) jest technologią telekomunikacyjną, która umożliwia przesyłanie głosu, obrazów wideo i danych przez sieci prywatne i publiczne. Podstawową porcją danych w sieciach ATM jest komórka, która ma stałą długość 53 bajtów. Tworzy ją 5-bajtowy nagłówek ATM i 48 bajtów treści zasadniczej. Małe komórki o stałej długości doskonale nadają się do przesyłania głosu i obrazów wideo, ponieważ ruch ten nie toleruje opóźnień. Ruch zawierający obrazy wideo i głos nie musi czekać na przesłanie większego pakietu danych.

ATM (ang. *Asynchronous Transfer Mode*) to asynchroniczny tryb przesyłania danych. Jest technologią telekomunikacyjną szerokopasmową, która umożliwia przesyłanie głosu, obrazów wideo i danych w sieciach prywatnych i publicznych z prędkością 155 Mb/s.

Podstawową porcją danych w sieciach ATM jest komórka, która ma stałą długość 53 bajtów. Tworzy ją 5-bajtowy nagłówek ATM i 48 bajtów treści zasadniczej. Małe komórki o stałej długości doskonale nadają się do przesyłania głosu i obrazów wideo, ponieważ ruch ten nie toleruje opóźnień. Ruch zawierający obrazy wideo i głos nie musi czekać na przesłanie większego pakietu danych. Standard ATM może być stosowany zarówno w sieciach lokalnych LAN, miejskich MAN, jak i rozległych WAN.

W standardzie ATM zdefiniowane są dwa podstawowe rodzaje styków (interfejsów):

- UNI (ang. *User Network Interface*) — miejsce styku użytkownika z siecią szerokopasmową,
- NNI (ang. *Network-to-Network Interface*) — styk umieszczony w węźle sieci wykorzystywany do połączenia z innymi węzłami.

Model architektury ATM składa się z trzech warstw:

- warstwy fizycznej — definiującej funkcje związane z dostępem do medium transmisyjnego,
- warstwy ATM — określającej format komórki oraz funkcje zapewniające niezawodny transfer ATM, bez względu na typ usługi,
- warstwy AAL (ang. *ATM Adaptation Layer*) — sterującej przepływem danych oraz utrzymującej wymagane parametry czasowe przekazu, jak również obsługującej błędy.

4.2.2. Protokoły warstwy internetowej

Zadaniem warstwy internetowej jest wybranie najlepszej ścieżki dla pakietów przesyłanych w sieci. Podstawowym protokołem działającym w tej warstwie jest **protokół IP** (ang. *Internet Protocol*). Tutaj następuje określenie najlepszej ścieżki i przełączanie pakietów.

Protokół IP spełnia następujące zadania:

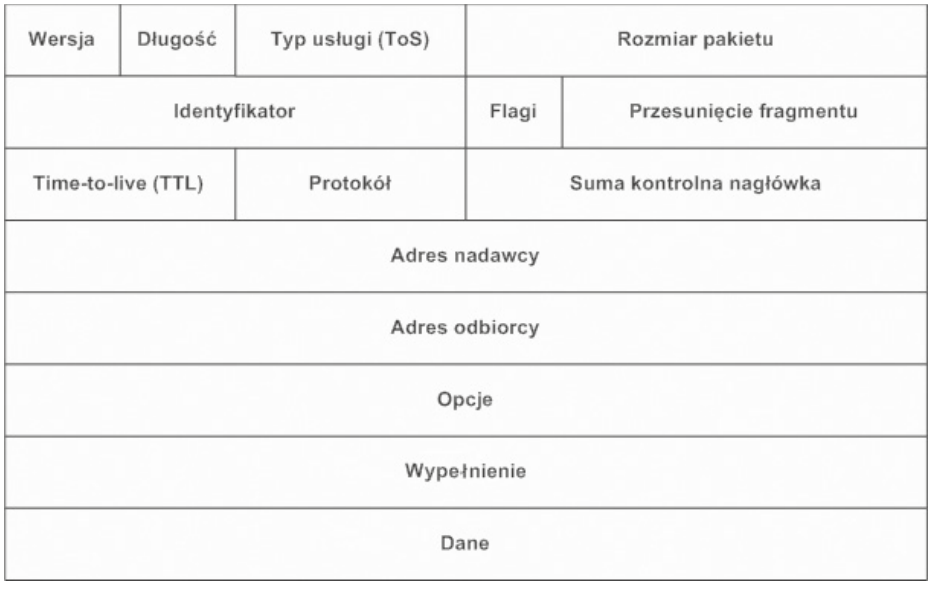
- definiuje format pakietu i schemat adresowania,
- kieruje pakiety do zdalnych hostów.

DEFINICJA

W warstwie internetowej modelu TCP/IP działają następujące protokoły:

- **Protokół IP** (ang. *Internet Protocol*), który zapewnia usługę bezpołączeniowego dostarczania pakietów przy użyciu dostępnych możliwości. Protokół IP nie uwzględnia zawartości pakietu, ale wyszukuje ścieżkę do miejsca docelowego.
- **Protokół ICMP** (ang. *Internet Control Message Protocol*), który pełni funkcje kontrolne i informacyjne. Jest on używany przez polecenia sprawdzające poprawność połączenia (np. polecenie `ping`).
- **Protokół ARP** (ang. *Address Resolution Protocol*), który znajduje adres warstwy łącza danych MAC dla znanego adresu IP.
- **Protokół RARP** (ang. *Reverse Address Resolution Protocol*), który znajduje adres IP dla znanego adresu MAC.
- **Protokoły routingu** (RIP, IGRP, EIGRP, OSPF, BGP).

Postać, w jakiej dane są przesyłane przez pakiety IP, została przedstawiona na rysunku 4.6. Jest to transmisja szeregowa, a kolejny wiersz tabeli zawiera następne dane.



Rysunek 4.6. Format pakietu IP

Poszczególne elementy oznaczają:

- **Wersja** — wersja protokołu IP.
- **Długość nagłówka** — wartość tego pola pomnożona przez 32 bity określa długość nagłówka w bitach.
- **Typ usługi** (ang. *Type of Service — ToS*) — informacja o pożądanej jakości usługi (np. Niska, Wysoka).
- **Rozmiar pakietu** — rozmiar całego pakietu IP podany w bajtach.
- **Identyfikator** — używany podczas łączenia fragmentów danych.
- **Flagi** — jest to 3-bitowe pole, gdzie pierwszy bit określa, czy dany pakiet może zostać podzielony na fragmenty; drugi — czy pakiet jest ostatnim fragmentem. Trzeci bit nie jest używany.
- **Przesunięcie fragmentu** — określa kolejną pozycję przesyłanych danych w oryginalnym datagramie w celu jego późniejszego odtworzenia.
- **Czas życia** (ang. *Time To Live* — **TTL**) — zawiera znacznik życia pakietu. Pole to jest liczbą zmniejszaną przez każdy router, przez który przechodzi. Kiedy wartość TTL osiągnie zero, pakiet jest zatrzymywany, a nadawca zostaje poinformowany, że pakietu nie udało się dostarczyć.
- **Protokół** — oznacza kod protokołu warstwy wyższej — transportowej.
- **Suma kontrolna nagłówka** — służy do wykrywania uszkodzeń wewnątrz nagłówka.

- **Adresy źródłowy i docelowy pakietu** — adres IP nadawcy i odbiorcy pakietu.
- **Opcje** — dodatkowe informacje, nie zawsze używane, mogą dotyczyć na przykład funkcji zabezpieczeń.
- **Wypełnienie** — opcjonalne pole, które uzupełnia nagłówek pakietu zerami, aby jego wielkość była wielokrotnością 32 bitów.
- **Dane** — pole, w którym są transportowane właściwe dane.

4.2.3. Protokoły warstwy transportowej

DEFINICJA

Warstwa transportowa (ang. *transport layer*) zapewnia usługi przesyłania danych z hosta źródłowego do hosta docelowego. Ustanawia logiczne połączenie między hostem wysyłającym i odbierającym. Protokoły transportowe dzielą i scalają dane wysyłane przez aplikacje wyższej warstwy w jeden strumień danych przepływający między punktami końcowymi.

Protokoły warstwy transportowej to TCP i UDP.

Protokół IP pozwala na przenoszenie pakietów między sieciami, jednak nie gwarantuje, że wysłane dane dotrą do adresata. Ta cecha powoduje, że protokół IP jest nazywany **bezpołączeniowym** — dane są wysyłane tylko w jedną stronę bez potwierdzenia.

Za niezawodność przesyłu danych jest odpowiedzialny **protokół TCP** nazywany protokołem **połączeniowym**. To on po odebraniu każdej porcji danych wysyła potwierdzenie do nadawcy, że dane zostały odebrane. W przypadku braku potwierdzenia dane są wysyłane ponownie.

Innym protokołem działającym na rzecz protokołu IP jest **UDP** (ang. *User Datagram Protocol*). Jest on bezpołączeniowym protokołem transportowym należącym do stosu protokołów TCP/IP. Służy do wysyłania datagramów (pakietów danych) bez potwierdzania czy gwarancji ich dostarczenia. Przetwarzanie błędów i retransmisja muszą być obsłużone przez protokoły warstwy aplikacji.

Protokół UDP jest zaprojektowany dla aplikacji, które nie mają potrzeby składania sekwencji segmentów. Nie przysyła on informacji o kolejności, w jakiej mają być odtworzone. Taka informacja jest zawarta w nagłówku segmentów protokołu TCP.

4.2.4. Protokoły warstwy aplikacji

DEFINICJA

Warstwa aplikacji (ang. *aplication layer*) zajmuje się świadczeniem usług dla użytkownika. Protokoły warstwy aplikacji definiują standardy komunikacji między aplikacjami (programami klienckimi a serwerowymi).

Najpopularniejsze protokoły warstwy aplikacji:

- **Telnet** — protokół terminala sieciowego, pozwalający na zdalną pracę z wykorzystaniem konsoli tekstowej.
- **FTP** (ang. *File Transfer Protocol*) — protokół transmisji plików.
- **SMTP** (ang. *Simple Mail Transfer Protocol*) — protokół wysyłania poczty elektronicznej.
- **POP3** (ang. *Post Office Protocol*) — protokół odbioru poczty elektronicznej.
- **HTTP** (ang. *Hypertext Transfer Protocol*) — protokół przesyłania stron WWW.
- **SSH** (ang. *Secure Shell*) — protokół terminala sieciowego zapewniający szyfrowanie połączenia.
- **DNS** (ang. *Domain Name System*) — system nazw domenowych. Odpowiada za tłumaczenie adresów domenowych na adresy IP i odwrotnie.
- **DHCP** (ang. *Dynamic Host Configuration Protocol*) — protokół dynamicznej konfiguracji urządzeń. Odpowiedzialny za przydzielanie adresów IP, adresu domyślnej bramki i adresów serwerów DNS.
- **NFS** (ang. *Network File System*) — protokół udostępniania systemów plików (dysków sieciowych).
- **SNMP** (ang. *Simple Network Management Protocol*) — prosty protokół zarządzania siecią. Pozwala na konfigurację urządzeń sieciowych i gromadzenie informacji na ich temat.
- **NTP** (ang. *Network Time Protocol*) — używany jest do synchronizacji czasu z serwerami NTP. Jest to protokół czasu rzeczywistego, którego zadaniem jest umożliwienie synchronizacji czasu klienta z serwerem czasu. Może nim być serwer zewnętrzny lub lokalny. Usługa ta nasłuchuje na porcie UDP 123.
- **HTTPS** (ang. *Hypertext Transfer Protocol Secure*) — wersja protokołu HTTP, która do komunikacji klient-serwer używa protokołu SSL odpowiadającego za szyfrowanie całej transmisji.

4.3. Protokoły używane w sieciach LAN

4.3.1. Protokół TCP/IP

Najpopularniejszym spośród protokołów komunikacyjnych jest **protokół IP**, powszechnie używany w sieciach LAN, a także w internecie. W sieciach IP dane są wysyłane w formie bloków określanych mianem pakietów. W przypadku transmisji z wykorzystaniem protokołu IP przed rozpoczęciem transmisji nie jest zestawiana wirtualna sesja komunikacyjna między dwoma urządzeniami.

Protokół IP jest protokołem zawodnym — nie gwarantuje, że pakiety dotrą do adresata, że nie zostaną pofragmentowane czy też zdublowane. Ponadto dane mogą dotrzeć do odbiorcy w innej kolejności niż ta, w jakiej zostały nadane. Niezawodność transmisji danych zapewniają protokoły warstw wyższych (np. protokół warstwy transportowej — TCP).

4.3.2. Protokół IPX/SPX

Dla sieci pracujących w środowisku Novell Netware został opracowany protokół **IPX** (ang. *Internet Packet Exchange*). Nie został on wyposażony w mechanizmy kontroli transmisji i nie gwarantuje, że wszystkie pakiety dotrą na miejsce. Podobnie jak w przypadku protokołu IP, niezawodność transmisji zapewnia protokół warstwy czwartej — **SPX** (ang. *Sequenced Packet Exchange*).

Adresacja w protokole IPX składa się z dwóch części: adresu sieci i adresu hosta. Pierwszy z nich jest liczbą 32-bitową, drugi — 48-bitową i odpowiada adresowi MAC karty sieciowej.

Obecnie protokoły IPX/SPX praktycznie nie są stosowane, ponieważ zostały wyparte przez stos protokołów TCP/IP.

4.3.3. AppleTalk

AppleTalk jest protokołem opracowanym przez firmę Apple, stosowanym w sieciach komputerowych opartych na systemie operacyjnym OS X. Protokół ten wykorzystują proste sieci równorzędne. Aktualnie protokół AppleTalk nie jest rozwijany, został zastąpiony przez protokół TCP/IP.

Protokoły IP, IPX i AppleTalk są **protokołami rutowalnymi** (ang. *routed protocol*). Oznacza to, że mogą być obsługiwane przez routery, a więc mogą przenosić dane między różnymi sieciami.

4.3.4. NetBEUI

NetBEUI to prosty protokół opracowany przez IBM i wykorzystywany jedynie w systemach operacyjnych firmy Microsoft. Protokół ten cechuje się minimalnymi wymaganiami i dużą odpornością na błędy. Sprawdza się jednak tylko w małych sieciach lokalnych — nie może być używany w internecie, gdyż nie jest protokołem rutowalnym. W najnowszych wersjach systemów Windows protokół ten został zastąpiony przez TCP/IP.

NetBEUI umożliwia identyfikację stacji przez nazwę przydzielaną przez użytkownika. Jest to ciąg znaków alfanumerycznych w formacie ASCIIZ (ostatni znak musi mieć kod zero). Wprowadzana nazwa musi być unikatowa.

4.4. Zasady transmisji w sieciach TCP/IP

Urządzenia pracujące w jednej sieci mają możliwość komunikacji tylko między sobą. Aby połączyć je z inną siecią, wymagany jest **router**. Jest to urządzenie, które przekierowuje pakiet do adresata znajdującego się w innej logicznej sieci IP.

4.4.1. Brama domyślna

DEFINICJA

Komunikacja w sieciach TCP/IP pozwala na wymianę danych tylko z urządzeniami znajdującymi się w danej sieci. Aby wysłać wiadomość poza sieć, w której pracuje urządzenie, należy ustawić parametr konfiguracyjny protokołu IP — **bramę domyślną**. Adres bramy domyślnej wskazuje na router, który przechowuje informacje o tym, jak dotrzeć do wybranej sieci.

Routery to urządzenia brzegowe, które znajdują się na styku dwóch sieci działających w innych klasach adresacji IP. Mają za zadanie przesyłać pakiety do adresata, a dokładnie do sieci, w której znajduje się jego adres IP. Pakiet zaadresowany do komputera znajdującego się w naszej sieci jest kierowany bezpośrednio do niego. Jeśli ma zostać wysłany poza sieć, trafia do routera, który sprawdza, czy pakiet ten jest kierowany do sieci bezpośrednio podłączonej do tego routera, czy ma być przesłany do urządzenia znajdującego się poza podłączonymi do niego sieciami. Pakiety wędrują od jednego węzła (routera) do drugiego poprzez wiele węzłów pośredniczących, często mogą też być transmitowane różnymi trasami. Zadaniem routera jest wybrać najlepszą dostępną drogę pomiędzy jednym a drugim węzłem. Decyzja o wyborze trasy jest podejmowana na podstawie wpisów znajdujących się w tablicy routingu — spisie sieci podłączonych bezpośrednio do routera oraz sieci dostępnych na routerach sąsiadujących.

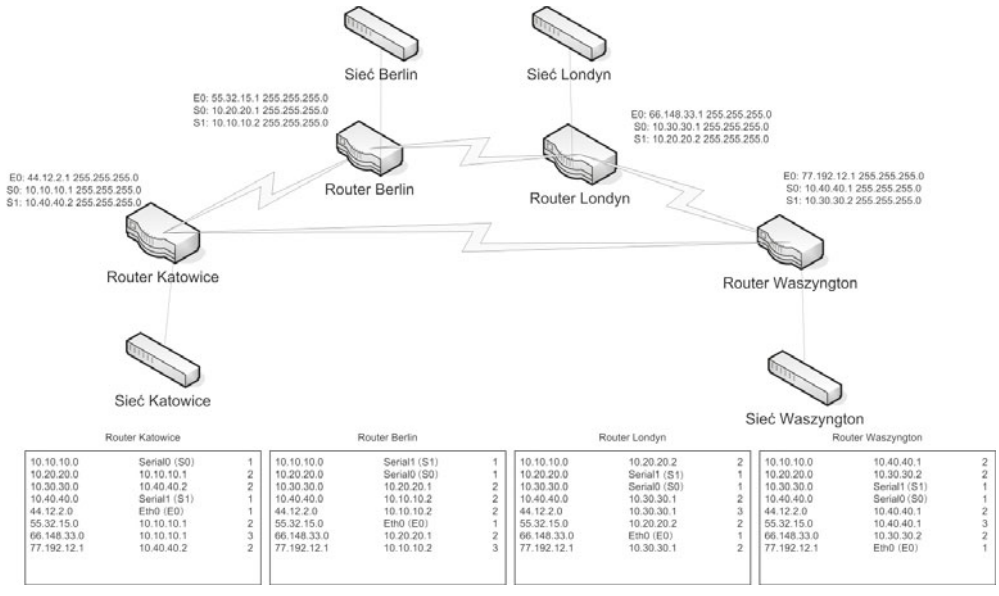
DEFINICJA

Tablica routingu (ang. *routing table*) może być utworzona przez administratora lub dynamicznie, przez protokoły routingu (nie mylić z protokołami rutowalnymi). **Routing** (**trasowanie**) polega na podjęciu decyzji, przez który fizyczny port lub przez którą sieć pakiety mają być wysłane, aby jak najszybciej dotarły do adresata.

Każdy wpis w tablicy routingu zawiera adres sieci docelowej oraz adres sieci lub interfejsu, przez który dana sieć docelowa jest osiągalna. Jeśli router zna więcej niż jedną trasę do sieci docelowej, wybiera trasę najkorzystniejszą na podstawie metryki — wartości określającej jakość danej trasy.

Metryki są zależne od konkretnego protokołu routingu. Mogą opierać się tylko na liczbie routerów znajdujących się na drodze do celu, ale również na chwilowym obciążeniu łącza, jego prędkości czy opóźnieniach występujących w transmisji.

Przykład 4.1. Rysunek 4.7 przedstawia infrastrukturę sieciową dla przykładowej sieci łączącej Katowice, Berlin, Londyn i Waszyngton. W każdym z miast do zainstalowanych routerów została podłączona sieć lokalna. Informacje o dostępnych sieciach są zapisane w tablicach routingu zamieszczonych pod rysunkiem. Kolejne wpisy w tablicach oznaczają: adres sieci, adres interfejsu (lub jego nazwę w przypadku sieci bezpośrednio podłączonych), przez który dana sieć jest osiągalna, oraz liczbę przeskoków do celu.



Rysunek 4.7. Przykładowa infrastruktura sieci

4.4.2. Protokoły routingu

Routery budują tablice routingu na podstawie informacji wymienionych z innymi routerami. Wymiana ta opiera się na **protokołach routingu**. Mają one za zadanie poinformować inne węzły sieci o sieciach, do których dany router ma dostęp. Takie rozwiązanie pozwala na dynamiczne budowanie struktury. Dołączenie kolejnej sieci do jednego z routerów nie wymaga rekonfiguracji pozostałych węzłów sieci. Zostaną one automatycznie „poinformowane" o zaistniałych zmianach.

Aby określić, która z dostępnych tras jest najlepsza, router wykorzystuję metrykę — wartość wyliczaną na podstawie określonych czynników zależnych od protokołu routingu, np. liczby przeskoków, szerokości pasma, opóźnienia, obciążenia czy niezawodności łącza.

Ze względu na sposoby działania rozróżnia się następujące protokoły routingu:

- protokoły wektora odległości (ang. *distance vector protocols*) — wysyłają w określonych interwałach czasowych do sąsiednich routerów zawartość tablicy routingu wraz z metrykami. Jeśli dana trasa nie jest dostępna (nie dotarła informacja od sąsiedniego routera), wówczas wpis dotyczący trasy i sieci, które były osiągalne, zostaje usunięty z tablicy routingu i — o ile to możliwe — jest zastępowany innym wpisem (np. wcześniej odrzuconym jako mniej korzystny).
- protokoły stanu łącza (ang. *link state protocols*) wysyłają do wszystkich routerów informację, która zawiera jedynie dane o podsieciach podłączonych do routera. Aktualizacje informacji są wysyłane okresowo lub wywoływane zmianami zachodzącymi w sieci.

Tabela 4.2 zawiera opis najpopularniejszych protokołów routingu.

Tabela 4.2. Opis protokołów routingu

Nazwa protokołu	Opis
RIP (ang. *Routing Information Protocol*)	Protokół wektora odległości, używający liczby przeskoków pomiędzy routerami jako metryki. Domyślnie wysyła uaktualnienia co 30 sekund.
IGRP (ang. *Interior Gateway Routing Protocol*) i EIGRP (ang. *Enhanced Interior Gateway Routing Protocol*)	Protokół wektora odległości opracowany i wykorzystywany w urządzeniach CISCO. Wyliczana metryka uwzględnia przepustowość i obciążenie pasma, opóźnienie i niezawodność łącza. Uaktualnienia są wysyłane co 90 sekund lub po zmianie stanu sieci.
OSPF (ang. *Open Shortest Path First*)	Protokół stanu łącza, który używa algorytmu Dijkstry do wyznaczenia najkrótszej ścieżki. Uaktualnienia domyślnie są wysyłane po zmianach w topologii sieci.
BGP (ang. *Border Gateway Protocol*)	Służy do wyznaczania niezapętlonych tras pomiędzy systemami autonomicznymi — siecią lub grupą sieci — wykorzystującymi spójny schemat routingu.

Dynamiczne przekazywanie informacji o stanie sieci poprawia jej działanie. Router, który utracił bezpośrednie połączenie z sąsiadującym węzłem, może połączyć się z nim inną drogą. Routery mają możliwość zdefiniowania **routingu domyślnego** — trasy określającej dostęp do wszystkich sieci, które nie są wpisane w tablicy routingu.

Przykład 4.2. Wróćmy do przykładu z rysunku 4.9. Węzeł Katowice ma dostęp do węzła Waszyngton dwoma drogami — przez Berlin i Londyn oraz bezpośrednio. Na podstawie informacji zawartych w tablicy routingu wszystkie pakiety są kierowane do sieci bezpośrednio łączącej oba węzły. Jeśli połączenie pomiędzy Katowicami a Berlinem — sieć 10.10.10.0 — zostanie zerwane (nie dotrze informacja protokołu routingu lub router wykryje niedostępną trasę), wówczas w tablicy routingu wpis dotyczący bezpośredniej dostępności węzła Berlin zostanie zamieniony na trasę przez Waszyngton.

Wpisy w tablicy routera Katowice będą wyglądać następująco:

```
10.20.20.0      10.40.40.2      2
10.30.30.0      10.40.40.2      1
10.40.40.0      Serial1         0
44.12.2.0       Eth0            0
55.32.15.0      10.10.40.2      3
66.148.33.0     10.10.40.2      2
77.192.12.1     10.40.40.2      1
```

Wpis dla sieci 10.10.10.0 został usunięty — sieć ta przestała działać.

4.4.3. Gniazdo

DEFINICJA

Transmisja w sieciach TCP/IP opiera się na dwóch elementach — adresie urządzenia i numerze portu. Taka para parametrów transmisji jest nazywana **gniazdem**. Adres IP odpowiada za zidentyfikowanie pojedynczego urządzenia w sieci, a numer portu oznacza, jaka aplikacja na urządzeniu docelowym ma przetwarzać przesłane dane.

Numery portów są dodawane do segmentów na poziomie warstwy czwartej (przez protokoły TCP i UDP). Numery portów zapewniają, że dane zostaną przetworzone przez konkretną aplikację. Na przykład podczas pobierania stron WWW zapytanie ze strony przeglądarki jest wysyłane na port 80 wybranego serwera WWW. Portem nadającym jest pierwszy wolny port powyżej 1023. Dane trafiają do serwera WWW na port 80 — jest to port, za którego obsługę odpowiada serwer HTTP. Serwer WWW wysyła dane (wybraną stronę) do klienta, kierując odpowiedź na port, z którego przyszło zapytanie. Komputer odbierający na podstawie portu kieruje odebrane dane do przetworzenia przez program, który wysłał zapytanie.

Oczywiście port 80 jest standardową i najczęściej spotykaną konfiguracją dla serwerów WWW, lecz ta usługa może nasłuchiwać na każdym innym wybranym przez administratora porcie.

Numery portów do numeru 1023 są przypisywane znanym usługom sieciowym, na przykład 21 — FTP, 22 — SSH, 23 — Telnet, 25 — SMTP, 80 — HTTP, 110 — POP3. Numery portów powyżej 1024 są przydzielane dynamicznie programom, które korzystają z połączeń sieciowych.

4.5. Adresacja IP

Protokół IP jest podstawowym protokołem sieciowym, używanym zarówno w sieciach lokalnych, jak i w internecie. Znajomość sposobu adresacji ma kluczowe znaczenie dla zrozumienia transmisji danych między sieciami.

Każde urządzenie podłączone do sieci działającej z wykorzystaniem protokołu IP powinno mieć niepowtarzalny identyfikator tworzony przez parę adres IP – maska podsieci.

4.5.1. Protokół IPv4

Adres IPv4 to liczba 32-bitowa podzielona na cztery oktety, składające się z liczb dziesiętnych z zakresu 0 – 255, rozdzielonych kropkami. Każda część odpowiada kolejnym 8 bitom adresu zapisanego w systemie binarnym. Taka postać adresu jest łatwiejsza do zapamiętania niż jedna liczba z zakresu $0 – 2^{32}$.

Przykład 4.3. Porównanie różnych sposobów zapisu tej samej liczby:

- zapis binarny: 11000000101010000000000000000001,
- zapis dziesiętny: 3 232 235 521,
- zapis tradycyjny: 192.168.0.1.

Jak widać, zapis w postaci czterech części oddzielanych kropką jest czytelniejszy i łatwiejszy do zapamiętania.

Klasa adresu IP

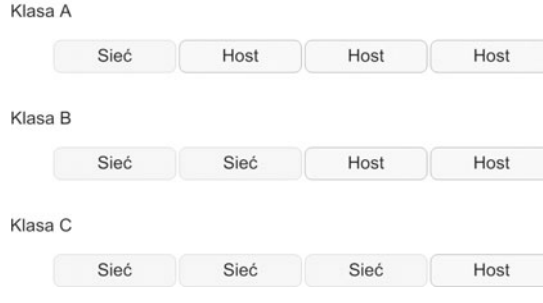
Dla adresów zgrupowanych w klasach przyjęto domyślne maski podsieci: 8-bitową dla klasy A, 16-bitową dla klasy B i 24-bitową dla klasy C. Maski podsieci (opisane dalej) określają, które bity w adresie identyfikują sieć, a które hosta (tabela 4.3).

Tabela 4.3. Klasy adresów IP

Klasa	Zakres adresów (pierwszy oktet)	Dostępne adresy	Maska
A	0 – 126 127 – adres używany do pętli zwrotnej, nieroutowany	1.0.0.0 – 126.0.0.0	255.0.0.0
B	128 – 191	128.1.0.0 – 191.254.0.0	255.255.0.0
C	192 – 223	192.0.1.0 – 223.255.254.0	255.255.255.0
D	224 – 239	224.0.0.0 – 239.255.255.254	-
E	240 – 255	240.0.0.0 – 255.255.255.255	-

W adresach z klasy A sieć jest identyfikowana przez pierwszych 8 bitów, tak więc w zapisie dziesiętnym identyfikator sieci jest określany przez pierwszą liczbę. Pozostałe bity identyfikują hosta pracującego w danej sieci (komputer, router, drukarkę sieciową).

W puli adresów klasy B dwa pierwsze oktety (16 bitów) identyfikują sieć, pozostała część adresu to identyfikator hosta. Z kolei w klasie C pierwsze 3 liczby dziesiętne (24 bity) identyfikują sieć, natomiast ostatnia liczba jest identyfikatorem hosta (rysunek 4.8).



Rysunek 4.8. Podział adresów na klasy

DEFINICJA

Adres IP ma budowę hierarchiczną. Część adresu IP oznacza identyfikator sieci, a część — identyfikator hosta (urządzenia). Adresy IP zostały pogrupowane w **klasy**. Klasa to logiczny podział puli adresów IP nazywany kolejnymi literami alfabetu (od A do E).

Klasa A zawiera adresy, których pierwszy bit to **0**, tak więc w adresach z tej klasy pierwsza część adresu należy do zakresu 0 – 127. Nie używa się adresu 0, z kolei adresy rozpoczynające się od 127 to adresy zarezerwowane dla tzw. pętli zwrotnej i niewykorzystywane do adresowania urządzeń sieciowych.

Klasa B jest oznaczana przez pierwsze 2 bity o wartości **10** (zakres adresów 128 – 191).

Klasa C jest oznaczana przez pierwsze 3 bity o wartości **110** (zakres adresów 192 – 223).

Klasa D jest oznaczana przez pierwsze 4 bity o wartości **1110** (zakres adresów 224 – 239).

Klasa E jest oznaczana przez pierwsze 4 bity o wartości **1111** (zakres adresów 240 – 255).

W adresowaniu urządzeń sieciowych wykorzystuje się tylko adresy z **klasy A**, **B** i **C**. Adresy z **klasy D** pozwalają na przesyłanie informacji do grupy adresów IP, dzięki czemu pojedyncze urządzenie podłączone do sieci jest w stanie rozsyłać informacje jednocześnie do wielu odbiorców (transmisja typu *multicast*). Z kolei pula adresów należąca do **klasy E** została zarezerwowana przez Internet Engineering Task Force — organizację odpowiedzialną za ustanawianie standardów w internecie.

Podział na klasy został wprowadzony w celu rozróżnienia wielkości sieci. Komunikacja w obrębie jednej sieci nie wymaga używania routerów, które są niezbędne w przypadku komunikacji między sieciami.

W przypadku klasy A istnieje możliwość utworzenia 126 użytecznych adresów sieci — od 1 do 126 (adres 0.0.0.0 nie jest wykorzystywany, sieć 127.0.0.0 jest siecią zarezerwowaną). Dla każdej z tych sieci można utworzyć po 16 777 216 adresów. Liczba adresów IP w sieci jest wyliczana na podstawie wzoru:

$L_{IP} = 2^n$,

gdzie: L_{IP} — liczba adresów IP w sieci (liczba adresów do wykorzystania wymaga odjęcia pierwszego i ostatniego adresu rozgłoszeniowego), n — liczba bitów w części hosta.

Dla klasy B istnieje możliwość utworzenia 16 384 sieci. Liczba ta wynika z możliwych kombinacji w części sieci adresu — 64 kombinacje w pierwszym oktecie i 256 kombinacji w drugim. W każdej sieci należącej do klasy B istnieje możliwość zaadresowania 65 536 adresów (2^{16}).

W klasie C istnieje możliwość utworzenia ponad 2 mln sieci ($32 \cdot 256 \cdot 256 = 2\,097\,152$) po 256 adresów ($2^8$).

Do przypisania można wykorzystać ogólną liczbę zmniejszoną o 2. Tak więc, na przykładzie klasy C, do wykorzystania mamy 254 adresy.

Tabela 4.4 prezentuje właściwości poszczególnych klas adresów.

Tabela 4.4. Liczba adresów dostępnych w poszczególnych klasach

Klasa adresu	Liczba bitów części sieci	Liczba bitów części hosta	Liczba dostępnych sieci	Liczba dostępnych adresów w sieci
Klasa A	8	24	127	16 777 214
Klasa B	16	16	16 384	65 534
Klasa C	24	8	2 097 152	254

Adres sieci i adres rozgłoszeniowy

Dla każdego adresu IP przypisanego do konkretnego urządzenia można określić dwa specyficzne adresy — adres sieci i adres rozgłoszeniowy.

Adres sieci (ang. *network address*) określa sieć, do której przynależy dany adres IP. **Adres rozgłoszeniowy** (ang. *broadcast*) to adres pozwalający na wysłanie informacji do wszystkich urządzeń w danej sieci.

Adres sieci jest określany jako liczba, która w części adresu IP identyfikującej hosta ma bity ustawione na 0. Adres rozgłoszeniowy dla danej sieci w części hosta ma bity ustawione na 1.

Adresy sieci są wykorzystywane w procesie przełączania pakietów IP — routery przechowują w tablicach routingu adresy sieci oraz adresy, przez które są one dostępne.

Sposób wyznaczania adresu sieci oraz adresu rozgłoszeniowego przedstawia przykład 4.4.

Przykład 4.4. Wyznaczanie adresu sieci oraz adresu rozgłoszeniowego

Adres IP:	77.213.126.82
Postać binarna:	01001101 11010101 01111110 01010010

Jest to adres z klasy A, więc część sieci jest określana przez pierwsze 8 bitów, a adres sieci uzyskuje się przez ustawienie na ostatnich 24 bitach liczby 0.

Postać binarna adresu sieci:	01001101 00000000 00000000 00000000
Postać dziesiętna adresu sieci:	77.0.0.0
Postać binarna adresu rozgłoszeniowego:	01001101 11111111 11111111 11111111
Postać dziesiętna adresu rozgłoszeniowego:	77.255.255.255

Maska podsieci

Podział adresów na klasy wprowadzono w celu zróżnicowania wielkości sieci. Niestety podział ten powodował, że wiele adresów IP pozostawało niewykorzystanych. Organizacje otrzymywały pulę adresów całej sieci, a więc w przypadku sieci klasy A ponad 16 mln adresów IP do wykorzystania. Szybki rozwój internetu w latach 90. XX wieku i ogromna liczba przyłączanych do sieci urządzeń spowodowały konieczność wprowadzenia innego podziału na część sieci i część hosta. W celu zmiany sztywnego podziału adresu IP na część sieci i część hosta wprowadzono maskę podsieci.

DEFINICJA

Maska podsieci (ang. *subnet mask*), podobnie jak adres IP, jest liczbą 32-bitową rozpoczynającą się określoną liczbą bitów o wartości 1, po których jest dopełniana bitami o wartości 0. Najczęściej przedstawiano ją jako cztery liczby dziesiętne oddzielone kropkami (np. 255.255.255.0). Alternatywnie maska podsieci jest zapisywana po znaku „/" jako liczba „aktywnych" bitów (np. 77.213.62.82/8 oznacza 77.213.62.82/255.0.0.0).

Kolejny bit w masce podsieci określa przynależność do części sieci lub hosta kolejnego bitu w adresie IP. **Bit maski oznaczony 1** mówi, że ten bit w adresie IP należy do części sieci, **bit oznaczony 0** mówi, że odpowiadający mu bit w adresie IP należy do części hosta.

Przykład 4.5. Zapis maski podsieci

Adres IP:	77.213.62.82
Postać binarna:	01001101 11010101 01111110 01010010
Maska podsieci:	255.0.0.0
Postać binarna maski:	11111111 00000000 00000000 00000000

Podział sieci na podsieci

Algorytm dzielenia sieci na podsieci polega na znajdowaniu optymalnego podziału bitów należących do części hosta adresu IP. W zależności od założeń problemu określamy liczbę bitów:

- należących do części podsieci (tak zwana pożyczka bitów z części hosta),
- należących do części hosta (liczba bitów do pozostawienia w części hosta).

Gdy zadana jest liczba wymaganych adresów w nowo tworzonej podsieci (z uwzględnieniem adresu sieci i adresu rozgłoszeniowego), znajdujemy taką liczbę bitów, na której można zapisać wymaganą liczbę adresów. Ta liczba odpowiada liczbie bitów w masce podsieci oznaczonej jako **0** i jest równa najmniejszej potędze liczby **2**, która jest większa lub równa wymaganej liczbie adresów IP. Ilustruje to wzór:

$2^n >= L_{IP} + 2$,

gdzie: L_{IP} — liczba adresów IP w podsieci, n — liczba bitów w masce podsieci oznaczających część hosta. Mając wyznaczoną prawidłową liczbę n, w masce podsieci oznaczamy liczbą **0** n najmłodszych bitów (znajdujących się po prawej stronie), pozostałe bity w masce oznacza się liczbą **1**.

Natomiast gdy zadana jest liczba podsieci, określamy minimalną liczbę bitów, która pozwoli zapisać liczbę większą lub równą wymaganej liczbie podsieci. Liczba ta jest najmniejszą potęgą liczby 2, która jest większa lub równa zadanej liczbie podsieci. Ilustruje to wzór:

$2^n >= L_{SUB}$,

gdzie: L_{SUB} — liczba podsieci, n — liczba bitów w części hosta oryginalnej maski oznaczających część sieci. Wyznaczona liczba n bitów określa liczbę bitów oznaczonych jako **1** w części hosta standardowej maski podsieci. Pozostałe bity są oznaczane jako **0**.

Przykład 4.6. Podział sieci klasy B 172.20.0.0 na 20 podsieci po 500 adresów

Do uzyskania 20 podsieci należy zgodnie z powyższym wzorem pożyczyć 5 bitów z części hosta ($2^4 = 16$, $2^5 = 32$; 5 bitów, czyli 32 podsieci). Nie da się uzyskać dokładnie 20 podsieci, z tego powodu, że nie da się „pożyczyć" ułamka bitu, dlatego zaokrąglamy liczbę podsieci w górę.

Gdy jest już ustalona liczba bitów pożyczonych, trzeba uzyskać liczbę bitów należących do części hosta. 500 hostów na podsieć oznacza 9 bitów ($2^8 = 256$, $2^9 = 512$; 9 bitów, czyli 512 hostów). W rzeczywistości szukamy liczby bitów dla 500 + 2 hostów, zgodnie z pierwszym wzorem, a to dlatego, że dodajemy do poszukiwanej liczby adres sieci i adres rozgłoszeniowy. Tak jak w przypadku obliczania liczby pożyczonych bitów, tak i w przypadku bitów pozostawianych nie da się wyznaczyć dokładnej liczby, dlatego ponownie zaokrąglamy w górę i uzyskujemy 9 bitów pozostawionych, czyli 512 hostów.

Wygląd adresu 172.20.0.0 w postaci binarnej został zaprezentowany w tabeli 4.5.

Tabela 4.5. Binarny zapis adresu IP i maski

	Część sieci	**Część hosta**	
Adres IP	10101100.00010100.	00000000.00000000	172.20.0.0
Maska	11111111.11111111.	00000000.00000000	255.255.0.0

Suma bitów pożyczonych i bitów pozostających przy części hosta (5 + 9, czyli 14 bitów) nie przekracza liczby bitów pozostawionych do dyspozycji przez klasę wybraną w tym przykładzie (sieć klasy B – 16-bitowa maska, czyli 16 pierwszych bitów zarezerwowanych, 16 ostatnich bitów do dyspozycji), co oznacza, że ten przykład da się rozwiązać. Jeśli liczba sumy bitów pożyczonych i pozostających przy części hosta jest większa od liczby dostępnych bitów określonych przez klasę, to należy zmienić klasę sieci. Gdy zmiana nie jest możliwa na taką, która oferuje większy zakres, oznacza to niestety, że nie da się zadania rozwiązać.

W naszym przypadku oprócz tego, że zmieściliśmy się w liczbie bitów pozostawionych nam przez maskę, to dodatkowo pozostają dwa nieprzypisane bity, które można przeznaczyć na zwiększenie liczby podsieci lub na zwiększenie liczby hostów w podsieci (tabela 4.6).

Tabela 4.6. Wpływ liczby bitów na liczbę podsieci i liczbę adresów

Bity pożyczone	Liczba podsieci	Bity w części hosta	Liczba adresów
5	32	11	2048
6	64	10	1024
7	128	9	512

Optymalnie jest wybrać wariant środkowy, czyli zwiększyć liczbę podsieci i dostępnych hostów (nigdy nie wiadomo, czy w danej podsieci z czasem liczba hostów się nie zwiększy albo czy nie będziemy potrzebować dodatkowych podsieci). Maska docelowej sieci została ustalona na 22 bity (16 bitów podstawowych z części sieci + 6 bitów pożyczonych) (tabela 4.7).

Tabela 4.7. Binarna postać adresu w przypadku maski 22-bitowej

	Część sieci	Bity pożyczone	Część hosta	
Adres IP	10101100.00010100.	000000	00.00000000	172.20.0.0
Maska	11111111.11111111.	111111	00.00000000	255.255.252.0

W tej chwili mamy już wszystkie potrzebne dane, aby zacząć tworzyć zakresy adresów IP każdej z podsieci. Sam schemat jest prosty i przedstawiony przykład obejmuje tylko kilka pierwszych i ostatnią podsieć.

Tabela 4.8. Końcowy podział sieci na podsieci

		Część sieci	Bity pożyczone	Część hosta	
Podsieć 1	Adres sieci	10101100.00010100.	000000	00.00000000	172.20.0.0
	Pierwszy adres IP	10101100.00010100.	000000	00.00000001	172.20.0.1
	Ostatni adres IP	10101100.00010100.	000000	11.11111110	172.20.3.254
	Adres rozgłoszeniowy	10101100.00010100.	000000	11.11111111	172.20.3.255
Podsieć 2	Adres sieci	10101100.00010100.	000001	00.00000000	172.20.4.0
	Pierwszy adres IP	10101100.00010100.	000001	00.00000001	172.20.4.1
	Ostatni adres IP	10101100.00010100.	000001	11.11111110	172.20.7.254
	Adres rozgłoszeniowy	10101100.00010100.	000001	11.11111111	172.20.7.255

		Część sieci	Bity pożyczone	Część hosta	
Podsieć 3	Adres sieci	10101100.00010100.	000010	00.00000000	172.20.8.0
	Pierwszy adres IP	10101100.00010100.	000010	00.00000001	172.20.8.1
	Ostatni adres IP	10101100.00010100.	000010	11.11111110	172.20.11.254
	Adres rozgłoszeniowy	10101100.00010100.	000010	11.11111111	172.20.11.255
(...)					
Podsieć 128	Adres sieci	10101100.00010100.	111111	00.00000000	172.20.252.0
	Pierwszy adres IP	10101100.00010100.	111111	00.00000001	172.20.252.1
	Ostatni adres IP	10101100.00010100.	111111	11.11111110	172.20.255.254
	Adres rozgłoszeniowy	10101100.00010100.	111111	11.11111111	172.20.255.255
	Maska	11111111.11111111.	111111	00.00000000	255.255.252.0

Jak widać w tabeli 4.8, uzyskaliśmy 128 podsieci, każda o liczbie 1022 użytecznych hostów (2n – 2, czyli 210 – 2 = 1024 – 2 = 1022).

Pętla zwrotna

W puli wszystkich adresów IP istnieje zakres adresów, które zostały zarezerwowane do specyficznego wykorzystania. Jednym z takich zakresów jest **sieć 127.0.0.0**, czyli adresy IP z przedziału 127.0.0.1 – 127.255.255.254. Adresy te są wykorzystywane w celu adresowania komputera (urządzenia) lokalnego. Komunikacja z tym adresem odwołuje się do urządzenia, które tę komunikację wywołało.

DEFINICJA

Mechanizm tej komunikacji jest nazywany **pętlą lokalną** lub **pętlą zwrotną** (ang. *loopback*). Pętla zwrotna to wirtualne urządzenie sieciowe, które z poziomu systemu operacyjnego nie różni się od fizycznej karty sieciowej. Komunikacja z adresem pętli zwrotnej może odbywać się poprzez dowolny adres należący do sieci 127.0.0.0 lub poprzez nazwę *localhost* (w systemie operacyjnym nazwa przypisana dla adresu 127.0.0.1). Za konfigurację pętli lokalnej odpowiada plik *hosts*, który, w systemie Windows, znaleźć można w katalogu *Windows/System32/drivers/etc/*, natomiast w Linuksie w */etc/*.

Mechanizm pętli zwrotnej może być wykorzystywany do kontroli poprawności instalacji obsługi protokołu IP w systemie operacyjnym.

Adresy prywatne i adresy publiczne

Część adresów IP jest wykorzystywana do adresowania urządzeń w sieciach lokalnych. Sieci lokalne działają na ograniczonym obszarze. Komunikacja między urządzeniami w tej sieci nie wymaga przypisywania im tzw. adresów publicznych. **Adresy prywatne** to adresy niepowtarzalne w ramach struktury sieci lokalnej, **adresy publiczne** są unikalne w skali całego internetu. Takie same adresy prywatne mogą być używane w wielu sieciach lokalnych. Adresy publiczne są przypisywane tylko i wyłącznie jednemu interfejsowi sieciowemu.

Zakresy adresów prywatnych:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Jak widać, w każdej klasie zostały wyznaczone adresy prywatne do wykorzystania w sieciach lokalnych, dzięki czemu istnieje możliwość budowy dowolnej, nawet bardzo rozbudowanej struktury sieci. Dostęp do internetu dla urządzeń z prywatnymi adresami IP jest możliwy dzięki zastosowaniu technologii translacji adresów.

Translacja adresów

Wzrost liczby komputerów w internecie spowodował, że groźba wyczerpania puli dostępnych adresów publicznych stała się całkiem realna. Aby temu zaradzić, przyjęto zasadę, że lokalne sieci komputerowe korzystające z adresów prywatnych (specjalna pula adresów tylko dla sieci lokalnych) mogą zostać podłączone do internetu przez router, mający mniej adresów publicznych, niż jest komputerów w tej sieci.

Router ten, gdy komputery z sieci lokalnej komunikują się ze światem, dynamicznie przekłada adresy prywatne na adresy publiczne, umożliwiając dostęp do zasobów sieci internet przez większą liczbę urządzeń, niż pozwalałaby na to dostępna liczba adresów zewnętrznych. Technika ta polega na zmianie adresów i portów źródłowych (dla pakietów wychodzących) lub docelowych (dla pakietów przychodzących). Adresem nadawcy pakietu staje się router z publicznym adresem IP, który również nadaje numer portu. Takie przekierowanie jest zapisywane w tablicy. Pakiety, które wracają do routera, są modyfikowane na podstawie zapisu w tablicy, otrzymując właściwy adres i port odbiorcy znajdującego się w sieci wewnętrznej (z prywatną adresacją IP).

DEFINICJA

Technologia NAT (ang. *Network Address Translation*) jest wykorzystywana przez niewielkie routery przeznaczone do użytku domowego oraz przez mechanizm udostępniania połączenia internetowego w systemie Windows.

Przydzielanie adresów IP

Adresy IP zwane są również adresami logicznymi. W przeciwieństwie do adresów fizycznych (MAC), przypisanych na etapie produkcji urządzenia, są one nadawane przez administratora sieci. Adres może być przypisany statycznie (ręczna konfiguracja urządzenia) lub dynamicznie — urządzenie otrzymuje wówczas adres z serwera DHCP działającego w sieci.

Serwerem umożliwiającym uzyskanie parametrów konfiguracyjnych takich jak adres IP, maska podsieci, adres bramy domyślnej jest **serwer DHCP** (ang. *Dynamic Host Configuration Protocol*). Jest on następcą protokołu BOOTP (ang. *BOOTstrap Protocol*). Urządzenie, które nie ma statycznie przypisanego adresu IP, wysyła do wszystkich komputerów w sieci (*broadcast*) zapytanie o parametry konfiguracyjne. Jeśli w sieci znajduje się serwer DHCP, odpowiada on na prośbę, wysyłając parametry takie jak adres IP, maska podsieci, brama domyślna i adres serwera DNS. Jeśli w sieci nie działa serwer DHCP lub nie jest on dostępny, to uruchomiony zostaje mechanizm APIPA (ang. *Automatic Private IP Addressing*). Jego zadaniem jest przypisanie adresu IP w przypadku nieotrzymania go od serwera działającego w sieci. Mechanizm APIPA przydziela adres z puli 169.254.0.1 – 169.254.255.254 (sieć 169.254.0.0, maska podsieci 255.255.0.0).

Dynamiczne konfigurowanie adresów pozwala na łatwiejsze zarządzanie siecią. Konfiguracja serwera umożliwia przypisywanie stałych adresów IP na podstawie adresów MAC, jak również przypisywanie adresów na zadany czas.

4.5.2. Protokół IPv6

Adresacja w sieci internet w chwili obecnej opiera się na protokole IP w wersji 4. (*IPv4*, ang. *Internet Protocol version 4*). Adres IP w wersji 4. to liczba 32-bitowa (od 0 do 4 294 967 295). Obecnie liczba publicznych adresów IP jest na wyczerpaniu. Jest to spowodowane dużym przyrostem liczby użytkowników sieci, a co za tym idzie, zwiększonym zapotrzebowaniem na usługi sieciowe, a więc także i adresy IP.

W latach 90. ubiegłego wieku podjęto prace nad zbudowaniem nowego systemu komunikacji. Stworzono protokół **IPv6 / IPNG** (ang. *Internet Protocol version 6* / *Internet Protocol Next Generation*). Protokół ten wprowadza 128-bitową adresację, a więc umożliwia zaadresowanie teoretycznie do 2^{128} urządzeń. Adres IP w wersji 6. jest przedstawiany w postaci szesnastkowej, z dwukropkiem co 16 bitów (np. 32fa:a237:0000:0000:cd21 :1521:1175:67af).

Specyfikacja IPv6 pozwala na pomijanie początkowych zer w bloku, a także na pomijanie kolejnych bloków składających się z samych zer i zastąpienie ich podwójnym dwukropkiem „::”. Dopuszczalny jest tylko jeden podwójny dwukropek „::” w adresie. Poniższy przykład pokazuje równoważne poprawne zapisy jednego adresu IPv6.

Przykład 4.7

5423:0246:0000:0000:0000:0000:2583:fa25

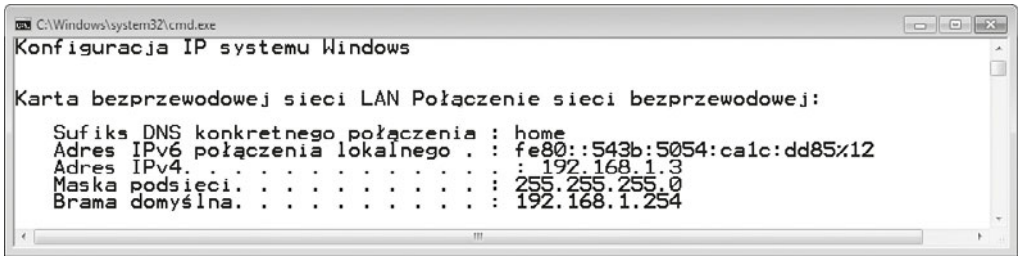
5423:0246:0:0:0:0:2583:fa25

5423:0246:0:0:0::2583:fa25

5423:0246::2583:fa25

5423:246::2583:fa25

Rysunek 4.9 przedstawia przykład adresacji IPv6 w systemie Windows 7.



Rysunek 4.9. Przykład adresacji w Windows 7

Adresy zarezerwowane

W specyfikacji adresacji IPv6 występują adresy specjalne i zarezerwowane do szczególnych celów. Najważniejsze z nich zostały przedstawione poniżej:

::/128 — adres nieokreślony, zawierający same zera.

::1/128 — adres pętli zwrotnej.

::/96 — pula adresów zarezerwowana w celu zachowania kompatybilności wstecznej z aktualnie używaną wersją protokołu IP.

2001:db8::/32 — pula adresów do wykorzystania w przykładach i dokumentacji, nieużywana w produkcyjnie działających systemach.

2002::/24 — są to adresy wygenerowane na podstawie istniejących aktualnie używanych publicznych adresów IPv4.

4.6. Narzędzia diagnostyczne protokołów TCP/IP

Poprawne skonfigurowanie protokołu IP pozwala na pracę z wykorzystaniem zasobów sieciowych. Każdy sieciowy system operacyjny oferuje narzędzia pozwalające sprawdzić poprawność konfiguracji.

4.6.1. Polecenie ipconfig

W systemach Windows poleceniem, które pozwala sprawdzić adresy przypisane do poszczególnych interfejsów, jest `ipconfig`. Narzędzie to pomaga przy wykrywaniu

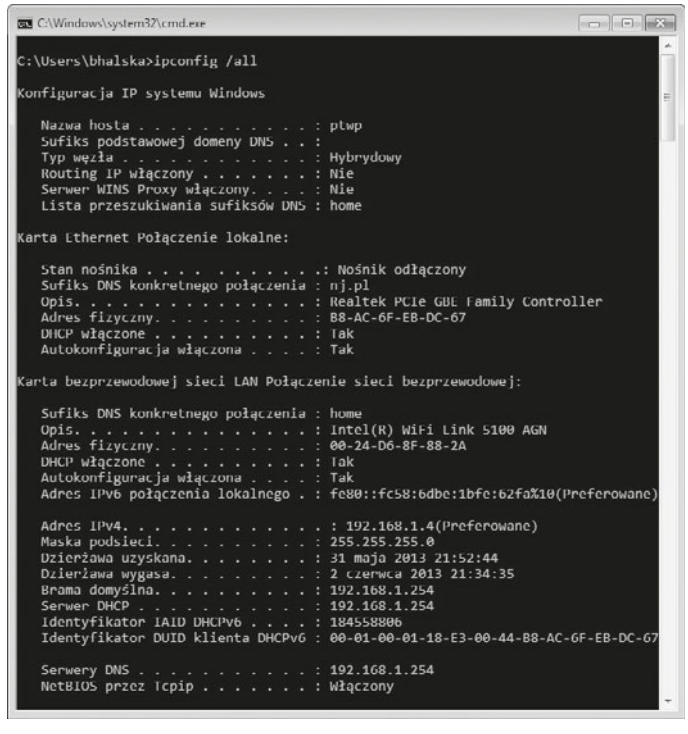
błędów w konfiguracji protokołu IP. Wynik działania polecenia `ipconfig/all` przedstawia rysunek 4.10.

WAŻNE

Najczęściej polecenie `ipconfig` jest wykorzystywane w następujący sposób:

- `ipconfig` — pokazuje skróconą informację o połączeniu.
- `ipconfig /all` — pokazuje szczegółowe dane o konfiguracji wszystkich interfejsów.
- `ipconfig /renew` — odnawia wszystkie karty.
- `ipconfig /release` — zwalnia wszystkie połączenia.
- `ipconfig /?` — wyświetla komunikat pomocy.
- `ipconfig /flushdns` — czyści bufor programu rozpoznającego nazwy DNS.

Rysunek 4.10. Wynik działania polecenia ipconfig/all



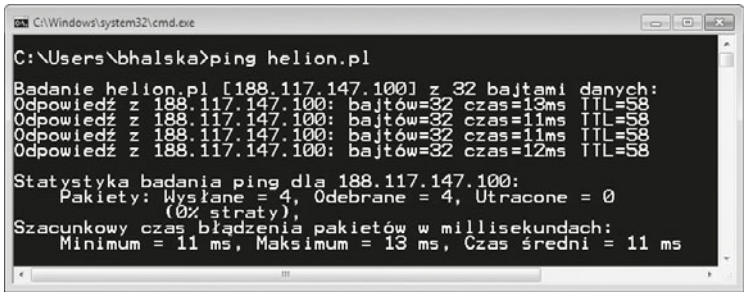
4.6.2. Polecenie ping

Do diagnozowania połączeń w sieciach komputerowych TCP/IP używa się polecenia `ping`. Pozwala ono na sprawdzenie, czy istnieje połączenie między dwoma urządzeniami, i umożliwia sprawdzanie jego jakości poprzez mierzenie liczby zgubionych pakietów

oraz czasu ich dotarcia do celu i z powrotem. Do badania jakości połączenia, `ping` korzysta z protokołu ICMP.

Polecenie `ping` jest dostępne zarówno w systemie Windows, jak i Linux. Aby sprawdzić poprawność konfiguracji połączenia IP, należy użyć składni (rysunek 4.11):

```
ping nazwa_lub_adres_do_sprawdzenia
```



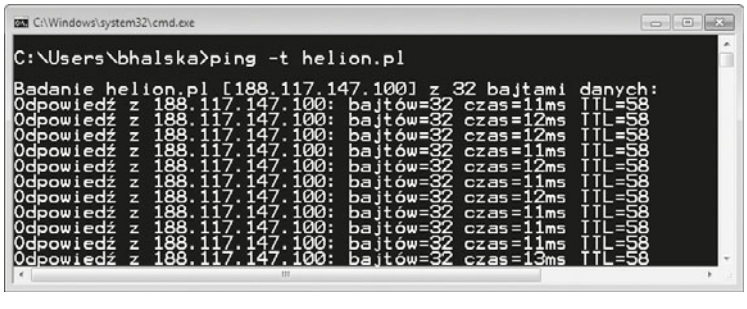
Rysunek 4.11. Wynik działania polecenia ping

Jak widać na rysunku 4.11, program przeprowadził badanie hosta helion.pl, którego adres IP to 188.117.147.100. Test został wykonany przy użyciu 32 bajtów danych (czyli 256 bitów danych). Program ping wysłał czterokrotnie pakiety danych, które dotarły do hosta docelowego w czasach od 11 ms do 13 ms (milisekund). Widoczny tu skrót TTL (ang. *Time To Live*) oznacza czas wygaśnięcia pakietu (maksymalną ilość skoków pakietu), stosowany w celu uniknięcia sytuacji zapętlenia pakietu w sieci, w przypadku np. złej konfiguracji sieci. W tym teście czas życia pakietu to 58. Żaden pakiet nie został utracony, co świadczy o poprawnie skonfigurowanej trasie routingu pomiędzy testowanymi hostami.

W celu otrzymania informacji, jakie funkcje oferuje polecenie `ping`, należy w wierszu poleceń wpisać:

```
ping -?
```

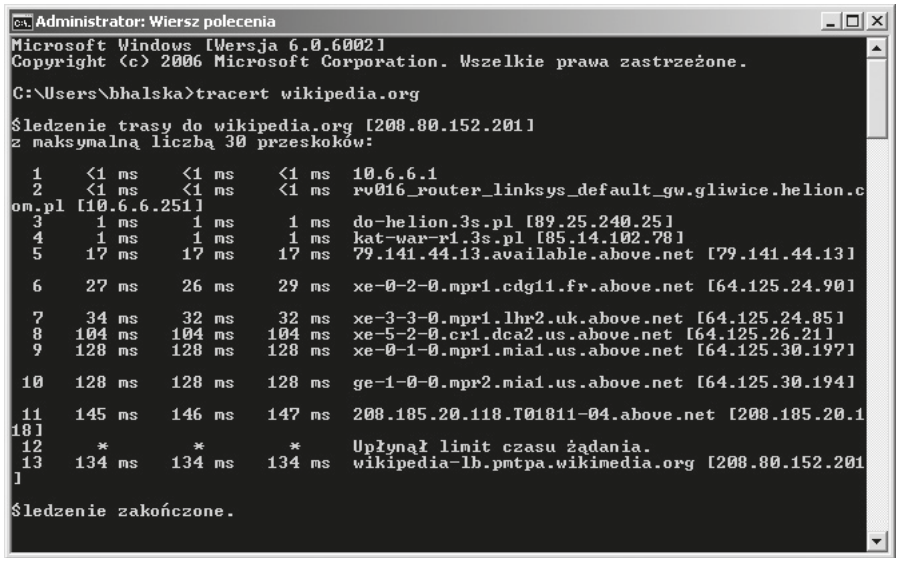
Po jego wpisaniu wyświetlą się wszystkie opcje dostępne dla tego polecenia. Jedną z najczęściej używanych jest `-t`, która powoduje, że adres jest sprawdzany nieustannie, dopóki użytkownik nie przerwie tego procesu (rysunek 4.12).



Rysunek 4.12. Wynik działania polecenia ping -t

4.6.3. Polecenie tracert

Komendą służącą do badania trasy pakietów IP w systemie Windows jest `tracert` (dla systemów Linux komenda `traceroute`). Sprawdza ona czasy dostępu do kolejnych routerów znajdujących się na drodze do adresu docelowego (rysunek 4.13).



Rysunek 4.13. Wynik działania funkcji tracert

WAŻNE

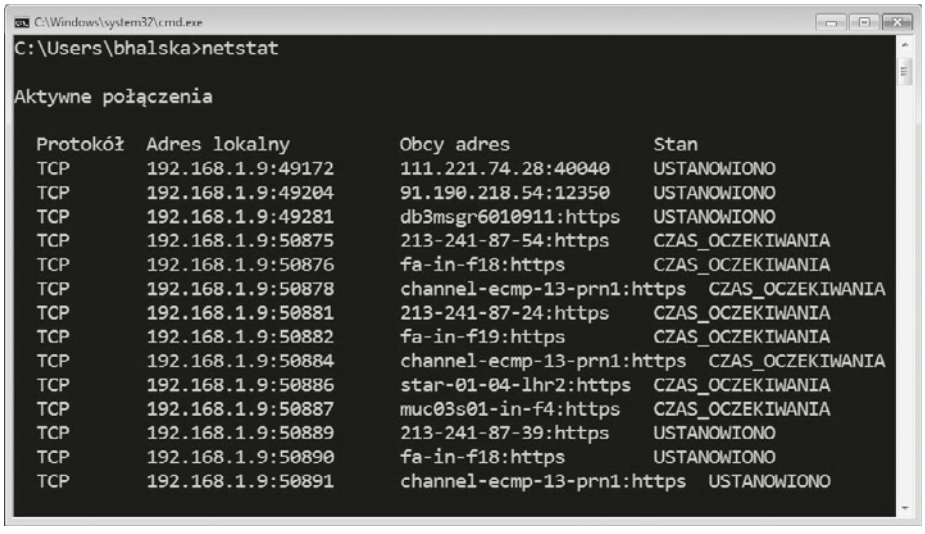
Często z wyników działania programu można odczytać przebieg wędrówki pakietów po sieci, ponieważ niektóre nazwy routerów zawierają ich lokalizację. W przykładzie podanym na rysunku 4.7 pakiety pokonały trasę z Katowic (z adresu **kat**-war-r1.3s.pl), przez Francję (xe-0-2-0.mpr1.cdg11.**fr**.above.net), Wielką Brytanię (xe-3-3-0.mpr1.lhr2.**uk**.above.net), do USA (xe-5-2-0.cr1.dca2.**us**.above.net).

4.6.4. Polecenie netstat

Polecenie `netstat` jest jednym z najbardziej rozbudowanych poleceń, pozwalającym na sprawdzanie połączeń sieciowych (rysunek 4.14). Dostępne jest zarówno dla systemu Windows, jak i Linux. Umożliwia wyświetlanie aktywnych połączeń sieciowych TCP, a także portów, na których komputer nasłuchuje, tabeli routingu, statystyk itp.

Polecenie `netstat` użyte bez parametrów powoduje wyświetlenie aktywnych połączeń protokołu TCP. Inne najważniejsze parametry polecenia w systemie Windows to:

- `-a` — służy do wyświetlania wszystkich aktywnych połączeń oraz portów nasłuchu protokołów TCP i UDP.



Rysunek 4.14. Przykład wykorzystania polecenia netstat — tablica routingu

- `-b` — służy do wyświetlania aktywnych połączeń protokołu TCP i nazw programów, które są przypisane do obsługi danego portu.
- `-e` — wyświetla statystykę sieci Ethernet. `-n` — wyświetla aktywne połączenia TCP (adresy i numery portów są wyrażane numerycznie).
- `-o` — wyświetla aktywne połączenia TCP i identyfikatory procesów (PID) poszczególnych połączeń.
- `-p` *protokół* — ukazuje połączenia wybranego protokołu (udp, tcpv6, tcp lub udpv6).
- `-s` — służy do wyświetlania oddzielnych statystyk dla poszczególnych protokołów.
- `-r` — służy do wyświetlania zawartości tabeli trasowania protokołu IP.

ĆWICZENIA

1. Wyświetl trasę routingu.
2. Sprawdź działanie poleceń: `ping`, `netstat`, `tracert`.
3. Sprawdź adres bramy domyślnej dla swojego komputera.
4. Sprawdź adres IP swojego komputera.

PYTANIA

1. Wymień wszystkie warstwy modelu OSI. Jakie funkcje pełnią one w transmisji danych?
2. Czym różni się model TCP/IP od modelu OSI?
3. Jakie urządzenia działają w warstwie dostępu do sieci oraz w warstwie internetu?
4. Wymień protokoły warstwy sieci.
5. Wymień protokoły warstwy aplikacji.
6. Czym różni się protokół TCP od UDP?
7. Jakie wpisy zawiera tablica routingu?
8. Wymień trzy protokoły routingu. Jakie jest ich zadanie?
9. Co oznacza termin gniazdo w przypadku transmisji sieciowej?
10. W której warstwie modelu ISO pracują switche?
11. Na jakich portach pracują takie usługi, jak FTP, SMTP, HTTP?
12. Wymień protokoły warstwy aplikacji.
13. Z ilu bitów składa się adres IPv4?
14. Z ilu bitów składa się adres IPv6?
15. Jak wygląda adres pętli zwrotnej w IPv4?
16. Jak wygląda adres pętli zwrotnej w IPv6?

5

Urządzenia sieciowe

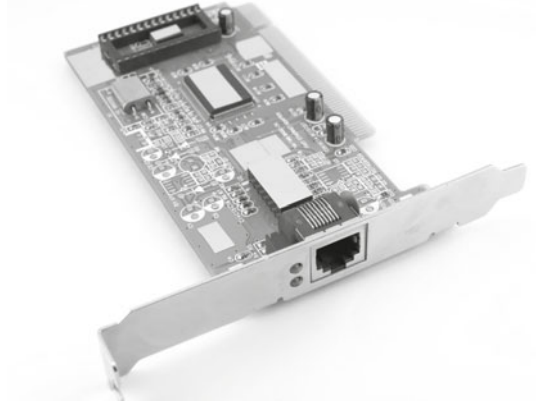
Urządzenia sieciowe, które są przyłączane bezpośrednio do segmentu sieci, można podzielić na dwie grupy:

- urządzenia końcowe — komputery (hosty), drukarki i inne urządzenia wykonujące usługi bezpośrednio dla użytkownika,
- urządzenia tworzące infrastruktury sieci — wszystkie urządzenia, które łączą urządzenia końcowe. Umożliwiają w ten sposób komunikację między nimi (np. routery, przełączniki, wtórniki, koncentratory, mosty itp.).

5.1. Karta sieciowa

DEFINICJA

Karta sieciowa (ang. *NIC Network Interface Card*) to urządzenie zapewniające komunikację z siecią komputerową. W komputerach stacjonarnych występuje ona jako karta rozszerzeń (rysunek 5.1) lub jest wbudowana na płycie głównej. Dostępne są również karty do połączeń bezprzewodowych podłączane jako karta rozszerzeń (rysunek 5.2), port **USB** (rysunek 5.3), **PCMCIA** (rysunek 5.4). Karta sieciowa funkcjonuje w warstwie fizycznej modelu ISO/OSI.



Rysunek 5.1. Karta sieciowa przewodowa podłączana jako karta rozszerzeń

Rysunek 5.2. Bezprzewodowa karta sieciowa podłączana jako karta rozszerzeń

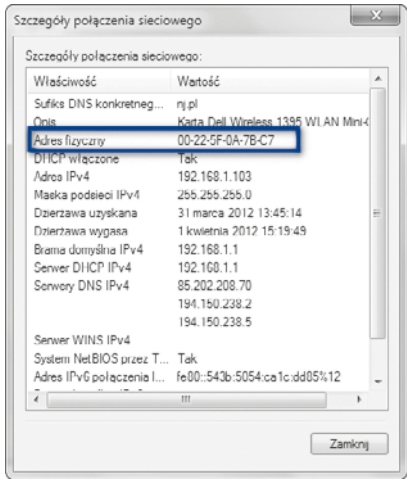
Rysunek 5.3. Bezprzewodowa karta sieciowa podłączana do USB

Rysunek 5.4. Bezprzewodowa karta sieciowa PCMCIA

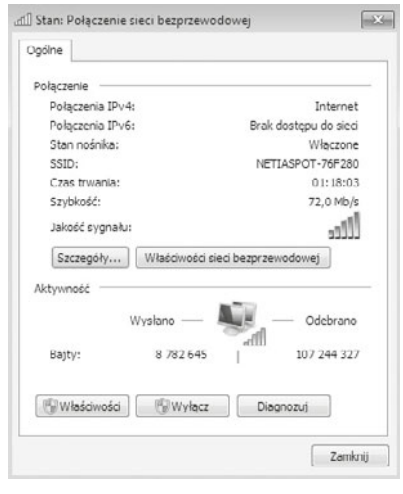
W przypadku urządzeń peryferyjnych pracujących w sieci, takich jak drukarka sieciowa czy skaner, **karty sieciowe** są wbudowane w urządzenie, a ich konfiguracja najczęściej odbywa się za pomocą specjalnych aplikacji dostarczanych przez producenta.

Przy wyborze karty sieciowej trzeba uwzględnić architekturę sieci, w której będzie ona pracowała. Najczęściej spotykane są karty sieciowe pracujące w standardzie **Ethernet, Fast Ethernet, Gigabit Ethernet**.

Każda karta sieciowa ma zapisany przez producenta unikalny adres fizyczny, zwany **MAC** (od ang. *Media Access Control*). Adres ten jest wykorzystywany podczas transmisji w drugiej warstwie modelu OSI (więcej w rozdziale 4.). Adres **MAC** jest adresem 48-bitowym zapisywanym w postaci 12 liczb szesnastkowych oddzielanych znakiem „-" lub „:" (rysunek 5.5).



Rysunek 5.5. Szczegóły dotyczące karty sieciowej



Rysunek 5.6. Stan połączenia sieciowego

UWAGA

Najprostszym sposobem na uzyskanie adresu MAC jest użycie polecenia `ipconfig /all`. Można też go znaleźć, przeglądając szczegóły połączenia sieciowego. Aby to zrobić, w systemach Windows Vista, Windows 7 oraz Windows 8 przechodzimy do *Centrum sieci i udostępniania* w Panelu sterowania, a następnie do konfiguracji wybranego połączenia sieciowego (rysunek 5.6), gdzie po kliknięciu zakładki *Szczegóły* otrzymamy szczegółowe informacje, a wśród nich adres fizyczny naszej karty sieciowej (rysunek 5.5).

5.2. Koncentratory

DEFINICJA

Koncentrator (ang. *hub*) to urządzenie łączące wiele urządzeń pracujących w sieci komputerowej w topologii gwiazdy (rysunek 5.7). Okablowanie biegnące od poszczególnych urządzeń schodzi się w centralnym miejscu sieci, które stanowi koncentrator. Pracuje on w pierwszej warstwie modelu OSI (więcej o modelu OSI w rozdziale 4). Jego zadaniem jest wzmocnienie sygnału przychodzącego i przekazanie go na pozostałe porty. Koncentrator nie może określić źródła ani miejsca docelowego odbieranych informacji, dlatego wysyła je do wszystkich portów. Może wysyłać i odbierać informacje, jednak nie jednocześnie. Mechanizm propagacji sygnałów na wszystkie porty powoduje, że podczas transmisji danych przez tego rodzaju urządzenie istnieje możliwość wystąpienia kolizji spowodowanych równoczesnym nadawaniem przez wiele urządzeń. Obszar sieci, w którym mogą wystąpić kolizje, jest nazywany domeną kolizyjną. Urządzenia podłączone do koncentratorów tworzą jedną domenę kolizyjną. Więcej informacji o sposobie dostępu do mediów w sieci Ethernet znajduje się w podrozdziale 2.2, „Topologie logiczne". Nie ma możliwości zmiany prędkości transmisji.

Wyróżnia się dwa rodzaje koncentratorów:

- **aktywny** — łączy kable oraz regeneruje sygnał, przez co zwiększa zasięg sieci,
- **pasywny** — tylko łączy kable.

Rysunek 5.7.
Koncentrator 4-portowy

5.3. Przełączniki

DEFINICJA

Przełącznik (ang. *switch*), podobnie jak koncentrator, stanowi centralny punkt sieci zbudowanej w topologii gwiazdy. Sygnał wychodzący nie jest jednak przesyłany na wszystkie wyjścia, lecz tylko do portu, do którego podłączone jest urządzenie docelowe będące adresatem danych (rysunek 5.8).

Rysunek 5.8.
Przełącznik

Przełącznik pracuje w warstwie drugiej modelu OSI. Przełączanie ramek jest realizowane na podstawie adresów MAC urządzeń podłączonych do sieci zapisywanych w tablicy adresów MAC.

Tablica adresów MAC jest tworzona dynamicznie podczas pracy urządzenia; jeśli dane są transmitowane do urządzenia o nieznanym adresie, wówczas są przesyłane na wszystkie wyjścia w urządzeniu — urządzenie działa jak koncentrator.

Zastosowanie przełączników ma duży wpływ na efektywne działanie sieci. Przełączanie ramek do odpowiednich portów w urządzeniu powoduje ograniczenie domen kolizyjnych — obszarów sieci, w których mogą występować zakłócenia spowodowane równoczesną transmisją przez wiele urządzeń.

Wygląd zewnętrzny koncentratorów i przełączników jest bardzo podobny, najważniejsza różnica tkwi w sposobie przekazywania sygnałów. Informacje dodatkowe na temat przełączników i ich konfiguracji zostały zawarte w podrozdziale 8.3 — „Konfiguracja przełącznika".

5.4. Routery

Funkcję routera mogą pełnić również serwery, które są podłączone równocześnie do kilku sieci — poprzez karty sieciowe lub karty umożliwiające konfigurację sieci wirtualnych VLAN łączą segmenty sieci lub całe sieci. Zadaniem routerów sprzętowych czy programowych (tych instalowanych na serwerze) jest przesyłanie ramki danych pomiędzy sieciami na podstawie informacji warstwy 3. Routery podejmują decyzje logiczne dotyczące wyboru najlepszej drogi transmisji danych. Następnie pakiety kierowane są

na odpowiedni port wyjściowy, gdzie przeprowadzany jest proces enkapsulacji. Podczas enkapsulacji strumień danych jest dzielony na segmenty, dodawane są odpowiednie nagłówki i stopki, po czym dane zostają przesłane. Procesy enkapsulacji i dekapsulacji zachodzą za każdym razem, gdy pakiet jest przesyłany przez router. Dekapsulacja jest procesem odwrotnym. Nagłówki i stopki są usuwane, a następnie tworzony jest jednolity strumień. Router musi zdekapsułować ramkę warstwy drugiej, aby uzyskać dostęp do nagłówka warstwy trzeciej i odczytać odpowiadający tej warstwie adres. Dodatkowe informacje na temat routingu znajdują się w podrozdziale 4.4, „Zasady transmisji w sieciach TCP/IP".

DEFINICJA

Router (rysunki 5.9 i 5.10) to urządzenie pracujące w warstwie trzeciej modelu OSI, bazujące na adresach **IP**. **Routery** łączą różne rodzaje sieci, pozwalają na przekazywanie pakietów pomiędzy oddzielnymi sieciami logicznymi (sieciami IP), a także pomiędzy sieciami zbudowanymi z wykorzystaniem różnych mediów i technologii transmisyjnych. Routery kierują pakiety do sieci docelowej, wybierając najlepszą dla nich drogę. Operacja ta nazywana jest **rutowaniem** lub **trasowaniem**.

Rysunek 5.9.
Router z modułem WiFi

Rysunek 5.10. Router WiFi – panel tylny. Widoczne elementy (od lewej): antena WiFi, 4 porty LAN, Port WAN, wejście zasilania, przycisk RESET

Router jest urządzeniem niezbędnym do podłączenia sieci lokalnej do internetu. Rozwój technologii oraz dostępność łączy internetowych to przyczyny upowszechniania się niewielkich routerów domowych. Najczęściej mają one jedno łącze do sieci WAN oraz wbudowany przełącznik do podłączenia kilku urządzeń sieci lokalnej. Urządzenia te są wyposażone w dodatkowe funkcje, takie jak **translacja adresów, serwer DHCP, moduł WiFi, porty USB do współdzielenia zasobów lub podłączania modemów 3G/4G**.

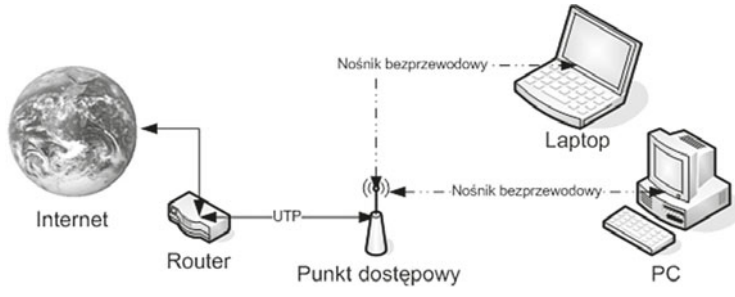
Informacje na temat konfiguracji routerów zostały zawarte w podrozdziale 8.4 — „Konfiguracja routera".

5.5. Punkty dostępowe sieci bezprzewodowych

DEFINICJA

Punkt dostępu lub **punkt dostępowy** (ang. *access point — AP*) — urządzenie, które zapewnia urządzeniom wyposażonym w bezprzewodowe karty sieciowe dostęp do zasobów sieci za pomocą bezprzewodowego medium transmisyjnego (rysunek 5.11).

Rysunek 5.11. Działanie punktu dostępowego



Punkt dostępowy pełni również rolę mostu łączącego sieć bezprzewodową z siecią przewodową (najczęściej Ethernet), dlatego też ma on minimum dwa interfejsy: interfejs bezprzewodowy komunikujący się z sieciami standardu 802.11 oraz drugi, służący do połączenia z siecią przewodową.

Punkty dostępowe mogą komunikować się ze sobą, co umożliwia budowę bardzo rozległych sieci bezprzewodowych.

Dodatkowo większość produkowanych aktualnie punktów dostępowych do zastosowań domowych i małego biznesu (ang. SOHO — *Small Office Home Office*) wyposażona jest również w router, serwer DHCP przydzielający adres sieciowy stacji zaraz po jej połączeniu z punktem dostępowym, część ma też możliwość translacji adresów prywatnych na publiczne (NAT), wiele może buforować ramki w celu oszczędzania energii stacji. Informacje na temat konfiguracji sieci WLAN zostały zawarte w podrozdziale 8.5 — „Konfiguracja urządzeń bezprzewodowych".

5.6. Modemy

DEFINICJA

Modem (ang. *modulator-demodulator*) — urządzenie, którego zadaniem jest zamiana sygnałów (danych) cyfrowych na sygnały analogowe (modulacja) i na odwrót (demodulacja) tak, aby możliwe było przesyłanie i odbieranie danych poprzez linię telefoniczną analogową (ADSL, DSL).

Modemy mogą być podłączane jako karty rozszerzeń do gniazd na płycie głównej lub jako urządzenia zewnętrzne do portów szeregowych COM, portów USB lub portów Ethernet. Najczęściej używanymi urządzeniami tego typu są modemy telefoniczne — zarówno wdzwaniane, jak i modemy technologii xDSL (rysunek 5.12) — a także modemy kablowe wykorzystywane do transmisji danych w sieciach telewizji kablowych.

Rysunek 5.12.
Modem DSL

5.7. Firewall sprzętowy

DEFINICJA

Sprzętowy firewall jest urządzeniem realizującym funkcje zabezpieczające jako dodatkowe urządzenie w sieci. Poza typowymi funkcjami zabezpieczającymi, takimi jak filtrowanie pakietów w sieci, może mieć szereg dodatkowych funkcji, jak np. szyfrowanie przesyłanych danych czy automatyczne powiadamianie administratora systemu o określonych zdarzeniach (przykładowo o włamaniu). Konfiguracja takiego urządzenia może się odbywać bezpośrednio przez podłączenie urządzeń wejścia/wyjścia do firewalla lub pośrednio poprzez przeglądarkę WWW. Sprzętowy firewall często wbudowany bywa również w inne urządzenia sieciowe, np. routery i modemy.

Najczęściej stosowane sprzętowe rozwiązania typu firewall:

- Firewall posiadający dwie karty sieciowe — w tym rozwiązaniu znajduje się pomiędzy siecią lokalną a siecią zewnętrzną. Dzięki temu, że jest podłączony do dwóch sieci, ma dostęp do pakietów danych pochodzących z obu sieci. Oprogramowanie serwera może kontrolować wszystkie przechodzące pakiety i na podstawie ustalonych reguł zezwalać lub nie na ich transmisję do drugiej sieci.
- Firewall z routerem ekranującym — serwer chronionej sieci komputerowej jest oddzielony od innej poprzez router kontrolujący przechodzące pakiety danych oraz ukrywający adresy poprzez usługę NAT.
- Firewall z dwoma routerami ekranującymi: jeden router kontroluje przepływ pakietów danych wewnątrz chronionej sieci komputerowej, natomiast drugi jest odpowiedzialny za transmisję pakietów danych do/z innej sieci. Zaletą jest to, że router podłączony do chronionej sieci może uniemożliwiać uzyskanie nieautoryzowanego dostępu do serwera z innej sieci.

Wydajność firewalla jest w dużym stopniu uzależniona od jego konfiguracji sprzętowej, natomiast o jego możliwościach decyduje sterujące nim oprogramowanie (często można je uaktualniać, zwiększając tym samym funkcjonalność). Dobór odpowiedniego firewalla sprzętowego uzależniony jest od wielkości oraz rodzaju chronionej sieci komputerowej.

Informacje na temat konfiguracji zabezpieczeń sieci zawarte są w podrozdziale 8.4.9, „Konfiguracja zabezpieczeń sieci — firewall".

5.8. Konwertery mediów

DEFINICJA

Konwerter (ang. *transceiver*) mediów jest połączeniem nadajnika i odbiornika (rysunek 5.13). W sieciach informatycznych jest wykorzystywany do konwersji sygnału przesyłanego światłowodem na sygnał przesyłany kablem miedzianym lub odwrotnie. Pracuje w pierwszej warstwie modelu ISO.

Konwertery mediów stosuje się przede wszystkim tam, gdzie zachodzi konieczność zmiany medium transmisyjnego.

Rysunek 5.13.
Mediakonwerter

PYTANIA

1. W jakiej warstwie modelu ISO pracuje karta sieciowa?
2. Czym różni się koncentrator od przełącznika?
3. Jakie zadanie pełni router?
4. Jak nazywa się punkt styku sieci kablowej i bezprzewodowej?
5. W jakiej warstwie modelu ISO pracuje przełącznik?
6. W jakiej warstwie modelu ISO pracuje router?
7. Jakiego urządzenia należy użyć, aby połączyć kilka komputerów w sieć?
8. Jak inaczej nazywa się koncentrator?

6

Konfiguracja sieciowa systemów Windows

System Windows to oprogramowanie, które może być instalowane na stacjach roboczych (np. Windows 8), serwerach (np. Windows Server 2008 R2), a także tabletach (np. Windows 8) czy smartfonach (np. Windows Phone 8). To, jaka wersja jest instalowana, jest uzależnione od funkcjonalności oraz potrzeb użytkownika czy administratora.

Obecnie najbardziej rozpowszechnionym systemem operacyjnym w stacjach roboczych jest system Windows XP, aktualnie z pakietem Service Pack 3 firmy Microsoft. System ten, mimo że został zaprezentowany w roku 2001, nadal funkcjonuje w środowisku sieciowym. Powoli jest jednak wypierany przez system Windows 7, a 8 kwietnia 2014 roku Microsoft kończy wsparcie techniczne dla Windows XP SP3.

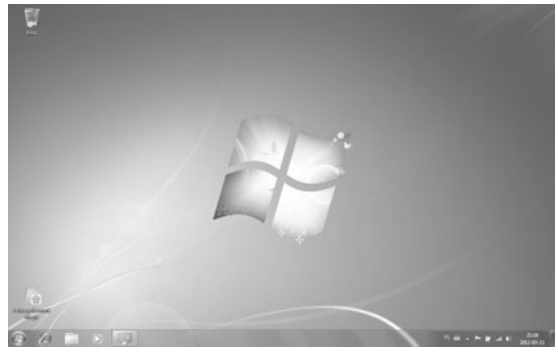
System był dostępny w dwóch wersjach:

- *Home Edition* — wersja dla użytkowników domowych,
- *Professional* — wersja dla firm zawierająca obsługę zasad zabezpieczeń lokalnych oraz obiektów zasad grupy, zapewniająca obsługę wielu procesorów oraz mechanizm uwierzytelniania sieciowego.

Następcą systemu Windows XP został wydany w roku 2006 Windows Vista. Mimo nowych funkcji system nie zdobył zbyt wielkiej popularności. Nowe opcje oraz nowy wygląd spowodowały zwiększenie minimalnych wymagań sprzętowych, przez co system nie działa zbyt wydajnie na starszych komputerach.

System Vista nie zdobył zaufania wśród administratorów, więc po dokonaniu poprawek w 2009 roku został wypuszczony jego następca, Windows 7, który okazał się bardziej wydajny oraz stabilny od Visty i jest aktualnie najbardziej popularnym systemem operacyjnym instalowanym na komputerach osobistych i firmowych (rysunek 6.1).

Rysunek 6.1.
Pulpit systemu Windows 7



System Windows 7 jest dostępny w kilku wersjach:

- Windows 7 Starter (podstawowe wydanie systemu operacyjnego);
- Windows 7 Home Premium (udostępnianie zasobów multimedialnych przy wykorzystaniu Media Center);
- Windows 7 Professional (dla firm, umożliwia podłączanie do domeny, szyfrowanie plików, uruchomienie wirtualnego środowiska Windows XP);
- Windows 7 Ultimate (najbardziej uniwersalna wersja dla firm, która łączy funkcjonalność Home Premium oraz Professional, dodatkowo wyposażona w funkcje BitLocker i BitLocker To Go umożliwiające zabezpieczenie danych);
- Windows 7 Home Basic (wydanie podstawowe, uzupełnione o dodatkowe opcje, przeznaczone dla użytkowników domowych);
- Windows 7 Enterprise (wersja dla klientów umów licencjonowania grupowego, posiada wszystkie opcje edycji Ultimate, różni się jedynie sposobem aktywacji).

Każda z omówionych wersji systemów operacyjnych może współpracować z 32- i 64-bitową architekturą procesora.

Ranking systemów operacyjnych na podstawie strony *ranking.pl* (rysunek 6.2).

Rysunek 6.2.
Statystyczne dane dotyczące popularności systemów operacyjnych w Polsce

SYSTEMY OPERACYJNE — CSV XLS

Lp.	Nazwa	27.02-04.03.2012	20.02-26.02.2012	13.02-19.02.2012
1	Windows XP	45.87%	46.02%	46.26%
2	Windows 7	37.98%	37.85%	37.60%
3	Windows Vista	12.21%	12.30%	12.39%
4	Android	0.99%	0.96%	0.95%
5	Mac OS X	0.84%	0.83%	0.81%
6	Linux	0.73%	0.72%	0.67%
7	iOS	0.49%	0.48%	0.47%
8	Symbian	0.41%	0.40%	0.40%
9	Windows 2000	0.13%	0.13%	0.13%
	Wielkość próby (liczba odsłon)	4 924 105 542	5 148 797 389	5 094 679 148

Pokaż wartości bezwzględne — Znajdź:

Następcą Windows 7 jest Windows 8, który jest dostępny od października 2012 roku. Od poprzedników różni go przede wszystkim nowy interfejs metro, oparty na kolorowych

kafelkach (rysunek 6.3). Każdy taki element na ekranie startowym jest połączony z programem, osobą, stroną internetową, folderem czy jakimkolwiek innym istotnym elementem. Tryb pulpitu znany z poprzednich wersji systemu jest w nim osobną aplikacją.

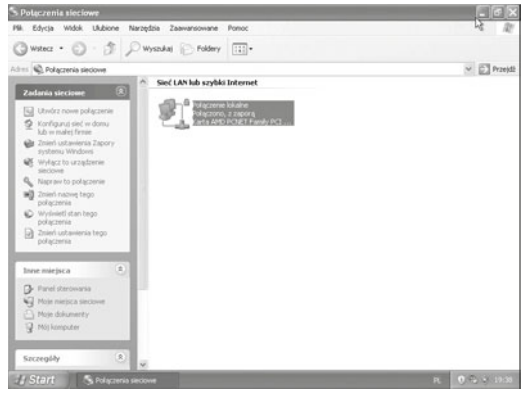
Rysunek 6.3.
Windows 8

6.1. Konfiguracja interfejsów sieciowych

Aby urządzenia w jednej podsieci mogły się ze sobą komunikować, należy przypisać im odpowiednie adresy IP, np. 192.168.1.1, 192.168.1.2 z maską 255.255.255.0 (patrz podrozdział 4.5 — „Adresacja IP"). Konfiguracja odbywa się w przeznaczonych do tego narzędziach:

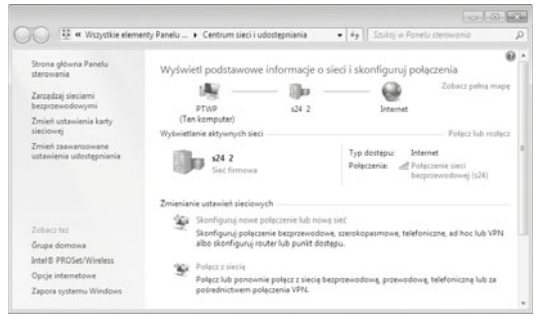
- Windows XP — *Połączenia sieciowe* (rysunek 6.4).

Rysunek 6.4.
Konfiguracja karty sieciowej — Windows XP

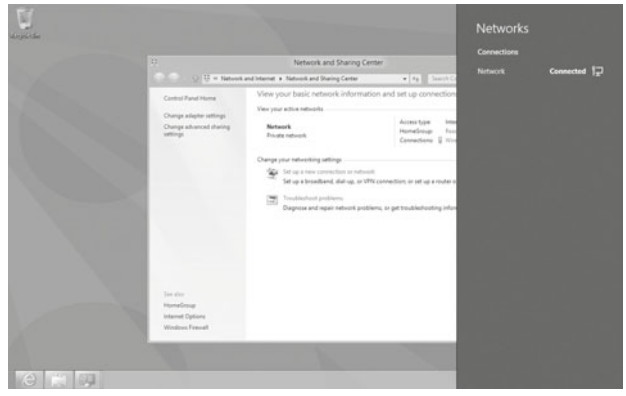


- Windows Vista, 7, 8 — *Centrum sieci i udostępniania* (rysunek 6.5 i 6.6).

Rysunek 6.5.
Konfiguracja karty sieciowej — Windows 7



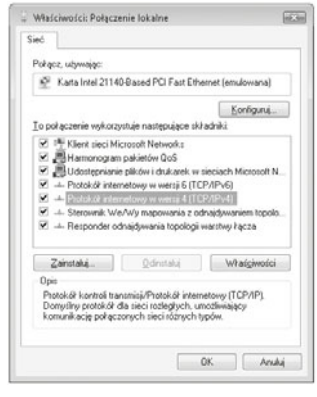
Rysunek 6.6. Konfiguracja karty sieciowej — Windows 8



Aby wybrać konfigurację połączenia z menu kontekstowego, należy kliknąć opcję *Właściwości*. Wyświetlone zostanie okno *Właściwości: Połączenie lokalne*, które pozwala na konfigurację parametrów połączenia.

Najważniejsze ustawienia są dostępne w zakładce *Sieć*, która zawiera spis wszystkich składników sieci wykorzystywanych przez wybrane połączenie. Aby dołączyć nowy składnik, należy wybrać przycisk *Zainstaluj*, aby usunąć — przycisk *Odinstaluj*. Konfiguracja wybranego składnika jest możliwa po wybraniu przycisku *Właściwości* (rysunek 6.7).

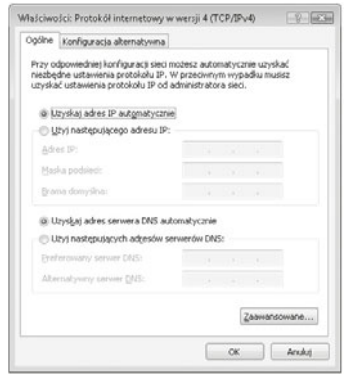
Rysunek 6.7. Okno właściwości połączenia lokalnego



Najważniejszym parametrem dla konfiguracji sieci jest przypisanie adresu IP, który umożliwia jednoznaczne określenie komputera podłączonego do sieci. Adresy IP mogą być wprowadzane ręcznie jako parametr konfiguracji urządzenia lub przypisywane dynamicznie przez serwery działające w sieci. Dodatkowe informacje dotyczące metod automatycznego przydzielania adresów IP zostały zawarte w podrozdziale 4.5 — „Adresacja IP".

Aby przypisać adres IP dla wybranego połączenia sieciowego, należy wskazać składnik *Protokół internetowy* (*TCP/IP*) (lub *Protokół internetowy w wersji 4* (*TCP/IPv4*) w przypadku systemu Windows Vista lub Windows 7), a następnie wybrać przycisk *Właściwości*. Pojawi się wówczas okno konfiguracji adresu IP (rysunek 6.8).

Rysunek 6.8.
Okno właściwości protokołu TCP/IP



Domyślnie zaznaczona jest opcja pozwalająca na pobieranie konfiguracji protokołu TCP/IP z sieci — *Uzyskaj adres IP automatycznie* (rysunek 6.8). Jeśli sieć, do której jest podłączone urządzenie, wymaga ręcznej konfiguracji parametrów, to należy wprowadzić dane otrzymane od administratora sieci. Podstawowe parametry sieci pozwalające na dostęp do sieci lokalnej to:

- *Adres IP* — unikalny identyfikator urządzenia w sieci,
- *Maska podsieci* — liczba określająca przynależność do podsieci.

Natomiast podczas podłączania do sieci zewnętrznej, czyli internetu, należy zdefiniować kolejne parametry:

- *Brama domyślna* — adres routera w sieci (urządzenia zapewniającego połączenie z innymi sieciami),
- *Preferowany serwer DNS*, *Alternatywny serwer DNS* — adresy serwerów, które zapewniają translację nazw domenowych na adresy IP.

Adresy uzyskiwane automatycznie są adresami przydzielanymi przez działający w sieci serwer DHCP. W konfiguracji protokołu IP w systemie Windows przy wyborze automatycznej konfiguracji IP istnieje możliwość zdefiniowania konfiguracji alternatywnej. Są to ustawienia, które są wczytywane, gdy serwer DHCP nie odpowie na żądanie podania adresu.

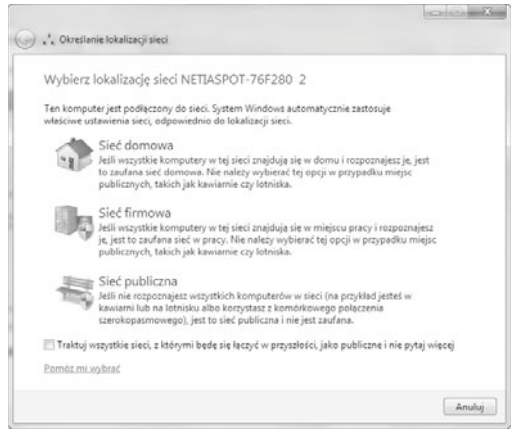
Jeśli konfiguracja alternatywna nie została wprowadzona, wówczas w przypadku braku odpowiedzi z serwera DHCP zostanie uruchomiony mechanizm APIPA (ang. *Automatic Private IP Addressing*), który przypisze adres z puli 169.254.0.1 – 169.254.255.254. Gdy serwer DHCP stanie się osiągalny, wówczas adres zostanie pobrany i wprowadzony do konfiguracji systemu.

Automatyczne przypisywanie adresów IP pozwala na łatwiejsze zarządzanie siecią — adresy są przydzielane przez usługę DHCP, wszelkie zmiany adresacji mogą być przeprowadzone z jednego miejsca. W przypadku ręcznej konfiguracji adresów każdorazowa zmiana w koncepcji adresacji wymaga rekonfiguracji wszystkich urządzeń działających w sieci.

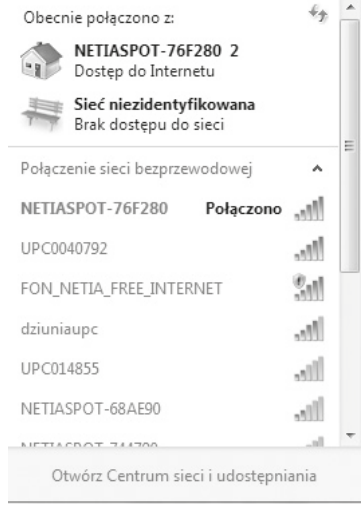
W przypadku systemu Windows 7 po skonfigurowaniu karty sieciowej należy również określić lokalizację sieci (rysunek 6.9), która wiąże się z zaporą sieciową oraz możliwością udostępniania zasobów.

Ostatnie lata przyniosły znaczący rozwój bezprzewodowego dostępu do sieci. Podobnie jak w przypadku kart sieci przewodowej, po zainstalowaniu karty umożliwiającej podłączenie do sieci bezprzewodowej w systemie w oknie *Połączenia sieciowe* dodawana jest ikona opisana jako *Połączenie sieci bezprzewodowej*. Konfiguracja parametrów sieci jest praktycznie taka sama jak w przypadku sieci kablowych, najważniejszą różnicą jest wybór sieci, do której komputer ma zostać podłączony. Po wybraniu w menu kontekstowym połączenia bezprzewodowego opcji *Wyświetl dostępne sieci bezprzewodowe* pojawi się okno z listą osiągalnych sieci radiowych (rysunek 6.10).

Rysunek 6.9. Określanie lokalizacji sieci



Rysunek 6.10. Dostępne sieci bezprzewodowe



Dodatkowe informacje na temat konfiguracji sieci bezprzewodowych zostały zawarte w podrozdziale 8.5 — „Konfiguracja urządzeń bezprzewodowych”.

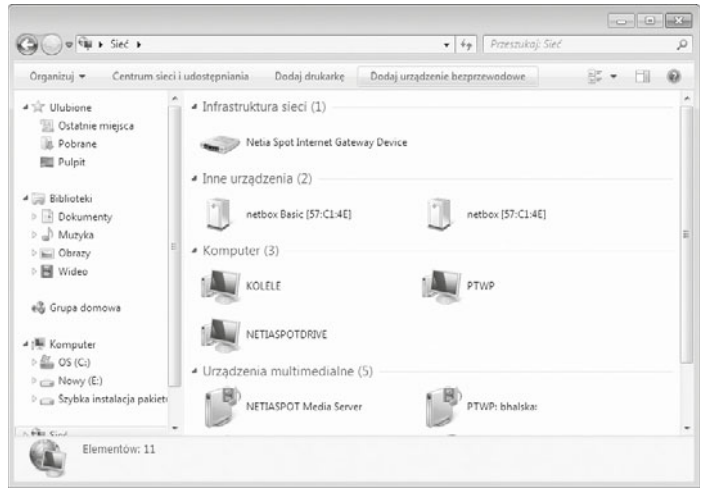
6.1.1. Grupa robocza — sieć równoprawna

Grupa robocza to lokalna sieć komputerowa, w której każdy z komputerów może korzystać z zasobów innych komputerów na tych samych zasadach. Oznacza to, że poszczególne komputery mogą udostępniać swoje zasoby użytkownikom oraz same mogą pobierać dane z innych komputerów pracujących w sieci.

DEFINICJA

Grupa robocza (ang. *workgroup*) to zbiór komputerów pracujących w obrębie lokalnej sieci (określany nazwą tej grupy).

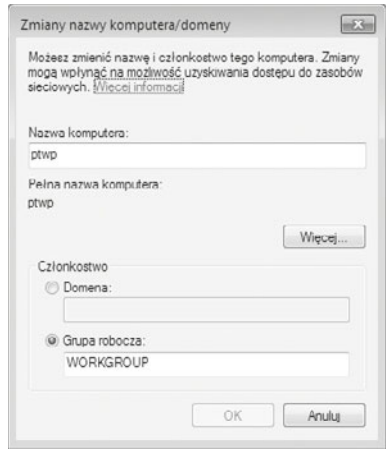
Komputery pracujące w grupie roboczej mogą udostępniać pliki i foldery oraz drukarki. Dostęp do zasobów sieci umożliwia folder *Moje miejsca sieciowe* (lub folder *Sieć* w systemie Windows Vista albo Windows 7, patrz rysunek 6.11) — wyświetla on komputery zgromadzone w dostępnych grupach roboczych. Aby przejrzeć zasoby sieciowe wybranego komputera, należy się z nim połączyć. Windows domyślnie loguje się na zdalnych komputerach z parametrami bieżącego użytkownika systemu. Jeśli taki użytkownik nie istnieje na komputerze zdalnym, wówczas należy podać nazwę i hasło użytkownika, który został dodany w systemie zdalnym.



Rysunek 6.11. Zbiór komputerów oraz urządzeń sieciowych w ramach grupy roboczej

Aby komputer mógł być widoczny wśród innych w otoczeniu sieciowym, musi mieć unikalną nazwę i przynależeć do grupy roboczej. Ustawienia te są dostępne poprzez przystawkę *System*, uruchamiany z Panelu sterowania, w zakładce *Nazwa komputera*. Zakładka zawiera bieżącą nazwę komputera. Aby ją zmienić, należy kliknąć przycisk *Zmień*.

Rysunek 6.12.
Okno umożliwiające zmianę przynależności do grupy roboczej



Nazwa komputera może składać się z liter, cyfr i symboli. Nie może jednak zawierać samych kropek i przekraczać 15 znaków, co związane jest z protokołem NetBIOS obsługującym rozpoznawanie nazw w sieci bez użycia serwera WINS czy DNS.

6.2. Udostępnianie zasobów sieciowych

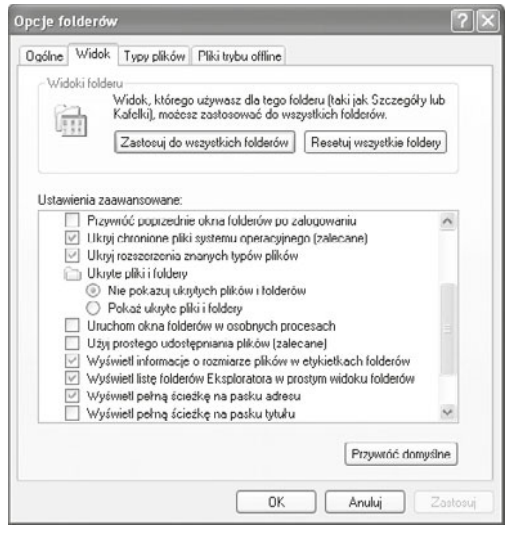
6.2.1. Udostępnianie folderów

System Windows pozwala w przypadku Windows XP na proste oraz klasyczne udostępnianie folderów. Pierwsze z nich pozwala łatwo udostępnić zasób, lecz nie umożliwia zaawansowanej konfiguracji praw dostępu. Klasyczny sposób udostępniania pozwala na kontrolę połączeń na poziomie poszczególnych użytkowników lub grup, a dostęp do plików i folderów jest weryfikowany przez uprawnienia systemu plików NTFS. Możliwa jest także kontrola jednoczesnych połączeń.

Udostępnianie plików w systemie Windows XP

Systemy Windows do zastosowań domowych korzystają tylko z prostego udostępniania plików, systemy dla zastosowań profesjonalnych pozwalają wybrać sposób udostępniania. Aby zmienić sposób udostępniania plików w wersjach profesjonalnych, należy zaznaczyć opcję *Użyj prostego udostępniania plików* (lub usunąć zaznaczenie) w oknie *Opcje folderów* (dostępnym w Panelu sterowania lub w programie Eksplorator Windows z menu *Narzędzia*) w zakładce *Widok* w części *Ustawienia zaawansowane* (rysunek 6.13).

Rysunek 6.13.
Wybór typu udostępniania plików w oknie Opcje folderów

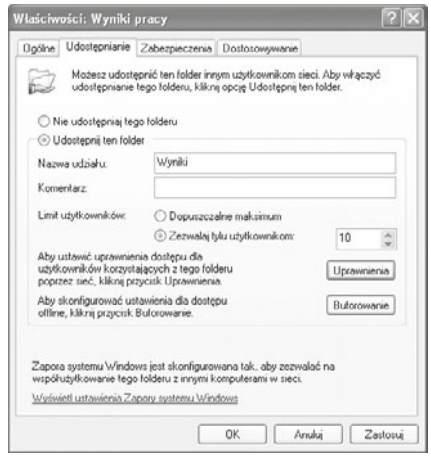


Aby udostępnić konkretny folder w systemie Windows XP, z menu kontekstowego tego folderu należy wybrać opcję *Udostępnianie i zabezpieczenia* (rysunek 6.12). W przypadku udostępniania prostego należy zaznaczyć opcję *Udostępnij ten folder w sieci* oraz podać nazwę, pod którą zasób będzie widoczny w sieci (rysunek 6.14). Nazwa zasobu nie musi być taka sama jak nazwa folderu. Jeśli użytkownicy zdalni mają mieć możliwość dodawania, edycji lub usuwania plików, wówczas należy zaznaczyć opcję *Zezwalaj użytkownikom sieciowym na zmianę moich plików*. Foldery mogą udostępniać użytkownicy należący do grup *Administratorzy* oraz *Użytkownicy zaawansowani*.

Rysunek 6.14.
Okno prostego udostępniania danych

W przypadku udostępniania klasycznego okno udostępniania zawiera więcej opcji (rysunek 6.15).

Rysunek 6.15.
Okno klasycznego udostępniania danych



Do udostępnionych folderów i stacji dysków można zastosować następujące typy uprawnień:

- *Odczyt* — umożliwia przeglądanie nazw plików i podfolderów, przechodzenie do podfolderów, przeglądanie danych w plikach, uruchamianie plików programów.
- *Zmiana* — umożliwia przeprowadzanie tych samych operacji co w przypadku odczytu, a dodatkowo dodawanie plików i folderów, zmienianie danych w plikach oraz usuwanie podfolderów i plików.
- *Pełna kontrola* — umożliwia przeprowadzanie tych samych operacji co w przypadku odczytu i zmiany, a dodatkowo pozwala na zmianę uprawnień NTFS dla plików i folderów oraz przejmowanie tych plików i folderów na własność.

Uprawnienia do udostępnianych zasobów dyskowych dotyczą tylko użytkowników korzystających z nich poprzez sieć. Dla lokalnych użytkowników dostęp do zasobów regulują uprawnienia oraz prawa systemu plików NTFS.

DEFINICJA

Uprawnienia są regułami skojarzonymi z obiektami znajdującymi się na komputerze lokalnym lub w sieci, takimi jak pliki i foldery, a nawet drukarki. Uprawnienia określają, czy dany użytkownik ma dostęp do określonego obiektu i co może z nim zrobić. Użytkownik może mieć na przykład dostęp do dokumentu w folderze udostępnionym w sieci, lecz tylko z prawem odczytu, bez możliwości wprowadzania zmian. Administratorzy systemu i użytkownicy korzystający z kont administratora mogą przypisywać uprawnienia poszczególnym użytkownikom lub grupom.

W tabeli 6.1 przedstawiono poziomy uprawnień dostępne dla plików i folderów.

Tabela 6.1. Poziomy uprawnień dla plików i folderów

Poziom uprawnień	Opis
Pełna kontrola	Użytkownicy mają prawo do wyświetlania zawartości pliku lub folderu, zmiany istniejących plików i folderów, tworzenia nowych plików i folderów oraz uruchamiania programów w folderze.
Modyfikowanie	Użytkownicy mają prawo do zmiany istniejących plików i folderów, ale nie mogą tworzyć nowych.
Odczyt i wykonanie	Użytkownicy mają prawo do wyświetlania zawartości istniejących plików i folderów oraz uruchamiania programów w folderze.
Odczyt	Użytkownicy mają prawo do wyświetlania zawartości folderu oraz otwierania plików i folderów.
Zapis	Użytkownicy mogą tworzyć nowe pliki i foldery oraz zmieniać istniejące.

Aby skorzystać z udostępnianych zasobów, należy znać nazwę komputera lub adres IP (rysunek 6.16). Wybór opcji *Wyświetl komputery grupy roboczej* (folder *Moje miejsca sieciowe* lub *Sieć*) spowoduje wyświetlenie komputerów przypisanych do grupy roboczej, w której znajduje się dany komputer. Żeby wyświetlić pozostałe dostępne grupy robocze, wystarczy wybrać opcję *Microsoft Windows Network*. W folderze wybranej grupy roboczej widnieją przypisane do niej komputery. Dwukrotne kliknięcie ikony komputera spowoduje wyświetlenie zasobów udostępnianych przez urządzenia, pod warunkiem że użytkownik ma odpowiednie uprawnienia. W innym przypadku użytkownik jest proszony o podanie hasła dostepu.

W systemach Windows istnieje możliwość wyszukiwania zasobów sieciowych. Służy do tego polecenie *Wyszukaj* znajdujące się w menu *Start*.

Bezpośredni dostęp do zdalnych komputerów jest możliwy z poziomu programu Eksplorator Windows. W pasku adresu należy wprowadzić sieciową nazwę zasobu poprzedzoną dwoma wstecznymi ukośnikami (ang. *backslash*):

```
\\nazwa_komputera\zasób
```

lub

```
\\ip_komputera\zasób
```

Rysunek 6.16. Udostępnione zasoby

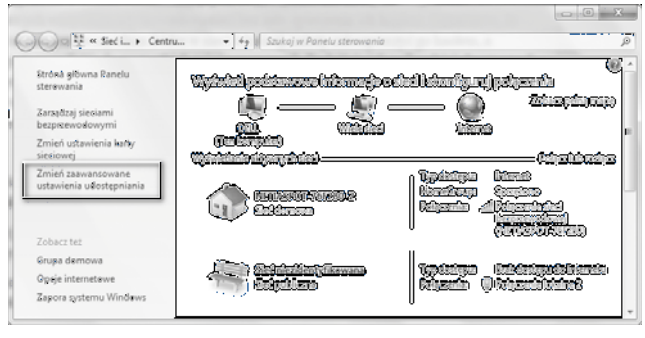
Innym sposobem dostępu do zasobów jest wprowadzenie adresu zasobu sieciowego w oknie *Uruchamianie* (menu *Start/Uruchom*). Otwarte zostanie okno zawierające udostępnione zasoby.

Korzystanie z danych udostępnionych na innych komputerach odbywa się w taki sam sposób jak korzystanie z danych na dyskach lokalnych. Kopiowanie i przenoszenie danych jest możliwe przy użyciu mechanizmu schowka.

Udostępnianie w systemie Windows 7

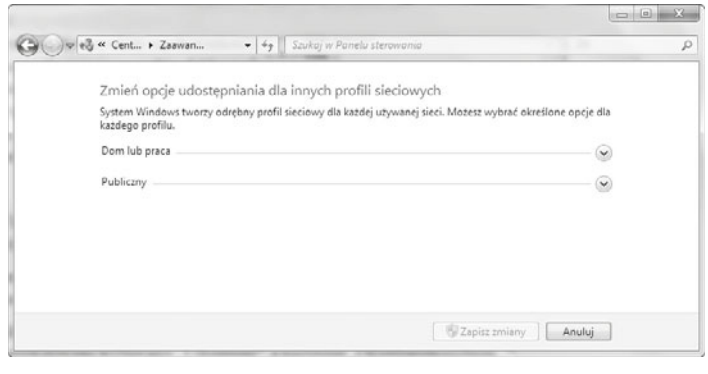
Udostępnianie w Windows 7 różni się tym, że domyślnie nie da się udostępnić zasobów dyskowych wszystkim użytkownikom sieci bez zabezpieczenia ich hasłem. Oznacza to, że gdy chce się udostępnić wszystkim folder w sieci lokalnej, należy zabezpieczyć go hasłem, a następnie rozesłać je do wszystkich zainteresowanych. Podejście to jest jak najbardziej słuszne pod względem bezpieczeństwa, czasami bowiem trzeba udostępnić zasoby, do których wszyscy mają mieć dostęp, np. sterowniki. W celu wyłączenia autoryzacji należy zmienić opcję *Udostępnianie chronione hasłem* znajdującą się w kategorii *Centrum sieci i udostępniania* w Panelu sterowania (rysunek 6.17).

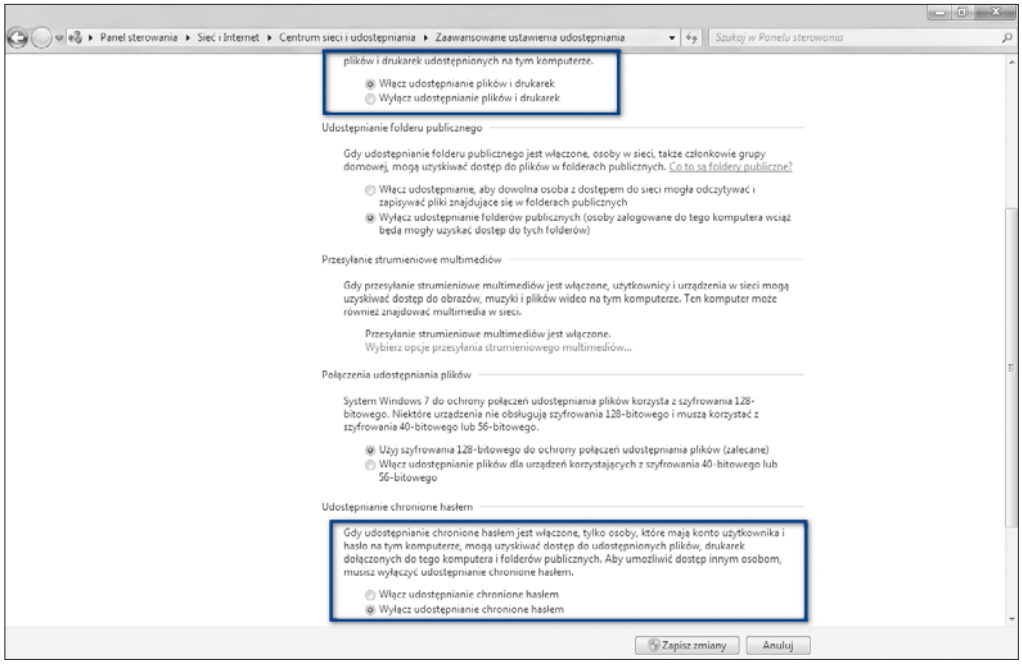
Rysunek 6.17.
Centrum sieci i udostępniania



W kolejnym oknie należy wybrać odpowiedni profil, rozwinąć jego ustawienia i włączyć udostępnianie chronione hasłem. Trzeba pamiętać, że te ustawienia są definiowane dla danego profilu, a nie dla danego folderu (rysunek 6.18 i 6.19).

Rysunek 6.18.
Profil udostępniania

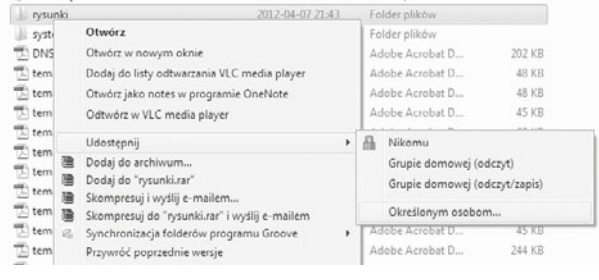




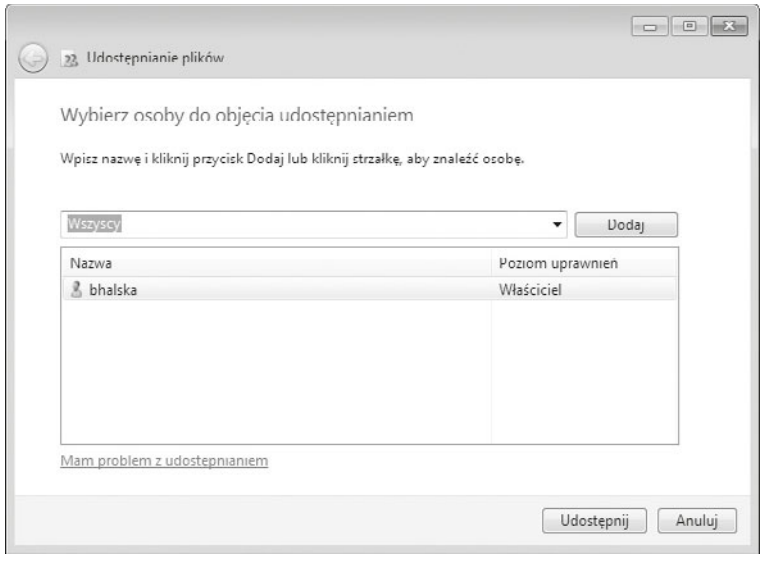
Rysunek 6.19. Ustawienia w ramach profilu

Ostatnim krokiem jest właściwe udostępnienie folderu dla odpowiedniej grupy użytkowników. Po kliknięciu prawym przyciskiem myszy wybranego dysku/folderu/pliku z menu kontekstowego należy wybrać *Udostępnij*, a następnie *Określonym osobom…* (rysunek 6.20).

Rysunek 6.20.
Udostępnianie zasobów

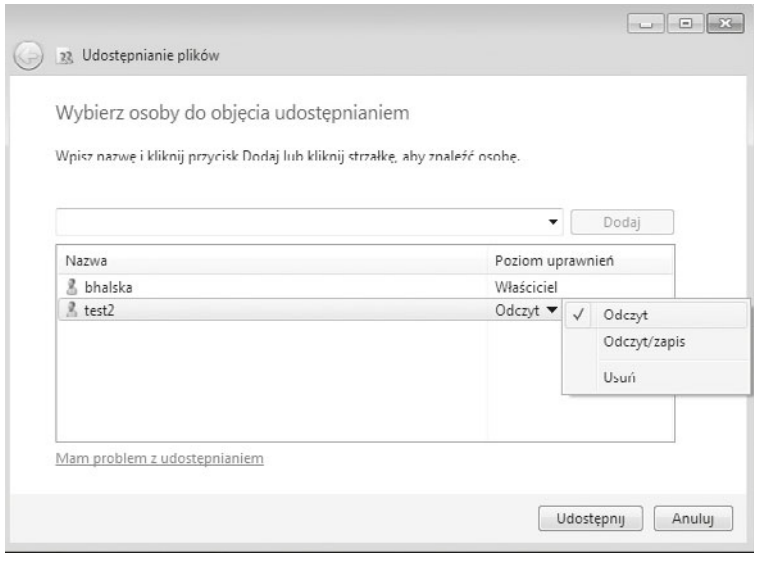


W nowo otwartym oknie z listy należy wybrać użytkownika lub grupę użytkowników, którzy mają mieć dostęp do zasobów (jeżeli zasoby mają być dostępne bez logowania, wystarczy wybrać grupę *Wszyscy*), a następnie kliknąć *Dodaj* (rysunek 6.21).



Rysunek 6.21. Definiowanie dostępu

Istnieje możliwość zdefiniowania uprawnień dla poszczególnych grup lub użytkowników. Aby określić uprawnienia dostępu do zasobów dla danej grupy lub użytkownika, należy kliknąć przypisane uprawnienia (rysunek 6.22), a następnie określić nowy poziom uprawnień.



Rysunek 6.22. Definiowanie uprawnień

ĆWICZENIA

Uwaga! Aby możliwe było prawidłowe wykonanie ćwiczeń w sali lekcyjnej przez wielu uczniów równocześnie, należy zróżnicować adresy IP. W tym celu proponuje się wykorzystanie numeru ucznia z dziennika. Jeśli ćwiczenia są wykonywane samodzielnie, numer ten może zostać zastąpiony dowolną liczbą z zakresu 1 – 40.

1. Sprawdź dostępne parametry w ustawieniach połączenia lokalnego. W jaki sposób komputer ma przypisany adres IP?
2. Sprawdź adres maski i określ, z jakiej klasy jest adres IP.
3. Udostępnij zasoby między stacjami roboczymi:
   a. Skonfiguruj kartę sieciową w wirtualnej maszynie z systemem operacyjnym Windows 7, np. 192.168.nr_z_dziennika.100.
   b. Skonfiguruj kartę sieciową w wirtualnej maszynie z systemem operacyjnym Windows 7, np. 192.168.nr_z_dziennika.101.
   c. Oba adresy powinny być w tej samej sieci.
   d. Udostępnij folder o nazwie *prywatne* i zdefiniuj dla niego tylko możliwość odczytu.
   e. Udostępnij folder o nazwie *publiczne* i zdefiniuj dla niego uprawnienia odczyt/zapis.

PYTANIA

1. Wymień i omów uprawnienia dla plików i folderów w systemie plików NTFS.
2. W jakich edycjach jest dostępny Windows 7, a w jakich Windows XP?
3. Jakie parametry karty sieciowej są niezbędne w celu skonfigurowania sieci?
4. Co to jest brama domyślna?
5. Czym jest grupa robocza?
6. Omów udostępnianie zasobów w systemie Windows 7.

Mapowanie dysków

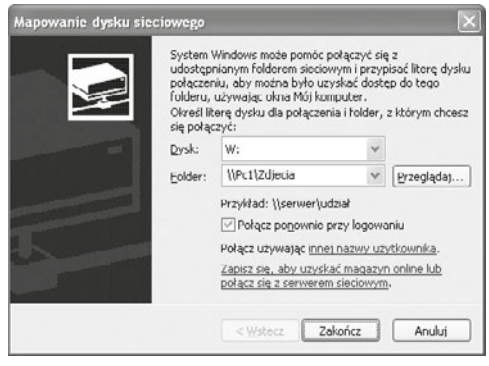
DEFINICJA

Jeśli udostępnione dane mają być widoczne w systemie jako osobny dysk, to należy przeprowadzić operację mapowania dysków. Polega ona na przypisaniu wybranej litery do udostępnionego zasobu, dzięki czemu jest on widoczny w folderze *Komputer* (*Mój Komputer*).

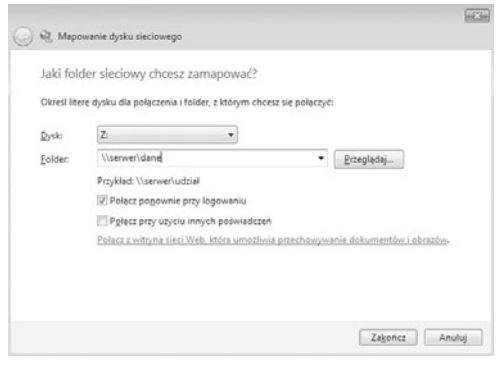
Aby zmapować dysk, w oknie programu Eksplorator Windows należy w menu *Narzędzia* wskazać opcję *Mapuj dysk*.

W oknie *Mapowanie dysku sieciowego* należy wybrać literę dysku, pod którą będzie widoczny zasób, oraz podać adres udostępnionego folderu (rysunek 6.23 i 6.24). Adres ten można wpisać z klawiatury lub wskazać w oknie, które wyświetli się po kliknięciu przycisku *Przeglądaj*. Jeśli mapowanie dysku ma być trwałe, należy zaznaczyć opcję *Połącz ponownie przy logowaniu*.

Rysunek 6.23. Mapowanie dysków — Windows XP



Rysunek 6.24. Mapowanie dysków — Windows 7



Podłączenie do zdalnych zasobów następuje z prawami użytkownika *Gość*. Jeśli podłączenie ma być realizowane z prawami innego użytkownika, to należy wprowadzić jego nazwę i hasło w oknie, które pojawia się po wybraniu opcji *Połącz używając innej nazwy użytkownika* (Windows XP) lub *Połącz przy użyciu innych poświadczeń* (Windows 7). Po wybraniu tej opcji zostaniemy poproszeni o podanie nazwy użytkownika oraz hasła. Po zatwierdzeniu działania przyciskiem *Zakończ* w folderze komputera zostaje dodana ikona kolejnego dysku opisana literą wybraną w procesie mapowania. Otwarcie dysku spowoduje wyświetlenie zawartości zdalnego folderu.

Mapowanie dysków jest możliwe także z poziomu trybu tekstowego, poprzez składnię polecenia `net use`:

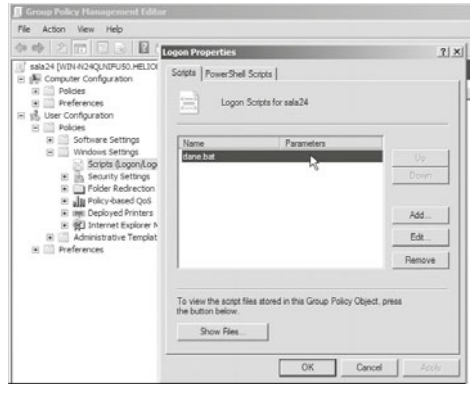
```
net use litera_dysku adres_zasobu [hasło] [/user:<nazwa_użytkownika>] [/
presistent:{yes/no}]
```

gdzie:

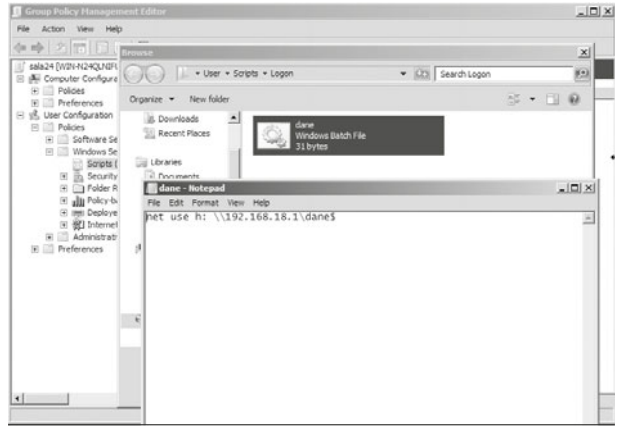
- `litera_dysku` — litera dysku, pod którą zasób ma być mapowany,
- `hasło` — hasło dostępu do zasobów (parametr opcjonalny),
- `nazwa_użytkownika` — nazwa użytkownika logującego się do zasobów (parametr opcjonalny),
- `presistent:yes/no` — określa, czy mapowanie ma być przeprowadzone po ponownym zalogowaniu do systemu (parametr opcjonalny).

Mapowanie dysków pozwala na dostęp do zdalnych zasobów z poziomu aplikacji użytkownika — dostęp do nich jest taki sam jak w przypadku dysków fizycznie zainstalowanych w komputerze.

W ramach domeny będącej główną usługą serwera mapowanie dysków jest możliwe przy użyciu skryptów logowania, które przy każdym logowaniu będą mapować określone zasoby (rysunek 6.25 i 6.26).



Rysunek 6.25. GPO — skrypt logowania — Windows Server 2008 R2

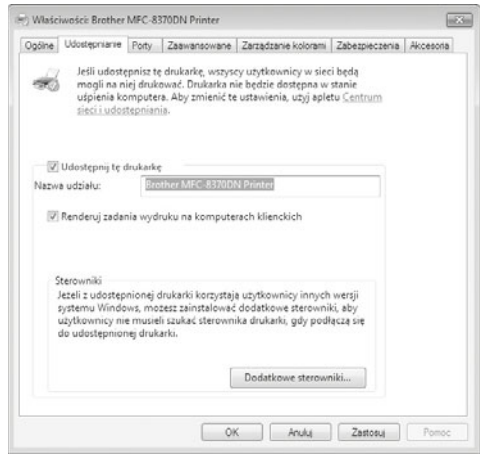


Rysunek 6.26. GPO — skrypt logowania mapujący dysk — Windows Server 2008 R2

Udostępnianie drukarek

Opcja udostępniania drukarek pozwala korzystać z urządzeń podłączonych do komputera innym użytkownikom sieci, co prowadzi do redukcji kosztów związanych z zakupami urządzeń drukujących. Aby udostępnić drukarkę innym użytkownikom, należy w folderze *Drukarki i faksy*, który znajduje się w Panelu sterowania, wyświetlić okno właściwości wybranej drukarki. Następnie w zakładce *Udostępnianie* trzeba wprowadzić nazwę, pod którą drukarka ma być widoczna w sieci (rysunek 6.27 i 6.28).

Rysunek 6.27. Udostępnianie drukarki — Windows XP



Rysunek 6.28. Udostępnianie drukarki — Windows 7

Po instalacji drukarki użytkownicy należący do grupy *Wszyscy* (a więc wszyscy użytkownicy komputera) mają uprawnienia do drukowania oraz zarządzania swoimi dokumentami oczekującymi w kolejce wydruku. Użytkownicy należący do grupy *Administratorzy* mają prawo do zarządzania wszystkimi dokumentami i drukarkami.

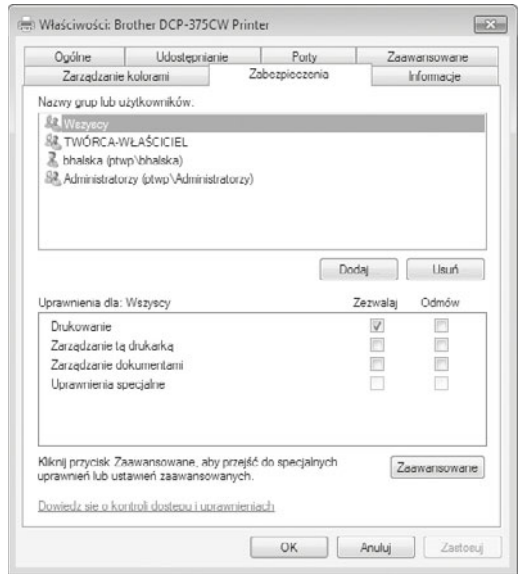
Prawa dostępu do drukarek dotyczą zarówno użytkowników lokalnych komputera, jak i użytkowników sieciowych. Prawa te mogą być ustawiane w zakładce *Zabezpieczenia* w oknie właściwości drukarki.

Z drukarkami są związane następujące uprawnienia:

- *Drukowanie* — pozwala na przesyłanie wydruku do drukarki,
- *Zarządzanie drukarkami* — pozwala na dodawanie i usuwanie drukarek w systemie,
- *Zarządzanie dokumentami* — pozwala na zarządzanie kolejką wydruku.

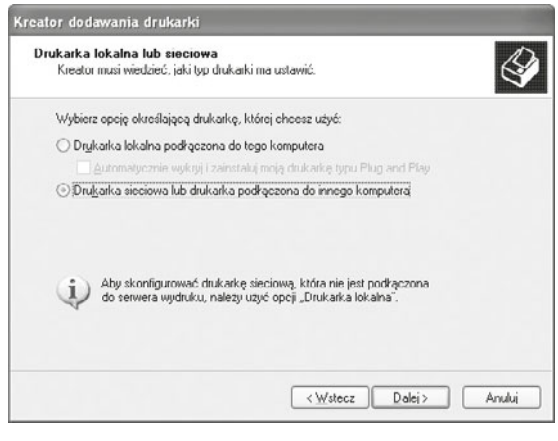
Podobnie jak w przypadku innych zasobów, uprawnienia mogą być nadawane i odbierane zarówno użytkownikom, jak i grupom (rysunek 6.29).

Rysunek 6.29. Uprawnienia do drukarek



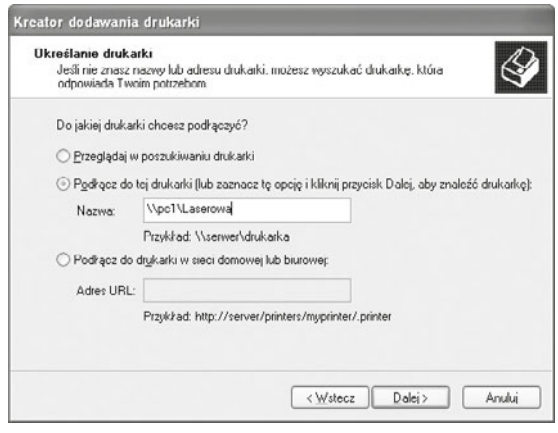
Aby zainstalować drukarkę sieciową w systemie Windows, należy w folderze *Drukarki i faksy* wybrać opcję *Dodaj drukarkę*. W oknie kreatora, które się wyświetli, trzeba wskazać, że instalowana będzie drukarka sieciowa (rysunek 6.30).

Rysunek 6.30. Instalacja drukarki sieciowej w systemie Windows XP



Następnym krokiem jest wprowadzenie adresu drukarki sieciowej. Można wprowadzić go ręcznie w polu *Podłącz do tej drukarki* lub wyszukać wśród komputerów w sieci (rysunek 6.31).

Rysunek 6.31. Udostępnianie drukarki w systemie Windows XP



Opcja *Podłącz do drukarki w sieci domowej lub biurowej* pozwala na używanie drukarek udostępnianych przez serwery wydruku korzystające z protokołu HTTP. W przypadku udostępniania drukarek w sieci równoprawnej należy wprowadzić adres w polu przy opcji *Podłącz do tej drukarki*.

Po wybraniu przycisku *Dalej* kreator rozpocznie instalację sterownika drukarki sieciowej. Kolejny krok pozwala wybrać instalowaną drukarkę jako domyślną.

Po zakończeniu pracy kreatora drukarka jest widoczna w folderze *Drukarki i Faksy*, co umożliwia korzystanie z niej jak z drukarki podłączonej bezpośrednio do komputera — jest ona na liście drukarek do wyboru wyświetlanych we wszystkich aplikacjach w systemie.

Podłączenie do zdalnej drukarki jest możliwe także podczas eksploracji udostępnionych zasobów. Należy wówczas w menu kontekstowym udostępnionej drukarki wybrać opcję *Połącz*.

ĆWICZENIA

1. Udostępnij wybrany folder w sieci. Sprawdź możliwe ustawienia uprawnień.
2. Podłącz się do udostępnionego folderu.
3. Wykonaj mapowanie wybranego folderu w sieci.
4. Za pomocą folderu *Sieć* (lub *Moje miejsca sieciowe*) sprawdź dostępne zasoby sieciowe.
5. Udostępnij drukarkę w sieci.
6. Podłącz udostępnioną w sieci drukarkę.

PYTANIA

1. Na czym polega udostępnianie drukarki?
2. Co to jest mapowanie dysków?
3. Jakie polecenie umożliwia mapowanie dysku z konsoli?
4. Wymień uprawnienia, z jakimi możemy udostępnić drukarkę.

6.3. Lokalne konta użytkowników i grup

Każdy użytkownik przed rozpoczęciem pracy musi zalogować się do systemu, dzięki czemu zostaną załadowane spersonalizowane ustawienia systemu. Dodatkowo dużym atutem kont użytkowników jest łatwiejsza kontrola dostępu do zasobów komputera.

Konta użytkowników dzielą się na trzy rodzaje:

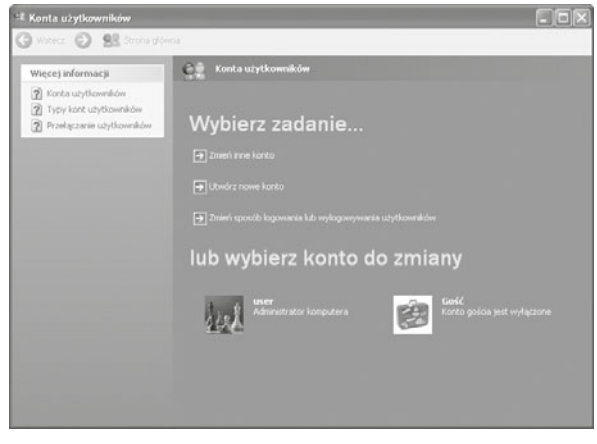
- **Konta wbudowane**, które są zakładane w momencie instalacji systemu operacyjnego. Są to konta *Administrator* oraz *Gość*. Nie można ich usunąć, przy czym konto *Gość* może być wyłączone.
- **Lokalne konta użytkowników** są wykorzystywane do pracy na pojedynczych komputerach lub komputerach połączonych w grupy robocze. Informacje o kontach są przechowywane na komputerze lokalnym i można z nich korzystać tylko na nim.
- **Domenowe konta użytkowników** wykorzystuje się w komputerach podłączonych do sieci pracującej pod kontrolą usługi katalogowej (Active Directory) (więcej informacji o usłudze w punkcie 6.4.5).

W desktopowych systemach Windows tworzone są następujące — wbudowane — grupy użytkowników:

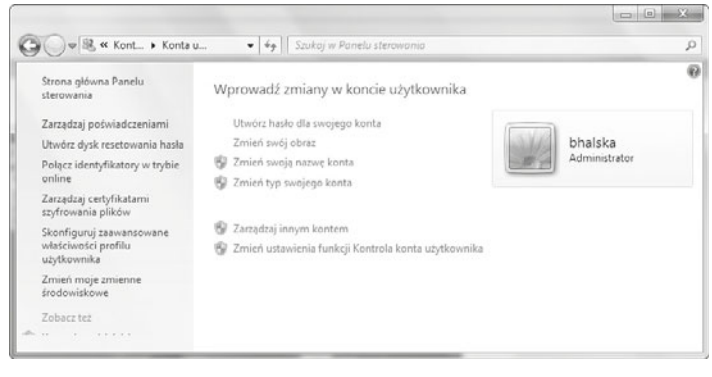
- **Administratorzy** — mają największe uprawnienia domyślne i możliwość zmieniania własnych uprawnień.
- **Operatorzy kopii zapasowych** — mają prawo wykonywania kopii zapasowych plików i ich przywracania na komputerze, bez względu na jakiekolwiek uprawnienia chroniące te pliki. Mogą także logować się na komputerze i zamykać go, ale nie są w stanie zmieniać ustawień zabezpieczeń.
- **Użytkownicy zaawansowani** — mogą tworzyć konta użytkowników, ale są w stanie modyfikować i usuwać tylko te konta, które sami utworzą. Mogą tworzyć grupy lokalne i usuwać użytkowników z utworzonych samodzielnie grup lokalnych, mogą również usuwać użytkowników z grup Użytkownicy zaawansowani, Użytkownicy i Goście. Nie mogą modyfikować grup Administratorzy i Operatorzy kopii zapasowych, przejmować własności plików, tworzyć kopii zapasowych katalogów i przywracać ich, ładować i zwalniać sterowników urządzeń ani zarządzać dziennikami zabezpieczeń i inspekcji.

- **Użytkownicy** — mogą wykonywać większość typowych zadań, takich jak uruchamianie aplikacji, korzystanie z drukarek lokalnych i sieciowych oraz zamykanie i blokowanie stacji roboczej. Użytkownicy mogą tworzyć grupy lokalne, ale mogą modyfikować tylko te grupy lokalne, które sami utworzyli. Użytkownicy nie mogą udostępniać katalogów ani tworzyć drukarek lokalnych.
- **Goście** — ta grupa umożliwia użytkownikom okazjonalnym lub jednokrotnym zalogowanie się na konto wbudowane *Gość* i uzyskanie ograniczonych możliwości. Mogą oni również zamknąć system na stacji roboczej.
- **Replikator** — grupa ta obsługuje funkcje replikacji katalogów. Jedynym członkiem tej grupy powinno być konto użytkownika domeny wykorzystywane do logowania się do usług Replikator kontrolera domeny. Do tej grupy nie należy dodawać kont rzeczywistych użytkowników.

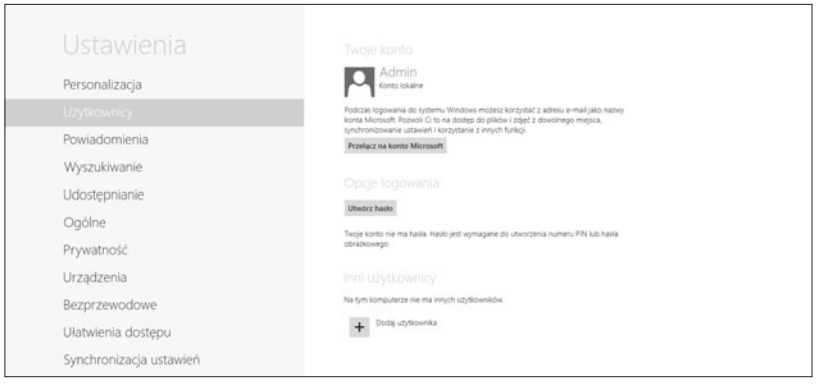
Aby dodać nowe konta użytkowników (rysunki 6.32, 6.33, 6.34), należy uruchomić przystawkę *Konta użytkowników* z Panelu sterowania. Po wybraniu opcji *Utwórz nowe konto* wystarczy wprowadzić nazwę nowego użytkownika oraz wybrać typ konta — administratora lub z ograniczonymi prawami.



Rysunek 6.32. Zarządzanie kontami użytkowników — Windows XP



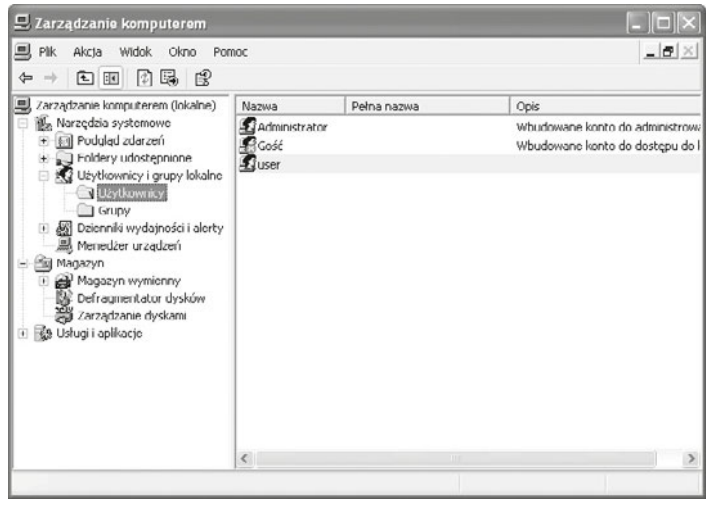
Rysunek 6.33. Zarządzanie kontami użytkowników — Windows 7



Rysunek 6.34. Zarządzanie kontami użytkowników — Windows 8

Innym sposobem na zarządzanie kontami użytkowników jest użycie opcji dostępnych w konsoli *Zarządzanie komputerem* (*Panel sterowania/Narzędzia administracyjne/Zarządzanie komputerem* lub opcja *Zarządzaj* z menu kontekstowego ikony *Mój komputer*). W menu znajdującym się po lewej stronie należy wybrać *Narzędzia systemowe/Użytkownicy i grupy lokalne/Użytkownicy*. Aby dodać nowego użytkownika, wystarczy wybrać opcję *Nowy użytkownik* z menu *Akcja*. W tym samym menu istnieje możliwość zmiany haseł użytkowników oraz ustawienia właściwości konta (rysunek 6.35).

Rysunek 6.35. Dodawanie kont z poziomu konsoli zarządzania

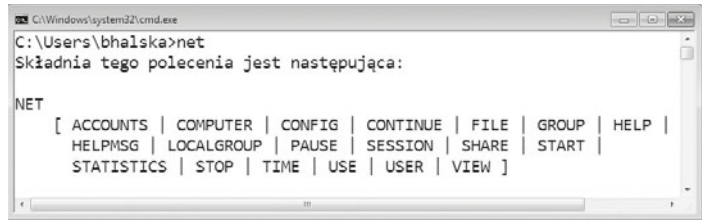


Konsola zarządzania systemem pozwala także na przypisanie użytkownika do wybranej grupy — w oknie właściwości danego użytkownika należy wybrać zakładkę *Członek grupy*, a następnie dodać lub usunąć grupę czy też grupy, do których użytkownik przynależy.

System Windows pozwala także na zarządzanie użytkownikami z poziomu wiersza poleceń. Służy do tego polecenie `net`.

Polecenie `net` jest narzędziem oferującym wiele możliwości (rysunek 6.36).

Rysunek 6.36.
Polecenie net



Przykład 6.1.

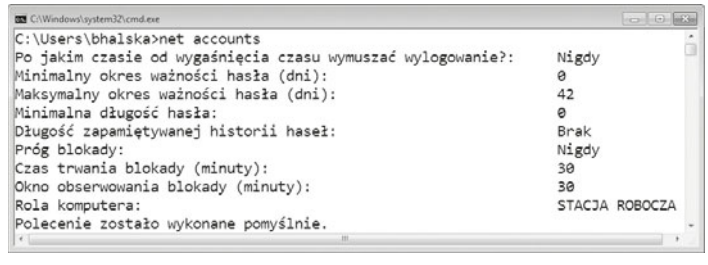
```
net accounts
```

Służy do aktualizowania bazy kont użytkowników oraz modyfikuje wymagania dotyczące haseł i logowania dla wszystkich kont (rysunek 6.37).

Składnia:

```
net accounts
[/forcelogoff:{minuty | no}] [/minpwlen:długośd]
    [/maxpwage:{dni | unlimited}] [/minpwage:dni]
    [/uniquepw:liczba] [/domain]
```

Rysunek 6.37.
Polecenie net accounts




```
net computer
```

Polecenie dodaje i usuwa konta użytkowników. Jest przydatne, gdy chce się utworzyć wiele kont.

Składnia:

```
net computer
\\nazwa_komputera {/add | /del}
net user
```

Dodaje lub modyfikuje konta użytkowników albo wyświetla informacje o koncie użytkownika (rysunek 6.38).

Składnia:

```
net user
[nazwa_uzytkownika [haslo | *] [opcje]] [/domain]
nazwa_uzytkownika {haslo | *} /add [opcje] [/domain]
nazwa_uzytkownika [/delete] [/domain]
nazwa_uzytkownika [/times:{czas | all}]
```

Parametry:

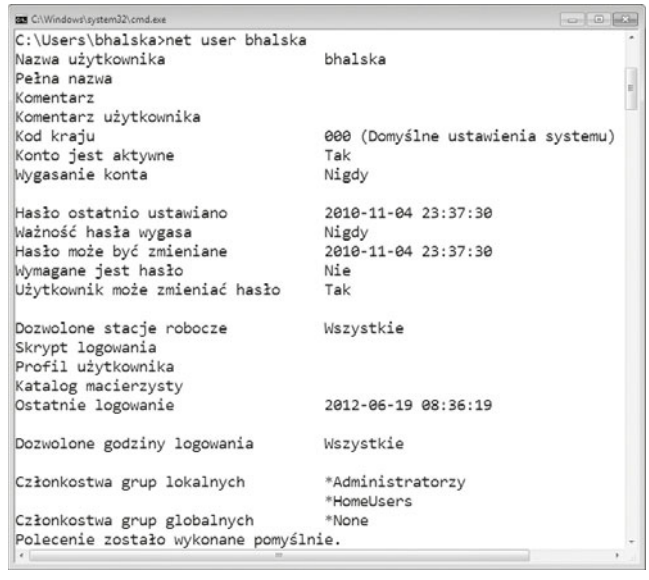
```
net user nazwa_uzytkownika
```

Określa nazwę konta użytkownika, które należy dodać, usunąć, zmodyfikować lub przeglądać. Nazwa konta użytkownika może zawierać maksymalnie 20 znaków.

```
net user nazwa_uzytkownika hasło
```

Przypisuje lub zmienia hasło konta użytkownika. Aby wyświetlić monit o hasło, należy wpisać gwiazdkę (*). Podczas wpisywania hasło nie jest wyświetlane (rysunek 6.38).

Rysunek 6.38.
Polecenie net user



ĆWICZENIA

1. Utwórz konto użytkownika *user01* za pomocą konsoli tworzenia użytkownika.
2. Utwórz konto użytkownika *user02*, wykorzystując polecenie z konsoli.
3. Korzystając z polecenia `NET`, wyświetl informacje o kontach, które zostały przez Ciebie stworzone.

PYTANIA

1. Wymień i omów rodzaje kont użytkowników.
2. Wymień grupy wbudowane, do jakich możemy dodać użytkowników.
3. Wymień narzędzia, za pomocą których dodaje się użytkowników.

6.4. Administrowanie systemem Windows Server

Systemy Windows zostały zaprojektowane do pracy zarówno w sieci równoprawnej, jak i w sieci z serwerem. Sieć **klient/serwer** oznacza podłączenie pojedynczego użytkownika z pojedynczej stacji roboczej do sieci zarządzanej przez serwer lub serwery — wydajne komputery, które zarządzają siecią i uprawnieniami użytkowników, a także udostępniają zasoby.

System Windows Server 2008, którego premiera odbyła się w lutym 2008 r., jest ostatnią wersją serwera dostępną zarówno w wersji 32-bitowej, jak i 64-bitowej. Jego następca, 2008 R2 (październik 2009 r.), został wydany jedynie w wersji 64-bitowej. Jest on dostępny w kilku edycjach (tabela 6.2). Każda z nich może być zainstalowana w wersji pełnej (z interfejsem graficznym) lub w wersji Core, która nie zawiera interfejsu graficznego, a zarządzanie odbywa się w niej w trybie tekstowym lub zdalnie, przy użyciu Microsoft Management Console.

Tabela 6.2. Najpopularniejsze edycje Windows Server 2008 R2

Funkcja	Standard	Enterprise	Datacenter	Web	Itanium
Maks. liczba obsługiwanych procesorów 32-bitowych	4	8	32	4	Brak wersji 32-bitowej
Maks. ilość obsługiwanej pamięci (procesor 32-bitowy)	4 GB	64 GB	64 GB	4 GB	Brak wersji 32-bitowej
Maks. liczba obsługiwanych procesorów 64-bitowych	4	8	64	4	64
Maks. ilość obsługiwanej pamięci (procesor 64-bitowy)	32 GB	2 TB	2 TB	32 GB	2 TB
II7	TAK	TAK	TAK	TAK	TAK
Serwer aplikacji	TAK	TAK	TAK	NIE	TAK
Usługi drukowania	TAK	TAK	TAK	NIE	NIE
Hyper-V	TAK	TAK	TAK	NIE	NIE
Usługi katalogowe	TAK	TAK	TAK	NIE	NIE
Serwer DHCP, DNS	TAK	TAK	TAK	NIE	NIE
Serwer plików	TAK	TAK	TAK	NIE	NIE

Funkcja	Standard	Enterprise	Datacenter	Web	Itanium
Usługi terminalowe	TAK (maks. 250 użytkowników	TAK (bez ograniczeń)	TAK (bez ograniczeń)	NIE	NIE
Obsługa Aero	TAK	TAK	TAK	TAK	NIE
Praca w klastrach	NIE	TAK	TAK	NIE	TAK
PowerShell	TAK	TAK	TAK	TAK	TAK
Wirtualizacja	1 wirtualny system	4 wirtualne systemy	Zależne od licencji CAL na procesor	Brak	Brak

Poszczególne wersje systemu Windows Server 2008 R2 zostały zbudowane w celu dopasowania do wymagań określonych grup klientów. Sugerowane przeznaczenie poszczególnych wersji to:

- Standard — serwer usług sieciowych i WWW dla małej firmy (maks. 250 użytkowników),
- Enterprise — serwer usług sieciowych i WWW dla średniej lub dużej firmy,
- Datacenter — serwer usług sieciowych i WWW dla firm wykorzystujących farmy obliczeniowe,
- Itanium — centra obliczeniowe,
- Web — serwer WWW.

PYTANIA

1. Ile procesorów 64-bitowych może maksymalnie obsłużyć Windows Server 2008 R2 Enterprise?
2. Ile pamięci RAM może maksymalnie obsłużyć Windows Server 2008 R2 Enterprise?

6.4.1. Instalacja systemu Windows Server 2008 R2

Wymagania sprzętowe

Podstawowe wymagania sprzętowe dla Windows Server 2008 R2 są zależne od konfiguracji systemu, zainstalowanych aplikacji i dodatków wybranych w czasie procesu instalacji. Minimalne i zalecane wartości są przedstawione poniżej.

Procesor:

- *Minimalny: 1 GHz (procesor x86) lub 1,4 GHz (procesor x64).*
- *Zalecany: 2 GHz lub szybszy.*

Pamięć:

- *Minimalna: 512 MB RAM.*
- *Zalecana: 2 GB RAM lub większa* (*instalacja pełna*), *1 GB RAM lub większa* (*instalacja Server Core*).
- *Maksymalna* (*systemy 32-bitowe*): *4 GB* (*Standard*) *lub 64 GB* (*Enterprise i Datacenter*).
- *Maksymalna* (*systemy 64-bitowe*): *32 GB* (*Standard*) *lub 2 TB* (*Enterprise, Datacenter i systemy dla komputerów z procesorem Itanium*).

Dysk:

- *Minimalny: 10 GB* (*wystarczający dla wersji Core*).
- *Zalecany: 40 GB lub większy.*

Licencjonowanie

Istnieją różne modele licencjonowania, zależne od edycji systemu Windows Server 2008 R2. Najczęściej spotykane to:

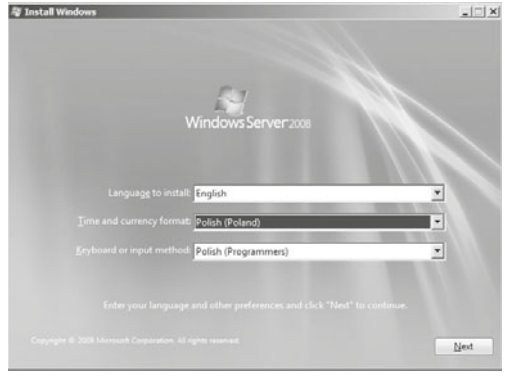
1. Licencja Serwera i na połączenie — wymaga zakupu licencji na każdy serwer i licencji dostępowej CAL (ang. *Client Access Licenses*) dla każdego użytkownika lub urządzenia:
   a) *Device CAL* — licencja dostępowa przypisana do każdego urządzenia, umożliwiająca korzystanie z niego wielu użytkownikom.
   b) *User CAL* — licencja dostępowa przypisana do każdego użytkownika, umożliwiająca mu korzystanie z wielu urządzeń.
2. Licencja na procesor i na połączenie — wymaga zakupu licencji „Processor licence" dla każdego procesora w serwerze i licencji na połączenie (CAL) dla każdego użytkownika lub urządzenia. Ten sposób licencjonowania jest wykorzystywany w edycji Datacenter i w systemach dla procesorów Itanium.
3. Licencja Serwera — wymaga zakupu licencji tylko na serwer, licencje dostępowe dla klientów nie są wymagane (model można wykorzystać tylko w przypadku systemu Web Server Edition).

Instalacja serwera rozpoczyna się od umieszczenia płyty instalacyjnej w napędzie, który w BIOS-ie należy ustawić jako pierwsze urządzenie rozruchowe. Jest to serwer, w którym jest możliwa instalacja do pliku VHD wykorzystywanego przez systemy wirtualizacji. Informacje na temat wirtualizacji zasobów zostały zawarte w podrozdziale 6.11 — „Wirtualizacja".

Kolejne kroki instalacji systemu Windows Server 2008 R2

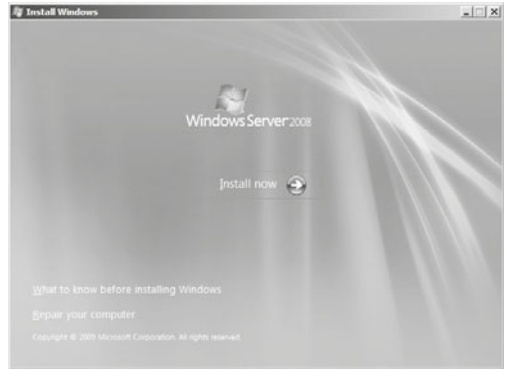
1. Wybór języka instalacji (*Language to install* (*Język, który chcesz zainstalować*)), formatu danych (*Time and currency format* (*Format godziny i waluty*)) oraz układu klawiatury (*Keyboard or input metod* (*Klawiatura lub metoda wprowadzania*)) (rysunek 6.39).

Rysunek 6.39.
Wybór języka
i strefy czasowej



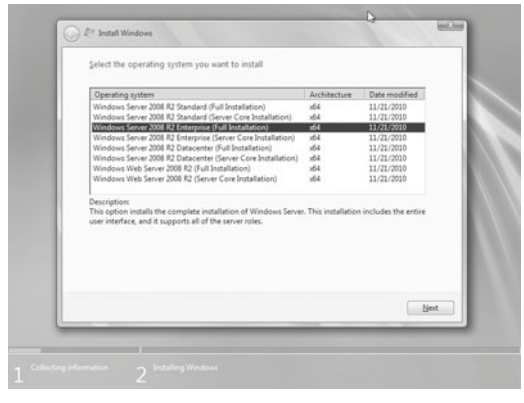
2. Rozpoczęcie instalacji po naciśnięciu przycisku *Install now* (*Zainstaluj teraz*). W tym miejscu można również naprawić wcześniej zainstalowany system (*Repair your computer* (*Napraw komputer*)) (rysunek 6.40).

Rysunek 6.40.
Instalacja oraz naprawa
zainstalowanego już
systemu



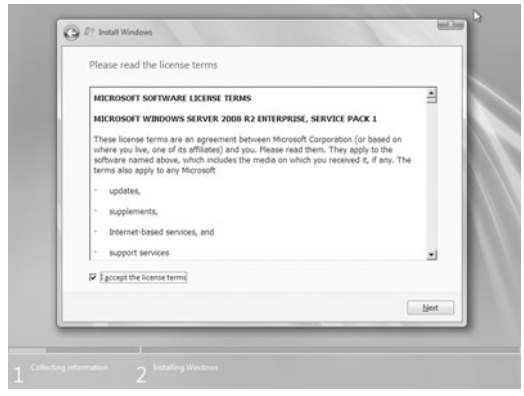
3. Wybór wersji systemu do zainstalowania (rysunek 6.41, patrz również tabela 6.2).

Rysunek 6.41.
Wybór edycji



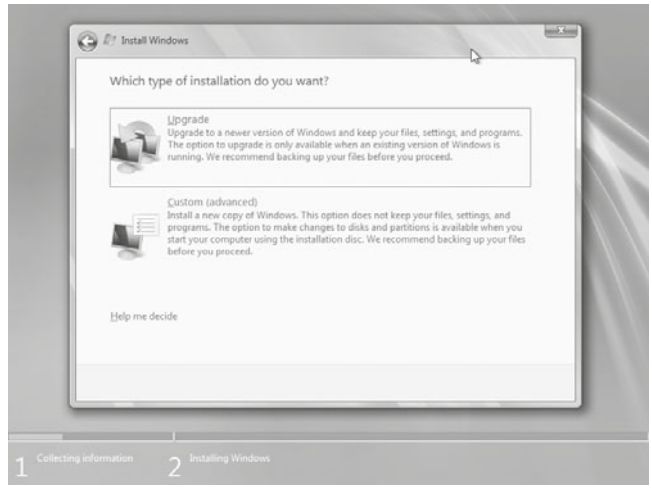
4. Akceptacja warunków licencji (*I accept the license terms* (*Akceptuję postanowienia licencyjne*)) (rysunek 6.42).

Rysunek 6.42.
Warunki licencji



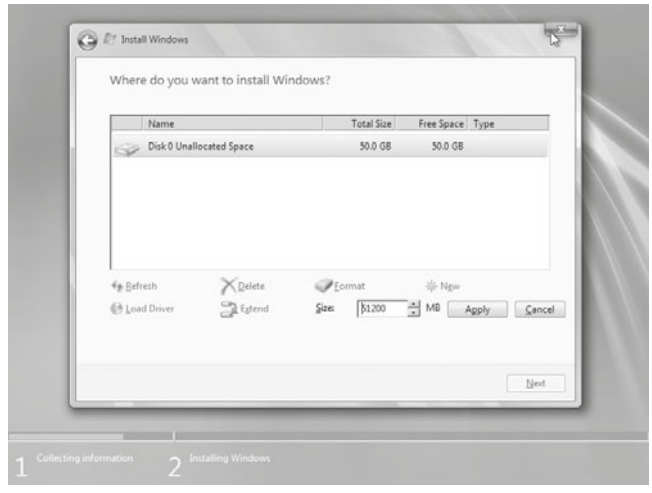
5. Wybór typu instalacji — *Custom* (*advanced*) (*Niestandardowa* (*zaawansowane*)) oraz jeżeli system jest instalowany na dysku, gdzie wcześniej był zainstalowany system operacyjny, dostępna jest opcja *Upgrade* (*Uaktualnienie*) (rysunek 6.43).

Rysunek 6.43.
Rodzaj instalacji



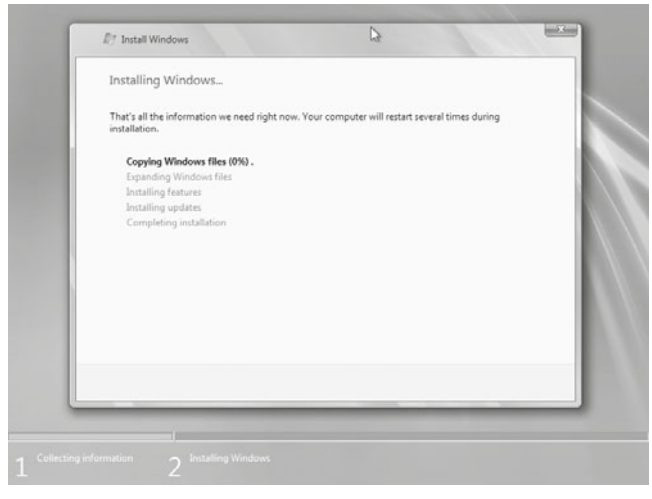
6. Wybór miejsca instalacji — istniejąca partycja lub tworzenie nowej i formatowanie w systemach plików FAT lub NTFS — (omówione w podręczniku *Kwalifikacja E.12. Montaż i eksploatacja komputerów osobistych oraz urządzeń peryferyjnych. Podręcznik do nauki zawodu technik informatyk*) poprzez wybór *Options* (*advanced*) (*Opcje dysku* (*zaawansowane*)) (rysunek 6.44).

Rysunek 6.44.
Tworzenie partycji



7. Proces kopiowania plików (rysunek 6.45).

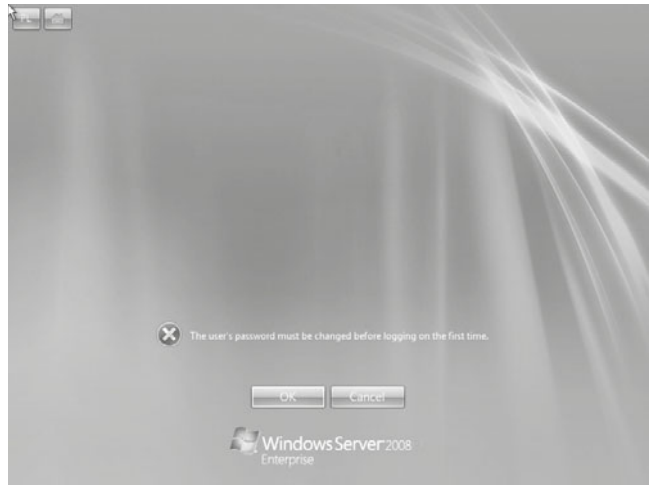
Rysunek 6.45.
Proces
kopiowania plików



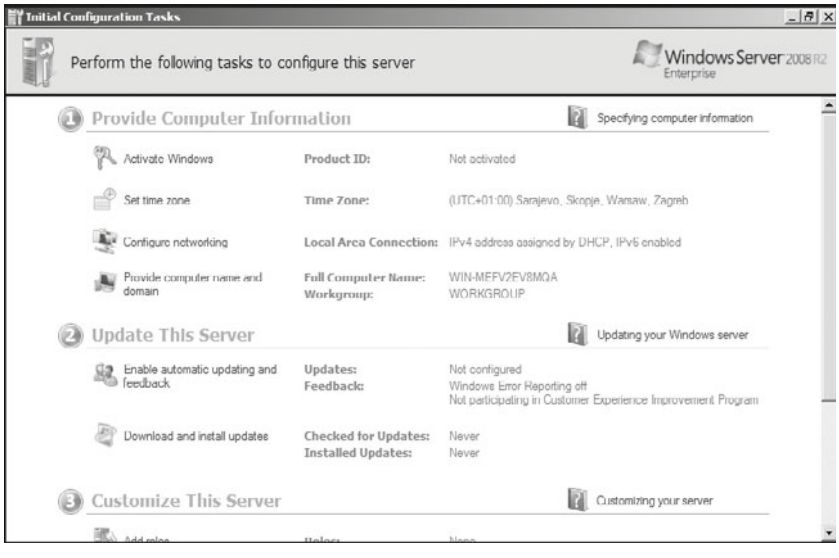
8. Po instalacji, przed pierwszym logowaniem, trzeba ustawić nowe hasło dostępu do konta administratora (*The user's password must be changed before logging on the first time* (*Hasło użytkownika musi zostać zmienione przed pierwszym zalogowaniem*)).

Hasło musi mieć odpowiednią złożoność — musi składać się z cyfr, dużych i małych liter i znaków specjalnych, np. *zaq1@WSX* lub *P@$$w0rd* (rysunek 6.46).

Rysunek 6.46.
Zmiana hasła



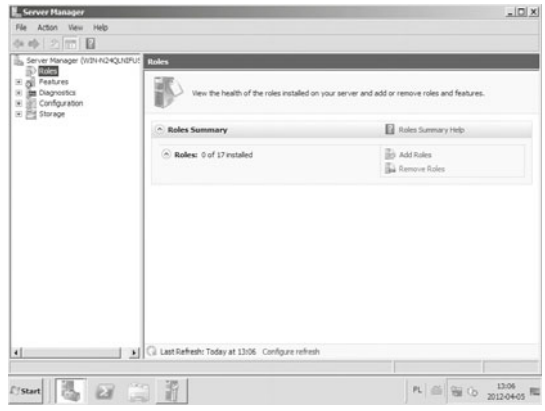
9. Po pierwszym uruchomieniu pojawi się *Initial Configuration Tasks* (*Zadania konfiguracji początkowej*) (rysunek 6.47).



Rysunek 6.47. Okno Zadania konfiguracji początkowej

10. Okno *Server Manager* (*Zarządzanie serwerem*) umożliwi instalację oraz konfigurację roli (rysunek 6.48).

Rysunek 6.48.
Okno zarządzania serwerem



6.4.2. Instalacja serwera w wersji Core

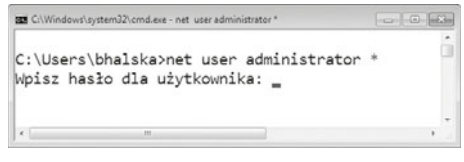
Wszystkie wersje serwera dostępne do instalacji mogą być zainstalowane w wersji Core. Jest to wersja bez interfejsu graficznego, a wszystkie opcje instalacyjne czy konfiguracyjne są w niej definiowane z konsoli lub za pomocą specjalnych skryptów. Instalacja przebiega tak samo jak instalacja wersji pełnej, różnice są widoczne dopiero po ponownym uruchomieniu komputera.

1. Po zalogowaniu należy ustawić hasło dla administratora. Jest to możliwe jedynie w konsoli (interpretator poleceń), którą należy uruchomić jako nowe zadanie w oknie menadżera zadań (rysunek 6.49).

Składnia polecenia:

```
net user administrator *
```

Rysunek 6.49.
Zmiana hasła



W wersji Server 2008 R2 Core hasło można zmienić podczas pierwszego logowania.

2. Powyższe polecenie oraz wszystkie, które będą niezbędne do zainstalowania lub skonfigurowania serwera, można wpisać do specjalnego pliku *Unattend.xml*, który umożliwia przeprowadzenie instalacji nienadzorowanej. Plik *Unattend.xml* pozwala na wykonanie większości początkowych zadań konfiguracji w trakcie działania programu instalacyjnego.

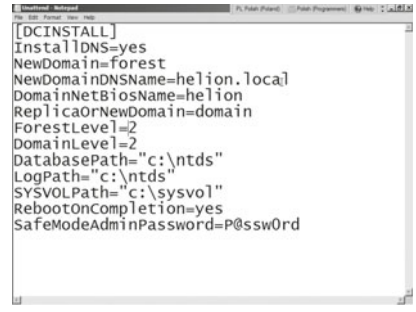
Korzyści związane z instalacją nienadzorowaną:

- Nie trzeba przeprowadzać początkowych konfiguracji przy użyciu narzędzi wiersza poleceń.

- W pliku instalacji nienadzorowanej można dołączyć ustawienia umożliwiające administrację zdalną (po zakończeniu instalacji).
- Można skonfigurować ustawienia, które trudno modyfikować w wierszu poleceń, takie jak rozdzielczość ekranu.

W celu zainstalowania systemu Windows Server 2008 R2 w wersji Core przy użyciu pliku instalacji nienadzorowanej należy:

- Utworzyć plik XML nazwany *Unattend.xml* (rysunek 6.50) za pomocą edytora tekstu lub programu Windows System Image Manager.
- Następnie skopiować plik *Unattend.xml* na dysk lokalny.



Rysunek 6.50. Tworzenie pliku Unattend.xml

W celu skorzystania z pliku instalacji nienadzorowanej należy:

1. W pierwszym kroku skopiować lub utworzyć plik *Unattend.txt* w głównym katalogu dysku C.
2. W konsoli wprowadzić poniższe polecenie i potwierdzić klawiszem *Enter*:

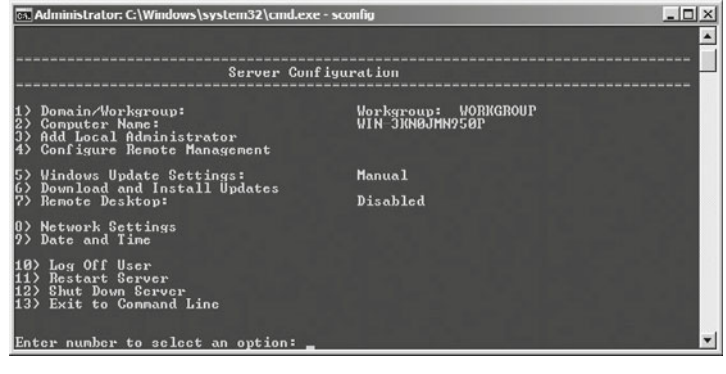
```
dcpromo /answer:C:\unattend.txt
```

3. Po zakończeniu nienadzorowanej instalacji serwer zostanie automatycznie ponownie uruchomiony.

System Windows Server 2008 R2 w wersji Core umożliwia uruchomienie najważniejszych ról serwera:

- usług domenowych w usłudze Active Directory,
- usług LDS w usłudze Active Directory (AD LDS),
- serwera DHCP,
- serwera DNS,
- usług plików,
- serwera wydruku,
- usług multimediów strumieniowych.

Do konfigurowania systemu Windows Server 2008 R2 w wersji Core można wykorzystać narzędzie `sconfig` (rysunek 6.51).



Rysunek 6.51. Narzędzie do konfiguracji serwera — sconfig

ĆWICZENIA

1. Zainstaluj na wirtualnej maszynie serwer 2008 R2 w pełnej wersji.
2. Zainstaluj na wirtualnej maszynie serwer w wersji Core.

PYTANIA

1. Wymień różnice pomiędzy systemami Windows Server 2008 w wersji pełnej i w wersji Core.
2. Wymień wymagania niezbędne do zainstalowania serwera w wersji pełnej.
3. Wymień wymagania sprzętowe niezbędne do zainstalowania serwera w wersji Core.
4. Wymień różnice w wymaganiach i przeznaczeniu pomiędzy wersją Standard a Enterprise.
5. Wymień narzędzia do zarządzania serwerem w pełnej wersji.
6. Wymień narzędzia do zarządzania serwerem w wersji Core.

6.4.3. Role serwera

W systemach operacyjnych z rodziny Windows Server jest dostępnych kilka ról serwerów. Rola określa usługi uruchamiane i udostępniane na serwerze. System Windows Server 2008 R2 może przyjmować następujące role:

- **Usługa katalogowa** (ang. *Active Directory*) umożliwia scentralizowane zarządzanie tożsamościami, uprawnieniami oraz obiektami w sieci. W Windows Server 2008 R2 z usługą katalogową jest związanych pięć ról, które zostały opisane w punkcie 6.4.5 — „Usługa katalogowa".
- **Serwer DHCP** (ang. *Dynamic Host Configuration Protocol*) automatycznie przydziela urządzeniom sieciowym adresy IP oraz inne parametry, które są niezbędne do prawidłowego działania sieci.
- **Serwer DNS** (ang. *Domain Name System*) dokonuje tłumaczenia nazw domenowych na adresy IP. Jest wymagany dla poprawnego działania usługi katalogowej.
- **Serwer plików** (ang. *file server*) dostarcza narzędzi umożliwiających zarządzanie plikami, szybkie wyszukiwanie plików oraz łatwe współdzielenie zasobów. Ta rola pozwala również na replikowanie zasobów między serwerami.
- **Serwer usług terminalowych** (ang. *terminal services*) — to technologia pozwalająca na zdalny dostęp do środowiska Windows na serwerze w celu uruchamiania programów, zapisywania plików i/lub korzystania z zasobów sieciowych dostępnych na serwerze.

- **Serwer kontroli dostępu przez sieć** (ang. *Network Access Services*) to mechanizm routingu w ruchu wymienianym z sieciami LAN oraz WAN. Odpowiada za wymuszanie przestrzegania zasad bezpieczeństwa skonfigurowanych w danej organizacji oraz kontrolowanie zdalnego dostępu do zasobów sieciowych przez kanały szyfrowane.
- **Serwer wydruku** (ang. *print server*) umożliwia udostępnianie drukarek, zarządzanie kolejkami wydruku oraz zarządzanie drukarkami na poziomie całej domeny.
- **Serwer internetowy** (ang. IIS — *Internet Information Services*) — serwer WWW.
- **Usługi WDS** (ang. *Windows Deployment Services*) służy do instalowania systemu operacyjnego na komputerach podłączonych do sieci. Oznacza to, że nie trzeba instalować każdego systemu operacyjnego z dysku CD lub DVD.

PYTANIA

1. Wymień role serwera.

6.4.4. Interfejsy sieciowe

Interfejsy sieciowe umożliwiają innym komputerom dostęp do usług oferowanych przez serwer. Najczęściej spotykane konfiguracje mają jeden lub dwa interfejsy (w zależności od roli serwera). Rysunek 6.52 przedstawia sytuację, gdzie obecne są dwa interfejsy: sieć lokalna (LAN) oraz sieć zewnętrzna (WAN), co może oznaczać, że serwer pełni również funkcję routera (udostępnia internet komputerom w sieci lokalnej). Serwery z jednym lokalnym interfejsem są zwykle oddzielone od sieci zewnętrznej ze względów bezpieczeństwa lub dlatego, że pełnią jedną funkcję, na przykład bazy danych dla serwera udostępniającego rozbudowany i często odwiedzany portal. Sytuacja, gdy jedyny interfejs jest połączony z siecią WAN, jest rzadko spotykana i niezalecana (łatwiej zaatakować taką maszynę).

Rysunek 6.52. Interfejsy sieciowe

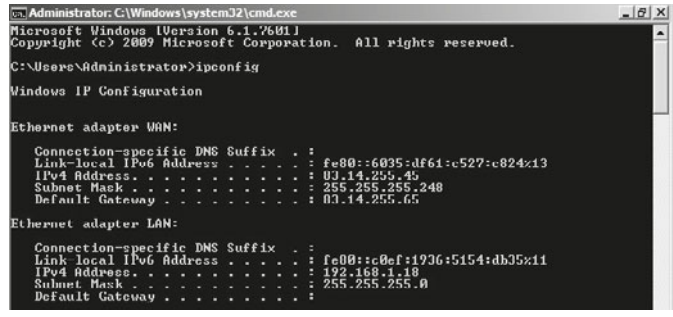
Interfejs lokalny (LAN, ang. *Local Area Network*) jest kartą sieciową, która komunikuje się z komputerami w wewnętrznej sieci lokalnej. Mianem sieci lokalnej można już nazwać nawet dwa bezpośrednio połączone ze sobą komputery.

Interfejs zewnętrzny (WAN, ang. *Wide Area Network*) jest zazwyczaj bezpośrednio wpięty do routera lub modemu, dzięki któremu uzyskuje dostęp do sieci zewnętrznej.

Najczęściej spotykaną konfiguracją wyżej wymienionych interfejsów jest: w przypadku LAN — adres statyczny przydzielany zgodnie z założeniami sieci lokalnej, a dla interfejsu WAN — adres dynamiczny (DHCP). Dzieje się tak, ponieważ w przypadku

zmiany zewnętrznej puli adresowej przez dostawcę internetu nie trzeba nic zmieniać w konfiguracji interfejsu.

Rysunek 6.53. Konfiguracja interfejsów — polecenie ipconfig



Konfiguracja interfejsów — polecenie ipconfig

Interfejsy mogą być konfigurowane zarówno w trybie graficznym (podrozdział 6.1, „Konfiguracja interfejsów sieciowych"), jak i w trybie konsoli. Pierwszym krokiem jest sprawdzenie identyfikatorów interfejsów przez polecenie:

```
netsh interface ipv4 show interfaces
```

Po uzyskaniu nazw i identyfikatorów zmianę konfiguracji można przeprowadzić za pomocą następujących poleceń:

LAN

```
netsh interface ipv4 set address name="Połączenie lokalne" source=static
address=192.168.18.1 mask=255.255.255.0 gateway=192.168.18.1
```

WAN

```
netsh interface ipv4 set address name="1" source=dhcp
netsh interface ipv4 set dns name="1" source=dhcp
```

ĆWICZENIA

1. Skonfiguruj dwie karty sieciowe: WAN i LAN, pamiętając o tym, że LAN oznacza kartę sieciową, która obsługuje ruch wewnątrz lokalnej sieci, a więc musi mieć zdefiniowany adres statyczny, np. 192.168.nr_z_dziennika.1. Kartę WAN ustaw jako dynamiczną w celu uzyskania dostępu do internetu w ramach sieci szkolnej.
2. Skonfiguruj kartę LAN przy użyciu polecenia `netsh`.

PYTANIA

1. Wymień informacje, jakie musimy znać, aby skonfigurować kartę z ustawieniami statycznymi.
2. Wymień polecenie do konfigurowania karty sieciowej z konsoli.

6.4.5. Usługa katalogowa

DEFINICJA

Usługa katalogowa (ang. *Active Directory*) to baza danych zawierająca następujące obiekty: jednostki organizacyjne, użytkowników, zasoby sieciowe, urządzenia sieciowe (np. drukarki).

Jedną z jej najważniejszych funkcji jest zapewnienie administratorom jednego, logicznego i precyzyjnego sposobu identyfikowania urządzeń i usług sieciowych oraz użytkowników. Usługa katalogowa oferuje dostęp za pośrednictwem bezpiecznego logowania i hierarchicznie organizuje zasoby sieciowe (takie jak użytkownicy, drukarki, zespoły robocze, aplikacje, woluminy, serwery plików, serwery baz danych, obiekty itp.) na drzewie katalogowym.

Usługa katalogowa składa się z kilku komponentów:

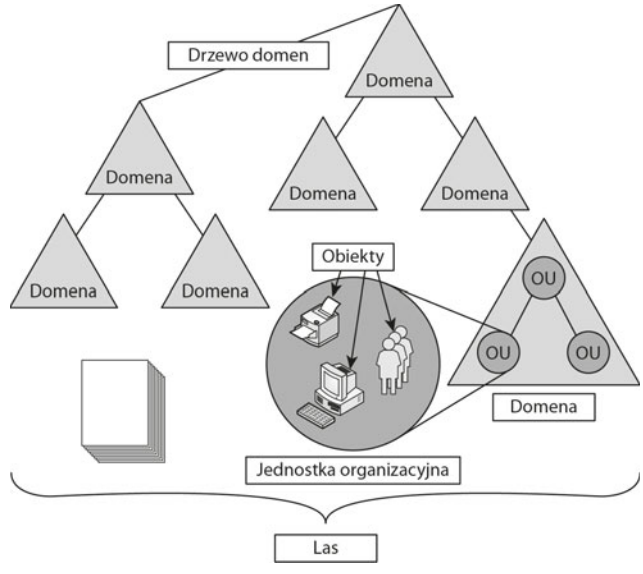
- *Active Directory Domain Services* — usługi domenowe w usłudze Active Directory (AD DS),
- *Active Directory Rights Management Services* — usługi zarządzania prawami dostępu w usłudze Active Directory (AD RMS),
- *Active Directory Federation Services* — usługi federacyjne w usłudze Active Directory (AD FS),
- *Active Directory Certificate Services* — usługa certyfikatów w usłudze Active Directory (AD CS),
- *Active Directory Lightweight Directory Services* — usługi LDS w usłudze Active Directory (AD LDS).

Struktura Active Directory Domain Services (AD DS)

Struktura AD DS opiera się na modelu usługi katalogowej X.500 i jest reprezentowana przez trójkąt określany jako domena (rysunek 6.54). Jej głównym zadaniem jest identyfikowanie usług katalogowych, zapewnia uwierzytelnianie i zarządzanie obiektami w obrębie organizacji.

Role związane z domeną

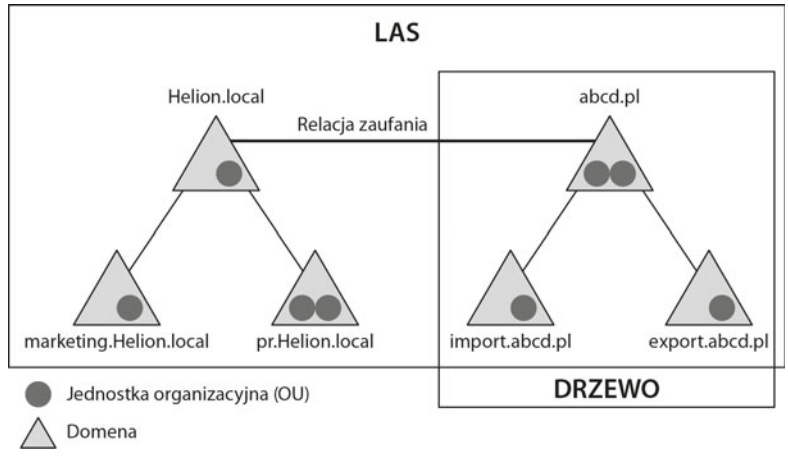
- **Podstawowy kontroler domeny** (ang. *Primary domain controller PDC*) jest głównym kontrolerem domeny odpowiedzialnym za zarządzanie uprawnieniami. W domenie może istnieć tylko jeden serwer pełniący tę rolę.
- **Wzorzec infrastruktury** (ang. *Infrastructure master*) — w każdej domenie może istnieć tylko jeden wzorzec infrastruktury, który jest odpowiedzialny za aktualizowanie odwołań z obiektów w swojej domenie do obiektów w innych domenach. Wzorzec infrastruktury porównuje swoje dane z tymi, które znajdują się w wykazie



Rysunek 6.54. Reprezentacja struktury AD DS

globalnym. Kiedy obiekt jest przenoszony z jednej domeny do innej, usługa ta uaktualnia obiekt odniesienia znajdujący się w domenie pierwotnej, wskazujący na obiekt w nowej domenie, co zapobiega utracie informacji o członkostwie grup skojarzonych z kontem użytkownika w przypadku zmiany nazwy tego konta lub jego przeniesienia.

Istnieje możliwość zbudowania drzewa domen, które musi się składać przynajmniej z dwóch domen połączonych dwukierunkowymi, przechodnimi relacjami zaufania. Z drzew domen można zbudować *las*, w obrębie którego domeny mają wspólną przestrzeń nazw, lecz mają także mechanizmy zabezpieczeń oddzielające prawa dostępu między nimi (rysunek 6.55).



Rysunek 6.55. Przykładowa struktura lasu z relacją zaufania pomiędzy dwoma drzewami domen

Role związane z lasem

- **Wzorzec schematu** (ang. *schema master*) — usługa, której zadaniem jest sprawowanie kontroli nad zmianami związanymi ze schematem. Zawiera on listę klas obiektów i atrybutów, które są używane do tworzenia obiektów Active Directory (np. użytkowników).
- **Wzorzec nazw domen** (ang. *domain naming master*) — usługa, której zadaniem jest nadzorowanie dodawanych i usuwanych domen w danym lesie. Kiedy jest tworzona nowa domena, tylko kontroler, który przechowuje tę rolę, może dokonać odpowiednich wpisów w AD. Zabezpiecza to przed dodaniem domen o już istniejących nazwach.

Dla każdego lasu istnieje tylko jeden wzorzec schematu i jeden wzorzec nazw domen. Jest to rola wzorca operacji nazywana rolami FSMO. Aby przenieść kontrolę na nowy serwer, należy przenieść wszystkie role FSMO (ang. *Flexible Single Operations Masters*), a więc:

- **Wzorzec schematu** (ang. *Schema Master*) — rola obejmująca cały las. W danym lesie może być tylko jeden wzorzec schematu. Rola ta jest wymagana do rozszerzania schematu lasu usługi katalogowej (AD) oraz do przeniesienia roli na inny kontroler przy użyciu polecenia `adprep/domainprep`.
- **Wzorzec nazw domen** (ang. *Domain Naming Master*) — rola obejmująca cały las. W danym lesie może być tylko jeden wzorzec nazw domenowych. Służy do dodawania domen lub partycji aplikacji do lasu oraz do usuwania ich z lasu.
- **Wzorzec RID** (ang. *Relative ID Master*) — rola obejmująca całą domenę. W danej domenie występuje tylko jeden wzorzec RID. Służy do przydzielania puli identyfikatorów RID, dzięki czemu nowe lub istniejące kontrolery domeny mogą tworzyć konta użytkowników, konta komputerów i grupy zabezpieczeń. Każdy z obiektów usługi katalogowej, którym można przyznawać uprawnienia, jest jednoznacznie identyfikowany za pomocą identyfikatora zabezpieczeń SID (ang. *Security ID*).
- **Emulator kontrolera PDC** (ang. *Primary Domain Controller Emulator*) — rola obejmująca całą domenę. W danej domenie występuje tylko jedna taka rola. Jest potrzebna na kontrolerach domeny, które wysyłają aktualizacje baz danych na zapasowe kontrolery domeny systemu. Kontroler domeny mający tę rolę podlega także działaniu pewnych narzędzi administracyjnych, a hasła kont komputerów i kont użytkowników przechowywanych na tym komputerze są odpowiednio aktualizowane.
- Wzorzec infrastruktury — rola obejmująca całą domenę. W danej domenie występuje tylko jeden wzorzec infrastruktury. Zarządza odwołaniami do obiektów domen spoza własnej domeny.

Na poniższej liście przedstawiono partycje wszystkich ról FSMO (tabela 6.3).

Tabela 6.3. Tabela ról FSMO

Rola FSMO	Partycja
Schemat	`CN=Schema,CN=configuration,DC=<domena główna lasu>`
Wzorzec nazw domen	`CN=configuration,DC=<domena główna lasu>`
Kontroler PDC	`DC=<domena>`
RID	`DC=<domena>`
Infrastruktura	`DC=<domena>`

WAŻNE

Nazwa wyróżniająca (ang. DN — *Distinguished Name*) opisuje położenie obiektu w strukturze hierarchicznej. Jej podstawowe elementy to:

- DC — *Domain Component* (`Helion`) — komponent domeny,
- DC — *Domain Component* (`local`) — kontroler domeny,
- CN — *Common Name* (`Basia`) — nazwa ogólna obiektu (np. nazwa użytkownika),
- OU — *Organisation Unit* (`ZS6`) — jednostka organizacyjna.

Przykładem nazwy wyróżniającej jest: `Basia.ZS6.Helion.local`.

Active Directory Rights Management Services (AD RMS)

Jest usługą, która umożliwia kontrolę plików. AD RMS pozwala na sprawowanie kontroli nad dokumentem po jego otwarciu. Dzięki niej możemy zastrzec, czy wysyłany plik do innego użytkownika może być tylko do odczytu, czy też będzie możliwy wydruk lub skopiowanie oraz modyfikacja jego zawartości. Usługa umożliwia również zastosowanie polityk dla dokumentów, niezależnie od tego, czy dany plik będzie otwierany w trybie offline, czy online, a także czy odbędzie się to wewnątrz firmy, czy poza nią. Daje to możliwość ochrony własności intelektualnej, zabezpieczenia zawartości dokumentów przed nieuprawnionymi zmianami, a także umożliwia ustalenie, kto i w jaki sposób korzysta z danego dokumentu.

Active Directory Federation Services

Jest usługą, która umożliwia stosowanie tożsamości i praw dostępu na wielu platformach, zarówno w środowiskach opartych na technologiach Windows, jak i nie-Windowsowych, a także dostarczanie dostępu zaufanym partnerom spoza sieci. W złożonych środowiskach każda organizacja sama kontroluje tożsamości i prawa dostępu wewnątrz własnej sieci, ale może również w bezpieczny sposób zaakceptować tożsamości pochodzące z zaufanych firm. Użytkownicy są uwierzytelniani w jednej sieci, jednak dostają uprawnienia do zasobów w innych sieciach. Taki proces jest nazywany SSO (ang. *Single Sign On*). AD FS rozszerza wewnętrzną strukturę AD DS.

Active Directory Certificate Services

Jest usługą, która umożliwia utworzenie centrum certyfikacyjnego. Dzięki niemu jest możliwe wystawianie cyfrowo podpisanych certyfikatów będących częścią infrastruktury PKI łączącej osoby, urządzenia lub usługi z ich prywatnymi kluczami. Certyfikaty mogą być wykorzystywane do uwierzytelniania użytkowników i urządzeń, autoryzacji opartej na kartach inteligentnych, autoryzacji stron WWW, a także aplikacji (np. bezpieczne sieci bezprzewodowe, VPN, EFS, podpis elektroniczny i inne). Usługa AD CS wewnątrz sieci może być zintegrowana z AD DS i może automatycznie wystawiać certyfikaty dla użytkowników i urządzeń.

Active Directory Lightweight Directory Services

Jest usługą, która umożliwia dostarczenie usług katalogowych dla aplikacji. AD LDS przetrzymuje i replikuje dane związane tylko z aplikacjami, wspiera wiele niezależnych baz danych w jednym systemie operacyjnym, dzięki czemu umożliwia każdej aplikacji stosowanie niezależnego schematu baz danych, portów SSL, oddzielnych logów. Usługa nie opiera się na AD DS, więc może być wdrożona na niezależnych serwerach oraz w środowisku grup roboczych. Jednakże w środowiskach, w których zostało wdrożone AD DS, AD LDS może wykorzystywać AD DS w celu potwierdzania tożsamości użytkowników, grup i komputerów. Usługa AD LDS jest przydatna przy przeprowadzaniu uwierzytelniania w sieciach wystawionych na większe ryzyko ingerencji z zewnątrz, np. przy autoryzacji użytkowników na stronach WWW. Takie rozwiązanie jest bezpieczniejsze niż wykorzystywanie do tego celu AD DS.

ĆWICZENIA

1. Stwórz strukturę lasu z dwoma drzewami i relacjami zaufania między nimi dla domeny nazwisko.local. Projekt wykonaj na kartce.

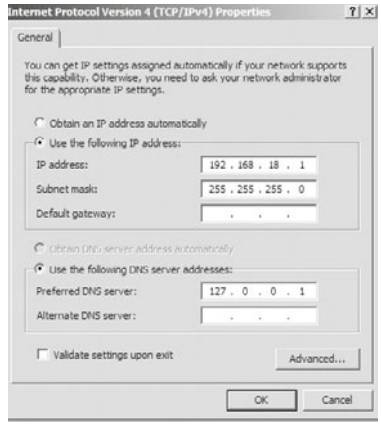
PYTANIA

1. Omów PDC.
2. Co to jest las domen?
3. Wymień zbiór ról FSMO.
4. Co to jest Active Directory?

6.4.6. Instalacja usługi katalogowej

Jest to pierwsza rola, jaką trzeba zainstalować dla nowej domeny w nowym lesie. Przed instalacją należy ustawić dla interfejsu prywatnego statyczny adres (rysunek 6.56).

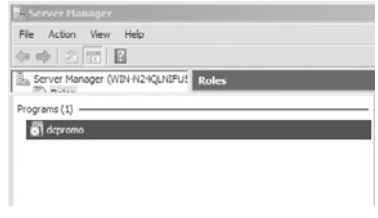
Rysunek 6.56. Konfiguracja adresu statycznego — Windows Server 2008 R2



Instalację można przeprowadzić, dodając nową rolę w menadżerze serwera lub wywołując z konsoli kreator instalacji poprzez wpisanie `dcpromo`. Ten kreator umożliwia zainstalowanie również usługi DNS, która jest niezbędna dla funkcjonowania domeny.

W dalszych krokach jest przedstawiona instalacja AD z wykorzystaniem kreatora `dcpromo` (rysunek 6.57).

Rysunek 6.57. dcpromo



1. Uruchomienie kreatora instalacji (rysunek 6.58).

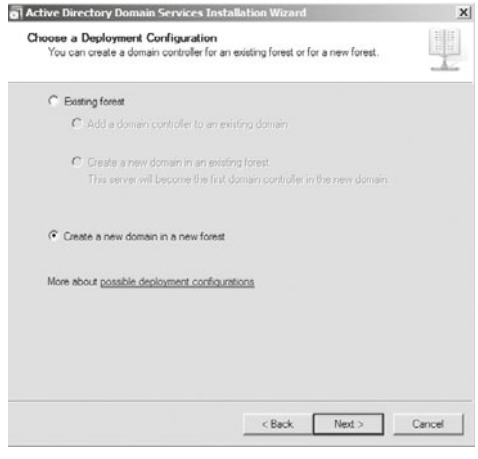
Rysunek 6.58. Kreator instalacji

2. W kolejnym kroku pojawia się okno zgodności systemu operacyjnego, gdzie są podane informacje dotyczące domyślnych zabezpieczeń, które mogą mieć wpływ na działanie ze starszymi systemami. Po zapoznaniu się z zawartymi w tym oknie informacjami należy wcisnąć *Next* (*Dalej*) (rysunek 6.59)

Rysunek 6.59.
Okno zgodności systemu operacyjnego

3. Należy określić, czy jest to nowa domena w nowym lesie, czy też chcemy dołączyć tę domenę do już istniejących. Dla nowej domeny należy wybrać *Create a new domain in a new forest* (*Utwórz nową domenę w nowym lesie*) (rysunek 6.60).

Rysunek 6.60.
Tworzenie nowej domeny

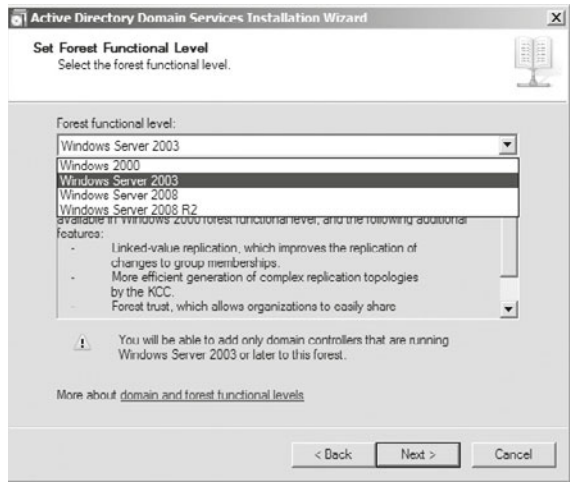


Następnie należy zdefiniować nazwę dla nowo tworzonej domeny. Nazwa może być dowolna, ważne, by kończyła się słowem *local*, co oznacza, że jest to domena lokalna (rysunek 6.61).

Rysunek 6.61.
Tworzenie nowej domeny helion.local

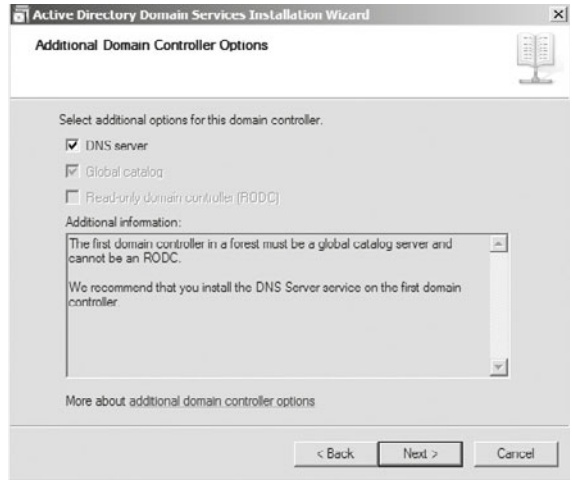
Kolejnym krokiem jest wybór poziomu funkcjonowania lasu, czyli funkcjonalności domeny zależnej od wersji serwerów Windows (rysunek 6.62). Jeśli poziom funkcjonalności zostanie określony jako Windows Server 2008 R2, do tego lasu nie będzie można podłączyć kontrolerów domeny pracujących pod kontrolą wcześniejszych wersji systemu Windows Server. Poziom funkcjonalności można zmienić na wyższy, ale nie ma możliwości zmiany na poziom niższy. Podobnie jest przy wyborze poziomu funkcjonalności domeny.

Rysunek 6.62. Poziom funkcjonalności lasu



Usługi domenowe w usłudze katalogowej do poprawnego działania wymagają zainstalowanej usługi DNS. Można ją zainstalować w oknie wyboru dodatkowej opcji dla kontrolera domeny (jeżeli serwer DNS nie został wcześniej zainstalowany) (rysunek 6.63).

Rysunek 6.63. Instalacja dodatkowych opcji



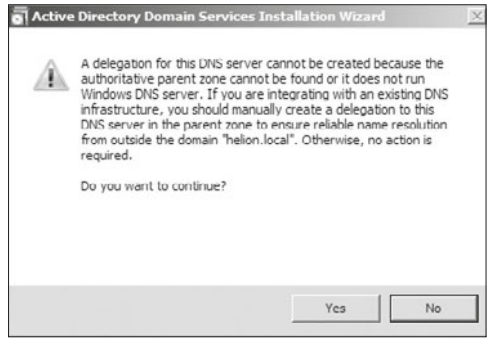
WAŻNE

Wykaz globalny (ang. *Global catalog*) służy do uwierzytelniania użytkowników i wyszukiwania obiektów katalogowych w lesie. Przechowuje kopię danych w trybie odczytu i zapisu.

Kontroler RODC przypomina serwer wykazu globalnego. Przechowuje kopię danych katalogowych tylko w trybie odczytu, może również uwierzytelniać użytkowników, natomiast żądania do zapisu przekazuje do kontrolera domeny.

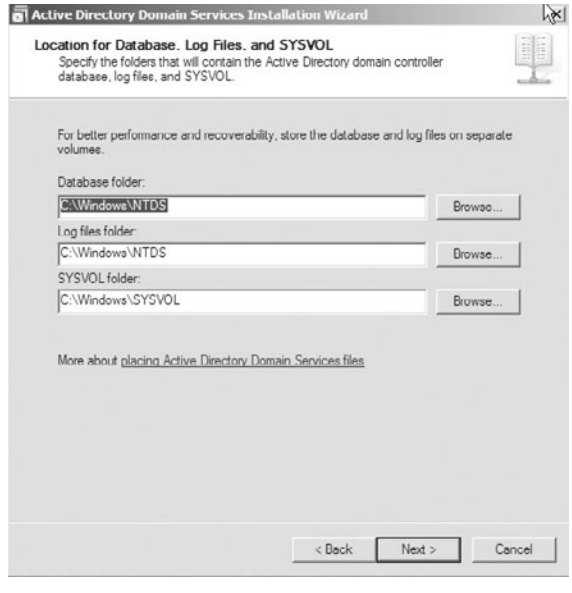
4. Wyświetla się komunikat o braku możliwości utworzenia delegowania dla tego serwera DNS. Pojawienie się tego okna jest spowodowane brakiem usługi DNS na serwerze. Po kliknięciu *Yes* (*Tak*) zostanie ona zainstalowana (rysunek 6.64).

Rysunek 6.64. Potwierdzenie instalacji serwera DNS



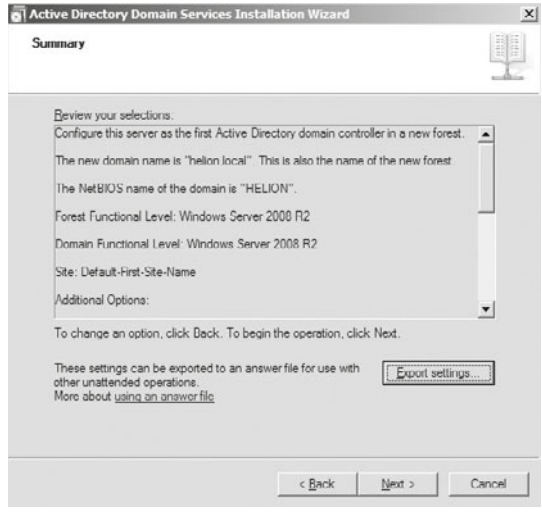
5. Należy określić lokalizację, gdzie będzie przechowywana baza danych oraz pliki dziennika i folder *SYSVOL* (rysunek 6.65). Można zmienić lokalizację za pomocą funkcji *Browse* (*Przeglądaj*) lub pozostawić wartości domyślne, klikając *Next* (*Dalej*).

Rysunek 6.65. Baza danych AD

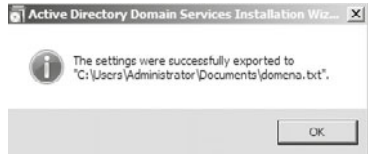


6. Należy zdefiniować hasło dla konta administratora trybu przywracania usług katalogowych, które różni się od konta administratora domeny. Z tego powodu zalecane jest wybranie innego hasła niż to, które zostało zdefiniowane dla konta administratora.
7. Po zapoznaniu się z oknem podsumowania kreatora tworzenia pierwszego kontrolera domeny w nowym lesie można całą konfigurację wyeksportować oraz zatwierdzić, klikając opcję *Next* (*Dalej*) (rysunek 6.66 i 6.67).

Rysunek 6.66. Podsumowanie kreatora tworzenia kontrolera domeny



Rysunek 6.67. Wyeksportowana konfiguracja



8. Nastąpi proces konfigurowania usług domenowych w usłudze AD. Po zakończeniu instalacji należy ponownie uruchomić serwer.

6.4.7. Podłączenie stacji roboczej do domeny

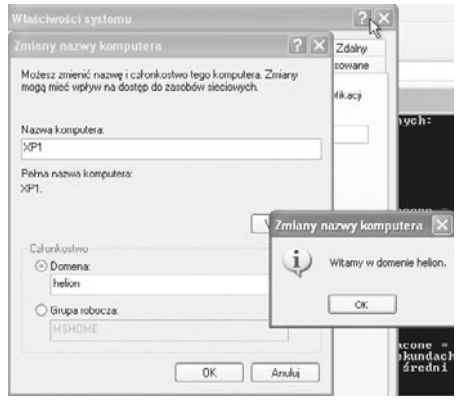
WAŻNE

Aby możliwe było korzystanie z sieci opartej na usłudze Active Directory, wymagane jest używanie systemu operacyjnego w wersji przeznaczonej dla zastosowań biznesowych (*Professional, Ultimate*) — wersje systemu dla użytkowników domowych nie zawierają mechanizmu pracy w domenie.

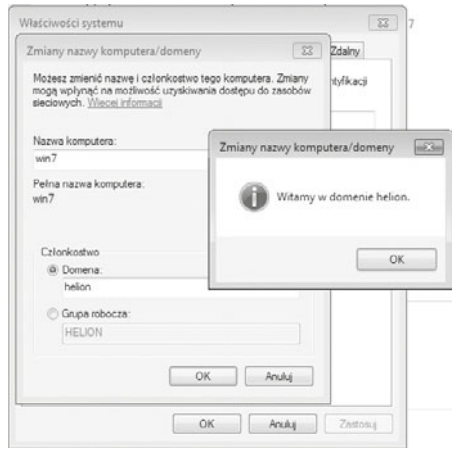
Aby podłączyć się do domeny Active Directory, należy posiadać konto użytkownika domeny, które przydziela administrator. Wymagane jest również, aby użytkownik miał prawo do przyłączenia komputera do domeny. Prawo to posiadają użytkownicy

przypisani do grupy *Administratorzy* domeny. Informacje na temat zakładania grup oraz użytkowników zostały opisane w punkcie 6.4.8 — „Obiekty usługi katalogowej".

W celu podłączenia się do domeny należy w Panelu sterowania wybrać narzędzie *System*, a następnie w oknie *Właściwości systemu* wybrać zakładkę *Nazwa komputera* i w dalszej kolejności przycisk *Zmień*. W oknie *Zmiany nazwy komputera* należy wprowadzić nazwę domeny, do której mamy być podłączeni, następnie podać nazwę i hasło użytkownika posiadającego prawa dołączania do domeny. W dalszej kolejności wymagany jest restart komputera (rysunek 6.68). W systemie Windows 7 przynależność do domeny można zmienić w oknie *Zaawansowane ustawienia systemu* dostępnym w oknie *Właściwości systemu* (rysunek 6.69).



Rysunek 6.68. Podłączanie do domeny — Windows XP



Rysunek 6.69. Podłączanie do domeny — Windows 7

Przed podłączeniem stacji roboczej należy ustawić jej adres w tej samej sieci, w której funkcjonuje serwer domeny, np:

- Adres IP — np. 192.168.18.100,
- Maska — 255.255.255.0,
- Serwer DNS — 192.168.18.1 (adres serwera DNS dla domeny).

ĆWICZENIA

1. Skonfiguruj adres statyczny dla karty lokalnej.
2. Zainstaluj usługę katalogową i stwórz nową domenę w nowym lesie.
3. Dodaj do domeny stację roboczą z Windows XP i Windows 7.

PYTANIA

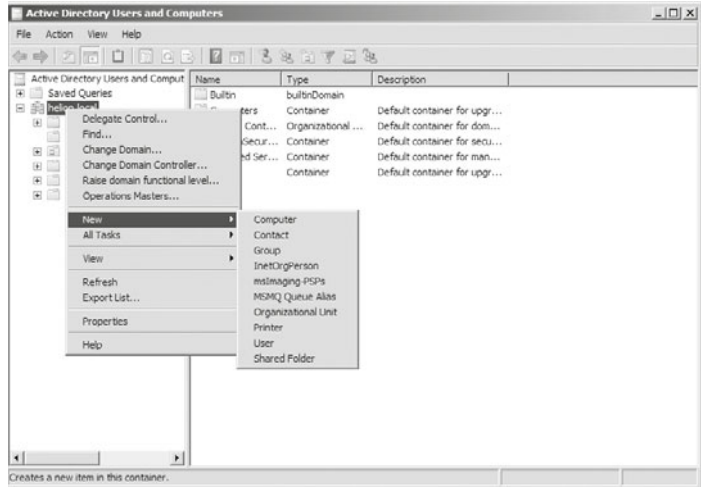
1. Jakie polecenie uruchamia kreator instalacji usługi katalogowej?
2. Jaka usługa musi być zainstalowana z usługą katalogową?
3. Co to jest domena?

6.4.8. Obiekty usługi katalogowej

Po zainstalowaniu i skonfigurowaniu usługi katalogowej należy stworzyć obiekty zgodnie z hierarchią w danym przedsiębiorstwie.

Obiekty, jakie można utworzyć w usłudze katalogowej, to (rysunek 6.70):

- jednostka organizacyjna,
- grupa,
- użytkownik,
- komputer,
- drukarka,
- udostępniony folder.



Rysunek 6.70. Obiekty usługi katalogowej

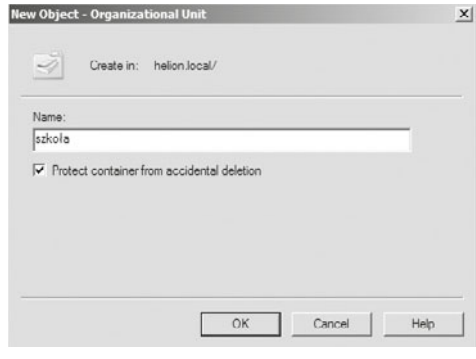
Aby utworzyć obiekt Active Directory, należy wybrać opcję *Active Directory Users and Computers* (*Użytkownicy i komputery usługi Active Directory*) dostępną w menu *Administrative tools* (*Narzędzia administracyjne*). Następnie należy wskazać domenę i wybrać z menu kontekstowego dostępnego po naciśnięciu prawego przycisku myszy opcję *New* (*Nowy*).

Jednostka organizacyjna

Jednostka organizacyjna to kontener usługi katalogowej, w którym można umieszczać użytkowników, grupy, komputery oraz inne jednostki organizacyjne. Jest najmniejszym zakresem lub jednostką, której można przypisać ustawienia zasad grupy lub nadać upoważnienia administracyjne. Przy użyciu jednostek organizacyjnych można utworzyć kontenery z domeną reprezentującą hierarchiczną, logiczną strukturę firmy. Pozwala to na zarządzanie konfiguracją oraz na korzystanie z kont i zasobów na podstawie modelu organizacyjnego.

W celu dodania jednostki organizacyjnej(rysunek 6.71) należy kliknąć domenę prawym klawiszem myszy i z menu kontekstowego wybrać opcję *New/Organizational Unit* (*Nowy Jednostka organizacyjna*).

Rysunek 6.71. Jednostka organizacyjna



Grupa użytkowników

Konto grupy stanowi kolekcję kont użytkowników, za pomocą której można przypisywać zbiory praw i uprawnień do wielu użytkowników jednocześnie. Grupa często zawiera także kontakty, komputery i inne grupy.

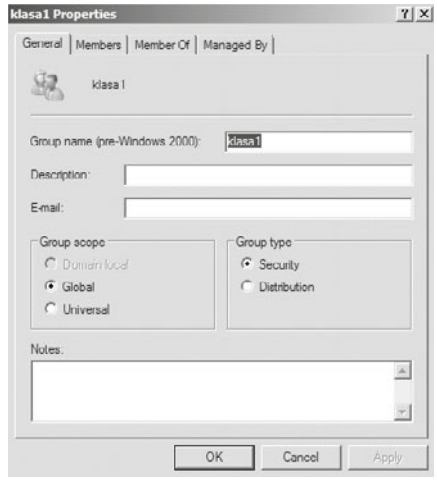
W usłudze katalogowej AD występują zasadniczo dwa typy grup:

- dystrybucyjne (ang. *distribution*) — mogą być używane tylko z aplikacjami poczty e-mail (np. Exchange) do wysyłania poczty e-mail do grup użytkowników. Grupy dystrybucyjne nie obsługują zabezpieczeń, co oznacza, że nie są wyświetlane na listach kontroli dostępu,
- zabezpieczeń (ang. *security*) — są używane do definiowania zabezpieczeń związanych z uprawnieniami jak również polityką bezpieczeństwa w ramach GPO.

Dodatkowo dla każdej grupy jest definiowany jej zakres, i tak mamy następujące grupy:

- lokalne domenowe (ang. *domain local*) — w domenie ułatwiają określanie dostępu do zasobów pojedynczej domeny i zarządzanie nimi,
- globalne (ang. *global*) — należy ich używać do zarządzania obiektami katalogowymi, które wymagają codziennej obsługi, takimi jak konta użytkowników i komputerów. Grupy o zakresie globalnym nie są replikowane poza ich własną domeną,
- uniwersalne (ang. *universal*) — należy ich używać do konsolidowania grup, które obejmują kilka domen. Aby to zrobić, trzeba dodać konta do grup o zakresie globalnym, a następnie zagnieździć te grupy w grupach o zakresie uniwersalnym.

W celu dodania nowej grupy musimy określić, gdzie ma się ona znajdować — np. w domyślnym katalogu, gdzie są tworzone grupy i użytkownicy podczas instalacji, czyli w katalogu *Users* (*Użytkownicy*) lub w danej jednostce organizacyjnej. Nową grupę tworzymy w taki sam sposób, w jaki tworzyliśmy nową jednostkę organizacyjną, a więc dodajemy nowy obiekt — *Group* (*Grupa użytkowników*) (rysunek 6.72).



Rysunek 6.72. Tworzenie grupy użytkowników

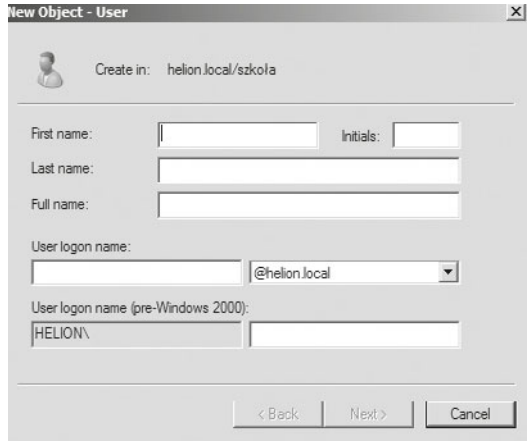
Użytkownik

Konta użytkowników służą do uwierzytelniania, autoryzowania i odmawiania dostępu do zasobów oraz do przeprowadzania inspekcji aktywności poszczególnych użytkowników w sieci. Za pomocą kont grup i użytkowników można w usłudze katalogowej (AD) zarządzać użytkownikami domeny. Tworząc konta grup i użytkowników na komputerze lokalnym, można zarządzać użytkownikami tego komputera (rysunek 6.73).

W polach *First name* (*Imię*) i *Last name* (*Nazwisko*) należy nadać imię i nazwisko użytkownika.

- W polu *Initials* (*Inicjały*) należy nadać inicjały użytkownika.
- W polu *User logon name* (*Nazwa logowania użytkownika*) należy nadać nazwę logowania użytkownika.

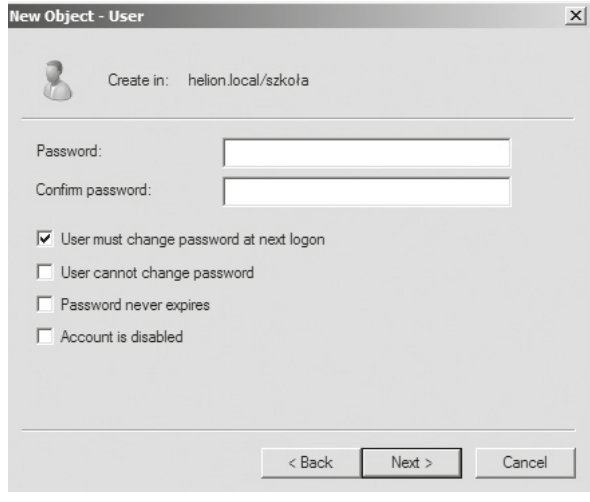
Rysunek 6.73.
Tworzenie
konta użytkownika



W polu *Password* (*Hasło*) i *Confirm password* (*Potwierdź hasło*) należy wpisać hasło użytkownika, a następnie wybrać odpowiednie opcje hasła, pamiętając o tym, aby hasło to było odpowiednio zdefiniowane, np. *xsw@!AZ* (rysunek 6.74).

- *User must change password at next logon* (*Użytkownik musi zmienić hasło przy następnym logowaniu*).
- *User cannot change password* (*Użytkownik nie może zmienić hasła*).
- *Password never expires* (*Hasło nigdy nie wygasa*).
- *Account is disabled* (*Konto jest wyłączone*).

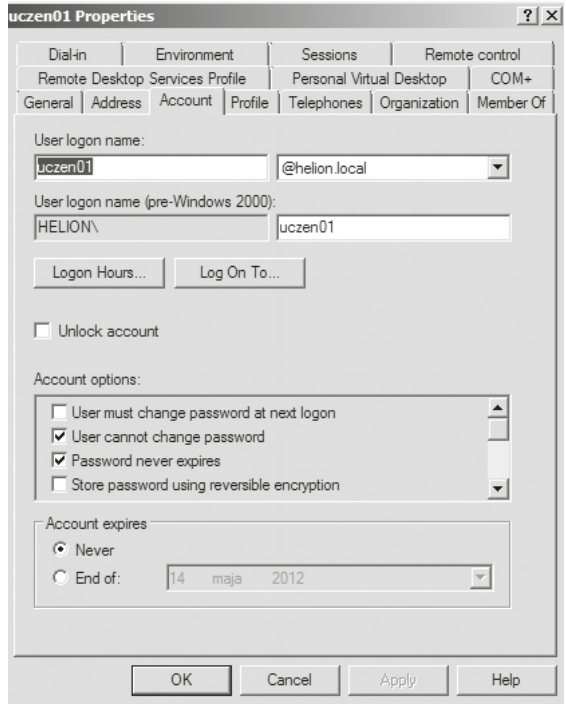
Rysunek 6.74.
Definiowanie hasła
dla użytkownika



Bardziej zaawansowana konfiguracja jest możliwa dopiero po utworzeniu konta, wtedy można zdefiniować (rysunek 6.75):

- dane dotyczące użytkownika (*General*, *Address*, *Telephones*),
- godziny logowania (*Logon Hours*),

- profil użytkownika (*Profile*),
- członkostwo w grupie (*Member Of*).



Rysunek 6.75. Zaawansowana konfiguracja użytkownika

Komputer

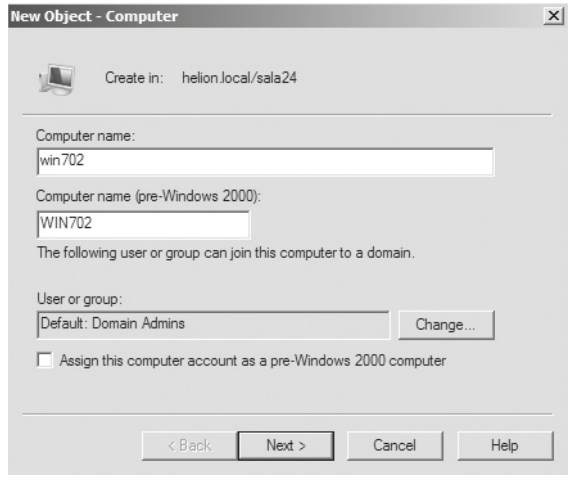
Każdy komputer należący do domeny ma swoje konto w usłudze katalogowej (AD).

Konto komputera w ramach usługi katalogowej można utworzyć na dwa sposoby:

- Użytkownik mający odpowiednie uprawnienia przyłącza komputer do domeny, w której nie ma obiektu odpowiadającego komputerowi. W takim przypadku konto zostanie automatycznie utworzone przez system we wbudowanej jednostce organizacyjnej *Computers* (*Komputery*). Takie konto komputera możemy przenieść do innej jednostki organizacyjnej.
- Administrator lub użytkownik z uprawnieniami tworzy konto komputera za pomocą odpowiednich narzędzi w wybranej przez siebie jednostce organizacyjnej i informuje użytkownika o nazwie konta. Użytkownik nazywa komputer według wskazówek administratora i przyłącza go do domeny.

W celu dodania komputera (rysunek 6.76) należy kliknąć prawym klawiszem myszy i z menu kontekstowego wybrać opcję *New/Computer* (*Nowy/Komputer*).

Rysunek 6.76.
Dodawanie nowego komputera do domeny

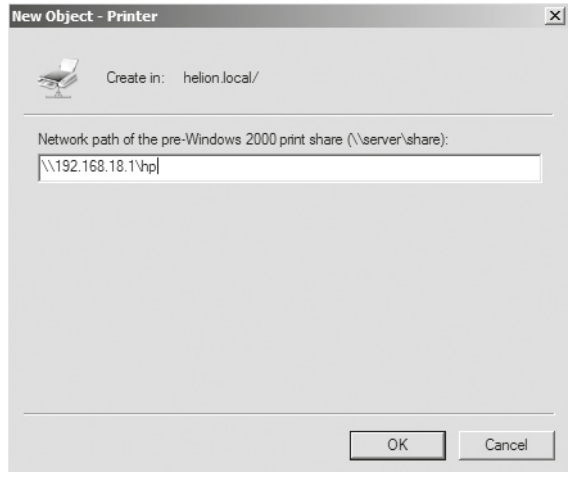


Drukarka

Drukarka jest obiektem w ramach domeny, który może zostać dodany globalnie lub w wybranej lokalnej jednostce organizacyjnej. Dodając ten obiekt, musimy znać adres, pod którym drukarka jest udostępniona w sieci (rysunek 6.77).

W celu dodania drukarki należy kliknąć prawym klawiszem myszy i z menu kontekstowego wybrać opcję *New/Printer* (*Nowy/Drukarka*).

Rysunek 6.77.
Dodawanie nowej drukarki do domeny



DEFINICJA

Narzędzia wiersza poleceń usług katalogowych to zbiór narzędzi (`dsadd`, `dsmod`, `dsrm`), które użyte z parametrami pozwalają tworzyć, modyfikować i usuwać obiekty. Są wygodne do stosowania w skryptach.

- `adprep` — wykonuje wstępne przygotowanie domeny Windows 2000 do zainstalowania domeny (dostępne na płycie instalacyjnej w katalogu *suport\adprep*).
- `dsadd` — dodaje do katalogów obiekty komputerów, kontaktów, grup i użytkowników oraz jednostek organizacyjnych.
- `dsget` — wyświetla właściwości obiektu podanego w parametrze wywołania.
- `dsmod` — zmienia właściwości obiektów istniejących w katalogu.
- `dsmove` — przenosi obiekt w obrębie jednej domeny lub zmienia mu nazwę.
- `dsrm` — usuwa obiekt z katalogu.
- `dsquery` — wyszukuje obiekty różnego rodzaju według podanych kryteriów.
- `ntdsutil` — umożliwia przeglądanie informacji o lokacjach, domenach i serwerach oraz wykonywanie konserwacji bazy danych Active Directory.
- *adsiedit.msc* — narzędzie do zarządzania obiektami i atrybutami w AD.
- `repadmin` — wyświetla informacje i diagnozuje problemy dotyczące replikacji pomiędzy kontrolerami domeny.
- `dcdiag` — diagnostyka kontrolera domeny.
- `redirusr` — zmiana domyślnego miejsca obiektu użytkownika.
- `redircmp` — zmiana domyślnego miejsca obiektu komputera.

ĆWICZENIA

1. Utwórz w domenie obiekty usługi katalogowej:
   a. Jednostkę organizacyjną o nazwie *grupa01*.
   b. Grupę zabezpieczeń o nazwie *grupa01* w jednostce organizacyjnej *grupa01*.
   c. Stwórz użytkownika w jednostce organizacyjnej *grupa01* i dodaj go do grupy *grupa01*.
2. Przetestuj polecenia związane z domeną.

PYTANIA

1. Sprawdź dostępne zasoby w sieci Active Directory.
2. Wymień obiekty usługi katalogowej.
3. Wymień narzędzia do zarządzania domeną.

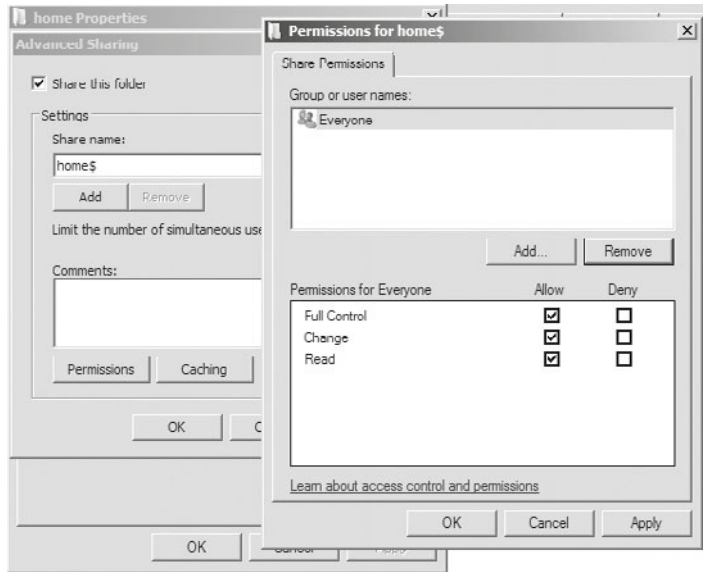
6.4.9. Profile użytkowników

Profile użytkowników umożliwiają automatyczne tworzenie i zachowywanie ustawień pulpitu dla środowiska pracy każdego użytkownika na komputerze lokalnym (profil lokalny).

Profil mobilny pozwala użytkownikom systemów Windows używać swoich ustawień programów i systemu na różnych komputerach w tej samej sieci pod warunkiem zalogowania się do tej samej domeny z tą samą nazwą użytkownika.

Tworzenie profilu mobilnego

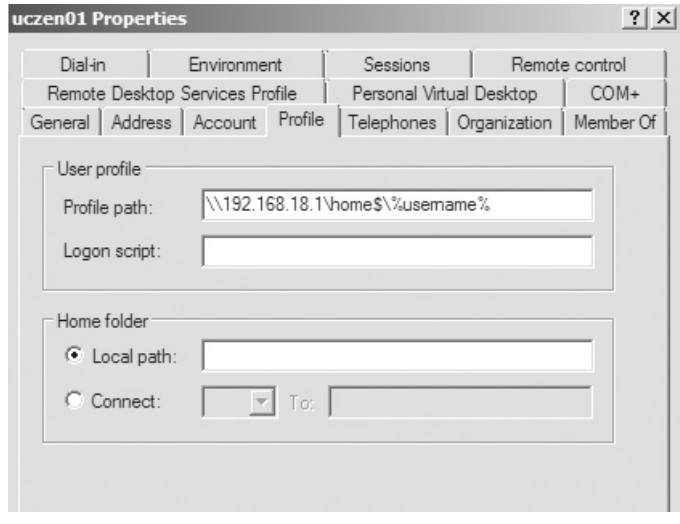
1. Na serwerze należy utworzyć folder, w którym będą przechowywane profile użytkowników. Będzie to folder najwyższego poziomu zawierający wszystkie profile poszczególnych użytkowników, np. *home*.
2. W kolejnym kroku należy skonfigurować ten folder jako folder udostępniony (ukryty dostęp jest możliwy przez dodanie *$* na końcu nazwy) oraz nadać wszystkim użytkownikom (*Everyone* (*Wszyscy*)) uprawnienia *Full Control* (*Pełna kontrola*). W pierwszym kroku należy kliknąć prawym klawiszem myszy katalog *home*, przejść do właściwości (*Properties* (*Właściwości*)), następnie do zakładki *Sharing* (*Udostępnianie*), gdzie trzeba wybrać *Advanced Sharing* (*Udostępnianie zaawansowane*). Należy zaznaczyć opcję *Share this folder* (*Udostępnij ten folder*), a następnie zdefiniować nazwę udziału (*Share name* (*Nazwa udziału*)) oraz nadać uprawnienia (*Permissions* (*Uprawnienia*)) (rysunek 6.78).



Rysunek 6.78. Konfiguracja uprawnień do katalogu przechowującego profil mobilny

3. Trzeba wybrać użytkownika, dla którego ma zostać zdefiniowany profil mobilny z *Active Directory Users and Computers* (*Użytkownicy i komputery usługi Active Directory*). W jego właściwościach należy przejść do zakładki *Profile* (*Profil*).
4. W polu *Profile path* (*Ścieżka profilu*) należy zdefiniować ścieżkę do folderu udostępnionego, w którym będzie przechowywany profil użytkownika (rysunek 6.78). Dla przykładowego użytkownika o nazwie sieciowej *uczen01* wpisanie ścieżki *\\udział_sieciowy\home$\%username%* spowoduje utworzenie katalogu o nazwie *uczen01* w folderze *home* na serwerze, na którym są przechowywane profile użytkowników (rysunek 6.79). Udział sieciowy może być podany w postaci adresu IP lub nazwy domenowej, np.: 192.168.18.1 lub `helion.local`. Katalog dla danego użytkownika zostanie utworzony dopiero w momencie pierwszego logowania się tego użytkownika.

Rysunek 6.79. Ścieżka profilu mobilnego



ĆWICZENIA

1. Utwórz konto użytkownika mobilnego o nazwie *mobilny01* w jednostce organizacyjnej *mobilni* oraz określ miejsce przechowywania jego profilu.

PYTANIA

1. Z jakimi uprawnieniami należy stworzyć folder do przechowywania mobilnego profilu?
2. Wymień uprawnienia dla udostępnionych zasobów.
3. Co oznacza *$* na końcu nazwy udostępnionego folderu?
4. Czym się różni profil mobilny od lokalnego?

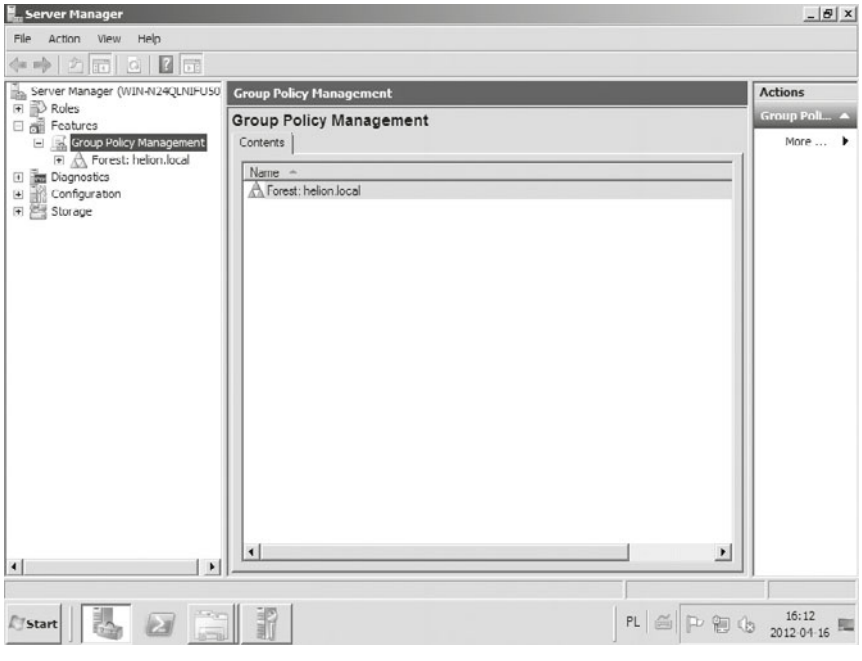
6.4.10. Zasady grup

W systemach Windows część parametrów systemu jest określana przez zasady grupy GPO (ang. *Group Policy Objects*). Zasady te dzielą się na parametry konfiguracyjne komputera oraz parametry konfiguracyjne użytkownika. Zasady dotyczące komputera są wprowadzane w czasie jego uruchomienia, zasady dotyczące użytkowników są wczytywane w trakcie logowania.

Ustawienia zasad grupy są przetwarzane w następującej kolejności:

- **lokalne zasady grupy,**
- **zasady grupy dla lokacji** — dotyczą obiektów połączonych z daną lokacją (przetwarzanie odbywa się synchronicznie i w kolejności określonej przez administratora),
- **zasady grupy dla domeny,**
- **zasady grupy dla jednostki organizacyjnej** — najpierw są przetwarzane obiekty połączone z jednostką organizacyjną znajdującą się najwyżej w hierarchii usługi Active Directory, następnie obiekty połączone z jej podrzędną jednostką organizacyjną, a na końcu obiekty powiązane z jednostką organizacyjną, do której należy dany użytkownik lub komputer.

Kontrolery domeny dostarczają mechanizm zarządzania zasadami grupy dla komputerów i użytkowników podłączanych do domeny. Jest on dostępny w narzędziu *Server Manager* (*Menedżer serwera*) w gałęzi *Features/Group Policy Management* (*Funkcje/Zarządzanie zasadami grupy*) (rysunek 6.80).

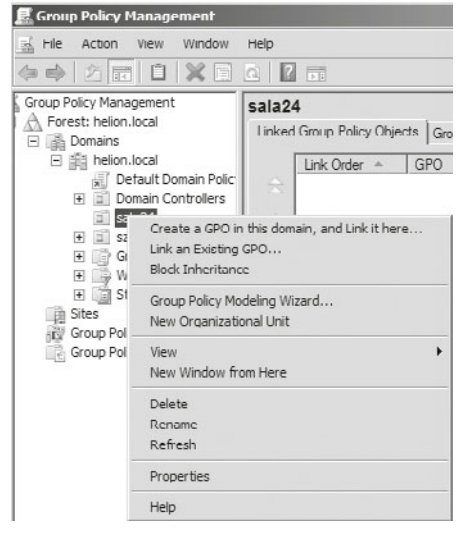


Rysunek 6.80. Zasady grup

Najważniejsze parametry ustawiane przez zasady grupy:

- *Computer Configuration* (*Konfiguracja komputera*):
  - *Software Settings* (*Ustawienia oprogramowania*) — przypisanie aplikacji — automatyczne zainstalowanie aplikacji przy starcie komputera, nie można jej usunąć z *Dodaj lub usuń programy*.
  - *Windows Settings* (*Ustawienia systemu Windows*) — zasady konta, zasady lokalne, dziennik zdarzeń, grupy z ograniczeniami, usługi systemowe, system plików, zasady zabezpieczeń IP.
  - *Administrative Templates* (*Szablony administracyjne*) — drukarki.
- *User Configuration* (*Konfiguracja użytkownika*):
  - *Software Settings* (*Ustawienia oprogramowania*) — opublikowanie — instalacja poprzez *Dodaj lub usuń programy* — oraz przypisanie aplikacji — tworzy skrót do instalacji w menu *Start*.
  - *Windows Settings* (*Ustawienia systemu Windows*) — przekierowanie folderu, Internet Explorer.
  - *Administrative Templates* (*Szablony administracyjne*) — menu *Start*, pasek zadań, Pulpit, Panel sterowania, foldery udostępnione.
- Pomocne narzędzia:
  - *rsop.msc* — wyświetla konsole wynikowego zestawu zasad aktualnie zalogowanego użytkownika i komputera.
  - `gpresult` — wyświetla informacje o zasadach grupy dla komputera i użytkownika w wierszu poleceń.
  - `gpupdate` — aktualizuje ustawienia zasad grupy.
  - `dcgpofix` — przywraca domyślne zasady grupy dla zasad domeny i dla kontrolerów domeny.
  - `ntfrsutl` — wyświetla informacje o kontrolerze domeny w wierszu poleceń.

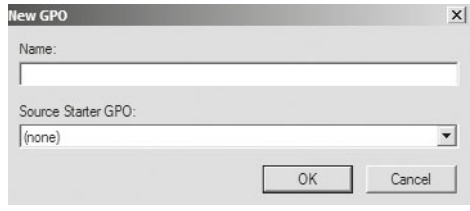
Żeby utworzyć nowy obiekt GPO, należy kliknąć prawym klawiszem myszy jednostkę organizacyjną, dla której chcemy go utworzyć, i wybrać tworzenie nowego GPO — *Create a GPO in this domain, and Link it here* (*Utwórz obiekt zasad grupy w tej domenie i umieść tu łącze*) (rysunek 6.81).



Rysunek 6.81. Tworzenie nowego obiektu GPO

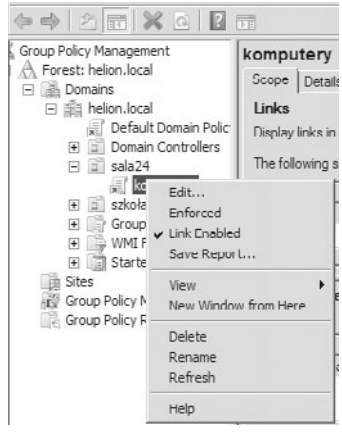
Nowo tworzonemu obiektowi GPO należy nadać nazwę (pole *Name* (*Nazwa*)), można go też powiązać z już istniejącym GPO (*Source Starter GPO* (*Źródłowy początkowy obiekt zasad grupy*)) (rysunek 6.82).

Rysunek 6.82. Nadawanie nazwy dla GPO oraz podłączenie do już istniejącego GPO



Gdy GPO zostanie utworzony, wówczas należy go edytować w celu zdefiniowania ustawień (rysunek 6.83).

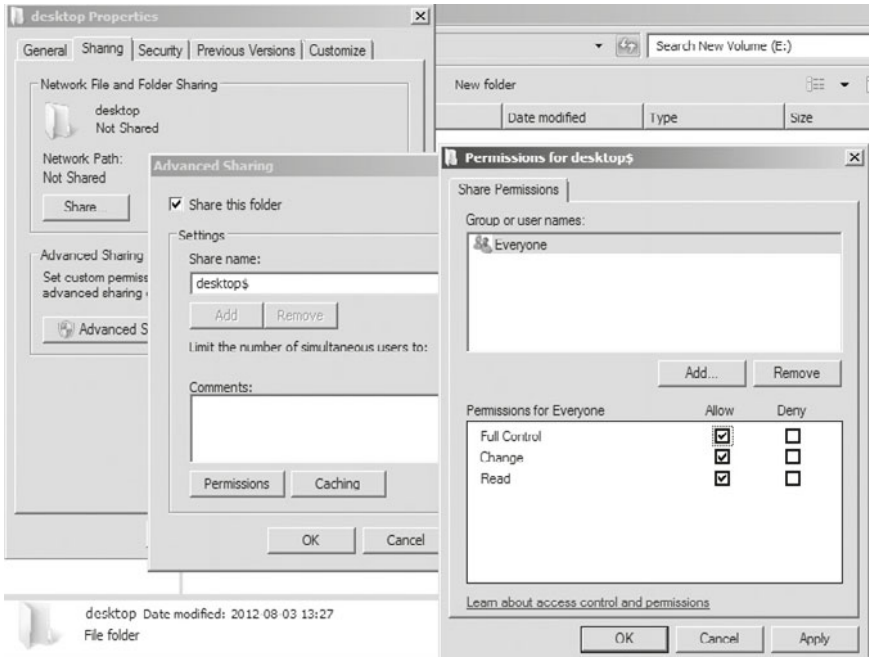
Rysunek 6.83. Edycja GPO



Zasady grupy mogą być wykorzystane w celu przekierowania folderów użytkownika w określone miejsce, np. na serwer, co pozwala zapewnić elastyczność mobilnym użytkownikom, a także scentralizować magazynowanie danych użytkowników (np. foldery *My Documents* (*Moje dokumenty*) czy *Desktop* (*Pulpit*)).

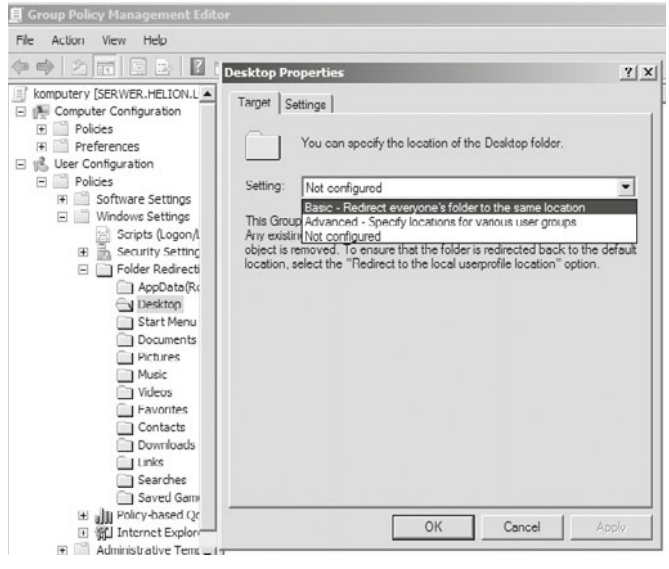
Opis przekierowania folderów został przedstawiony poniżej:

1. Tak jak w przypadku profilu mobilnego, należy najpierw utworzyć foldery, do których zostaną przekierowane foldery użytkowników (rysunek 6.84).
2. Wybranie opcji *User configuration/Policies*/*Windows Settings* (*Konfiguracja użytkownika/Zasady/Ustawienia systemu Windows*) w części *Folder redirection/Desktop* (*Przekierowanie folderu/Pulpit*) umożliwia przekierowanie folderu przechowującego pliki z pulpitu (rysunek 6.85).

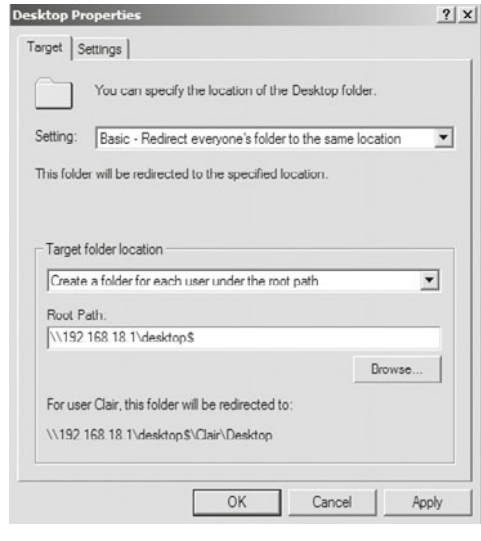


Rysunek 6.84. Tworzenie folderu, do którego będzie przekierowany pulpit użytkownika

Rysunek 6.85. Położenie gałęzi Przekierowanie folderu w GPO



3. Konfiguracja przekierowania folderu wymaga ustawienia we właściwościach wybranego katalogu stosownych opcji. W celu ich skonfigurowania należy wybrać opcję *Properties* (*Właściwości*) z menu kontekstowego. Zakładka *Target* (*Miejsce docelowe*) służy do określenia sposobu konfiguracji:
   - *Basic — Redirect everyone's folder to the same location* (*Podstawowy — Przekieruj wszystkie foldery do tej samej lokalizacji*).
   - *Advanced — Specify locations for various user groups* (*Zaawansowane — Określaj lokalizacje dla różnych grup użytkowników*).
   - *Not configured* (*Nie skonfigurowano*).
   - Dostępna może być też opcja *Follow the Documents* (*Przejdź do folderu Dokumenty*) związana z katalogami: *Pictures* (*Obrazy*), *Music* (*Muzyka*), *Videos* (*Wideo*). Zapewnia ona kompatybilność ze wcześniejszymi wersjami systemów operacyjnych, w których wymienione powyżej katalogi były podkatalogami katalogu *My Documents* (*Moje dokumenty*).
4. Po wybraniu opcji konfiguracji należy zdefiniować *Target folder location* (*Lokalizacja folderu docelowego*). Można wybrać jedną z trzech opcji:
   - *Create a folder for each user under the root path* (*Utwórz folder dla każdego użytkownika w ścieżce katalogu głównego*). Po wybraniu tej opcji należy w polu *Root Path* (*Ścieżka katalogu głównego*) wpisać lokalizację. W tym celu wystarczy skorzystać ze ścieżki UNC (ang. *Universal Naming Convention*), np.: `\\udział_sieciowy\desktop$\%username%` (rysunek 6.86).
   - *Redirect to the following location* (*Przekieruj do następującej lokalizacji*).
   - *Redirect to the local userprofile location* (*Przekieruj do lokalnej lokalizacji profilu użytkownika*).



Rysunek 6.86. Konfiguracja podstawowa przekierowania folderu ze ścieżką UNC

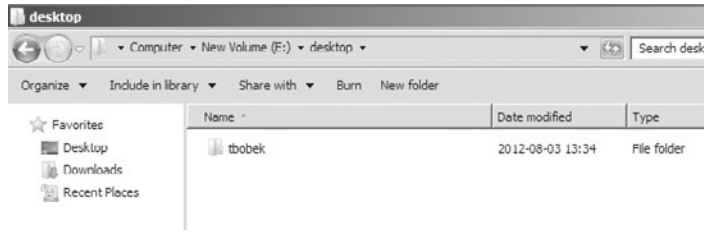
WAŻNE

W ścieżce UNC można używać następujących zmiennych środowiskowych:

- `%username%`
- `%userprofile%`
- `%homeshare%`
- `%homepath%`

5. Po zalogowaniu się użytkownika znajdującego się w jednostce organizacyjnej, dla której zdefiniowano GPO, na serwerze w folderze udostępnionym *Desktop* (*Pulpit*) powinien się pojawić katalog o nazwie zalogowanego użytkownika (rysunek 6.87). Przekierowania innych folderów przeprowadza się analogicznie.

Rysunek 6.87. Przykładowa struktura zasobu przechowującego foldery przekierowane



6. Konfiguracja zaawansowana folderów przekierowanych (rysunek 6.88) umożliwia przypisanie różnych lokalizacji przekierowania w zależności od przynależności użytkownika do grupy (*Advanced — Specify locations for various user groups* (*Zaawansowane — Określaj lokalizacje dla różnych grup użytkowników*)). Jest to jednocześnie sposób zagnieżdżenia zarządzania mechanizmu przekierowania folderów wykonywanego za pomocą różnych GPO.

Rysunek 6.88. Tryb zaawansowanej konfiguracji folderów przekierowanych

Na rysunku przedstawiono konfigurację dla grupy *klasa1*, w której katalogi członków grupy zostaną przekierowane do katalogów w lokalizacji `\\192.168.18.1\desktop$\%Username%\Desktop` lub `\\serwer\desktop$\%Username%\Desktop`.

W ramach przekierowania folderów możliwe jest skonfigurowanie aż 13 folderów:

- *AppData* (*Roaming*),
- *Desktop* (*Pulpit*),
- *Start Menu* (*Menu Start*),
- *Documents* (*Dokumenty*),
- *Pictures* (*Obrazy*),
- *Music* (*Muzyka*),
- *Videos* (*Wideo*),
- *Favorites* (*Ulubione*),
- *Contacts* (*Kontakty*),
- *Downloads* (*Pobieranie*),
- *Links* (*Łącza*),
- *Searches* (*Wyszukiwania*),
- *Saved Games* (*Zapisane gry*).

ĆWICZENIA

1. Wykonaj następujące zadania:
   a. Utwórz jednostki organizacyjne: *grupa_A* i *grupa_B*, *mobilni*.
   b. Stwórz w każdej jednostce organizacyjnej grupę zabezpieczającą o nazwach odpowiednio: *grupa_A* i *grupa_B*, *mobilni*.
   c. W każdej jednostce organizacyjnej utwórz po jednym użytkowniku, a następnie przypisz ich do grup.
   d. Stwórz dla każdej z jednostek nowe GPO nazwane tak samo jak jednostki organizacyjne.
   e. Zdefiniuj przekierowanie folderów: *Pulpit*, *Moje dokumenty*.

PYTANIA

1. Co to jest profil użytkownika?
2. Co to jest GPO?
3. Jaka zmienna środowiskowa przechowuje nazwę użytkownika?
4. Jakie polecenie aktualizuje GPO?

6.5. Usługi sieciowe

6.5.1. DNS

Usługa DNS (ang. *Domain Name System*) to hierarchiczna, rozproszona baza danych, zawierająca odwzorowanie nazw domenowych na adresy IP. System DNS umożliwia lokalizowanie komputerów i usług na podstawie nazw przyjaznych dla użytkownika, a także odnajdowanie innych informacji przechowywanych w bazie danych. Jest integralną częścią usługi Active Directory, gdzie podstawowym zadaniem jest rozwiązywanie nazw obiektów w ramach domeny.

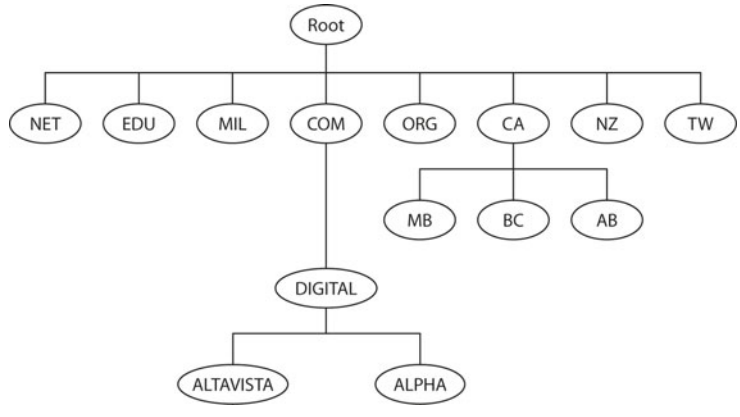
DNS jest usługą, która musi być zainstalowana przed instalacją usługi katalogowej (*Active Directory*) lub w trakcie tej instalacji. Jednym z wymogów, jakie należy spełnić przed instalacją usługi, jest zdefiniowanie dla interfejsu prywatnego (sieci lokalnej) statycznego adresu IP.

Przestrzeń nazw DNS-u

Przestrzeń nazw domen jest drzewiastą strukturą obejmującą wszystkie istniejące domeny (rysunek 6.89). Początkiem drzewa jest domena określana angielskim terminem *root*, czyli korzeń.

Rysunek 6.89. Struktura DNS

Źródło: B. Komar, *TCP/IP dla każdego*, Gliwice: Helion, 2002, s. 137



W odróżnieniu od pozostałych domen, domenie root nie odpowiada żadna występująca w nazwach stacji etykieta. Do jej określenia stosuje się czasem znak kropki (.).

Poniżej domeny root znajdują się domeny pierwszego poziomu. Są one dwojakiego rodzaju: pierwsza grupa odpowiada typom działalności korzystających z nich organizacji, druga stosuje dwuliterowe oznaczenia krajów, w których znajdują się poszczególne organizacje.

Informacje na temat domen najwyższego poziomu można znaleźć pod adresem organizacji IANA — Internet Assigned Numbers Authority — *http://www.iana.org/domains/root/db/*. Najczęściej wykorzystywane zostały przedstawione poniżej:

- *com* — organizacje komercyjne,
- *edu* — instytucje edukacyjne,
- *org* — organizacje niekomercyjne,
- *net* — organizacje związane z siecią,
- *gov* — pozamilitarne organizacje rządowe,
- *mil* — wojskowe organizacje rządowe,
- *num* — numery telefonów,
- *arpa* — domeny wyszukiwania odwrotnego,
- *??* — dwuliterowe kody krajów (np. *pl* dla Polski).

DNS stosuje hierarchiczną metodę rozwiązywania nazw, w której zapytanie o nazwę jest przekazywane w górę i w dół bazy z nazwami domenowymi, którym odpowiadają adresy IP, dopóki nie zostanie znaleziony poszukiwany rekord. Poszczególne poziomy hierarchii są oddzielone od siebie kropkami określającymi podział. Pełna złożona nazwa domeny (FQDN, ang. *Fully Qualified Domain Name*) w sposób jednoznaczny identyfikuje miejsce zasobu w hierarchii DNS, np. serwer.helion.local. Podstawowym typem serwerów DNS są serwery główne. Z praktycznego punktu widzenia każdy serwer przechowujący dane źródłowe dotyczące rekordów jest traktowany jako serwer główny dla danego poziomu w hierarchii nazw domenowych. Wśród tego typu serwerów szczególną funkcję pełnią tzw. „root serwery", czyli serwery przechowujące informacje o serwerach głównych, obsługujących domeny pierwszego poziomu. Ze względu na dość specyficzną rolę, która ma krytyczne znaczenie dla sprawnego działania całego systemu nazw w Internecie, serwery te realizują tylko i wyłącznie tę jedną funkcję. Wszystkie inne serwery DNS muszą znać adresy „root serwerów", co jest podstawowym warunkiem umożliwiającym rozwiązanie wszystkich poprawnych nazw. Domyślnie usługa serwera DNS pobiera informacje dotyczące serwerów głównych (ang. *root hints*) przy użyciu pliku *Cache.dns*, który jest przechowywany w folderze *%systemroot%\System32\Dns* na serwerze. Ten plik zawiera zazwyczaj rekord zasobu serwera nazw (NS) i rekord zasobu hosta (A) dla internetowych serwerów głównych. Jeśli jednak usługa serwera DNS jest używana w sieci prywatnej, można edytować ten plik lub zastąpić go podobnymi rekordami, które będą wskazywać wewnętrzne serwery główne DNS.

Serwery przekazujące (ang. *forwarders*) są serwerami nazw obsługującymi wszystkie zapytania klienta, których zadaniem jest przekazywanie ich do serwerów znajdujących się poziom wyżej w hierarchii.

Strefy DNS

Strefa w usłudze DNS oznacza część przestrzeni nazw kontrolowanych przez określony serwer DNS lub grupę serwerów.

- Strefa wyszukiwania do przodu służy do rozwiązywania nazw domenowych na adresy IP. Jeżeli użytkownik będzie chciał sprawdzić adres serwera, na który wskazuje dana domena, np. helion.local, otrzyma zwrotnie adres IP, np. 192.168.18.1.

- Strefa wyszukiwania wstecznego działa dokładnie na odwrót, czyli przypisuje nazwę domenową do konkretnego adresu IP. Przypomina to sytuację, gdy znamy numer telefonu, ale nie znamy nazwiska właściciela. Strefy wyszukiwania wstecznego musimy tworzyć ręcznie, np. 192.168.18.1 na serwer.helion.local.

Czas życia (TTL)

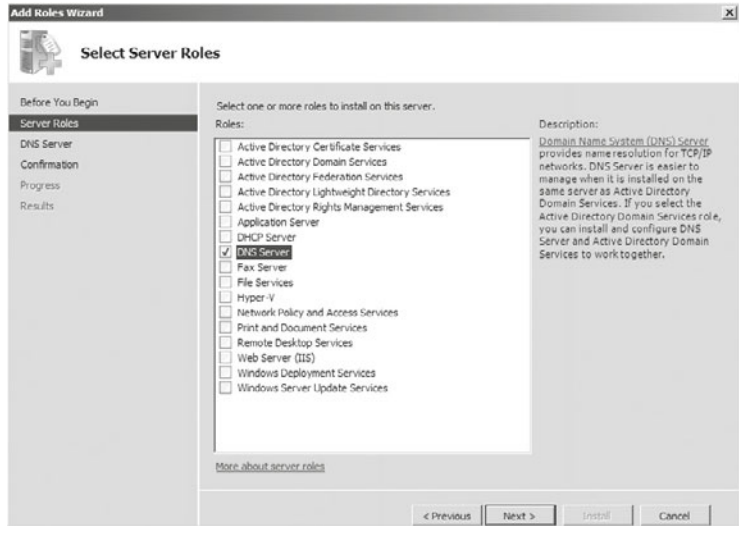
Wartość czasu życia (*TTL — Time To Live*) oznacza dla rekordu zasobów czas w sekundach, przez jaki serwer nazw będzie przetrzymywać w pamięci podręcznej odpowiedź na żądanie, zanim zażąda jej ponownie od serwera nazw.

Diagnostyka DNS

W celu diagnostyki problemów dotyczących serwera DNS należy zajrzeć do Podglądu zdarzeń (ang. *Event Viewer*). Aby uzyskać bardziej zaawansowaną diagnostykę dziennika zdarzeń, można włączyć rejestrację uruchomieniową (ang. *Debug Logging*) dla poszczególnych serwerów. Możliwe jest też monitorowanie serwera DNS za pomocą monitora niezawodności i wydajności, które pozwalają monitorować wiele ważnych liczników związanych z zapytaniami, transferami sfer czy wykorzystaniem pamięci.

Instalacja usługi

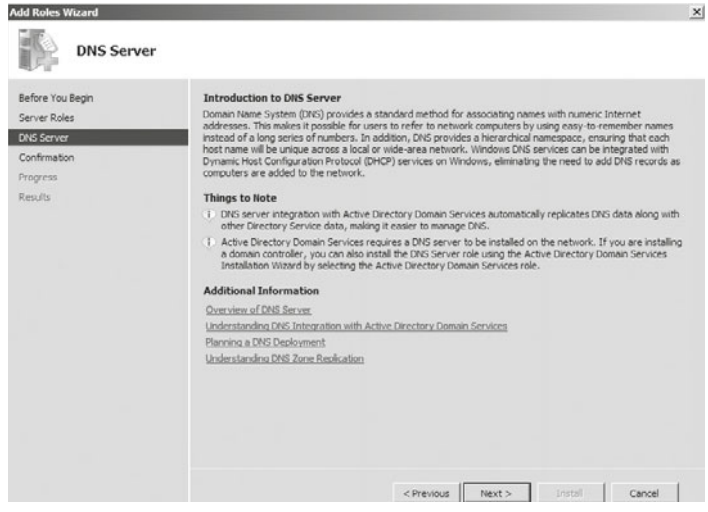
1. Usługa DNS jest niezbędna do rozwiązywania nazw w domenie, dlatego powinna zostać zainstalowana przed instalacją roli usługi katalogowej. Jeżeli tego nie zrobimy, to kreator instalacji usługi katalogowej AD uczyni to za nas.
2. Tak jak wszystkie usługi w ramach serwera, ta również jest osobną rolą, którą należy wybrać do instalacji (rysunek 6.90).



Rysunek 6.90. Instalacja usługi DNS

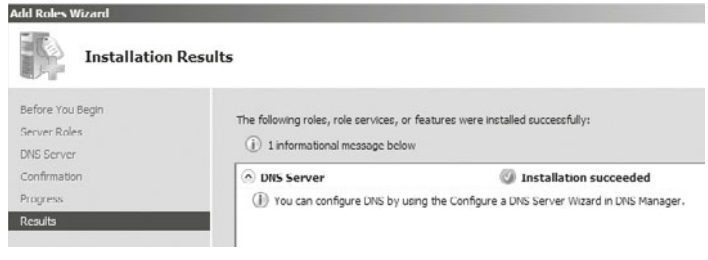
3. W kolejnym oknie pojawia się informacja o usłudze. W następnym oknie należy zaakceptować instalację (*Install* (*Zainstaluj*)) (rysunek 6.91).

Rysunek 6.91. Informacje na temat instalowanej usługi



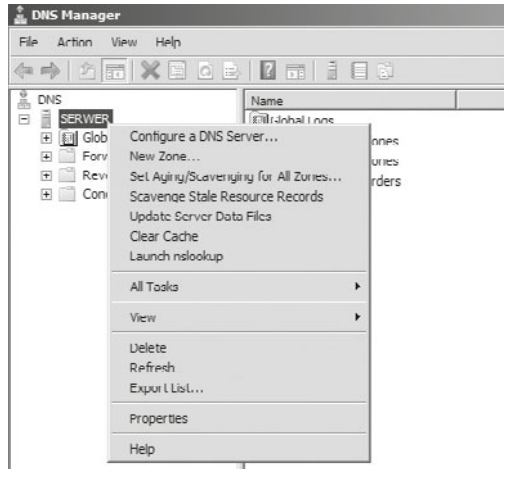
4. Jeżeli instalacja przebiegła pomyślnie, wyświetla się odpowiedni komunikat (*succeeded* (*Instalacja powiodła się*)) (rysunek 6.92).

Rysunek 6.92. Instalacja zakończona pomyślnie



5. Po zainstalowaniu ustawienia usługi są dostępne w narzędziu *DNS Manager* (*Menedżer DNS*) (rysunek 6.93). Usługę należy skonfigurować przez kliknięcie serwera prawym klawiszem myszy i wybranie opcji *Configure a DNS Server* (*Kreator konfigurowania serwera DNS*).

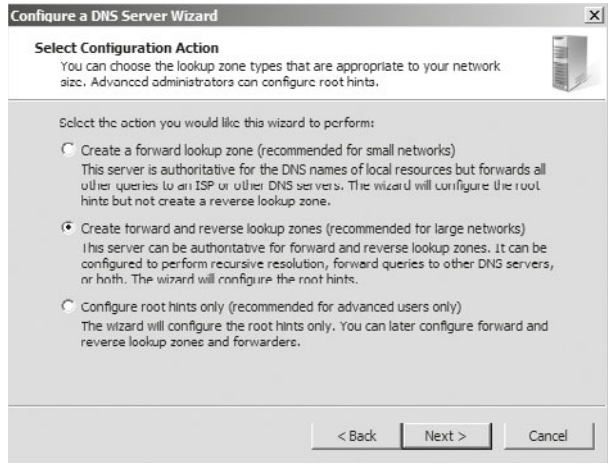
Rysunek 6.93. Menedżer DNS



6. Zostanie uruchomiony Kreator konfigurowania serwera DNS (rysunek 6.94), w którym są do wyboru trzy opcje:

- *Create a forward lookup zone* (*Utwórz strefę wyszukiwania do przodu*) — zalecane dla małych sieci. Jest to serwer, który tłumaczy nazwy w ramach domeny na adresy IP.
- *Create forward and reverse lookup zones* (*Utwórz strefę wyszukiwania do przodu i wyszukiwania wstecznego*) — zalecane dla dużych sieci. Serwer odpowiedzi dla przeszukiwania strefy do przodu i wstecznego. W ramach tej opcji jest konfigurowany *Root hints*. Jest to główny plik, który zawiera listę adresów IP serwerów DNS uważanych za wiarygodne na poziomie korzenia hierarchii DNS (znany również jako serwer nazw głównych).
- *Configure root hints only* (*Skonfiguruj tylko wskazówki dotyczące serwerów głównych*) — zalecane dla zaawansowanych użytkowników. Kreator konfiguruje tylko wskazówki dotyczące serwerów głównych. Strefy przeszukiwania są konfigurowane później.

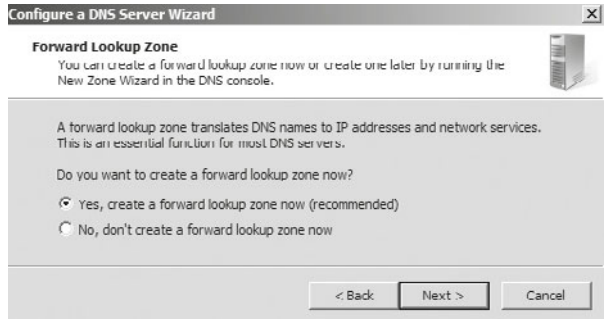
Rysunek 6.94. Kreator tworzenia strefy przeszukiwania



W celu skonfigurowania domeny lokalnej na potrzeby usługi Active Directory należy wybrać drugą opcję.

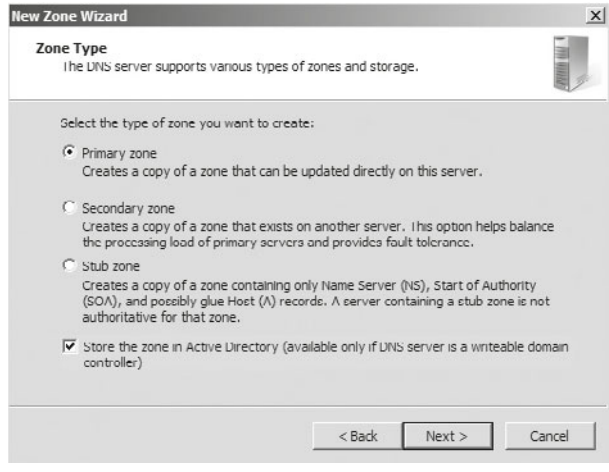
7. W kolejnym oknie kreatora (rysunek 6.95) należy potwierdzić utworzenie strefy wyszukiwania do przodu (ang. *foward lookup zone*).

Rysunek 6.95. Kreator tworzenia strefy wyszukiwania



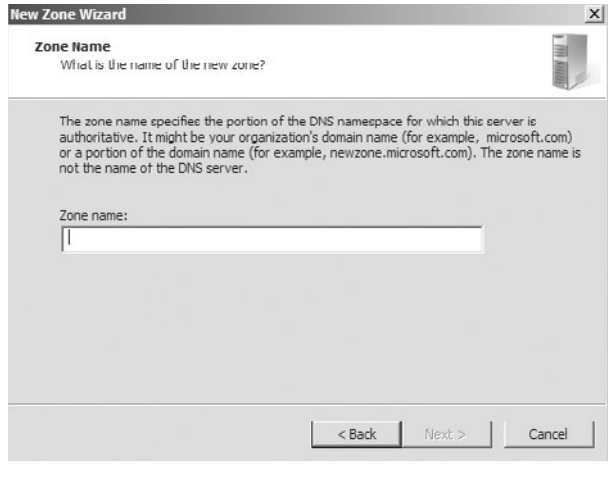
8. W kolejnym oknie kreatora (rysunek 6.96) należy wybrać typ strefy — w tym przypadku *Primary zone* (*Strefa podstawowa*) — i przejść do dalszego okna konfiguracji. Jeżeli ten serwer jest kontrolerem domeny, to trzeba również zaznaczyć opcję *Store the zone in Active Directory* (*Przechowuj strefę w usłudze katalogowej AD*).

Rysunek 6.96. Kreator dodawania strefy wyszukiwania



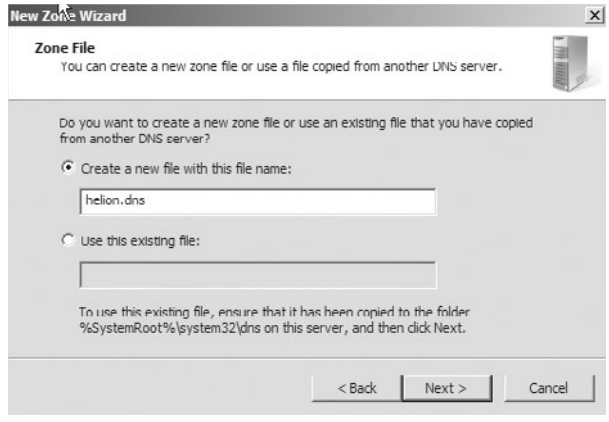
9. W kolejnym oknie kreatora (rysunek 6.97) należy nadać nazwę dla nowej strefy DNS. Jeśli serwer DNS będzie wykorzystywany dla celów usługi Active Directory, trzeba nazwę domeny zakończyć przyrostkiem *local* (np. *helion.local*), który odróżnia ją od nazw domen internetowych.

Rysunek 6.97. Kreator nadawania nazwy dla nowej strefy, np. helion



10. W kolejnym etapie można utworzyć nowy plik strefy lub zaimportować strefy z istniejącego pliku (rysunek 6.98). Jeśli plik nie został wcześniej utworzony, należy wybrać opcję *Create a new file with this file name* (*Utwórz nowy plik o tej nazwie*) i zaakceptować domyślną nazwę.

Rysunek 6.98. Kreator tworzenia pliku dla nowej strefy

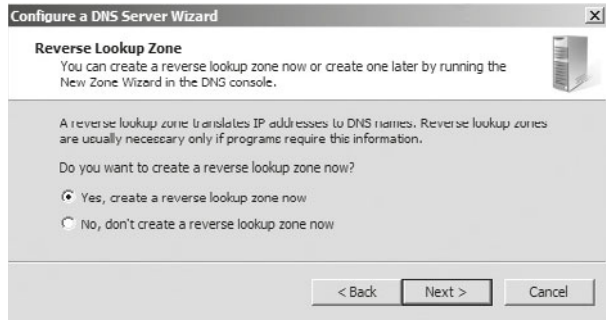


11. Kolejne okno kreatora pozwala zdefiniować aktualizacje dynamiczne:

- *Allow only secure dynamic updates* (*Zezwalaj tylko na zabezpieczone aktualizacje dynamiczne*). Jeśli strefa jest zintegrowana z usługą katalogową AD, można się posłużyć listami kontroli dostępu w celu określenia, którzy klienci mogą dokonywać aktualizacji dynamicznych.
- *Allow both nonsecure and secure dynamic updates* (*Zezwalaj na zabezpieczone oraz niezabezpieczone aktualizacje dynamiczne*). Ta opcja umożliwia dynamiczne aktualizacje wszystkim klientom, bez względu na to, czy są oni uwierzytelniani, czy też nie.
- *Do not allow dynamic updates* (*Nie zezwalaj na aktualizacje dynamiczne*). Wybranie tej opcji wyłącza aktualizacje dynamiczne. Należy jej użyć, jeśli strefa nie jest zintegrowana z usługą katalogową AD.

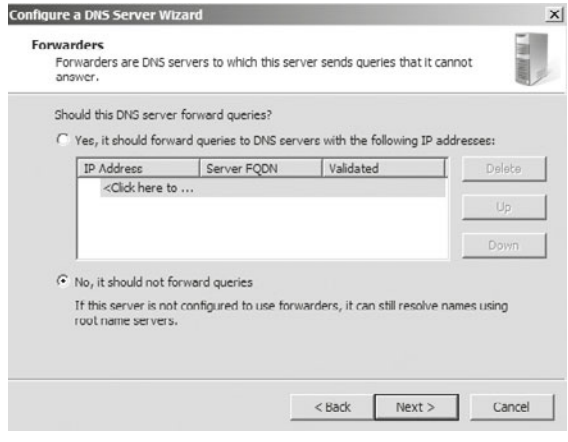
12. W kolejnym kroku (rysunek 6.99) można zdefiniować strefę wyszukiwania wstecznego (ang. *reverse lookup zone*) — zadaniem tej strefy jest zamiana adresów IP na adresy domenowe, np.: 192.168.18.1 na serwer.helion.local. Po wybraniu opcji tworzenia strefy wyszukiwania wstecznego trzeba określić informacje takie jak w kroku 8., tylko dotyczące wyszukiwania wstecznego. Należy również podać adres sieci dla wyszukiwania wstecznego, np. 18.168.192.in-addr.arpa.

Rysunek 6.99. Kreator tworzenia strefy wyszukiwania wstecznego



13. W oknie *Forwardes* (*Usługi przesyłania dalej*) (rysunek 6.100) istnieje możliwość ustawienia przekazywania zapytań do pozostałych serwerów DNS. Wybranie tej konfiguracji powoduje przesyłanie dalej wszystkich kwerend DNS dla nazw DNS spoza sieci do serwera DNS obsługiwanego przez usługodawcę internetowego lub centralę. Jeżeli nie chcemy, aby zapytania były przekazywane dalej, należy wybrać drugą opcję.

Rysunek 6.100. Kreator przesyłania zapytań dalej



14. Ostatnie okno (rysunek 6.101) wyświetla podsumowanie konfiguracji.

Rysunek 6.101. Podsumowanie

W ramach DNS-u obiekty są identyfikowane za pomocą rekordów zasobów (rysunek 6.101).

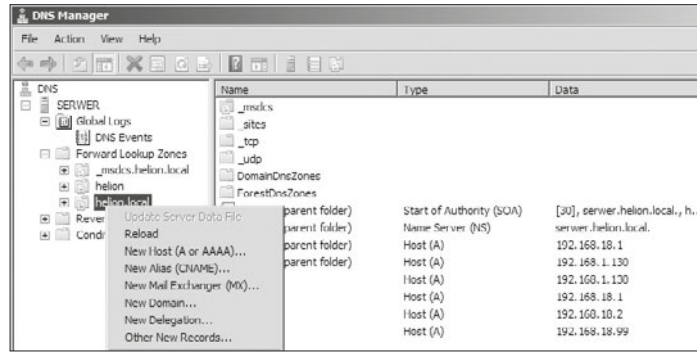
Najczęściej używanymi rekordami zasobów są:

- *Host* (*A*) — odwzorowuje nazwy domeny DNS na adres IPv4.
- *Host* (*AAAA*) — odwzorowuje nazwy domeny na adres IPv6.
- *Alias* (*CNAME*) — służy do mapowania nazwy aliasu domeny DNS na inną nazwę podstawową lub kanoniczną.

- *Rekord wymiany poczty* (*MX*) — służy do mapowania nazwy domeny DNS na adres serwera, który wymienia lub przesyła dalej pocztę elektroniczną z danej domeny.
- *Wskaźnik* (*PTR*) — służy do mapowania wstecznej nazwy domeny DNS na adres IP komputera, który wskazuje nazwę do przodu domeny DNS tego komputera.
- *Lokalizacja usługi* (*SRV*) — służy do mapowania nazwy domeny DNS na określoną listę komputerów DNS, które oferują określony typ usługi, na przykład na kontrolery domen usługi katalogowej AD.

W celu dodania nowego rekordu typu A dla stacji roboczej XP należy kliknąć prawym klawiszem myszy daną domenę i dodać nowy rekord (rysunek 6.102).

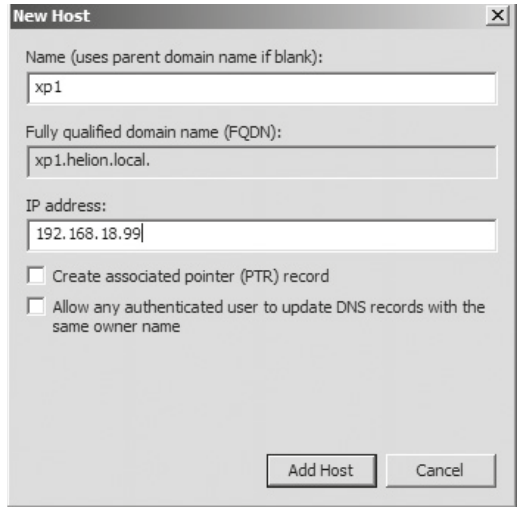
Rysunek 6.102. Dodawanie nowego rekordu



Poprawna konfiguracja rekordu obejmuje takie informacje, jak (rysunek 6.103):

- *Name* (*Nazwa*), np. xp1,
- *IP address* (*Adres IP*), np. 192.168.18.99.

Rysunek 6.103. Dodawanie nowego rekordu do DNS-u



Narzędzia związane z DNS-em:

- `nslookup` — pozwala sprawdzić, jaki jest domyślny serwer DNS dla danej domeny.
- `ipconfig` — umożliwia konfigurowanie interfejsów sieciowych. Dla DNS-u są wykorzystywane poniższe opcje:
  - `ipconfig /flushdns` — czyści bufor programu rozpoznającego nazwy DNS;
  - `ipconfig /registerdns` — wymusza ponowne zarejestrowanie się klienta w DNS-ie;
  - `ipconfig /displaydns` — wyświetla zawartość pamięci podręcznej, w której są zapisane tłumaczenia DNS – IP.
- `tracert` — wyświetla serię routerów IP, które są używane przy dostarczaniu pakietów z danego komputera do miejsca docelowego, a także czas trwania każdego przeskoku.

ĆWICZENIA

1. Sprawdź strefy wyszukiwania do przodu i wyszukiwania wstecznego w usłudze DNS, która jest zdefiniowana dla usługi katalogowej.
2. Dodaj nowe rekordy w DNS-ie z adresami IP stacji roboczej z Windows 7 i Windows XP.
3. Sprawdź działanie narzędzi związanych z usługą DNS.

PYTANIA

1. Podaj definicję usługi DNS.
2. Podaj nazwę polecenia, które umożliwia wyczyszczenie bufora DNS.
3. Wymień rekordy DNS.
4. Podaj nazwę polecenia, które wyświetla serię routerów IP używanych przy dostarczaniu pakietów.
5. Podaj nazwę domeny, która określa organizację.

6.5.2. DHCP

DEFINICJA

Usługa DHCP wykorzystuje protokół dynamicznej konfiguracji hosta (ang. *Dynamic Host Configuration Protocol — DHCP*) w celu automatycznego przekazywania klientom danych konfiguracyjnych sieci, adresu IP, maski, bramy, serwera DNS i innych.

Najważniejsze funkcje usługi:

- Pozyskiwanie przez klientów DHCP adresacji IP na określony czas, po upływie którego jest wysyłane żądanie odświeżenia i adres jest automatycznie odnawiany.
- Rezerwacja adresów IP dla specyficznych komputerów lub urządzeń w sieci. Pozwala to na przypisanie adresowi fizycznemu (MAC) konkretnego adresu IP.
- Dodawanie wykluczeń, czyli wyodrębnianie adresów IP lub zakresów adresów IP z puli DHCP dla urządzeń lub serwerów, które wymagają statycznego adresowania.
- Integracja serwera DHCP z serwerem DNS.
- Obsługa adresów IPv6.

Proces pobierania adresu z serwera polega na wymianie odpowiednich sygnałów (rysunek 6.104).

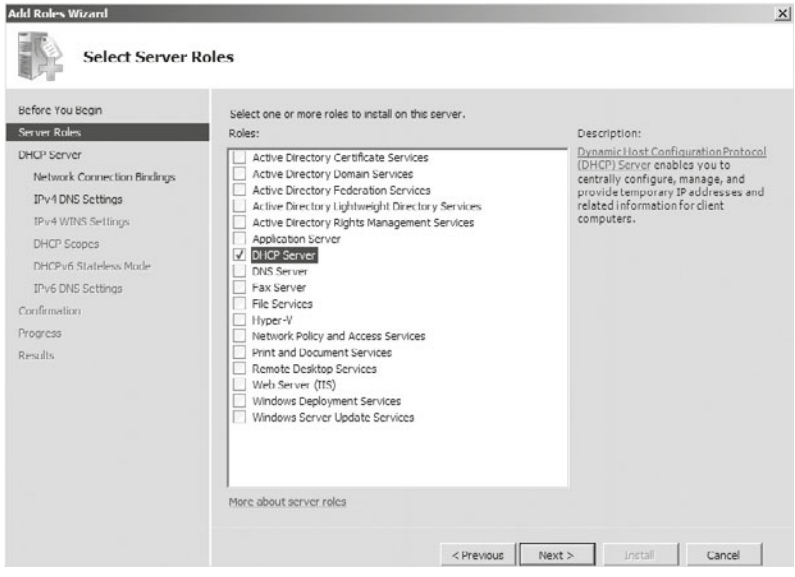
Rysunek 6.104. Wymiana sygnałów między klientem i serwerem

W celu uzyskania adresu klient DHCP wysyła na adres rozgłoszeniowy specjalną wiadomość zwaną `DHCPDISCOVER`. Serwer po otrzymaniu zapytania sprawdza swoją wewnętrzną bazę i odpowiada wiadomością zwaną `DHCPOFFER`, która zawiera dostępny adres IP. Klient po otrzymaniu pakietów DHCPOFFER wysyła `DHCPREQUEST` do serwera. Serwer po otrzymaniu `DHCPREQUEST` oznacza adres IP jako „używany".

Kolejne kroki przedstawiają sposób instalacji usługi DHCP na serwerze 2008.

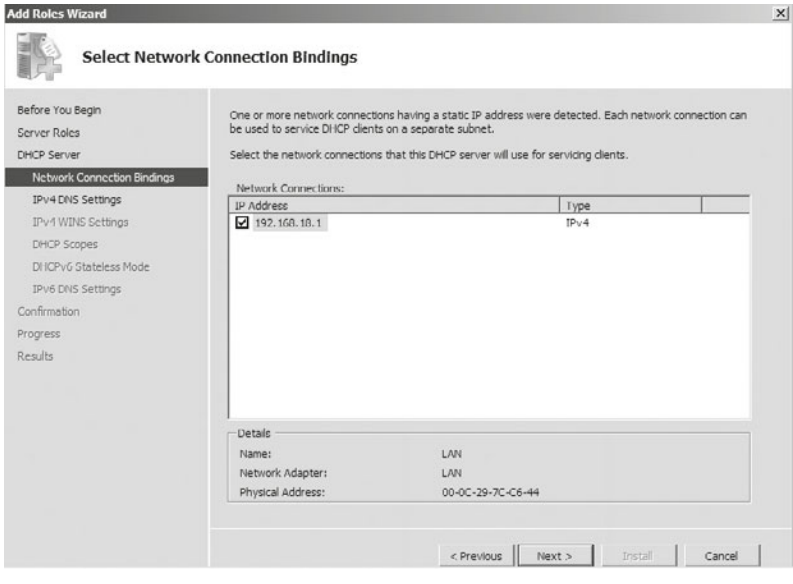
1. Tak jak usługa DNS, usługa DHCP wymaga statycznego adresu IP na maszynie, na której ma być uruchomiona.

2. Instalacja usługi DHCP wymaga dodania nowej roli do serwera 2008 R2. W tym celu należy uruchomić *Server Manager* (*Menedżer serwera*) i dodać rolę (rysunek 6.105).



Rysunek 6.105. Kreator dodawania nowej roli

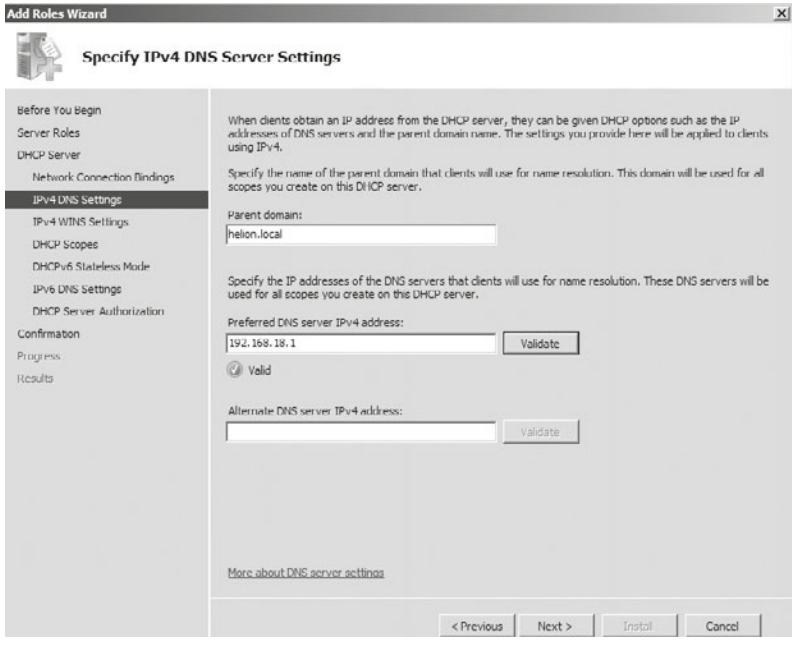
3. W kolejnym kroku trzeba określić interfejs karty sieciowej, do której będzie przypisana usługa. Zawsze powinna być przypisana do karty sieciowej, na której ma być aktywna. Ważne jest, by wiedzieć, jaki to jest adres IP oraz nazwa (rysunek 6.106).



Rysunek 6.106. Okno wyboru interfejsu

4. W kolejnym oknie można przekazać informację o konfiguracji serwera DNS. Te dane będą przekazywane stacjom roboczym razem z adresem IP (rysunek 6.107). Informacje, jakie należy mieć, to:
   - Nazwa domeny nadrzędnej (powinna zostać wykryta automatycznie).
   - Preferowany adres IPv4 — jeżeli nie istnieje lokalny serwer DNS, automatycznie zostanie pobrany adres serwera DNS dostawcy usługi internetowej.
   - Alternatywny adres IPv4 jest opcją dodatkową.

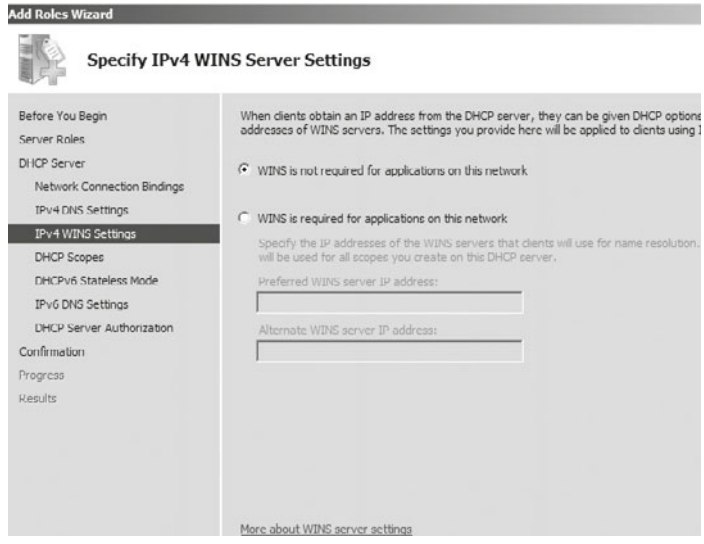
Wprowadzone adresy IP podlegają *weryfikacji* (ang. *validate*). Jeżeli weryfikacja przebiegnie pomyślnie, poniżej pola adresu pojawi się zielona ikona — symbol zaznaczenia. W przeciwnym razie zostanie wyświetlona czerwona ikona x.



Rysunek 6.107. Okno konfiguracji serwera DNS

5. W kolejnym oknie kreatora instalacji należy dodać ustawienia dotyczące usługi WINS, która jest następną usługą umożliwiającą rozwiązywanie nazw w sieci. Jeśli jest ona wymagana, należy wprowadzić jej adres IP (rysunek 6.108).

Rysunek 6.108.
Ustawienia usługi WINS

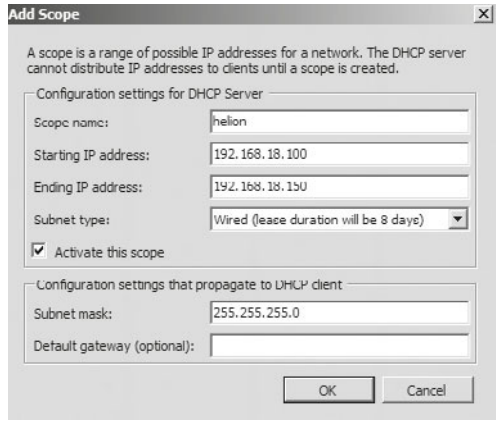


6. Teraz należy zdefiniować zakres adresów (pulę adresów). Trzeba nadać nazwę dla zakresu oraz pierwszy i ostatni adres, aktywować zakres i ustalić maskę podsieci, można również opcjonalnie podać adres bramy domyślnej (ang. *default gateway*) (rysunek 6.109). Należy również określić typ podsieci (*Subnet type* (*Typ podsieci*)), który określa czas trwania dzierżawy. Do wyboru mamy:

a. *Wireless* (*Bezprzewodowa*).

b. *Wired* (*Przewodowa*).

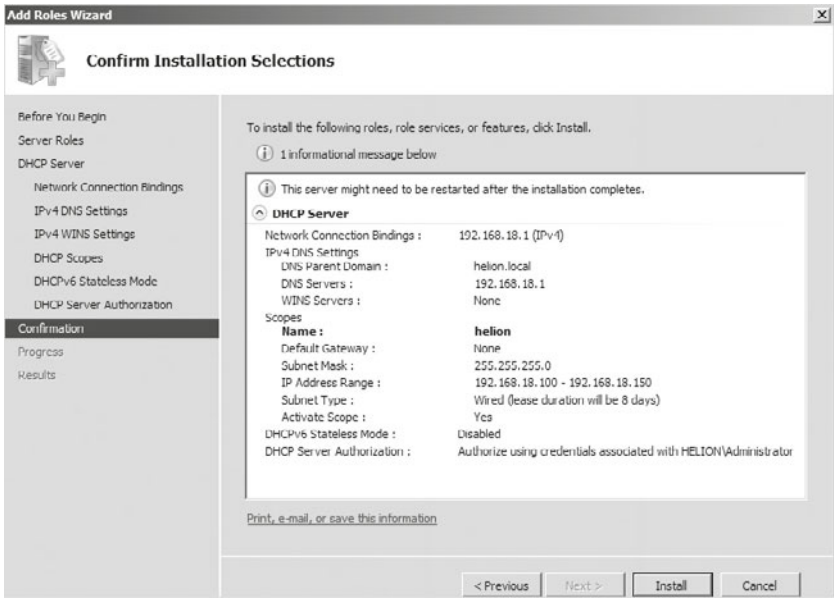
Rysunek 6.109.
Okno definiowania zakresów



7. W oknie *Configure DHCPv6 Stateless Mode for this server* (*Konfigurowanie trybu bezstanowego protokołu DHCPv6*) są dostępne dwie opcje. Jeżeli jest wymagany tryb bezstanowy, należy włączyć możliwość przydzielania adresów IPv6 *Enable DHCPv6 stateless mode for this Server* (*Włącz tryb bezstanowy protokołu DHCPv6 dla tego serwera*). W przeciwnym przypadku trzeba zaznaczyć opcję *Disable DHCPv6 Stateless Mode for this Server* (*Wyłącz tryb bezstanowy protokołu DHCPv6 dla tego serwera*).

Jeżeli wybrano drugą opcję, można skonfigurować ustawienia dotyczące DHCPv6 później, w narzędziu do zarządzania serwerem DHCP.

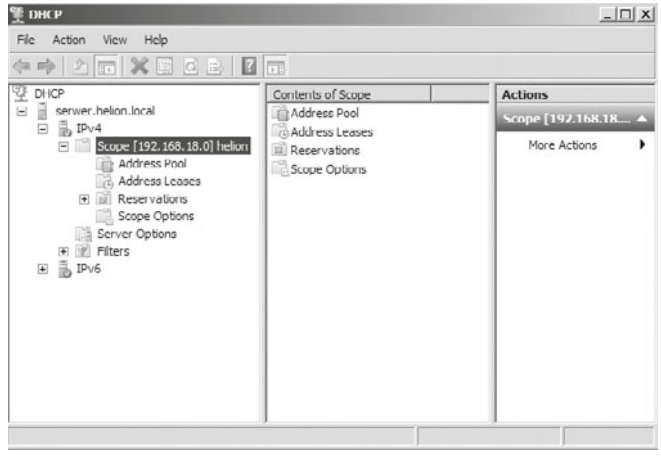
8. W kolejnym kroku *DHCP Server Authorization* (*Autoryzowanie serwera DHCP*) należy podać konto, które posłuży do autoryzowania serwera DHCP.
9. Ostatni krok procesu instalacji nowej roli to sekcja *Confirm Installation Selections* (*Potwierdzenie opcji instalacji*) (rysunek 6.110). Należy sprawdzić, czy konfiguracja jest poprawna, i wybrać *Install* (*Instaluj*).



Rysunek 6.110. Okno instalacji usługi

Do zarządzania mamy przystawkę *dhcpmgmt.msc* (rysunek 6.111) znajdującą się w *Administrative Tools* (*Narzędzia administracyjne*).

Rysunek 6.111. Okno zarządzania usługą

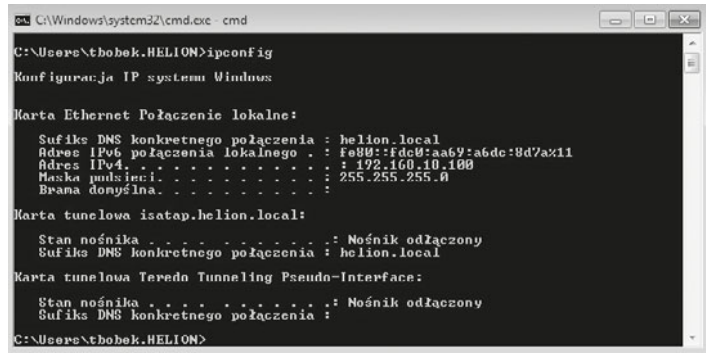


Po skonfigurowaniu serwera i zakresu adresów należy sprawdzić, czy stacje robocze się z nimi dogadują i czy pobierają od serwera informacje zgodnie z konfiguracją (rysunek 6.112).

Każdy zakres ma takie elementy, jak:

- *Address Pool* (*Pula adresów*) — adresy dostępne w ramach zakresu.
- *Address Leases* (*Dzierżawa adresów*) — zbiór adresów dzierżawionych wraz z czasem wygaśnięcia dzierżawy.
- *Reservations* (*Zastrzeżenia*) — pokazuje, które adresy IP są zarezerwowane.
- *Scope Options* (*Opcje zakresu*) — lista opcji zdefiniowanych dla zakresu.

Rysunek 6.112. Dzierżawa adresu dla stacji roboczej



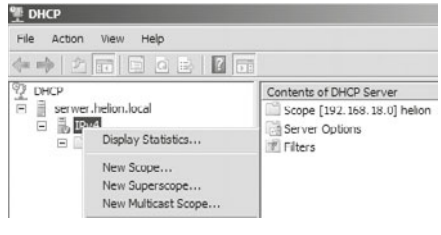
Zakres adresów

Zanim serwer DHCP będzie mógł przydzielać adresy, musi mieć zdefiniowany zakres adresów IP, które będzie dystrybuował. Zakres definiuje pojedynczą podsieć. Jeżeli w sieci dla każdej z kart są wykorzystywane dwie podsieci: 192.168.18.0/24 oraz 192.168.24.0/24, na serwerze DHCP trzeba skonfigurować je jako dwa osobne zakresy.

Kolejne kroki przedstawiają definiowanie zakresu dla puli adresów 192.168.24.0/24.

1. W konsoli do zarządzania serwerem za pomocą kreatora należy skonfigurować nowy zakres. W pierwszym kroku trzeba określić, dla jakiego węzła będzie on definiowany. W naszym przypadku będzie to IPv4 (rysunek 6.113). Należy kliknąć węzeł prawym klawiszem myszy i z menu kontekstowego wybrać *New Scope* (*Nowy zakres*).

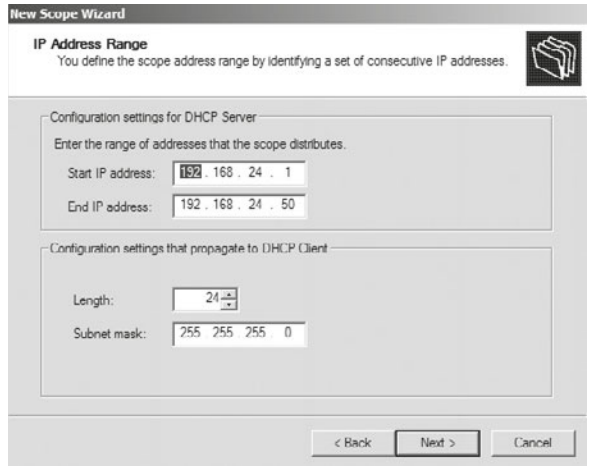
Rysunek 6.113. Tworzenie nowego zakresu



2. W pierwszym oknie kreatora dodawania nowego zakresu należy określić nazwę dla nowego zakresu oraz jego przeznaczenie.

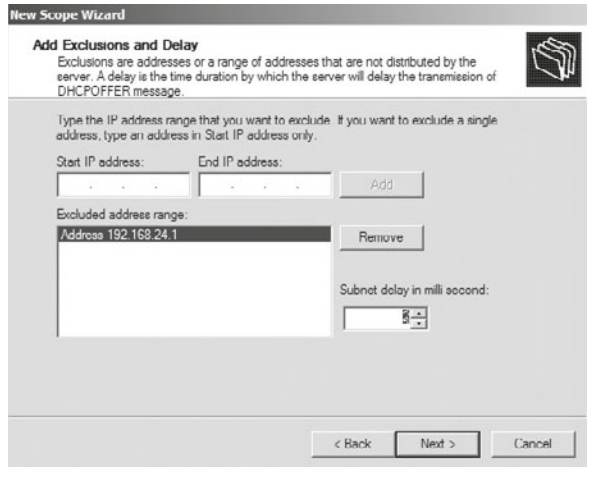
3. W kolejnym oknie kreatora trzeba podać adres początkowy i końcowy zakresu oraz maskę (rysunek 6.114).

Rysunek 6.114. Okno konfiguracji zakresu adresów



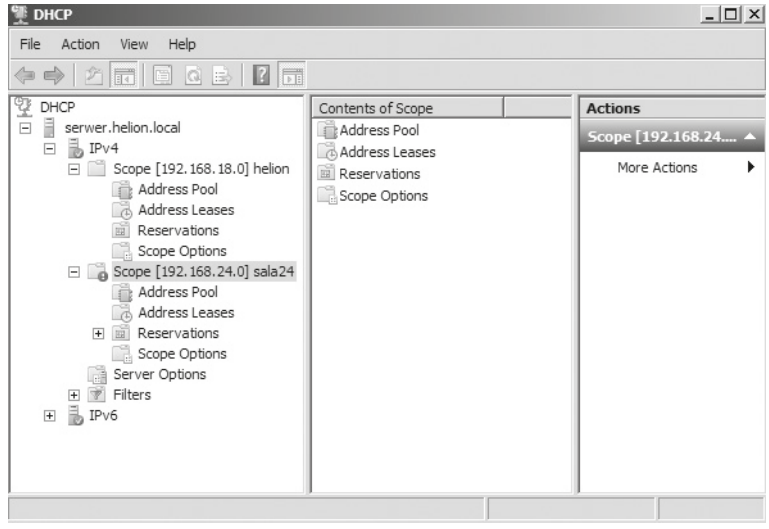
4. W ramach każdego zakresu można określić wykluczenia (ang. *exclusions*), a więc adresy, które nie będą przydzielane w ramach usługi (rysunek 6.115).

Rysunek 6.115. Wykluczenia w ramach zakresu



5. Następnym ważnym elementem jest zdefiniowanie czasu dzierżawy adresu, domyślnie wynosi on 8 dni.
6. Kolejny krok to konfiguracja podstawowych opcji DHCP, takich jak brama domyślna czy ustawienia DNS. Należy wybrać *Yes* (*Tak*), aby konfigurować opcje od razu.
7. Konfiguracja routera, czyli bramy domyślnej, umożliwia sprecyzowanie adresów dla ruchu wychodzącego. Możliwe jest dodanie więcej niż jednego adresu oraz ustawienie kolejności adresów na liście.
8. W ostatnim kroku należy aktywować zakres. Po aktywacji można sprawdzić, czy nowy zakres pojawił się w usłudze DHCP (rysunek 6.116).

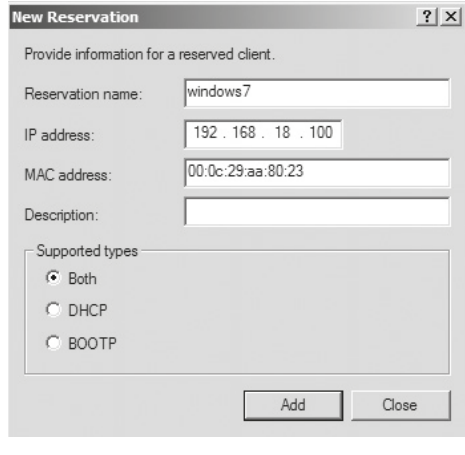
Rysunek 6.116.
Nowy zakres



Możemy również zdefiniować rezerwację adresu w ramach zakresu dla określonego adresu fizycznego MAC (ang. *Media Access Control* — 48-bitowy, zapisywany w postaci 12 liczb szesnastkowych oddzielonych znakiem - lub :). Należy rozwinąć dany zakres i przejść do *Reservation* (*Zastrzeżenia*). Następnie z menu kontekstowego trzeba wybrać *New Reservation* (*Nowe zastrzeżenie*) (rysunek 6.117). W celu konfiguracji zastrzeżeń należy podać adres IP, adres MAC karty sieciowej oraz określić obsługiwany typ:

- *Both* (*Oba*),
- *DHCP*,
- *BOOTP* — protokół komunikacyjny typu UDP umożliwiający komputerom w sieci uzyskanie od serwera danych konfiguracyjnych, np. adresu IP. Rozwinięciem i następcą protokołu BOOTP jest DHCP.

Rysunek 6.117.
Rezerwacja adresu dla karty MAC



ĆWICZENIA

1. Zainstaluj usługę DHCP dla karty lokalnej LAN.
2. Utwórz nowy zakres dla sieci, np.: 10.0.0.1 – 10.0.0.100. Sprawdź, czy adresy zostały pobrane przez klientów.
3. Zdefiniuj wykluczenia w ramach nowego zakresu adresów: adres 10.0.0.1 — dla serwera.
4. Przetestuj narzędzia do obsługi serwera DHCP.

PYTANIA

1. Podaj definicję usługi DHCP.
2. Wymień sygnały, jakie są wysyłane między klientem DHCP a serwerem.
3. Co to jest MAC?

6.5.3. NAT

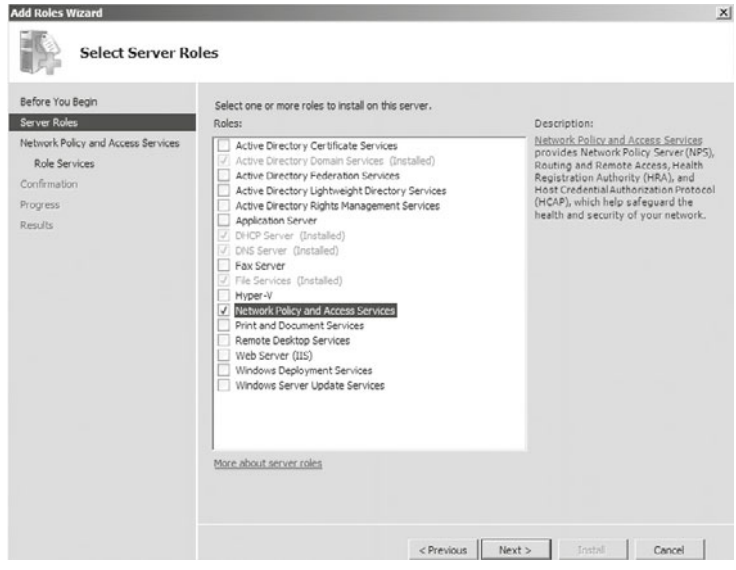
Translacja adresów sieciowych (NAT) pozwala komputerom w sieci prywatnej (np. sieć firmowa — LAN) uzyskać dostęp do komputerów w sieci publicznej (internet — WAN). Pozwala również rozwiązać problem związany z ograniczoną liczbą adresów IPv4, wykorzystując jeden adres do komunikacji z sieciami publicznymi. Z tego powodu, że cały ruch musi się odbywać za pośrednictwem routera z włączoną usługą NAT, jest możliwe ukrywanie adresów urządzeń pracujących w sieci wewnętrznej, a więc zwiększa się bezpieczeństwo.

Tabela 6.4. Funkcje usługi NAT

Składnik	Opis
Translacja	Wykonuje translację adresów IP między siecią prywatną a internetem.
Adresowanie	Składnik odpowiedzialny za przydzielanie adresu IP, maski podsieci, bramy domyślnej oraz adresu IP serwera DNS.
Rozpoznawanie nazw	Po zebraniu zapytań związanych z rozpoznaniem nazw w sieci przesyła je dalej do serwera DNS w internecie, który został określony w konfiguracji. Następnie zwraca odpowiedzi do komputera w sieci prywatnej.

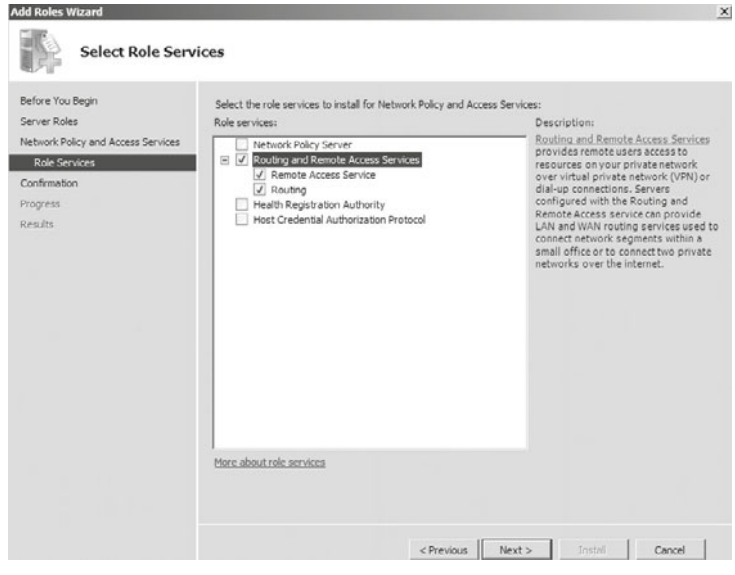
W Windows Server 2008 usługa NAT jest instalowana jako kolejna z ról serwera, która kryje się pod nazwą *Network Policy and Access Services* (*Usługa zasad i dostępu sieciowego*) (rysunek 6.118).

Rysunek 6.118. Kreator instalacji usługi



W następnym oknie kreatora (rysunek 6.119) należy wybrać składniki usługi, które mają być zainstalowane w ramach RRAS — *Routing and Remote Access* (*Usługi routingu i dostępu zdalnego*).

Rysunek 6.119. Wybór usług instalowanych w ramach RRAS

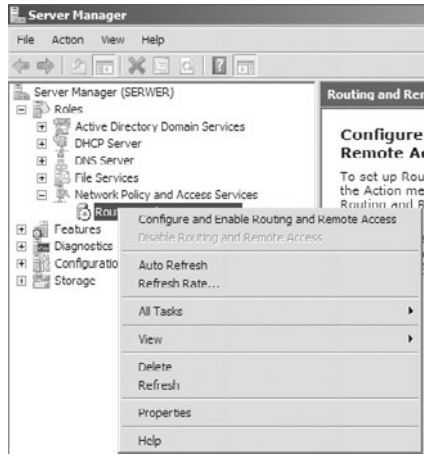


Po zakończonej instalacji należy uruchomić usługę *Routing and Remote Access* (*Usługi routingu i dostępu zdalnego*), która znajduje się wśród zainstalowanych ról serwera.

Rysunek 6.120.
Okno usługi

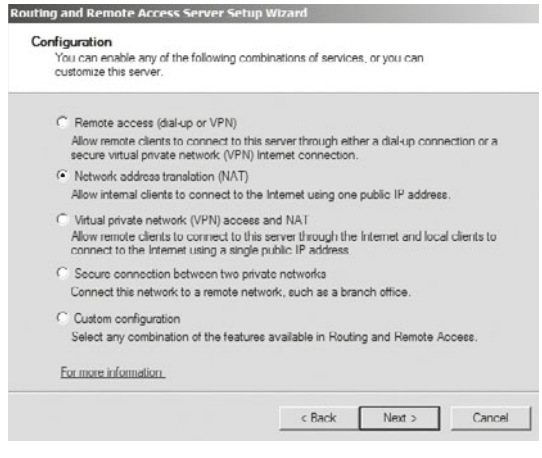
Usługa RRAS po zainstalowaniu musi zostać skonfigurowana. Aby to zrobić, należy kliknąć prawym klawiszem myszy nazwę serwera i wybrać *Configure and Enable Routing and Remote Access* (*Konfiguruj i włącz routing i dostęp zdalny*) (rysunek 6.121).

Rysunek 6.121.
Okno zarządzania serwerem



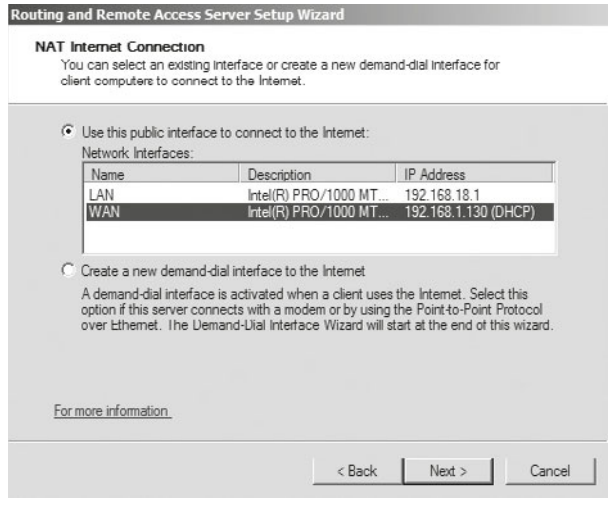
W pierwszym kroku kreatora (rysunek 6.122) należy wybrać usługę, którą zamierzamy uruchomić w ramach serwera RRAS.

Rysunek 6.122.
Okno kreatora usługi NAT



W następnym oknie kreatora (rysunek 6.123) należy wybrać interfejs sieciowy podłączony do sieci WAN (publicznej).

Rysunek 6.123. Okno wyboru interfejsów WAN

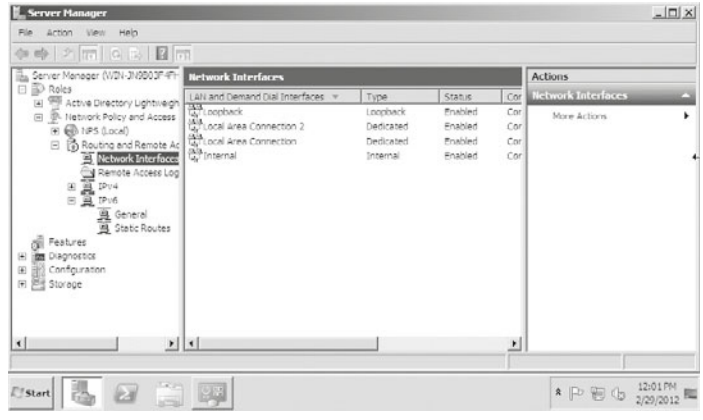


W kolejnych krokach instalacji wybieramy opcje domyślne, aż otrzymamy informację o skonfigurowanej usłudze (rysunek 6.124).

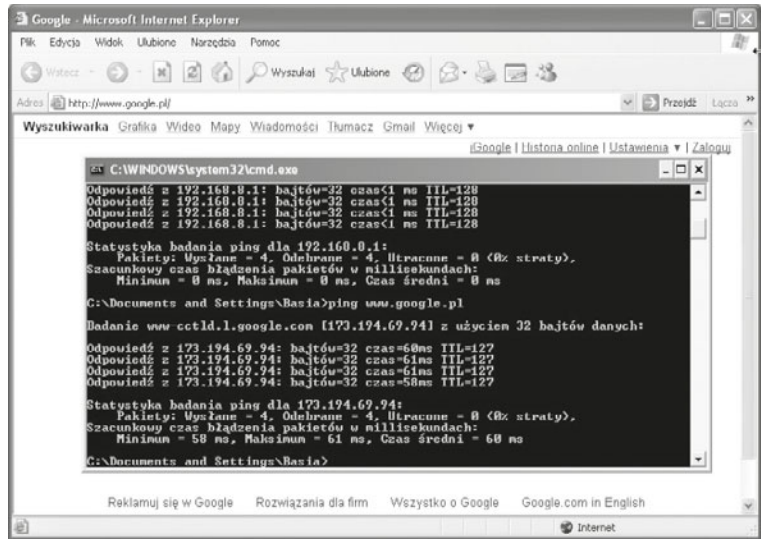
Rysunek 6.124. Okno podsumowania konfiguracji

Po ponownym uruchomieniu usługi (rysunek 6.125) jest ona skonfigurowana oraz pełni funkcję translatora adresów między dwoma sieciami, co pozwala na korzystanie z internetu komputerom w ramach domeny (rysunek 6.126).

Rysunek 6.125.
Okno skonfigurowanej usługi



Rysunek 6.126.
Funkcjonalność usługi NAT



ĆWICZENIA

1. Zainstaluj usługę NAT oraz skonfiguruj przekierowanie adresów z karty LAN na kartę WAN.

PYTANIA

1. Omów usługę NAT.
2. Wymień funkcje usługi NAT.

6.5.4. VPN

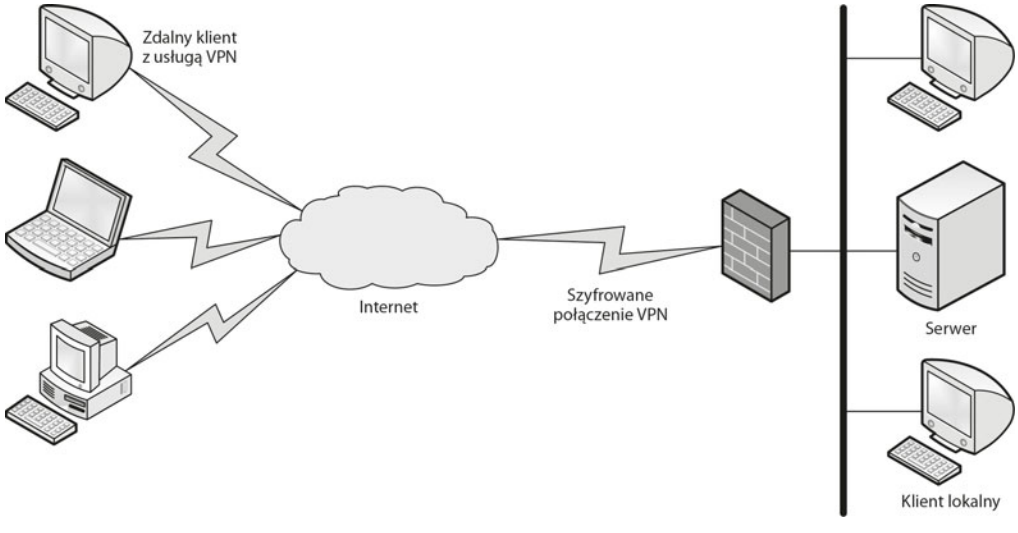
DEFINICJA

VPN (ang. *Virtual Private Network*, Wirtualna Sieć Prywatna) — tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych tak pakietów. Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa.

Sieci VPN możemy podzielić w zależności od:

- protokołów użytych w procesie tunelowania ruchu sieciowego;
- punktu końcowego tunelowania, może być nim na przykład sam klient bądź dostarczyciel internetu;
- dostępu punkt-punkt lub zdalnego dostępu;
- dostarczanych poziomów bezpieczeństwa;
- wykorzystywanej warstwy modelu OSI łączonej sieci, takiej jak połączenia w warstwie 2. bądź łączności warstwy 3.

Zasadę działania sieci VPN przedstawia rysunek 6.127.



Rysunek 6.127. Graficzne przedstawienie funkcjonalności VPN-u

DEFINICJA

Protokół PPTP (ang. *Point to Point Tunneling Protocol*) to protokół komunikacyjny umożliwiający tworzenie sieci VPN poprzez wykorzystanie tunelowania. Polega to na zdalnym łączeniu się do stacji roboczych lub sieci (głównie opartych na systemie operacyjnym Windows) za pośrednictwem internetu i tworzeniu wirtualnego połączenia z lokalną siecią.

DEFINICJA

Protokół L2TP (ang. *Layer Two Tunneling Protocol*) — protokół tunelowania, który pozwala na przenoszenie ruchu IP, IPX oraz NetBEUI i przekazywanie go poprzez dowolne medium transmisyjne, obsługujące dostarczanie datagramów w połączeniu punkt-punkt, np. IP, X.25, Frame Relay czy ATM.

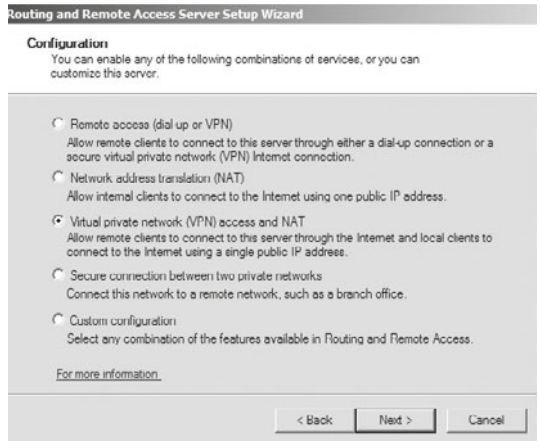
Zestawy funkcji VPN na serwerze RRAS:

- **Brama VPN dla klientów** — najbardziej rozpowszechniony scenariusz, potrzebuje dwóch kart sieciowych zainstalowanych na serwerze.
- **Site–to–site VPN** — w tym scenariuszu jest tworzony tunel VPN z innym serwerem RRAS, co umożliwia zakodowaną komunikację między serwerami.
- **Serwer telefoniczny RAS** — w tym scenariuszu do serwera jest doinstalowany modem lub zbiór modemów dostarczających usługi telefoniczne.
- **NAT pomiędzy sieciami** — scenariusz, który umożliwia tłumaczenie adresów publicznych na prywatne i odwrotnie.
- **Routing pomiędzy sieciami** — ten scenariusz pozwala na bezpośredni routing komunikacji pomiędzy segmentami sieci.
- **Zapora podstawowa** — scenariusz, w którym serwer RRAS zachowuje się jak standardowy router, blokując ruch przy użyciu portów.

Konfiguracja usługi:

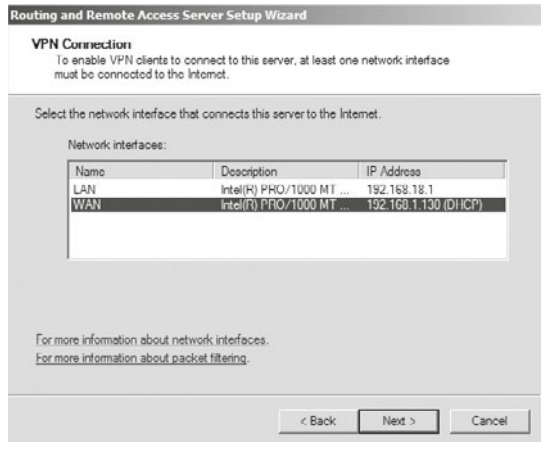
1. Usługa wchodzi w skład serwera routingu i dostępu zdalnego (ang. *Routing and Remote Access* — RRAS), więc w celu jej dodania należy uruchomić program *Server Manager* (*Menedżer serwera*) i dodać rolę lub w już dodanej roli doinstalować obsługę sieci VPN. Jeżeli jest już zainstalowana, należy aktualną dezaktywować i ponownie skonfigurować usługę (rysunek 6.128).

Rysunek 6.128.
Kreator konfiguracji usługi VPN



2. W następnym oknie kreatora (rysunek 6.129) należy wybrać interfejs sieciowy podłączony do sieci WAN (publicznej).

Rysunek 6.129.
Kreator wyboru interfejsu WAN

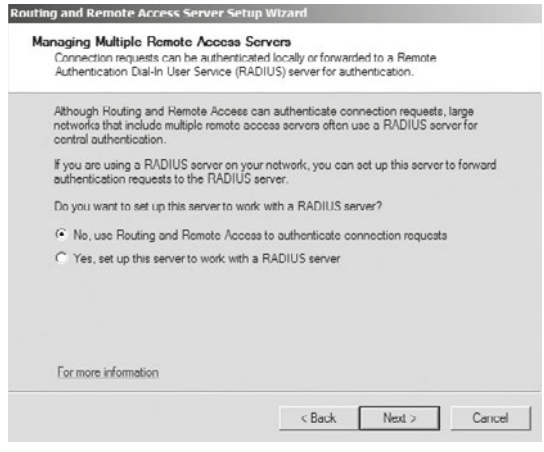


3. W następnym oknie kreatora (rysunek 6.130) należy określić, czy klienci zdalni będą otrzymywać adresy IP z serwera DHCP w sieci prywatnej, czy z konfigurowanego serwera dostępu zdalnego sieci VPN.

Rysunek 6.130.
Kreator konfiguracji korzystania z usługi DHCP

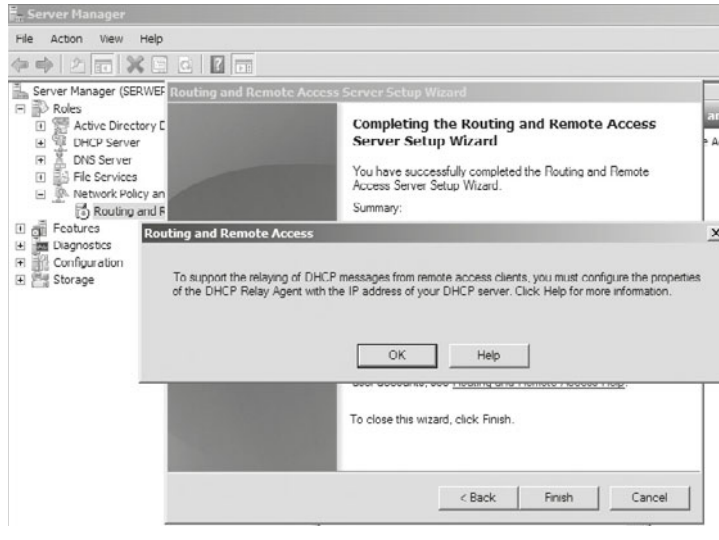
4. Następnie należy określić, czy żądania połączeń od klientów sieci VPN mają być uwierzytelniane przez serwer RADIUS (ang. *Remote Authentication Dial-In User Service*), czy przez konfigurowany serwer dostępu zdalnego sieci VPN (rysunek 6.131).

Rysunek 6.131. Kreator konfiguracji usługi RADIUS



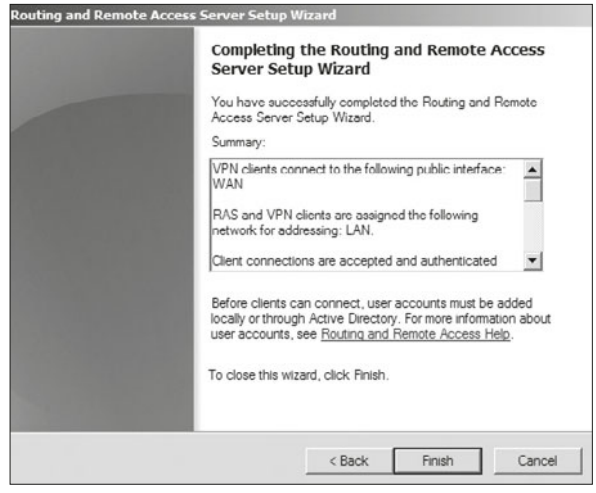
5. W kolejnym oknie kreatora należy określić, czy klienci VPN będą mogli wysyłać komunikaty DHCP do serwera DHCP w sieci prywatnej (rysunek 6.132).

Rysunek 6.132. Kreator potwierdzenia korzystania z usługi DHCP



6. W ostatnim oknie kreatora zostaniemy poinformowani o tym, że usługa została skonfigurowana (rysunek 6.133).

Rysunek 6.133. Potwierdzenie skonfigurowania usługi



ĆWICZENIA

1. Zainstaluj i skonfiguruj usługę VPN.

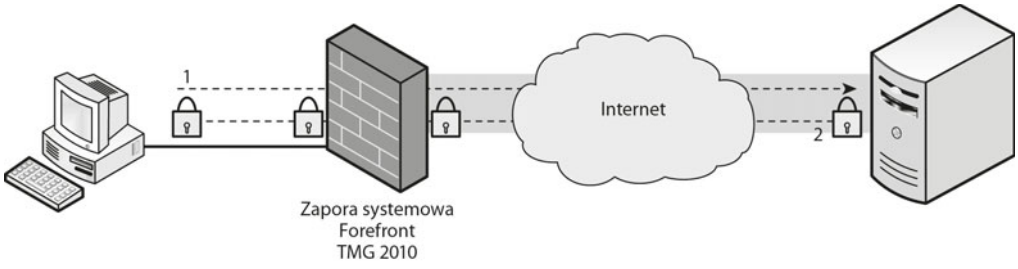
PYTANIA

1. Wymień protokoły wykorzystywane przez usługę VPN.
2. Omów serwer RADIUS.

6.5.5. Zapora systemowa

Mechanizmy zabezpieczeń w sieci dotyczą nie tylko bezpieczeństwa transmisji, ale również zabezpieczeń komputerów i sieci przed niepowołanym dostępem lub atakiem. Podstawową metodą ochrony są tzw. ściany ogniowe (ang. *firewall*). Termin ten może odnosić się zarówno do sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera. Ściany ogniowe zapewniają ochronę sieci wewnętrznej LAN lub komputera przed dostępem z zewnątrz, tzn. z sieci publicznych. Do podstawowych zadań firewalla należy filtrowanie połączeń wchodzących i wychodzących, a tym samym odmawianie żądań dostępu uznanych za niebezpieczne.

W systemach serwerowych firewall jest realizowany za pomocą dodatkowych płatnych funkcji. W przypadku serwera 2003 i 2008 w wersji 32-bitowej taką usługą jest ISA 2006, dla serwera 2008 R2 usługa nosi nazwę Forefront TMG 2010 (rysunek 6.134).



Rysunek 6.134. Graficzna interpretacja umiejscowienia usługi TMG

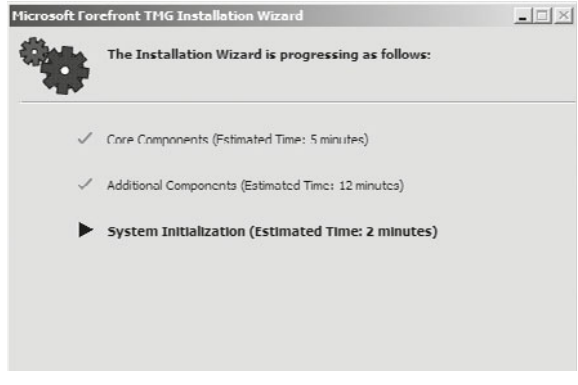
Serwery TMG zapewniają filtrowanie przesyłanych danych w warstwie sieci i w warstwach wyższych, istnieje możliwość wykorzystania filtrów dla wielu protokołów warstwy aplikacji, jak: HTTP, SMTP, POP3.

Minimalne wymagania dla serwera TMG:

- Procesor 64-bitowy o częstotliwości co najmniej 1,86 GHz, minimum dwa rdzenie lub dwa procesory jednordzeniowe.
- System operacyjny Windows Server (2008 lub 2008 R2) w wersji 64-bitowej.
- Minimum 2 GB pamięci RAM.
- 2,5 GB dostępnej przestrzeni dyskowej.

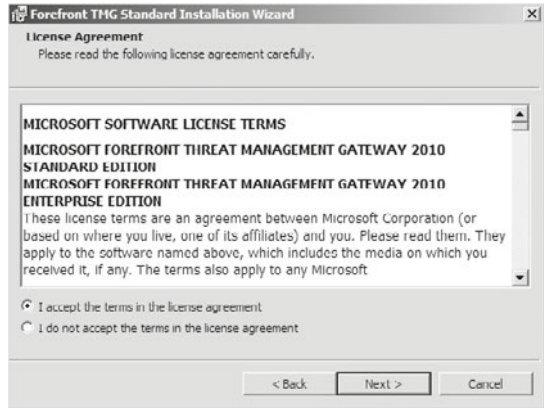
1. Po uruchomieniu instalatora (rysunek 6.135) następuje instalacja komponentów rdzeniowych, komponentów dodatkowych oraz inicjalizacja komponentów systemowych. Właściwa instalacja rozpoczyna się po fazie zrealizowanej za pomocą narzędzia *Microsoft Forefront TMG Preparation Tool*.

Rysunek 6.135. Kreator instalacji komponentów



2. W kolejnym oknie należy po przeczytaniu zaakceptować warunki licencji (rysunek 6.136).

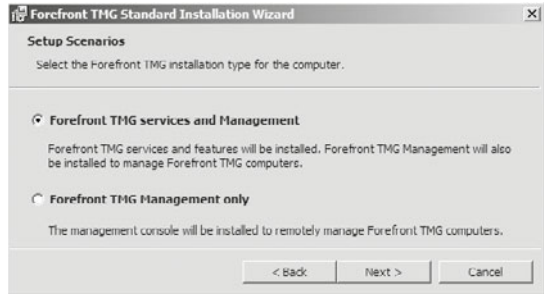
Rysunek 6.136.
Okno akceptacji licencji



3. W kolejnym oknie kreatora (rysunek 6.137) należy wybrać komponent, który ma zostać zainstalowany:

- *Forefront TMG services and Management* — komponenty serwera oraz narzędzia administracyjne,
- *Forefront TMG Management only* — tylko narzędzia administracyjne.

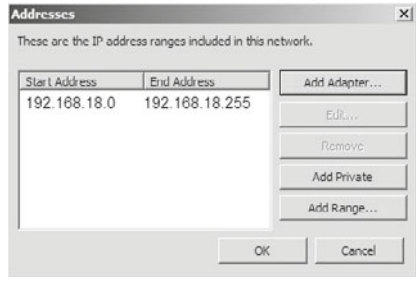
Rysunek 6.137.
Okno kreatora wyboru usługi



4. W kolejnym kroku instalacji (rysunek 6.138) należy określić zakres adresów dla sieci lokalnej (wewnętrznej). Możliwe są trzy sposoby:

- *Add Adapter* — adresy zostaną pobrane z konfiguracji interfejsu sieciowego,
- *Add Private* — automatycznie przypisane zostaną adresy z pul prywatnych,
- *Add Range* — będzie można podać żądany zakres adresów.

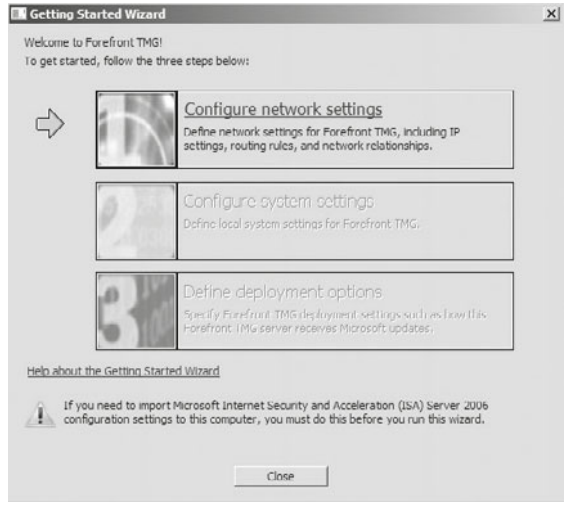
Rysunek 6.138.
Kreator dodania interfejsów



Po instalacji usługi przy pierwszym uruchomieniu pojawia się konfigurator usługi (rysunek 6.139), którego działanie jest podzielone na trzy etapy:

- *Configure network setting* — pozwala na zmianę ustawień sieciowych i wybór scenariusza pracy TMG,
- *Configure system settings* — pozwala na wybór trybu pracy — w domenie lub w grupie roboczej — oraz konfigurację DNS,
- *Define deployment options* — pozwala na zmianę konfiguracji aktualizacji i subskrypcji.

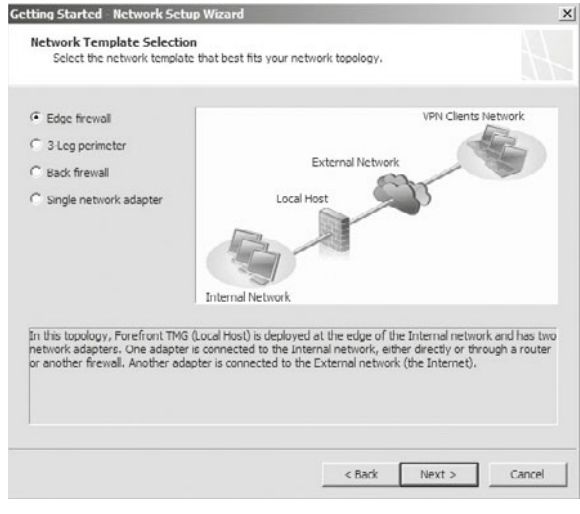
Rysunek 6.139. Konfigurator usługi



Podczas konfiguracji ustawień sieciowych mamy do dyspozycji cztery scenariusze pracy serwera TMG:

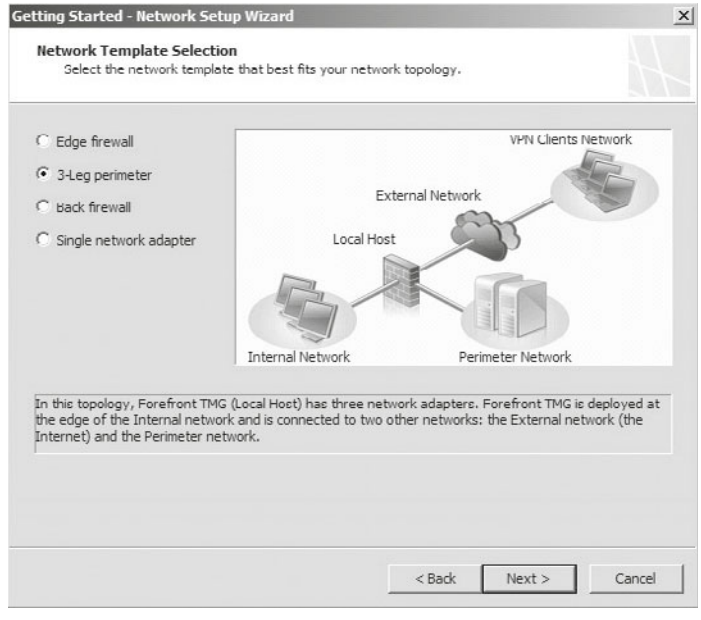
- *Edge firewall* — zapora systemowa brzegowa (rysunek 6.140).

Rysunek 6.140. Zapora systemowa brzegowa



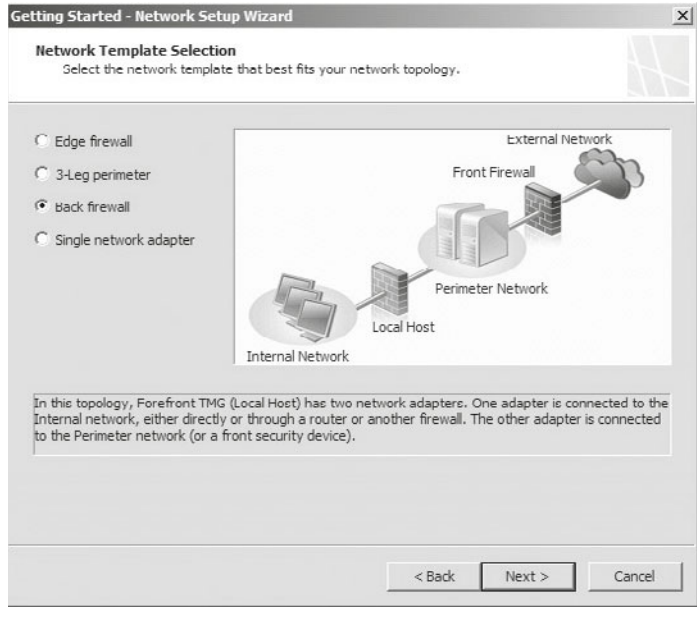
- *3-Leg perimeter* — zapora systemowa brzegowa z dodatkowym interfejsem określanym jako DMZ (rysunek 6.141).

Rysunek 6.141. Zapora systemowa brzegowa z DMZ

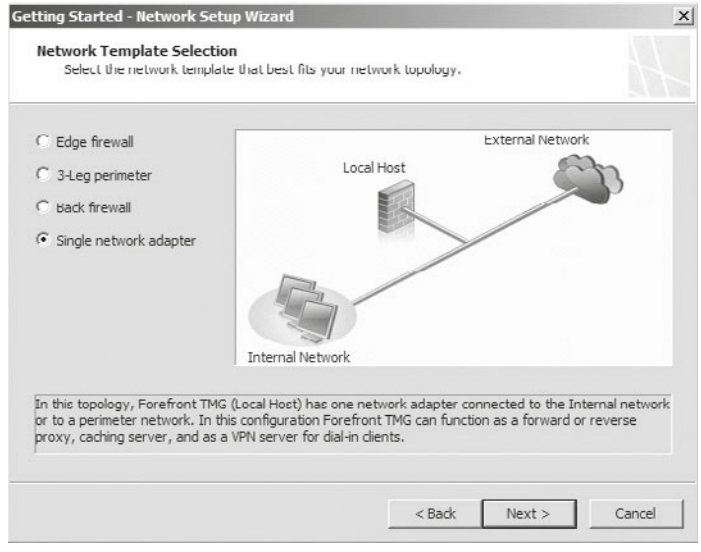


- *Back firewall* — ta konfiguracja jest wybierana, kiedy pomiędzy TMG a internetem istnieje jeszcze jedna zapora (rysunek 6.142).

Rysunek 6.142. Wsteczna zapora systemowa

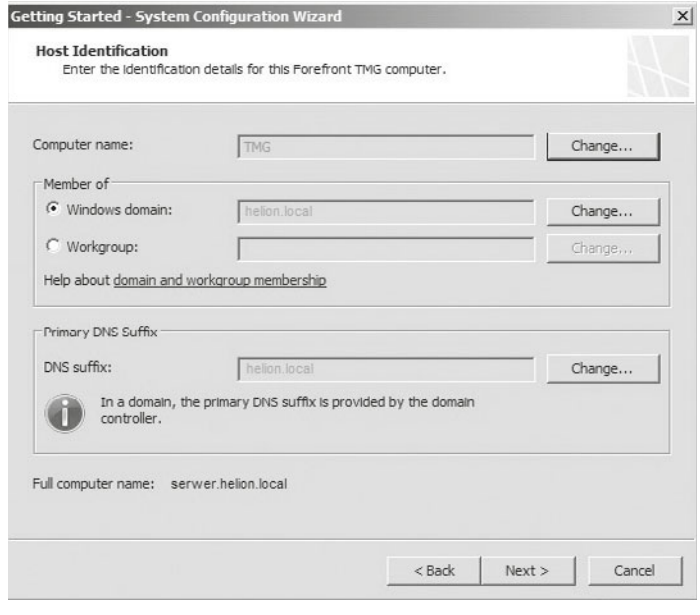


- *Single network adapter* — stosowana przy serwerach typu WEB-PROXY (rysunek 6.143).



Rysunek 6.143. Konfiguracja jednointerfejsowa

Po wybraniu odpowiedniego scenariusza uaktywnia się następna faza konfiguracji, w której należy zdefiniować domenę lub grupę roboczą oraz określić serwer DNS (rysunek 6.144).



Rysunek 6.144. Potwierdzenie ustawień domeny lub grupy roboczej oraz serwera DNS

W ostatnim oknie pojawi się podsumowanie tego, co zostało zdefiniowane.

ĆWICZENIA

1. Zainstaluj usługę zapory systemowej i dokonaj konfiguracji:
   a. Odblokuj usługę http.
   b. Odblokuj usługę związaną z DHCP, DNS, Kerberos.

PYTANIA

1. Wymień dostępne zapory systemowe dla serwerów.
2. Wymień wymagania dla usługi TMG.

6.6. Usługi serwerowe

6.6.1. Serwer plików

DEFINICJA

Udostępnianie plików to jedna z najbardziej obecnie rozpowszechnionych funkcji systemów. Pozwala na kontrolowanie dostępu do zasobów dyskowych. Serwer plików umożliwia przechowywanie plików i udostępnianie ich użytkownikom w sieci. Gdy użytkownicy potrzebują ważnego pliku, na przykład planu projektu, mogą uzyskać do niego dostęp na serwerze plików, zamiast przenosić go z komputera na komputer. Jeżeli użytkownicy sieci potrzebują tych samych plików i aplikacji dostępnych w sieci, należy skonfigurować komputer jako serwer plików. Serwer plików umożliwia nadzór nad tym, co się dzieje z udostępnionym zasobem, pozwala przechowywać poprzednie kopie oraz zarządzać przydziałem dyskowym.

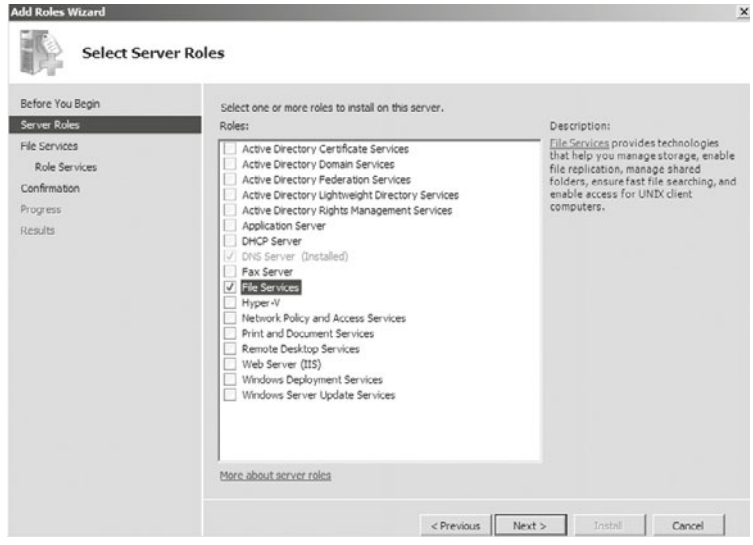
Z serwerem plików mamy do czynienia w chwili udostępnienia w sieci pierwszego folderu. Jeżeli chcemy wykorzystać w pełni tę rolę, warto najpierw zainstalować usługę, a dopiero później zacząć udostępniać foldery.

W skład usługi serwera plików (ang. *File Services*) wchodzą:

- Rozproszony system plików (DFS, ang. *Distributed File System*),
- Menedżer zasobów serwera plików (FSRM, ang. *File Server Resource Manager*).

Kroki związane z instalacją serwera plików

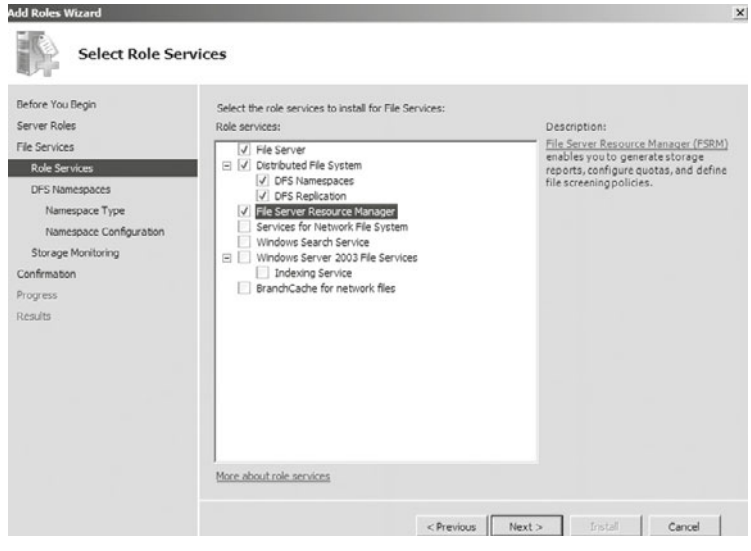
1. W Menedżerze serwera dodajemy nową rolę serwera plików (rysunek 6.145).



Rysunek 6.145. Dodawanie roli serwera plików (ang. File Services)

2. W kolejnym kroku (rysunek 6.146) należy wybrać elementy, które będą zainstalowane wraz z usługą:

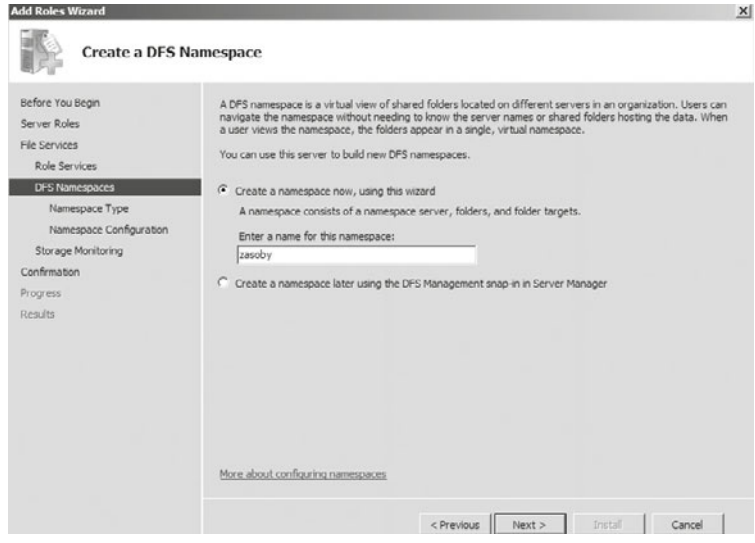
- serwer plików,
- DFS,
- FSRM.



Rysunek 6.146. Wybór usług instalowanych w ramach serwera plików

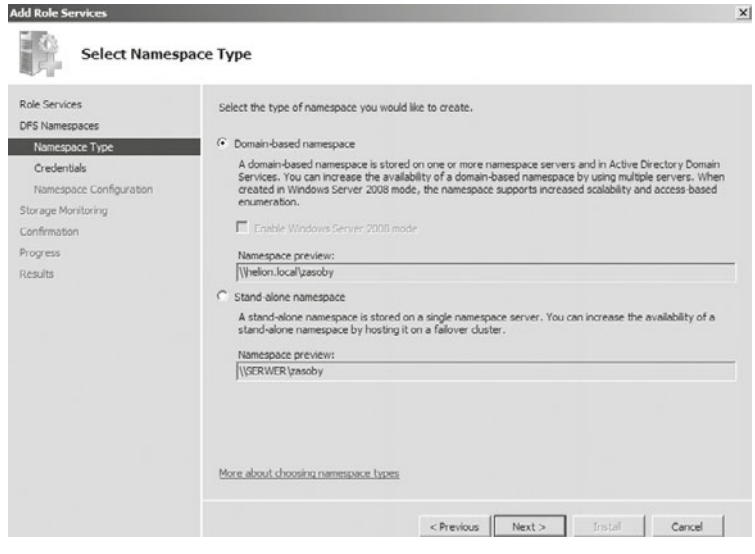
3. W kolejnym kroku należy zdefiniować obszar nazw (ang. *namespace*) (rysunek 6.147).

Rysunek 6.147. Definiowanie obszaru nazw



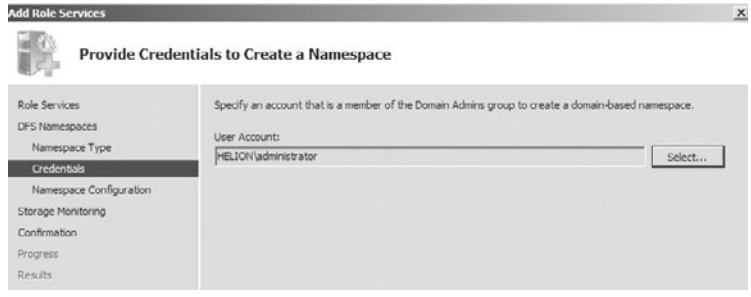
4. Należy określić, w jaki sposób będzie rozpoznawany obszar nazw w sieci (rysunek 6.148):
   - *Domain-based namespace* (*Obszar nazw oparty na domenie*),
   - *Stand-alone namespace* (*Autonomiczny obszar nazw*).

Rysunek 6.148. Kreator rozpoznawania obszaru nazw w sieci



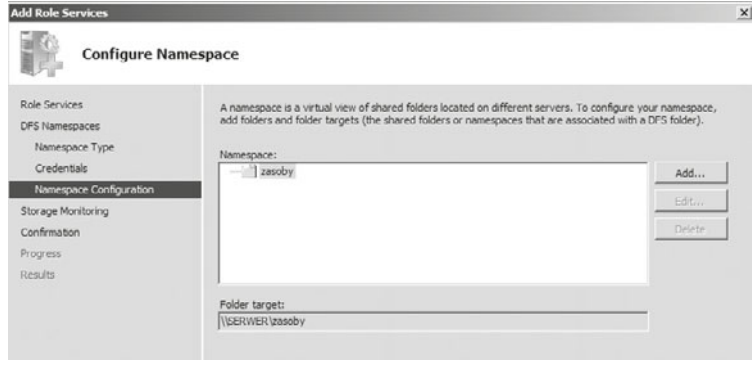
5. W kreatorze tworzenia poświadczeń dla obszaru nazw należy wybrać konto, które ma tego typu uprawnienia (rysunek 6.149).

Rysunek 6.149. Kreator tworzenia poświadczeń



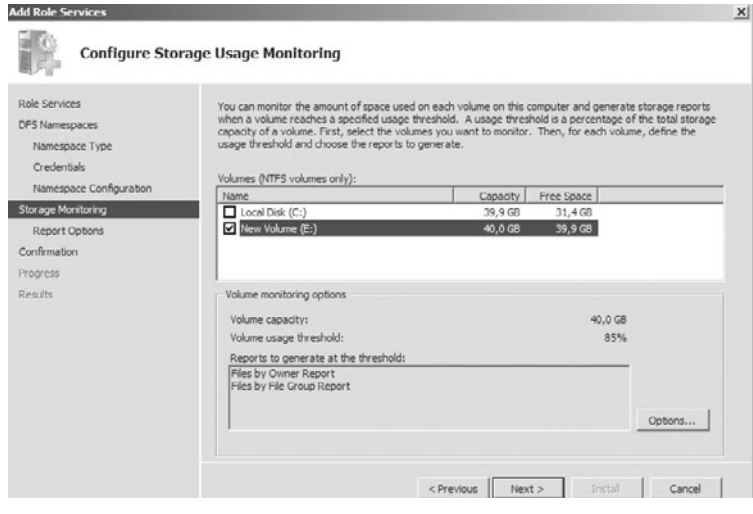
6. W kolejnym oknie należy określić położenie udostępnionego folderu (rysunek 6.150).

Rysunek 6.150. Położenie folderu udostępnionego w ramach przestrzeni nazw



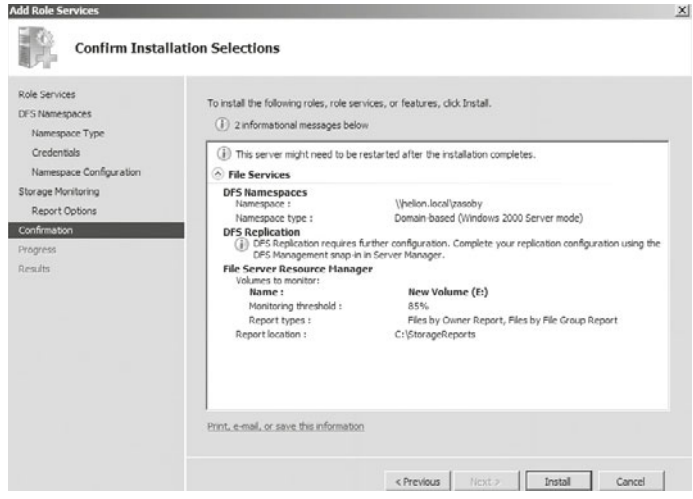
7. Kolejne okna pozwalają zdefiniować, które z partycji będą monitorowane pod względem wykorzystania pamięci przestrzeni dyskowej (rysunek 6.151), oraz skonfigurować mechanizmy raportowania wykorzystania przestrzeni na dyskach.

Rysunek 6.151. Konfigurowanie monitorowania wykorzystania przestrzeni dyskowej



8. W ostatnim oknie konfiguracji otrzymujemy podsumowanie instalacji i konfiguracji usługi (rysunek 6.152).

Rysunek 6.152. Podsumowanie instalowanej usługi oraz konfiguracji przestrzeni nazw



Rozproszony system plików

Technologie rozproszonego systemu plików (DFS) zapewniają replikację w sieci rozległej (WAN) oraz uproszczony dostęp do plików rozproszonych geograficznie. System DFS udostępnia następujące dwie technologie:

- Obszary nazw systemu plików DFS. Umożliwiają grupowanie folderów udostępnionych znajdujących się na różnych serwerach w jeden lub kilka obszarów nazw o strukturze logicznej. Użytkownicy widzą każdy obszar nazw jako pojedynczy folder udostępniony z podkatalogami.
- Replikacja systemu plików DFS. Usługa ta pozwala na synchronizację folderów między serwerami w połączeniach sieciowych o ograniczonej przepustowości.

Menedżer zasobów serwera plików

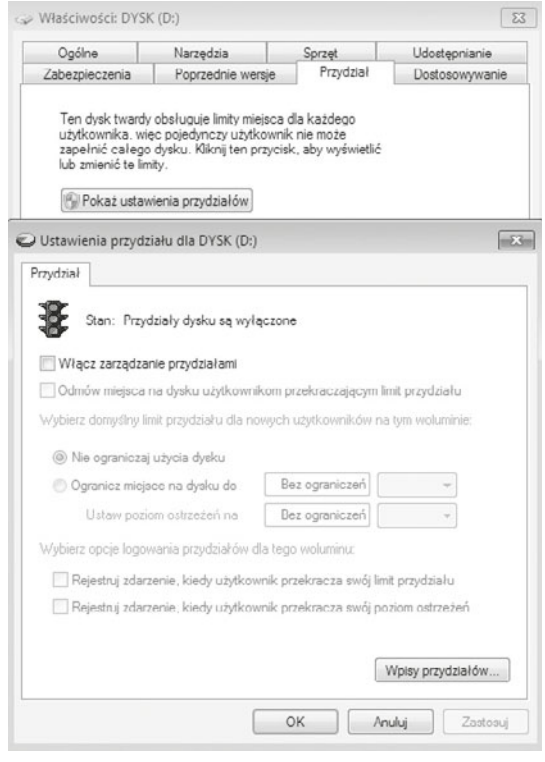
Menedżer zasobów serwera plików jest zestawem narzędzi, który umożliwia administratorom kontrolowanie i zarządzanie rodzajem i ilością danych przechowywanych na serwerach. Za jego pomocą administratorzy mogą definiować przydziały dyskowe w folderach i woluminach oraz generować szczegółowe raporty magazynowe. Ten zestaw zaawansowanych narzędzi nie tylko pomaga administratorowi efektywnie monitorować istniejące zasoby pamięci masowej, ale także ułatwia planowanie i realizację przyszłych zmian.

Przydział dyskowy

Przydział dyskowy służy do śledzenia i kontrolowania wykorzystania miejsca przez użytkowników na woluminach NTFS. Monitorowanie wykorzystywania miejscu na dysku jest możliwe nie tylko na serwerach, ale również na stacjach roboczych niekoniecznie znajdujących się w domenie.

W ramach stacji roboczej, która nie jest podłączona do domeny, konfiguracja przydziału dyskowego jest możliwa przez zakładkę *Przydział* (rysunek 6.153).

Rysunek 6.153. Przydział dyskowy — stacja robocza



W ramach serwera konfiguracja przydziału dyskowego jest możliwa przy wykorzystaniu narzędzia *File Server Resource Manager* (*Menedżer zasobów serwera plików*). Umożliwia ono:

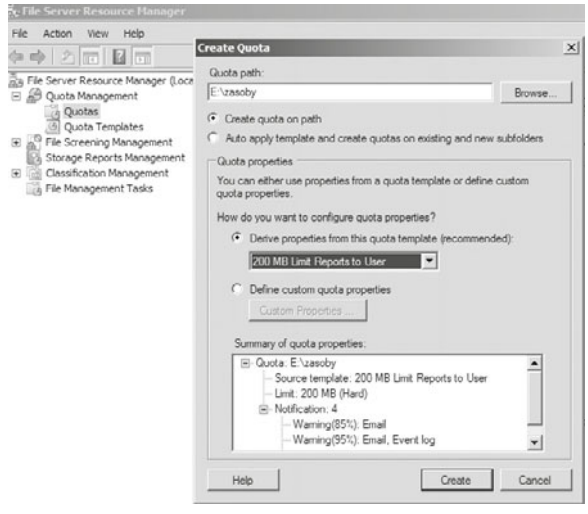
- Zapobieganie dalszemu wykorzystywaniu miejsca na dysku i rejestrowanie zdarzenia w dzienniku, jeżeli użytkownik przekroczy określony limit miejsca na dysku, czyli dozwoloną ilość miejsca na dysku, z której może korzystać.
- Rejestrowanie w dzienniku zdarzenia, jeśli użytkownik przekroczy określony poziom ostrzegania dotyczący miejsca na dysku, czyli punkt, w którym użytkownik zbliża się do limitu przydziału.

W celu dodania limitu w ramach Menedżera zasobów serwera plików należy rozwinąć węzeł dotyczący zarządzania przydziałami (*Quota Management* (*Zarządzanie przydziałami*)), następnie w części dotyczącej przydziałów (*Quotas* (*Przydziały*)) rozpocząć tworzenie nowego przydziału (*Create Quota* (*Utwórz przydział*)), np. dla dysku *E:*. W ramach kreatora tworzenia nowego przydziału określa się:

- *Quota path* (*Ścieżka przydziału*) — ścieżkę przydziału,
- *Quota properties* (*Właściwości przydziału*) — limit w ramach szablonu lub ustawiany samodzielnie.

Kiedy wymagane opcje zostaną skonfigurowane, należy kliknąć *Create* (*Utwórz*). Ograniczenia będą już aktywne (rysunek 6.154).

Rysunek 6.154. Przydział dyskowy w ramach usługi serwera plików



ĆWICZENIA

1. Zainstaluj serwer plików i zdefiniuj przestrzeń nazw.
2. Stwórz nową przestrzeń nazw.
3. Stwórz replikację między przestrzeniami nazw.
4. Zdefiniuj przydział dyskowy.

PYTANIA

1. Co to jest serwer plików?
2. Co to jest przestrzeń nazw?
3. Co to jest quota?
4. Co to jest replikacja?

6.6.2. Serwer wydruku

DEFINICJA

Serwer wydruku (ang. *print server*) — udostępnia obsługę zadań drukowania, obejmującą rozmaite usługi od prostego kolejkowania wydruków (ustawiania ich w odpowiedniej kolejności do odpowiednich drukarek), poprzez formatowanie wydruków (np. zmianę z popularnych formatów do postscriptu), aż po bardziej wyszukane funkcje, takie jak rozliczanie i raportowanie wydrukowanych stron.

WAŻNE

Serwer wydruku można również skonfigurować na systemach domowych. Obsługą drukowania na drukarkach lokalnych zajmuje się podsystem drukowania (ang. *spooler*), który jest w istocie lokalnym serwerem drukowania.

Drukarki mogą być podłączone do serwera wydruku bezpośrednio lub pośrednio:

- Połączenie bezpośrednie jest realizowane za pomocą portu równoległego lub portu szeregowego USB.
- Połączenie pośrednie jest realizowane przez sieć komputerową.

WAŻNE

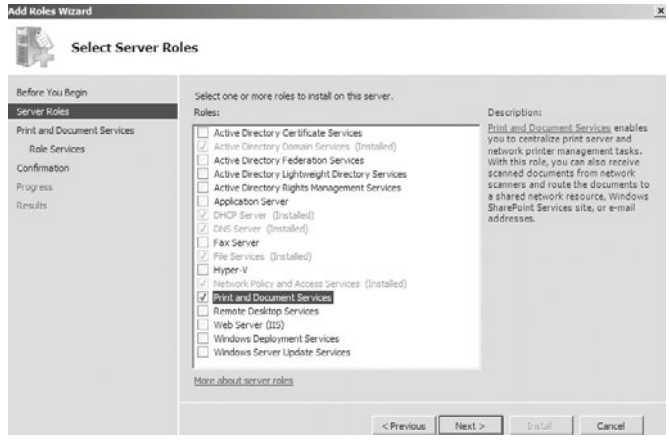
Przed dodaniem roli serwera wydruku:

- Określ wersję systemu operacyjnego klientów, z których będą wysyłane zadania do drukarki.
- Przejdź do drukarki i wydrukuj stronę konfiguracyjną lub testową, na której znajdują się informacje dotyczące producenta, modelu, języka i zainstalowanych opcji.
- Określ sposób łączenia się serwera wydruku z drukarką.
- Określ, czy potrzebujesz nowego lub zaktualizowanego sterownika drukarki.
- Wybierz nazwę drukarki. Długość nazwy drukarki zazwyczaj nie przekracza 31 znaków.
- Wybierz nazwę udziału. Długość nazwy udziału zazwyczaj nie przekracza 8 znaków.

Tak jak poprzednie usługi, serwer wydruku jest rolą, którą należy zainstalować, a następnie skonfigurować. Poniżej są przedstawione kroki instalacji i konfiguracji.

1. W celu uruchomienia serwera wydruku należy dodać odpowiednią rolę *Print and Document Services* (*Usługi drukowania i zarządzania dokumentami*) (rysunek 6.155).

Rysunek 6.155. Dodawanie roli serwera wydruku

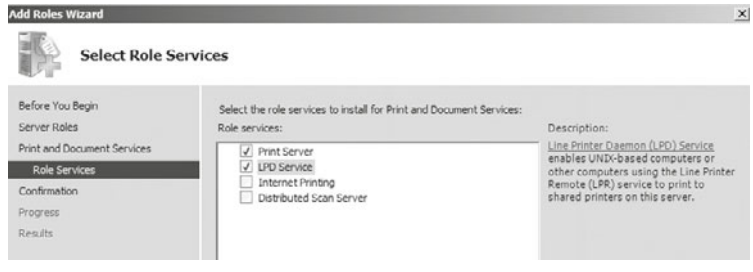


2. Po wybraniu opcji serwera wydruku *Print and Document Services* (*Usługi drukowania i zarządzania dokumentami*) w kolejnym oknie kreatora pojawi się informacja o zadaniach, jakie może pełnić serwer wydruku.

3. W kolejnym oknie (rysunek 6.156) należy wybrać usługi instalowane wraz z rolą serwera wydruku. Domyślnie jest zaznaczona jedna pozycja — *Print Server* (*Serwer wydruku*). Dodatkowo możemy wybrać *LPD Service* (*Usługa LPD*) — LPD (ang. *Line Printer Daemon*). Pozostałe opcje to *Distributed Scan Server* (*Serwer skanów rozproszonych*) oraz *Internet Printing* (*Drukowanie internetowe*).

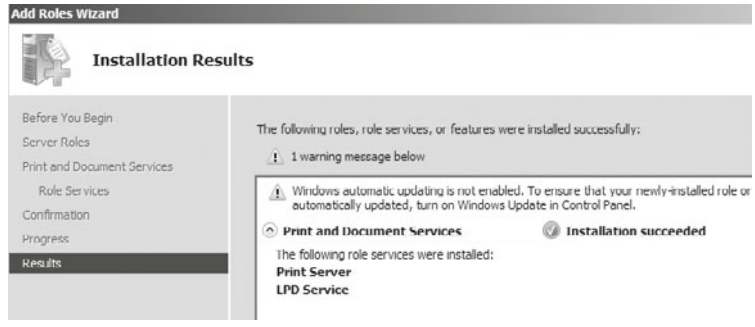
- *LPD Service* (*Usługa LPD*) — oferuje możliwość wydruku na serwerze Windows dokumentów przychodzących od klientów pracujących w systemach Unix i Linux.
- *Internet Printing* — pozwala na drukowanie dokumentów przez internet lub intranet.

Rysunek 6.156. Kreator dodawania usługi



4. Po wybraniu dodatkowych ról w usłudze następuje instalacja usługi, po czym wyświetlane jest okno podsumowujące (rysunek 6.157).

Rysunek 6.157. Potwierdzenie zainstalowania usługi



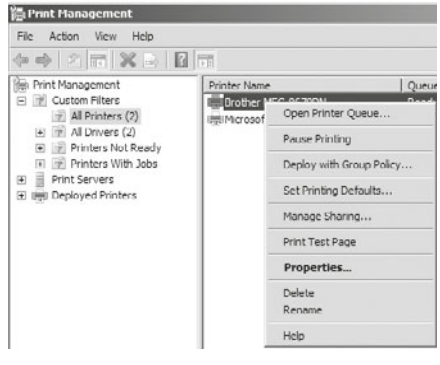
Po uruchomieniu serwera wydruku należy go skonfigurować w narzędziu *Server Manager* (*Menedżer serwera*) i wybrać odpowiednią rolę.

1. Trzeba sprawdzić, czy drukarki, które są już zainstalowane, są dodane. Jeżeli nie chcemy, aby któraś była dostępna przez serwer wydruku, to ją usuwamy (rysunek 6.158).

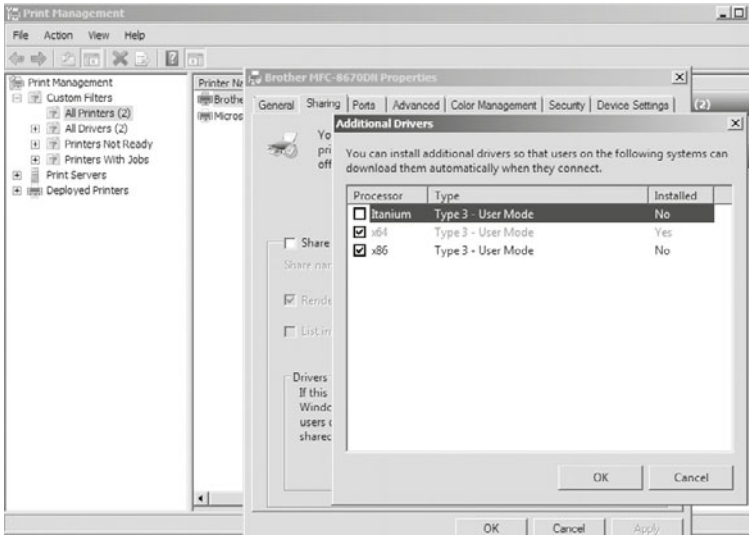
Rysunek 6.158. Serwer wydruku

2. Jeżeli chcemy, aby drukarki udostępnione w ramach usługi były dostępne dla użytkowników po ich ponownym zalogowaniu, należy je wdrożyć w domenie poprzez GPO (rysunek 6.159).

Rysunek 6.159. Wdrażanie drukarek przy użyciu GPO



3. Jeśli drukarka ma zostać udostępniona użytkownikom korzystającym z innych wersji systemu Windows (32- i 64-bitowych), należy dodać obie wersje sterowników (rysunek 6.160).



Rysunek 6.160. Dodawanie sterowników dla udostępnionej drukarki

ĆWICZENIA

1. Zainstaluj serwer wydruku.
2. Dodaj drukarkę bezpośrednio podpiętą do serwera oraz sieciową.
3. Wykonaj wydruk próbny.

PYTANIA

1. Co to jest serwer wydruku?
2. W jaki sposób sprawdzić, jakie drukarki zostały zainstalowane w systemie?
3. W jaki sposób wydrukować stronę testową?

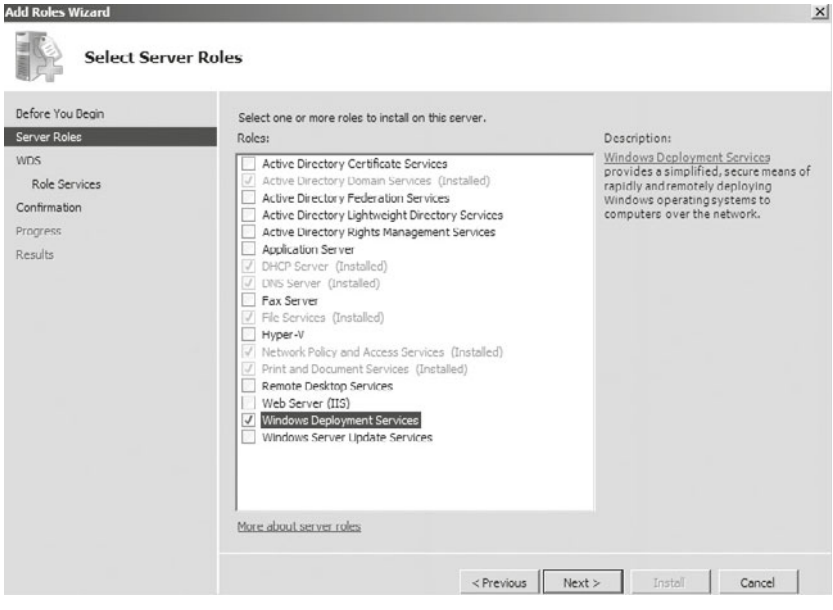
6.6.3. WDS

Windows Deployment Services (*Usługi wdrażania systemu Windows*) jest uproszczonym i zarazem bezpiecznym rozwiązaniem dla zdalnej oraz szybkiej instalacji systemów operacyjnych na komputerach podłączonych bezpośrednio do sieci LAN.

WAŻNE

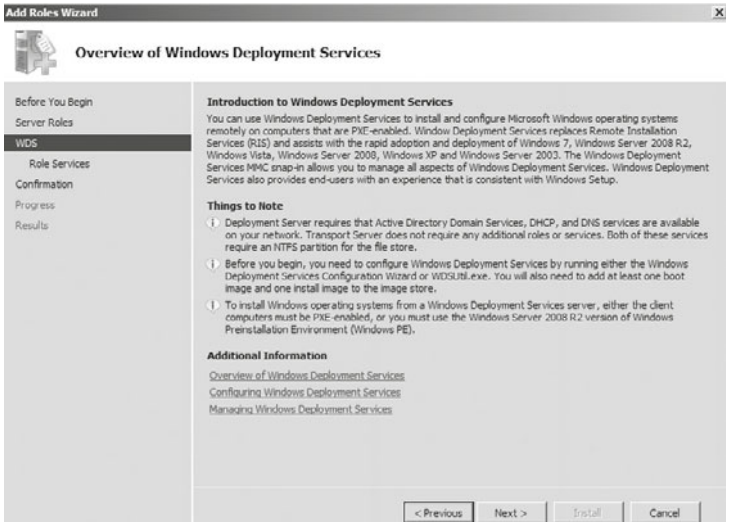
Serwer, na którym ma być zainstalowana usługa WDS, wcześniej powinien być wyposażony w następujące role: usługę katalogową AD, DNS oraz DHCP. AD umożliwi uwierzytelnienie użytkowników mających dostęp do pobieranych obrazów oraz tych, którzy chcą wysłać przygotowany obraz do domeny. Karta sieciowa PXE podczas uruchomienia komputera nie ma adresu IP, aby móc się komunikować z serwerem WDS — potrzebuje tego adresu z serwera DHCP. Dostęp do udziału, gdzie są przechowywane obrazy systemów, odbywa się po nazwie, a nie po adresie IP, co umożliwia usługa rozwiązywania nazw DNS. PXE to tryb pracy, w którym komputer wyposażony w kartę sieciową łączy się z serwerem i z niego pobiera system operacyjny.

1. Usługa wdrażania systemu Windows jest kolejną z ról Windows Server 2008, zatem cały proces instalacji roli rozpoczynamy od uruchomienia narzędzia *Server Manager* (*Menedżer serwera*) i dodania roli *Windows Deployment Services* (*Usługi wdrażania systemu Windows*) (rysunek 6.161).



Rysunek 6.161. Dodawanie roli WDS

2. Po zaznaczeniu wyżej wymienionej usługi i kliknięciu przycisku *Next* (*Dalej*) pojawia się kolejne okno (rysunek 6.162), w którym przed instalacją wyświetla się informacja o kilku istotnych kwestiach dotyczących wstępnej konfiguracji serwera. Ta usługa wymaga zainstalowanego serwera DHCP oraz DNS, a także tego, by partycja, na której będą przechowywane obrazy, była partycją NTFS. Po zapoznaniu się z powyższymi informacjami należy kliknąć *Next* (*Dalej*).

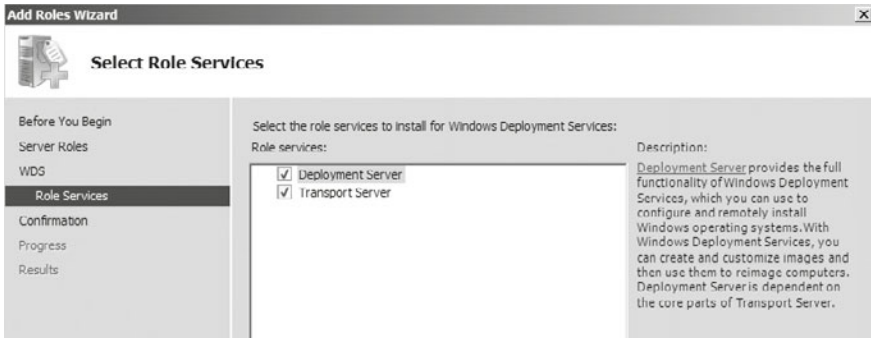


Rysunek 6.162. Okno kreatora informujące o wymaganiach instalowanej usługi

3. W kolejnym oknie kreatora (rysunek 6.163) mamy do wyboru dwie usługi:

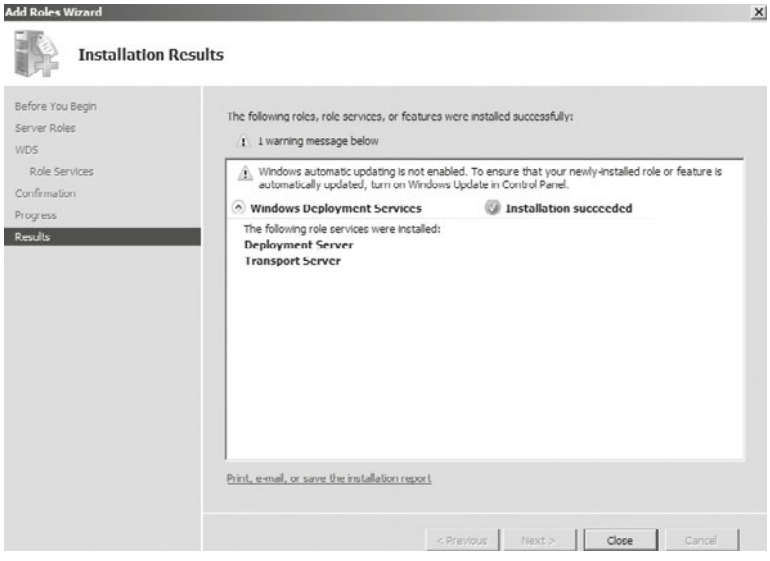
- *Deployment Server* (*Serwer wdrażania*) — funkcja, która umożliwia konfigurowanie oraz zdalne instalowanie systemów operacyjnych Windows. Za pomocą tej usługi można tworzyć i dostosowywać obrazy, a następnie instalować je na komputerach.
- *Transport Server* (*Serwer transportu*) — funkcja, która pozwala tworzyć obszary nazw multiemisji, które służą do przesyłania danych (w tym obrazów systemu operacyjnego) z serwera autonomicznego.

  Należy wybrać obie opcje.



Rysunek 6.163. Kreator wyboru instalowanych usług

4. W następnym oknie należy potwierdzić instalację usługi (rysunek 6.164).



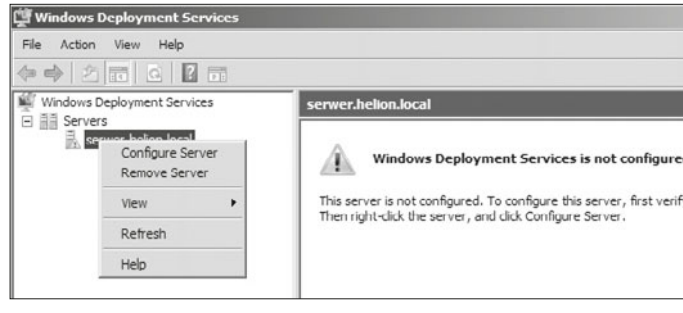
Rysunek 6.164. Podsumowanie instalowanej usługi

5. Jeżeli wszystko jest w porządku, instalacja powinna zakończyć się sukcesem.

Konfiguracja serwera WDS

Po instalacji serwera należy go skonfigurować. Aby to zrobić, z *Administration Tools* (*Narzędzia administracyjne*) należy wybrać *Windows Deployment Services* (*Usługi wdrażania systemu Windows*) lub *Start*/*Uruchom* i wpisać `wdsmgmt.msc` (konsola WDS) (rysunek 6.165).

Rysunek 6.165. Okno zarządzania usługą WDS

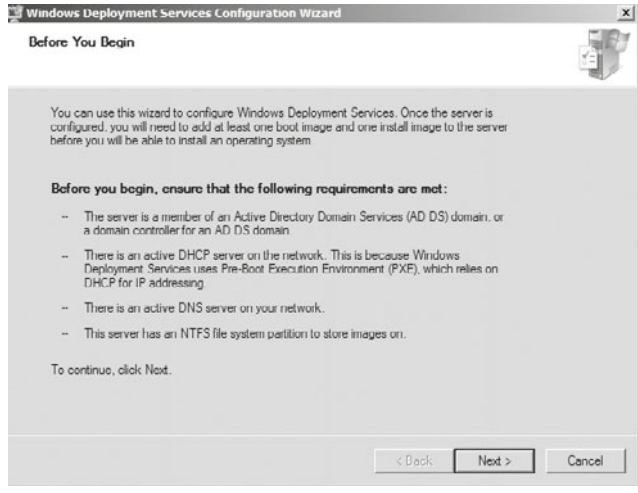


1. Przed rozpoczęciem konfiguracji trzeba się upewnić, czy są spełnione następujące wymagania (rysunek 6.166):

- na serwerze musi być zainstalowana usługa katalogowa, DHCP oraz DNS;
- na serwerze muszą być poprawnie skonfigurowane usługi DHCP i DNS; na serwerze znajduje się partycja systemu NTFS, na której zostaną zapisane obrazy.

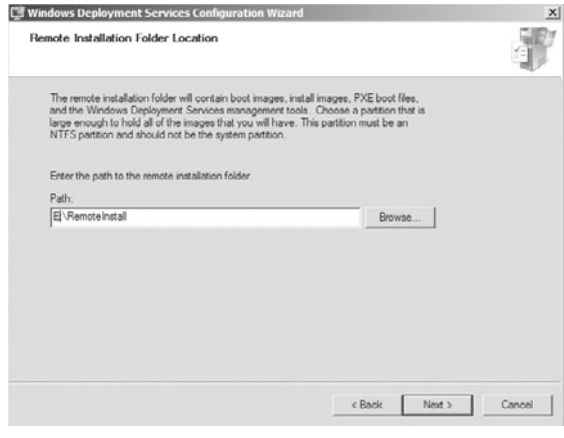
Jeżeli są spełnione powyższe wymagania, to należy kliknąć *Next* (*Dalej*).

Rysunek 6.166. Okno kreatora konfiguracji WDS z informacją o wymaganiach



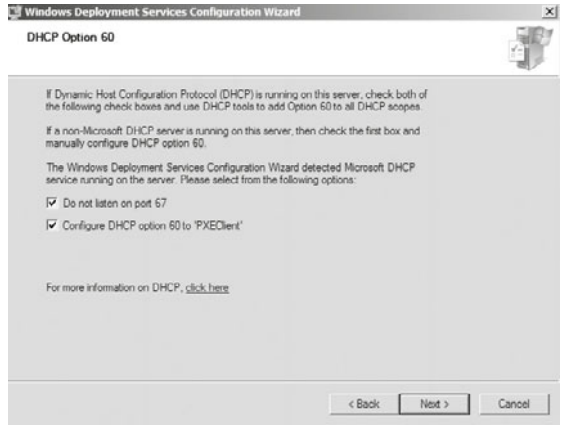
2. W kolejnym oknie konfiguracji (rysunek 6.167) należy wskazać lokalizację folderu instalacji zdalnej. W tym folderze będą zapisywane przygotowane obrazy systemów. Domyślnie jest to *C:\RemoteInstall*. Należy zmienić ją na partycję, na której będą przechowane obrazy — nie powinna to być partycja systemowa.

Rysunek 6.167. Okno kreatora konfiguracji katalogu przechowującego obrazy



3. W kolejnym kroku kreatora (rysunek 6.168) należy skonfigurować opcje DHCP. Do poprawnego działania tej usługi niezbędny jest protokół DHCP. Zaznaczamy obie opcje. W przypadku gdy serwer DHCP nie jest serwerem Microsoftu, wybieramy tylko pierwszą.

Rysunek 6.168. Konfiguracja opcji DHCP

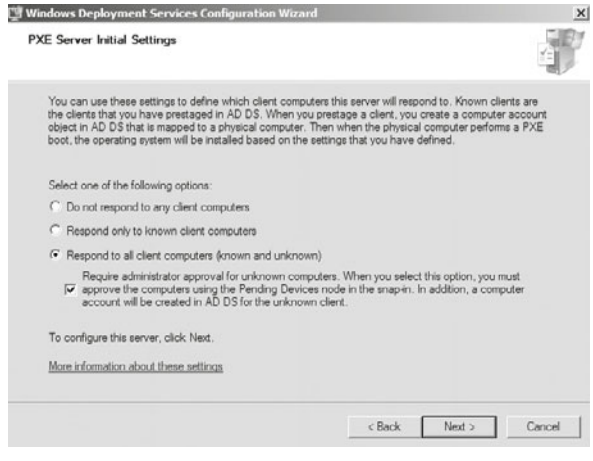


4. W kolejnym oknie kreatora należy zdefiniować ustawienia Preboot Execution Environment (PXE). Za pomocą poniższych ustawień definiuje się sposób odpowiedzi dla komputerów klienckich (rysunek 6.169):

- Pierwsza opcja spowoduje brak odpowiedzi podczas rozruchu środowiska PXE (*Do not respond to any client computer* (*Nie odpowiadaj żadnym komputerom klienckim*)).
- Druga opcja spowoduje uruchomienie PXE tylko na komputerach dodanych do domeny (*Respond only to known client computer* (*Odpowiadaj tylko znanym komputerom klienckim*)).
- Trzecia opcja pozwoli na uruchomienie ww. środowiska na komputerach z oraz spoza domeny (*Respond to all client computer* (*known and unknown*) (*Odpowiadaj wszystkim komputerom klienckim* (*znanym i nieznanym*))).

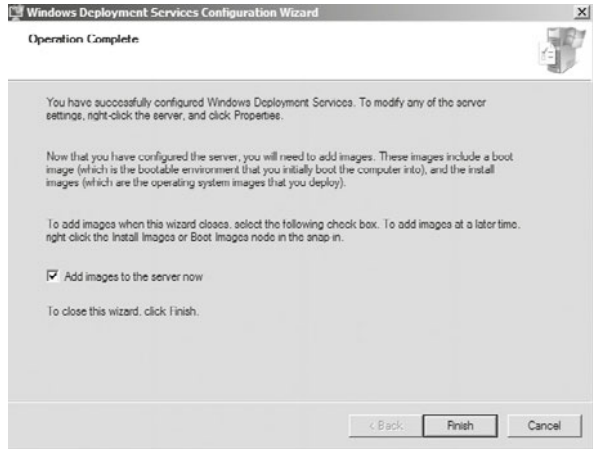
Wybierając opcję trzecią, dodatkowo trzeba zatwierdzić komputer przy użyciu zakładki *Pending devices* (*Urządzenia oczekujące*) znajdującej się w przystawce *Windows Deployment Services* (*Usługi wdrażania systemu Windows*). Należy zaznaczyć opcję trzecią i przejść do następnego kroku poprzez kliknięcie *Next* (*Dalej*). Usługa zostaje skonfigurowana.

Rysunek 6.169. Ustawienia PXE



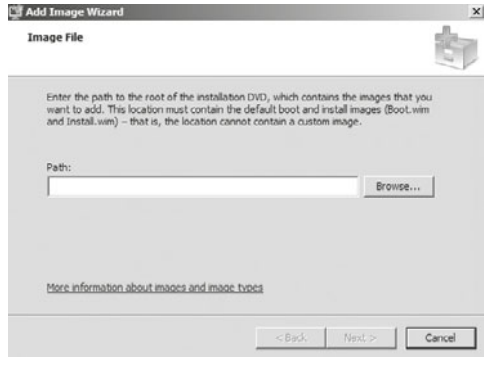
5. Kolejny krok polega na dodaniu obrazu do serwera (rysunek 6.170). Należy włożyć do napędu DVD dysk instalacyjny systemu, np. Windows 7, i przejść do kolejnego kroku — Kreatora dodawania obrazu.

Rysunek 6.170. Okno kreatora dodawania obrazu

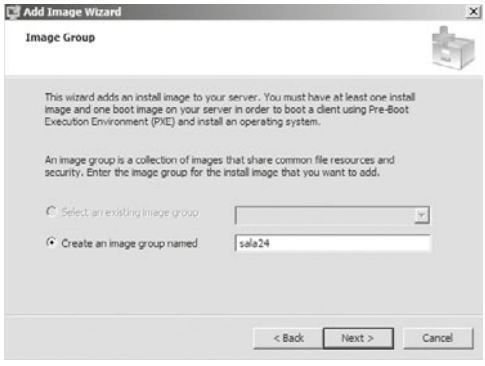


6. Plik *.wim* (*Windows Image File*) jest skompresowanym plikiem obrazu umożliwiającym instalację systemu Windows. Pliki niezbędne do tworzenia obrazu (*boot.wim* i *install.wim*) są umieszczone w katalogu instalacyjnym systemu operacyjnego; począwszy od systemu Vista, jest to katalog *sources*. Aby dodać obraz, w oknie kreatora dodawania obrazu należy podać ścieżkę do napędu DVD (rysunek 6.171).

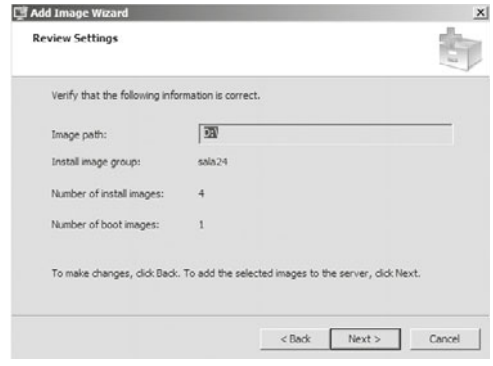
Rysunek 6.171. Katalog przechowywania obrazów



7. W następnym kroku (rysunek 6.172) należy utworzyć grupę obrazów, do której zostaną przyporządkowane pliki instalacyjne. Tworzymy grupę *sala24*.
8. Końcowym oknem w kreatorze dodawania obrazów jest okno podsumowania (rysunek 6.173). Jest to ostatni etap, w którym można dokonać zmian. Jeśli wszystko jest w porządku, należy kliknąć *Next* (*Dalej*). Trwa dodawanie obrazów systemu Windows.

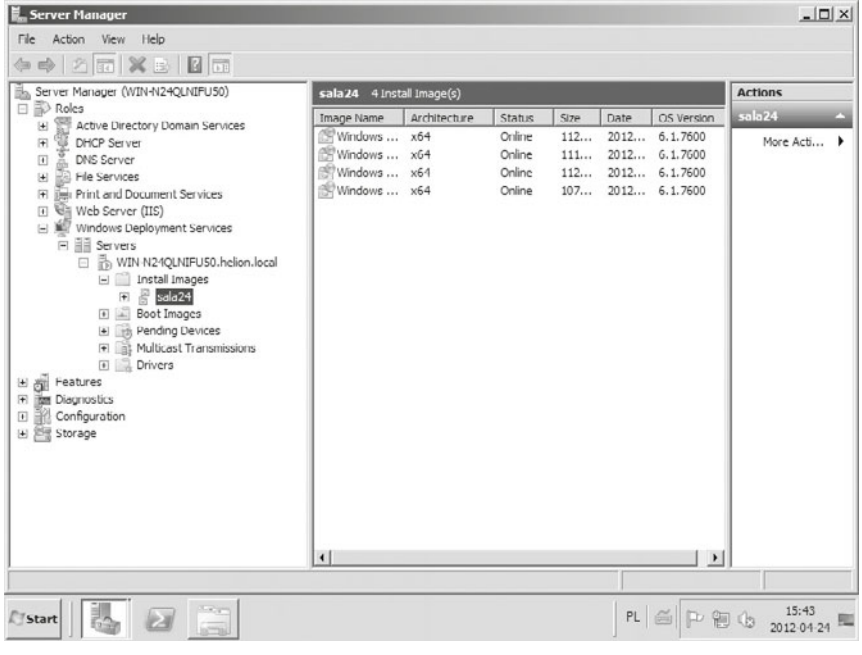


Rysunek 6.172. Tworzenie grupy obrazów



Rysunek 6.173. Podsumowanie dodawania obrazów

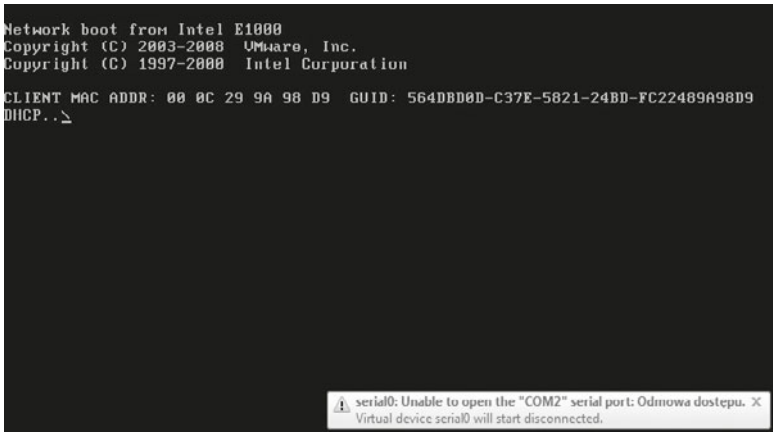
9. W celu przeprowadzenia konfiguracji należy w programie *Server Manager* (*Menedżer serwera*) wybrać rolę *Windows Deployment Services* (*Usługi wdrażania systemu Windows*), gdzie widnieje grupa *sala24*, do której dodane zostały 4 obrazy 64-bitowej wersji systemu (plik *install.wim*) (rysunek 6.174). Natomiast w zakładce *Boot Images* (*Obrazy rozruchowe*) został dodany plik rozruchu PXE (*boot.wim*).



Rysunek 6.174. Zarządzanie przygotowanymi obrazami

Instalacja systemu Windows 7 z wykorzystaniem obrazów przygotowanych w WDS

1. Po uruchomieniu komputera, na którym ma być zainstalowany system, przy wykorzystaniu usługi WDS zostanie uruchomiony agent PXE. Rozpocznie on od pobrania adresu sieciowego z serwera w celu podłączenia się do usługi WDS oraz obrazu, z którego nastąpi instalacja (rysunek 6.175).



Rysunek 6.175. Bootowanie systemu za pomocą PXE

2. W dalszej kolejności nastąpi nadzorowana instalacja, podczas której należy:
   - wybrać język,
   - wprowadzić ustawienia regionalne,
   - określić nazwę instalowanego systemu,
   - nadać hasło administratora,
   - podać klucz produktu,
   - zaakceptować warunki licencji,
   - skonfigurować automatyczne aktualizacje,
   - ustawić datę i godzinę.
3. Aby uniknąć wprowadzania tych informacji, można utworzyć plik XML, który pozwoli przeprowadzić nienadzorowaną instalację systemu. Ważne jest, by tak przygotowany plik był podłączony do obrazu, z którego ma być zainstalowany system.

ĆWICZENIA

1. Zainstaluj i skonfiguruj usługę WDS.
2. Dodaj obraz Windows 7 do usługi.

PYTANIA

1. Omów usługę WDS.
2. Co to jest PXE?
3. Wymień rozszerzenia plików używanych do tworzenia obrazów.
4. Podaj nazwę pliku obrazu.

6.7. Konfiguracja usług internetowych

6.7.1. Serwer WWW

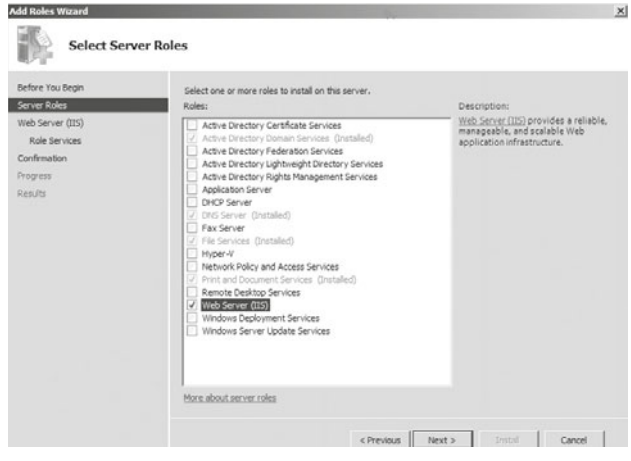
DEFINICJA

Serwer sieci WEB (ang. *Internet Information Services*, *IIS*) — jest zbiorem usług internetowych udostępnianych przez systemy Windows. Pełni funkcje m.in. serwera FTP oraz HTTP.

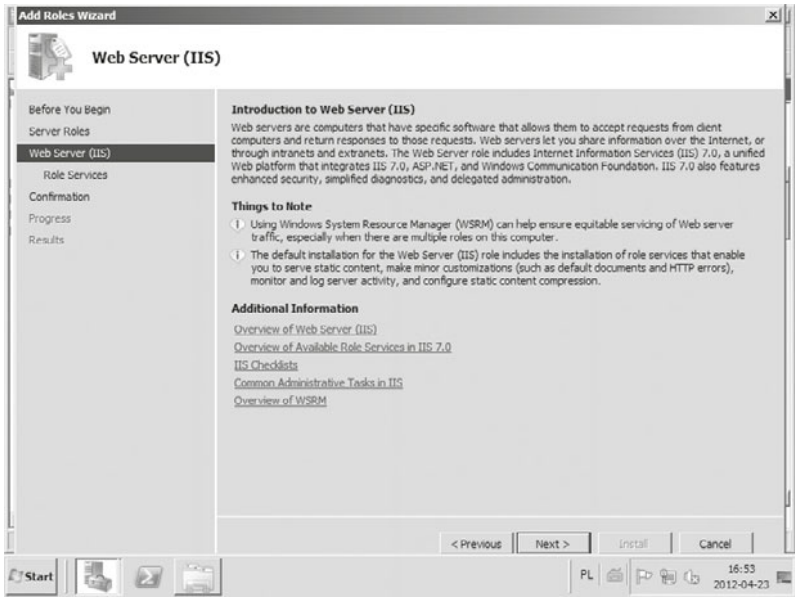
IIS jest jedną z ról Windows Server 2008 R2. Aby go zainstalować, należy dodać nową rolę.

1. W kreatorze ról należy wybrać opcję *WEB Server* (*IIS*) (*Serwer sieci WEB*) (rysunek 6.176).

Rysunek 6.176. Dodawanie roli IIS



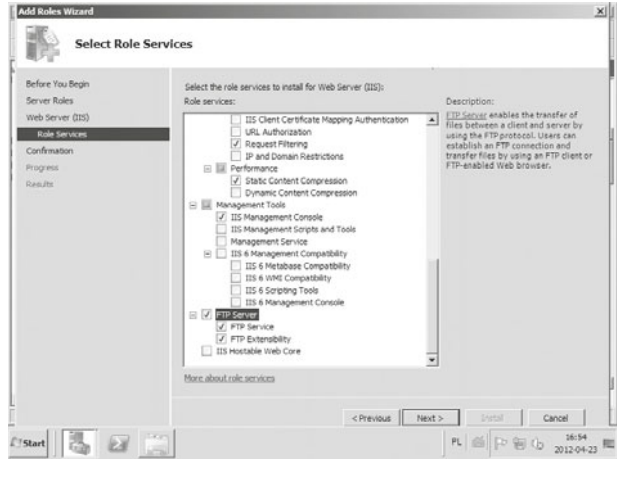
2. W kolejnym oknie kreatora dodawania ról (rysunek 6.177) wyświetli się krótka informacja na temat usługi sieci Web (IIS). Należy kliknąć *Next* (*Dalej*).



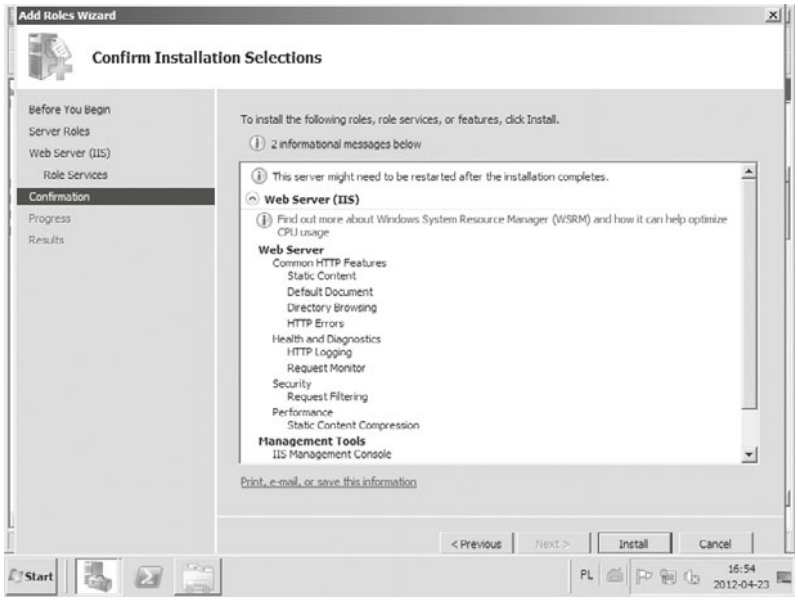
Rysunek 6.177. Informacja na temat instalowanej usługi

3. W kolejnym kroku należy wybrać komponenty wchodzące w skład serwera (rysunek 6.178). Poza podstawowymi, jak serwer http czy ftp, można zainstalować m.in. funkcje projektowania aplikacji odpowiedzialne za uruchamianie dynamicznych skryptów po stronie serwera, funkcje kondycji i diagnostyki zapewniające narzędzia diagnostyczne i monitorujące serwer web, funkcje wydajności umożliwiające przyspieszenie serwowania stron WWW czy funkcje zarządzania pozwalające na zaawansowane administrowanie usługą.

Rysunek 6.178. Wybór komponentów wchodzących w skład usługi

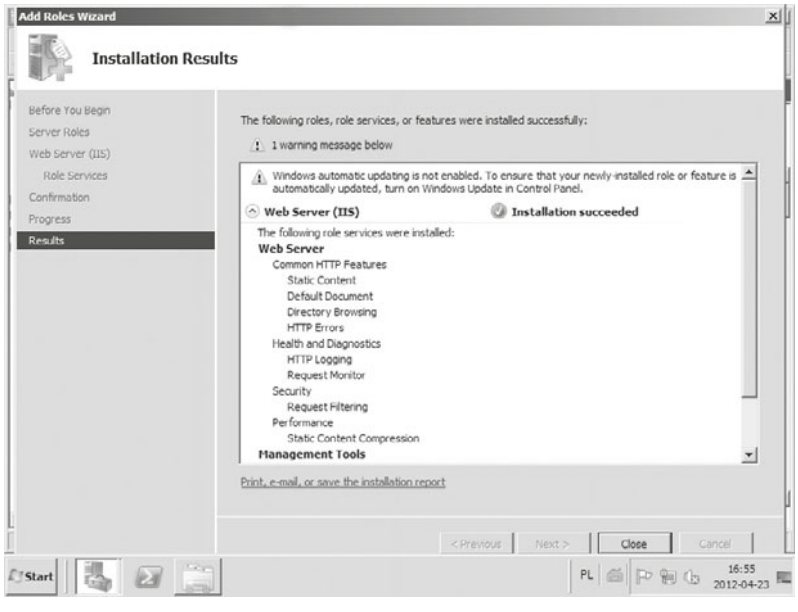


4. Po wybraniu opcji *Install* (*Instaluj*) na stronie podsumowującej wybrane komponenty (rysunek 6.179) rozpoczyna się właściwy proces instalacji serwera.



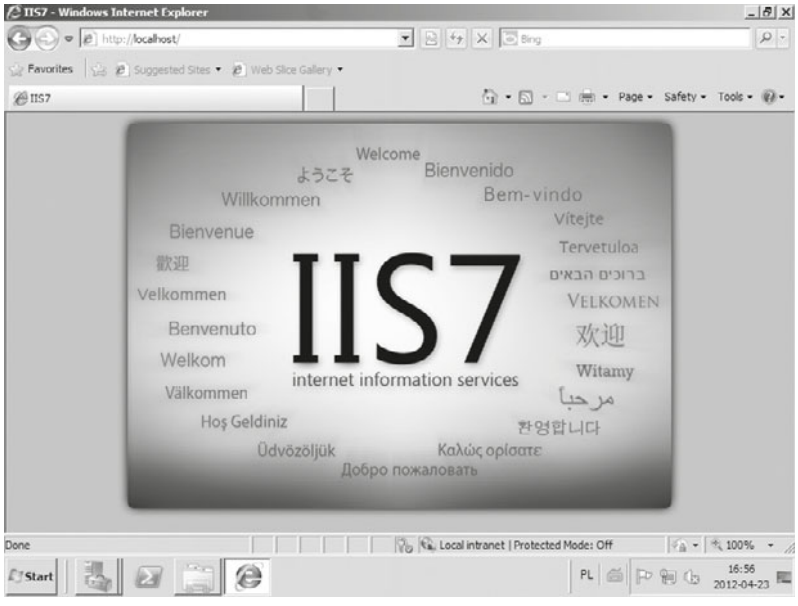
Rysunek 6.179. Informacja na temat instalowanych usług

5. W ostatnim oknie jest wyświetlane potwierdzenie zainstalowania usługi (rysunek 6.180).



Rysunek 6.180. Potwierdzenie zainstalowania usługi

6. Aby przetestować działanie serwera Web, należy w przeglądarce internetowej uruchomionej na serwerze otworzyć adres *http://localhost* (rysunek 6.181).

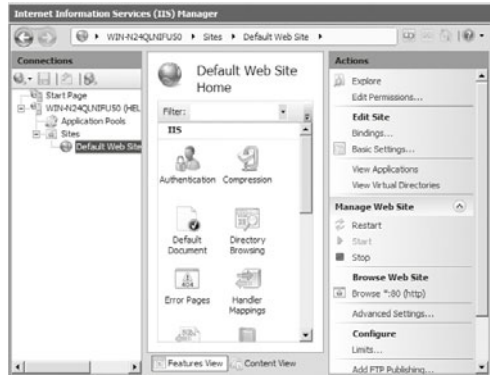


Rysunek 6.181. Strona startowa usługi IIS

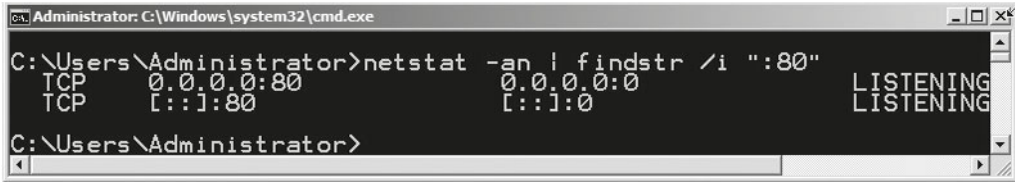
Wszystkie pliki związane z konfiguracją oraz ze stroną, która jest wyświetlana jako domyślna, znajdują się w katalogu *C:/inetpub/wwwroot*.

W celu skonfigurowania usługi należy uruchomić Internet Information Services Manager (Menedżer Internetowych Usług Informacyjnych) znajdujący się w menu *Administrative tools* (*Narzędzia Administracyjne*). Konfiguracja obejmuje m.in. umieszczenie katalogów zawierających serwisy www na dysku serwera, mechanizmy uwierzytelniania, certyfikaty SSL czy strony błędów (rysunek 6.182).

Rysunek 6.182.
Serwer WWW (IIS)



Po zakończeniu instalacji na pierwszy rzut oka nic nowego się nie pojawia. Jeżeli jednak sprawdzi się otwarte porty TCP/IP, korzystając z polecenia `netstat`, okaże się, że serwer działa i nasłuchuje na porcie 80 (rysunek 6.183).



Rysunek 6.183. Wynik działania polecenia netstat

Konfiguracja serwera IIS

W panelu przystawki menedżera internetowych usług informacyjnych (IIS) są widoczne następujące katalogi lub węzły:

- *Start Page* (*Strona początkowa*) — pierwsza pozycja, która pełni funkcję cyfrowego pulpitu sterowania zawierającego aktualne informacje o połączeniach, serwerach i związanych z nimi zadaniach.
- Serwer — główne miejsce, w obrębie którego zarządza się właściwościami i funkcjami serwera.
- *Application Pools* (*Pule aplikacji*) — obszary fizycznej pamięci przydzielonej aplikacjom działającym w obrębie puli. Pule oddzielają aplikacje od reszty zasobów pamięci wykorzystywanej przez inne usługi serwera IIS. Zapewnia to większą niezawodność oraz bezpieczeństwo, oznacza jednak konieczność fizycznego zwiększenia ilości pamięci RAM.
- *Sites* (*Witryny WWW*) — w tym katalogu znajdują się wszystkie witryny obsługiwane przez serwer WWW. Domyślna witryna jest utworzona podczas instalacji serwera (*Default Web Site*) (jest dostępna pod adresem *http://localhost*).
- Witryny FTP — w tym katalogu zlokalizowane są wszystkie witryny FTP obsługiwane przez serwer WWW.

Najpierw należy skonfigurować opcje dostępne z poziomu serwera, a dopiero później opcje dostępne z poziomu strony. Zachowując taką kolejność konfigurowania każda nowa strona odziedziczy ustawienia i już w chwili utworzenia będzie poprawnie skonfigurowana oraz gotowa do pracy. Praktycznym rozwiązaniem jest ustawienie właściwości na poziomie całego serwera na maksymalnie bezpieczny. Jeżeli gdzieś poziom taki przeszkadza w poprawnym funkcjonowaniu serwisu WWW, można go zmienić dla danego serwisu.

Kolejne opcje, które powinniśmy skonfigurować, to:

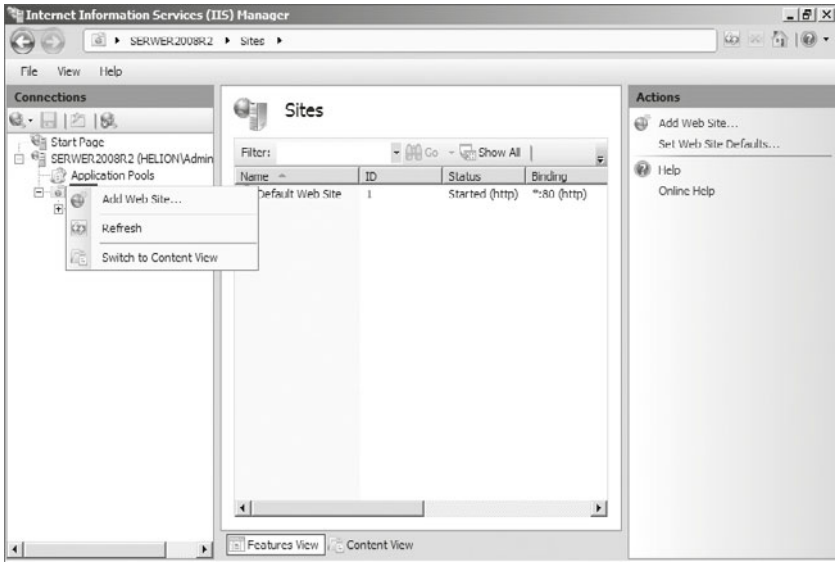
- Poziom serwera — użytkownik ma do dyspozycji opcje *start*, *stop* oraz *restart*. Uruchamiają one i zatrzymują cały serwer HTTP.
- *Authentication* (*Autoryzacja*) — opcje dostępne w tym widoku zależą bezpośrednio od wybranych w czasie instalacji metod uwierzytelniania. Dla metody Anonymous najważniejszym parametrem jest nazwa konta, którym IIS się posługuje, odczytując strony z dysku. Domyślnie wartość parametru jest równa IUSR i to ta grupa musi mieć prawa odczytu katalogów, w których znajdują się pliki html.

- *Compression* (*Kompresja*) — strony są zapisywane w skompresowanej postaci i tak wysyłane klientowi. Dzięki temu znacząco zmniejsza się obciążenie łącza. Możemy też ustalić minimalny rozmiar pliku, który jest poddawany kompresji. Jest to ważne dlatego, że pliki bardzo małe nie zyskują na kompresji na tyle dużo, żeby operacja taka była opłacalna. Możemy również zmienić domyślny katalog, w którym przechowywane są skompresowane dane, oraz limit objętości skompresowanych danych na dysku.
- *Default Document* (*Domyślny dokument*) — lista dokumentów domyślnych z rozszerzeniami, które zwraca serwer, gdy użytkownik wprowadzi np. *http://localhost czy http://helion.local*.
- *Directory Browsing* (*Przeglądanie katalogów*) — odpowiada za uprawnienia do przeglądania katalogów znajdujących się na serwerze WWW. Ze względów bezpieczeństwa na poziomie serwera należy wyłączyć przeglądanie katalogów i jedynie w konkretnych katalogach włączać tylko wtedy, kiedy jest to potrzebne. Opcja ta jest domyślnie wyłączona. Serwer IIS najpierw sprawdza obecność domyślnego dokumentu i jeśli go nie znajduje, pozwala na przeglądanie katalogu. W opcjach IIS Manager dotyczących przeglądania katalogów określić można, które z widocznych na rysunku parametrów pliku (data, czas, rozmiar i rozszerzenie) są wyświetlane. Należy pamiętać, że nieuzasadnione wyświetlanie katalogów serwera jest uznawane za poważne naruszenie reguł bezpiecznej konfiguracji.
- *Error Pages* (*Strony błędów*) — protokół HTTP określa, że dla każdego zapytania od klienta w odpowiedzi zwracanej z serwera powinien się znaleźć kod liczbowy informujący, jakiego rodzaju jest to odpowiedź. W normalnych warunkach kod ten ma numer 200 i oznacza, że wszystko poszło dobrze. W przypadku błędu serwer może zamiast samego kodu wysłać również jakieś dane. Przykładowo błąd 404 informuje klienta, że na serwerze nie ma strony, o którą zapytał.
- *Logging* (*Logowanie zapytań*) — jedna z najważniejszych funkcji, która powinna być włączona w każdym serwerze. Nawet jeśli logi nie wydają się w danym momencie potrzebne, na pewno w przyszłości zdarzy się tak, że trzeba będzie do nich sięgnąć.

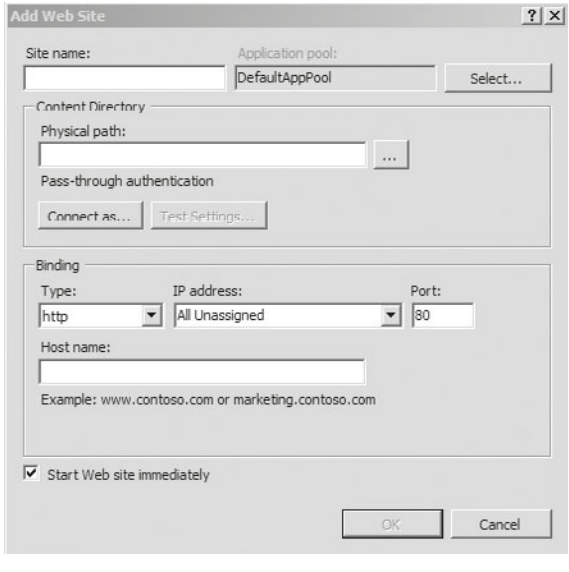
Gdy już skonfigurowaliśmy lub sprawdziliśmy ustawienia na naszym serwerze, należy utworzyć nową stronę dla naszej usługi. W celu rozpoczęcia procesu tworzenia nowej witryny WWW należy w pierwszym kroku w oknie *Internet Information Services (IIS) Manager* (*Menedżer internetowych usług informacyjnych (IIS)*) prawym przyciskiem kliknąć *Sites* (*Witryny*), a następnie opcję *Add Web Site* (*Dodaj witrynę sieci Web*) (rys. 6.184).

Pojawi się okno *Add Web Site* (*Dodawanie witryny sieci Web*) (rysunek 6.185). Należy wprowadzić nazwę witryny, np. nowastrona. W sekcji *Content Directory* (*Katalog zawartości*) należy wprowadzić ścieżkę identyfikującą fizyczną lokalizację katalogu dla nowej witryny WWW. Może to być domyślny folder *c:\inetpub\wwwroot*. Następnie trzeba zdecydować, czy nowa witryna będzie używać protokołu http, czy https, podać dla niej adres IP lub pozostawić pole adresu IP puste. Dodatkowo należy określić port — można zostawić domyślny lub ustawić inny, na którym będzie dostępna witryna. Można również podać nagłówek dla nowo tworzonej witryny. Po zamknięciu okna

strona zostanie uruchomiona automatycznie, ponieważ jest zaznaczona domyślnie opcja *Start Web Site immediately* (*Uruchom witrynę sieci Web natychmiast*). Stronę wywołujemy, wpisując *http://localhost*.



Rysunek 6.184. Menedżer IIS. Dodawanie nowej strony



Rysunek 6.185. Ustawienia w oknie dialogowym Add Web Site (Dodawanie witryny sieci Web)

ĆWICZENIA

1. Zainstaluj serwer WWW i skonfiguruj go.
2. Utwórz własną stronę startową.

PYTANIA

1. Jaki protokół umożliwia oglądanie stron WWW?
2. Pod jakim adresem znajduje się strona startowa?
3. Na jakich portach musi przepuszczać ruch brama internetowa, aby użytkownicy sieci lokalnej mogli przeglądać strony WWW przy użyciu protokołów HTTP i HTTPS?

6.7.2. FTP

DEFINICJA

Serwer FTP (ang. *File Transfer Protocol*) umożliwia udostępnianie plików i folderów w internecie.

Domyślny katalog dla udostępnionych zasobów to *inetpub\ftproot* w katalogu głównym dysku systemowego.

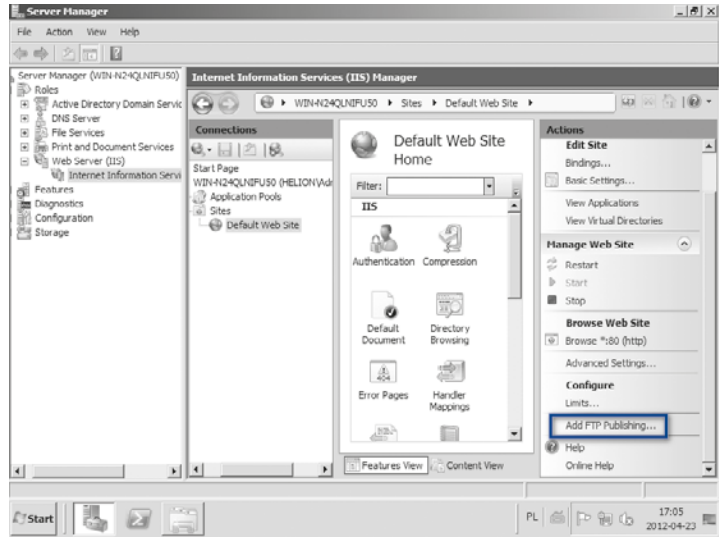
W celu spersonalizowania praw dostępu do zasobów należy utworzyć konta użytkowników w systemie. Wcześniej utworzeni użytkownicy systemu też będą mogli zalogować się na serwer FTP, jednak ponieważ w protokole FTP hasła są przesyłane w postaci niezaszyfrowanej i mogą łatwo zostać „podsłuchane" (szczególnie w sieciach z koncentratorami), powinno się korzystać tylko ze specjalnie do tego celu utworzonych użytkowników oraz praw przydzielonych na poziomie zabezpieczeń NTFS.

Aby dodać serwis FTP w usłudze IIS, należy uruchomić konsolę zarządzania IIS (rysunek 6.186) i wybrać opcję *Add FTP Publishing* (*Dodaj Publikację FTP*).

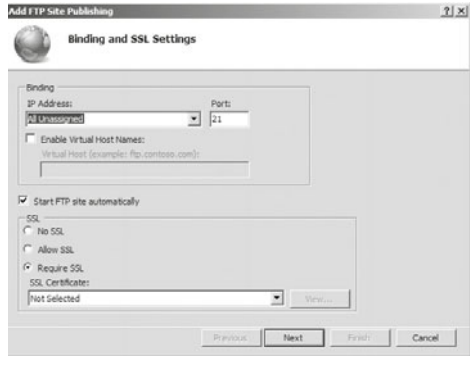
Zostanie uruchomiony kreator konfiguracji usługi. W pierwszym oknie należy podać adres IP oraz port, na którym usługa będzie aktywna (rysunek 6.187). Jeżeli chcemy, aby użytkownicy logowali się bezpiecznie, należy zaznaczyć opcję *Allow SSL* (*Dostęp przez SSL*).

W następnym oknie należy określić, w jaki sposób będzie przebiegać identyfikacja osób korzystających z serwera oraz z jakimi uprawnieniami będą się one logowały (rysunek 6.188).

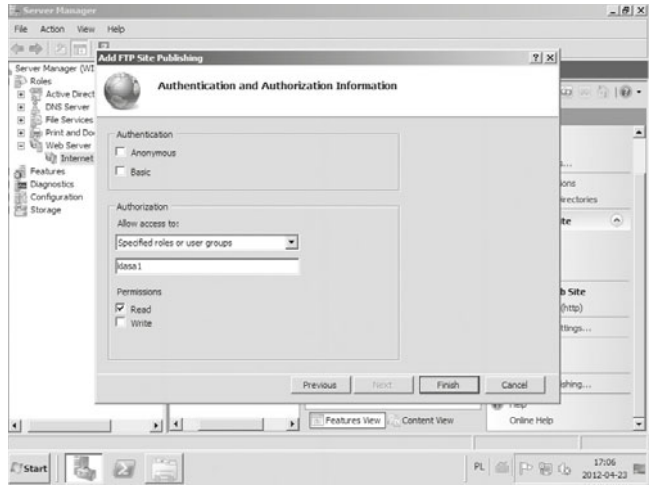
Rysunek 6.186.
Publikacja serwera FTP



Rysunek 6.187.
Konfiguracja usługi FTP



Rysunek 6.188.
Konfiguracja autoryzacji oraz uprawnień



Połączenie z serwerem FTP zapewnia program — klient FTP. W systemie Windows jest dostępny tekstowy klient FTP, z którego można korzystać w wierszu polecenia, oraz klient wbudowany do programu Internet Explorer.

Klient tekstowy FTP może być uruchomiony z wiersza poleceń (rysunek 6.189). Aby połączyć się z wybranym serwerem, należy wprowadzić komendę:

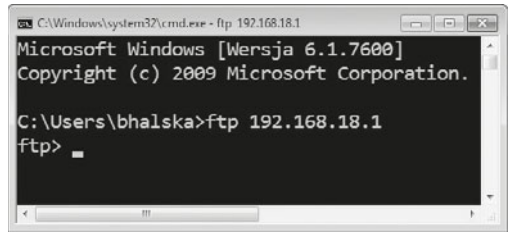
```
ftp <adres_serwera>
```

np.:

```
ftp 192.168.18.1
```

Po połączeniu z serwerem użytkownik zostanie zapytany o login i hasło. Po udanej autoryzacji można korzystać z zasobów serwera.

Rysunek 6.189.
Klient tekstowy FTP



Nawigacja po folderach jest podobna do tej znanej z wiersza poleceń. Najczęściej używane komendy w tekstowych klientach ftp to:

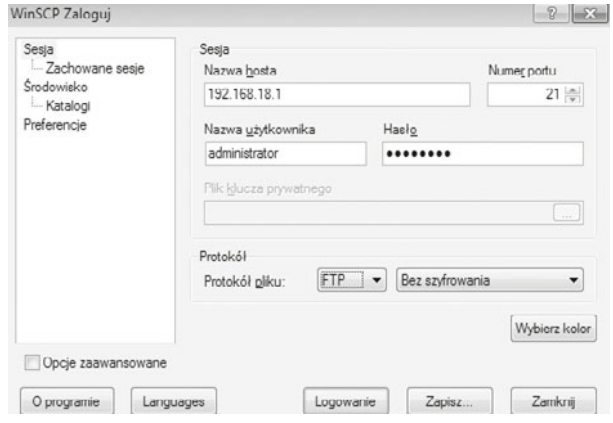
- `cd` — zmiana katalogu zdalnego,
- `lcd` — zmiana katalogu lokalnego,
- `dir` — wyświetla zawartość bieżącego katalogu,
- `mkdir` — tworzy katalog na serwerze,
- `get` — pobiera wybrany plik na dysk lokalny,
- `put` — wysyła na serwer plik z dysku lokalnego,
- `pwd` — wyświetla nazwę bieżącego katalogu na serwerze,
- `ascii` — zmienia tryb transmisji na znakowy — wykorzystywany przy kopiowaniu plików tekstowych,
- `binary` — zmienia tryb transmisji na binarny — zalecany dla plików innych niż tekstowe,
- `bye` — zamyka połączenie z serwerem.

Pliki pobierane z serwera są zapisywane do katalogu, z którego został uruchomiony klient FTP.

W internecie jest dostępnych wiele programów — klientów FTP, które ułatwiają korzystanie z udostępnianych zasobów. Jednym z nich jest program WinSCP (*www.winscp.net*). Aby połączyć się z serwerem FTP, należy skonfigurować połączenie do serwera. Po uruchomieniu programu wystarczy podać adres serwera, nazwę użytkownika oraz hasło i wybrać rodzaj protokołu — FTP dla połączeń nieszyfrowanych lub SFTP dla połączeń

szyfrowanych (rysunek 6.190). Parametry te mogą być zapisane w celu późniejszego wykorzystywania. Po wprowadzeniu danych i wybraniu przycisku *Logowanie* pojawi się ekran zawierający dwa panele — w jednym znajdują się zasoby lokalne, w drugim zasoby udostępnione na serwerze.

Rysunek 6.190. Program WinSCP — klient FTP



Operacje na plikach są przeprowadzane za pomocą klawiszy funkcyjnych. Kopiowanie, przenoszenie plików, zakładanie katalogów jest możliwe zarówno na dysku lokalnym, jak i na serwerze (w zależności od praw dostępu).

Najważniejsze skróty klawiszowe programu WinSCP zostały przedstawione poniżej:

F3 — zapewnia podgląd podświetlonego pliku.

F4 — pozwala na edycję podświetlonego pliku.

F5 — pozwala na kopiowanie podświetlonego pliku lub wielu plików zaznaczonych za pomocą klawisza *Insert* z katalogu wyświetlanego w jednym panelu do katalogu, który jest wyświetlany w drugim panelu.

F6 — przenosi pliki lub zmienia ich nazwy.

F7 — tworzy katalog w katalogu bieżącym.

F8 — usuwa plik lub katalog.

ĆWICZENIA

1. Utwórz w usłudze katalogowej nową grupę o nazwie FTP, dodaj do tej grupy dwóch użytkowników *ftp_1* i *ftp_2*.
2. Utwórz folder FTP, który będzie miejscem publikacji plików.
3. Utwórz w folderze FTP katalogi i zdefiniuj dla nich następujące uprawnienia:
   a. *ftp_1* — pełny dostęp ma tylko użytkownik *ftp_1*,
   b. *ftp_2* — pełny dostęp ma tylko użytkownik *ftp_2*,
   c. *sterowniki* — prawa do odczytu mają obaj użytkownicy.

PYTANIA

1. Co to jest usługa FTP?
2. Na jakim porcie jest aktywna usługa FTP?
3. Wymień programy, które umożliwią połączenie z serwerem FTP.
4. Jakie polecenie pozwala połączyć się z serwerem FTP z konsoli?

6.7.3. Serwer pocztowy

Jest to usługa, która nie jest instalowana jako dodatkowa rola, ale jako oddzielny program. Gdy planuje się utworzenie serwera dla wąskiej grupy użytkowników, można skorzystać z bezpłatnego oprogramowania, takiego jak MailEnable (*www.mailenable.com*). Program oprócz hostingu skrzynek użytkowników dostępnych poprzez protokół POP3 i SMTP oferuje także webmail wykonany w technologii .NET. Dostępnych jest też wiele innych funkcji administracyjnych związanych z doręczaniem e-maili, autoryzacją użytkowników oraz funkcjonowaniem serwera. Administracja jest bardzo wygodna i przebiega z poziomu konsoli MMC, a na uwagę zasługuje to, że MailEnable potrafi uwierzytelniać użytkowników z wykorzystaniem Active Directory.

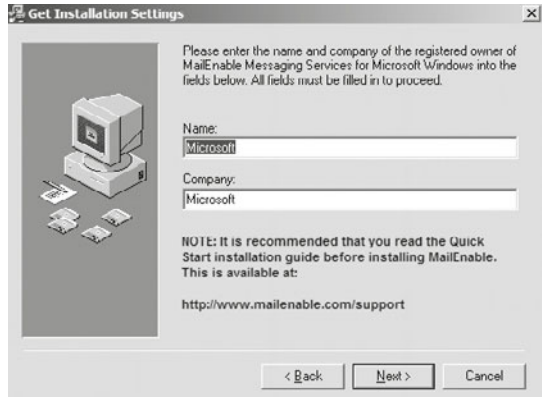
Aby zainstalować usługę, należy pobrać program, a następnie dokonać instalacji, tak jak w poniższych krokach:

1. W pierwszym kroku wyświetla się informacja o usłudze, którą zamierzamy zainstalować (rysunek 6.191).

Rysunek 6.191. Kreator instalacji usług MailEnable

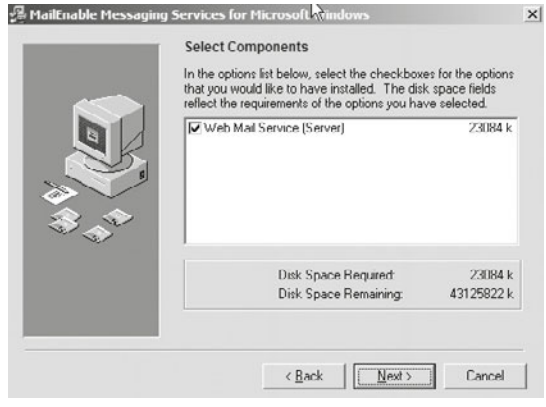
2. W następnym oknie należy podać nazwę użytkownika oraz firmy, na którą program będzie zarejestrowany (rysunek 6.192). W dalszej kolejności są wyświetlane warunki korzystania z oprogramowania.

Rysunek 6.192.
Instalacja usługi



3. Kolejne okno (rysunek 6.193) wymaga wybrania komponentu do instalacji — *Web Mail Service*, a następnie należy wskazać folder do instalacji oprogramowania oraz nazwę grupy w menu *Start*, w której oprogramowanie będzie dostępne.

Rysunek 6.193.
Wybór instalowanych usług

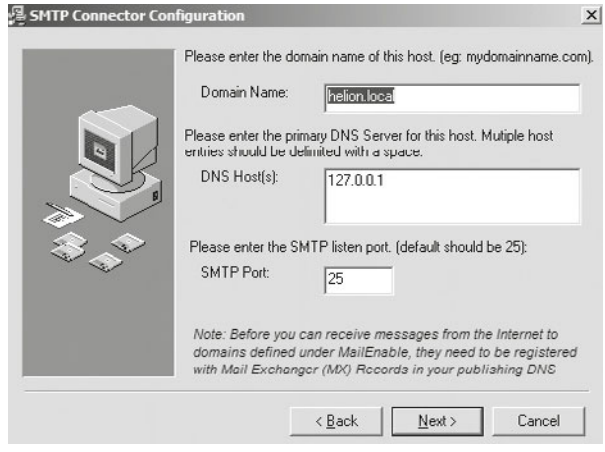


4. Kolejnym elementem, który należy skonfigurować, jest nazwa serwera oraz hasło (rysunek 6.194).

Rysunek 6.194.
Nadanie nazwy i hasła dla instalowanej usługi

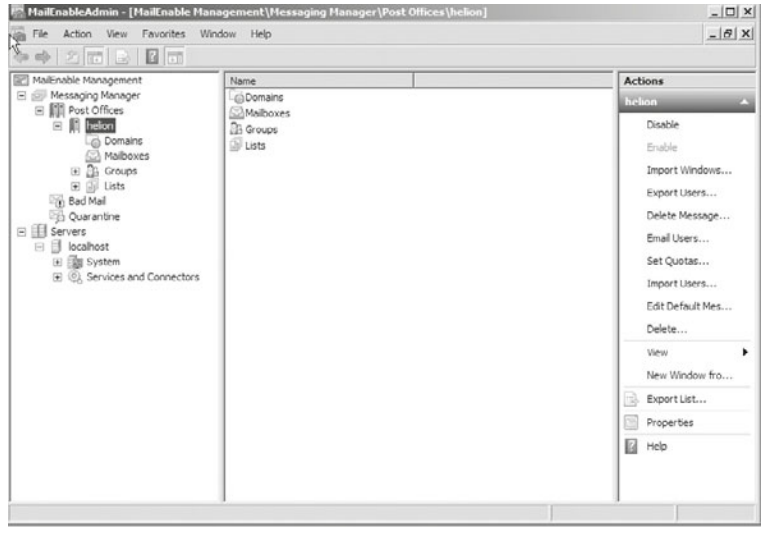
5. Podczas instalacji należy skonfigurować serwer SMTP (protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w internecie) dla uruchamianej usługi (rysunek 6.195).

Rysunek 6.195. Konfiguracja serwera SMTP



Administracja przebiega z poziomu konsoli MMC (rysunek 6.196). Program MailEnable potrafi uwierzytelniać użytkowników z wykorzystaniem usługi katalogowej, co bardzo ułatwia administrację.

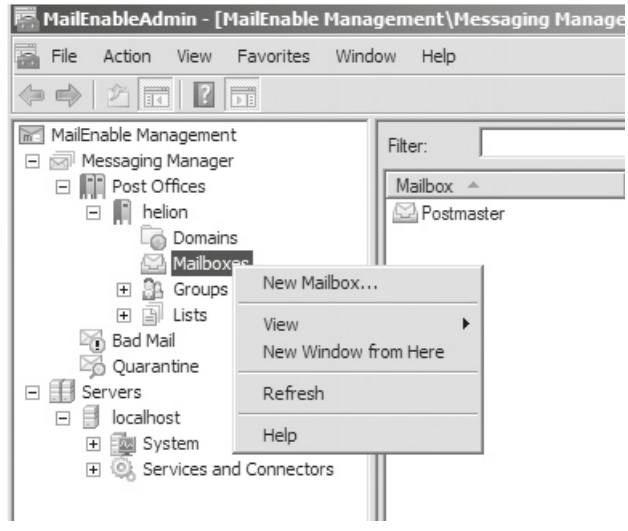
Rysunek 6.196. Konsola do zarządzania usługą



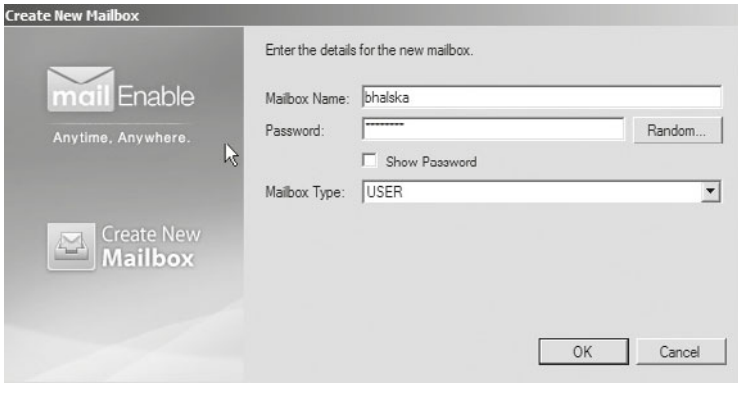
Program pozwala m.in. na tworzenie wielu domen w ramach jednego serwera pocztowego (opcja *Create domain*), tworzenie skrzynek pocztowych (*Create Mailbox*), grup użytkowników (*Create a Group*), import użytkowników (*Import Users*) czy ustawienie ograniczeń dyskowych dla skrzynek (*Set Quota*).

Aby założyć skrzynkę mailową dla użytkownika, należy kliknąć prawym przyciskiem myszy *Mailboxes* i wybrać opcję *New Mailbox* (rysunek 6.197).

Rysunek 6.197. Tworzenie nowej skrzynki pocztowej

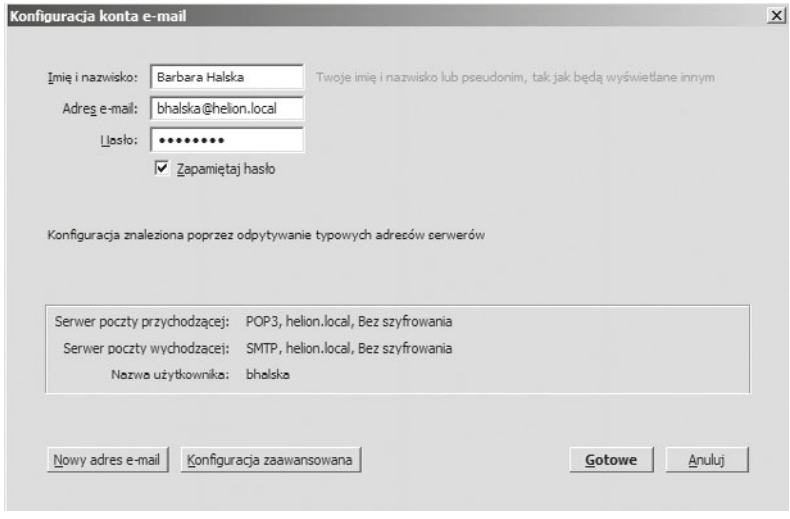


Pojawi się okno, w którym zostaniemy poproszeni o podanie loginu oraz hasła do skrzynki pocztowej (rysunek 6.198).



Rysunek 6.198. Konfigurowanie skrzynki pocztowej

Po zatwierdzeniu konfiguracji zostanie utworzone konto. Teraz już tylko trzeba zainstalować klienta pocztowego, który umożliwi nam wysyłanie i odbieranie maili. Dostępnych jest wiele klientów, program wykorzystany w przykładzie to Mozilla Thunderbird 17.0.6, który można pobrać ze strony *http://www.mozilla.org/pl/thunderbird*. Po zainstalowaniu klienta należy skonfigurować nową pocztę, podając nazwę właściciela konta pocztowego, adres e-mail oraz adresy serwerów SMTP i POP3 (rysunek 6.199).



Rysunek 6.199. Konfiguracja klienta pocztowego

ĆWICZENIA

1. Zainstaluj serwer pocztowy i skonfiguruj go.
2. Skonfiguruj konta dla użytkowników.
3. Zainstaluj klienta pocztowego na stacjach roboczych.

PYTANIA

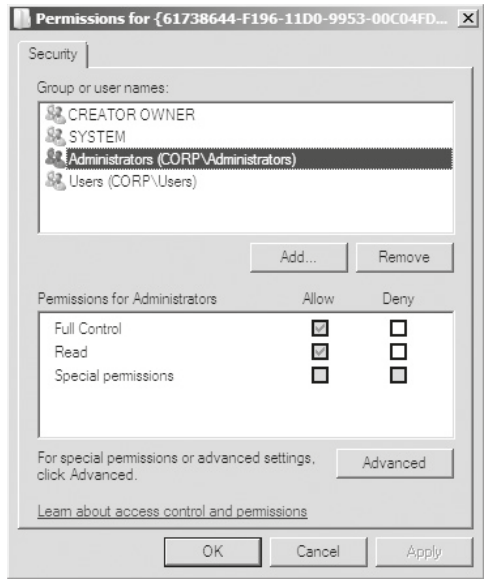
1. Omów protokół SMTP, POP3.
2. Wymień port dla usługi SMTP.

6.8. Bezpieczeństwo

6.8.1. Uprawnienia

Uprawnienia określają, czy dany użytkownik ma dostęp do określonego obiektu i co może z nim zrobić (rysunek 6.200).

Rysunek 6.200.
Uprawnienia



Uprawnienia do zasobów kontrolują dostęp użytkowników do folderów oraz zawartych w nich plików i podfolderów. Mogą być one nadawane lub odbierane pojedynczym użytkownikom oraz grupom użytkowników. Ich wykaz zawierają tabele 6.5 oraz 6.6.

Tabela 6.5. Uprawnienia NTFS do folderów

Uprawnienie	Możliwości
Wyświetlanie zawartości folderu (*List Folder Contents*)	Widok nazw plików i podfolderów w folderze.
Odczyt (*Read*)	Widok plików i podfolderów w folderze oraz przeglądanie własności, uprawnień i atrybutów folderu (*Tylko do odczytu* (*Read-only*), *Ukryty* (*Hidden*), *Archiwalny* (*Archive*), *Systemowy* (*System*)).
Odczyt i wykonywanie (*Read & Execute*)	Przechodzenie przez foldery prowadzące do plików i folderów, nawet przy braku uprawnień do folderów, przez które się przechodzi. Wykonywanie działań, na które zezwalają uprawnienia odczytu i wyświetlanie zawartości folderu.
Zapis (*Write*)	Tworzenie nowych plików i podfolderów w folderze, zmiana atrybutów folderu oraz przeglądanie własności i uprawnień do folderu.
Modyfikacja (*Modify*)	Usuwanie folderu, wykonywanie działań, na które zezwalają uprawnienia zapisu, odczytu i wykonywania.
Pełna kontrola (*Full Control*)	Zmiana uprawnień, przejmowanie na własność oraz usuwanie podfolderów i plików, wykonywanie działań, na które zezwalają pozostałe uprawnienia NTFS do folderów.

Uprawnienia NTFS do plików kontrolują dostęp użytkowników do plików.

Tabela 6.6. Uprawnienia NTFS do plików

Uprawnienie	Możliwości
Odczyt (*Read*)	Odczyt pliku oraz przeglądanie jego własności, uprawnień i atrybutów.
Odczyt i wykonywanie (*Read & Execute*)	Uruchamianie aplikacji, wykonywanie działań, na które zezwala uprawnienie odczytu.
Zapis (*Write*)	Zastępowanie („nadpisywanie") pliku, zmiana jego atrybutów oraz przeglądanie własności i uprawnień do niego.
Modyfikacja (*Modify*)	Modyfikacja i usuwanie pliku, wykonywanie działań, na które zezwalają uprawnienia zapisu, odczytu i wykonywania.
Pełna kontrola (*Full Control*)	Zmiana uprawnień i przejmowanie na własność, wykonywanie działań, na które zezwalają pozostałe uprawnienia NTFS do plików.

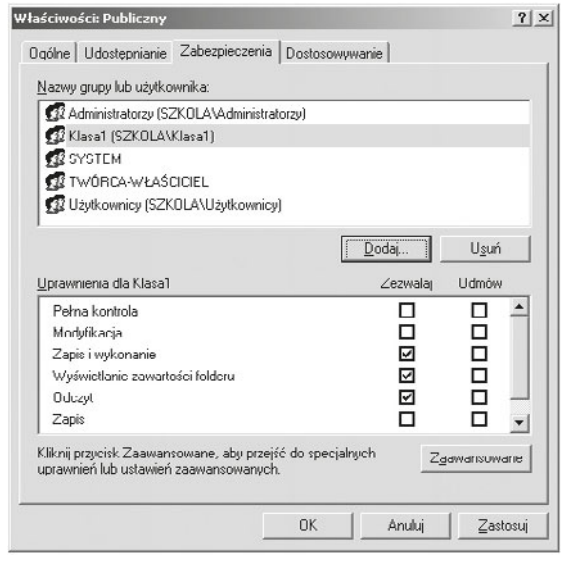
Aby zmienić uprawnienia dla wybranego pliku lub folderu, należy kliknąć jego ikonę prawym przyciskiem myszy, a następnie z menu kontekstowego wybrać opcję *Właściwości*. Na zakładce *Zabezpieczenia* (rysunek 6.201) wyświetlane są dwie sekcje: *Nazwy grupy lub użytkownika* oraz *Uprawnienia dla* (tutaj pojawia się nazwa wskazanego użytkownika). W pierwszej części okna wybierany jest użytkownik lub grupa użytkowników, w drugiej wyświetlane są jego (ich) prawa. System umożliwia dodawanie użytkowników do listy oraz nadawanie lub odbieranie im konkretnych praw. Możliwość nadawania lub zabraniania dostępu do zasobów mają ich właściciele, czyli osoby, które dany plik lub folder utworzyły, wszyscy członkowie grupy *Administratorzy* oraz inni użytkownicy, którzy otrzymali do niego uprawnienie specjalne *Modyfikacja* lub uprawnienie *Pełna kontrola*.

Aby nadać prawa użytkownikowi, który wcześniej ich nie miał, na zakładce *Zabezpieczenia* należy wybrać przycisk *Dodaj*, a następnie wpisać nazwę tego użytkownika. Aby wprowadzić więcej niż jeden wpis, wystarczy je tylko oddzielić średnikami. Aby sprawdzić poprawność nazw, należy wybrać przycisk *Sprawdź nazwy*.

Sumowanie uprawnień

System NTFS sumuje nadane uprawnienia. Członek dwóch grup, z których jedna ma przypisane uprawnienie Odczyt, a druga Zapis, może zarówno czytać, jak i zapisywać dane. Wyjątkiem jest prawo odmowy — nadpisuje ono inne uprawnienia. Jeśli grupa, do której należy użytkownik, lub jego konto mają ustawioną odmowę dostępu, staje się ona efektywna nawet wtedy, gdy użytkownik jest członkiem grup, które dane uprawnienie mają.

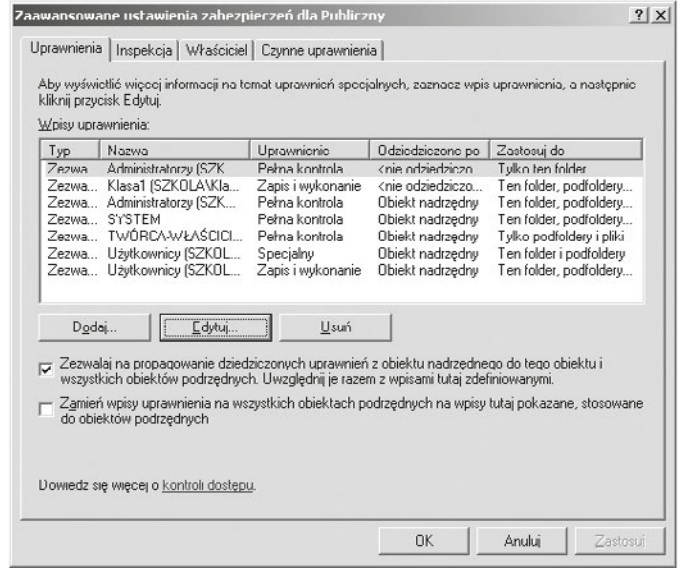
Rysunek 6.201. Nadawanie uprawnień NTFS



Dziedziczenie uprawnień

Ważną cechą systemu uprawnień jest ich dziedziczenie (rysunek 6.202). Uprawnienia przypisywane do folderu nadrzędnego (rodzicielskiego) są domyślnie dziedziczone i rozprzestrzeniane na podfoldery i pliki zawarte w tym folderze.

Rysunek 6.202. Zaawansowane ustawienia zabezpieczeń



Aby zapobiec dziedziczeniu uprawnień do wybranego folderu, trzeba usunąć zaznaczenie odpowiedniej opcji w oknie *Zaawansowane ustawienia zabezpieczeń*.

W celu wyświetlenia okna *Zaawansowane ustawienia zabezpieczeń* należy wybrać opcję *Właściwości* z menu kontekstowego wybranego folderu, a następnie w wyświetlonym oknie przejść do zakładki *Zabezpieczenia* i wybrać przycisk *Zaawansowane*.

Okno to składa się z czterech zakładek. Pierwsza z nich — *Uprawnienia* — pozwala na przegląd i zmianę uprawnień specjalnych. W zakładce tej znajduje się opcja *Zezwalaj na propagowanie dziedziczonych uprawnień z obiektu nadrzędnego do tego obiektu i wszystkich obiektów podrzędnych. Uwzględnij je razem z wpisami tutaj zdefiniowanymi*. Po usunięciu zaznaczenia tej opcji dziedziczenie uprawnień do podfolderów zostanie wstrzymane.

Specjalne uprawnienia obejmują następujące opcje:

- *Przechodzenie przez folder/Wykonanie pliku*,
- *Odczyt atrybutów*,
- *Odczyt atrybutów rozszerzonych* (m.in. atrybutów kompresji i szyfrowania),
- *Tworzenie plików/Zapis danych*,
- *Tworzenie folderów/Dołączanie danych*,
- *Zapis atrybutów*,
- *Zapis rozszerzonych atrybutów*,
- *Usuwanie podfolderów i plików*,
- *Usuwanie*,
- *Odczyt uprawnień*,
- *Zmiana uprawnień*,
- *Przejęcie na własność*,
- *Synchronizacja*.

Zakładka *Inspekcja* pozwala ustalić, jakie zdarzenia związane z wybranym obiektem mają być zapisywane w dzienniku systemowym, czyli podlegać inspekcji. Zakładka *Właściciel* pozwala na przypisanie właściciela danego zasobu, na zakładce *Czynne uprawnienia* istnieje możliwość sprawdzenia, jakie uprawnienia ma wybrany użytkownik po uwzględnieniu sumowania i dziedziczenia.

Należy pamiętać, że odmówienie danego prawa jest ważniejsze niż jego posiadanie. Odmówienie prawa nadpisuje wszystkie uprawnienia, zarówno jawne, jak i dziedziczone.

6.8.2. Szyfrowanie

Szyfrowanie EFS

System szyfrowania plików EFS (ang. *Encrypting File System*) pozwala bezpiecznie przechowywać dane. System EFS chroni dane, szyfrując je w wybranych plikach i folderach systemu plików NTFS.

Szyfrowanie plików można scharakteryzować następująco:

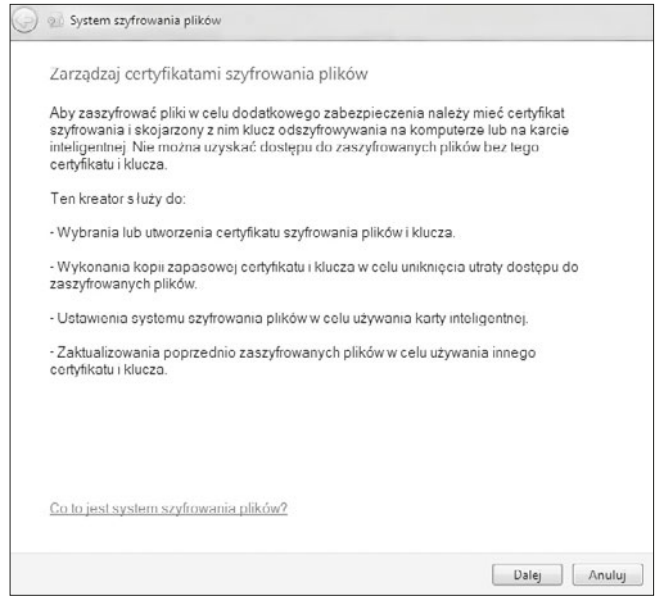
- Każdy plik ma unikatowy klucz szyfrowania pliku, który jest później wykorzystywany do jego odszyfrowywania.
- Klucz szyfrowania pliku jest również zaszyfrowany — jest chroniony przez klucz publiczny odpowiadający certyfikatowi użytkownika w systemie EFS.
- Klucz szyfrowania pliku jest chroniony także przez klucz publiczny każdego dodatkowego użytkownika systemu EFS, który został upoważniony do odszyfrowywania pliku, oraz każdego agenta odzyskiwania.

Odszyfrowywanie plików można scharakteryzować następująco:

- Aby odszyfrować plik, należy wcześniej odszyfrować klucz szyfrowania pliku. Klucz szyfrowania pliku jest odszyfrowywany, jeśli użytkownik ma klucz prywatny, który pasuje do klucza publicznego.
- Oryginalny użytkownik może nie być jedyną osobą uprawnioną do odszyfrowywania klucza szyfrowania pliku. Mogą go również odszyfrowywać inni wyznaczeni użytkownicy lub agenci odzyskiwania za pomocą własnych kluczy prywatnych.

Aby zaszyfrować folder lub plik, należy kliknąć prawym przyciskiem myszy jego ikonę, wybrać *Właściwości*, następnie na karcie *Ogólne* wybrać przycisk *Zaawansowane* i zaznaczyć opcję *Szyfruj zawartość, aby zabezpieczyć dane*. Przy szyfrowaniu folderu wyświetlone zostanie pytanie, czy szyfrowane mają być również podfoldery. Po zatwierdzeniu i poprawnym zaszyfrowaniu nazwa folderu zostanie wyświetlona czcionką w kolorze zielonym. Odszyfrowanie polega na usunięciu zaznaczenia wcześniej wskazanej opcji.

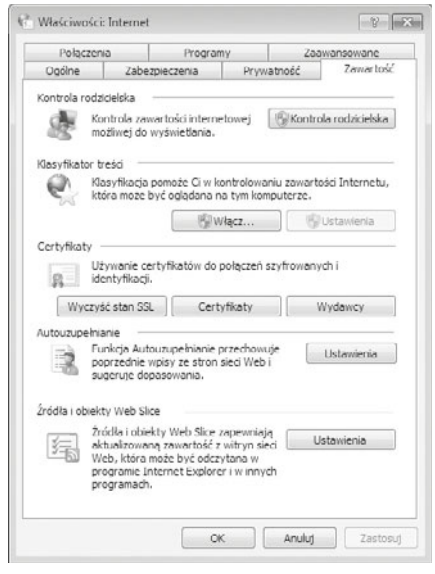
System Windows 7 przed pierwszym uruchomieniem szyfrowania uruchamia kreator zarządzania certyfikatami służącymi do szyfrowania plików (rysunek 6.203).



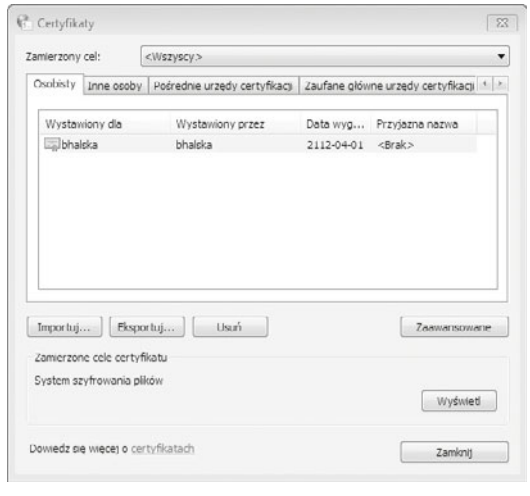
Rysunek 6.203. Szyfrowanie plików w Windows 7

Po wygenerowaniu certyfikatu dla użytkownika możemy zrobić jego kopię zapasową. Aby tego dokonać, należy w panelu sterowania wybrać narzędzie *Opcje internetowe*, a następnie zakładkę *Zawartość* (rysunek 6.204). Wówczas będziemy mieli dostęp do certyfikatów (rysunek 6.205) nie tylko zalogowanego użytkownika, ale również pozostałych certyfikatów, np. sterowników.

Rysunek 6.204. Opcje internetowe — zakładka Zawartość



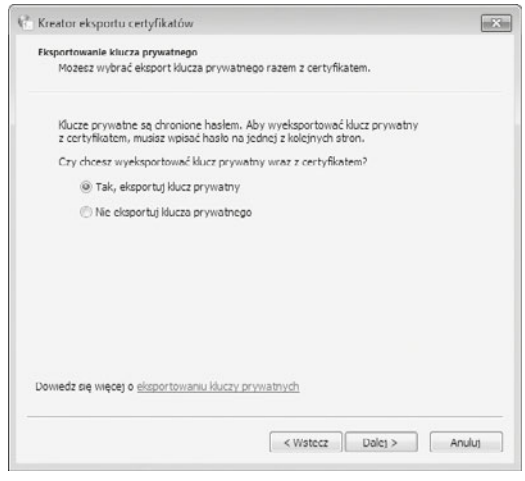
Rysunek 6.205. Certyfikaty



W tym miejscu możemy wyeksportować certyfikat, co pozwoli nam na odzyskanie danych, gdyby certyfikat został usunięty z komputera. W celu wyeksportowania certyfikatu należy wybrać opcję *Eksportuj*. Zostanie uruchomiony kreator eksportu certyfikatów.

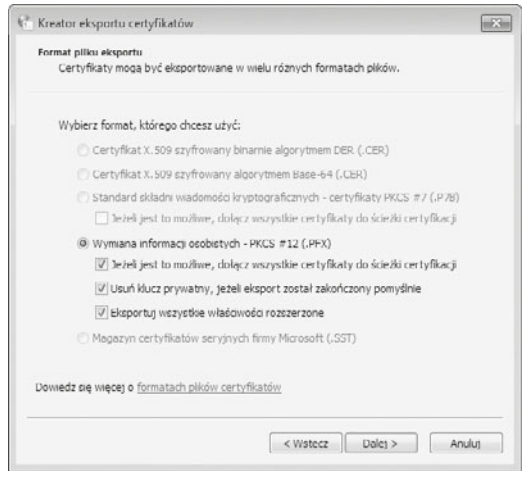
W pierwszym oknie kreatora jedynie klikamy *Dalej*. Dopiero w kolejnym oknie (rysunek 6.206) musimy zdecydować, czy chcemy wyeksportować tylko certyfikat, czy również klucz prywatny dla zalogowanego użytkownika. Należy wybrać opcję *Tak, eksportuj klucz prywatny*.

Rysunek 6.206. Eksportowanie klucza prywatnego



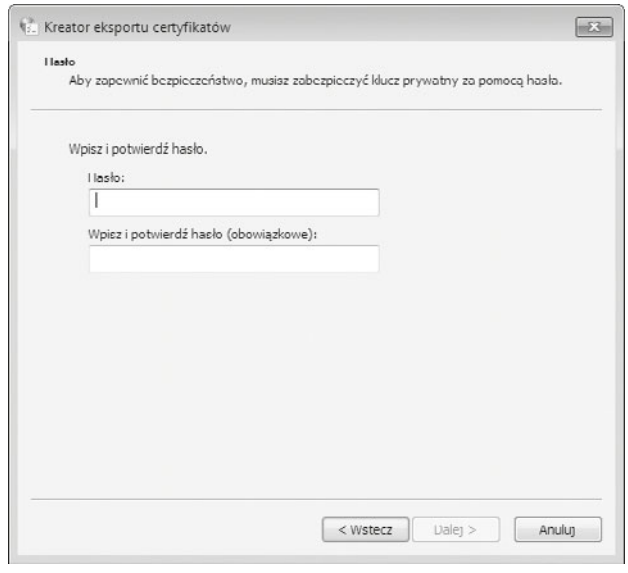
Przechodzimy do kolejnego okna kreatora (rysunek 6.207), w którym wybieramy rozszerzenie dla tworzonego pliku, jak również to, czy ma być usunięty klucz, gdy eksport zostanie wykonany poprawnie, oraz czy należy dołączyć wszystkie certyfikaty oraz szczegółowe informacje. Dla bezpieczeństwa należy wybrać wszystkie dostępne opcje.

Rysunek 6.207. Format pliku eksportu



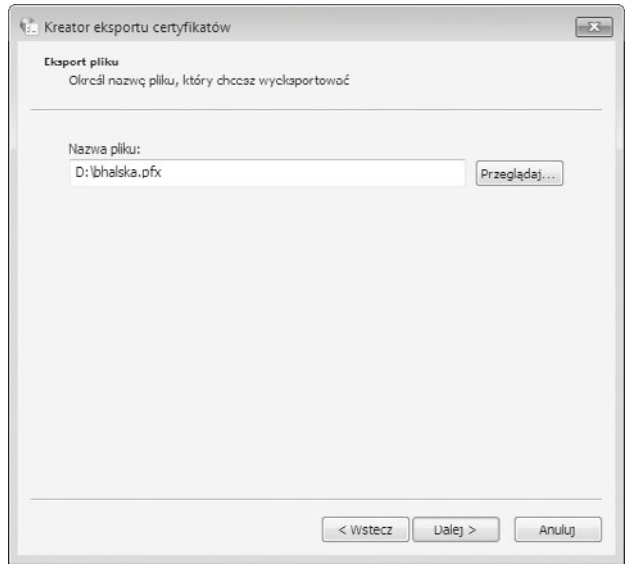
W kolejnym oknie kreatora (rysunek 6.208) jesteśmy proszeni o wprowadzenie hasła, które będzie dodatkowo zabezpieczać nasz klucz, by nikt z niego nie skorzystał w celu odszyfrowania zasobów.

Rysunek 6.208.
Wprowadzanie hasła



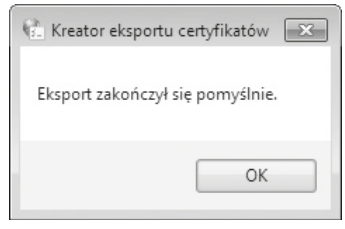
Po nadaniu hasła jesteśmy proszeni o podanie nazwy oraz miejsca przechowywania klucza (rysunek 6.209). Rzecz jasna nie powinna to być partycja systemowa. Dla bezpieczeństwa warto go umieścić na dodatkowych nośnikach pamięci, dysku zewnętrznym, serwerze plików przechowujących dane w „chmurze".

Rysunek 6.209.
Eksport pliku



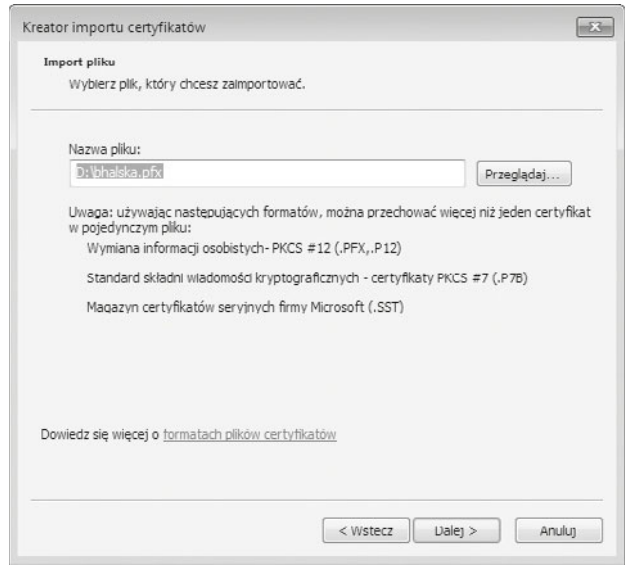
Ostatnie okno kreatora wyświetla podsumowanie ustawień dotyczących eksportu klucza. Jeżeli wszystkie informacje w nim zawarta są poprawne, należy zakończyć działanie kreatora. Gdy wszystko jest poprawnie, pojawia się komunikat potwierdzający to (rysunek 6.210).

Rysunek 6.210. Potwierdzenie eksportu klucza



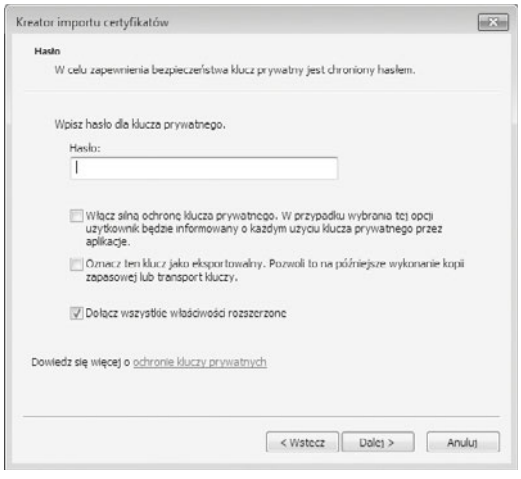
Natomiast jeżeli chcemy odzyskać certyfikat, który został usunięty, należy uruchomić kreator przywracania klucza. Wystarczy dwukrotnie kliknąć wyeksportowany klucz. Pojawi się kreator importu klucza (rysunek 6.211). W kolejnym oknie kreatora wybieramy plik, który chcemy zaimportować.

Rysunek 6.211. Import pliku

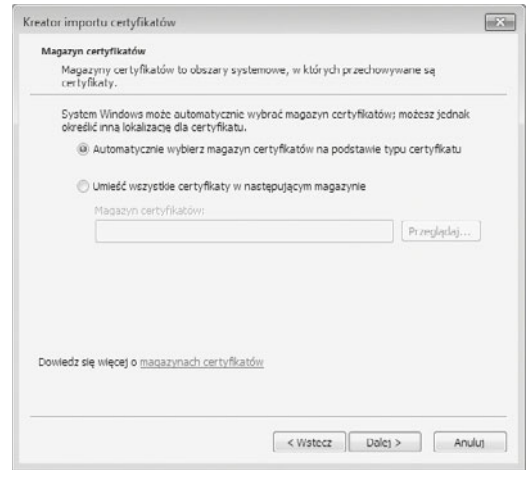


Gdy plik zostanie już wybrany, należy podać hasło (rysunek 6.212), które zostało wprowadzone podczas eksportu klucza. Jeżeli jest poprawne, przechodzimy do następnego okna, w którym należy określić magazyn dla tego klucza (rysunek 6.213). Możemy skorzystać z domyślnego położenia lub samodzielnie zdecydować, w którym miejscu chcemy umieścić klucz.

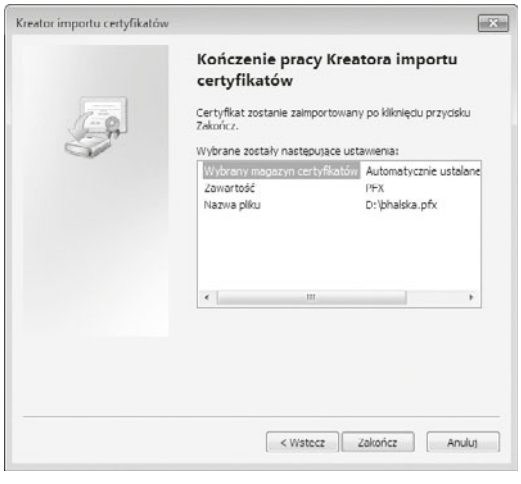
Ostatnie okno kreatora (rysunek 6.214) wyświetla podsumowanie konfiguracji. Gdy ją potwierdzimy i jeśli wszystko zostało poprawnie skonfigurowane, otrzymamy potwierdzenie wyeksportowania certyfikatu (rysunek 6.215).



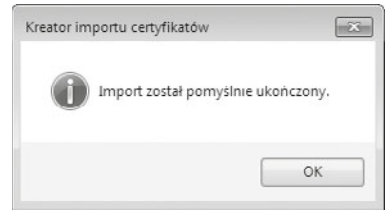
Rysunek 6.212. Hasło



Rysunek 6.213. Magazyn certyfikatów



Rysunek 6.214. Kreator importu certyfikatów



Rysunek 6.215. Import został pomyślnie ukończony

ĆWICZENIA

1. Utwórz folder o nazwie *dane*, następnie zapisz wewnątrz niego plik *dane.txt* zawierający Twoje imię i nazwisko. Folder wraz z zawartością zaszyfruj.
2. Zaloguj się na inne konto i spróbuj odczytać pliki.
3. Spróbuj odszyfrować folder.
4. Spróbuj skopiować niezaszyfrowane pliki do zaszyfrowanego folderu. Czy są zaszyfrowane?

ĆWICZENIA ciąg dalszy

5. Spróbuj skopiować zaszyfrowany folder na tej samej partycji NTFS. Czy jest zaszyfrowany?
6. Spróbuj skopiować zaszyfrowany folder na inną partycję NTFS. Czy jest zaszyfrowany?
7. Spróbuj skopiować zaszyfrowany folder na partycję FAT32. Czy jest zaszyfrowany?
8. Spróbuj przenieść niezaszyfrowane pliki do zaszyfrowanego folderu. Czy są zaszyfrowane?
9. Spróbuj przenieść zaszyfrowany folder na tej samej partycji NTFS. Czy jest zaszyfrowany?
10. Spróbuj przenieść zaszyfrowany folder na inną partycję NTFS. Czy jest zaszyfrowany?
11. Spróbuj przenieść zaszyfrowany folder na partycję FAT32. Czy jest zaszyfrowany?
12. Spróbuj zmienić nazwę zaszyfrowanego folderu.
13. Spróbuj usunąć zaszyfrowany folder.
14. Wyeksportuj klucz, skasuj go i po przelogowaniu sprawdź, czy możesz odczytać pliki na koncie, do którego należał klucz.
15. Zaimportuj klucz i sprawdź, czy teraz możesz odczytać pliki.

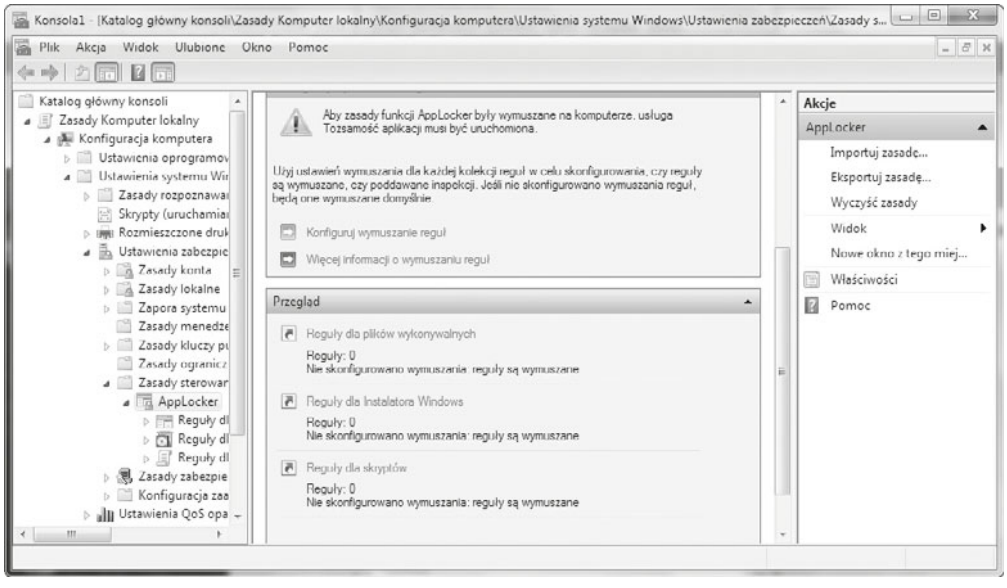
AppLocker

AppLocker umożliwia tworzenie reguł zezwalających (lub nie) na uruchomienie aplikacji z wykorzystaniem unikalnych tożsamości plików, w celu wskazania użytkowników (albo grup), którzy mogą te aplikacje uruchamiać.

Najważniejsze funkcje AppLocker:

- Kontrolowanie następujących typów aplikacji: plików wykonywalnych (*.exe*, *.com*), skryptów (*.js*, *.ps1*, *.vbs*, *.cmd*, *.bat*), plików Instalatora systemu Windows (*.msi*, *.msp*) oraz plików DLL (*.dll*, *.ocx*).
- Definiowanie reguł opartych na atrybutach plików pochodzących z podpisu cyfrowego, w tym wydawcy, nazwy produktu, nazwy pliku oraz jego wersji. Można na przykład utworzyć reguły na bazie atrybutu wydawcy, który pozostaje niezmienny we wszystkich aktualizacjach, lub utworzyć reguły dla określonej wersji pliku.
- Przypisanie reguły do grupy zabezpieczeń lub do indywidualnego użytkownika.
- Tworzenie wyjątków od reguł. Możliwe jest na przykład utworzenie reguły, która zezwala na uruchamianie wszystkich procesów systemu Windows z wyjątkiem Edytora rejestru (*Regedit.exe*).

- Użycie trybu *Audit-only* do wdrażania zasad i zrozumienia ich wpływu przed ich wprowadzeniem ich w życie.
- Importowanie i eksportowanie reguł. Importowanie i eksportowanie wpływa na wszystkie zasady. Jeśli na przykład eksportujemy zasadę, eksportowane są również wszystkie reguły z wszystkich zbiorów reguł, w tym ustawienia egzekwowania dla zbiorów reguł. Kiedy importujemy zasady, wszystkie kryteria w istniejących zasadach zostają nadpisane.



Rysunek 6.216. Konfiguracja zabezpieczeń AppLocker

AppLocker jest konfigurowany poprzez Group Policy. Aby uruchomić interfejs konfiguracji AppLocker, należy uruchomić konsolę mmc Edytor obiektów zasad dla komputera lokalnego. W sekcji *Konfiguracja komputera* należy rozwinąć węzeł *Ustawienia systemu Windows*, następnie *Ustawienia zabezpieczeń*, a na końcu *Zasady sterowania aplikacjami*. W tym momencie pojawi się AppLocker (rysunek 6.216).

WAŻNE

Samo stworzenie roli nie spowoduje jeszcze jej natychmiastowego zastosowania — nim nowe zasady zostaną wprowadzone, należy uruchomić usługę AppID Service. Bez tej usługi nie będą działały reguły zdefiniowane w AppLocker.

Aby aktywować tę usługę, należy uruchomić konsolę *Usługi*, wpisując `Services.msc` w polu wyszukiwania w menu Start. Zaleca się, aby — zwłaszcza przy pierwszym kontakcie z AppLocker — uruchamiać tę usługę manualnie.

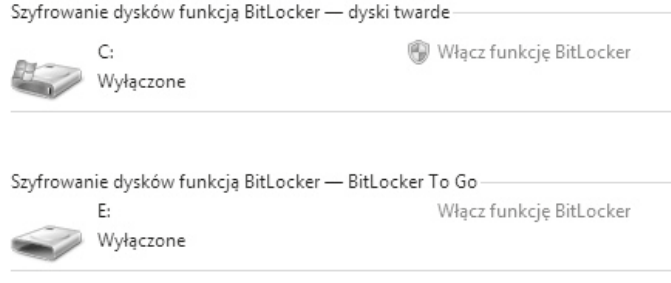
BitLocker

BitLocker jest systemem szyfrującym partycję systemową (domyślnie), ale za jego pomocą można także zaszyfrować każdą inną partycję z wyjątkiem partycji rozruchowej. Najważniejszą zaletą systemu BitLocker jest jednak to, że w całości zaszyfrowane zostają takie pliki systemowe, jak plik hibernacji, plik stronicowania oraz katalog *Windows*, *Users* i *Program Files*, włączając wszystkie katalogi tymczasowe.

BitLocker może pracować w trzech trybach — w zależności od wymagań użytkownika co do poziomu bezpieczeństwa oraz technicznych możliwości komputera:

- **Tryb bez dodatkowych kluczy** — jest to tryb domyślny, w którym funkcja BitLocker szyfruje dane oraz generuje specjalne hasło odzyskiwania. Hasła tego można użyć w celu przywrócenia dostępu do dysku w momencie, gdy zostanie on zablokowany przez system BitLocker.
- **Tryb z numerem PIN** — różni się od domyślnego jedynie wymogiem podania ustalonego przed zaszyfrowaniem danych numeru PIN. Jeśli użytkownik zapomni numer lub dostęp do dysku zostanie zablokowany z innych powodów, konieczne jest podanie hasła odzyskiwania.
- **Tryb z kluczem USB** — najwyższy poziom bezpieczeństwa zapewnia tryb z obsługą klucza USB, na którym jest zapisane hasło uruchomieniowe. Różni się ono jednak od hasła odzyskiwania. Przy każdym normalnym uruchomieniu komputera użytkownik zostaje poproszony o włożenie klucza USB w celu odczytania hasła uruchomieniowego. Zaleca się stosowanie kluczy kryptograficznych. W przypadku zgubienia nośnika USB jedyną możliwością uzyskania dostępu do danych jest podanie hasła odzyskiwania.

Rysunek 6.217.
Szyfrowanie BitLocker

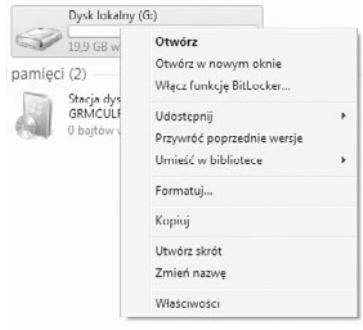


Aby zaszyfrować partycję systemową funkcją BitLocker, należy posiadać moduł zabezpieczający TPM, natomiast pozostałe partycje możemy już bez problemu szyfrować, używając narzędzia BitLocker To Go. W systemie Windows 7 wprowadzono nową funkcję, która umożliwia szyfrowanie nie tylko partycji, ale również przenośnych urządzeń magazynujących, takich jak dyski flash USB i zewnętrzne dyski twarde.

Jeżeli posiadamy wersję Ultimate lub Enterprise, możemy przystąpić do szyfrowania partycji narzędziem BitLocker To Go. Najpierw musimy włączyć szyfrowanie na danej

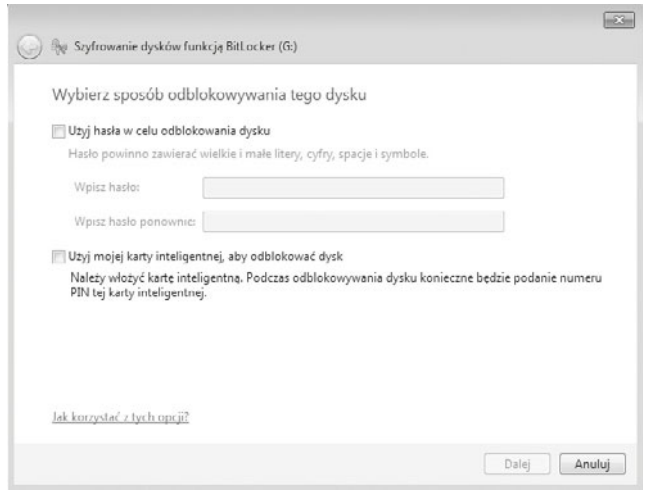
partycji, klikając prawym przyciskiem myszy dysk (dysk zewnętrzny, pamięć flash) i wybierając opcję *Włącz funkcję BitLocker* (rysunek 6.218).

Rysunek 6.218. Włączanie funkcji BitLocker



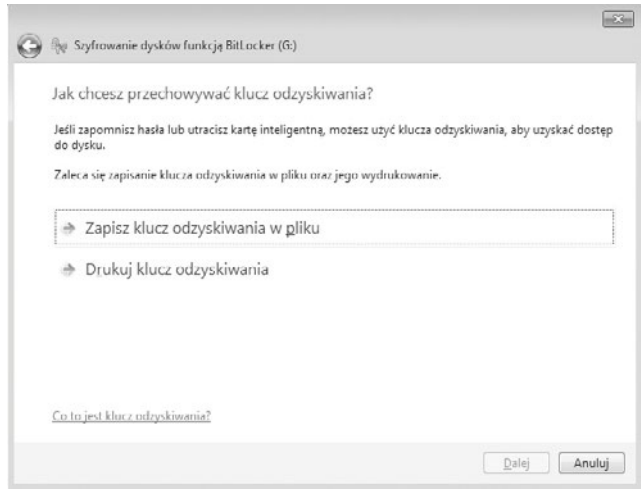
Po włączeniu usługi uruchomi się kreator tworzenia klucza prywatnego dla szyfrowanego urządzenia, w którym musimy podać hasło do odzyskiwania danych lub skorzystać z karty inteligentnej (rysunek 6.219).

Rysunek 6.219. Wybór sposobu odblokowywania urządzenia



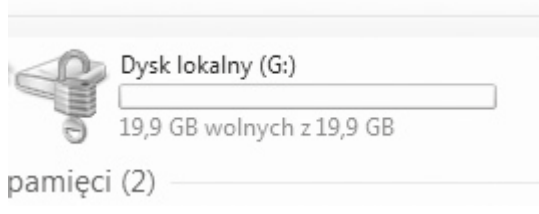
Jeżeli wybraliśmy pierwszą opcję, a więc odblokowanie (odszyfrowanie) przez podanie hasła, w kolejnym kroku kreatora jesteśmy proszeni o wybranie sposobu przechowania klucza odzyskiwania. Do wyboru mamy możliwość wydruku lub zapisania klucza. Pamiętajmy, że nie powinniśmy go przechowywać w miejscu dostępnym dla wszystkich użytkowników (rysunek 6.220).

Rysunek 6.220.
Sposób przechowywania klucza odzyskiwania



Po wyborze sposobu przechowywania klucza następuje szyfrowanie urządzenia. Jeżeli wszystko przebiegnie bez problemów, otrzymamy potwierdzenie powodzenia operacji, zmieni się też oznaczenie urządzenia (rysunek 6.221).

Rysunek 6.221.
Zaszyfrowany dysk



Należy pamiętać, że funkcją BitLocker możemy szyfrować dyski tylko w wersji Ultimate i Enterprise, natomiast odszyfrowywać już w wersji Windows XP z SP3.

ĆWICZENIA

1. Zaszyfruj dane w folderze w systemie Windows XP oraz Windows 7.
2. Wyeksportuj klucz.
3. Zaszyfruj dane, wykorzystując BitLocker.

PYTANIA

1. Co to jest EFS?
2. Co to jest klucz?
3. Omów usługę BitLocker.
4. Omów usługę AppLocker.

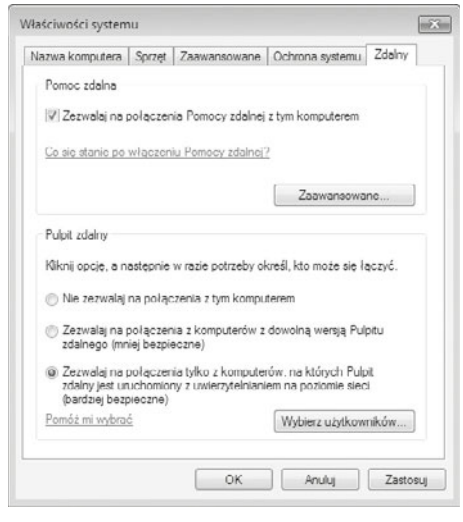
6.9. Centralne zarządzanie stacjami roboczymi/serwerami

Zdalne zarządzanie klientami jest bardzo popularną formą pracy administratorów. Omówione w tej części podręcznika usługi pozwalają na podłączenie wirtualnego pulpitu, co umożliwia administratorom sieci lub zespołowi pomocy technicznej (ang. *Help Desk*) wykonanie zdalnie czynności konserwacyjnych i naprawczych lub zmianę ustawień na komputerach użytkowników.

6.9.1. Pulpit zdalny

W systemach Windows usługa podłączenia pulpitu zdalnego jest instalowana domyślnie z systemem operacyjnym.

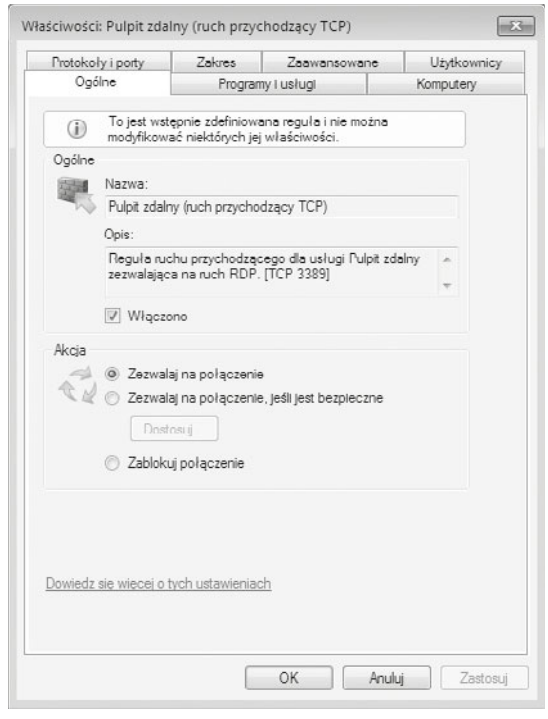
1. Aby możliwe było podłączanie do stacji przez pulpit zdalny, we właściwościach systemu w zakładce *Zdalny* (rysunek 6.222) należy włączyć możliwość łączenia się z danym komputerem zdalnie poprzez wskazanie określonej opcji połączeń — z dowolną wersją pulpitu zdalnego lub z komputerem, na którym jest uruchomiony zdalny pulpit z uwierzytelnianiem na poziomie sieci (system Windows 7 i wyższe). Można tutaj również zdefiniować, kto może łączyć się z naszym komputerem. Użytkownicy z grupy *Administratorzy* mają prawo łączyć się z usługą zdalnego pulpitu, użytkownicy z innych grup muszą zostać wskazani poprzez wybór opcji *Wybierz użytkowników*.



Rysunek 6.222. Zezwolenie na podłączenie pulpitu zdalnego

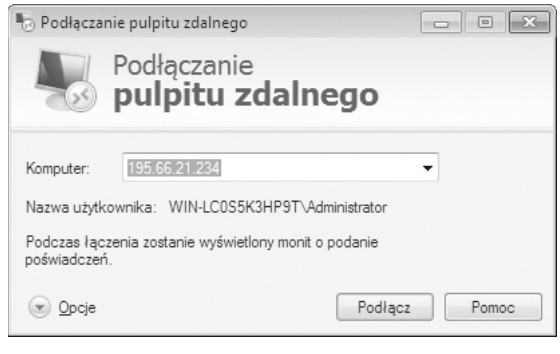
2. Gdy chce się uzyskać dostęp do komputera spoza sieci lokalnej chronionej firewallem, należy pamiętać o odblokowaniu odpowiedniego portu na zaporze. Dla usługi Pulpit zdalny domyślnie jest to port 3389. Gdy korzysta się z wbudowanej Zapory systemu Windows, należy zezwolić na ruch przychodzący i wychodzący (rysunek 6.223).

Rysunek 6.223. Konfiguracja zapory systemowej



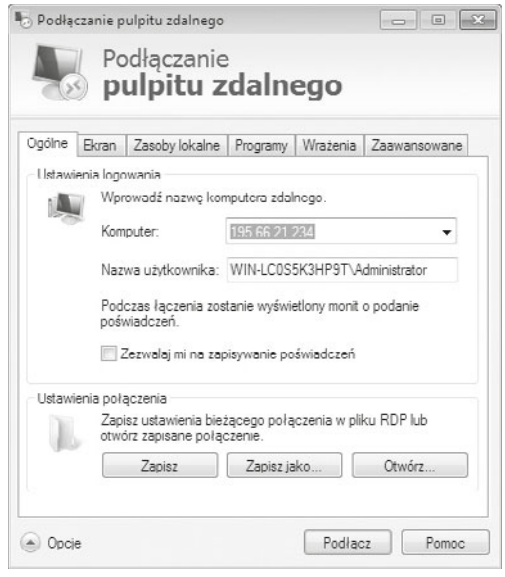
3. W celu uruchomienia zdalnego pulpitu należy uruchomić aplikację *Podłączanie pulpitu zdalnego*, która znajduje się w grupie *Akcesoria* (rysunek 6.224). W głównym oknie aplikacji trzeba podać adres zdalnego komputera, do którego chcemy się podłączyć. W celu ustawienia dodatkowych parametrów połączenia należy wybrać przycisk *Opcje*.

Rysunek 6.224. Główne okno aplikacji Podłączanie pulpitu zdalnego



4. W kolejnych zakładkach definiujemy szczegóły połączenia, m.in. nazwę użytkownika, konfigurację ekranu, współdziałanie zasobów lokalnych ze zdalnym komputerem czy programy, które powinny być uruchomione podczas sesji zdalnego pulpitu (rysunek 6.225).

Rysunek 6.225. Konfiguracja pulpitu zdalnego



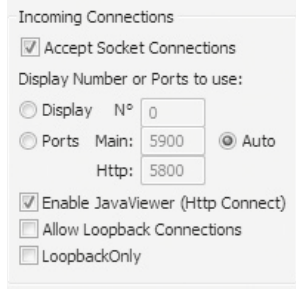
Jeżeli chcemy się łączyć ze stacjami roboczymi z serwera, cała konfiguracja może zostać zapisana z wykorzystaniem GPO. Wszystkie stacje robocze muszą być podłączone do domeny, a więc mieć konto w jednostce organizacyjnej, dla której zostaną zdefiniowane odpowiednie zasady.

1. Opcje związane ze zdalnym zarządzaniem mieszczą się w ustawieniach *Konfiguracja komputera/Zasady/Szablony administracyjne/Składniki systemu Windows/Usługi pulpitu zdalnego*, gdzie można wprowadzić odpowiednie parametry.
2. Z perspektywy udostępniania danych istotnym czynnikiem są ustawienia związane z bezpieczeństwem dostępu. Pierwsza z opcji, na którą należy zwrócić uwagę, to *Zawsze monituj klienta o hasło po połączeniu* — wymusza ona podawanie hasła przy korzystaniu ze zdalnego pulpitu.

6.9.2. UltraVNC

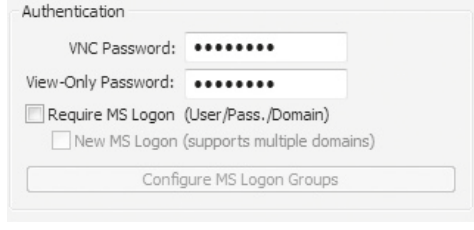
UltraVNC (*www.uvnc.com*) to implementacja systemu przekazywania obrazu z graficznych środowisk pracy (ang. *Virtual Network Computing*). Jest to program, który umożliwia podłączenie pulpitu na różnych platformach. Do funkcjonowania potrzebuje modułu *Serwer* instalowanego w systemie, który ma umożliwiać pracę zdalną, oraz modułu klienta do pobierania i wyświetlania danych. Program UltraVNC może pełnić zarówno rolę serwera, jak i klienta, pozwala również na udostępnianie danych przez przeglądarkę internetową z obsługą Javy. Po zainstalowaniu i uruchomieniu usługi należy skonfigurować takie opcje serwera, jak porty wykorzystywane do połączenia oraz możliwość połączenia przez przeglądarkę (opcja *Enable JavaViewer*) (rysunek 6.226).

Rysunek 6.226. Konfiguracja portów VNC



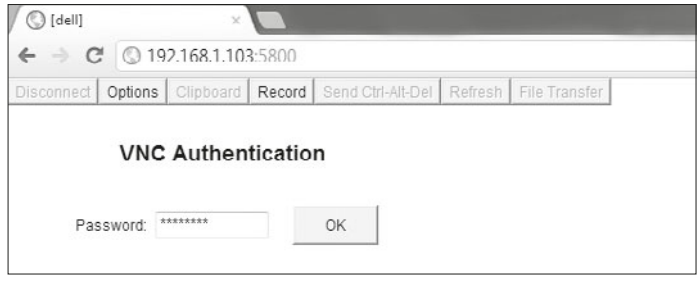
1. W celu zabezpieczenia połączenia należy zdefiniować hasło. Istnieje możliwość wykorzystania uwierzytelniania systemu Windows, w tym także przy użyciu domeny (rysunek 6.227).

Rysunek 6.227. Ustawienie haseł VNC



2. Gdy usługa zostanie już zainstalowana, do podglądu pulpitu wystarczy przeglądarka internetowa. Trzeba w niej podać adres IP i port, na którym nasłuchuje usługa (rysunek 6.228).

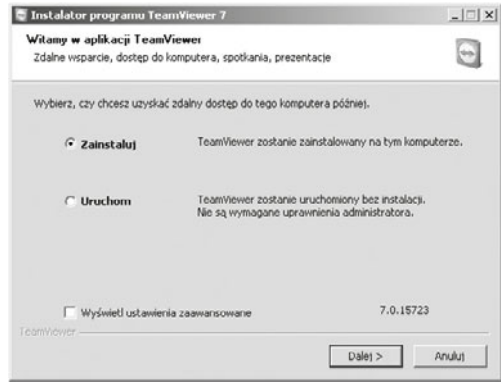
Rysunek 6.228. Dostęp do serwera UltraVNC przez przeglądarkę internetową



6.9.3. TeamViewer

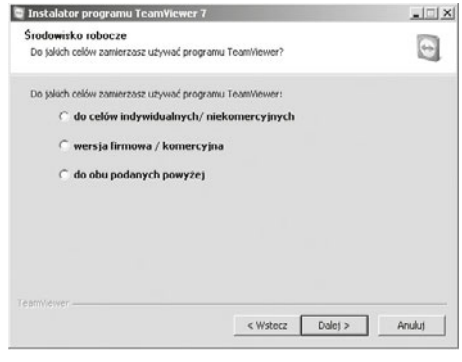
TeamViewer (*www.teamviewer.pl*) to narzędzie przeznaczone do zdalnego kontrolowania systemu przez sieć bez konieczności instalacji serwera/klienta na dysku twardym komputera. Połączenie między komputerami jest bezpieczne, gdyż program wykorzystuje szyfrowanie RSA oraz AES. Do głównych zadań programu należy m.in. zdalne kontrolowanie komputerów i serwerów, przenoszenie plików pomiędzy komputerami, prowadzenie pokazów, prezentacji szkoleń czy też połączeń wideo. Do największych zalet programu należy bezproblemowa komunikacja przez internet, nawet z poziomu sieci prywatnych bez konieczności rekonfigurowania sieci czy przekierowania portów. Dodatkowo program może zostać uruchomiony bez instalacji (rysunek 6.229).

Rysunek 6.229.
Instalacja/uruchamianie programu



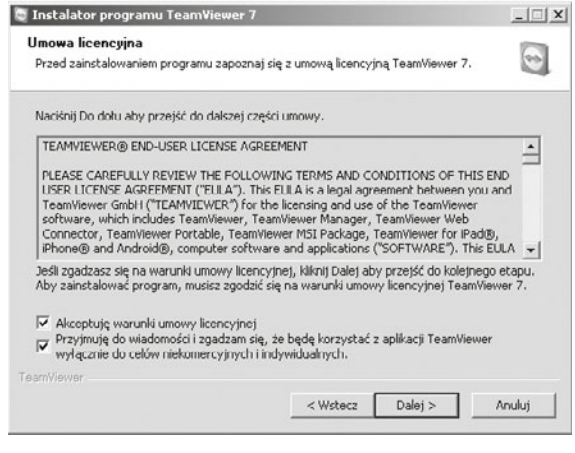
Przy instalacji należy wskazać rodzaj licencji (rysunek 6.230). Darmowa wersja do celów niekomercyjnych nie może być uruchamiana na systemie Windows Server.

Rysunek 6.230.
Wybór licencji



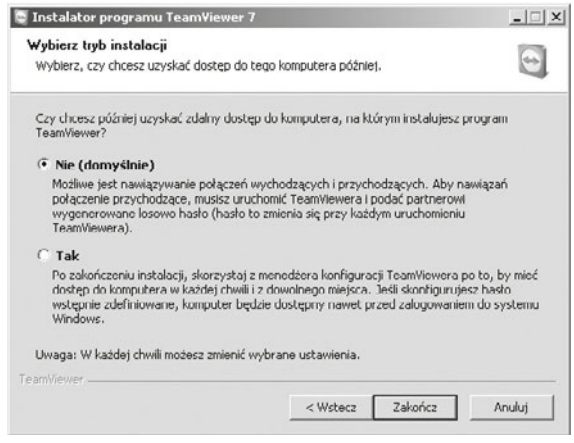
1. Kolejny krok instalacji to akceptacja warunków licencji (rysunek 6.231).

Rysunek 6.231.
Akceptacja warunków licencji



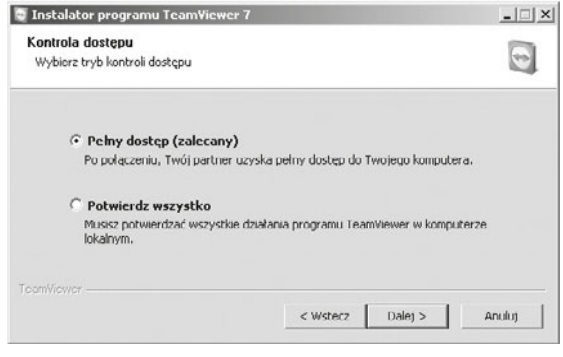
2. Kolejny ekran programu instalacyjnego pozwala wybrać tryb instalacji (rysunek 6.232).

Rysunek 6.232.
Tryb instalacji



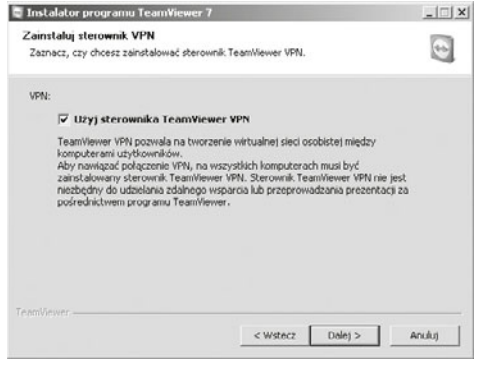
3. Następnie należy określić rodzaj dostępu: pełny dostęp automatycznie przyznawany zdalnemu użytkownikowi lub dostęp do poszczególnych działań na komputerze lokalnym potwierdzany przez użytkownika lokalnego (rysunek 6.233).

Rysunek 6.233.
Rodzaj dostępu



4. W kolejnym kroku (rysunek 6.234) istnieje możliwość instalacji sterownika VPN programu TeamViewer. Pozwala on na tworzenie wirtualnej sieci prywatnej pomiędzy użytkownikami — nie jest on wymagany do korzystania ze zdalnego pulpitu.

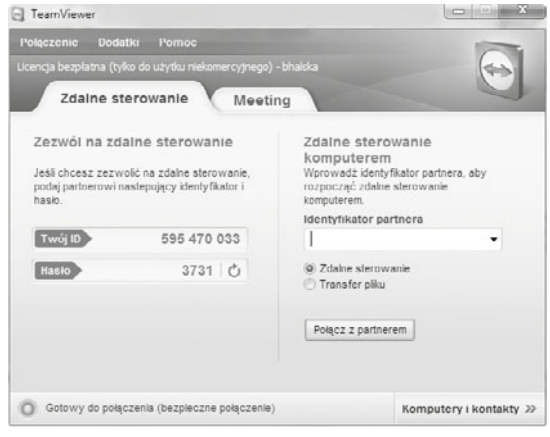
Rysunek 6.234.
Instalacja
sterownika VPN



5. Następnie należy wybrać katalog docelowy i instalacja zostaje zakończona.

Po instalacji i uruchomieniu programu istnieje możliwość podłączenia do komputera zdalnego. W tym celu należy uzyskać identyfikator oraz hasło komputera zdalnego (*Twój ID* oraz *Hasło*). Identyfikator zdalnego komputera należy podać w polu *Identyfikator partnera* w głównym oknie programu (rysunek 6.235). Po wybraniu opcji *Połącz z partnerem* pojawia się pytanie o hasło. Po podaniu poprawnego hasła zostaje wyświetlone okno z pulpitem zdalnego komputera.

Rysunek 6.235. TeamViewer



ĆWICZENIA

1. Połącz się pulpitem zdalnym ze stacją roboczą.
2. Zainstaluj programy i dokonaj połączenia przy ich wykorzystaniu.

PYTANIA

1. Co to jest pulpit zdalny?

6.10. Monitorowanie w systemach Windows

Monitorowanie (ang. *monitoring*) to działania polegające na obserwowaniu systemu w celu jak najwcześniejszego wykrycia nieprawidłowości. Najczęściej monitoruje się systemy pod kątem bezpieczeństwa, ciągłości działania lub wydajności.

Informacje na temat monitorowania urządzeń sieciowych oraz transmisji w sieci zostały opisane w podrozdziale 8.7 — „Monitoring sieci i urządzeń sieciowych”.

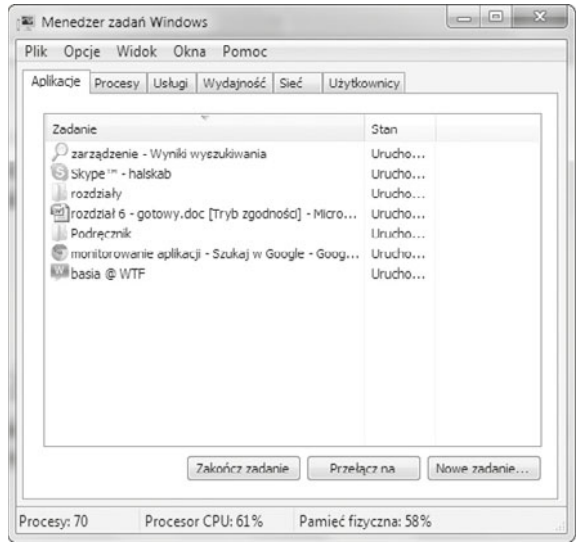
6.10.1. Menedżer zadań Windows

DEFINICJA

Menedżer zadań (ang. *task manager*) jest narzędziem służącym do monitorowania w systemie Windows. Z jego pomocą możemy sprawdzić uruchomione aplikacje i działające procesy, ilość używanej i dostępnej pamięci RAM, obciążenie procesora, użycie łącza internetowego oraz aktywności użytkowników.

Aby go uruchomić, po zalogowaniu się do systemu operacyjnego należy wybrać kombinację klawiszy *Ctrl+Alt+Delete*, a następnie opcję *Menedżer zadań*. Główne okno programu składa się z zakładek pozwalających monitorować różne parametry uruchomionego systemu (rysunek 6.236).

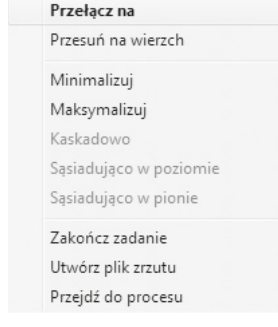
Rysunek 6.236. Menedżer zadań Windows



Aplikacje to pierwsza zakładka, która informuje o uruchomionych programach oraz ich stanie.

Zarządzanie aplikacjami jest możliwe poprzez menu kontekstowe (rysunek 6.237), które udostępnia między innymi polecenia:

Rysunek 6.237. Menu kontekstowe

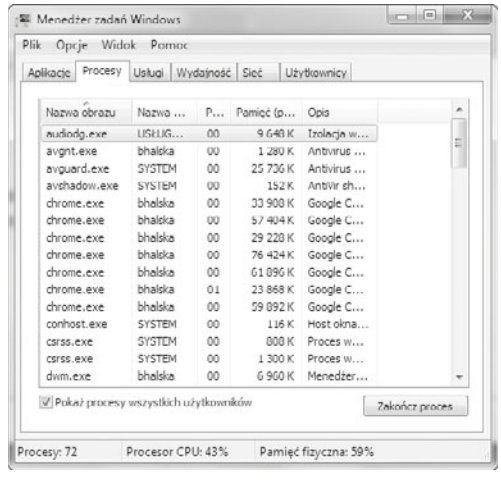


- *Przełącz na* — pozwala na przełączenie użytkowania na wybraną aplikację i minimalizuje okno Menedżera zadań Windows,
- *Przesuń na wierzch* — otwiera okno wybranej aplikacji,
- *Zakończ zadanie* — pozwala na wyłączenie wybranego programu z poziomu systemu operacyjnego,
- *Przejdź do procesu* — przenosi do zakładki *Procesy*, w której jest zaznaczony proces odpowiadający wybranej aplikacji.

Zakładka *Procesy* (rysunek 6.238) wyświetla aktywne procesy wraz z dodatkowymi informacjami dotyczącymi:

- *Nazwy obrazu*,
- *Nazwy użytkownika*,
- procentowego wykorzystania procesora — *Procesor CPU*,
- ilości pamięci przydzielonej poszczególnym procesom — *Pamięć*,
- opisu procesu — *Opis*, opcja dostępna tylko w Windows 7 i Vista.

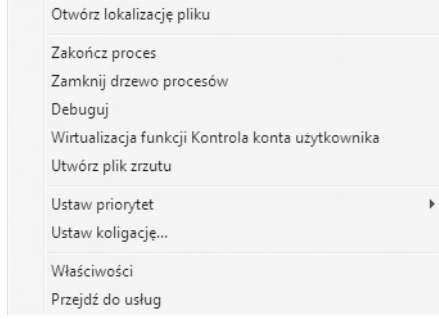
Rysunek 6.238. Procesy



Wybór kolumn w tabeli procesów jest możliwy w menu *Widok* po wybraniu opcji *Wybierz kolumny*.

Opcje w menu kontekstowym (rysunek 6.239) pozwalają m.in. na zamknięcie procesu — *Zakończ proces*, zamknięcie procesu oraz wszystkich procesów potomnych — *Zamknij drzewo procesów*, przypisanie priorytetu — *Ustaw priorytet* oraz określenie procesora lub rdzenia, na którym zadanie ma być wykonywane — *Ustaw koligację*. Przypisanie wyższego priorytetu do danego procesu powoduje, że pracuje on szybciej kosztem pozostałych aplikacji.

Rysunek 6.239.
Menu kontekstowe Windows 7



Kolejna zakładka Menedżera zadań Windows — *Usługi* — wyświetla informacje na temat usług uruchomionych w systemie operacyjnym (rysunek 6.240). Na liście usług są wyświetlane następujące informacje:

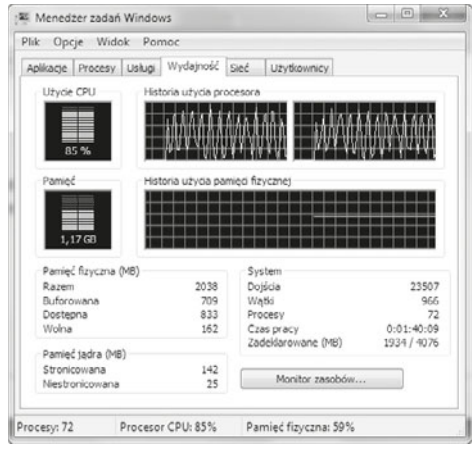
- nazwa usługi — *Nazwa*,
- unikalny identyfikator procesu PID (ang. *Process IDentifier*) — *PID*,
- opis usługi — *Opis*,
- stan usługi (uruchomiona lub zatrzymana) — *Stan*,
- grupa, do której należy usługa — *Grupa*.

Rysunek 6.240.
Usługi

Wydajność to zakładka, która umożliwia zapoznanie się z wykorzystaniem zasobów komputera — procesora i pamięci fizycznej (rysunek 6.241). Taka informacja jest szczególnie przydatna, gdy niezbędne jest odnalezienie najmniej wydajnego elementu systemu, który przyczynia się do obniżenia jego wydajności. Informacje, jakich dostarcza ta zakładka, to:

- użycie procesora CPU oraz historia użycia,
- użycie pamięci oraz historia użycia,
- informacje o dostępnej pamięci fizycznej,
- informacje dotyczące pamięci stronicowania.

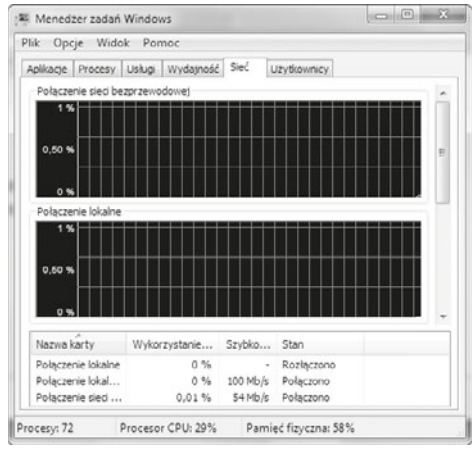
Rysunek 6.241.
Wydajność



Zakładka *Sieć* (rysunek 6.242) umożliwia zapoznanie się z danymi dotyczącymi interfejsów sieciowych. Informacje, jakich dostarcza, to:

- nazwa interfejsu,
- wykorzystanie łącza w procentach,
- prędkość transmisji,
- stan połączenia.

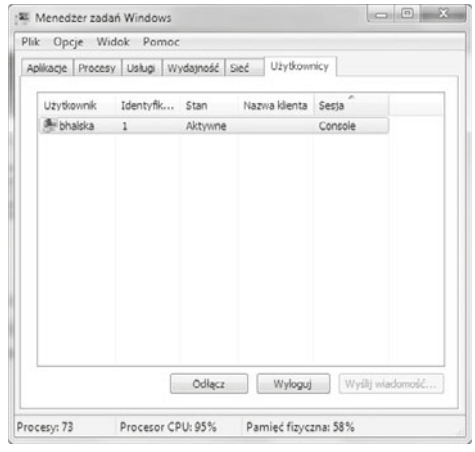
Rysunek 6.242.
Monitoring sieci



Ostatnia zakładka Menedżera zadań Windows — *Użytkownicy* — pozwala na monitorowanie użytkowników systemu operacyjnego. Wyświetla listę użytkowników połączonych lub zalogowanych do systemu wraz z dodatkowymi informacjami (rysunek 6.243):

- nazwą użytkownika,
- identyfikatorem sesji,
- nazwą klienta,
- stanem sesji,
- sesją.

Rysunek 6.243.
Użytkownicy



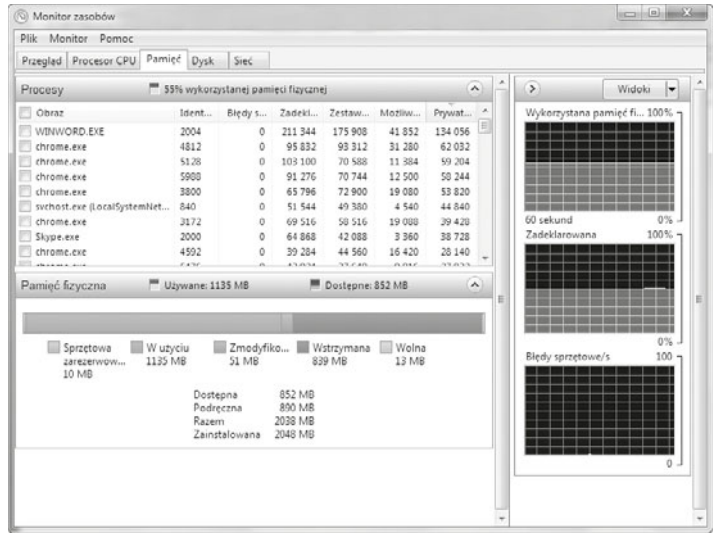
6.10.2. Monitor zasobów

Dodatkowe informacje dotyczące używanych zasobów są przedstawione w narzędziu *Monitor zasobów* (rysunek 6.244). Jest to aplikacja dostępna w systemach Windows 7 oraz Vista, która przedstawia graficznie zużycie zasobów dostępnych dla systemu operacyjnego, takich jak:

- *Procesor CPU*,
- *Pamięć*,
- *Dysk*,
- *Sieć*.

Monitor zasobów jest dostępny w *Start/Akcesoria/Narzędzia systemowe* oraz w zakładce *Wydajność* Menedżera zadań Windows.

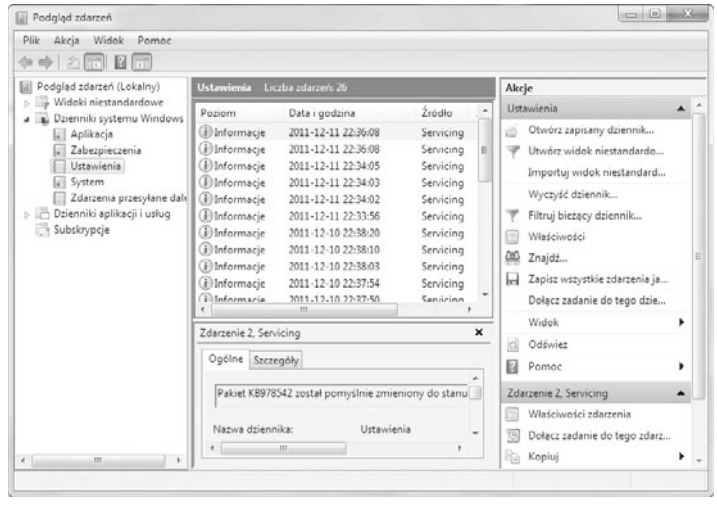
Rysunek 6.244.
Monitor zasobów



6.10.3. Dzienniki zdarzeń systemu Windows

Do kontrolowania działania systemu operacyjnego system Windows udostępnia dzienniki zdarzeń (ang. *event log*), w których są rejestrowane zdarzenia zachodzące w systemie. Wraz z rejestrowanym zdarzeniem są zapisywane data i godzina jego wystąpienia, źródło (np. aplikacja, która je wywołała) oraz typ informacji (*Informacja*, *Ostrzeżenie* lub też *Błąd*). Aby przejrzeć zawartość dzienników zdarzeń, można użyć graficznego narzędzia *Podgląd zdarzeń* (rysunek 6.245) dostępnego w menu *Narzędzia administracyjne* lub polecenia `wevtutil` w trybie tekstowym.

Rysunek 6.245. Podgląd zdarzeń



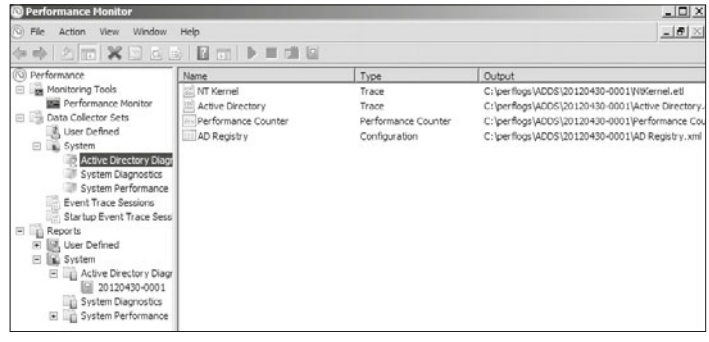
Systemy Windows 7 oraz Windows Server 2008 R2 udostępniają następujące dzienniki zdarzeń:

- **Aplikacja** — rejestruje zdarzenia generowane przez uruchomioną aplikację. O tym, które zdarzenia są rejestrowane, decydują projektanci programu.
- **Zabezpieczenia** — rejestruje zdarzenia związane z zabezpieczeniami, jak udane lub nieudane próby logowania, czy zdarzenia związane z dostępem do zasobów, takie jak tworzenie lub otwieranie plików albo innych obiektów. O tym, które zdarzenia będą zapisywane w dzienniku zabezpieczeń, decydują administratorzy systemu.
- **Ustawienia** — zakładka rejestruje zdarzenia związane z instalacją aplikacji.
- **System** — rejestruje zdarzenia systemu Windows, np. ładowanie sterowników lub bibliotek.
- **Zdarzenia przesyłane dalej** — rejestruje zdarzenia przesłane do dziennika przez inne komputery.
- **Dzienniki aplikacji i usług** — rejestrują zdarzenia pochodzące z konkretnych aplikacji lub usług, które nie wpływają na działanie całego systemu operacyjnego. Ta kategoria dzienników składa się z dzienników: administracyjnych, operacyjnych, analitycznych i debugowania.

6.10.4. Monitor wydajności systemu

System Windows udostępnia narzędzie do badania wydajności systemu operacyjnego — program *Performance Monitor* (*Monitor wydajności*) (rysunek 6.246). Jest on dostępny w menu *Administrative Tools* (*Narzędzia administracyjne*).

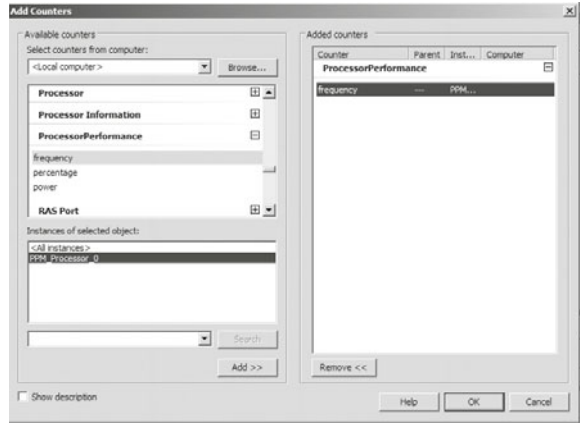
Monitor wydajności korzysta z modułów zbierających dane (*Data Collector Set*), które rejestrują wybrane parametry pracy systemu operacyjnego określone przez administratora. Aby utworzyć zestaw zdefiniowany przez użytkownika (*User Defined*), należy wybrać opcję *New/Data Collector Set* (*Nowy/Zestaw modułów zbierających dane*) w menu *Action* (*Akcja*). Dane zarejestrowane przez monitor wydajności pozwalają na analizę wpływu uruchamianych programów i usług na wydajność systemu.



Rysunek 6.246. Performance Monitor — Monitor wydajności

Dodawanie liczników do monitora wydajności

Aby dodać licznik do monitora wydajności, wystarczy skorzystać z paska narzędzi. Po kliknięciu przycisku *Add* (*Dodaj*) pojawi się okno *Add counters* (*Dodawanie liczników*). W sekcji *Available counters* (*Dostępne liczniki*) należy wybrać interesujący nas licznik, np. *Processor Performance* (*Wydajność procesora*), *frequency* (*licznik częstotliwości*). W tej sekcji możemy również zdefiniować wystąpienia wybranego obiektu (*Instances of selected object*). Gdy już wszystko zostanie ustawione, należy kliknąć *Add* (*Dodaj*). Wówczas licznik pojawi się w sekcji *Added counters* (*Dodane liczniki*). Następnie klikamy OK i wtedy licznik zostanie dodany (rysunek 6.247).



Rysunek 6.247. Dodawanie liczników programu Monitor wydajności

ĆWICZENIA

1. Sprawdź, w jaki sposób są wyświetlane informacje w programie Menedżer zadań oraz Monitor wydajności.
2. Stwórz nowy licznik w Monitorze wydajności.

PYTANIA

1. Wymień narzędzia do monitorowania systemu Windows znajdujące się w systemie.

6.11. Wirtualizacja

Wirtualizacja zasobów komputerowych to technologia, która pozwala na jednoczesne udostępnianie danych wielu programom, np. wielu systemom operacyjnym uruchomionym równocześnie na jednej platformie sprzętowej. W wirtualnym środowisku używane systemy operacyjne nie mają bezpośredniego dostępu do zasobów sprzętowych, za ich zarządzanie odpowiada platforma wirtualizacji. Wprowadzenie warstwy wirtualizacji pomiędzy sprzęt a systemy operacyjne pozwala uniezależnić się od faktycznie wykorzystywanego sprzętu, co daje ogromne korzyści i elastyczność w budowie infrastruktury sieciowej (rysunek 6.248). Wirtualny system operacyjny może zostać szybko i bezproblemowo przeniesiony na inny serwer działający na innych komponentach sprzętowych (np. w przypadku awarii używanego serwera), ponieważ na nowym sprzęcie będzie działał w środowisku wirtualnym, które będzie przydzielało takie same „wirtualne" komponenty, jakie były wykorzystywane wcześniej.

Rysunek 6.248.
Schemat wirtualizacji

Oprogramowanie do wirtualizacji pozwala na tworzenie i uruchamianie wirtualnych maszyn z 32- lub 64-bitowym systemem operacyjnym zarówno Windows, Linux, jak i innym, takim jak Solaris, FreeBSD czy Novell. Najbardziej popularne oprogramowanie do wirtualizacji to:

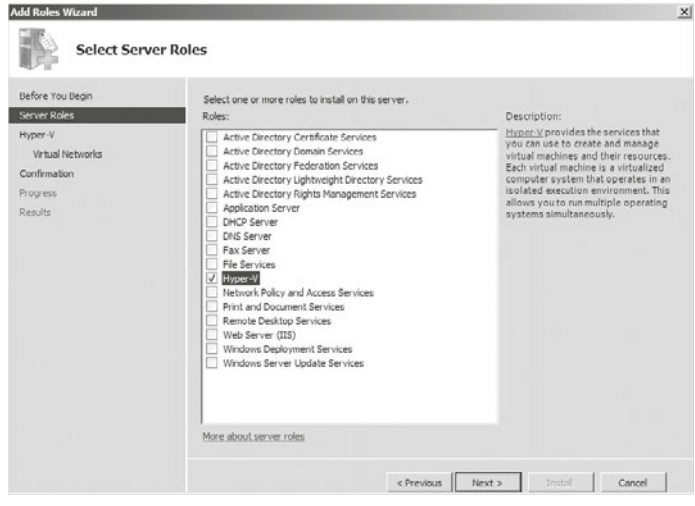
- Hyper-V — możliwa jest tylko instalacja na serwerze 2008 i nowszych.
- VMware Player — możliwa instalacja na systemach Windows oraz Linux.
- VirtualBox — możliwa instalacja na systemach Windows oraz Linux.

6.11.1. Hyper-V

Hyper-V to oprogramowanie do wirtualizacji firmy Microsoft. Narzędzie to jest dostępne jako osobny produkt — Hyper-V Server 2008 — lub jako rola w systemie Windows Server 2008 oraz Windows Server 2008 R2.

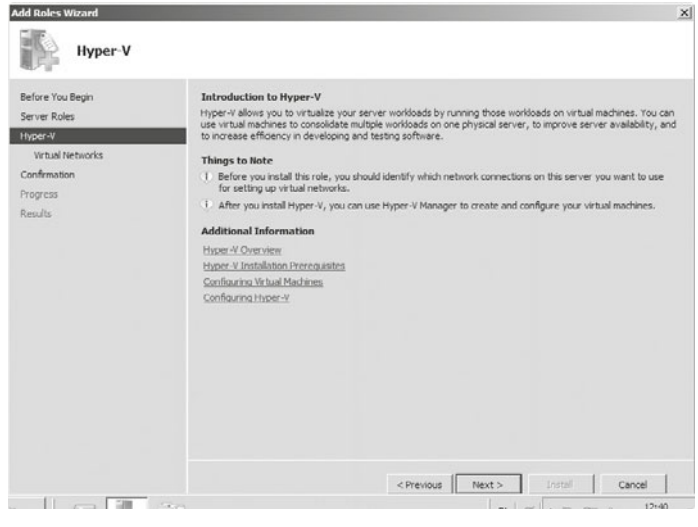
Do zainstalowania roli Hyper-V wymagany jest procesor 64-bitowy, który wspiera wirtualizację sprzętową (Intel VT – Intel Virtualization Technology lub AMD-V – AMD Virtualization). Instalacja serwera Hyper-V polega na dodaniu nowej roli (rysunek 6.249).

Rysunek 6.249. Instalacja roli Hyper-V



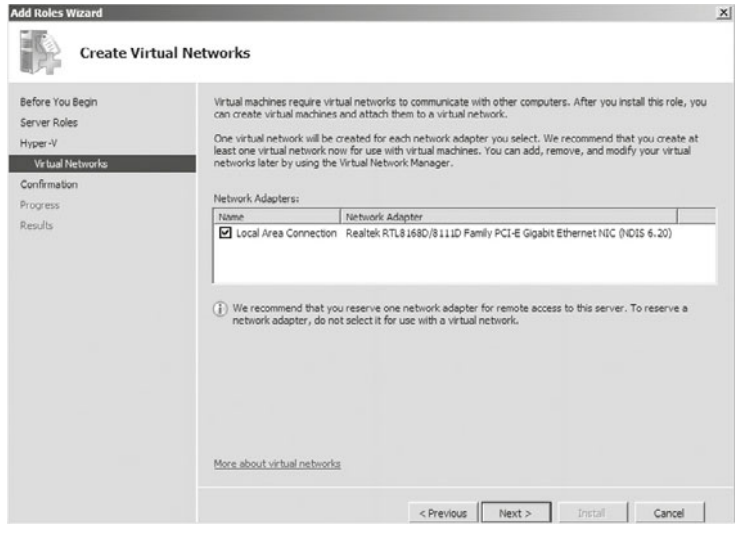
W kolejnym oknie kreatora wyświetlają się informacje na temat instalowanej usługi (rysunek 6.250).

Rysunek 6.250. Informacja na temat instalacji usługi



Kolejny krok instalacji pozwala na wybór fizycznego interfejsu, który ma być użyty jako połączenie zewnętrzne dla maszyn wirtualnych (rysunek 6.251).

Rysunek 6.251. Tworzenie wirtualnego interfejsu sieciowego

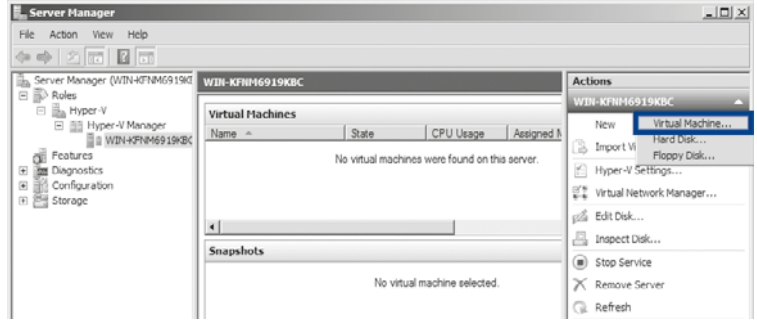


W następnym oknie należy potwierdzić instalację usługi.

Kroki tworzenia wirtualnej maszyny

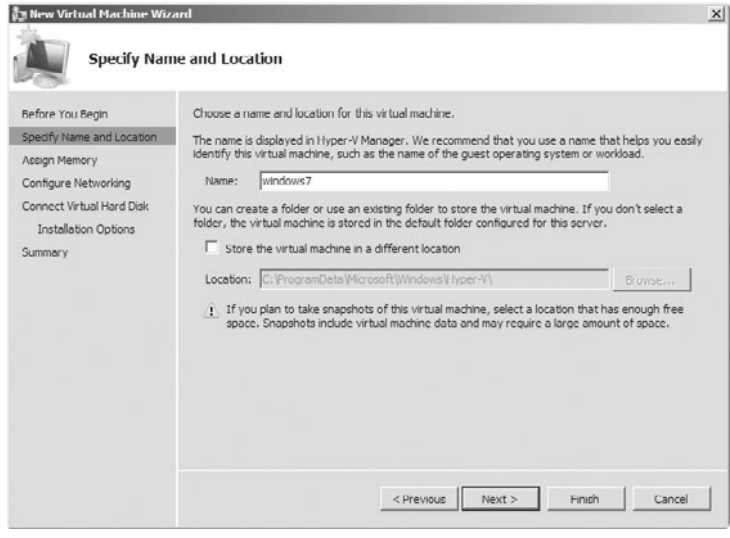
Aby utworzyć wirtualną maszynę, należy w narzędziu *Server Manager* (*Menedżer serwera*) wybrać rolę *Hyper-V*. Następnie klikając prawym przyciskiem myszy nazwę serwera, z menu kontekstowego należy wybrać opcję *New/Virtual Machine* (*Nowy/Wirtualna maszyna*) (rysunek 6.252), która uruchomi kreator tworzenia wirtualnej maszyny.

Rysunek 6.252. Tworzenie nowej wirtualnej maszyny



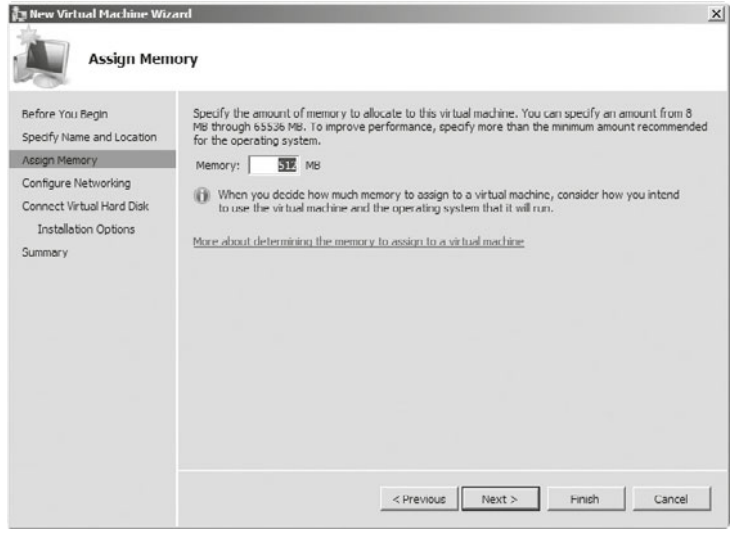
W kolejnym oknie należy podać nazwę dla nowo tworzonej maszyny oraz ścieżkę dostępu, gdzie ma być utworzona (rysunek 6.253).

Rysunek 6.253.
Okno definiowania nazwy i ścieżki



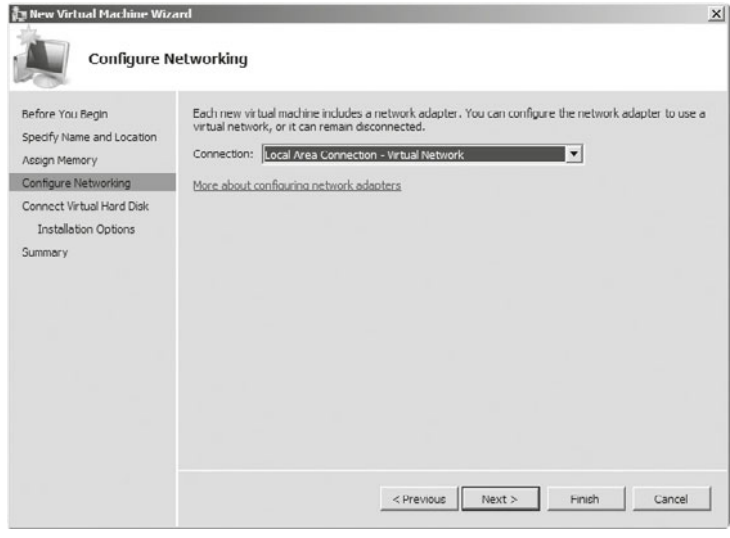
W kolejnym oknie (rysunek 6.254) należy określić rozmiar pamięci RAM, która będzie przydzielona dla nowej maszyny wirtualnej — minimalna wartość to 8 MB, a maksymalna to aż 65 536 MB.

Rysunek 6.254.
Rozmiar pamięci RAM



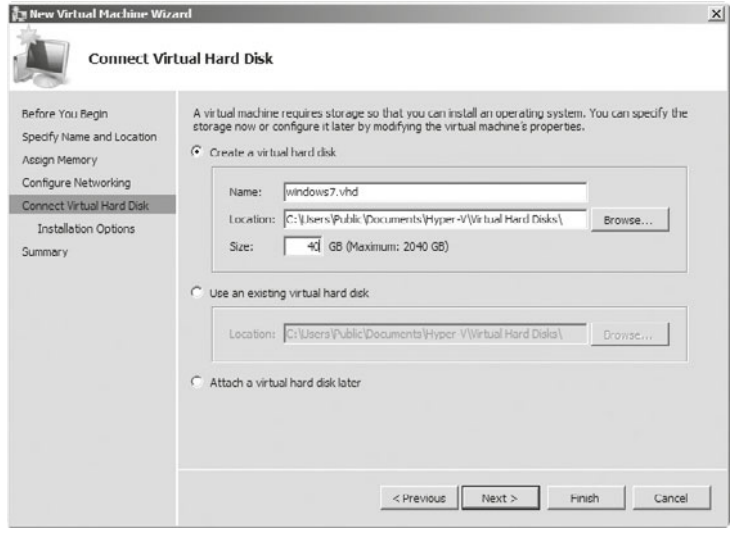
W kolejnym kroku należy wskazać kartę sieciową, z której będzie korzystać wirtualna maszyna (rysunek 6.255).

Rysunek 6.255.
Konfiguracja interfejsu



Kolejny ekran (rysunek 6.256) wymaga określenia rozmiaru dysku wirtualnej maszyny oraz opcjonalnie wskazania pliku VHD zawierającego dysk dla wirtualnej maszyny.

Rysunek 6.256.
Konfiguracja wirtualnego dysku

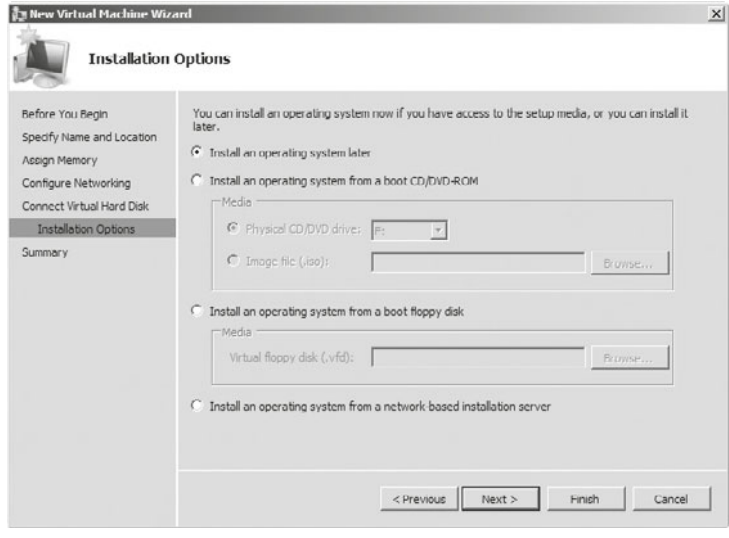


W kolejnym kroku (rysunek 6.257) należy określić, w jaki sposób będzie instalowany system na nowej wirtualnej maszynie. Można:

- dokonać późniejszej instalacji (*Install an operating system later*),
- rozpocząć instalację z fizycznego dysku (*Physical CD/DVD drive*) lub z obrazu ISO (*Imagefile* (*.iso*)),

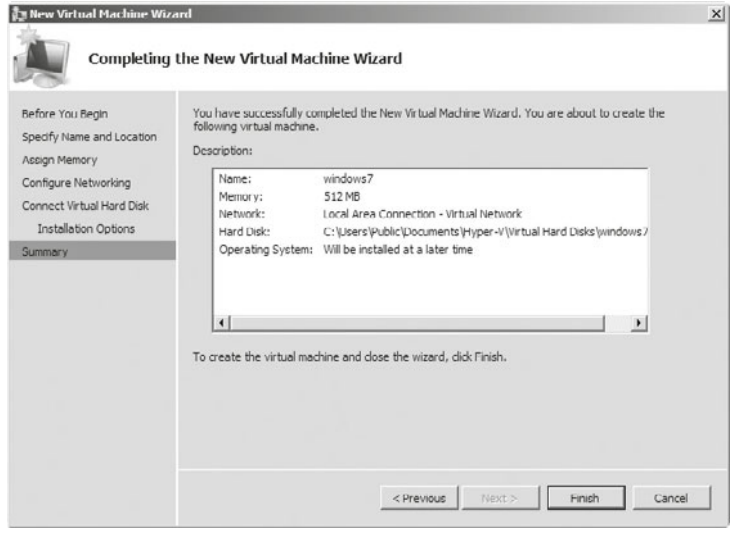
- rozpocząć instalację ze stacji dyskietek (*Install an operating system from a boot flopy disk*) lub wirtualnej stacji dyskietek (*Virtual floppy disk* (*.vfd*)),
- rozpocząć instalację, korzystając z sieciowego serwera instalacji (*Install an operating system from a network-based installation server*).

Rysunek 6.257. Opcje instalacji dla wirtualnej maszyny



W ostatnim oknie kreatora wyświetla się podsumowanie konfiguracji tworzonej maszyny (rysunek 6.258).

Rysunek 6.258. Podsumowanie dla instalowanej maszyny



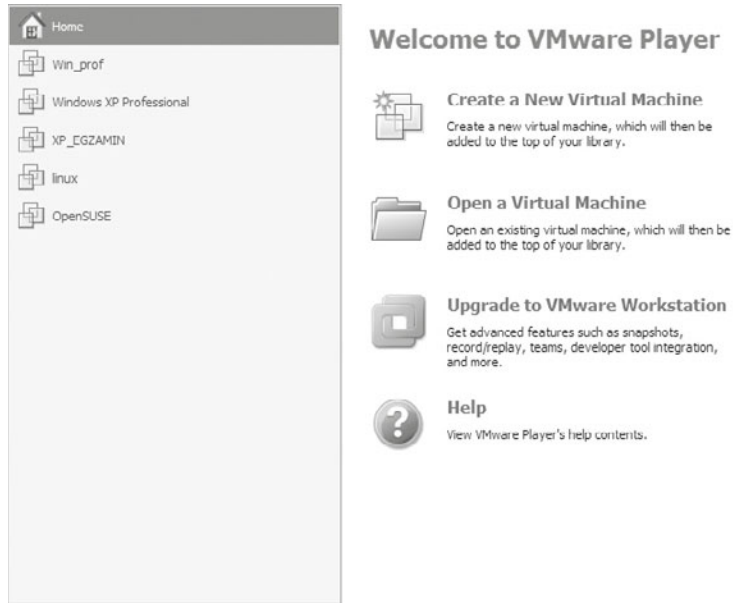
6.11.2. VMware Player

DEFINICJA

VMware Player (*http://www.vmware.com/products/player/*) jest programem, który umożliwia tworzenie wirtualnych maszyn bez konieczności instalowania serwera. To bezpłatne oprogramowanie służy do tworzenia i uruchamiania wcześniej przygotowanych maszyn wirtualnych. Narzędzie pozwala na uruchomienie ponad 200 systemów operacyjnych — w tym m.in. różnych wersji Windowsa i dystrybucji Linuksa. Program pozwala obsłużyć do 8 rdzeni procesora i 32 GB pamięci RAM dla każdej z wirtualnych maszyn.

W celu stworzenia nowej wirtualnej maszyny w głównym oknie programu (rysunek 6.259) należy wybrać kreator tworzenia wirtualnej maszyny (*Create a New Virtual Machine*).

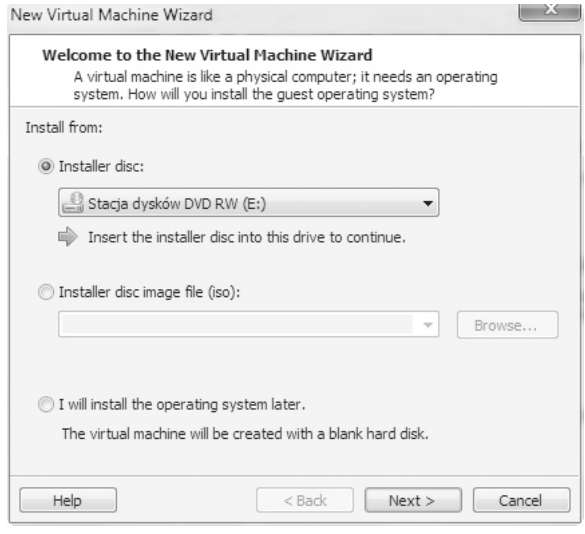
Rysunek 6.259. VMware Player



Po uruchomieniu kreatora należy określić, w jaki sposób będzie instalowany system operacyjny na nowej wirtualnej maszynie (rysunek 6.260):

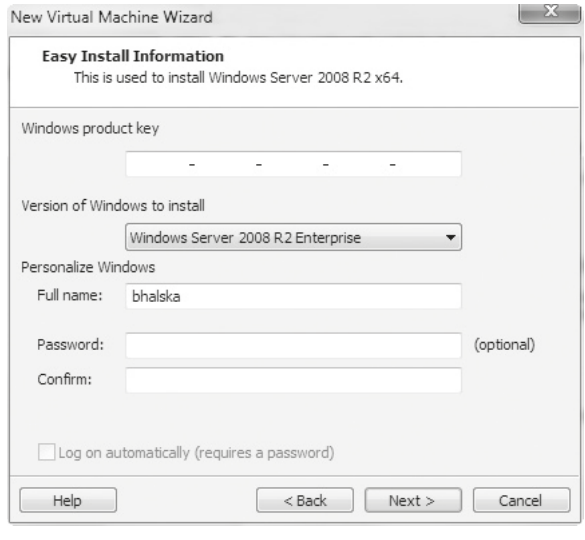
- z fizycznego CD-ROM-u,
- z obrazu ISO,
- instalacja zostanie przeprowadzona później.

Rysunek 6.260. Definiowanie sposobu instalacji systemu operacyjnego



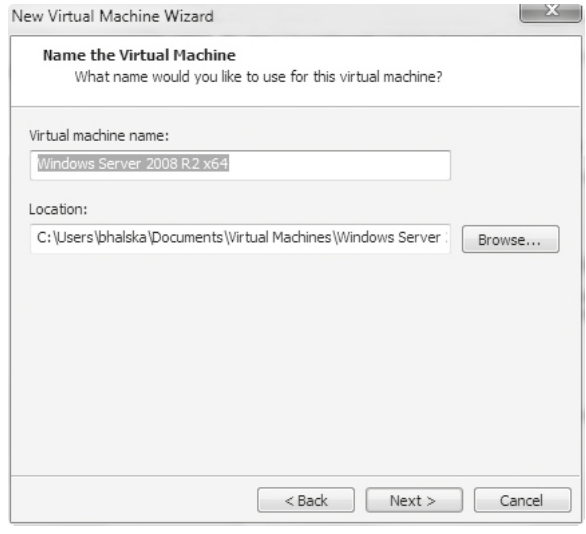
Kolejne okno to funkcja *Easy Install* odpowiedzialna za automatyczną, nienadzorowaną instalację systemów operacyjnych. Opcja ta pozwala na pominięcie większości kolejnych kroków programu instalacyjnego, takich jak wybór partycji czy dodanie użytkowników systemu (rysunek 6.261).

Rysunek 6.261. Instalacja nienadzorowana



W następnym kroku (rysunek 6.262) należy podać nazwę wirtualnej maszyny oraz miejsce, gdzie zostanie ona utworzona.

Rysunek 6.262.
Nazwa dla nowej wirtualnej maszyny

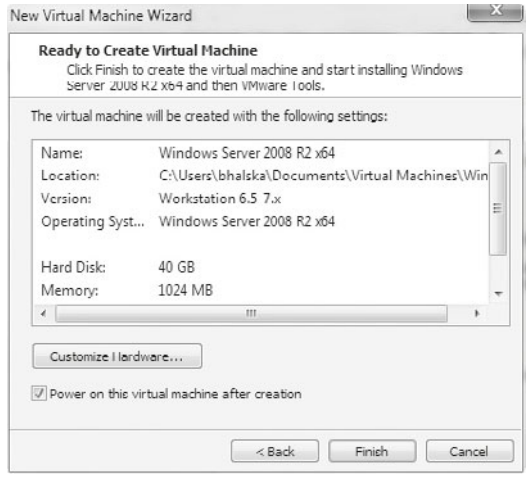


W kolejnym oknie (rysunek 6.263) należy określić rozmiar wirtualnego dysku poprzez podanie jego maksymalnej wielkości. Można podzielić wirtualny dysk na części, wybierając *Split virtual disk as a multiple file*. Należy pamiętać o zabezpieczeniu odpowiedniej ilości miejsca na partycji, na której została wskazana lokalizacja plików. Na tym etapie istnieje tylko możliwość utworzenia nowego dysku, nie można wskazać istniejącego.

Rysunek 6.263.
Wirtualny dysk

W ostatnim oknie kreatora (rysunek 6.264) wyświetla się podsumowanie konfiguracji. Zaznaczona opcja *Power on this virtual machine after creation* odpowiada za automatyczne uruchomienie maszyny po jej utworzeniu i rozpoczęcie instalacji systemu.

Rysunek 6.264. Podsumowanie tworzenia nowej wirtualnej maszyny



6.11.3. VirtualBox

VirtualBox jest kolejnym popularnym oprogramowaniem, które umożliwia tworzenie wirtualnych maszyn. Pod względem funkcjonalności to oprogramowanie jest bardzo podobne do programu VMware Player omawianego wcześniej.

Program można pobrać ze strony:

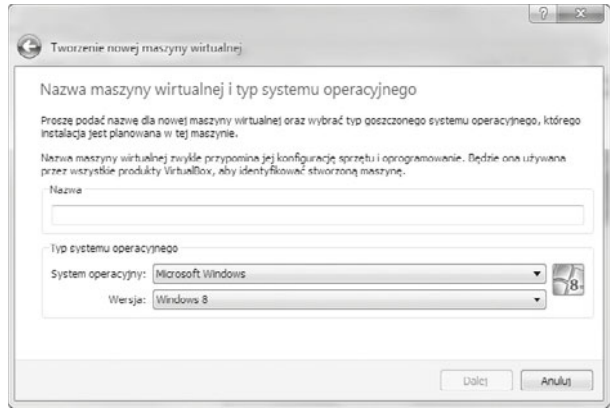
https://www.virtualbox.org/wiki/Downloads

Aby utworzyć nową wirtualną maszynę, w głównym oknie programu (rysunek 6.265) należy wybrać przycisk *Nowa*, który uruchomi kreator tworzenia nowej maszyny wirtualnej.

Rysunek 6.265. Główne okno programu VirtualBox

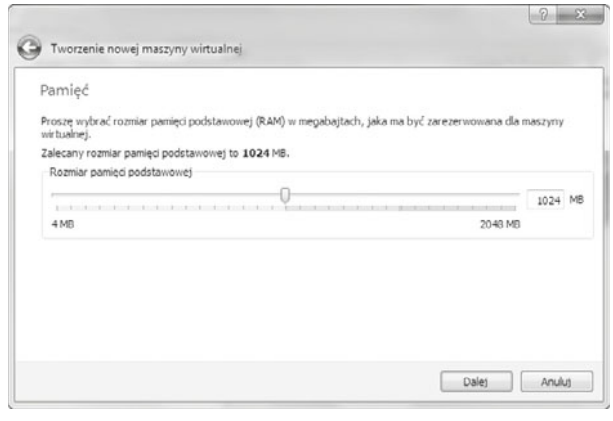
Instalację nowej maszyny należy rozpocząć od określenia nazwy nowo tworzonej wirtualnej maszyny oraz rodzaju i wersji systemu operacyjnego, który będzie instalowany (rysunek 6.266).

Rysunek 6.266.
Tworzenie nowej maszyny wirtualnej



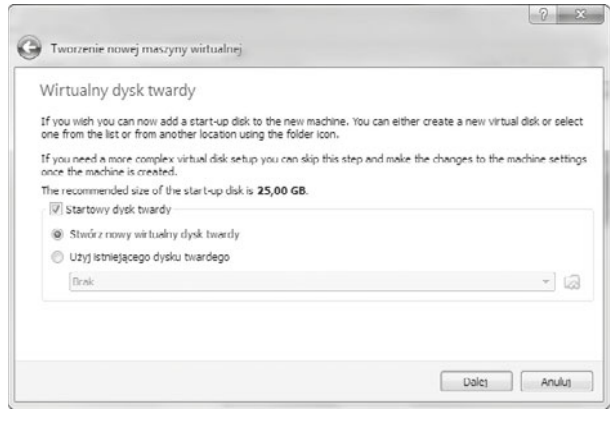
Kolejnym krokiem jest określenie rozmiaru pamięci operacyjnej RAM, która będzie przydzielona dla tej maszyny (rysunek 6.267).

Rysunek 6.267.
Rozmiar pamięci RAM dla wirtualnej maszyny

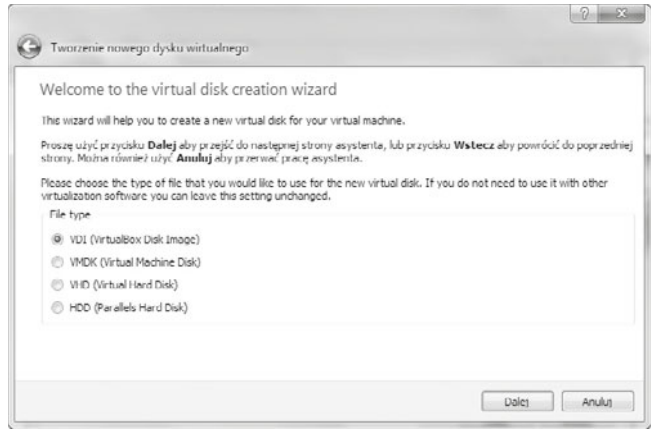


W następnym kroku należy określić rozmiar wirtualnego dysku (rysunek 6.268) oraz typ pliku, w jakim będzie zapisany dysk wirtualny (rysunek 6.269).

Rysunek 6.268.
Określenie rozmiaru wirtualnej partycji

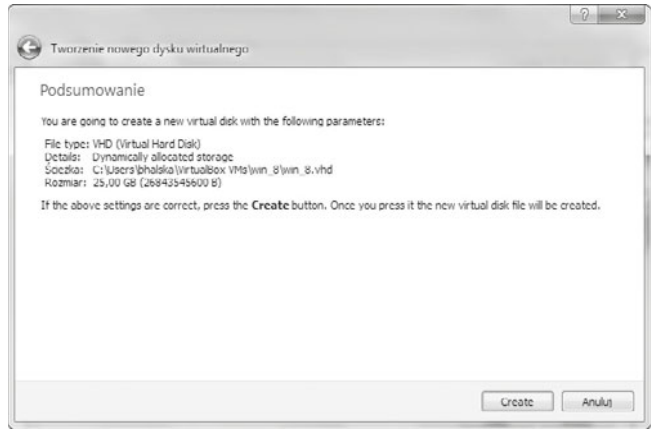


Rysunek 6.269. Określenie typu, w jakim będzie zapisany wirtualny dysk



W ostatnim oknie kreatora jest wyświetlane podsumowanie dla nowo tworzonej maszyny (rysunek 6.270).

Rysunek 6.270. Podsumowanie dla nowo tworzonej wirtualnej maszyny



ĆWICZENIA

1. Zainstaluj program VirtualBox, utwórz wirtualną maszynę oraz zainstaluj na niej dowolny system operacyjny.
2. Zainstaluj program VMware Player, utwórz wirtualną maszynę oraz zainstaluj na niej dowolny system operacyjny.

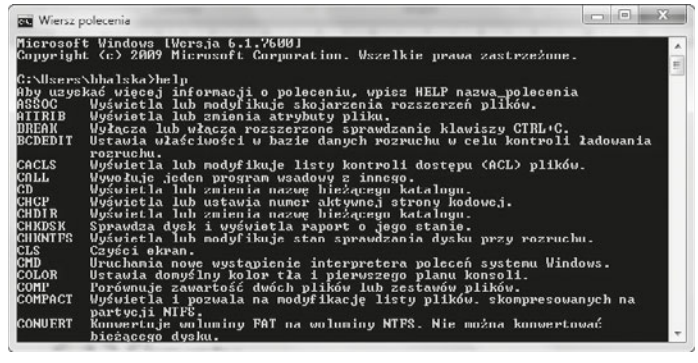
PYTANIA

1. Co to jest wirtualizacja?

6.12. Pliki wsadowe

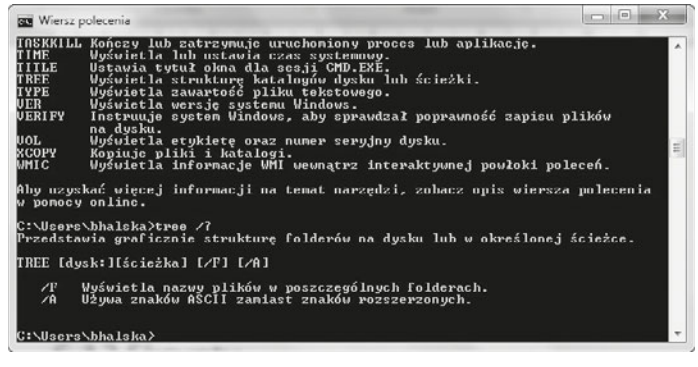
Pliki wsadowe (ang. *batch files*) to zestaw poleceń systemu operacyjnego wykonywanych w trybie wsadowym, zapisywanych w plikach tekstowych — (tzw. skryptach). Do działania nie wymagają trybu graficznego i są wykonywane w trybie tekstowym. Pliki wsadowe w systemach Windows są zapisywane w plikach z rozszerzeniem *.bat* lub *.cmd*. Do tworzenia skryptów wystarczy Notatnik oraz znajomość poleceń systemu Windows. Aby uzyskać pomoc na ich temat, należy wpisać w wierszu poleceń `help` (rysunek 6.271).

Rysunek 6.271. Wiersz poleceń



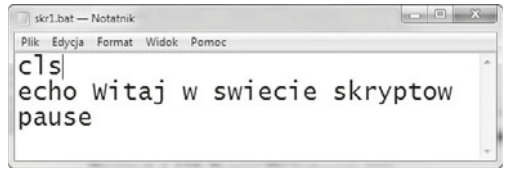
By otrzymać pomoc dla konkretnego polecenia, należy po wpisaniu nazwy polecenia dodać `/?`, np.: `tree /?` (rysunek 6.272).

Rysunek 6.272. Pomoc dla polecenia tree



Skrypt nr 1

Rysunek 6.273. Skrypt nr 1



- `cls` — czyszczenie ekranu.
- `echo` — wyświetlanie komunikatu na ekranie.
- `pause` — zatrzymanie przetwarzania pliku wsadowego do naciśnięcia dowolnego klawisza.

Aby zablokować wyświetlanie wykonywanych komend w danym pliku, należy jako pierwszą dodać linijkę: `@echo off`.

Skrypt nr 2

Rysunek 6.274.
Skrypt nr 2

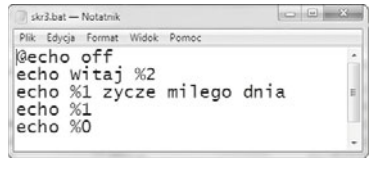
- `mkdir` — tworzenie katalogu.
- `dir` — wyświetlanie zawartości katalogu.

Istnieje możliwość stosowania parametrów wywołania skryptów:

- `%0` — zawsze zwróci nazwę skryptu, w którym jest zastosowany.
- Zmienne od `%1` do `%9` mogą przechowywać kolejne wartości przekazywane jako parametry uruchomieniowe skryptu.

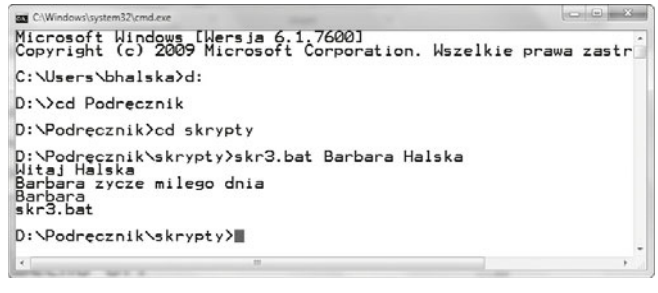
Skrypt nr 3

Rysunek 6.275.
Skrypt nr 3



Uruchamiając ten skrypt, po podaniu jego nazwy należy podać wartości dla dwóch parametrów, np.: dla `%1` — `Barbara %2 Halska`.

Rysunek 6.276.
Efekt działania skryptu nr 3

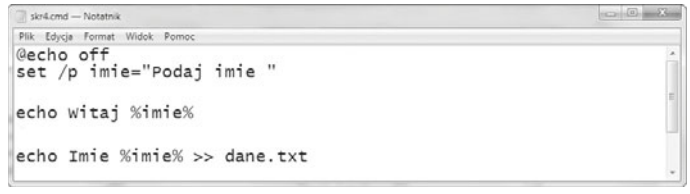


Istnieje możliwość pobierania wartości do zmiennych podczas wykonywania programów poprzez polecenie

```
set /p
```

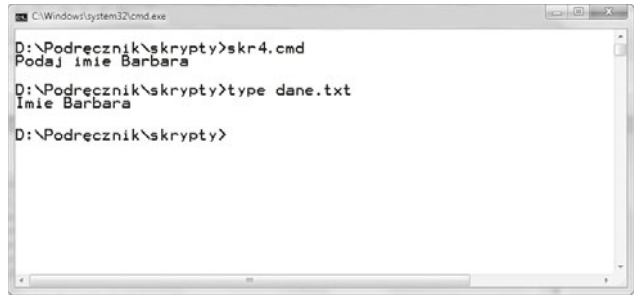
Skrypt nr 4

Rysunek 6.277.
Skrypt nr 4



- `set /p imie="Podaj imie"` — umożliwia wyświetlenie na ekranie *Podaj imie*, a następnie zapisanie w zmiennej *imie* tego, co użytkownik wprowadzi z klawiatury.
- `%imie%` — umożliwia odwołanie do zawartości zmiennej `imie`.
- >> — umożliwia przesłanie strumieniowo wyników polecenia znajdującego się z lewej strony znaków >> do pliku znajdującego się z prawej strony.

Rysunek 6.278.
Wynik działania skryptu nr 4

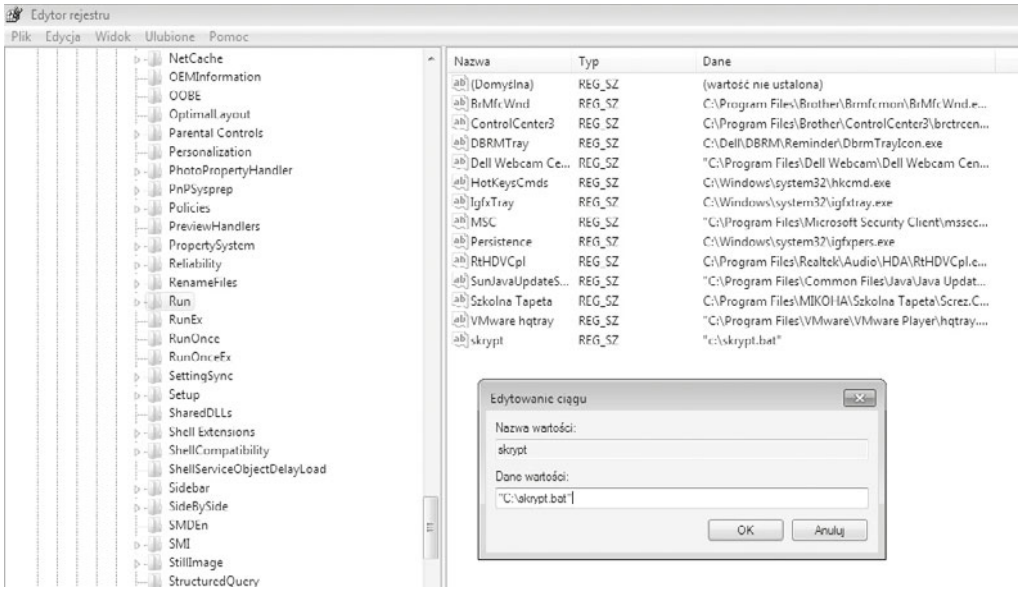


Jeżeli chcemy, aby plik wsadowy uruchamiał się podczas startu systemu Windows, po jego przygotowaniu i zapisaniu z rozszerzeniem *.bat* należy za pomocą polecenia *regedit* umieścić w rejestrze klucz, w którym będzie znajdowała się ścieżka dostępu do tego pliku.

Po uruchomieniu Edytora rejestru odszukujemy klucz:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,

po czym z menu wybieramy *Edycja/Nowy/Wartość ciągu*. Po wpisaniu nazwy naszego wpisu klikamy go prawym przyciskiem myszy, z menu kontekstowego wybieramy *Modyfikuj* i wpisujemy w polu *Dane wartości* ścieżkę dostępu do pliku wsadowego (rysunek 6.279).



Rysunek 6.279. Tworzenie klucza w rejestrze systemu

6.12.1. Polecenia związane z obsługą sieci

Dodawanie do domeny

Systemy Windows oferują wiele poleceń związanych z obsługą sieci.

Dodawanie do domeny umożliwia skrypt:

```
@echo off
netdom join %computername% /domain:helion.local /userd:administrator /
passwordd:p@ssw0rd /reboot:5
```

Odłączenie komputera od domeny:

```
@echo off
netdom remove %computername% /domain:helion.local /userd:administrator /
passwordd:p@ssw0rd /reboot:5
```

Poniższe polecenie konfiguruje statycznie kartę sieciową (interfejs) o nazwie Local Area Network o adresie 192.168.18.1 oraz masce podsieci 255.255.255.0:

```
netsh interface ip set address name="Local Area Network" source=static
addr=192.168.18.1 mask=255.255.255.0
```

Poniższe polecenie konfiguruje kartę sieciową do pobierania adresu IP z serwera DHCP:

```
netsh interface ip set address name="Local Area Network" source=dhcp
```

Poniższe polecenie dodaje ustawienie serwera DNS dla interfejsu sieciowego:

```
netsh interface ip set dns name="Local Area Network" source=static
addr=194.204.159.1
```

Poniższe polecenie podłącza (mapuje) zdalny katalog *dane* do dysku X:

```
net use x: \\192.168.18.1\dane
```

Poniższe polecenie odłącza katalog *dane* od dysku X:

```
net use x: \\192.168.18.1\dane /delete
```

ĆWICZENIA

1. Utwórz powyższe skrypty i sprawdź ich działanie.

PYTANIA

1. Z jakim rozszerzeniem możemy zapisywać skrypty w systemach Windows?
2. Który z parametrów zwraca nazwę skryptu?
3. Jakie polecenie pozwala utworzyć katalog?
4. Jakie polecenie pozwala podpiąć komputer pod domenę?
5. Jakie polecenie pozwala mapować udział sieciowy?

7 Linux

Linux jest systemem operacyjnym, który może występować w wersji dla stacji roboczej, np. OpenSUSE, lub dla serwera, np. SUSE Linux Enterprise Server (SLES). Systemy operacyjne w wersji dla stacji roboczej zostały omówione w podręczniku *Kwalifikacja E.12. Montaż i eksploatacja komputerów osobistych oraz urządzeń peryferyjnych. Podręcznik do nauki zawodu technik informatyk*.

SUSE Linux Enterprise Server (SLES) — komercyjna dystrybucja Linuksa rozpowszechniana przez firmę Novell, która udostępnia wiele aplikacji umożliwiających utrzymanie i administrację. Flagowym narzędziem do administracji jest YaST2.

Najważniejsze cechy tej dystrybucji to:

- mechanizm wirtualizacji — serwer Xen,
- samba — serwer pozwalający na współdzielenie zasobów,
- serwer WWW — oparty na serwerze Apache,
- serwer wydruku — cups.

Graficzne interfejsy linuksowe

Bazą dla każdego graficznego interfejsu użytkownika jest X Window System, zwany również X lub X11.

Dystrybucje Linuksa najczęściej opierają się na dwóch środowiskach (omówionych w podręczniku *Kwalifikacja E.12. Montaż i eksploatacja komputerów osobistych oraz urządzeń peryferyjnych. Podręcznik do nauki zawodu technik informatyk*):

- KDE,
- GNOME.

7.1. Instalacja systemu SUSE Linux Enterprise Server (SLES)

UWAGA

Wymagania systemowe:

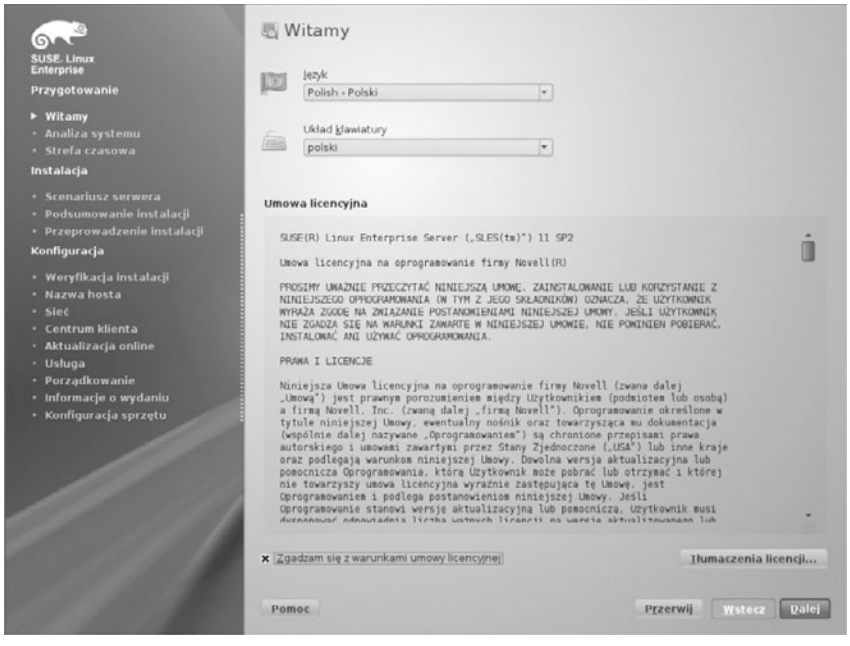
- Komputer osobisty z procesorem Pentium* III 500 MHz lub lepszym (zalecany Pentium 4 2.4 GHz lub lepszy albo dowolny procesor AMD64 lub Intel* EM64T).
- Fizyczna pamięć RAM 512 MB (zalecana 1 GB).
- Dostępna przestrzeń dyskowa 3 GB (zalecana większa).
- Ekran o rozdzielczości 800×600 (zalecana 1024×768 lub większa).

ISO instalacyjne systemu SUSE Linux Enterprise Server (SLES) 11 SP 2 można pobrać ze strony *www.suse.pl*.

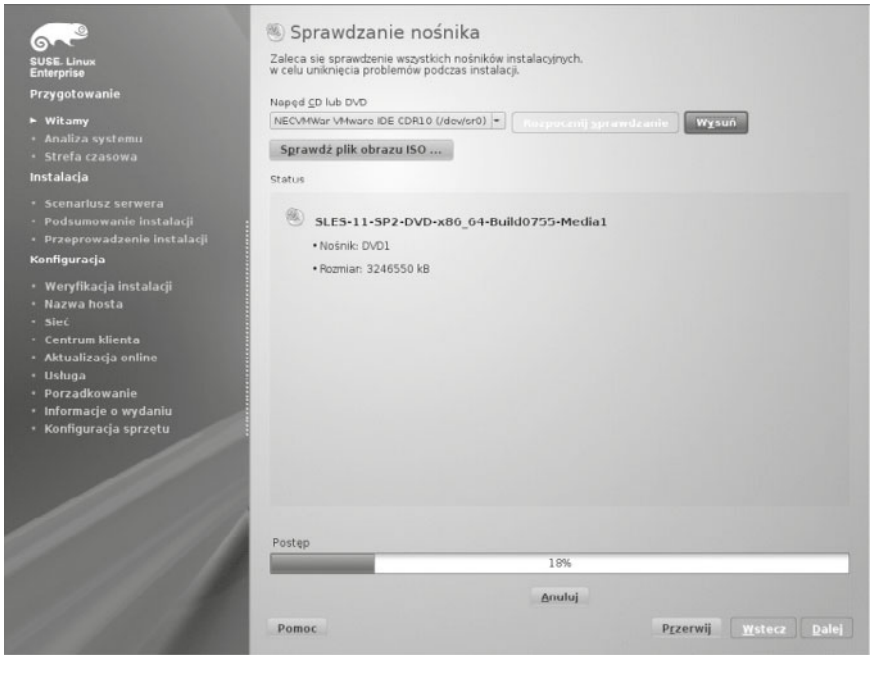
1. W pierwszym oknie instalatora (rysunek 7.1) należy wybrać opcję *Instalacja*, można również zdefiniować język, co pozwoli przeprowadzić instalację w języku polskim (*F2 Język Polski*).

Rysunek 7.1. Kreator instalacji SUSE

2. W kolejnym oknie kreatora (rysunek 7.2) trzeba określić język oraz układ klawiatury i zapoznać się z licencją, którą należy zaakceptować, aby przejść do następnego okna.
3. W kolejnym kroku (rysunek 7.3) można sprawdzić nośnik. Jeżeli na nośniku będą jakieś błędy, instalacja zostanie anulowana. Ten krok zabezpiecza przed błędami, które mogą wystąpić podczas instalacji.

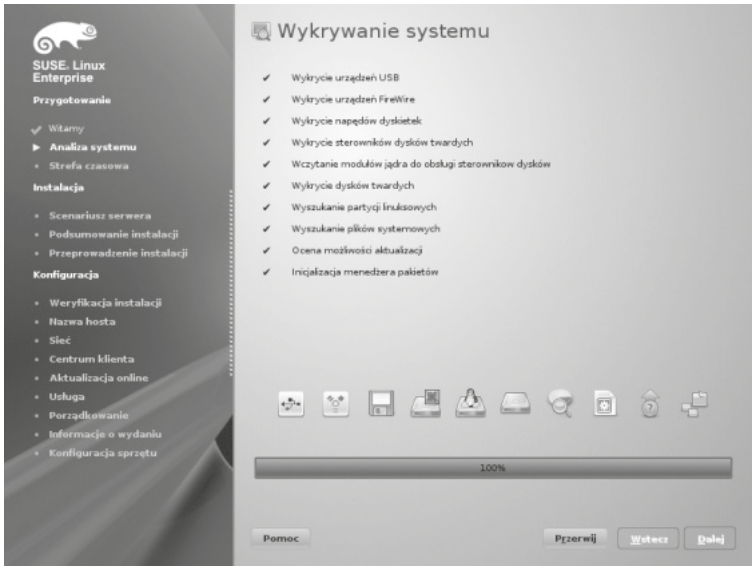


Rysunek 7.2. Kreator instalacji



Rysunek 7.3. Sprawdzanie nośnika

5. Po sprawdzeniu nośnika następuje faza instalacji, podczas której są wykrywane i sprawdzane podzespoły (rysunek 7.4).



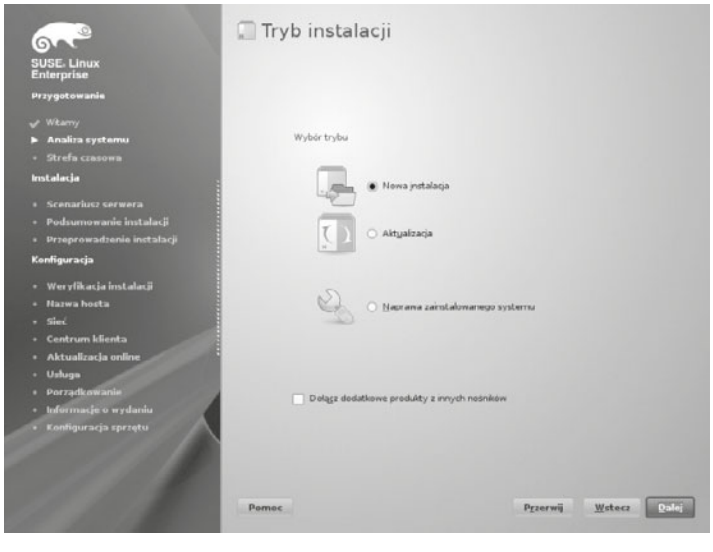
Rysunek 7.4. Wykrywanie podzespołów komputera

6. Po sprawdzeniu podzespołów należy wybrać tryb instalacji (rysunek 7.5):

a) *Nowa instalacja*,

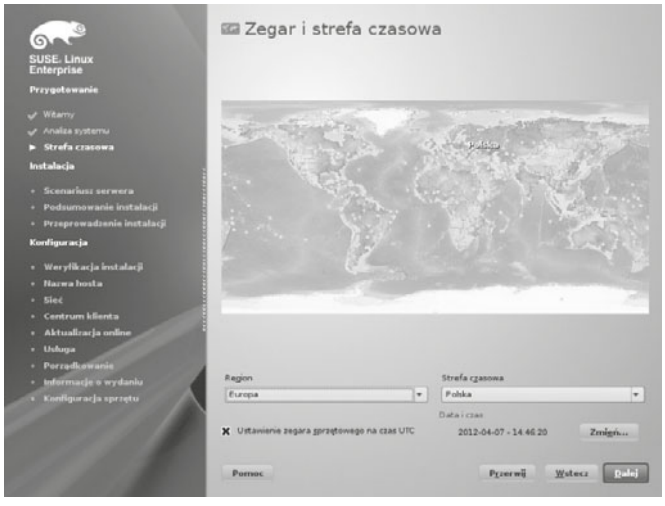
b) *Aktualizacja*,

c) *Naprawa zainstalowanego systemu*.



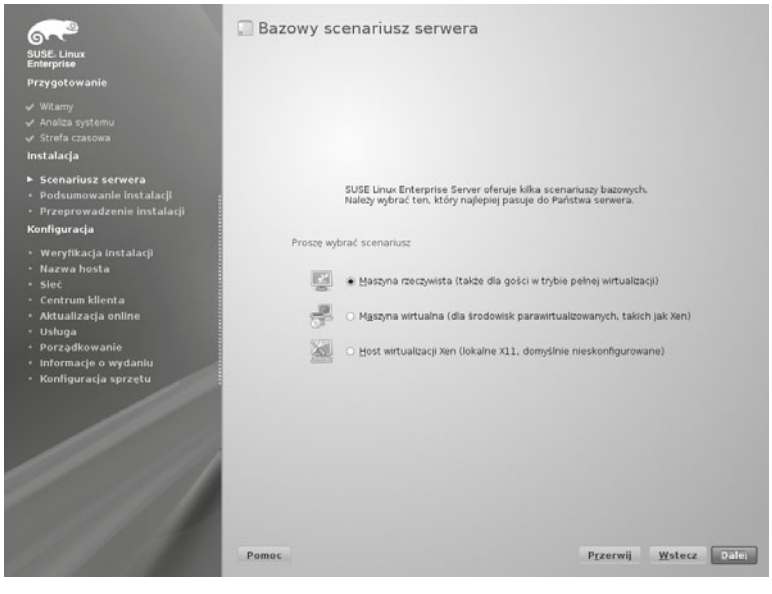
Rysunek 7.5. Tryb instalacji

7. W kolejnym kroku (rysunek 7.6) trzeba określić strefę czasową.



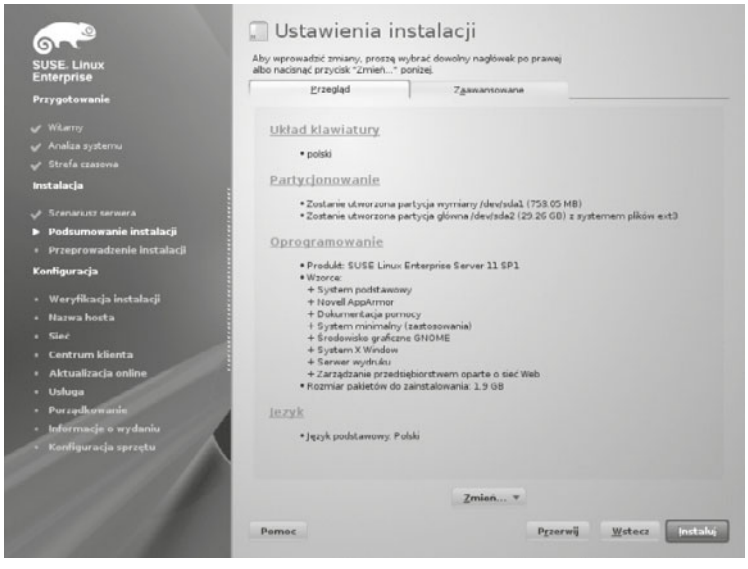
Rysunek 7.6. Zegar i strefa czasowa

8. Krok siódmy pozwala na wybór scenariusza pracy serwera (rysunek 7.7), który obejmuje: maszynę fizyczną (używaną także dla w pełni wirtualizowanych maszyn), maszynę wirtualną (dla środowisk parawirtualizowanych, takich jak Xen) i host wirtualizacji Xen (do użycia jak platforma hostowa hypervisora). Dorównuje to rosnącej liczbie opcji dopuszczanych w serwerowych edycjach Windows 2008, gdzie wirtualne maszyny są obecnie częścią procesu preinstalacji.



Rysunek 7.7. Wybór scenariusza instalacji

9. Okna *Ustawienia instalacji* (rysunek 7.8) można użyć do przeglądania zaproponowanych opcji instalacji i partycjonowania oraz do zmiany poszczególnych opcji w razie potrzeby. Zakładka *Przegląd* zawiera opcje wymagające interwencji ręcznej (w większości instalacji). Zakładka *Zaawansowane* zawiera bardziej rozbudowane opcje. Na tym etapie jest możliwe samodzielne ustawienie partycjonowania dysku.



Rysunek 7.8. Ustawienia instalacji

UWAGA

Systemy plików dostępne w Linuksie:

a) ext2, ext3, ext4 — popularny system plików, omówiony w podręczniku *Kwalifikacja E.12. Montaż i eksploatacja komputerów osobistych oraz urządzeń peryferyjnych. Podręcznik do nauki zawodu technik informatyk*,

b) reiserFS — system plików, który obsługuje duże partycje oraz duże pliki do 16 TB,

c) XFS — to 64-bitowy system plików przeznaczony do serwerów.

Domyślnym systemem plików SLES 11 jest ext3, aczkolwiek reiserFS jest również obsługiwany, tak jak inne, w tym: ext2, jfs, NTFS, ext4.

SWAP to partycja wymiany, używana przez system do tymczasowego przechowywania danych w pamięci RAM,

Jeżeli dokonujemy samodzielnego partycjonowania dysku, należy pamiętać, że system Linux do prawidłowego funkcjonowania potrzebuje partycji rozruchowej z systemem plików ext. Ponadto zaleca się również utworzenie partycji SWAP.

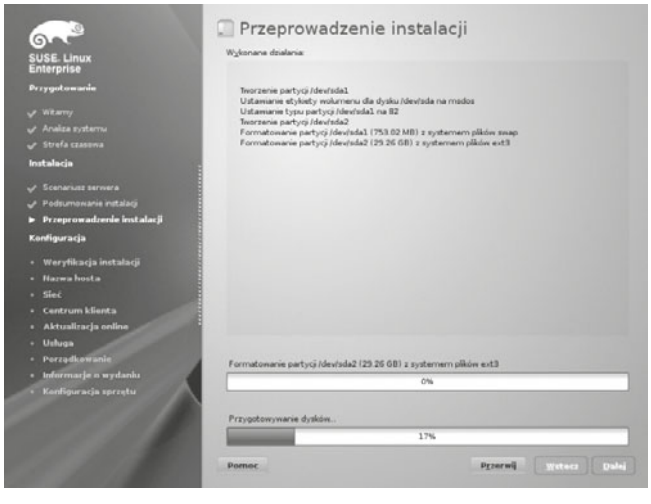
WAŻNE

Jeśli nie dokonano żadnych zmian w wybranym oprogramowaniu, domyślnym środowiskiem graficznym będzie GNOME. Aby zainstalować KDE, należy kliknąć odnośnik *Oprogramowanie* i wybrać *KDE*. Zależnie od dostępnej przestrzeni na dysku można wybrać instalację obu środowisk. Aby kontynuować, należy nacisnąć *Instaluj*.

10. W kolejnym oknie (rysunek 7.9) wyświetla się informacja o warunkach licencji czcionek od Agfa. Po akceptacji można przejść do następnego kroku instalacji.

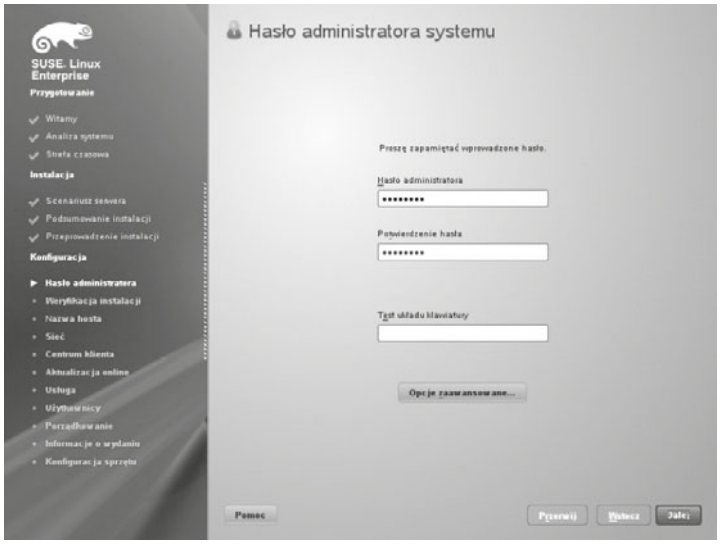
Rysunek 7.9. Warunki licencji

11. Po zaakceptowaniu warunków licencji oraz zatwierdzeniu instalacji rozpoczyna się podstawowy proces instalacji, w wyniku którego dysk zostanie podzielony na partycje (rysunek 7.10).



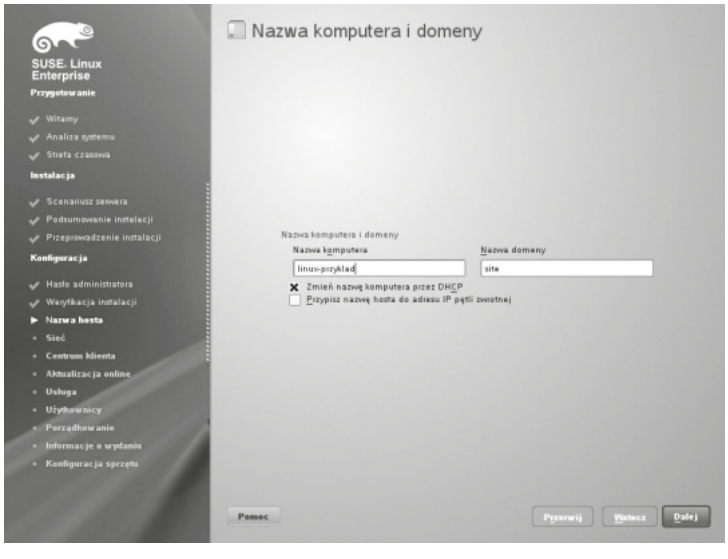
Rysunek 7.10. Przeprowadzenie podstawowej instalacji

12. Po zakończeniu podstawowej instalacji i restarcie systemu można przystąpić do konfiguracji, a pierwszym krokiem jest nadanie hasła dla konta *root*, czyli administratora (rysunek 7.11).



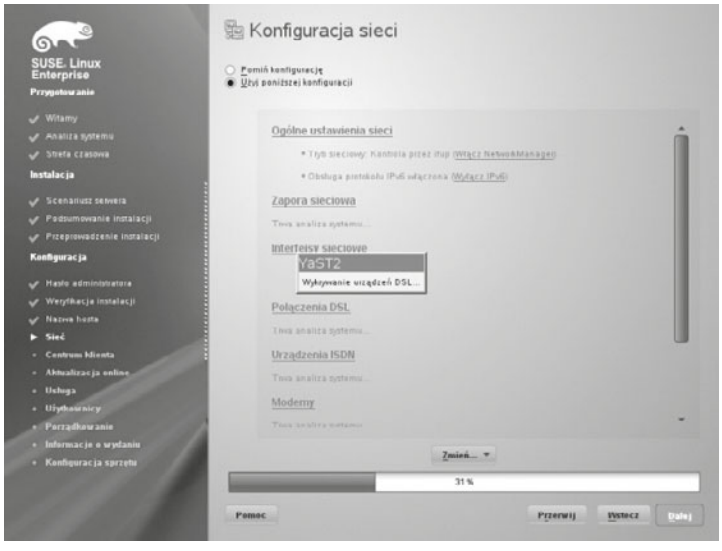
Rysunek 7.11. Definiowanie hasła dla administratora

13. W następnym oknie konfiguracji (rysunek 7.12) należy nadać nazwę dla serwera oraz nazwę domeny DNS, do której on należy.



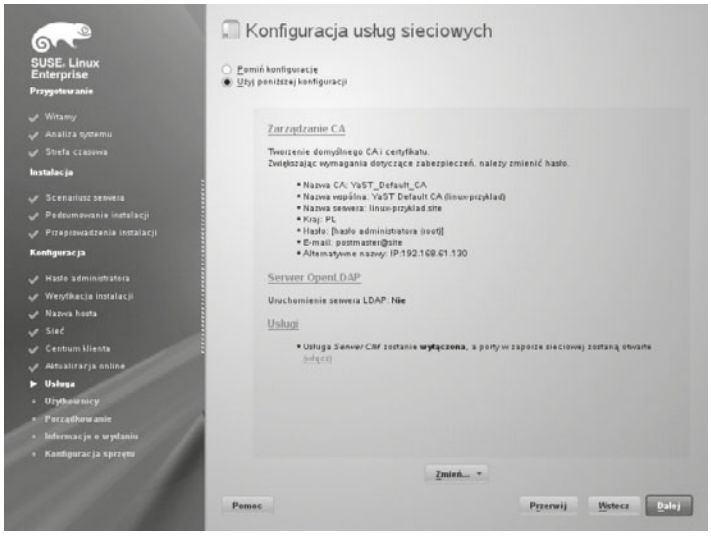
Rysunek 7.12. Nazwa komputera i domeny

14. W kolejnym oknie kreatora konfiguracji (rysunek 7.13) można skonfigurować ustawienia interfejsów sieciowych czy zapory systemowej.



Rysunek 7.13. Konfiguracja sieci

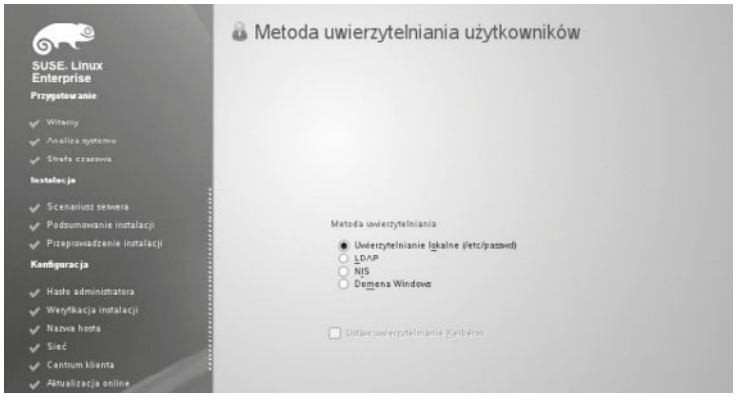
15. W kolejnych krokach następuje testowanie konfiguracji sieci i po zakończeniu zostaje wyświetlona informacja o tym, jaką konfigurację usług sieciowych wybraliśmy. Można jeszcze zmodyfikować ustawienia lub zatwierdzić je, przechodząc do następnego kroku (rysunek 7.14).



Rysunek 7.14. Podsumowanie konfiguracji usług sieciowych

16. W kolejnych oknach można określić centrum klienta oraz aktualizację online.

17. Następne okno (rysunek 7.16) umożliwia utworzenie konta dla użytkownika oraz zmianę domyślnych ustawień konfiguracyjnych dla nowo tworzonego konta (zostało to omówione w części dotyczącej zakładania konta użytkownika).



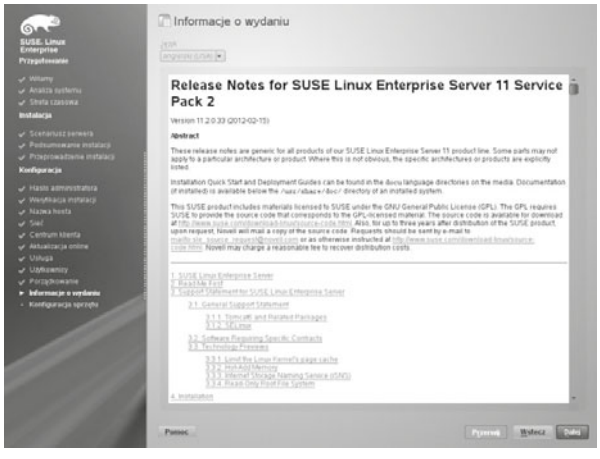
Rysunek 7.15. Metoda uwierzytelniania

18. W oknie *Metoda uwierzytelniania użytkowników* (rysunek 7.15) *można wybrać jedną z następujących opcji*:

- **a)** *Uwierzytelnianie lokalne (/etc/passwd)*,
- **b)** *LDAP* (ang. *Lightweight Directory Access Protocol*) — jest zbiorem protokołów przeznaczonym do uzyskiwania dostępu i zarządzania informacją dotyczącą zasobów,
- **c)** *NIS* (ang. *Network Information Service*) — jest protokołem typu klient-serwer, opracowanym przez Sun Microsystems, służącym do śledzenia użytkowników i nazw hostów w sieci,
- **d)** *Domena Windows*.

Rysunek 7.16. Konto użytkownika

19. W ostatnich oknach instalacji wyświetla się informacja o systemie, który właśnie zainstalowaliśmy (rysunek 7.17), konfiguracji sprzętowej oraz o możliwości wygenerowania pliku AutoYaST. Jest on kopią ustawień zdefiniowanych podczas tej instalacji i może być wykorzystany do automatycznej instalacji następnych systemów.



Rysunek 7.17. Informacja o zainstalowanym systemie

20. Po zakończeniu instalacji system się resetuje i pozwala na pierwsze zalogowanie (rysunek 7.18).

Rysunek 7.18. Pierwsze logowanie do systemu

ĆWICZENIA

1. Zainstaluj SLES ze środowiskiem graficznym GNOME.

PYTANIA

1. Jaki system plików jest wymagany do instalacji systemu Linux?
2. Wymień dwa środowiska graficzne.
3. Wymień wymagania systemowe.

7.2. Podstawy systemu operacyjnego Linux

7.2.1. System plików

System plików tworzy mechanizm bezpośredniego przechowywania i dostępu do danych zapisanych na dyskach. Na potrzeby Linuksa został stworzony system plików ext (ang. *Extended File System*). Wraz z rozwojem systemu operacyjnego były tworzone kolejne wersje systemu plików — w 2008 roku został wydany system ext4, który umożliwia obsługę woluminów o wielkości do 1024 petabajtów (1 petabajt = 1024 terabajty).

System plików Linuksa w przeciwieństwie do windowsowych nie dzieli przestrzeni dyskowej na dyski logiczne — w ramach niego jest dostępny tylko jeden katalog główny z hierarchiczną strukturą katalogów.

Katalog główny jest oznaczany ukośnikiem — znakiem /. Katalogi w systemie Linux zostały przedstawione poniżej.

/ — katalog główny,

/bin — zawiera wykonywalne pliki najbardziej podstawowych narzędzi systemowych dostępne dla wszystkich użytkowników,

/boot — zawiera pliki niezbędne do uruchomienia systemu w przypadku większości dystrybucji, a także obraz jądra systemu,

/dev — zawiera pliki specjalne wskazujące na urządzenia w systemie — za ich pomocą system komunikuje się z nimi,

/etc — zawiera pliki konfiguracyjne systemu,

/home — w tym katalogu znajdują się katalogi domowe użytkowników systemu,

/lib — zawiera dzielone biblioteki systemowe oraz moduły jądra w katalogu */lib/modules*,

/mnt — tutaj są montowane (podłączane do systemu) dodatkowe dyski (np. partycje systemu Windows),

/proc — wirtualny katalog zawierający informacje o uruchomionych procesach,

/root — katalog domowy użytkownika *root*,

/sbin — zawiera pliki wykonywalne, które mogą być uruchomione tylko przez administratora systemu,

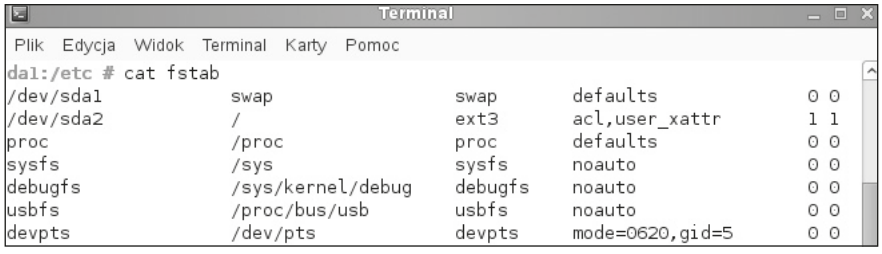
/sys — zawiera pliki systemu operacyjnego,

/tmp — katalog służący do zapisu plików tymczasowych,

/usr — katalog zawierający dodatkowe oprogramowanie (odpowiednik katalogu *Program Files* w systemie Windows),

/var — katalog przeznaczony na pliki, które często ulegają zmianie, np. logi systemowe, pliki udostępniane przez serwer WWW itp.

Informacje na temat montowanych partycji i systemu plików znajdują się w pliku */etc/fstab* (rysunek 7.19).



Rysunek 7.19. Zawartość pliku fstab

Tabela 7.1. Wybrane opcje montowania systemu plików

Opcja	Opis	Ext2	Ext3	Ext4	ReiserFS	XSF	SWAP
Montowanie z wykorzystaniem */etc/fstab*	Zawiera informacje dotyczące identyfikacji systemu plików	+	+	+	+	+	+
Montowanie przez użytkownika	Udostępnia funkcję montowania przez zwykłego użytkownika	+	+	+	+	+	–
Lista kontroli dostępu ACL	Pomaga kontrolować prawa dostępu do plików i katalogów	+	+	+	+	–	–
Tryb księgowania	Określa tryb księgowania danych	–	+	+	+	–	–
Priorytety SWAP	Określa numer priorytetu partycji	–	–	–	–	–	+

W systemie Linux wyróżnia się następujące rodzaje plików:

- plik zwykły (oznaczany znakiem „–” w wynikach działania komendy `ls -l`) — zbiór danych zapisanych na dysku,
- katalog (oznaczany „d”) — określający katalog na dysku,
- dowiązanie symboliczne (oznaczane „l”) — określające plik wskazujący na inny plik w systemie,
- urządzenie znakowe (oznaczane „c”) — plik specjalny reprezentujący urządzenie, do którego dostęp jest realizowany znak po znaku (bajt po bajcie),
- urządzenie blokowe (oznaczane „b”) — plik specjalny reprezentujący urządzenie, do którego dostęp jest realizowany przez większe porcje danych zwane blokami,

- nazwany potok (ang. *named pipe*, oznaczany literą „p") — plik wymiany informacji między procesami działający jako kolejka FIFO (ang. *first in first out*),
- gniazdo (ang. *socket*, oznaczane „s") — plik wymiany między procesami.

W systemie plików Linux dane są uporządkowane. Podłączenie kolejnego dysku do systemu wymaga jego **zamontowania** (od ang. *mount*) — dotyczy to zarówno dysków CD, jak i dysków twardych. Dostęp do danych zapisanych na tych dyskach jest możliwy poprzez katalog, w którym zostały one zamontowane. Dla przykładu gdy mamy dysk C:\ w systemie FAT32 i zamontujemy go w katalogu */mnt/drivec* — ten folder zawiera całą zawartość dysku C:\.

Jeśli na dysku FAT32 w systemie Windows został utworzony katalog *c:\dokumenty*, w systemie Linux będzie on dostępny pod adresem*/mnt/drivec/dokumenty*.

Przykład montowania partycji FAT:

```
mount -t vfat /dev/sda1 /mnt/drivec
```

gdzie `- t` oznacza system plików, a `/dev/sda1` miejsce, gdzie znajduje się partycja, natomiast `/mnt/drivec` miejsce, gdzie zostanie zamontowana, a więc katalog, w którym znajdzie się Windowsowy dysk *C*. Jeżeli chcemy dowiedzieć się więcej na temat polecenia `mount`, wystarczy skorzystać z parametru `d--help` polecenia:

```
: mount --help
```

lub użyć wbudowanego system pomocy "man":

```
: man mount
```

7.2.2. Urządzenia w systemie Linux

Linux postrzega urządzenia podłączone do komputera jako pliki, co powoduje, że każde urządzenie ma swój odpowiednik w katalogu */dev*. Aby odwołać się do jakiegoś urządzenia, system wykorzystuje odpowiedni plik w tym katalogu. W przypadku dysków zarówno fizyczne urządzenia, jak i poszczególne partycje są reprezentowane w katalogu */dev*.

Najważniejsze urządzenia w systemie operacyjnym są przedstawiane za pomocą następujących katalogów:

/dev/console — konsola systemu operacyjnego,

/dev/mouse — mysz szeregowa,

/dev/hda — pierwszy dysk IDE,

/dev/hda1 — pierwsza partycja pierwszego dysku,

/dev/hda2 — druga partycja pierwszego dysku,

/dev/hdb — drugi dysk IDE,

/dev/hdb1 — pierwsza partycja drugiego dysku,

/dev/sda — pierwszy dysk SATA,

/dev/sda1 — pierwsza partycja na pierwszym dysku,

/dev/null — urządzenie puste (do testów).

7.2.3. Interpreter poleceń

Jądro systemu operacyjnego (ang. *kernel*) zapewnia zarządzanie pamięcią i procesami, dostęp do zgromadzonych danych itp. Za komunikację z użytkownikiem jest odpowiedzialna **powłoka** systemu operacyjnego (ang. *shell*), zwana także **interpreterem poleceń**. Powłoka systemu Linux pełni taką samą funkcję jak konsola cmd w systemie Windows, jej zadaniem jest wykonywanie poleceń konsolowych. Przy czym użytkownik może wybrać jedną z kilku dostępnych powłok systemowych.

Powłoka systemu operacyjnego to program, który udostępnia interfejs pomiędzy użytkownikiem a jądrem systemu; w przypadku systemu Linux ma ona postać wiersza poleceń. Jądro systemu zawiera wszelkie procedury potrzebne do przeprowadzania operacji wejścia i wyjścia, zarządzania plikami itp.; powłoka pozwala z nich korzystać.

Powłoki obsługują również skryptowy język programowania, który umożliwia tworzenie tzw. **skryptów powłoki** (odpowiedników plików wsadowych w systemie Windows).

W systemie Linux najczęściej są używane następujące powłoki systemowe:

- **sh** (od ang. *Shell*) — to powłoka stworzona dla systemów Unix przez Stephena Bourne'a; zwana jest także powłoką Bourne'a.
- **rsh** (od ang. *Remote Shell*)— jest jedną z odmian powłoki Bourne'a. Litera R w jej nazwie odnosi się do słowa *reduced*, czyli ograniczona. Udostępnia okrojone funkcje powłoki sh.
- **csh** (od ang. *C Shell*) — jest jedną z powłok systemowych, która nawiązuje do składni języka C. Powłoka csh wniosła wiele ulepszeń w stosunku do sh, m.in. aliasy i historię komend.
- **ksh** (od ang. *Korn Shell*) — jest całkowicie kompatybilna wstecz z powłoką sh, zawiera także wiele elementów z powłoki csh, np. historię wpisanych komend. ksh obejmuje wbudowany system obliczania wyrażeń arytmetycznych oraz zaawansowane funkcje skryptów, podobne do tych używanych w bardziej zaawansowanych językach programowania, takich jak AWK, Sed i Perl.
- **bash** (od ang. *Bourne Again Shell*) — rozszerzona powłoka zawierająca historię poleceń oraz konstrukcje umożliwiające sterowanie przepływem danych (`if`, `while`, `for`). Jest ona domyślną powłoką systemu Linux.
- **zsh** (od ang. *Z Shell*) - nadaje się zarówno do interaktywnej pracy z systemem, jak i do wykonywania skryptów. Jest powłoką najbardziej przypominającą Korn shell (ksh), jednak zawiera wiele ulepszeń, takich jak: edycja wiersza poleceń, historia oraz programowalne dopełnianie poleceń.

W systemie Linux powłoka jest ładowana po zalogowaniu użytkownika.

Polecenia rozpoznawane przez interpreter dotyczą:

- tworzenia procesów i zarządzania nimi,
- obsługi wejścia-wyjścia,
- administrowania pamięcią pomocniczą i operacyjną,
- dostępu do plików i katalogów.

7.2.4. Konsola, terminal

System Linux powstał jako system tekstowy. Graficzny interfejs użytkownika jest nakładką na system tekstowy. W niektórych dystrybucjach po instalacji domyślnie jest ładowany graficzny system okienek dla systemu Linux zwany X Window.

System Linux powstał na bazie systemu Unix, który był eksploatowany na komputerach typu mainframe — wydajnych maszynach, gdzie praca odbywała się poprzez terminal pozwalający na komunikację z komputerem. Aby lepiej wykorzystywać moc obliczeniową, do komputera podłączano wiele terminali, które umożliwiały pracę wielu użytkownikom jednocześnie.

Mianem konsoli określa się sposób tekstowej komunikacji z systemem operacyjnym — przykładem konsoli może być wiersz poleceń w systemie Windows lub tryb tekstowy systemu Linux. Aktualnie terminy konsola i terminal są używane zamiennie, przy czym ich geneza jest różna.

Po uruchomieniu systemu Linux dla użytkownika jest domyślnie (konfiguracja w /etc/inittab) dostępnych 7 konsol wirtualnych — 7 środowisk pozwalających na równoczesną pracę użytkowników. Przełączanie między nimi umożliwia kombinacja klawiszy *Alt+F1* — *Alt+F7*. Przejście do poszczególnych konsol z uruchomionego środowiska X Window (uruchamianego w domyślnej konfiguracji) umożliwia kombinacja *Ctrl+Alt+F1* — *Ctrl+Alt+F6*.

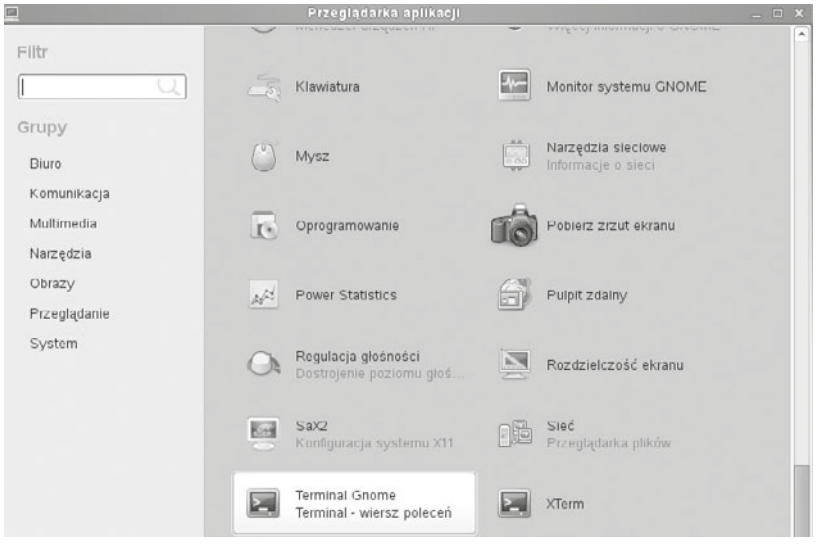
Na każdej konsoli można zalogować się jako inny użytkownik, dzięki czemu można wykonywać wiele zadań równocześnie. Pracując na konsoli tekstowej, użytkownik może uruchamiać zadania w tle, co pozwala na przetwarzanie naraz wielu zadań, a także pozostawienie działających programów po wylogowaniu użytkownika.

Linux umożliwia pracę na konsoli tekstowej, gdy jest uruchomione środowisko X Window. W tym celu należy uruchomić tzw. emulator terminala, który otwiera okno tekstowe z prawami aktualnie zalogowanego użytkownika.

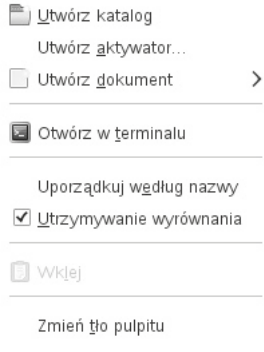
W systemie Linux istnieje możliwość zdalnej pracy — poprzez program emulujący terminal można połączyć się z serwerem przez sieć i uruchamiać wybrane zadania. Zdalne logowanie do systemu pozwala na uruchamianie wszystkich zadań, w tym także środowiska graficznego. Programy umożliwiające zdalną pracę to **telnet** (transmisja jest nieszyfrowana) oraz **ssh** (transmisja szyfrowana).

Terminal możemy znaleźć w aplikacjach dystrybucji SLES w kategorii dotyczącej systemu, gdzie mamy do dyspozycji *Terminal Gnome* lub *XTerm* (rysunek 7.20), możemy

go również wywołać, klikając na pulpicie prawym klawiszem myszy — pojawi się okno, w którym należy wybrać opcję *Otwórz w terminalu* (rysunek 7.21).



Rysunek 7.20. Przeglądarka aplikacji/System/Terminal Gnome



Rysunek 7.21. Okno dialogowe

7.2.5. Uprawnienia w systemie Linux

W systemie Linux nadaje się prawa dostępu do plików i katalogów. Te prawa to *odczyt* (*read*), *zapis* (*write*), *wykonanie* (*execute*). Mogą być one przydzielone użytkownikowi (właścicielowi), grupie, która jest właścicielem pliku, oraz wszystkim pozostałym użytkownikom.

Poszczególne prawa oznaczane są literami: odczyt — „r”, zapis — „w”, wykonanie — „x”, a także za pomocą liczb: odczyt — „4”, zapis — „2”, wykonanie — „1”. Sumowanie poszczególnych liczb odpowiadających uprawnieniom pozwala na ich proste przedstawianie. Poniższa tabela prezentuje zapis uprawnień oraz ich wyjaśnienie.

Tabela 7.2. Uprawnienia w postaci liczbowej

Odczyt 4	Zapis 2	Wykonanie 1	
			0 — brak uprawnień
		X	1 — wykonanie
	X		2 — zapis
	X	X	3 — zapis, wykonanie
X			4 — odczyt
X		X	5 — odczyt, wykonanie
X	X		6 — odczyt, zapis
X	X	X	7 — odczyt, zapis, wykonanie

Każdy plik oraz katalog ma przypisanego swojego właściciela oraz grupę właściciela — dla nich oraz pozostałych użytkowników są przydzielane prawa dostępu.

Aby wyświetlić listę plików i katalogów w konsoli tekstowej, należy skorzystać z polecenia `ls`. Opcje tej komendy, które pozwolą wyświetlić więcej informacji, to:

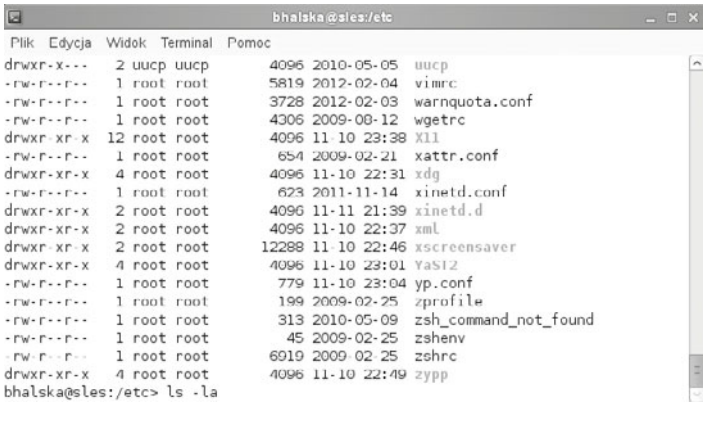
`-a` — wyświetla wszystkie pliki i katalogi (w tym także ukryte),

`-l` — wyświetla szczegółową informację o plikach (w tym czas utworzenia oraz prawa dostępu),

`-s` — wyświetla rozmiar plików (w blokach),

`-sh` — wyświetla rozmiar plików w przejrzystym formacie (np. 3 K, 300 M, 3 G).

Po wydaniu polecenia `ls -la` zostanie wyświetlona lista wszystkich plików i katalogów wraz z prawami dostępu (rysunek 7.22).



Rysunek 7.22. Wynik działania polecenia ls –la

Przykład pokazuje katalogi znajdujące się w katalogu */etc*. Kolejne kolumny oznaczają:

- prawa dostępu,
- liczbę dowiązań,
- nazwę właściciela pliku,
- nazwę grupy,
- rozmiar pliku,
- datę modyfikacji,
- nazwę pliku.

Pierwsza część wyświetlanych danych oprócz praw dostępu zawiera również informację o typie danej pozycji na liście. Pierwszy znak przyjmuje jedną z następujących postaci:

- „–" oznacza zwykły plik,
- „b" oznacza specjalny plik blokowy,
- „c" oznacza specjalny plik znakowy,
- „d" oznacza katalog,
- „l" oznacza link symboliczny,
- „p" oznacza potok,
- „s" oznacza gniazdo.

Kolejne litery oznaczają prawa dostępu dla właściciela pliku (znaki od 2–4), grupy (znaki 5–7) oraz pozostałych użytkowników (8–10). Przykładowy wpis:

```
drwx------ 7 user  users        4096 07-21 13:00 user
```

oznacza katalog (pierwsza litera d) z prawami odczytu, zapisu i wykonania dla właściciela (grupa i pozostali użytkownicy nie mają żadnych praw do tego katalogu), właścicielem jest użytkownik user, grupa, do której należy właściciel pliku, to users, katalog zajmuje na dysku 4 kb, ostatnia modyfikacja została przeprowadzona 21 lipca bieżącego roku o godzinie 13:00, nazwa katalogu to user.

Zmianę praw dostępu do katalogu lub pliku umożliwia polecenie `chmod`. Wymaga ono określenia, czyje uprawnienia należy zmienić, na jakie oraz jakiego pliku lub katalogu ta zmiana będzie dotyczyć. Prawa dostępu mogą być podane zarówno w postaci liczbowej, jak i znakowej. W przypadku postaci liczbowej podaje się trzy kolejne liczby reprezentujące prawa dla właściciela, grupy oraz pozostałych użytkowników. Składnia polecenia wygląda następująco:

```
chmod kod_prawa_dostępu nazwa_pliku_lub_katalogu
```

Dla przykładu

```
chmod 640 info.txt
```

oznacza, że plik *info.txt* będzie miał następujące prawa dostępu:

dla właściciela: odczyt i zapis (4+2),

dla grupy: odczyt (4),

dla pozostałych użytkowników: brak praw (0).

Przy nadawaniu praw dostępu w postaci znakowej, składnia wygląda nieco inaczej:

```
chmod kto_operacja_prawo nazwa_zasobu
```

gdzie: kto — określa komu są nadawane prawa (u — właścicielowi pliku, g — grupie właściciela pliku, o — innym użytkownikom, a — wszystkim),

operacja — oznacza przypisanie lub odebranie prawa (+ lub –),

prawo — oznacza prawa, które się zmienia (w — zapis, r — odczyt, x — wykonanie).

Dla przykładu

```
chmod u-w info.txt
```

oznacza, że właściciel pliku *info.txt* stracił prawo zapisu do pliku.

Zmianę właściciela plików umożliwia polecenie `chown`, ze składnią:

```
chown nowy_właściciel nazwa_pliku_lub_katalogu
```

np.

```
chown user katalog1
```

Zmianę grupy pliku umożliwia polecenie `chgrp`, ze składnią:

```
chgrp nowa_grupa nazwa_pliku_lub_katalogu
```

np.

```
chgrp users katalog1
```

Można również, w jednym poleceniu, dokonać zmiany zarówno grupy, jak i właściciela pliku:

```
chown user:grupa plik
```

Poleceniem `chown` możemy również zmienić właściciela grupy plików:

```
chown user:grupa *.odt
```

7.2.6. Podstawowe polecenia systemu Linux

System Linux zawiera polecenia związane z usługami działającymi zarówno na rzecz użytkownika, jak i systemu operacyjnego.

Polecenia związane z uzyskiwaniem pomocy:

- `man [polecenie]` — wyświetla podręcznik systemowy (ang. *manual*) dotyczący wybranego polecenia, np. `man ls`,
- `[polecenie] --help` — wyświetla krótką pomoc na temat wybranego polecenia, np. `ls --help`,
- `apropos [temat]` — wyświetla listę poleceń związanych z wskazanym tematem, np. `apropos director`.

Polecenia związane z systemem operacyjnym:

- `su` — pozwala na logowanie na różne konta użytkowników,
  np. `su basia`; jeżeli wpiszemy tylko `su`, nastąpi logowanie na konto root,
- `sudo` — umożliwia wykonanie innego polecenia z uprawnieniami superużytkownika (root),
- `pwd` — wyświetla bieżący katalog (ścieżkę wskazującą, gdzie się aktualnie znajdujemy),
- `date`, `time` — wyświetla/ustawia datę lub czas systemowy,
- `last` — wyświetla listę ostatnich logowań do systemu,
- `uptime` — wyświetla czas, który upłynął od ostatniego restartu systemu,
- `history` — wyświetla listę ostatnio wykonywanych komend,
- `./nazwa_programu` — uruchamia program wykonywalny znajdujący się w bieżącym katalogu,
- `shutdown [-opcja] [-t liczba_sekund]` — zamyka (opcja `-h`)/restartuje (opcja `-r`) system operacyjny po określonej liczbie sekund, wymaga uprawnień administratora,
- `mount/unmount` — pozwala na zamontowanie (odmontowanie) dysku,
- `find` — pozwala na odszukanie pliku spełniającego odpowiednie warunki,
- np. `find / -name muzyka` odszuka w całym drzewie katalogów pliki i katalogi o nazwie *muzyka*,
- `startx` — uruchamia z poziomu terminala sesję graficznego interfejsu X Window.

Powyżej zostały wymienione tylko przykłady, więcej poleceń związanych z działaniem systemu operacyjnego jest dostępnych m.in. w katalogach */bin* oraz */sbin*.

Polecenia związane z plikami i katalogami

- `cp [plik_źródłowy] [plik_docelowy]` — kopiuje plik źródłowy na plik docelowy,
  np. `cp plik plik2`,
  np. `cp /home/halska/plik /home/halska/kopia`,
- `mv [plik_źródłowy] [plik_docelowy]` — przenosi lub zmienia nazwę pliku źródłowego,
- `rm [plik]` — kasuje pliki, `rm -r [katalog]` — kasuje katalog wraz z zawartością,
- `mkdir [nazwa_katalogu]` — tworzy nowy katalog,
- `cat [nazwa pliku]` — wyświetla zawartość pliku bez możliwości edycji,
- `touch [nazwa pliku]` — tworzy pusty plik.

Archiwizacja, kompresja i dekompresja plików

Podstawowym programem do archiwizacji — łączenia wielu plików w jedno archiwum — jest program **tar**. Program ten domyślne archiwizuje wskazane pliki bez ich kompresji — jest ona wymuszana parametrem. Użycie programu `tar` umożliwia składnia:

```
tar -opcje [nazwa_nowego_archiwum.tar] pliki_katalogi_
do_zarchiwizowania.
```

Najważniejsze opcje będące argumentami programu `tar` to:

`-c` — tworzy nowe archiwum,

`-f` — zapisuje archiwum do pliku (zamiast wysyłać do strumienia wyjściowego),

`-x` — rozpakowuje pliki z archiwum,

`-t` — wyświetla listę plików znajdujących się w archiwum,

`-u` — dodaje do archiwum tylko zmienione pliki,

`-r` — dołącza kolejne pliki do archiwum,

`-z` — kompresuje/dekompresuje archiwum programem gzip (tworzy archiwum *.tar.gz*).

Przykładem użycia programu `tar` może być kompresja plików zawierających logi systemowe — pliki zapisujące pewne operacje występujące w systemie operacyjnym:

```
tar -czf log.tar.gz /var/log/
```

Aby zdekompresować wybrany plik, można użyć polecenia:

```
tar -xzf log.tar.gz
```

System Linux oferuje wiele programów do kompresji danych (zmniejszania ich wielkości na dysku). Jednym z najpopularniejszych formatów pozwalających na kompresowanie plików zarówno w systemach Windows, jak i dystrybucjach Linuksa jest **ZIP**.

Aby utworzyć archiwum `ZIP` w systemach Linux, należy skorzystać z następującego polecenia:

```
zip nazwa_archiwum.zip pliki_do_kompresji
```

gdzie:

`nazwa_archiwum.zip` to plik wynikowy, który zostanie utworzony przez program kompresujący,

`pliki_do_kompresji` — to pliki, które mają zostać skompresowane.

Aby uzyskać informacje o skompresowanym pliku, można skorzystać z programu `zipinfo`, z parametrem w postaci nazwy pliku skompresowanego.

Do dekompresji archiwum ZIP jest używane polecenie ze składnią `unzip` *`nazwa_pliku.zip`*.

Innym formatem kompresji jest **gzip**, który tworzy pliki z rozszerzeniem *.gz*. Kompresja tym programem odbywa się przy użyciu składni:

```
gzip plik_do_kompresji
```

Aby przeprowadzić dekompresję, wykorzystuje się składnię:

```
gunzip archiwum.gz
```

7.2.7. Obsługa programu vi/vim

Wraz z każdą dystrybucją systemu Linux są rozprowadzane różne edytory tekstu. Jednym z najpopularniejszych jest edytor **vi** (od ang. *visual*) i jego następca — **vim** (od ang. *vi improved* — vi poprawione) (rysunek 7.23). Edytor ten mimo pracy w trybie tekstowym oferuje wiele opcji znanych z rozbudowanych graficznych edytorów tekstów, takich jak kopiowanie, zaznaczanie bloku tekstu, kolorowanie składni w przypadku edycji kodu źródłowego itp.

Praca w trybie tekstowym początkowo może się wydawać niewygodna, jednak po zapoznaniu się z programem staje się bardzo efektywna.

Aby uruchomić edytor tekstu, należy użyć składni:

```
vi nazwa_pliku
```

która uruchomi okno programu z wczytanym plikiem do edycji.

Edytor vi pracuje w dwóch trybach — **trybie wprowadzania tekstu** (tryb edycji) oraz **trybie poleceń** (w którym są przeprowadzane operacje na wprowadzonym tekście). Edytor vim oferuje dodatkowo **tryb wizualny**, który pozwala na operowanie na blokach tekstu.

Program uruchamia się w trybie poleceń, na ekranie jest wyświetlana zawartość edytowanego pliku.

Aby rozpocząć wprowadzanie danych do pliku, należy przejść w tryb edycji poprzez naciśnięcie klawisza *I* (od ang. *insert* — znaki są wprowadzane w miejscu, w którym znajduje się kursor) lub klawisza *A* (od ang. *append* — znaki są wprowadzane w miejscu za kursorem), po czym na dole ekranu pojawi się nazwa trybu — *insert* (lub *wprowadzanie*). Wprowadzanie tekstu odbywa się w sposób intuicyjny poprzez klawisze alfanumeryczne. Nawigacja po tekście jest możliwa za pomocą klawiszy kursora.

Aby wrócić do trybu poleceń, należy nacisnąć klawisz *Esc*. W tym trybie można przeprowadzać zaawansowaną edycję tekstu za pomocą odpowiednich poleceń. Najważniejsze z nich, pozwalające na zakończenie pracy z programem i zapis pliku, to:

`:w` — zapisuje plik,

`:w` *`nazwa_pliku`* — zapisuje zmiany w pliku pod nową nazwą,

`:q` — zamyka program,

`:q!` — zamyka program bez zapisania zmian.

Polecenia można łączyć ze sobą, np.

`:wq` — zapisuje plik i zamyka program.

Inne polecenia dostępne w trybie poleceń są związane z edycją tekstów:

`i` — przechodzi w tryb edycji (dopisuje dane od miejsca, w którym znajduje się kursor),

`a` — przechodzi w tryb edycji (dopisuje dane za kursorem),

`A` — przechodzi do trybu edycji z dopisywaniem na końcu linii,

`R` — przechodzi do trybu edycji z nadpisywaniem znaków,

`o` — tworzy nową linię pod linią, w której znajduje się kursor, i przechodzi do trybu edycji,

`O` — tworzy nową linię nad linią, w której znajduje się kursor, i przechodzi do trybu edycji,

`r<litera>` — zmienia literę znajdującą się pod kursorem,

`h` — przesuwa kursor o znak w lewo,

`j` — przesuwa kursor o linię w dół,

`k` — przesuwa kursor o linię do góry,

`l` — przesuwa kursor o znak w prawo,

`W` — przesuwa kursor o słowo do przodu,

`B` — przesuwa kursor o słowo do tyłu,

`G` — przechodzi do ostatniego wiersza,

`<liczba>G` — przechodzi do wskazanego wiersza,

`x` — usuwa znak pod kursorem,

`dd` — usuwa bieżącą linię,

`yy` — kopiuje bieżącą linię do schowka,

`p` — wstawia dane ze schowka,

`u` — cofa ostatnią operację,

CTRL+R — powtarza operację usuniętą,

`/wzorzec` — wyszukuje wyraz zgodnie z `wzorcem` w dokumencie, nawigacja po wynikach jest możliwa przez klawisze *n/N*,

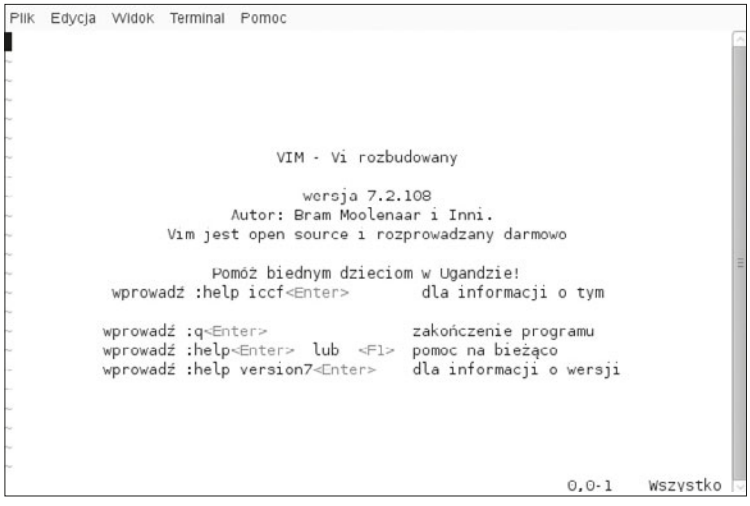
`:s/tekst1/tekst2` — zmienia `tekst1` na `tekst2`,

`v` — przechodzi do trybu wizualnego (wyłącznie w vim), który pozwala na zaznaczanie danych. Zaznaczenia mogą być kopiowane, przenoszone, usuwane itp.,

`:sp<nazwa_pliku>` — dzieli okno programu na dwie części i otwiera plik w nowej części okna,

CTRL+W — przenosi kursor między kolejnymi oknami programu.

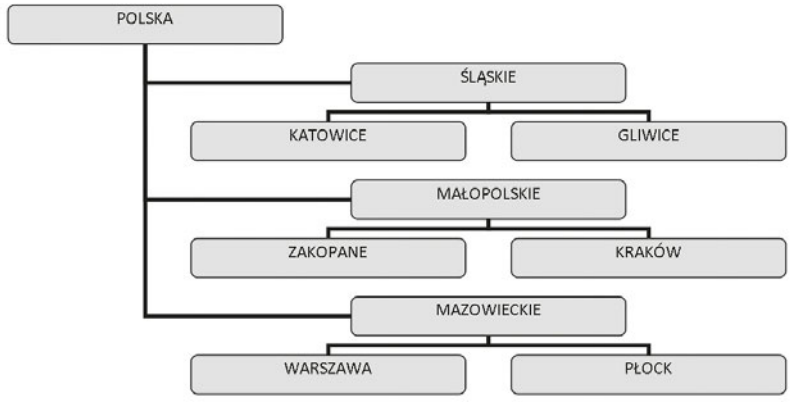
Powyżej przedstawiono jedynie podstawowe polecenia programu vi, który, jak widać, oferuje bardzo wiele wygodnych funkcji pozwalających na zaawansowaną edycję tekstu. Korzystanie z programu na początku wydaje się skomplikowane, jednak z czasem edycja tekstu przy użyciu trybu poleceń pozwala na bardzo wydajną pracę.



Rysunek 7.23. Edytor vi

ĆWICZENIA

1. Sprawdź zawartość pliku *fstab*.
2. Wywołaj konsolę i korzystając z edytora vi, stwórz w swoim katalogu plik o nazwie *dane*, a następnie wprowadź do niego swoje imię i nazwisko.
3. Sprawdź prawa dostępu do tego pliku.
4. Zrób kopię tego pliku, nazywając ją *kopiadane*.
5. Stwórz katalog *kopie* i do niego skopiuj plik *dane*.
6. Stwórz katalog *dane* i do niego przenieś plik *dane*.
7. Zrób archiwum z katalogu *dane*.
8. W swoim katalogu domowym utwórz następującą strukturę katalogów:



PYTANIA

1. Wymień najważniejsze katalogi systemowe zapisywane w katalogu głównym systemu Linux. Jakie dane są w nich przechowywane?
2. Który z katalogów systemu Linux przechowuje pliki konfiguracyjne?
4. Wymień najważniejsze katalogi zapisywane w katalogu głównym systemu Linux. Jakie dane są w nich przechowywane?
5. Jakim poleceniem możemy znaleźć plik?
6. Jakim poleceniem możemy sprawdzić bieżącą ścieżkę?
7. W jaki sposób powtórzyć ostatnio wykonane polecenia w trybie tekstowym?
8. W jaki sposób sprawdzić parametry wywołania dostępne dla wybranego polecenia?
9. Wymień polecenia związane z zarządzaniem katalogami w systemie Linux.
10. Jakie polecenie pozwala na wyszukiwanie plików?
11. Jakie polecenie pozwala na bezpieczne zamknięcie systemu Linux?

7.3. Pakiety systemu Linux

Instalacja oprogramowania w systemie Linux wygląda nieco inaczej niż w systemach Windows — oprogramowanie jest rozprowadzane jako **pakiety dystrybucyjne**, **programy instalacyjne** lub **kody źródłowe** do samodzielnej kompilacji.

7.3.1. Pakiety dystrybucyjne

Aby uprościć sposób instalacji dodatkowych programów, wydawcy dystrybucji tworzą tzw. **repozytoria oprogramowania** — specjalne serwery, na których są składowane wszystkie **pakiety** (czyli programy, biblioteki, sterowniki, dokumentacja itd.) dla danej dystrybucji, dzięki czemu stają się one łatwo dostępne i mogą być instalowane w jednakowy sposób.

Pakiety to odpowiednio przygotowane archiwa w formie binarnej, zawierające pliki z oprogramowaniem. Dodatkowo zawierają one także specjalne metadane, które umożliwiają automatyczne skonfigurowanie programu do instalacji, oraz dokumentację dla danej paczki.

Niektóre pakiety do poprawnego działania wymagają innych pakietów — pomiędzy nimi tworzą się **zależności**. Aby instalacja była kompletna, należy wraz z pakietem głównym zainstalować te pakiety, z którymi łączą go wspomniane zależności.

Istnieją różne rodzaje pakietów dystrybucyjnych — najczęściej powiązanych z dystrybucją systemu operacyjnego:

- **rpm** — Red Hat Package — występują w dystrybucjach opartych na Red Hat — jak Fedora Core, Mandriva, SUSE,

- **deb** — występują w dystrybucjach opartych na Debianie — Ubuntu, Mepis, Knoppix,
- **tgz** — archiwa tar — pakiety dystrybucyjne w Slackware.

W każdej dystrybucji systemu jest dołączane oprogramowanie do zarządzania pakietami dystrybucyjnymi, które pozwala na pobieranie, instalowanie, aktualizowanie i usuwanie pakietów. Takie oprogramowanie jest dostępne zarówno w wersji graficznej, jak i tekstowej.

W dystrybucji SUSE Linux za zarządzanie pakietami odpowiada program `zypper`. Zypper to konsolowy menedżer pakietów. Pozwala on na zarządzanie oprogramowaniem oraz aktualizacjami systemu operacyjnego.

Poniżej zostały przedstawione najczęściej wykorzystywane funkcje pozwalające na zarządzanie oprogramowaniem.

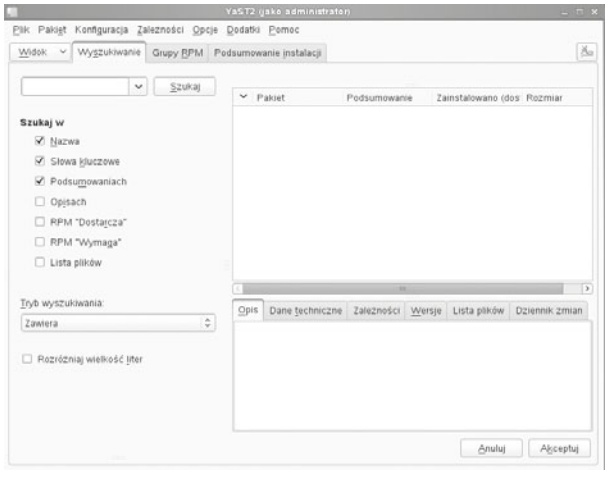
Najczęściej wykorzystywane komendy zyppera pokazuje tabela 7.3.

Tabela 7.3. Komendy dla narzędzia zypper

`zypper`	wyświetla wszystkie informacje o użyciu zyppera
`zypper help search`	wyświetla pomoc związaną z `search`, czyli wyszukiwaniem
`zypper list-patches`	wyświetla informację o poprawkach
`zypper patch`	nakłada poprawki (czyli aktualizuje system)
`zypper search sqlite`	wyszukuje pakiety, których nazwa zawiera `sqlite`
`zypper remove sqlite2`	usuwa `sqlite2`
`zypper install sqlite3`	instaluje `sqlite3`
`zypper install YaST2 *`	instaluje wszystkie pakiety, których nazwa zaczyna się od `YaST2 *`
`zypper update`	aktualizuje pakiety do ich najnowszych wersji — o ile to możliwe
`zypper repos` lub `zypper lr`	wyświetla listę repozytoriów
`zypper lr -u`	wyświetla informacje o położeniu (URI) repozytorium
`zypper lr -d`	wyświetla dodatkowe informacje o repozytoriach
`zypper lr -P`	wyświetla priorytet repozytoriów i sortuje je według niego
`zypper lr -e moja_lista`	zapisuje (eksportuje) repozytoria do pliku *moja_lista.repo*

`zypper ref`	odświeża informacje o dostępnych pakietach
`zypper dup`	pobiera i instaluje pakiety — UWAGA! zalecane, gdy trzeba zmienić dostawców pakietów
`zypper addrepo` *`położenie_repozytorium nazwa`*	umożliwia dodanie repozytoriów
`zypper refresh`	odświeża repozytoria
`zypper removerepo`	usuwa repozytoria

Aby zainstalować program w trybie graficznym, należy uruchomić menedżer pakietów dla trybu graficznego — znajduje się on w YaST2 w sekcji *Oprogramowanie* w narzędziu *Zarządzanie oprogramowaniem* (rysunek 7.24).



Rysunek 7.24. Okno dodawania i usuwania programów w GNOME

Różne narzędzia do instalacji programów:

- `apt` (ang. *Advanced Packaging Tool*) w dystrybucji Debian, Ubuntu,
- `urpmi` w dystrybucji Mandriva,
- `slapt-get` w dystrybucji Slackware,
- `rpm`, `zypper` w dystrybucji SUSE.

7.3.2. Programy w postaci plików binarnych

Instalacja programów za pomocą instalatorów odbywa się podobnie jak w systemie Windows — polega na uruchomieniu programu. Aby uruchomić program, należy najpierw nadać plikowi prawo do uruchamiania, używając komendy:

```
chmod u+x nazwa_pliku
```

a następnie go uruchomić:

```
./nazwa_pliku
```

W przypadku instalacji w trybie graficznym wystarczy uruchomić plik poprzez dwukrotne kliknięcie.

7.3.3. Kompilacja z plików źródłowych

Jeśli wybrany program jest rozprowadzany jako pliki źródłowe, można przeprowadzić jego kompilację. Większość programów dla systemu Linux jest rozprowadzana na licencji GPL, więc ich pliki źródłowe również są udostępnione, co pozwala na ich kompilację oraz poprawianie. Kompilacja programu bezpośrednio na komputerze, na którym ma on pracować, pozwala na lepsze dopasowanie kodu, dzięki czemu programy skompilowane w niektórych przypadkach pracują wydajniej niż te zainstalowane z pakietów dystrybucyjnych.

Najczęściej pliki źródłowe są rozprowadzane jako pliki skompresowane, w związku z czym pierwszym krokiem przed właściwą kompilacją jest rozpakowanie plików.

Dekompresja jest przeprowadzana w zależności od programu kompresującego:

Dla plików tar:

```
tar -xvf plik.tar
```

dla plików tar.gz:

```
tar -xvzf plik.tar.gz
```

dla plików tar.bz2

```
tar -xvjf plik.tar.bz2
```

Po dekompresji plików źródłowych należy wejść do katalogu, w którym się one znajdują, a następnie uruchomić skrypt `configure`, sprawdzający dostępność wszystkich potrzebnych bibliotek oraz ostrzegający przed możliwymi błędami w kompilacji. Do kompilacji pakietów jest niezbędne posiadanie kompilatora. Aby go uruchomić, należy użyć komendy:

```
./configure
```

Po sprawdzeniu dostępności bibliotek trzeba przeprowadzić właściwą kompilację poprzez komendę:

```
make
```

Instalację skompilowanych plików źródłowych umożliwia wydanie komendy z uprawnieniami root:

```
make install
```

Aby odinstalować oprogramowanie zainstalowane ze źródeł, z poziomu tego samego katalogu, z którego przeprowadzana była instalacja, należy użyć komend:

```
make uninstall
```

a następnie:

```
make clean
```

ĆWICZENIA

1. Zainstaluj Kadu przy użyciu dowolnych pakietów.

PYTANIA

1. Jakie są pakiety dystrybucyjne w systemach Linux?
2. Jakim poleceniem w SLES instalujemy pakiety z konsoli?
3. Jakim poleceniem kompilujemy program z plików źródłowych?

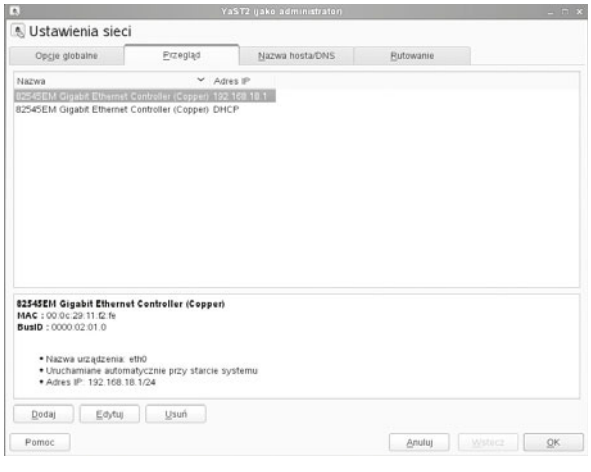
7.4. Konfiguracja interfejsów sieciowych

W systemie SLES wykrywanie sprzętu jest w dużym stopniu zautomatyzowane. Podczas instalacji systemu narzędzie administracyjne YaST2 wykrywa kartę sieciową oraz inne urządzenia sieciowe.

Jeżeli w sieci istnieje jakiś serwer DHCP, to system po wykryciu karty i otrzymaniu odpowiedzi od serwera DHCP od razu ją uaktywni. Jeśli chcemy zdefiniować statyczny adres, możemy do tego wykorzystać narzędzie *Ustawienia sieciowe* w YaST2 lub konsolę i polecenie `ifconfig`. Przed uruchomieniem narzędzia administracyjnego zostaniemy poproszeni o podanie hasła do konta *root*.

W celu skonfigurowania karty należy w narzędziu YaST2 wybrać *Urządzenia sieciowe*, następnie *Ustawienia sieciowe*.

Otworzy się okno *Ustawienia sieci* z listą wykrytych zainstalowanych kart sieciowych w zakładce *Przegląd* (rysunek 7.25).



Rysunek 7.25. Konfiguracja kart sieciowych

W zakładce *Opcje globalne* należy wybrać jedną z dwóch metod konfiguracji sieci:

- opcję *Kontrola użytkownika przez program NetworkManager* — aplet *NetworkManager* będzie używany do zarządzania wszystkimi interfejsami sieciowymi,
- metodę tradycyjną, czyli opcję *Kontrola przez ifup*.

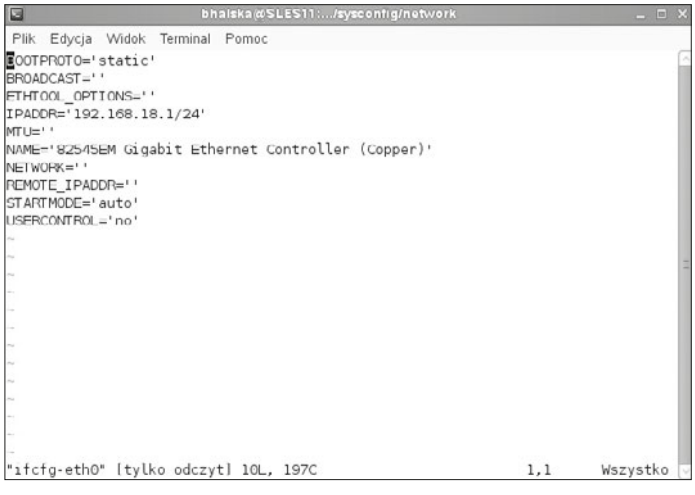
W tej zakładce można również włączyć/wyłączyć obsługę IPv6 i wybrać opcje konfiguracji klienta DHCP.

W celu modyfikacji ustawień karty należy wybrać opcję *Edytuj* w zakładce *Przegląd*.

7.4.1. Konfiguracja karty sieciowej w terminalu

Jeśli mamy jedną kartę sieciową w komputerze, to będzie ona widoczna w systemie jako eth0, kolejna będzie miała numer eth1 itd.

W celu konfiguracji karty eth0 musimy edytować plik */etc/sysconfig/network/ifcfg-eth0/* za pomocą dowolnego edytora pliku, np. vi (rysunek 7.26).



Rysunek 7.26. Zawartość pliku /etc/sysconfig/network/ifcfg-eth0

Aby karta działała poprawnie, w tym pliku powinny znaleźć się następujące ustawienia:

- `IPADDR='192.168.0.2/24'` — opcja określająca adres karty sieciowej oraz maskę podsieci. `/24` odpowiada masce 255.255.255.0.
- `NETWORK=''` — adres samej sieci.
- `BROADCAST=''` — określa adres rozgłoszeniowy sieci. Pusty parametr oznacza, że adres rozgłoszeniowy wynika z adresu IP/maski podsieci, zgodnie z konfiguracją w */etc/sysconfig/network/config*.
- `STARTMODE=` — określa start urządzenia, może to być: `auto` — urządzenie jest uruchamiane automatycznie przy starcie systemu lub przy inicjalizacji; `manual` — urządzenie musi być uruchomione „ręcznie”.

- `BOOTPROTO='none'` — pozwala wybrać, w jaki sposób karta sieciowa ma otrzymywać adres. `"none"` można zastąpić przez `"static"` (statyczna konfiguracja) albo `"dhcp"` (konfiguracja zostanie dostarczona przez serwer DHCP).
- `MTU=''` — określa wartość MTU (*Maximum Transmission Unit*). Pusty parametr spowoduje przyjęcie wartości domyślnej, która dla protokołu Ethernet jest równa 1500 bajtów.
- `NAME=''` — nazwa karty sieciowej.

Jeżeli chcemy skonfigurować ustawienia karty sieciowej za pomocą polecenia `ifconfig`, musimy mieć uprawnienia użytkownika *root*, inaczej system zwróci komunikat błędu. Żeby zmienić uprawnienia, należy w konsoli wpisać polecenie `su`, następnie system poprosi o hasło do konta *root*.

Przykładowa konfiguracja (rysunek 7.27):

```
ifconfig eth0 192.168.18.1 netmask  255.255.255.0
```

Polecenie `ifconfig` poza umożliwieniem konfiguracji karty sieciowej pozwala również na sprawdzenie, w jaki sposób są już skonfigurowane interfejsy sieciowe. Aby uruchomić to polecenie, użytkownik musi mieć je przypisane do swojej zmiennej środowiskowej PATH. Jest to zmienna zawierająca oddzieloną dwukropkami listę katalogów — na niej powłoka będzie szukać programu, którego nazwę do wykonania wprowadził użytkownik (np. `ifconfig`). Jeżeli program nie zostanie znaleziony, powłoka wyświetli komunikat o błędzie (rysunek 7.27). Polecenie to można także uruchomić, korzystając z konta administratora. W tym celu należy w konsoli uzyskać uprawniania administratora poleceniem `su`, a następnie uzyskamy konfigurację kart przy użyciu polecenia `ifconfig`.

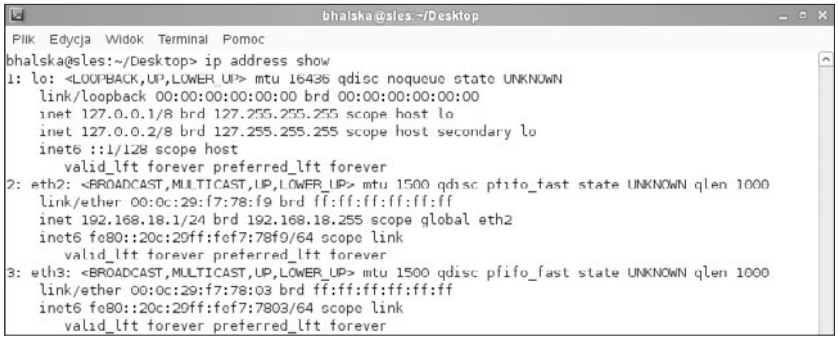
Rysunek 7.27. Wywołanie polecenia ifconfig

W celu dodania poleceń z */sbin* do zmiennej środowiskowej danego użytkownika należy wywołać polecenie:

```
export PATH="$PATH:/sbin"
```

Kolejnym narzędziem, które umożliwia konfigurację interfejsów sieciowych, jest polecenie `ip` (rysunek 7.28).

Np. `ip address show` — zostaną zwrócone adresy interfejsów sieciowych.



Rysunek 7.28. Wywołanie polecenia ip

Polecenia związane z interfejsami sieciowymi:

- `ifconfig` lub `ip` — umożliwia wyświetlanie statusu aktywnych interfejsów sieciowych oraz ich modyfikację.

ĆWICZENIA

1. Skonfiguruj dwa interfejsy:
   a. Pierwszy jako lokalny LAN z adresem statycznym: 192.168.*nr_w_dzienniku*.1.
   b. Drugi jako zewnętrzny WAN z adresem uzyskiwanym z serwera DHCP.
2. Sprawdź zawartość pliku konfiguracyjnego karty sieciowej.
3. Sprawdź adresy, wykorzystując polecenie `ifconfig`.
4. Sprawdź informację na temat interfejsów, wykorzystując polecenie `ip`.

PYTANIA

1. Jakim poleceniem sprawdzamy adres IP w systemie Linux?
2. W jakim pliku znajduje się konfiguracja interfejsów sieciowych?
3. Jaki wpis w pliku konfiguracyjnym dotyczy adresu?

7.5. Zarządzanie użytkownikami i grupami

W systemach operacyjnych Linux rozróżniamy dwa główne rodzaje użytkowników:

- zwykli użytkownicy: są to konta pozwalające na dostęp użytkowników do systemu i bezpieczną pracę w systemie,
- użytkownicy systemowi: są to konta tworzone podczas instalacji systemu używane przez rozmaite usługi, narzędzia i aplikacje, aby zapewnić efektywną pracę serwera.

Najważniejszym kontem w systemie Linux jest konto *root*. Jest to konto o najwyższych uprawnieniach i jedyne konto, które do przechowywania profilu ma przypisany katalog *root*. Pozostałe konta użytkowników są przechowywane w katalogu *home*.

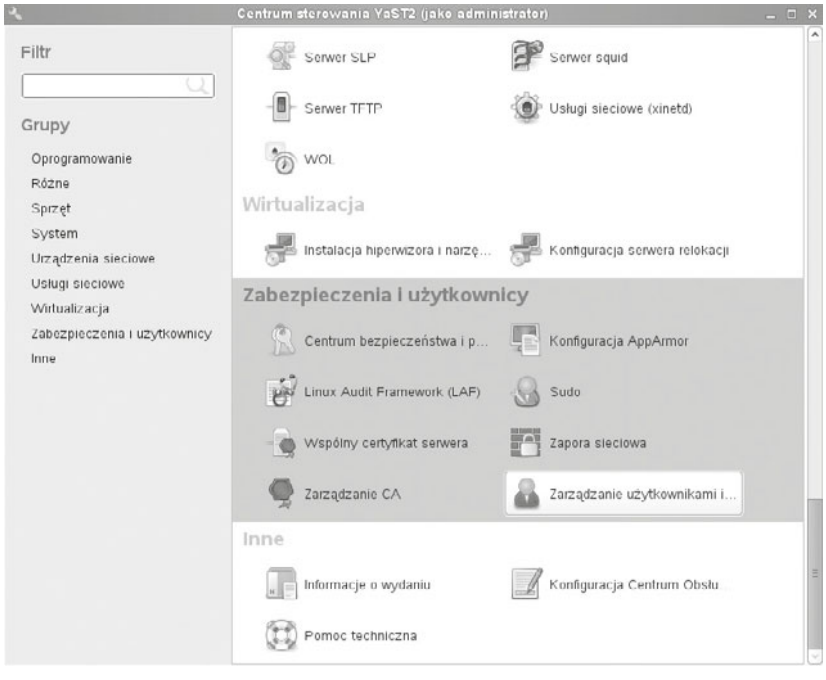
Konto root jest tworzone podczas instalacji systemu. Tworzenie innych kont nie jest wymagane, ale mocno zalecane.

Każde konto ma numer identyfikacyjny użytkownika UID (ang. *User Id*):

- dla root UID = 0,
- dla pozostałych UID ⩾ 1000 w dystrybucji SUSE.

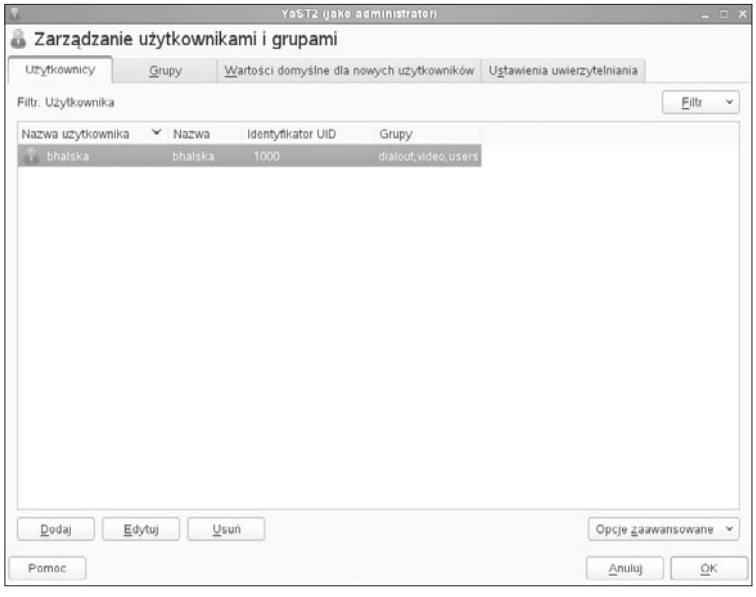
Nowe konto użytkownika można utworzyć, korzystając z YaST2 lub konsoli.

W celu dodania użytkownika uruchamiamy YaST2, a następnie wybieramy *Zabezpieczenia i użytkownicy* (rysunek 7.29).



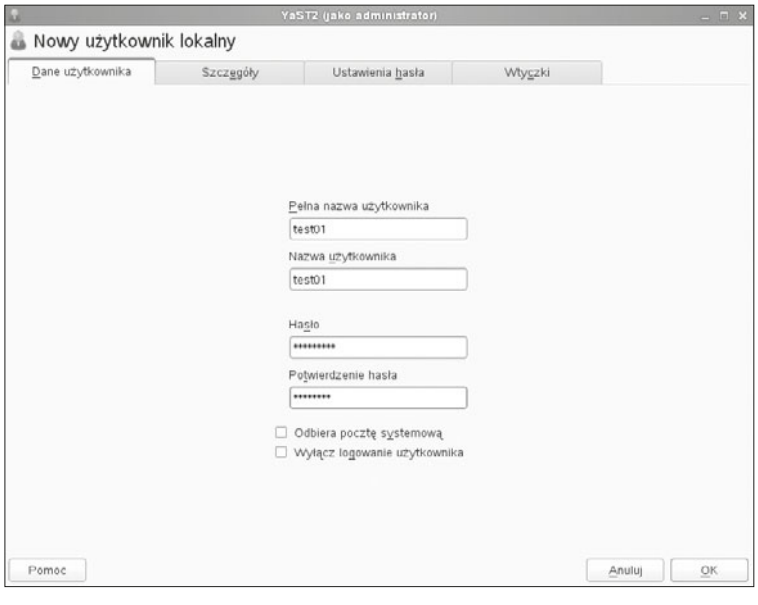
Rysunek 7.29. YaST2: Użytkownicy

Następnie wystarczy wybrać *Zarządzanie użytkownikami i grupami*, potem w zakładce *Użytkownicy* kliknąć *Dodaj* (rysunek 7.30).



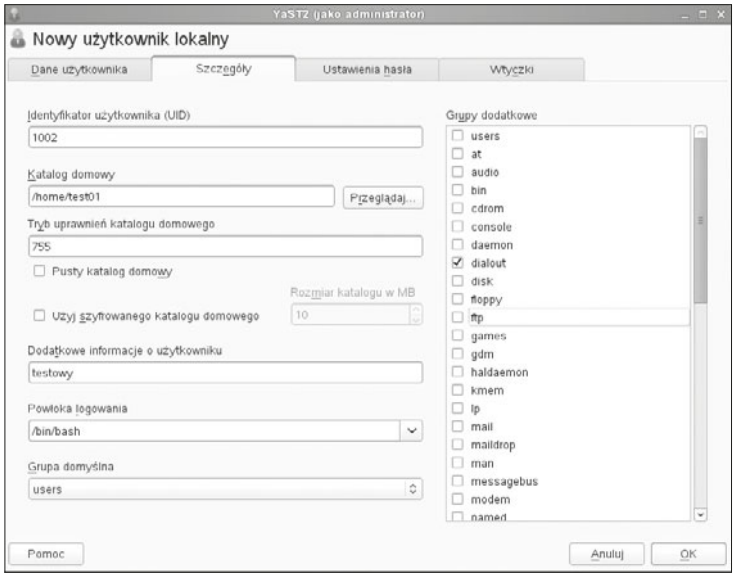
Rysunek 7.30. Zakładka Użytkownicy

W dalszej kolejności należy nadać nazwę dla nowo tworzonego użytkownika oraz hasło (rysunek 7.31).



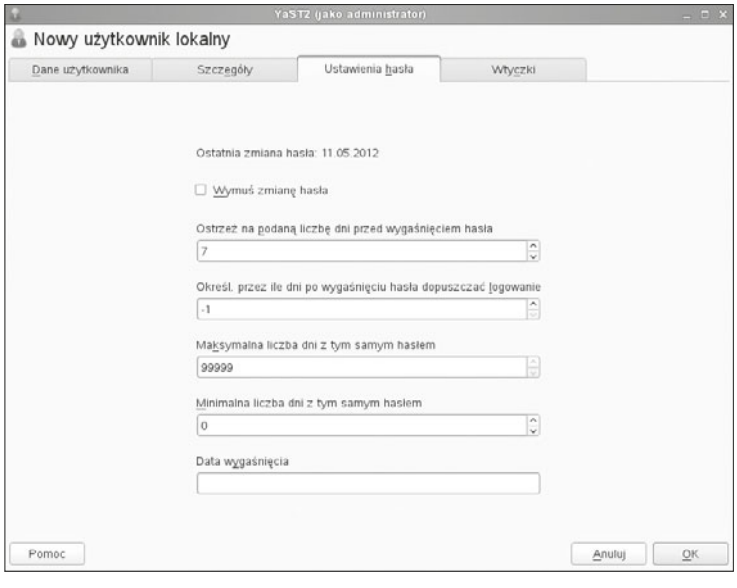
Rysunek 7.31. Dodawanie nowego użytkownika

W kolejnej zakładce *Szczegóły* (rysunek 7.32) można zmienić domyślne ustawienia dla nowo tworzonego użytkownika, takie jak katalog domowy (domyślnie *home)*, uprawnienia do tego katalogu (domyślnie 775) oraz domyślne grupy (*users*).



Rysunek 7.32. Szczegóły dotyczące nowego użytkownika

W zakładce *Ustawienia hasła* można zdefiniować wymagania dotyczące hasła oraz czas jego ważności (rysunek 7.33).



Rysunek 7.33. Ustawienia hasła

Aby dodać użytkownika w konsoli, należy skorzystać z poniższych poleceń, które wymagają uprawnień administratora:

- `useradd` (SUSE) lub `adduser` (inne dystrybucje) — dodanie użytkownika,
- `passwd` — nadanie hasła dla użytkownika.

Jak w przypadku użytkowników, również każdej grupie, do której może należeć użytkownik, jest przydzielony unikatowy identyfikator GID (ang. *Group Id*).

Grupy są tworzone dla użytkowników charakteryzujących się daną cechą. Dzięki grupom jest możliwe ustalenie uprawnień dla większego grona użytkowników jednocześnie — nie zaś dla każdego indywidualnie.

Większość zwykłych użytkowników jest dodawana do grupy *users*.

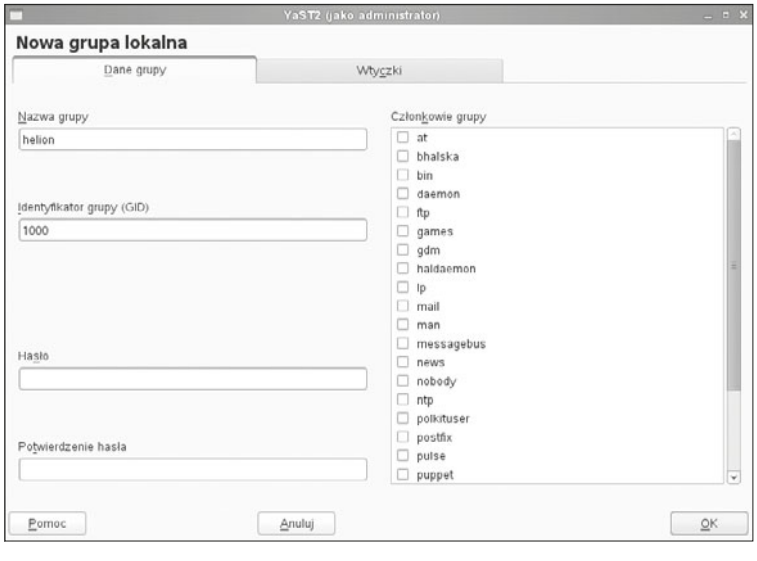
W systemie są też inne grupy, zazwyczaj używane do zadań specjalnych.

Istnieją trzy typy grup:

- grupy standardowe (GID ≥ 100),
- grupy systemowe (GID 1 do 99),
- grupa *root* (GID = 0).

Aby dodać nową grupę, postępujemy tak jak przy dodawaniu nowego użytkownika: jest to druga zakładka w narzędziu *Zarządzanie użytkownikami i grupami* (rysunek 7.34).

Należy nadać nazwę dla nowej grupy, można również określić hasło, które stanowi zabezpieczenie przed modyfikacją ustawień dla grupy. Można też określić, do jakich innych grup będzie należeć dana grupa.



Rysunek 7.34. Tworzenie nowej grupy

Dodawanie nowej grupy z konsoli jest możliwe przy użyciu polecenia `groupadd`.

Polecenia związane z użytkownikami i grupami:

- `useradd` — tworzenie nowego użytkownika,
- `id` — wyświetlenie ID użytkownika,
- `passwd` — nadanie/zmiana hasła,
- `logout` — wylogowanie,
- *`w, users, who`* — mniej lub bardziej szczegółowo podają informacje o zalogowanych użytkownikach,
- `whoami` — sprawdzenie, kim jesteśmy,
- `mesg` — zezwolenie na przyjmowanie komunikatów,
- `write` — wysłanie wiadomości do danego użytkownika,
- `finger` — wyświetlenie szczegółowych informacji o użytkownikach,
- `su` — umożliwienie logowania na konto innego użytkownika,
- `sudo` — umożliwienie wykonywania poleceń jako inny użytkownik (np. root),
- `chown` — umożliwienie zmiany właściciela pliku lub katalogu.

Domyślnie, kiedy plik jest tworzony przez użytkownika, jego właścicielem jest ten użytkownik, a grupa, do której użytkownik należy, jest również przypisywana do pliku.

ĆWICZENIA

1. Stwórz nową grupę *grupa_A*.
2. Stwórz użytkownika *user01*.
3. Dodaj użytkownika *user01* do *grupa_A*.
4. Sprawdź, jakie UID posiada nowo tworzony użytkownik.
5. Sprawdź, kto jest aktualnie zalogowany.

PYTANIA KONTROLNE

1. Jakim poleceniem z konsoli tworzymy nowego użytkownika?
2. Jaki numer UID ma *root*?
3. Jakie uprawnienia są nadawane dla katalogu domowego użytkownika?
4. Jakim poleceniem możemy sprawdzić numer ID użytkownika?

7.6. Zarządzanie procesami i usługami

W systemach operacyjnych wszystkie uruchomione programy to **procesy**. Zadaniem jądra systemu operacyjnego jest sterowanie procesami, zarządzanie czasem dostępu do procesora, przekazywanie go pomiędzy kolejne procesy (**wielozadaniowość**), które mogą przyjmować następujące stany:

- działający — aktualnie wykonujący jakąś operację,
- uśpiony — proces czeka na jakieś zdarzenie systemowe, np. odczyt danych z dysku,
- gotowy do wykonania — proces czeka na przydzielenie mu procesora,
- zombie — proces zakończył działanie, czeka na zakończenie go przez proces macierzysty.

Procesy dzielimy również na:

- proces potomny (podrzędny) (ang. *child process*) — proces rozpoczęty przez inny proces, który jest procesem nadrzędnym (rodzicielskim) dla procesu potomnego,
- proces nadrzędny — rodzicielski (ang. *parent process*) — proces rozpoczynający (wywołujący) inne procesy (procesy potomne).

Każdy proces w systemie ma przyporządkowany unikalny numer **PID** (ang. *Process IDentifier*), który zostaje mu nadany podczas uruchamiania. Pozwala on na jednoznaczną identyfikację procesu w systemie.

Wszystkie procesy w systemie Linux są procesami potomnymi procesu **init**, który ma identyfikator 1 — jest on tworzony podczas startu systemu operacyjnego. System wykonuje dany proces przez pewien czas, a następnie przekazuje procesor do dyspozycji kolejnemu procesowi.

Dla każdego procesu istnieje przypisany użytkownik, który go uruchomił. Na potrzeby usług takich, jak serwer WWW czy serwer pocztowy są tworzone specjalne konta, które służą do uruchomienia wybranej usługi. Usługi w systemach Linux są nazywane **demonami** (ang. *daemon*).

Jako system wielozadaniowy system Linux pozwala na uruchamianie zadań w tle w trybie tekstowym. Standardowo programy są uruchamiane na pierwszym planie (następuje interakcja z terminalem) lub w tle (program działa, ale nie ma interakcji z terminalem).

Zarządzanie procesami pierwszoplanowymi i procesami w tle

Środowisko powłoki Linuksa pozwala na pracę procesu na pierwszym planie (*foreground*) bądź w tle (*background*).

Procesy wykonywane na pierwszym planie są rozpoczynane w oknie terminala i pracują, dopóki proces się nie zakończy.

Okno terminala nie wróci do znaku zachęty, dopóki wykonywanie programu nie zostanie zakończone.

Istniejące procesy mogą być przeniesione z pierwszego planu do działania w tle, gdy są spełnione poniższe warunki:

- proces musi być rozpoczęty w oknie terminala bądź w powłoce konsoli,
- proces nie potrzebuje danych wejściowych z okna terminala.

Polecenia w powłoce mogą zostać zaczęte na pierwszym planie bądź w tle.

Aby uruchomić program, który rozpocznie przetwarzanie *w tle*, na końcu polecenia uruchamiającego należy wpisać znak `&`,

np. `xeyes &`

To polecenie uruchomi *w tle* działanie programu xeyes — dla użytkownika zostanie wyświetlona informacja o numerze uruchomionego procesu (*PID*).

Aby sprawdzić zadania wykonywane w tle, należy skorzystać z polecenia `jobs` (rysunek 7.35), które wyświetla numer zadania w tle, nazwę procesu, jego status (działający — ang. *running*, zatrzymany — ang. *stopped*, zakończony — ang. *done*).

Rysunek 7.35. Wynik działania polecenia jobs

W celu zatrzymania bieżącego zadania po to, aby ponownie je uruchomić do działania (przenieść), należy nacisnąć kombinację klawiszy *Ctrl+Z* (rysunek 7.36) — program zostanie zatrzymany i będzie mógł być ponownie uruchomiony poleceniem `fg`. Natomiast kombinacja *Ctrl+C* kończy bieżący proces uruchomiony na pierwszym planie.

Aby przywrócić wybrane polecenie na pierwszy plan, należy użyć polecenia `fg`, podając jako parametr numer zadania w tle, który wyświetla polecenie `jobs`. Polecenie `fg` bez parametru przeniesie na pierwszy plan zadanie, które zostało przeniesione na drugi plan jako ostatnie.

Np. wywołujemy polecenie `xeyes`, następnie zatrzymujemy je kombinacją klawiszy *Ctrl+Z*, po czym sprawdzamy, jaki ma numer, i poleceniem `fg 1` przywracamy do

działania. Kiedy proces zostanie przywrócony, kończymy jego działanie kombinacją *Ctrl+C* (rysunek 7.36).

```
basia@linux:~/Desktop
Plik  Edycja  Widok  Terminal  Pomoc
basia@linux:~/Desktop> xeyes
^Z
[1]+  Stopped                 xeyes
basia@linux:~/Desktop> jobs
[1]+  Stopped                 xeyes
basia@linux:~/Desktop> fg 1
xeyes
^C
```

Rysunek 7.36. Przykład działania fg, Ctrl+Z, Ctrl+C

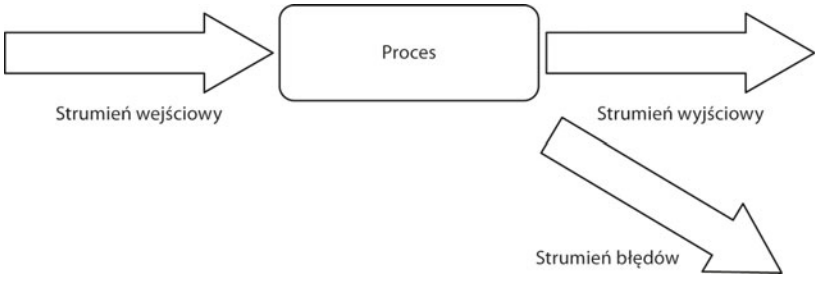
Aby zmienić status zadania wykonywanego w tle, należy użyć komendy `bg` z numerem zadania. Polecenie to powoduje, że status zadania w tle zmienia się z zatrzymanego na działający (rysunek 7.37).

```
basia@linux:~/Desktop
Plik  Edycja  Widok  Terminal  Pomoc
basia@linux:~/Desktop> xeyes
^Z
[1]+  Stopped                 xeyes
basia@linux:~/Desktop> bg 1
[1]+ xeyes &
```

Rysunek 7.37. Przykład działania polecania bg

Z każdym procesem w systemie Linux jest związane pojęcie **strumienia**, czyli danych przekazywanych do programu i danych, które generuje dany proces — zwykle występują trzy strumienie (rysunek 7.38):

- **stdin** — strumień wejściowy, domyślnie związany z klawiaturą, z której są wprowadzane dane,
- **stdout** — strumień wyjściowy, domyślnie związany z ekranem, na którym są wyświetlane wyniki pracy programu,
- **stderr** — strumień wyjściowy, domyślnie związany z ekranem, na którym są wyświetlane błędy generowane przez dany proces.



Rysunek 7.38. Przepływy strumieni danych

Jedną z zalet ułatwiających pracę w systemie Linux jest możliwość **przekierowania strumieni** do plików. Operatory przekierowań to:

> — przekierowuje strumień wyjściowy do zwykłego pliku podanego jako parametr. Jeśli plik nie istnieje, zostanie utworzony, jeśli istnieje, cała zawartość zostanie zastąpiona.

>> — przekierowuje strumień wyjściowy do pliku, dopisując dane na koniec pliku.

< — przekierowuje na strumień wejściowy dane zawarte we wskazanym pliku.

Aby przekierować wyniki pracy wybranego programu do pliku, należy użyć konstrukcji:

```
nazwa_polecenia [parametry] > plik_z_wynikami
```

np.

```
ls -la > moje_dane.txt
```

Polecenie to zapisze w pliku *moje_dane.txt* zawartość bieżącego katalogu (wynik działania polecenia `ls -la`). Użycie konstrukcji:

```
nazwa_polecenia [parametry] >> plik_z_wynikami
```

spowoduje, że wyniki działania programu zostaną dopisane na końcu wybranego pliku.

W celu przekierowania strumienia wejściowego używa się konstrukcji:

```
nazwa_polecenia [parametry] < plik_z_danymi
```

np.

```
mail uczen1999@wp.pl < informacja.txt
```

Powyższa linijka spowoduje wysłanie zawartości pliku *informacja.txt* na adres pocztowy *uczen1999@wp.pl*.

Kolejnym przykładem funkcjonalności rozwiązań związanych z pracą w trybie tekstowym są **potoki danych** — są to strumienie wyjściowe jednego procesu przekazywane jako dane wejściowe do innego procesu. W przypadku potoków operatorem pozwalającym na przekazanie jest symbol `|`, dla przykładu:

```
program_pierwszy | program_drugi
```

np.

```
ls -la | grep uczen
```

W przytoczonym przykładzie wyniki działania funkcji `ls` zostają przekazane na wejście dla programu `grep`. Ma on za zadanie wypisanie tylko tych linii, w których znajduje się słowo `uczen`. Danymi wejściowymi drugiego programu (`grep`) jest lista plików będąca wynikiem działania pierwszego programu (`ls`).

Podczas przekazywania potoków między procesami bardzo często jest używana wspomniana komenda `grep`. Służy ona do wyświetlania tylko tych linii, które pasują (lub nie pasują) do określonego wzorca.

Uproszczona składnia wygląda w sposób następujący:

```
grep [-v] wzorzec [plik]
```

gdzie

`-v` — oznacza opcję negacji wzorca,

`wzorzec` — oznacza treść do wyszukania,

`plik` — oznacza plik, którego zawartość ma być sprawdzona (gdy nie używamy potoków).

Wzorce są tworzone na bazie wyrażeń regularnych. W tabeli 7.4 przedstawiono znaki specjalne, pozwalające na tworzenie dowolnych wyrażeń.

Tabela 7.4. Znaki specjalne wykorzystywane w wyrażeniach regularnych

Znak	Opis
`.`	Dopasuj dowolny znak
`$`	Dopasuj poprzedzające wyrażenie do końca wiersza
`^`	Dopasuj występujące po operatorze wyrażenie do początku wiersza
`*`	Dopasuj zero lub więcej wystąpień znaku poprzedzającego operator
`[]`	Dopasuj dowolny znak ujęty w nawiasy, np. `[abc012]`
`[ — ]`	Dopasuj dowolny znak z przedziału, np. `[0-9]` — wszystkie cyfry; `[a-z]` — wszystkie małe litery; `[0-9a-zA-Z]` — wszystkie litery i cyfry
`[^ ]`	Dopasuj znak, który nie znajduje się w nawiasach

Aby lepiej zilustrować mechanizm tworzenia wyrażeń regularnych, w tabeli 7.5 zostały przedstawione przykłady zastosowań.

Tabela 7.5. Wykorzystanie wyrażeń reglarnych w programie grep

Polecenie	Opis
`grep ,Ala' plik`	Wypisze linie zawierające wyraz Ala
`grep ,A.a' plik`	Wypisze linie zawierające wyrazy takie jak Ala, Aga, Ara, A+a itp.
`grep ,A[lg]a' plik`	Wypisze linie zawierające wyrazy Ala i Aga
`grep ,^Ala' plik`	Wypisze linie rozpoczynające się od słowa Ala
`grep ,Go*gle' plik`	Wypisze linie zawierające wyrazy rozpoczynające się na literę „G", kończące się na „gle", które między tymi literami zawierają dowolną liczbę liter „o"

Innym programem wykorzystywanym podczas przekazywania potoków jest `more`, który wyświetla dane z podziałem na strony (po zapełnieniu ekranu danymi czeka na naciśnięcie klawisza przez użytkownika, aby kontynuować wyświetlanie).

PYTANIA

1. Jaki proces jest ładowany jako pierwszy?
2. Rozwiń skrót PID.
3. Jakim skrótem klawiszowym zatrzymujemy proces?
4. Jakie polecenie wyświetla procesy działające w tle?

7.6.1. Monitorowanie procesów i priorytety

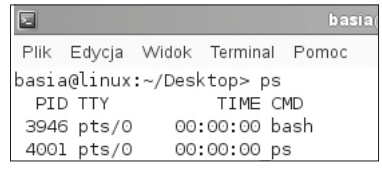
Możemy przeglądać informacje o procesach i przydzielać priorytety, zarówno dla zadań wykonywanych na pierwszym planie, jak i w tle, następującymi narzędziami:

- `ps`
- `pstree`
- `nice` i `renice`
- `top`
- `kill`
- `sleep`

ps

Możemy przeglądać pracujące procesy poleceniem `ps` (ang. *process status*) (rysunek 7.39).

Rysunek 7.39.
Wynik działania polecenia ps



Opcje tej komendy, które pozwolą wyświetlić więcej informacji, to:

`-A` — wyświetla wszystkie procesy, także procesy innych użytkowników (rysunek 7.40),

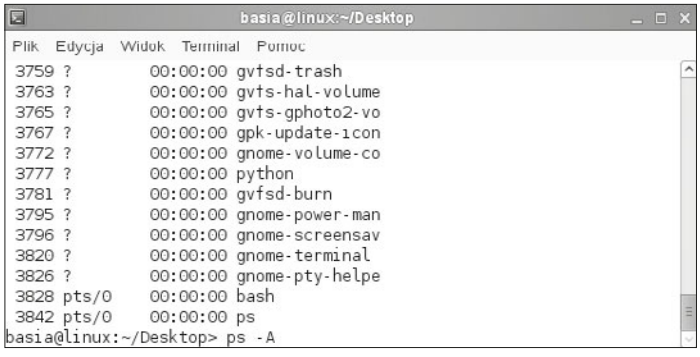
`-a` — wyświetla wszystkie procesy uruchomione w aktualnym oknie terminala,

`-l` — wyświetla szczegółową listę informacji o procesach (w tym czas utworzenia oraz prawa dostępu),

`-m` — sortuje według zużycia pamięci,

`-u` — wyświetla informację o procesach wybranego użytkownika,

`-x` — przegląd procesów, które nie są kontrolowane z żadnego terminala.



Rysunek 7.40. Wynik działania polecenia ps –A

Poniżej, w tabeli 7.6 znajduje się opis niektórych pól w liście procesów otrzymanej za pomocą polecenia `ps`.

Tabela 7.6. Tabela pól w liście procesów polecenia ps

Pole	Opis
`UID`	ID użytkownika
`PID`	ID procesu
`PPID`	ID procesu rodzica
`TTY`	Numer terminala kontrolnego
`PRI`	Numer priorytetu (im niższy, tym więcej czasu pracy procesora jest przydzielane do procesu)
`NI (nice)`	Wpływa na regulację dynamicznego priorytetowania
`STAT`	Obecny stan procesu
`TIME`	Użyty czas CPU
`COMMAND`	Nazwa polecenia

Możliwe wartości pola `STAT` (stan procesu) pokazuje tabela 7.7.

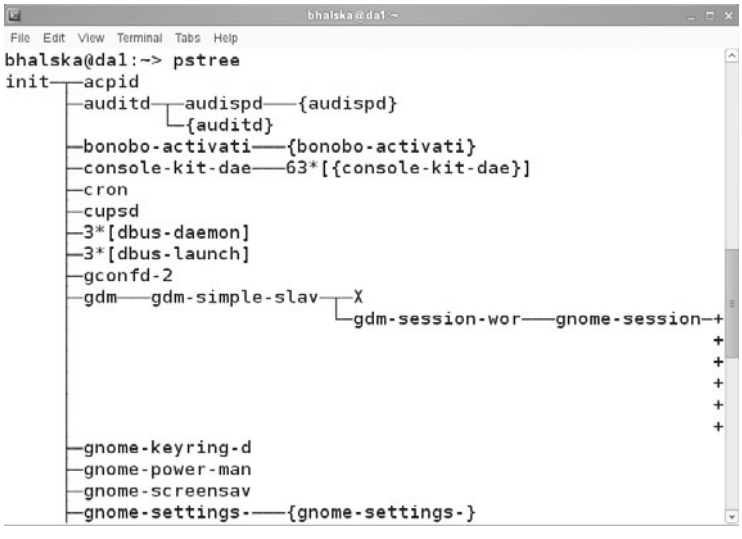
Tabela 7.7. Tabela opisu wybranych stanów procesu

Kod	Opis
`R` (*runnable*)	Wykonywanie — proces jest uruchomiony i wykonuje kolejne instrukcje
`S` (*sleeping*)	Oczekiwanie — czeka na zewnętrzne zdarzenie (takie jak dostarczenie danych)

Kod	Opis
D (*Uninterruptablesleep*)	Blokada przerwań — proces nie może być zakończony w tym momencie
T (*TracedorStopped*)	Zawieszenie
X	Jest martwy
Z (*zombie*)	Proces zakończył się, ale nie było jeszcze żądania jego wyniku (wartości zwrotnej) — czyli zamknięcie procesu nie zostało jeszcze obsłużone przez proces rodzica
S	Lider sesji
+	Jest w grupie procesów planowanych

pstree

Za pomocą polecenia `pstree` można przeglądać procesy w formacie struktury drzewa, czyli hierarchii (rysunek 7.41).



Rysunek 7.41. Wynik działania polecenia pstree

By zakończyć serię procesów, należy znaleźć właściwy nadrzędny proces (rodzica) i go zakończyć. Polecenie `pstree` pomaga zidentyfikować poszukiwany proces źródłowy.

Opcja `-p` wyświetla PID procesów. Opcja `-u` wyświetla ID użytkownika, jeśli zmienił się właściciel.

Ponieważ lista procesów jest przeważnie długa, można wprowadzić polecenie w formacie: `pstree -up | less`, by wyświetlać ją „strona po stronie”, a właściwie „ekran po ekranie”.

nice i renice

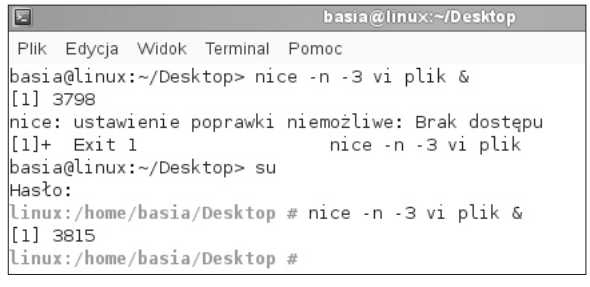
Linux zawsze stara się rozdzielić dostępny czas pracy na komputerze sprawiedliwie dla wszystkich procesów. Niestety nie jest to możliwe, dlatego że procesy mają różne priorytety. Im wyższy priorytet, tym więcej zasobów otrzymuje proces. Jako użytkownicy mamy możliwość zmiany priorytetów, gdy potrzebujemy, aby dla danego procesu zostało przydzielone mniej lub więcej czasu procesora.

Możemy to zrobić, wprowadzając priorytety dla procesów za pomocą polecenia `nice` (rysunek 7.42). Jest to polecenie, które uruchamia proces z podanym, a nie domyślnym priorytetem. Domyślna wartość wynosi zero, najmniej ważny to wartość 19, a najważniejszy to –20. Im ważniejszy jest proces, a więc im wyższy ma priorytet, tym więcej zasobów i czasu procesora zostaje dla niego przydzielone.

Polecenie `nice` przydziela procesowi specyficzną wartość atrybutu `-n`, która wpływa na obliczenie priorytetu procesu (zwiększenie lub zmniejszenie). Tylko użytkownik *root* ma prawo uruchomienia procesu z ujemnym poziomem `nice`. Gdy zwykły użytkownik spróbuje to zrobić, pojawi się komunikat o błędzie.

Np. `nice -n -3 vi plik &`

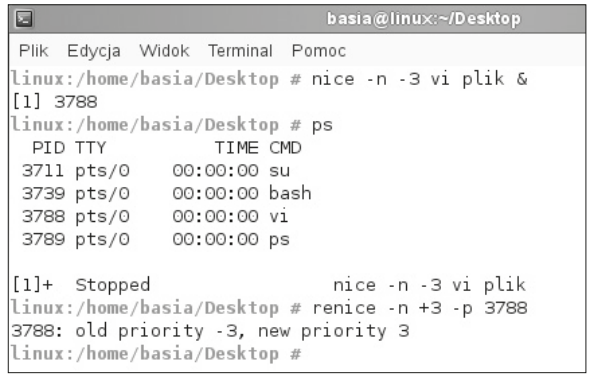
Rysunek 7.42. Zmiana priorytetu dla procesu vi



Powiązane polecenie `renice` służy do zmiany priorytetu procesu, który jest już uruchomiony, w odróżnieniu od polecenia `nice`, które dotyczy uruchamianego procesu. Tak jak w przypadku polecenia `nice`, tylko root ma prawo zmiany priorytetu na wyższy (np. na –3).

Wykorzystamy przykład powyżej i dokonamy zmiany priorytetu dla tego procesu za pomocą polecenia `renice: sleep: renice -n +3 -p 3788` (rysunek 7.43).

Rysunek 7.43. Zmiana priorytetu dla procesu sleep za pomocą polecenia renice

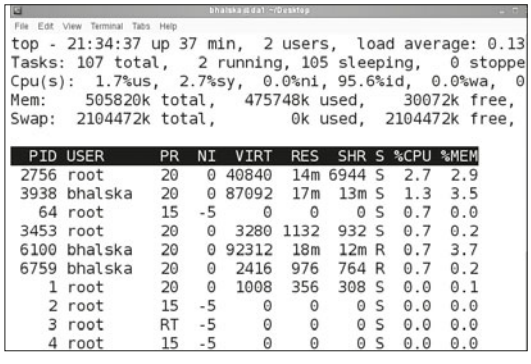


top

Polecenie `top` pozwala na obserwowanie procesów w sposób ciągły — wyświetla aktualizowaną w krótkich odstępach czasu listę. Umożliwia to monitorowanie pracujących procesów praktycznie w czasie rzeczywistym. Może również służyć do przydzielania nowej wartości `nice` procesom bądź do ich kończenia.

Przy użyciu `top` obowiązują te same zasady co przy zmianie poziomu `nice` procesu za pomocą polecenia `renice`. Użytkownik bez uprawnień administratora może podwyższyć poziom `nice`, jednak nie może go obniżyć.

Po wprowadzeniu polecenia `top` zostanie wyświetlona lista, jak poniżej na rysunku 7.44.



Rysunek 7.44. Wynik działania polecenia top

Wyświetlona lista jest domyślnie sortowana według czasu pracy i aktualizowana co 3 sekundy. Opis jej poszczególnych kolumn został zawarty w tabeli 7.8.

Można zakończyć działanie `top` wprowadzeniem `q`.

Tabela 7.8. Opis domyślnych kolumn

Kolumna	Opis
PID	ID procesu
USER	Nazwa użytkownika
PR	Priorytet
NI	Wartość NICE
VIRT	Obraz wirtualny (w kB)
RES	Stały rozmiar (w kB)
SHR	Rozmiar dzielonej pamięci (w kB)

Kolumna	Opis
S	Status procesu
%CPU	Użycie CPU w procentach
%MEM	Użycie pamięci (RES) w procentach
TIME+	Czas CPU
COMMAND	Nazwa polecenia

Polecenia zarządzające procesami dostępne w `top` można przeglądać poprzez wprowadzenie `?` lub `h`.

Opcje linii poleceń mogą być użyte do zmiany domyślnego zachowania `top`:

- `top -d 5` (opóźnienie — *delay*) zmieni domyślne opóźnienie przed odświeżeniem (3 sekundy) na 5 sekund,
- `top -n 3` (pętla — *iterations*) spowoduje, że `top` zrezygnuje po trzecim odświeżeniu.

kill

Procesy w systemach Linux na ogół kończą się samoistnie. Czasem jednak istnieje potrzeba wymuszenia wcześniejszego zakończenia procesu — np. procesu zawieszonego, w nieskończonej pętli itd. Zakończenie programu można wymusić przez wysłanie do procesu odpowiedniego sygnału.

Do wysyłania sygnałów do procesów służą narzędzia `kill` i `killall`.

Składnia polecenia:

`kill -sygnał numer_procesu`

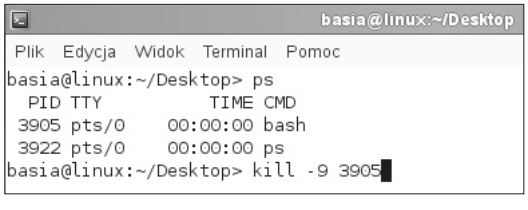
Różnica między narzędziami:

- `kill` — jako wymagany parametr przyjmuje PID procesu, do którego ma być wysłany sygnał,
- `killall` — parametrem jest nazwa procesu (sygnał zostanie wysłany do wszystkich procesów o wybranej nazwie).

W parametrach poleceń możemy użyć nazw sygnałów lub ich numerów:

np.

`kill -SIGKILL` lub `kill -9`
`kill -STOP` lub `kill -19`
`kill -9 PID` (np. `kill -9 3905`) — to polecenie spowoduje zakończenie procesu (rysunek 7.45)



Rysunek 7.45. Działanie polecenia kill, które spowoduje zamknięcie konsoli

Sygnał `SIGKILL` spowoduje natychmiastowe zakończenie działania procesu, sygnał `STOP` — jego zatrzymanie.

Inny przykład poleceń wywołujących tę samą procedurę zakończenia procesu — obsługę sygnału `TERM`:

```
kill -TERM
kill -SIGTERM
kill -17
```

Jeżeli użyjemy narzędzi `kill` lub `killall` bez parametrów, domyślnie do wybranego procesu zostanie wysłany sygnał `TERM`, który spowoduje, że proces podejmie działania prowadzące do prawidłowego zakończenia.

Aby wyświetlić dostępne sygnały w systemie, można użyć polecenia:

```
kill -l
1) SIGHUP      2) SIGINT      3) SIGQUIT     4) SIGILL
5) SIGTRAP     6) SIGABRT     7) SIGBUS      8) SIGFPEl
9) SIGKILL     10) SIGUSR1     11) SIGSEGV     12) SIGUSR2
13) SIGPIPE     14) SIGALRM     15) SIGTERM     16) SIGSTKFLTl
17) SIGCHLD     18) SIGCONT     19) SIGSTOP     20) SIGTSTP
21) SIGTTIN     22) SIGTTOU     23) SIGURG     24) SIGXCPU
25) SIGXFSZ     26) SIGVTALRM     27) SIGPROF     28) SIGWINCH
29) SIGIO     30) SIGPWR     31) SIGSYS     34) SIGRTMIN
35) SIGRTMIN+1     36) SIGRTMIN+2     37) SIGRTMIN+3     38) SIGRTMIN+4
39) SIGRTMIN+5     40) SIGRTMIN+6     41) SIGRTMIN+7     42) SIGRTMIN+8
43) SIGRTMIN+9     44) SIGRTMIN+10     45) SIGRTMIN+11     46) SIGRTMIN+12
47) SIGRTMIN+13     48) SIGRTMIN+14     49) SIGRTMIN+15     50) SIGRTMAX-14
51) SIGRTMAX-13     52) SIGRTMAX-12     53) SIGRTMAX-11     54) SIGRTMAX-10
55) SIGRTMAX-9     56) SIGRTMAX-8     57) SIGRTMAX-7     58) SIGRTMAX-6
59) SIGRTMAX-5     60) SIGRTMAX-4     61) SIGRTMAX-3     62) SIGRTMAX-2
63) SIGRTMAX-1     64) SIGRTMAX
```

sleep

`sleep` to polecenie, które opóźnia działanie wybranych akcji, czyli wymusza przerwę w działaniu. Po skończeniu się czasu przerwy terminal wyświetli nową linię i polecenia będzie można wpisywać dalej.

Np. `sleep 2`

ĆWICZENIA

1. Polecenia `ps`, `jobs`, `bg`, `fg`, `top`, `sleep`,`killal`, `kill`
2. Uruchom kilka procesów `sleep 150`, każdy z nich przerwij *Ctrl+Z*.
3. Wywołaj polecenie `jobs` i zobacz, jaki status mają wywołane wcześniej procesy.
4. Wywołaj polecenie `bg %1`.
5. Wywołaj polecenie `fg %1`, a następnie użyj skrótu *Ctrl+Z*.
6. Wywołaj polecenie `bg %1`.
7. Uruchom w konsoli Firefoksa.
8. Wywołaj w drugiej konsoli `ps -au`.

ĆWICZENIA cd.

9. W tej konsoli, w której został uruchomiony Firefox, użyj skrótu klawiaturowego *Ctrl+Z*.
10. Jeszcze raz wywołaj w drugiej konsoli `ps -au`.
11. Zakończ proces Firefoksa.
12. Wywołaj `ps -aux`.
13. Spróbuj zabić proces `init.d` poleceniem `kill -9 1`
14. Zakończ proces powłoki `bash`.
15. Uruchom program `xeyes` w tle poleceniem `xeyes &`.
16. Zatrzymaj („zabij”) proces `xeyes` poleceniem `killall xeyes`.

PYTANIA

1. Do czego służy polecenie `bg`?
2. Podaj nazwę polecenia, którym można zabić proces.
3. Jakie polecenie pozwala sprawdzić procesy użytkownika zalogowanego?

7.7. Monitoring

Informacje o sprzęcie można uzyskać z plików z katalogu */proc* oraz za pomocą poleceń. Pliki związane z monitoringiem systemu Linux:

/proc/cpuinfo — informacja o procesorze,

/proc/meminfo — informacja o pamięci operacyjnej,

/proc/devices — urządzenia używane w systemie,

/proc/ioports — porty wejścia-wyjścia (I/O),

/proc/interrupts — lista IRQ (przerwań),

/proc/dma — kanały DMA (bezpośredni dostęp do pamięci),

/proc/bus/pci/devices — urządzenia PCI,

/proc/scsi/scsi — urządzenia SCSI.

Natomiast polecenia są następujące:

`hwinfo` — generuje spore podsumowanie o sprzęcie. Możemy też dodać parametry, np. `--short` (skrócone podsumowanie) lub `--log` *`plik`* (wtedy wynik będzie przekierowany do pliku):

```
# hwinfo | less
# hwinfo --short
# hwinfo --log raport.txt
```

`hdparm` — pozwala obejrzeć lub ustawić parametry dysków.

`fdisk` — pozwala obejrzeć partycje oraz zarządzać nimi.

`iostat` — pokazuje statystyki użycia urządzeń pod kątem operacji wejścia-wyjścia, wymaga doinstalowania pakietu systat.

`lspci` — lista urządzeń PCI; opcje `-v` i `-vv` pozwalają ujawnić nieco więcej szczegółów.

`df`, `du` — pozwala ustalić zużycie miejsca na dysku.

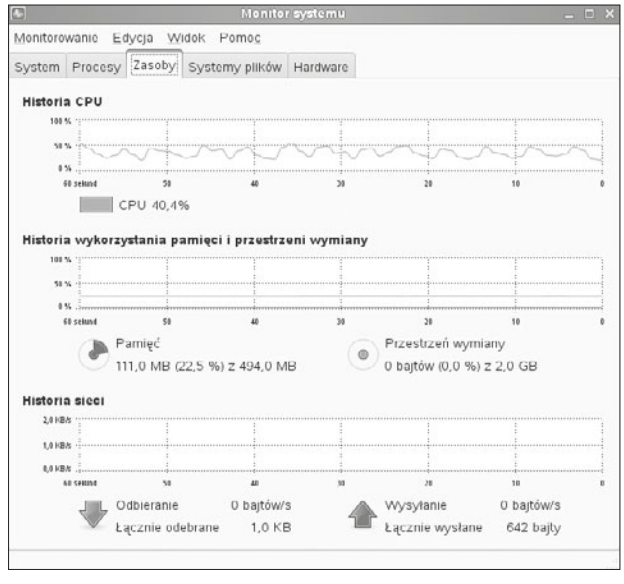
`free` — użycie pamięci operacyjnej.

`vmstat` — narzędzie monitoringu, które dostarcza informacji o użyciu pamięci operacyjnej, a także informacji o Block IO i aktywności CPU.

`lpstat` — wypisuje informację o stanie usług drukowania LP.

Monitoring systemu jest możliwy również w trybie graficznym. Służy do tego narzędzie *Monitor systemu* (rysunek 7.46). Pakiet pozwala na graficzne przeglądanie uruchomionych procesów systemu i zarządzanie nimi. Dostarcza również przegląd dostępnych zasobów, takich jak użycie procesora i pamięci.

Rysunek 7.46. Monitoring systemu



ĆWICZENIA

1. Korzystając z powyższych poleceń, sprawdź konfigurację partycji.
2. Sprawdź, ile jest użytej pamięci RAM.
3. Sprawdź listę przerwań IRQ.
4. Ustal zużycie miejsca na dysku.

PYTANIA

1. Jakim poleceniem w Linuksie możesz stworzyć partycję?
2. Jakie polecenie generuje raport o stanie systemu?
3. Jaki plik przechowuje informacje o procesorze?

7.8. Usługi sieciowe

7.8.1. DNS

WSKAZÓWKA

BIND (ang. *Berkeley Internet Name Domain*) jest jednym z najpopularniejszych serwerów DNS wykorzystywanym w systemach Linux i Unix. BIND stanowi niezmiernie ważny składnik zapewniający poprawne rozwiązywanie nazw. Serwer DNS to wielka rozproszona baza danych, w której są przechowywane odwzorowania nazw domenowych na adresy IP.

Głównym plikiem konfiguracyjnym serwera DNS jest plik */etc/named.conf*. Zawiera on informacje na temat obsługiwanych stref oraz opcji działania samego serwera.

Aby zapewnić poprawne działanie serwera związanego z rozwiązywaniem nazw, należy wyedytować dwa pliki:

- */etc/host.conf* — zawiera informacje o kolejności, w jakiej system powinien odpytywać różne systemy (serwery DNS, NIS) przy rozwiązywaniu nazwy sieciowej,
- */etc/resolv.conf* — definiuje kolejność przeszukiwania domen i zawiera adresy serwerów nazw.

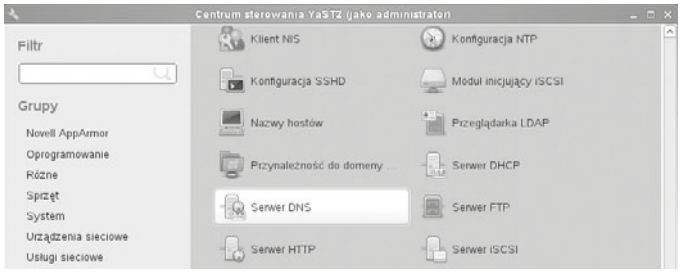
Plik *host.conf* może zawierać następujące opcje:

- `order` — polecenie to określa kolejność, w jakiej będą odpytywane systemy,
- `multi` — pozwala określić, ile wyników może zwrócić system rozwiązywania nazw.

Najczęściej przy konfiguracji w pliku */etc/resolv.conf* stosuje się dwa słowa kluczowe:

- `nameserver` — określa adres serwera DNS,
- `domain` — określa nazwę domeny, do której należy komputer.

W celu zainstalowania usługi rozwiązywania nazw w systemie SUSE należy w YaST2 w grupie *Usługi sieciowe* odnaleźć *Serwer DNS* (rysunek 7.47).



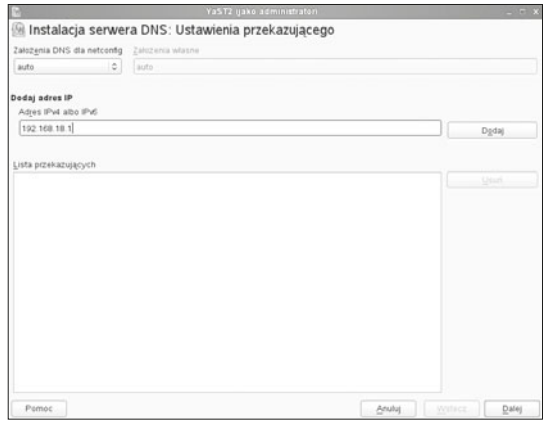
Rysunek 7.47. YaST2: Usługi sieciowe/Serwer DNS

Po kliknięciu tej usługi uruchomi się kreator inicjalizacji konfiguracji (rysunek 7.48), który najpierw sprawdzi, czy usługa jest zainstalowana; jeżeli nie jest, przeprowadzi instalację.

Rysunek 7.48. Inicjalizacja konfiguracji serwera DNS

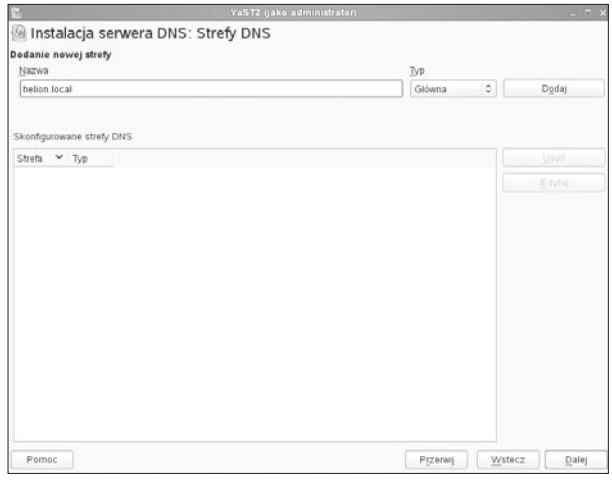
Po zainstalowaniu usługi jest przeprowadzana wstępna konfiguracja. W pierwszym oknie należy podać adresy pośredniczące (rysunek 7.49), z których usług będzie korzystał serwer, jeśli sam nie będzie potrafił rozwiązać nazw.

Rysunek 7.49. Dodawanie adresu pośredniczącego



W następnym oknie trzeba skonfigurować strefę DNS dla danej domeny (rysunek 7.50). Należy podać nazwę domenową oraz zdefiniować typ jako główny.

Rysunek 7.50. Strefy DNS



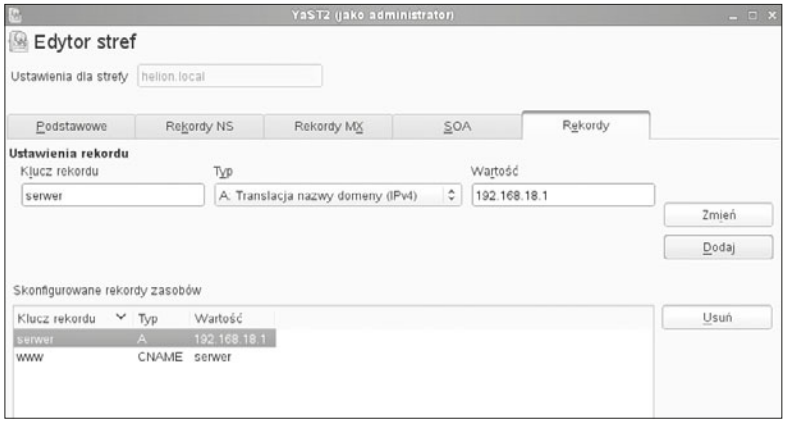
W ostatnim oknie kreatora (rysunek 7.51) należy otworzyć port oraz określić sposób uruchamiania dla usługi.

Rysunek 7.51. DNS — kończenie pracy kreatora

Jeżeli usługa została już zainstalowana oraz wstępnie skonfigurowana, można przejść do konfiguracji zaawansowanej poprzez ponowne uruchomienie kreatora usługi DNS, który tym razem nic nie instaluje, tylko wczytuje ustawienia.

W celu dodania rekordów do strefy DNS należy jeszcze raz uruchomić usługę i edytować *strefę* (ang. *zone*). Następnie przejść do zakładki *Rekordy* (ang. *records*) i dodać rekordy (rysunek 7.52). W celu dodania rekordu należy uzupełnić trzy pola:

- *Klucz rekordu* — tutaj wprowadza się nazwę konkretnego hosta,
- *Typ* — określa rodzaj odwzorowania, jaki ma realizować dany rekord:
  - » *A* — translacja nazwy domenowej na adres IPv4,
  - » *AAAA* — translacja nazwy domenowej na adres IPv6,
  - » *CNAME* — alias dla nazwy domenowej,
  - » *PTR* — przypisanie adresu hosta do IP. Rekordy wskaźnika (PTR) są używane do wyszukiwania wstecznego,
- *Wartość* — adres hosta lub nazwa aliasu.



Rysunek 7.52. Edytor stref

ĆWICZENIA

1. Zainstaluj i skonfiguruj usługę DNS.

PYTANIA

1. Jak nazywa się serwer DNS w Linuksie?
2. Podaj nazwę oraz ścieżkę pliku konfiguracyjnego serwera DNS.

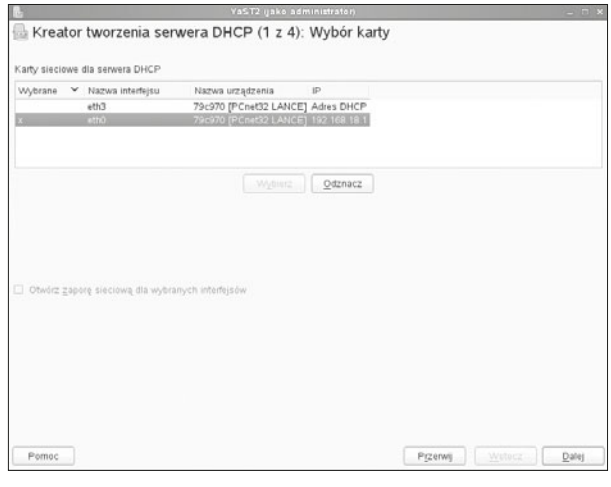
7.8.2. DHCP

W celu zainstalowania lub skonfigurowania usługi DHCP należy przejść w YaST2 do narzędzi *Usługi sieciowe* i wyszukać *Serwer DHCP*. Jeżeli nie jest on jeszcze zainstalowany, to po uruchomieniu pojawi się komunikat pozwalający na instalację (rysunek 7.53). Pliki konfiguracyjne serwera to */etc/dhcpd* oraz */etc/sysconfig/dhcpd*.

Rysunek 7.53.
Kreator konfiguracji DHCP

Po zainstalowaniu pojawia się *Kreator tworzenia serwera DHCP*. W pierwszym kroku poprosi o wybranie karty sieciowej, dla której serwer DHCP będzie świadczył swoje usługi (rysunek 7.54). Powinna to być karta dla sieci wewnętrznej, czyli lokalnej, o adresie statycznym.

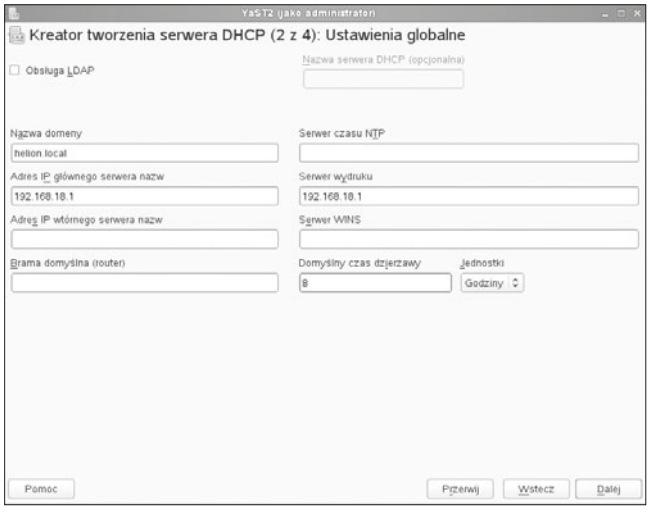
Rysunek 7.54.
Wybór karty sieciowej dla usługi DHCP



W kolejnym oknie kreatora (rysunek 7.55) należy zdefiniować ustawienia globalne, takie jak:

- *Nazwa domeny*, np. *helion.local*,
- *Adres IP głównego serwera nazw*,
- *Adres IP wtórnego serwera nazw*,
- *Brama domyślna (router)*,
- *Serwer czasu NTP*,
- *Serwer wydruku*,
- *Serwer WINS*,
- *Domyślny czas dzierżawy*.

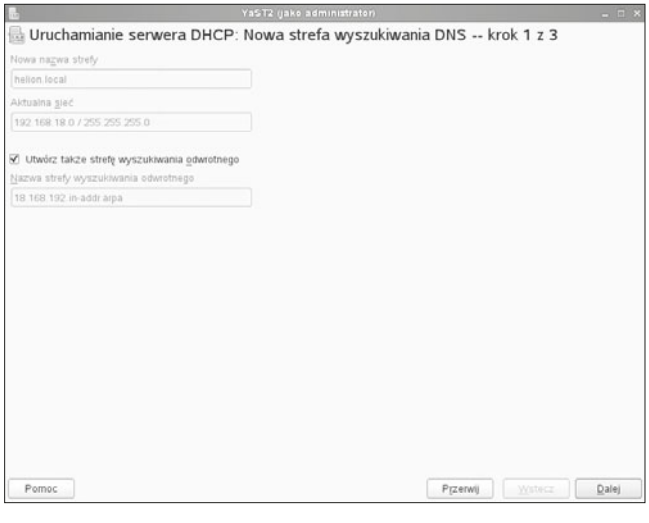
Są to dane, które są przekazywane przy pobieraniu adresu IP dla klienta.



Rysunek 7.55. Ustawienia globalne serwera DHCP

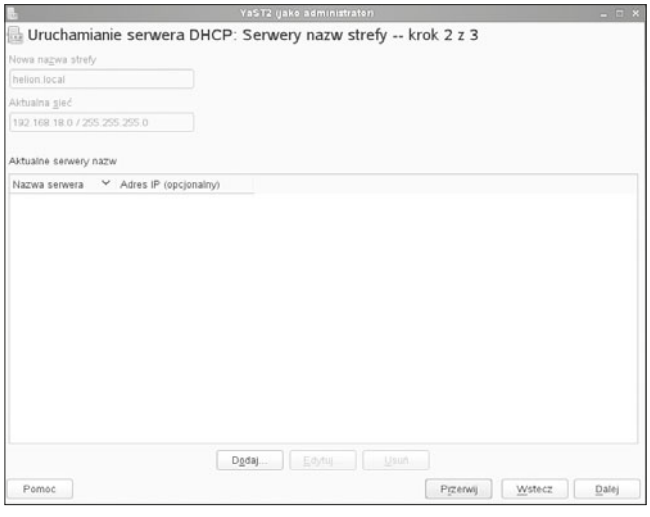
W kolejnym kroku konfiguracji można określić zakres adresów oraz czas dzierżawy. W tym oknie można również dodać strefy przeszukiwania dla serwera DNS.

Uruchamia się kolejny kreator: *Nowa strefa wyszukiwania DNS*, w którym są zapisane ustawienia podane podczas konfiguracji serwera DHCP (rysunek 7.56).



Rysunek 7.56. Uruchamianie serwera DHCP: Nowa strefa wyszukiwania DNS

W kolejnym oknie (rysunek 7.57) należy dodać serwery przeszukiwania DNS. Gdy zostaną dodane, można wrócić do konfiguracji serwera DHCP. Jeżeli nasza lokalna strefa nie potrafi rozwiązać nazw, należy dodać inne serwery DNS, które to umożliwią.

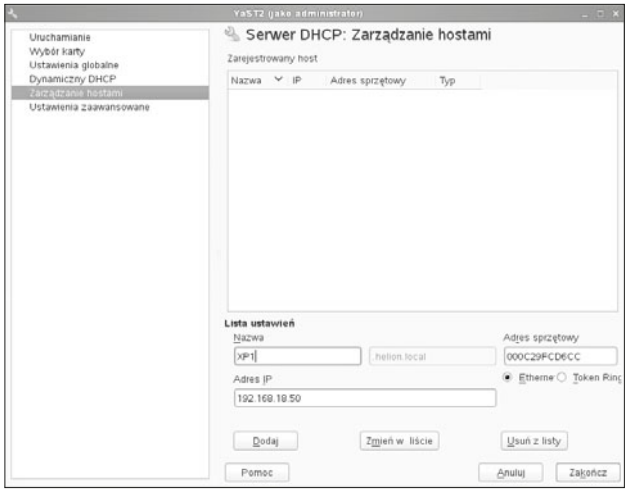


Rysunek 7.57. Uruchamianie serwera DHCP: Serwery nazw strefy

W ostatnim oknie kreatora (rysunek 7.58) należy zdefiniować, w jaki sposób ma być uruchamiany serwer DHCP.

Rysunek 7.58. Kreator tworzenia serwera DHCP: Uruchamianie

Usługa została zainstalowana oraz wstępnie skonfigurowana, można więc przejść do konfiguracji zaawansowanej, w której można określić statyczne przydzielanie adresów IP na podstawie adresów MAC (rysunek 7.59).



Rysunek 7.59. Serwer DHCP: Zarządzanie hostami

Usługę taką jak DHCP można również uruchomić z konsoli:

```
/etc/init.d/dhcpd (start|stop|restart|status)
```

`start` — uruchamia usługę,

`stop` — zatrzymuje usługę,

`restart` — restartuje usługę,

`status` — wyświetla status usługi.

Aby zatrzymać, uruchomić lub przeładować dowolną usługę, należy zalogować się do powłoki jako root. Uruchamianie usług za pomocą konsoli jest bardzo przydatne podczas wprowadzania zmian w ustawieniach usługi. Pozwala sprawdzić, czy usługa wystartuje, a jeżeli nie, zostaną wyświetlone komunikaty, które wskazują błędy popełnione podczas konfiguracji. Wszystkie usługi, jakie możemy w ten sposób uruchomić lub sprawdzić ich status, znajdują się w katalogu */etc./init.d*, np. cups, sshd, pure-ftpd, smb.

ĆWICZENIA

1. Zainstaluj i skonfiguruj usługę DHCP.
2. Zdefiniuj przydzielenie adresu IP na podstawie adresu fizycznego (MAC).

PYTANIA

1. Omów usługę DHCP.
2. Co to jest MAC?
3. Jakim poleceniem uruchamiamy usługę ręcznie?

7.8.3. Routing

Routing jest procesem wyznaczania tras, wykorzystującym mechanizmy z trzeciej warstwy (sieci) modelu OSI.

Funkcja określania ścieżki pozwala routerowi na porównanie adresu odbiorcy z dostępnymi trasami zawartymi w tablicy routingu i na wybór najlepszej trasy. Routery mogą zdobyć informacje na temat dostępnych tras za pomocą routingu statycznego lub dynamicznego. Trasy skonfigurowane ręcznie przez administratorów sieci są określane mianem tras statycznych. Trasy, o których informacje zostały otrzymane od innych routerów za pomocą protokołu routingu, są określane mianem tras dynamicznych.

Wpisy wewnątrz tablicy routingu zawierają przede wszystkim:

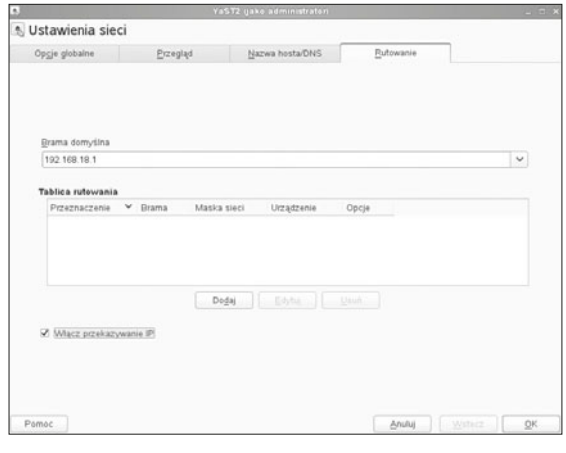
- przeznaczenie — sieć docelową podaną w formie adresu sieci,
- urządzenie, przez które trasa jest osiągalna — fizyczne urządzenie bądź adres następnego skoku.

Tablica routingu jest skonfigurowana w SLES za pomocą plików konfiguracyjnych znajdujących się w */etc/sysconfig/network/* w pliku *routes* — określenie tras. Dla każdego interfejsu, który wymaga określenia trasy pakietów, należy zmodyfikować plik */etc/sysconfig/network/ifroute-eth0* dla pierwszej karty sieciowej. Dla każdej kolejnej nazwa pliku to *ifroute-**, gdzie * oznacza numer interfejsu, tj. kolejno eth1, eth2 itd.

Poniższe skrypty w katalogu */etc/sysconfig/network/scripts/* pomagają przy obsłudze tras:

- `ifup-route` — na utworzenie trasy,
- `ifdown-route` — wyłączanie trasy,
- `ifstatus-route` — do sprawdzania stanu tras.

Konfigurację routingu można również przeprowadzić przy użyciu narzędzia YaST2. W tym celu należy przejść do zakładki *Rutowanie*. Pierwszą opcją, jaką należy skonfigurować, jest *Brama domyślna* (rysunek 7.60). To ustawienie pozwoli określić trasę domyślną dla pakietów.

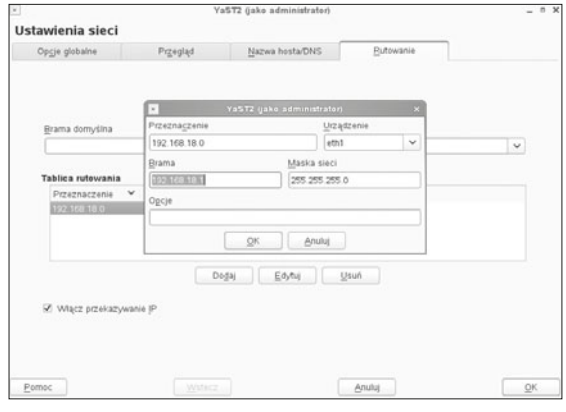


Rysunek 7.60. Rutowanie

Można również dodać nowy wiersz do tablicy rutowania. Żeby to zrobić, trzeba skonfigurować kilka istotnych opcji, takich jak:

- *Przeznaczenie* — określa adres podsieci, który jest jednocześnie pierwszą kolumną w tablicy, np. 192.168.18.0,
- *Brama* — adres urządzenia sieciowego pełniącego rolę lokalnego routera, do którego zostaną skierowane pakiety, np. 192.168.18.1,
- *Maska sieci* — maska podsieci przypisana do adresu określonego w pierwszej kolumnie, np. 255.255.255.0,
- *Urządzenie* (opcjonalnie) — nazwa urządzenia dla określonego wiersza w tablicy trasowania,
- *Opcje* — można określić dodatkowe opcje dla dodawanych tras.

Ostatnią opcją, jaką można ustawić, jest włączenie przekazywania IP. Jest ona niezbędna w przypadku, gdy serwer ma pełnić rolę routera dla innych komputerów w sieci (rysunek 7.61).



Rysunek 7.61. Dodawanie trasy routingu

Aby sprawdzić tablicę routingu, należy w konsoli wywołać polecenie `route` (rysunek 7.62).

```
basia@linux:~/Desktop
Plik  Edycja  Widok  Terminal  Pomoc
linux:/home/basia/Desktop # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.18.0    linux.site      255.255.255.0   UG    0      0        0 eth1
192.168.1.0     *               255.255.255.0   U     0      0        0 eth2
link-local      *               255.255.0.0     U     0      0        0 eth1
loopback        *               255.0.0.0       U     0      0        0 lo
default         192.168.1.2     0.0.0.0         UG    0      0        0 eth2
linux:/home/basia/Desktop #
```

Rysunek 7.62. Tablica routingu

Pierwsza kolumna w tablicy na powyższym rysunku odnosi się do adresu przeznaczenia, czyli adresu hosta, podsieci, sieci, do której jest zaadresowany pakiet. W drugiej kolumnie jest określony adres IP routera będącego następnym skokiem dla pakietu pasującego do

pary `destination/genmask`, czyli kolumny 1. i 3. z rysunku 7.62. Kolumna, która zawiera `genmask`, jest ściśle związana z kolumną oznaczającą przeznaczenie i pozwala zdefiniować, ile mamy adresów w danej podsieci w każdej z klas adresu IP (to zagadnienie zostało omówione w podrozdziale 4.6). Interesująca jest też ostatnia kolumna. W niej są podane nazwy interfejsów sieciowych, przez które dany pakiet jest kierowany do sieci. Urządzenie sieciowe może mieć kilka takich interfejsów (kart sieciowych) i każdy z nich może być przyłączony do innej sieci. Ważne jest więc, aby dane zostały przekierowane do odpowiedniego interfejsu. Pierwszy zapis w danej tablicy wskazuje dokładnie, że datagram adresowany do komputerów w podsieci 192.168.18.0 ma być skierowany do interfejsu eth1. Wyraz default określa adres domyślny, czyli każdy adres, który nie znajdował się w pierwszej kolumnie na poprzednich pozycjach. Określenie loopback określa pętlę lokalną, czyli odniesienie do siebie samego.

ĆWICZENIA

1. Skonfiguruj nową trasę routingu.

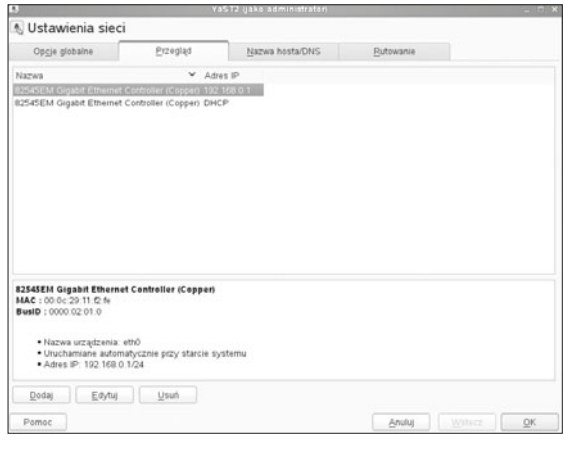
PYTANIA

1. W jakim pliku znajduje się konfiguracja tras routingu?
2. Jakie polecenie pozwala na tworzenie nowej trasy?
3. Jakim poleceniem sprawdzamy trasę routingu?

7.8.4. NAT

Do skonfigurowania usługi NAT, tak jak i routingu, są potrzebne co najmniej dwa interfejsy sieciowe. Jeden będzie obsługiwał sieć zewnętrzną (internet), a drugi sieć wewnętrzną (lokalną).

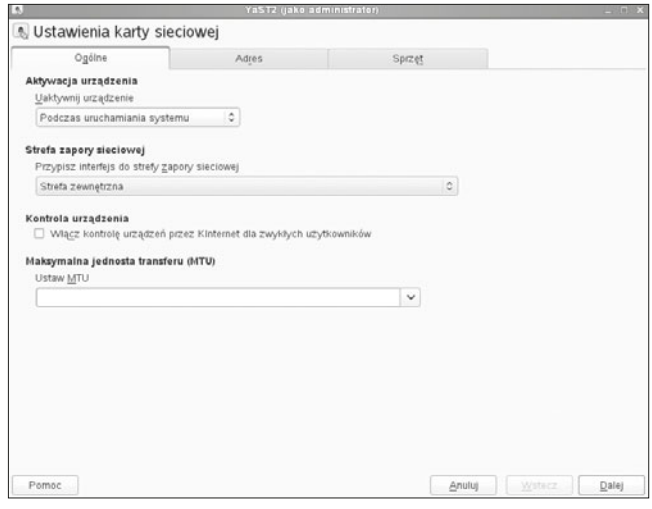
Pierwszym krokiem jest konfiguracja ustawień kart sieciowych w YaST2 (rysunek 7.63).



Rysunek 7.63. Konfiguracja kart sieciowych

W ramach routingu dwa interfejsy sieciowe należy podzielić na strefę zewnętrzną dla karty, która jest podłączona do internetu, i na strefę wewnętrzną dla karty podłączonej do sieci lokalnej.

W ustawieniach karty, która obsługuje połączenie z internetem, w zakładce *Ogólne* należy zmienić ustawienia *Strefa zapory sieciowej* na *Strefa zewnętrzna* (rysunek 7.64).



Rysunek 7.64. Ustawienia karty sieciowej: strefa zewnętrzna

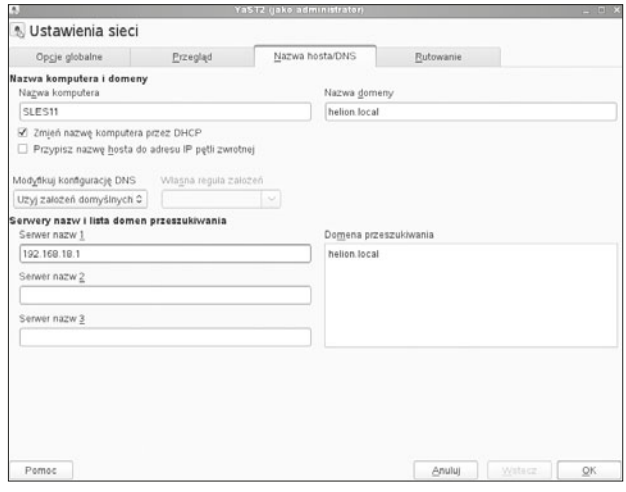
Należy zapisać wszystkie ustawienia. Następnie można przejść do ustawień kolejnej karty, tym razem obsługującej sieć lokalną (rysunek 7.65).

Należy zmienić ustawienia zapory sieciowej dla tej karty, ustawiając ją na *Strefę wewnętrzną (niechroniony)*.

Rysunek 7.65. Określenie strefy dla interfejsu

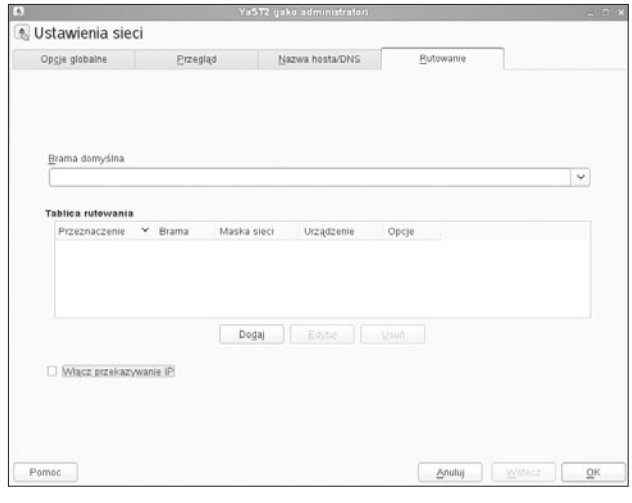
Kolejną czynnością, jaką należy wykonać, jest przypisanie nazwy hosta do pętli zwrotnej IP (*Loopback IP*). Po przejściu w ustawieniach sieci YaST2 do zakładki *Nazwa hosta/DNS*, trzeba włączyć opcję *Przypisz nazwę hosta do adresu IP pętli zwrotnej* (rysunek 7.66).

Rysunek 7.66. Przypisanie nazwy hosta do pętli zwrotnej

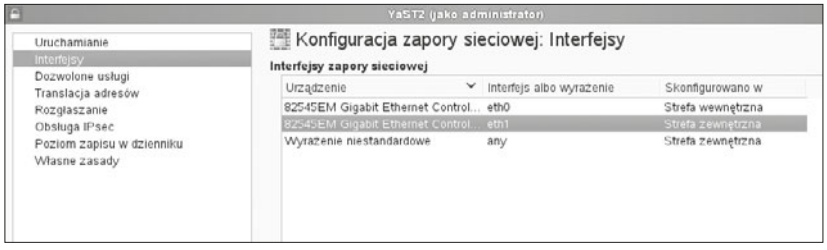


Teraz należy włączyć przekierowanie IP (*IP Forwarding*). Można to zrobić w ustawieniach sieci YaST2, w zakładce *Rutowanie*. Wystarczy zaznaczyć odpowiednią opcję: *Włącz przekazywanie IP* (rysunek 7.67).

Rysunek 7.67. Włączenie przekazywania w zakładce Rutowanie



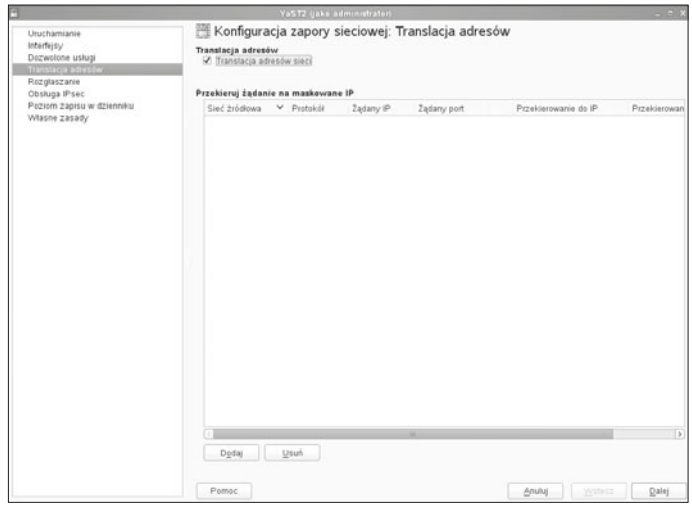
Jeżeli karty sieciowe zostały skonfigurowane poprawnie, w kolejnym kroku należy skonfigurować *Zaporę sieciową*. Zapora sieciowa jest narzędziem, które znajduje się w YaST2 w grupie *Zabezpieczenia i użytkownicy*. W oknie zapory sieciowej należy dla każdego interfejsu zdefiniować rodzaj strefy. Dla karty wewnętrznej, czyli lokalnej, wybieramy strefę wewnętrzną, natomiast dla karty zewnętrznej (np. internet) określamy strefę zewnętrzną (rysunek 7.68).



Rysunek 7.68. Konfiguracja zapory sieciowej

Kolejną czynnością, którą należy wykonać, jest włączenie translacji adresów (maskarady). W oknie *Konfiguracja zapory sieciowej* wybieramy opcję *Translacja adresów* i następnie *Translacja adresów sieci* (rysunek 7.69).

Rysunek 7.69. Konfigurowanie maskarady w zaporze sieciowej



Teraz wystarczy kliknąć przycisk *Dalej*. Wyświetli się wówczas podsumowanie translacji adresów, a translacja adresów IP zostanie włączona.

ĆWICZENIA

1. Zainstaluj i skonfiguruj usługę NAT.

PYTANIA

1. Na czym polega technologia translacji adresów IP?
2. Jak są oznaczane karty sieciowe w systemie Linux?

7.8.5. VPN

VPN (ang. *Virtual Private Network*, Wirtualna Sieć Prywatna) — jest tunelem, przez który płynie ruch w ramach sieci pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych tak pakietów. Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa.

Jedną z propozycji do tworzenia sieci VPN jest OpenVPN. Oprogramowanie to jest wydawane na licencji GNU GPL, jest darmowe i ma otwarty kod. Do budowania szyfrowanych tuneli, w odróżnieniu od wielu innych rozwiązań, nie jest wykorzystywany protokół IPSec, ale szyfrowanie oparte na bibliotekach OpenSSL. Wykorzystywany OpenSSL jest rozwijany na bieżąco, co gwarantuje duże bezpieczeństwo i szybką reakcję na wykryte błędy. Wadą pakietu OpenVPN jest nigdzie nieopisany protokół komunikacji, który mimo wykorzystania OpenSSL-a może być powodem problemów z bezpieczeństwem.

Instalację przeprowadza się z konsoli za pomocą polecenia `zypper` (rysunek 7.70) (instalacja za pomocą polecenia `zypper` została omówiona w punkcie 7.3.1).

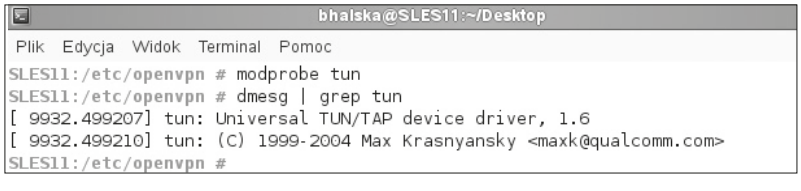
```
zypper install openvpn
```

Rysunek 7.70. Instalacja OpenVPN za pomocą polecenia zypper

Sprawdzamy, czy mamy sterownik wirtualnego interfejsu TUN/TAP, za pomocą poleceń (rysunek 7.71):

`#modprobe tun` — powinno nic nie wyświetlić,

`#dmesg | grep tun` — wyświetla sterownik wirtualnego interfejsu.



Rysunek 7.71. Polecenia sprawdzające sterownik wirtualnego interfejsu

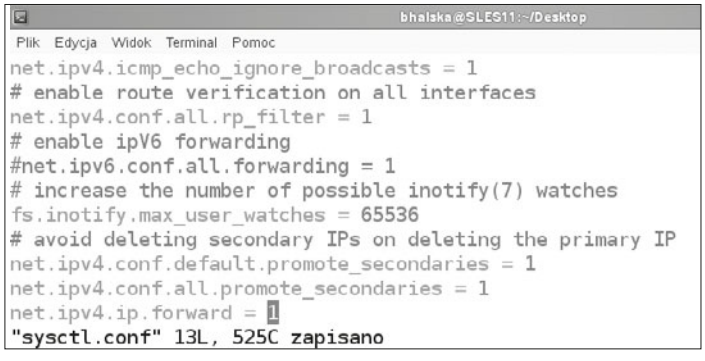
Następnie należy wygenerować na routerze klucz, który będzie wykorzystywany do szyfrowania i uwierzytelniania transmisji (rysunek 7.72).

```
openvpn --genkey --secret /etc/openvpn/static.key
```

Rysunek 7.72. Generowanie klucza

Serwer będzie forwardował pakiety, wobec czego w pliku */etc/sysctl.conf* należy dopisać linijkę, wykorzystując np. edytor vi (rysunek 7.73):

```
net.ipv4.ip_forward=1
```



Rysunek 7.73. Wpis w pliku sysctl.conf

Następnie należy utworzyć grupę oraz konto użytkownika na potrzeby tunelu (rysunek 7.74):

```
groupadd openvpn
 useradd -g openvpn -d /usr/local/etc/openvpn –s/bin/false -f 1 openvpn
```

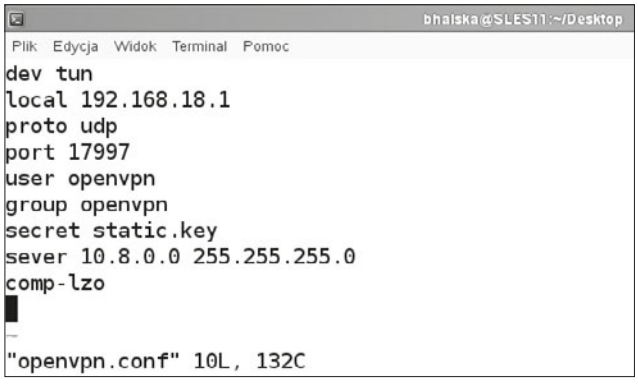
Rysunek 7.74. Tworzenie grupy i użytkownika

W następnym kroku należy stworzyć plik konfiguracyjny */etc/openvpn/openvpn.conf* dla naszego tunelu z wpisami (rysunek 7.75).

Jego treść powinna wyglądać mniej więcej tak:

```
dev tun                          #rodzaj interfejsu
local 192.168.18.1               #adres IP serwera
proto udp                        #protokół transportowy tunelu
```

```
port 17997
user openvpn
group openvpn
secret static.key                    #klucz prywatny serwera
ifconfig 10.8.0.0 255.255.255.0      #klasa adresowa, z której przydzielamy IP klientom
comp-lzo                             #algorytm kompresji
```

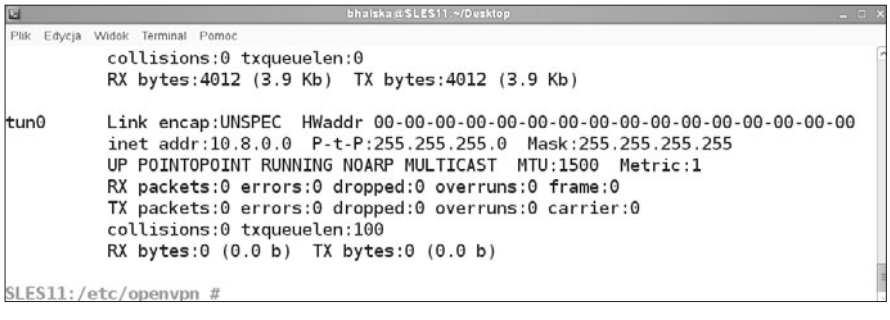


Rysunek 7.75. Plik konfiguracyjny openvpn.conf

Gdy już wszystko zostanie skonfigurowane, należy uruchomić serwer (rysunek 7.76).

Rysunek 7.76. Uruchomienie usługi z konsoli

Jeżeli wszystko jest dobrze skonfigurowane, to usługa wystartuje, a w interfejsach sieciowych pojawi się dodatkowy interfejs sieciowy (rysunek 7.77).



Rysunek 7.77. Interfejs sieciowy: Interfejs tunelowania tun0

Żeby mogło zostać zrealizowane połączenie, należy również odblokować port dla tej usługi: 17997.

ĆWICZENIA

1. Zainstaluj i skonfiguruj usługę VPN.

PYTANIA KONTROLNE

1. W jakiej warstwie modelu OSI pracuje VPN?
2. Co oznacza skrót VPN? Do czego służy VPN?
3. Z jakich protokołów korzysta usługa openVPN?

7.8.6. Firewall, czyli zapora sieciowa

Bezpieczeństwo systemu informatycznego jest jednym z priorytetowych elementów podczas projektowania struktury budowanej sieci. Z tego też względu bardzo ważne jest zabezpieczenie serwera pełniącego rolę routera.

Zapora sieciowa w Linuksie składa się z poniższych tabel:

- `filter` — zawiera większość reguł filtrowania oraz określa, czy dany pakiet zostaje dopuszczony (`ACCEPT`), czy odrzucony (`DROP`).
  - `INPUT` — obsługuje pakiety przychodzące z zewnątrz, przeznaczone do lokalnego hosta.
  - `FORWARD` — obsługuje pakiety rutowane przez hosta (pomiędzy interfejsami sieciowymi).
  - `OUTPUT` — obsługuje pakiety generowane lokalnie przez hosta.
- `nat` — wspiera mechanizm maskarady, czyli translacji adresów.
  - `PREROUTING` — służy do modyfikowania pakietów przychodzących.
  - `OUTPUT` — służy do modyfikowania pakietów generowanych lokalnie jeszcze przed routingiem.
  - `POSTROUTING` — służy do modyfikowania pakietów tuż przed wysłaniem.
- `mangle` — służy do wprowadzania zmian w pakietach.
  - `INPUT` — obsługuje pakiety przychodzące z zewnątrz, przeznaczone do lokalnego hosta.
  - `OUTPUT` — obsługuje pakiety generowanie lokalnie przez hosta.
  - `FORWARD` — obsługuje pakiety rutowane przez hosta (pomiędzy interfejsami sieciowymi).
  - `PREROUTING` — służy do modyfikowania pakietów przychodzących.
  - `POSTROUTING` — służy do modyfikowania pakietów tuż przed wysłaniem.
- `raw` — jest tabelą o najwyższym priorytecie i do niej trafiają najpierw pakiety.

Opcje filtrowania:

- `ACCEPT` (zaakceptuj pakiet) — przepuszcza pakiet.
- `DROP` (odrzuć pakiet) — nie przepuszcza pakietu.
- `REJECT` (blokuj i usuń) — blokuje i usuwa pakiet, informując o tym nadawcę.
- `QUEUE` (przepuść) — przepuszcza pakiet do przestrzeni użytkownika.

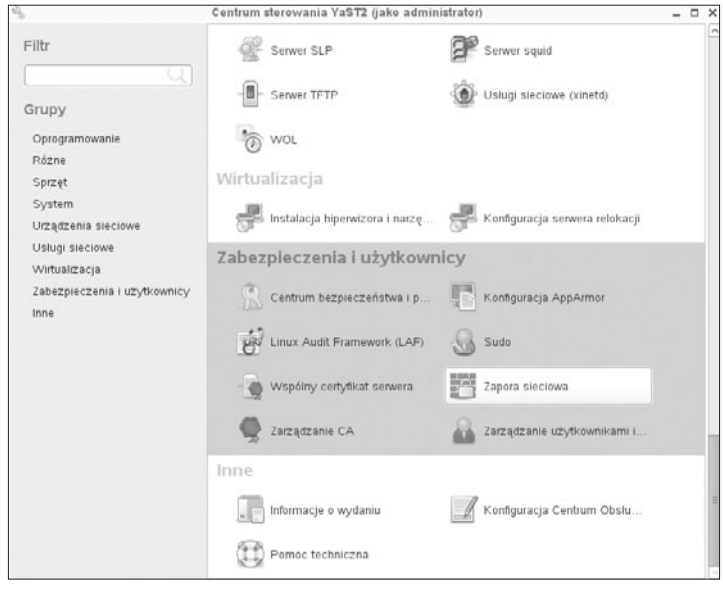
Do ręcznego zarządzania służy polecenie `iptables`. W celu sprawdzenia domyślnie skonfigurowanych reguł należy wpisać `iptables -l`. Pliki `iptables` znajdują się w katalogu */usr/sbin/iptables* (w SLES), a w niektórych dystrybucjach w */sbin/iptables*.

PRZYKŁAD

Po wpisaniu poniższych komend komputer będzie akceptował wyłącznie połączenia skierowane na porty HTTP i SSH:

```
 # iptables -P FORWARD DROP
 # iptables -P INPUT DROP
 # iptables -A INPUT --protocol tcp --destination-port 22
-j ACCEPT
 # iptables -A INPUT --protocol tcp --destination-port 80
-j ACCEPT
```

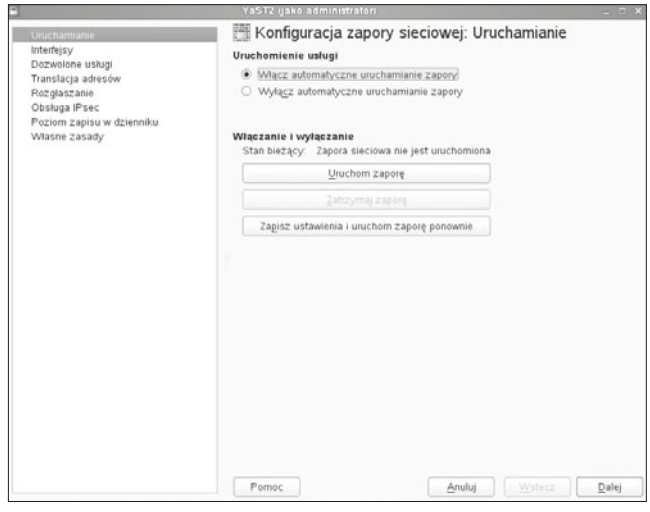
Zapora znajduje się w grupie *Zabezpieczenia i użytkownicy* w YaST2 (rysunek 7.78). Jest usługą domyślnie instalowaną w serwerze, natomiast użytkownik musi ją skonfigurować oraz włączyć.



Rysunek 7.78. YaST2: Zapora sieciowa (firewall)

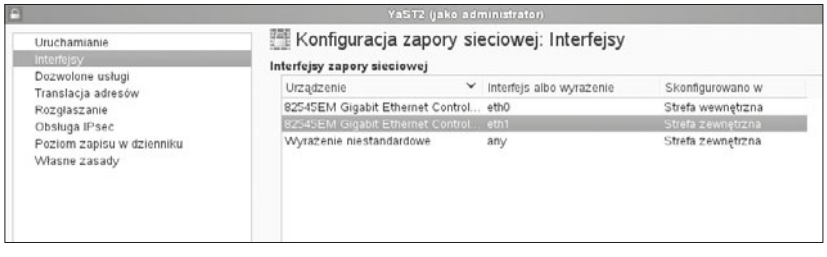
W pierwszym oknie konfiguracji zapory sieciowej należy określić opcje uruchamiania. Możemy zdefiniować automatyczne lub ręczne uruchamianie zapory oraz włączyć ją bądź wyłączyć (rysunek 7.79).

Rysunek 7.79. Firewall: Włączanie/wyłączenie usługi



Kolejnym elementem konfiguracji są interfejsy, którym powinna zostać przyporządkowana odpowiednia strefa (rysunek 7.80):

- zewnętrzna (internet) — strefa, z której przychodzące pakiety są kontrolowane, zanim zostaną przekazane do sieci wewnętrznej,
- wewnętrzna (lokalna) — strefa chroniona przez zaporę sieciową.

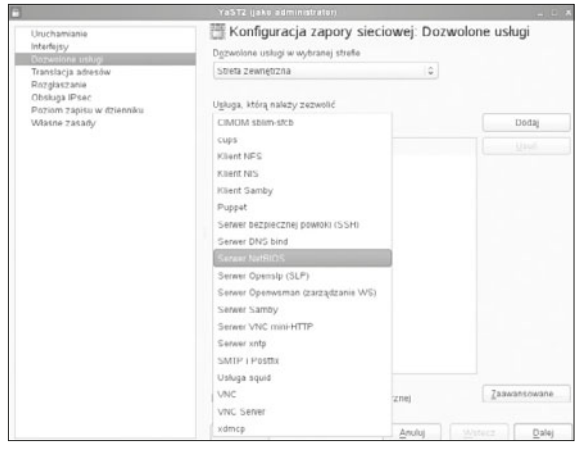


Rysunek 7.80. Firewall: Konfiguracja interfejsów

W kolejnym oknie można określić, jakie usługi będą przepuszczane między siecią zewnętrzną oraz siecią wewnętrzną (rysunek 7.81). Należy określić reguły wychodzące oraz przychodzące, a więc filtrowanie ruchu sieciowego. Filtrowanie pakietów może odbywać się według różnych kryteriów, takich jak:

- numer portu źródłowego,
- numer portu docelowego,
- protokół,
- nazwa usługi.

Podczas konfiguracji usługi należy zdefiniować, które usługi (protokoły, porty) będą w sieci dostępne.



Rysunek 7.81. Firewall: Dozwolone usługi

Podczas wyboru usługi i dodawania jej do grupy usług, które są dozwolone, system od razu otwiera porty, na których usługi pracują (tabela 7.9). Porty można również samodzielnie skonfigurować, wybierając opcję *Zaawansowane* w oknie konfiguracji dozwolonych usług.

Tabela 7.9. Usługi i ich porty według standardu IANA

Serwis	Porty TCP	Porty UDP
CUPS (aka IPP)	631	631
HTTP	80	80
HTTPS	443	443
Samba serwer	139	139
netbios serwer	137, 138	137, 138
Samba klient		137
SSH	22	22
VNC Server	5900	5900
FTP	20, 21	20, 21
DHCP	67, 68	67, 68
DNS	53	53

ĆWICZENIA

1. Uruchom usługę i skonfiguruj interfejsy, na których usługa będzie nasłuchiwać.
2. Stwórz skrypt odblokowujący usługę DNS za pomocą `iptables`.
3. Odblokuj poszczególne usługi:
   a. Samba serwer
   b. DNS
   c. DHCP
   d. SSH

PYTANIA

1. Omów usługę zapora sieciowa.
2. Na jakim porcie działa usługa HTTP, HTTPS, SSH?
3. Jakie polecenie dotyczy pakietów przychodzących, a jakie pakietów wychodzących?

7.9. Usługi serwerowe

7.9.1. Autoryzacja usług

Lightweight Directory Access Protocol (LDAP) jest protokołem przeznaczonym do uzyskiwania dostępu do usług katalogowych i zarządzania informacją.

Usługa katalogowa LDAP służy do przechowywania informacji m.in. o użytkownikach, grupach, urządzeniach sieciowych. Upraszcza w znaczący sposób zarządzanie użytkownikami, urządzeniami, aplikacjami i relacjami pomiędzy nimi. Informacje są zorganizowane w strukturze drzewa (*DIT — Directory Information Tree*), natomiast poszczególne obiekty identyfikuje się poprzez nazwę wyróżniającą (*DN — Distinguished Name*). Pierwszy, a zarazem najbardziej szczegółowy atrybut jest nazywany względną nazwą wyróżniającą (*RDN — Relative DN*). Przykładem DN-a będzie: `CN=Barbara Halska, OU=E13, O=Helion, C=Local`, gdzie `CN=Barbara Halska` to RDN dla tego DN-a.

W ramach dystrybucji SLES jako implementacje protokołu LDAP wykorzystujemy OpenLDAP. Usługę trzeba doinstalować. Aby to zrobić, wystarczy w YaST2 w usługach sieciowych uruchomić serwer LDAP, po czym nastąpi doinstalowanie pakietu openldap2.

Po zainstalowaniu jest uruchamiana usługa. W pierwszym oknie należy określić warunki uruchamiania:

- czy ma być automatyczne uruchamiana przy starcie systemu, czy nie,

- czy ma się po uruchomieniu zarejestrować w usłudze SLP (*Service Locator Protocol*) umożliwiającej automatyczne wykrycie usługi przez klientów.

Można również otworzyć port w zaporze sieciowej (firewallu).

W kolejnym oknie należy określić typ serwera (rysunek 7.82), do wyboru jest:

- *Serwer autonomiczny*,
- *Serwer nadrzędny w konfiguracji replikacji*,
- *Serwer repliki (podrzędny)*.

Rysunek 7.82. Typ serwera: autonomiczny

W kolejnym oknie przechodzimy do konfiguracji TLS (rysunek 7.83). Komunikacja w środowisku OpenLDAP jest szyfrowana za pomocą protokołu TLS.

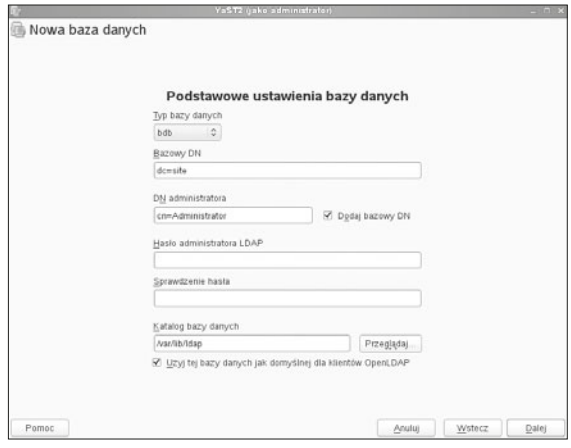
Konfiguracja na tym poziomie sprowadza się do włączenia szyfrowania i podania podstawowych parametrów:

- *Włącz TLS* — włączenie TLS, należy podać lokalizację certyfikatu,
- *Włącz interfejs LDAP przez SSL* — serwer przyjmuje połączenia na porcie 636,
- *Użyj wspólnego certyfikatu serwera* — możemy użyć do celów testowych certyfikatu stworzonego podczas instalacji SLES11; w warunkach normalnej pracy należy użyć innego certyfikatu, podając jego parametry w odpowiednich polach.

Rysunek 7.83. Ustawienia TLS

W kolejnym oknie należy skonfigurować bazę danych (rysunek 7.84).

Rysunek 7.84. Konfiguracja bazy danych LDAP



W polu *Typ bazy danych* (*Database Type*) należy wybrać typ bazy *bdb*, a do wyboru jest:

- *bdb* — *Berkley Data Base*,
- *hdb* (domyślnie) — *Hierarchical Berkley Data Base*.

Kolejne opcje, które również należy zdefiniować, to:

- *Bazowy DN* — określa nazwę korzenia bazy danych,
- *DN administratora* — określa nazwę uprzywilejowanego użytkownika bazy danych, w tym miejscu należy również zaznaczyć opcję *Dodaj bazowy DN*, co umożliwi dołączenie nazwy domeny bazowej zdefiniowanej wyżej,
- *Hasło administratora LDAP* — umożliwia ustawienie hasła użytkownika bazy danych, domyślnie jest to hasło do konta *root*,
- *Sprawdzenie hasła*,
- *Katalog bazy danych*, gdzie trzeba zaznaczyć opcję *Użyj tej bazy danych jako domyślnej dla klientów OpenLDAP*.

W ostatnim oknie konfiguracji wyświetla się podsumowanie (rysunek 7.85).

Rysunek 7.85. Podsumowanie konfiguracji serwera LDAP

Główne pliki konfiguracyjne to *slapd.conf* oraz *ldap.conf* znajdujące się w katalogu */etc/openldap*.

Centrum certyfikacji — CA (ang. certification authority)

Zarządzanie CA udostępnia możliwość konfiguracji oraz wygenerowania certyfikatu, który będzie stanowił lokalny urząd certyfikacji na potrzeby usług sieciowych. Jest usługą, która pozwala na użycie zaawansowanych mechanizmów autoryzacji, np. przy serwerach WWW, co zwiększa bezpieczeństwo.

W celu konfiguracji usługi certyfikacji należy w pierwszym kroku ją włączyć oraz określić, czy korzystamy już z istniejącego serwera CA, czy tworzymy nowy (rysunek 7.86). Usługę tę należy wybrać z YaST2 *Zabezpieczenia i użytkownicy/Zarządzanie CA*.

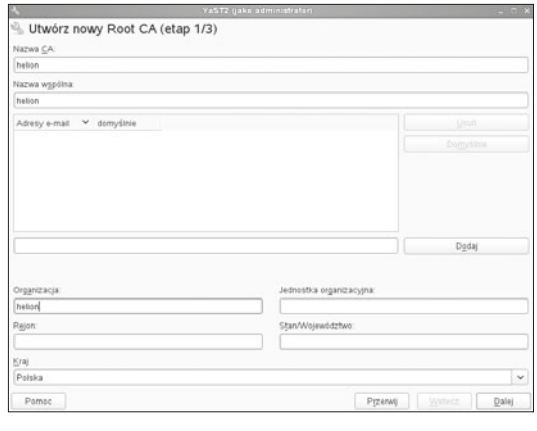
Rysunek 7.86.
Wybór CA

Po uruchomieniu centrum certyfikacji trzeba wygenerować główny certyfikat — *Utwórz główny CA*. Na początku należy określić dwie nazwy dla certyfikatu:

- *Nazwę CA* — jest nazwą techniczną dla tworzonego obiektu,
- *Nazwę wspólną* — określa nazwę tworzonego centrum certyfikacji CA.

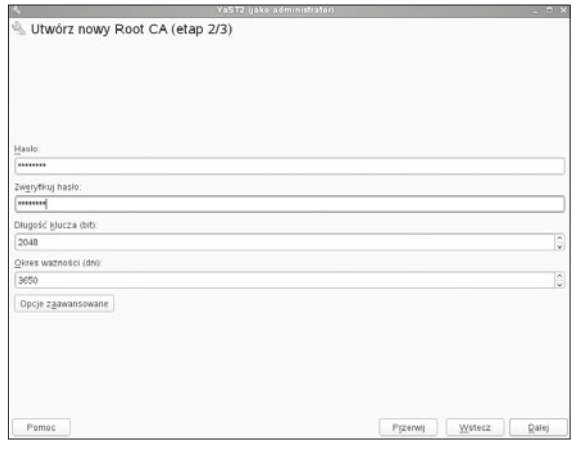
Należy również dodać adres e-mailowy administratora oraz informacje dotyczące organizacji (rysunek 7.87).

Rysunek 7.87.
Tworzenie nowego CA



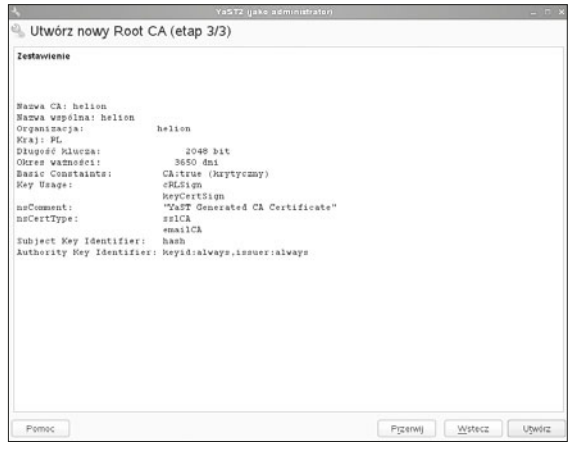
W następnym oknie konfiguracji należy określić hasło dostępu, długość klucza używanego dla certyfikatu oraz długość ważności certyfikatu (rysunek 7.88). W opcjach zaawansowanych można dookreślić ustawienia związane z certyfikatem z uwzględnieniem standardu X.509.

Rysunek 7.88. Hasło dla nowego CA



Po wprowadzeniu informacji wyświetla się podsumowanie konfiguracji (rysunek 7.89).

Rysunek 7.89. Podsumowanie dla nowego CA



Jeżeli wszystko jest skonfigurowane zgodnie z oczekiwaniami, należy wybrać opcję *Utwórz*.

7.9.2. Serwer wydruku

Zarządzanie serwerem wydruków jest jednym z zadań, które może pełnić serwer. Zadaniem takiego serwera jest rozgłaszanie drukarek w sieci, kolejkowanie zadań wydruku oraz organizacja praw dostępu do drukarek konkretnym komputerom lub użytkownikom.

Proces instalacji we wszystkich systemach operacyjnych przebiega w prawie identyczny sposób.

- Po pierwsze, należy wybrać rolę, jaką w naszej sieci będzie spełniała drukarka — czy będzie drukarką sieciową, a więc będzie z niej korzystać wielu użytkowników, czy też drukarką lokalną, czyli dostęp będą miały do niej tylko osoby korzystające z komputera, do którego jest fizycznie podpięta.
- Potem pozostaje tylko konfiguracja sieci w przypadku drukarki sieciowej lub wybór lokalnego portu przy drukarce lokalnej.

Instalacja drukarki lokalnej

Drukarki lokalne podłącza się do serwera, wykorzystując do tego jeden z fizycznych portów.

W zależności od modelu drukarki może to być port równoległy, szeregowy, podczerwieni (IrDA) lub USB.

Do każdego z wymienionych interfejsów jest przypisany plik urządzenia znajdujący się w katalogu */dev*.

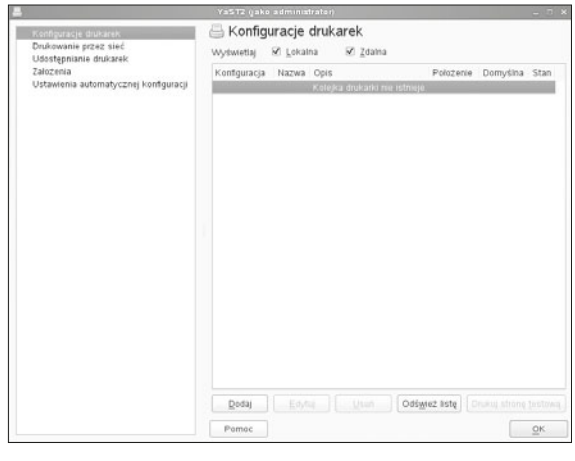
Interfejsy i przypisane im urządzenia

- Port równoległy — */dev/lp0*.
- Port szeregowy — */dev/ttyS0*, */dev/ttyS1*.
- Port IrDA — od */dev/irlpt0* do */dev/irlpt3*.
- Port USB — od /*dev/usb/lp0* do */dev/usb/lp15*.

Instalacja drukarki sieciowej

Aby podłączyć drukarkę sieciową, trzeba znać jej adres IP.

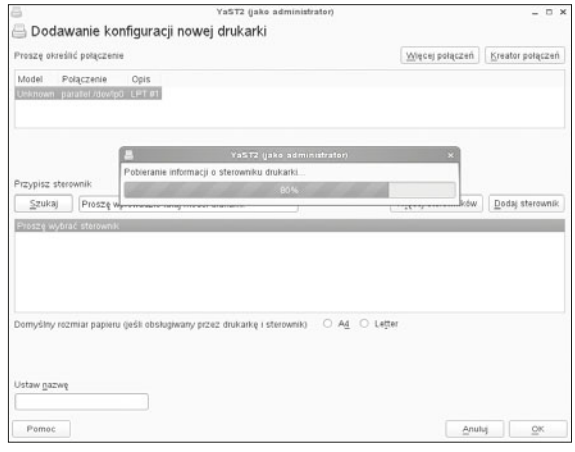
Drukarkę można dodać, korzystając z graficznego narzędzia administracyjnego YaST2, w którym należy wybrać narzędzie *Drukarka*, następnie *Konfiguracje drukarek* i kliknąć *Dodaj* (rysunek 7.90).



Rysunek 7.90. Konfiguracja drukarek

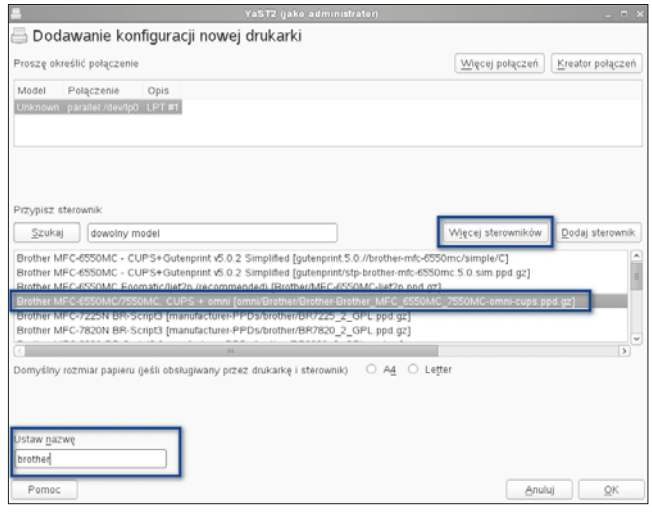
Po dodaniu drukarki system w pierwszym kroku będzie skanował w poszukiwaniu drukarki, a następnie pobierze informacje o odpowiednich sterownikach dla danej drukarki (rysunek 7.91).

Rysunek 7.91. Pobieranie informacji o sterowniku drukarki



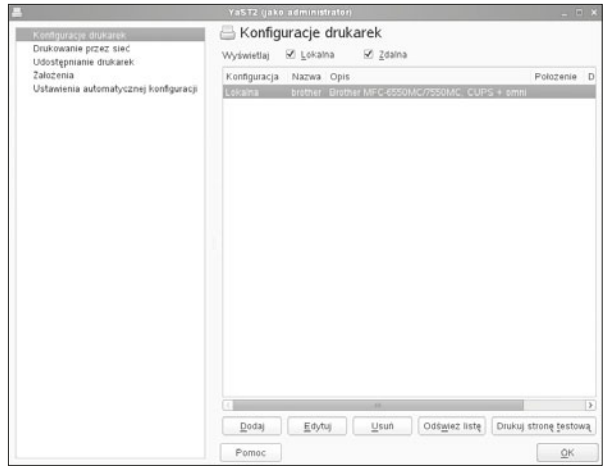
Jeżeli system nie znajdzie urządzenia, przeprowadzamy ręczną konfigurację (rysunek 7.92). Dodajemy sterownik dla drukarki, klikając *Więcej sterowników*. Dodatkowo trzeba nadać nazwę dla kolejki — w naszym przypadku będzie to *brother*.

Rysunek 7.92. Ręczna konfiguracja drukarki



Po dodaniu drukarki można wrócić do okna konfiguracji drukarek, gdzie wśród drukarek lokalnych powinna pojawić się nasza drukarka (rysunek 7.93).

Rysunek 7.93. Drukarka widoczna w oknie konfiguracji



Aby dodać drukarkę sieciową, należy w oknie dodawania drukarki wybrać opcję *Kreator połączeń*. Kreator ten został podzielony na 4 części (rysunek 7.94):

- *Urządzenie podłączone bezpośrednio* — jest to część, która dotyczy konfiguracji drukarki podłączonej bezpośrednio przez wybór odpowiedniego portu lub usługi, takich jak:
  - » *Port równoległy*,
  - » *Port USB*,
  - » *Port szeregowy*,
  - » *Urządzenie Bluetooth*,
  - » *SCSI*,
  - » *Urządzenia HP (HPLIP)* — linuksowy system obsługi drukarek HP.
- *Dostęp do drukarki sieciowej albo serwera z usługą wydruku* — w tej części należy skonfigurować wydruk sieciowy:
  - » *Port TCP* — port dla drukarki lub serwera wydruku,
  - » *Protokół LPD* — protokół drukowania w sieci,
  - » *Protokół IPP* — protokół wykorzystywany do komunikacji z drukarką w sieci.
- Sewer wydruku — w tej części należy wybrać odpowiedni serwer wydruku, przez który będzie możliwy wydruk:
  - » *Microsoft Windows/SAMBA (SMB/CIFS)* — wydruk w oparciu o udostępnianie drukarki za pomocą Microsoft lub usługi Samba,
  - » *Tradycyjny serwer UNIX (LPR)* — tradycyjny uniksowy serwer wydruku w oparciu o protokół LPR,
  - » *Serwer CUPS*,
  - » *Serwer drukujący Novell Netware (IPX)*.
- Ustawienia specjalne.

Rysunek 7.94. Konfiguracja połączenia z drukarką sieciową

W cześci *Dostęp do drukarki sieciowej albo serwera z usługą wydruku* należy wybrać *Port TCP*, gdzie w *Ustawieniach połączenia* trzeba podać adres IP drukarki, z listy rozwijanej wybrać producenta i przetestować połączenie. Jeżeli test zostanie zakończony sukcesem, można wrócić do okna dodawania drukarki, gdzie powinna się pojawić nasza drukarka.

Serwer wydruku CUPS

Obecnie najczęściej stosowanym serwerem wydruku w systemach Linux jest CUPS (ang. *Common UNIX Printing System*). Ten najbardziej uniwersalny serwer jest domyślnie zainstalowany w dystrybucji SLES, wymaga jednak konfiguracji.

Pakiety, które są niezbędne do udostępnienia serwera wydruków opartego na CUPS, pokazuje tabela 7.10.

Tabela 7.10. Pakiety CUPS

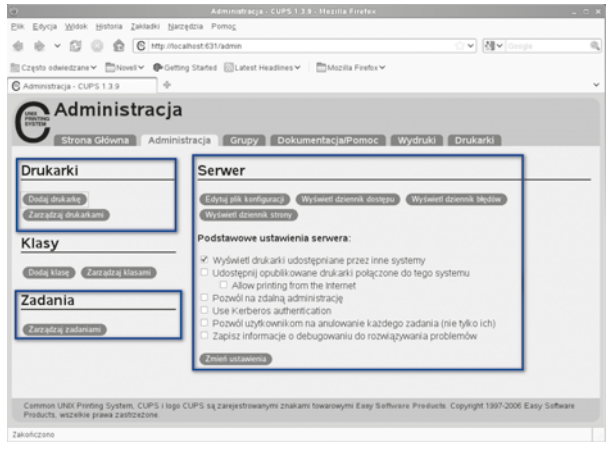
Pakiet	Zawartość
`cups`	Demon usługi drukowania: `cupsd`
`cups-client`	Umożliwia uruchomienie klienta `cups`
`cups-drivers`	Sterowniki dla kolejek drukowania
`cups-libs`	Biblioteki usługi drukowania

Konfiguracja serwera CUPS odbywa się z wykorzystaniem dowolnej przeglądarki WWW. Aby połączyć się z serwerem z komputera, na którym jest on zainstalowany, w polu adresu trzeba wpisać `http://localhost:631` (w przypadku konfiguracji serwera uruchomionego na innym komputerze wpisujemy zamiast localhost adres IP komputera z uruchomionym CUPS). Uruchomiony CUPS i prawidłowo wpisany adres pozwoli nam na zobaczenie strony domowej serwera (rysunek 7.95).

Rysunek 7.95.
Konfiguracja serwera wydruku CUPS

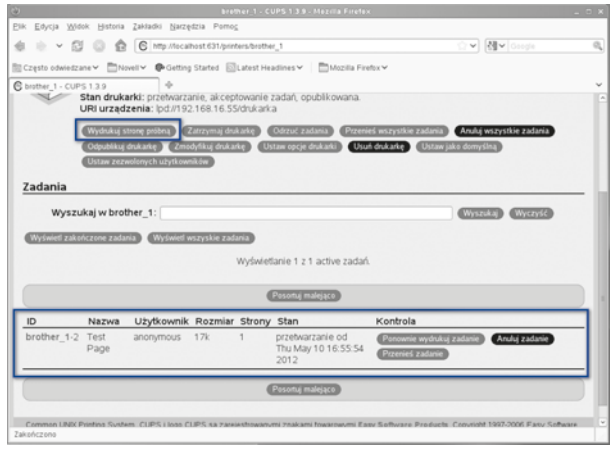
Poszczególne zakładki serwisu umożliwiają skonfigurowanie tej usługi. W zakładce *Administracja* (rysunek 7.96) można dodać drukarki, zadania, skonfigurować serwer.

Rysunek 7.96.
Administracja serwerem wydruku

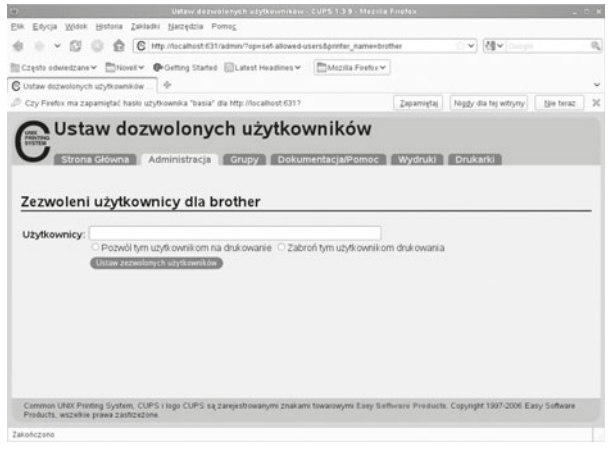


Kolejna bardzo ważna zakładka to *Drukarki*, w której można zmienić ustawienia drukarki, określić uprawnienia dla użytkowników, wydrukować stronę testową, co skutkuje pojawieniem się zadania, które m.in. można anulować (rysunek 7.97).

Rysunek 7.97.
Konfiguracja drukarek



Aby określić, czy dany użytkownik może drukować, czy nie, należy wybrać opcję *Ustaw zezwolonych użytkowników* i wpisać nazwę użytkownika oraz ustalić, czy dla danego użytkownika drukowanie będzie dozwolone, czy zabronione (rysunek 7.98).



Rysunek 7.98. Ustawienie zezwolonych użytkowników

ĆWICZENIA

1. Zainstaluj drukarkę lokalną lub sieciową.
2. Zainstaluj i skonfiguruj serwer wydruku.
3. Utwórz grupę, która jako jedyna będzie mogła drukować na zainstalowanej przez Ciebie drukarce.

PYTANIA

1. Omów serwer wydruku.
2. W jaki sposób drukarki mogą być podłączane do serwera wydruku?
3. Pod jakim adresem jest dostępna usługa CUPS?

7.9.3. Serwer plików Samba

Serwer Samby umożliwia udostępnienie linuksowych usług drukowania oraz serwera plików stacjom roboczym Windows, OS X, OS/2, Linux. Użytkownicy mogą współdzielić katalogi i drukarki systemu linuksowego tak, jak to robią na serwerze Windows. Można też skonfigurować Sambę jako kontroler domeny, a nawet podłączyć do domeny Usługi Katalogowej.

Usługa ta używa protokołu SMB (ang. *Server Message Block*). Serwer Samby to trzy współpracujące ze sobą demony. Pierwszy z nich to smbd, który jest odpowiedzialny za

współdzielenie plików, drukarek, uwierzytelnianie oraz blokowanie zasobów. Drugi to nmbd, który zapewnia wsparcie dla usług nazewniczych w standardzie WINS (pozwala rejestrować i rozpoznawać nazwy NetBIOS jako używane w sieci adresy IP). Ostatnim demonem jest winbindd, który integruje bazy danych wykorzystywane podczas weryfikacji praw użytkowników.

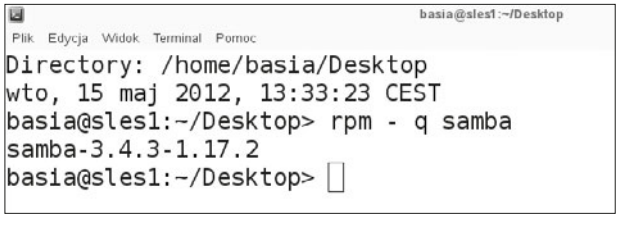
Należy zainstalować następujące pakiety Samby:

- `samba`: główny pakiet Samby, zawiera oprogramowanie serwera,
- `samba-client`: zawiera narzędzia klienta Samby.

Można sprawdzić, czy wymagane pakiety są już zainstalowane, przy użyciu poleceń (informacja o pakietach w podrozdziale 7.3):

- `rpm -q samba`
- `rpm -q samba-client`

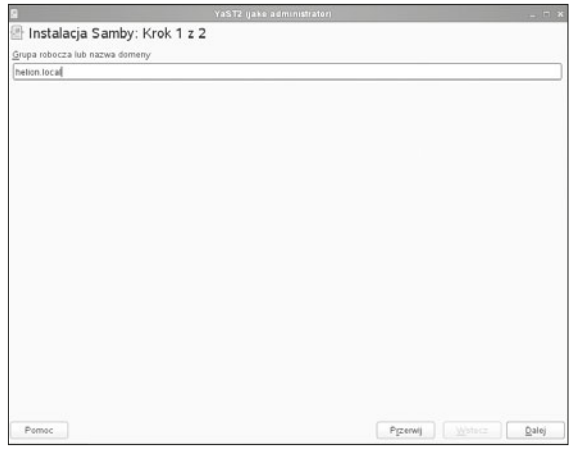
Jeżeli są zainstalowane, zostanie podana ich wersja, jeżeli nie, pojawi się komunikat o błędzie (rysunek 7.99).



Rysunek 7.99. Sprawdzenie wersji zainstalowanej usługi Samba

W wersji serwerowej SUSE Enterprise ta usługa jest już zainstalowana, więc pozostaje ją tylko skonfigurować. Aby to zrobić, trzeba przejść do zakładki *Usługi sieciowe* i wybrać serwer Samby. Po uruchomieniu kreatora konfiguracji należy określić nazwę grupy roboczej lub domeny (rysunek 7.100).

Rysunek 7.100. Nadanie nazwy dla grupy roboczej lub domeny



W kolejnym kroku należy określić, jaką rolę ma pełnić serwer Samby (rysunek 7.101), wybierając jedną spośród następujących opcji:

- *Podstawowy sterownik domeny (PDC)* — główny kontroler domeny,
- *Zapasowy sterownik domeny (BDC)* — zapasowy kontroler domeny,
- *Nie jest sterownikiem domeny*.

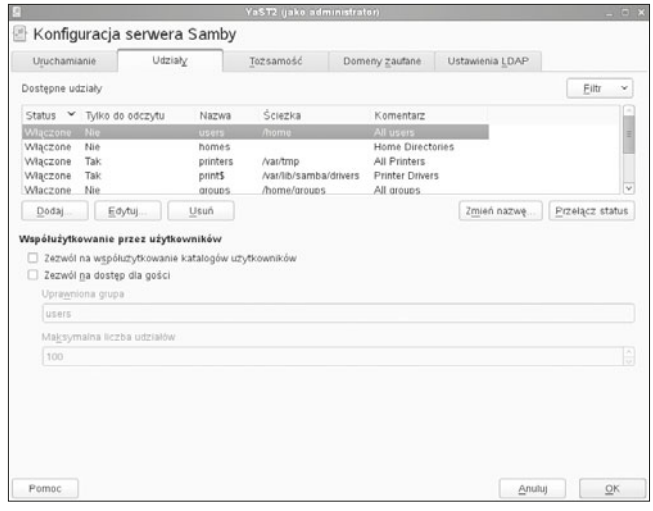
Rysunek 7.101. Rodzaj serwera Samby

Po wybraniu typu serwera wyświetli się kolejne okno konfiguracyjne dla serwera. Pierwsza zakładka *Uruchamianie* pozwala zdefiniować, w jaki sposób będzie uruchamiana usługa, oraz dostosować zaporę sieciową do współpracy z serwerem poprzez otwarcie portów dla usługi (rysunek 7.102).

Rysunek 7.102. Uruchamianie usługi

Kolejna zakładka nosi nazwę *Udziały* i umożliwia konfigurację oraz dodawanie udziałów dyskowych, drukarek (rysunek 7.103). Tabela w górnej części okna przedstawia zasoby serwera. Każdy z widocznych w tym miejscu udziałów odpowiada oddzielnej sekcji w pliku *smb.conf*. Wybrany udział jest określany przez pięć zmiennych w kolejnych kolumnach. W pierwszej jest informacja o statusie udziału — włączony lub nie. W celu zmiany statusu udziału należy użyć przycisku *Przełącz status*. Kolejna kolumna *Tylko do odczytu* informuje, z jakimi prawami został dodany udział. Następna kolumna informuje

Rysunek 7.103.
Udziały



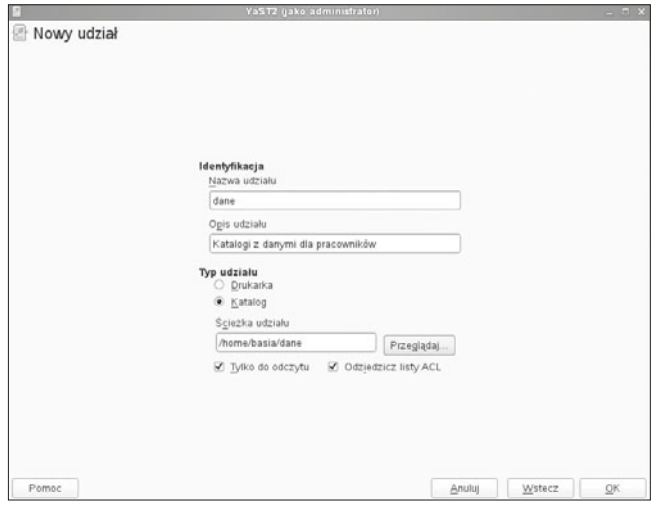
o nazwie udziału i nie ma większego znaczenia dla konfiguracji. Kolejna — określa ścieżkę do udziału. Ostatnia kolumna to komentarz dla danego udziału.

W celu dodania nowego udziału należy kliknąć opcję *Dodaj*. Pojawi się kreator dodawania, który nas poprowadzi. W pierwszym oknie kreatora trzeba podać nazwę udziału, następnie określić typ udziału — katalog czy drukarka — oraz ścieżkę udziału i uprawnienia (rysunek 7.104):

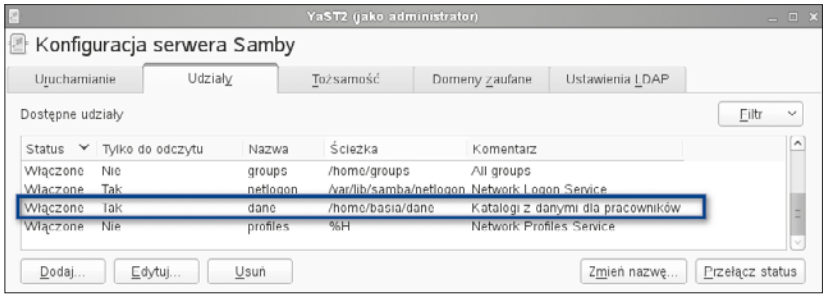
- *Tylko do odczytu*,
- *Odziedzicz listy ACL* — listy kontroli dostępu (ang. *Access Control List* — *ACL*).

Jeśli dany katalog nie został wcześniej utworzony, system umożliwi jego utworzenie podczas określania ścieżki udziału.

Rysunek 7.104.
Nowy udział



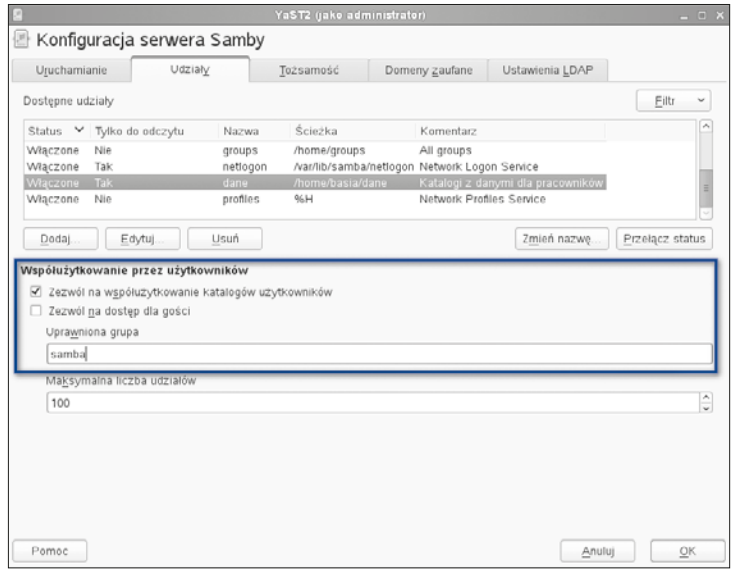
Jeżeli udział został poprawnie dodany, powinien pojawić się na liście udziałów (rysunek 7.105). Każdemu z udziałów odpowiada oddzielna sekcja w pliku konfiguracyjnym *smb.conf*.



Rysunek 7.105. Potwierdzenie dodania nowego udziału

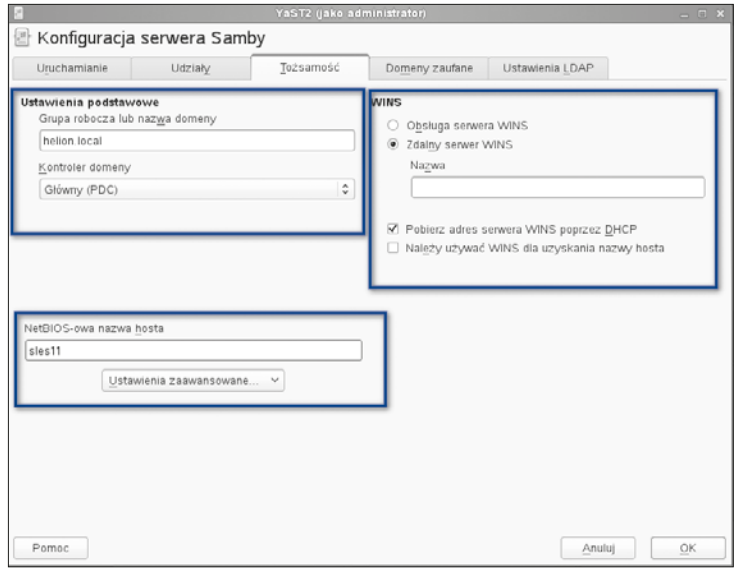
W tym miejscu można również zdefiniować, którzy użytkownicy (z jakiej grupy) będą mogli korzystać z tego zasobu, oraz ograniczyć maksymalną liczbę udziałów (rysunek 7.106).

Rysunek 7.106. Współużytkowanie przez użytkowników



W zakładce *Tożsamość* można zmienić ustawienia (rysunek 7.107), takie jak:

- *Grupa robocza lub nazwa domeny*,
- *Kontroler domeny*,
- *WINS* — umożliwia rozwiązywanie nazw netbiosowych,
- *NetBIOS-owa nazwa hosta* — umożliwia identyfikację hosta w sieci.



Rysunek 7.107. Zakładka Tożsamość w oknie Konfiguracja serwera Samby

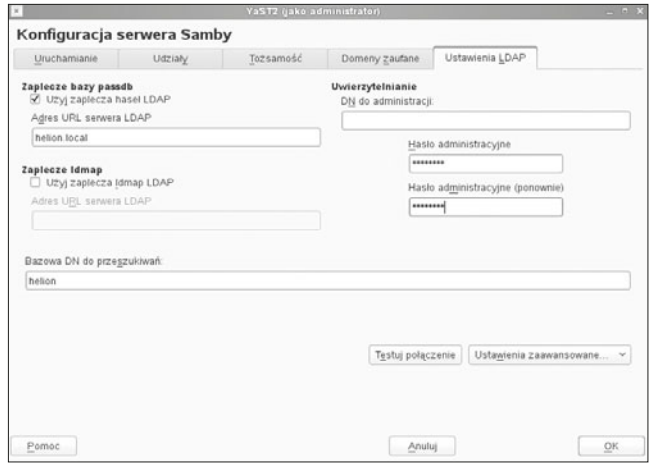
W kolejnej zakładce (rysunek 7.108) można dodać domeny zaufane. Można w tym miejscu zdefiniować domeny, których użytkownicy będą mieli na zasadzie zaufania dostęp do konfigurowanej domeny Samby. Ważne jest, aby przy dodaniu domeny zaufania nadać hasło, które będzie wykorzystywane podczas przydzielania dostępu do zaufanej domeny.

Rysunek 7.108. Zakładka Domeny zaufane w oknie Konfiguracja serwera Samby

W ostatniej zakładce istnieje możliwość skonfigurowania uwierzytelniania przy użyciu LDAP (rysunek 7.109). Aby to zrobić, trzeba znać:

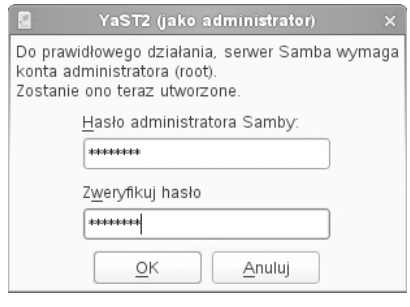
- adres serwera LDAP — protokół przeznaczony do korzystania z usług katalogowych, pozwalający na wymianę informacji za pośrednictwem TCP/IP (został omówiony w punkcie 7.9.1).
- nazwę bazy użytkowników.
- hasło administracyjne.

Rysunek 7.109.
Ustawienia LDAP



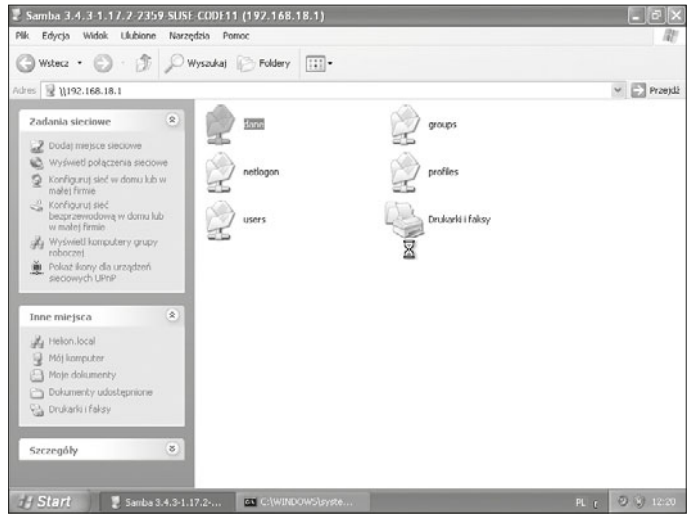
W ostatnim kroku konfiguracji serwera Samby trzeba nadać hasło do celów administracyjnych (rysunek 7.110). Ważne jest, aby to hasło było inne od hasła konta *root*.

Rysunek 7.110.
Definiowanie hasła



W celu sprawdzenia udziałów należy uruchomić lub wpisać w przeglądarce adres serwera Samby: *\\192.168.18.1*. Jeżeli wszystko jest dobrze skonfigurowane, zgłosi się serwer Samby (rysunek 7.111).

Rysunek 7.111.
Serwer Samby



Aby zalogować się do serwera Samby, trzeba mieć założone konto użytkownika na serwerze. W tym celu z konsoli należy wpisać:

```
smbpasswd -a basia
```

Po wpisaniu powyższego polecenia trzeba podać hasło dla użytkownika. Po poprawnym zweryfikowaniu hasła konto zostanie utworzone.

ĆWICZENIA

1. Zainstaluj i skonfiguruj usługę Samba jako główny kontroler domeny.
2. Dodaj do usługi udostępniany zasób o nazwie *wspolny*, do którego wszyscy mają prawa tylko do odczytu.

PYTANIA

1. Omów usługę `samba`.
2. Co oznacza zapis PDC?
3. W jaki sposób mogą być uwierzytelniani użytkownicy?
4. Jakim poleceniem dodajemy użytkowników do serwera Samby?

7.10. Usługi internetowe

7.10.1. Serwer WWW (Apache)

Apache — otwarty serwer HTTP, dostępny dla wielu systemów operacyjnych (m.in. UNIX, GNU/Linux, BSD, OS X, Microsoft Windows).

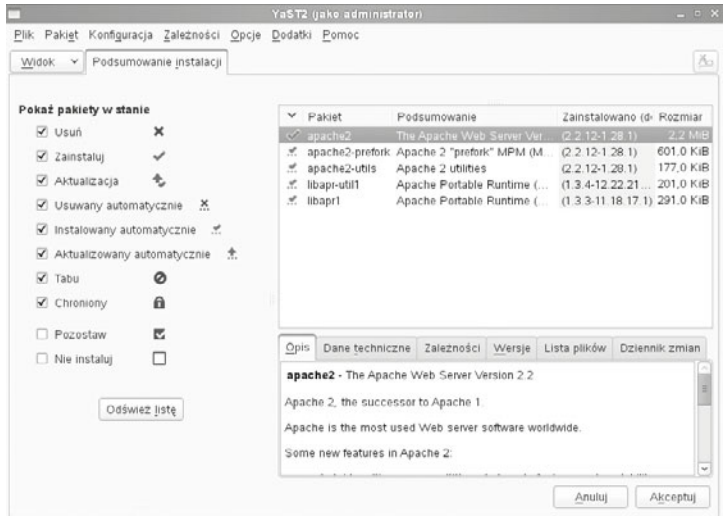
Apache jest najszerzej stosowanym serwerem HTTP w internecie. W połączeniu z interpreterem języka skryptowego PHP i bazą danych MySQL Apache stanowi jedno z najczęściej spotykanych środowisk w firmach oferujących miejsce na serwerach sieciowych.

Instalacja serwera Apache

W celu zainstalowania serwera Apache w repozytoriach oprogramowania należy wyszukać apache2, a system wybierze związane z nim pakiety, takie jak (rysunek 7.112):

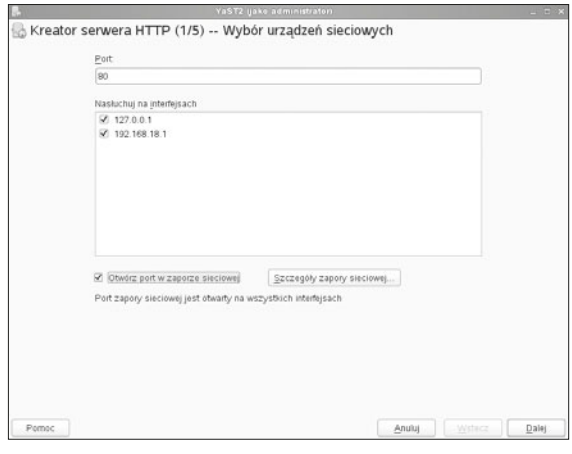
- `apache2`
- `apache2-example-pages`
- `apache2-prefork`

Rysunek 7.112. Wybór pakietów do instalacji



Po zainstalowaniu i uruchomieniu usługi *Serwer HTTP*, która jest składową *Usługi sieciowe* w YaST2, pojawi się kreator konfiguracji serwera HTTP. W pierwszym oknie poprosi o podanie portu dla usługi oraz interfejsów, na których ta usługa będzie nasłuchiwała, oraz otwarcie portu w zaporze sieciowej (rysunek 7.113).

Rysunek 7.113. Wybór urządzeń sieciowych



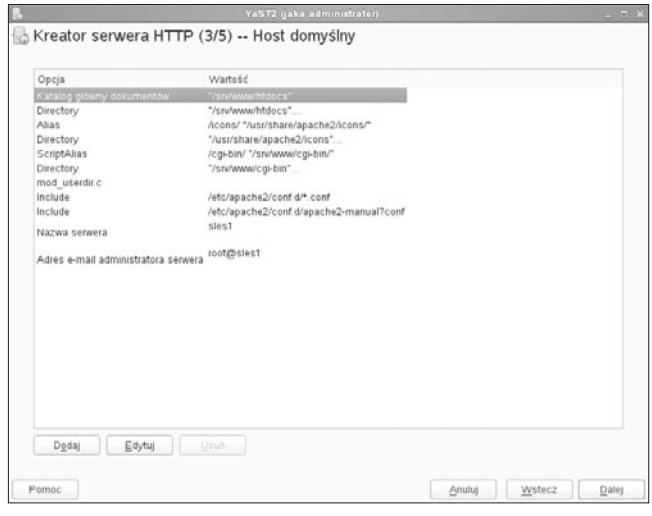
W kolejnym oknie można wybrać moduły, które mają być doinstalowane (rysunek 7.114):

- obsługę skryptów PHP,
- obsługę skryptów Perl,
- obsługę skryptów Python.

Rysunek 7.114. Wybór modułów

W następnym oknie kreatora konfiguracji wyświetla się informacja dotycząca konfiguracji serwera oraz miejsca przechowywania plików (rysunek 7.115). Można to zmodyfikować lub pozostawić bez zmian, przechodząc do następnego okna konfiguracji.

Rysunek 7.115. Podsumowanie konfiguracji serwera

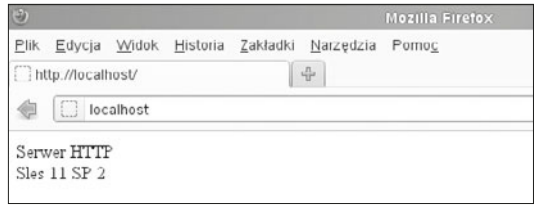


W kolejnym oknie konfiguracji istnieje możliwość stworzenia wirtualnych hostów, czyli poddomen, a więc wielu różnych serwisów internetowych. W naszym przypadku nie jest to wymagane.

W ostatnim oknie kreatora konfiguracji wyświetla się podsumowanie, można w nim także określić sposób uruchamiania usługi oraz dokonać zaawansowanej konfiguracji serwera HTTP.

Po zakończeniu procesu instalacji i konfiguracji usługi należy sprawdzić, czy usługa działa, przez wpisanie w przeglądarce *http://localhost* (rysunek 7.116). Usługa jest również dostępna pod adresem, który został zdefiniowany podczas konfiguracji. W tym przykładzie jest to: 192.168.18.1.

Domyślnym katalogiem, w którym są przechowywane dokumenty obsługiwanej witryny, jest */srv/www/htdocs*. W innych dystrybucjach często jest to */var/www/localhost/htdocs* lub */var/www/htdocs*.



Rysunek 7.116. Sprawdzenie usługi w przeglądarce

Sama usługa może być konfigurowana w trybie graficznym za pomocą YaST2, jak również w pliku konfiguracyjnym */etc/apache2/httpd.conf*. Pozostałe pliki związane z usługą znajdują się w katalogach */etc/apache2*, */etc/apache2/conf.d*, */etc/apache2/vhosts.d* oraz */etc/apache2/sysconfig.d*.

Do najważniejszych katalogów serwera Apache należą:

- *conf.d* — przechowuje pliki konfiguracyjne dodane przez inne moduły,
- *sysconfig.d* — zawiera pliki konfiguracyjne utworzone automatycznie na podstawie pliku */etc/sysconfig/apache2*,
- *vhosts.d* — zawiera pliki konfiguracyjne hostów wirtualnych.

Do najważniejszych plików konfiguracyjnych należą:

- *httpd.conf* — główny plik konfiguracyjny serwera WWW, zawiera instrukcje i ustawienia globalne, a także dotyczące lokalizacji dodatkowych plików konfiguracyjnych,
- *default-server.conf* — przechowuje opcje globalne dla hostów wirtualnych, które są tworzone na serwerze,
- *errors.conf* — plik określający zachowanie się serwera po wykryciu błędów, opcje zawarte w tym pliku są wyspecyfikowanymi opcjami domyślnymi dla dodawanych na serwerze hostów wirtualnych,
- *listen.conf* — przechowuje adresy IP oraz powiązane z nimi numery portów, na których będzie nasłuchiwał serwer,
- *server-tuning.conf* — konfiguracja parametrów zwiększających wydajność,
- *ssl-global.conf* — konfiguracja połączeń szyfrowanych przez SSL,
- *uid.conf* — tożsamość, w kontekście której będzie działał proces serwera Apache (w dystrybucji Suse domyślnie użytkownik wwwrun i grupa www w innych może być apache, apache2 lub www-data),
- *mod_*.conf* — są to pliki konfiguracyjne modułów instalowanych domyślnie przez serwer Apache; pliki modułów instalowanych dodatkowo znajdują się w katalogu *conf.d*.

Zawartość katalogu */etc/apache2/conf.d* zależy od tego, które moduły zostały wybrane podczas instalacji. Mogą znajdować się w nim następujące pliki:

- *apache2-manual.conf* — dokumentacja konfiguracji serwera Apache,
- *inst_server.conf.in* — plik konfiguracji instalacji z pliku *httpd.conf*,
- *mod_perl.conf* — konfiguracja modułu interpretera dla Perl,
- *php5.conf* — konfiguracja modułu interpretera dla PHP,
- *phpmyadmin.conf* — konfiguracja narzędzia phpMyAdmin.

ĆWICZENIA

1. Zainstaluj i skonfiguruj serwer Apache.
2. Stwórz własną stronę internetową i opublikuj ją na swoim serwerze WWW.
3. Stwórz własną stronę internetową w PHP i opublikuj ją na serwerze WWW.

PYTANIA KONTROLNE

1. Omów usługę serwera WWW.
2. Jak nazywa się główny plik konfiguracyjny serwera Apache?
3. Z jakim rozszerzeniem należy zapisywać strony WWW i do jakiego katalogu serwera Apache należy je skopiować?

7.10.2. Serwer FTP

Pure-FTPd to szybki serwer FTP. Oprogramowanie charakteryzuje się bardzo łatwą obsługą i wsparciem dla najnowszych wersji Linuksa. Serwer wspiera protokoły IPv4 i IPv6, wirtualne domeny i wiele innych usług. Platforma zawiera również narzędzia do zarządzania portami, ograniczeniami transferu. Ważną cechą serwera Pure-FTPd jest możliwość wznowienia transmisji danych w przypadku zerwania połączenia, od miejsca, w którym została ona przerwana. Sesja w ramach usługi jest zestawiana z wykorzystaniem protokołu TCP w taki sposób, że aktywowane są dwa oddzielne połączenia. Jedno służy do przekazywania poleceń (port 21) i określa się je mianem połączenia kontrolnego, drugie służy do przesyłania danych. Protokół FTP może pracować w dwóch trybach:

- aktywnym — połączenie kontrolne na porcie 21, nawiązywane przez klienta, przesył danych na porcie 20, nawiązywane przez serwer,
- pasywnym — port 21 dla poleceń i port powyżej 1024 dla transmisji, zestawiane przez klienta.

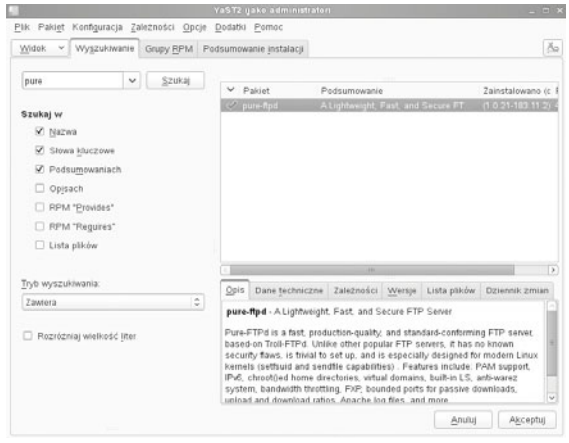
Pakiety dla serwera Pure-FTPd możemy zainstalować z repozytoriów (zostało to omówione w podrozdziale 7.3) znajdujących się na nośniku lub z YaST2 (rysunek 7.117).

Po wybraniu instalacji usługi kreator instaluje jeszcze dodatkowe niezbędne pakiety (rysunek 7.118).

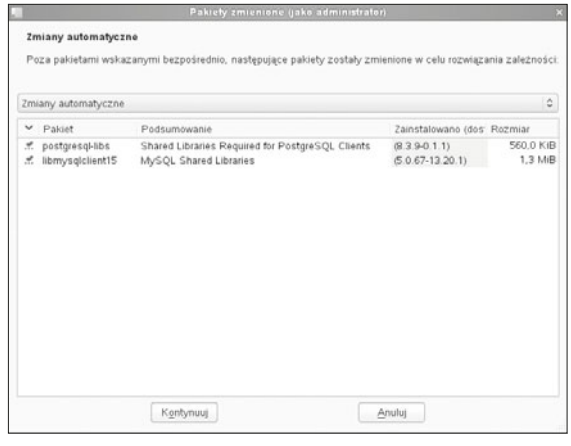
Po zainstalowaniu usługi w celu jej skonfigurowania oraz uruchomienia z usług sieciowych w YaST2 należy wybrać *Serwer FTP*.

Wyświetla się kreator konfiguracji, gdzie w pierwszym oknie należy zdefiniować sposób uruchamiania usługi i można ją od razu uruchomić (rysunek 7.119).

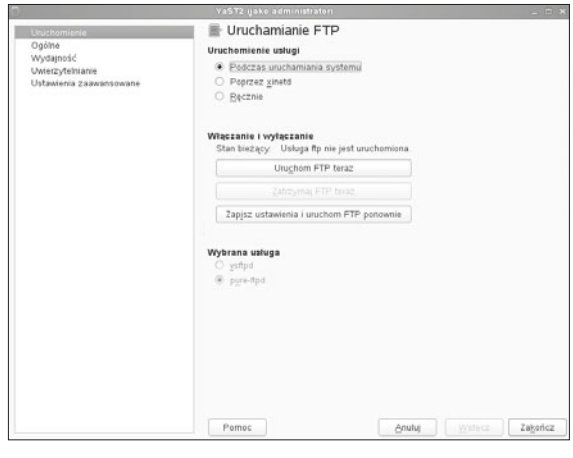
Rysunek 7.117.
Instalacja serwera FTP z repozytoriów



Rysunek 7.118.
Instalacja dodatkowych pakietów do FTP



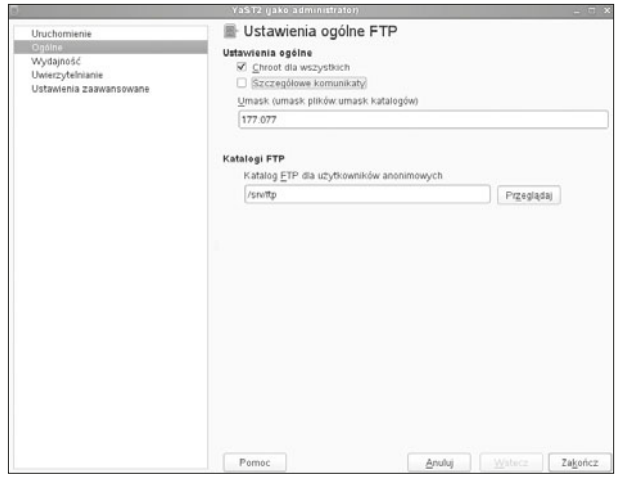
Rysunek 7.119.
Konfiguracja uruchamiania FTP



W następnym oknie kreatora (rysunek 7.120) są definiowane informacje ogólne, takie jak:

- umask — to maska uprawnień nowo tworzonych plików (w momencie tworzenia nowego pliku),
- położenie katalogu FTP dla użytkowników anonimowych.

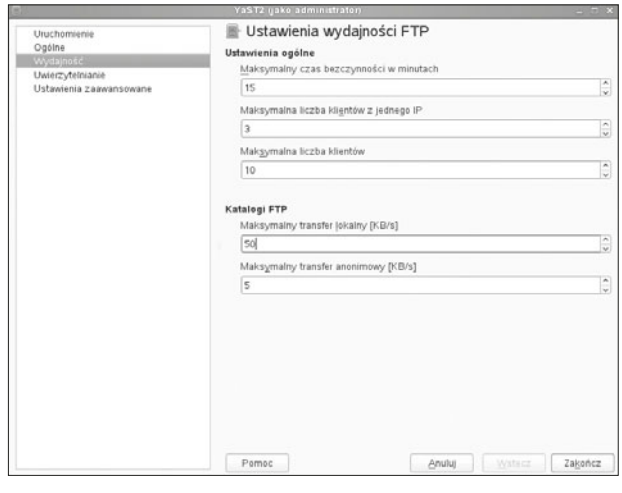
Rysunek 7.120. Ustawienia ogólne



W kolejnym oknie należy określić wydajność serwera (rysunek 7.121), a więc podać takie informacje, jak:

- *Maksymalny czas bezczynności w minutach*,
- *Maksymalna liczba klientów z jednego IP*,
- *Maksymalna liczba klientów*,
- *Maksymalny transfer lokalny* podany w kB/s,
- *Maksymalny transfer anonimowy* podany w kB/s.

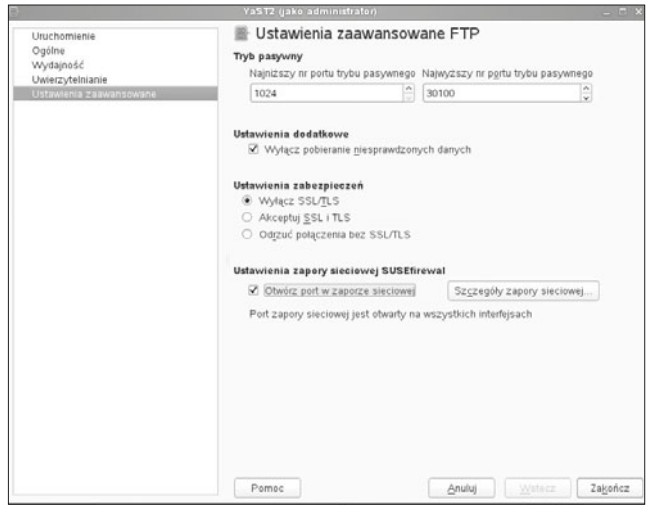
Rysunek 7.121. Ustawienia wydajności FTP



W następnym oknie kreatora (rysunek 7.122) należy określić sposób uwierzytelniania:

- *Tylko dla anonimowych*,
- *Tylko dla uwierzytelnionych*,
- *Dla wszystkich*.

Rysunek 7.122. Ustawienia zaawansowane



W ostatnim oknie konfiguracji serwera FTP (rysunek 7.123) można zmienić ustawienia dotyczące bezpieczeństwa oraz otworzyć port w zaporze sieciowej.

Po konfiguracji należy sprawdzić status usługi. W tym celu z konsoli wystarczy wpisać:

```
/etc/init.d/pure-ftpd status
```

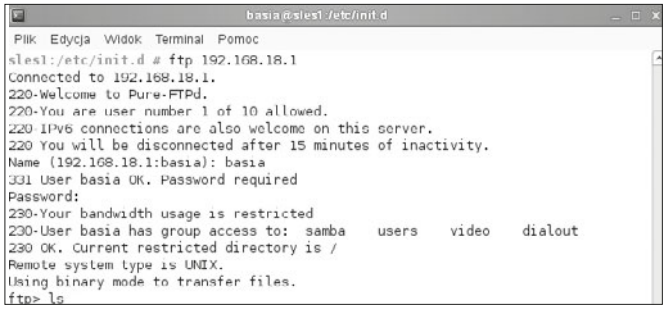
Rysunek 7.123. Status usługi

Łączenie z serwerem z konsoli SUSE (rysunek 7.124):

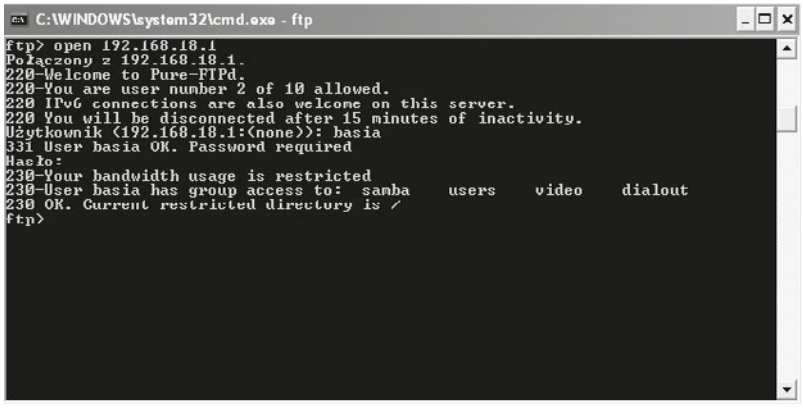
```
ftp 192.168.18.1
```

Łączenie z serwerem z konsoli Windows (rysunek 7.125):

```
ftp
open 192.168.18.1
```

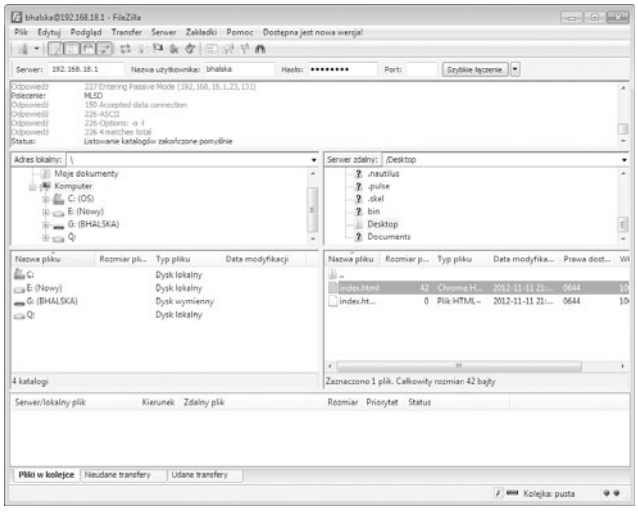


Rysunek 7.124. Połączenie z serwerem FTP z konsoli SUSE



Rysunek 7.125. Połączenie z serwerem FTP z konsoli Windows XP

Łączenie z serwerem przez klienta FTP, np. FileZilla (rysunek 7.126):



Rysunek 7.126. Łączenie z serwerem FTP przez klienta FTP FileZilla

ĆWICZENIA

1. Zainstaluj i skonfiguruj usługę FTP.
2. Stwórz nową grupę w usłudze katalogowej o nazwie FTP, dodaj do tej grupy dwóch użytkowników *ftp_1* i *ftp_2*.
3. Stwórz folder FTP, który będzie miejscem publikacji plików.
4. Stwórz w folderze FTP katalogi i zdefiniuj do nich następujące uprawnienia:
   a. *ftp_1* — pełny dostęp ma tylko użytkownik *ftp_1*,
   b. *ftp_2* — pełny dostęp ma tylko użytkownik *ftp_2*,
   c. *sterowniki* — prawa do odczytu mają obaj użytkownicy.

PYTANIA KONTROLNE

1. Omów usługę FTP.
2. Na jakim porcie jest aktywna usługa FTP?
3. W jaki sposób można się połączyć z usługą FTP?
4. Jakie polecenie pozwala połączyć się z serwerem FTP z konsoli?

7.10.3. Serwer pocztowy

Podczas instalacji serwera SLES od razu zostaje zainstalowany serwer poczty elektronicznej Postfix (MTA), który jest odpowiedzialny za przekazywanie i dostarczanie poczty elektronicznej.

Pojęcia podstawowe

MTA — *Mail Transfer Agent* — są to programy takie jak Postfix, które zajmują się przesyłaniem poczty w sieci.

MUA — *Mail User Agent* — są to programy wykorzystywane przez użytkownika do komponowania wiadomości, odczytu wiadomości itp., czyli programy takie jak Mutt.

MDA — *Mail Delivery Agent* — przykładem takiego programu jest procmail, który jest odpowiedzialny za dostarczenie poczty lokalnie do użytkownika (wykonuje m.in. filtrowanie poczty).

FQDN — *Fully Qualified Domain Name* — pełna nazwa domenowa, składa się z nazwy hosta oraz domeny, w której dany host się znajduje.

QM — *Queue Manager* — program wchodzący w skład serwera Postfix, odpowiedzialny za przetworzenie poczty czekającej w kolejce.

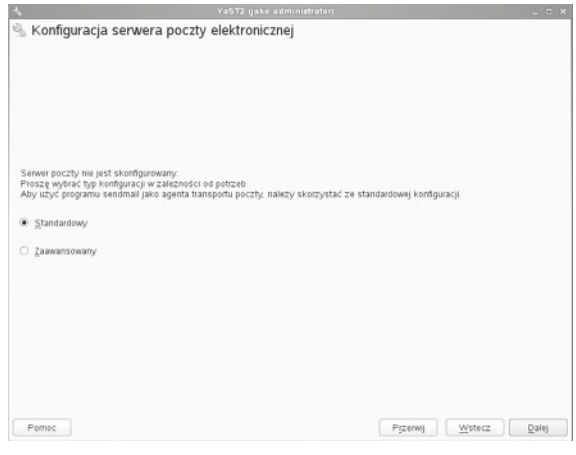
Open Relay — to określenie serwera pocztowego, którego oprogramowanie nie jest zabezpieczone przed nieautoryzowanym wykorzystaniem przez osoby niepowołane do wysyłki poczty elektronicznej, zazwyczaj spamu.

UCE — *Unsolicited Commercial Email* — ogólne określenie dla niepożądanej poczty, dotyczy ono poczty docierającej do serwera, której z określonych powodów nie chcemy przetwarzać.

Żeby można było skutecznie zainstalować serwer za pomocą YaST2, w sieci muszą działać usługi LDAP, DHCP, DNS oraz musi być włączone uwierzytelnianie lokalnych użytkowników systemowych. Można również samodzielnie przeprowadzić instalację, ale trzeba ręcznie skonfigurować odpowiednie pliki znajdujące się w katalogu */etc/postfix*.

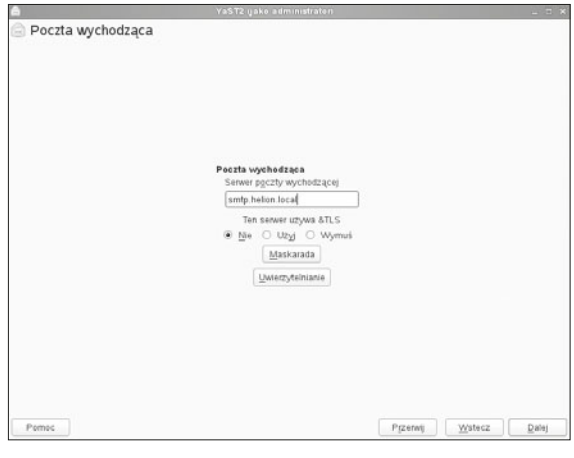
W celu konfiguracji serwera pocztowego należy uruchomić YaST2 i z usług sieciowych wybrać serwer pocztowy. W pierwszym oknie konfiguracji (rysunek 7.127) trzeba określić typ konfiguracji, do wyboru jest prosty i zaawansowany.

Rysunek 7.127. Konfiguracja serwera pocztowego



W kolejnym oknie konfiguracji należy zdefiniować rodzaj połączenia internetowego, natomiast w następnym oknie określić adres serwera poczty wychodzącej (rysunek 7.128).

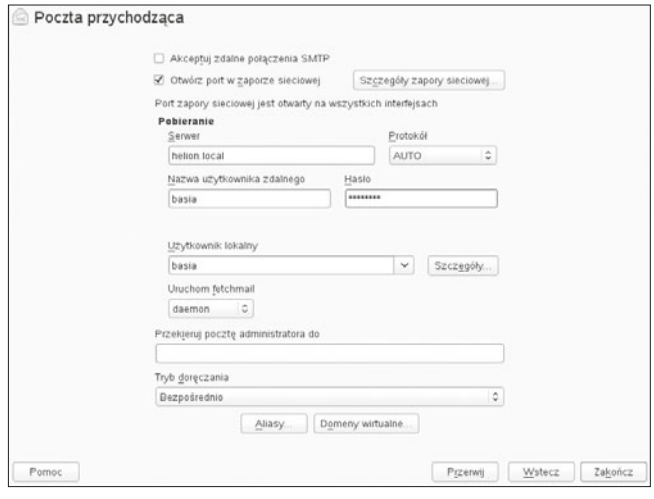
Rysunek 7.128. Poczta wychodząca



Po przejściu do następnego okna konfiguracji poczty przychodzącej (rysunek 7.129) można skonfigurować następujące informacje:

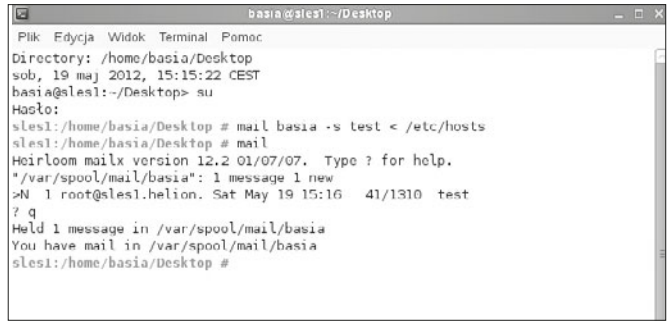
- otwarcie portu w zaporze sieciowej,
- serwer poczty przychodzącej wraz z protokołem,
- nazwę użytkownika zdalnego,
- użytkownika lokalnego,
- przekierowanie e-maili adminstratora.

Rysunek 7.129. Poczta przychodząca



W celu sprawdzenia serwera pocztowego można wysłać e-mail, korzystając z konsoli (rysunek 7.130).

Rysunek 7.130. Testowanie serwera pocztowego



Pocztę można też odbierać, wykorzystując program pocztowy, np. Mutt (rysunek 7.131), który znajduje się w aplikacjach SUSE.

Rysunek 7.131.
Program pocztowy Mutt

Po uruchomieniu klienta pocztowego (rysunek 7.132) dostępna jest konsola, gdzie można skonfigurować konto pocztowe, które umożliwi wysyłanie i odbieranie poczty.

Rysunek 7.132.
Klient pocztowy Mutt

7.11. Wirtualizacja

SLES 11 ma wbudowane wsparcie wirtualizacji przez mechanizm Xen. Dzięki wirtualizacji można zwiększyć efektywność wykorzystywania dostępnych zasobów systemu oraz poprawić jego skalowalność. Na bazie mechanizmu wirtualizacji Xen mogą pracować nie tylko systemy z rodziny UNIX, ale także Microsoft.

Najważniejsze korzyści ze stosowania wirtualizacji to:

- efektywne i optymalne wykorzystanie sprzętu (ang. *efficient hardware utilzation*),
- niezależność od sprzętu (systemy pracujące na maszynach wirtualnych nie muszą mieć sterowników sprzętu maszyny bazowej),
- łatwość migracji maszyn wirtualnych, co znacząco redukuje czasy przestoju (ang. *reduced down time*) przy awariach,
- płynne przydzielanie zasobów sprzętowych — „na żądanie” (ang. *flexible resource allocation*),
- uproszczenie zarządzania zasobami sprzętowymi.

Xen składa się z trzech głównych składowych, którymi są:

- monitor wirtualnej maszyny (*Virtual Machine Monitor*), zwany hypervisorem (*hypervisor*),
- jądro Xen (*Xenkernel*) — zmodyfikowane pod parawirtualizację jądra Linuksa (używane dla Domeny 0 lub Domeny U),
- narzędzia Xen (*Xentools*) — zestaw poleceń konsolowych i graficznych aplikacji stosowanych do zarządzania wirtualnymi maszynami.

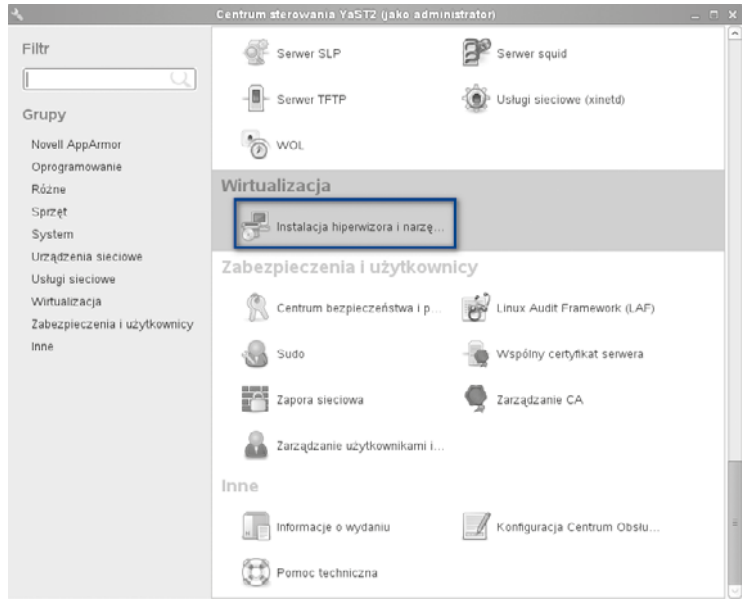
Hypervisor jest ładowany do pamięci podczas uruchamiania systemu poprzez GRUB.

```
title Xen
kernel=/xen.gz
module=/vmlinuz-xen
module=/inird-xen
```

Instalacja Xen

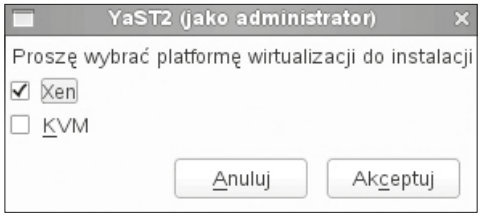
System wirtualizacji Xen można zainstalować przy instalacji systemu operacyjnego — jako jego składową — albo można go doinstalować do systemu wcześniej zainstalowanego.

W tym celu w *Wirtualizacja* wybieramy opcje *Instalacja hiperwizora i narzędzi* oraz *Konfiguracja serwera relokacji* (rysunek 7.133).



Rysunek 7.133. YaST2: Instalacja hyperwizora

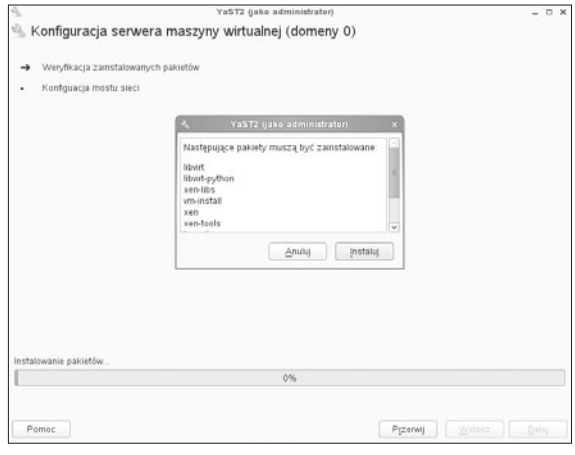
Wyświetla się okno, w którym należy wybrać, którą platformę wirtualizacji chcemy zainstalować (rysunek 7.134).



Rysunek 7.134. Wybór platformy do wirtualizacji

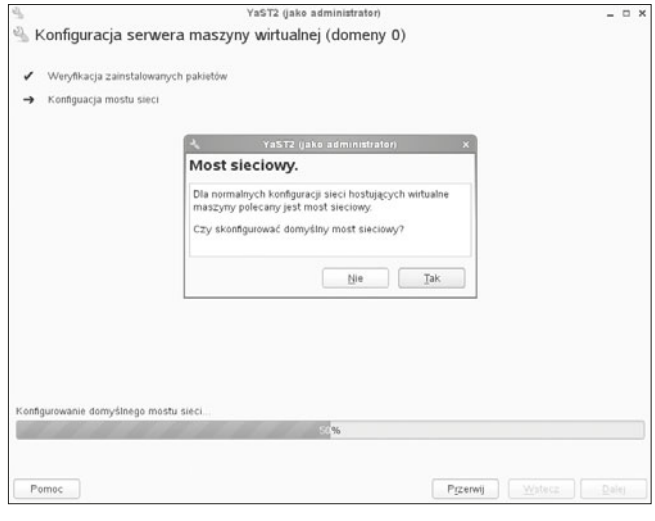
W kolejnym oknie pojawia się informacja o niezbędnych pakietach, które muszą być doinstalowane, aby usługa działała poprawnie (rysunek 7.135). Należy wybrać opcję *Instaluj*.

Rysunek 7.135. Kreator instalacji — wybór usług, które muszą być zainstalowane



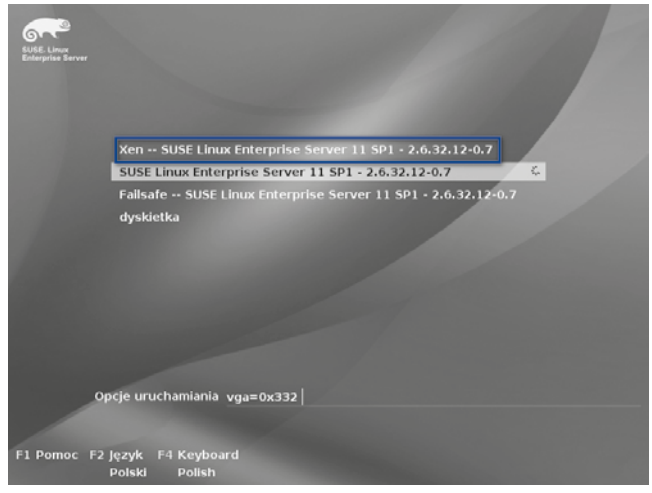
Po zainstalowaniu pakietów następuje pierwsza konfiguracja, w której należy określić interfejs sieciowy. Można w tym miejscu potwierdzić tworzenie mostu sieciowego dla sieci hostujących wirtualne maszyny (rysunek 7.136).

Rysunek 7.136. Konfiguracja mostu sieci



Po zainstalowaniu należy zrestartować system, po czym w menu bootloadera pojawia się dodatkowa opcja Xen (rysunek 7.137).

Rysunek 7.137. Bootloader



WAŻNE

Jeżeli zależy nam na domyślnym uruchamianiu jądra Xen, trzeba zmodyfikować wpis o domyślnej opcji w pliku */boot/grub/menu.lst*:

```
timeout 8
gfxmenu (hd0,1) /boot/message
```

`default 0` uruchamia pierwszą opcję od góry w menu, `default 1` — drugą itd. Należy wpisać numer opcji odpowiadającej Xen.

Tworzenie wirtualnej maszyny

Można to zrobić poleceniem z konsoli:

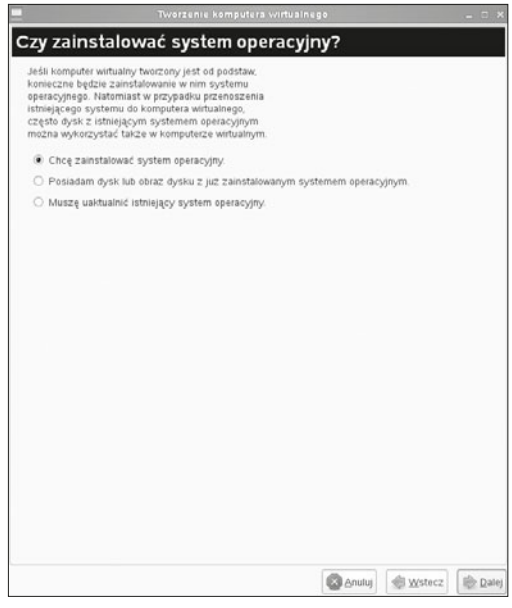
```
vm-install
```

albo narzędziem *YaST2/Wirtualizacja/Tworzenie maszyn wirtualnych* (*YaST2/Virtualization/Create Virtual Machines*).

Kreator tworzenia wirtualnej maszyny prowadzi przez kolejne etapy tworzenia (rysunek 7.138). Należy uważnie czytać sugestie i informacje wyświetlane w kolejnych oknach.

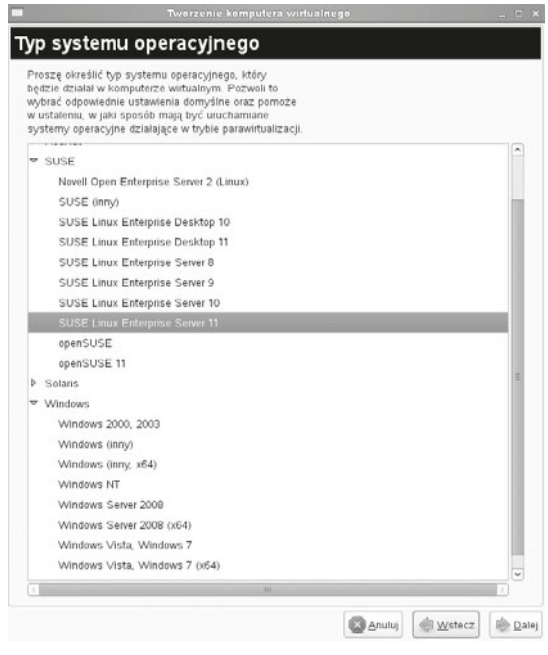
W pierwszym oknie kreatora wyświetla się informacja na temat tego, co będzie się działo w następnych oknach oraz jakie dane będą potrzebne do utworzenia nowej wirtualnej maszyny. W następnym oknie należy wybrać nową instalację lub użycie istniejącego obrazu.

Rysunek 7.138. Tworzenie nowej wirtualnej maszyny



Przy nowej instalacji należy wybrać z listy typ systemu operacyjnego (rysunek 7.139).

Rysunek 7.139. Wybór systemu instalowanego na wirtualnej maszynie



W zależności od wybranego typu systemu operacyjnego pojawiają się sugestie wartości parametrów maszyny wirtualnej, które można modyfikować (rysunek 7.140). Ustawienie *Instalacja systemu operacyjnego* (ang. *Installation operating system*) pozwala na określenie medium, z którego instalujemy system.

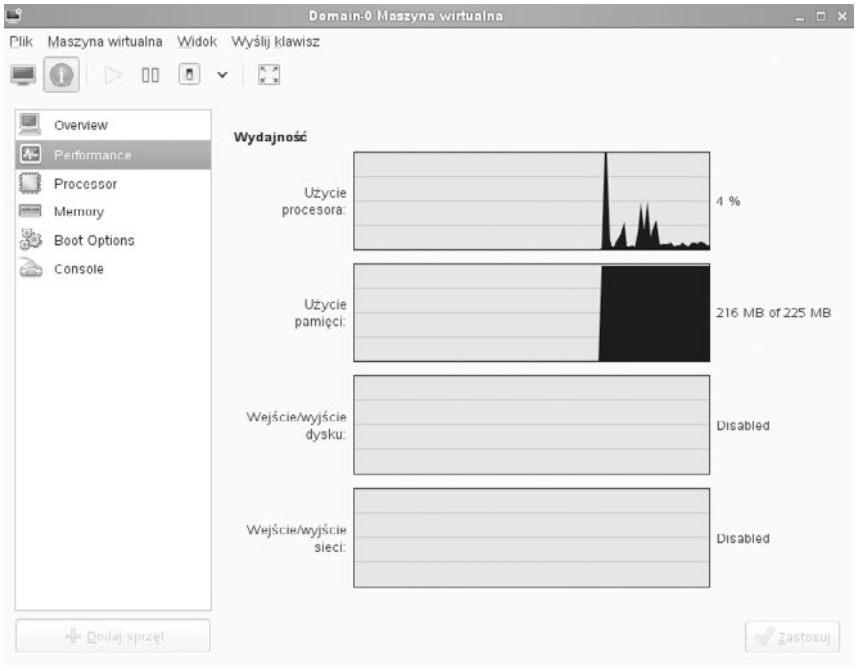
Rysunek 7.140. Podsumowanie ustawień dla wirtualnej maszyny

Przed instalacją należy określić źródło instalacji. W tym celu trzeba kliknąć niebieski napis *Instalacja systemu operacyjnego* i utworzyć wirtualny dysk (rysunek 7.141).

Rysunek 7.141. Tworzenie wirtualnego dysku do instalacji wirtualnej maszyny

Do zarządzania wirtualnymi maszynami służy graficzne narzędzie znajdujące się *YaST2/Wirtualizacja/Menadżer Maszyn Wirtualnych*.

Po kliknięciu prawym przyciskiem wybranej pozycji z listy maszyn wirtualnych można obejrzeć dotyczące jej szczegóły: wydajność, zajętość zasobów. Natomiast w zakładce sprzęt można przejrzeć i zmodyfikować parametry sprzętu maszyny (rysunek 7.142).



Rysunek 7.142. Parametry wirtualnej maszyny

System operacyjny maszyny wirtualnej można „zamrozić" (ang. *suspend*), zatrzymać, zrestartować, uruchomić.

ĆWICZENIA

1. Zainstaluj i skonfiguruj moduł Xen.
2. Stwórz wirtualną maszynę dowolnego systemu operacyjnego.

PYTANIA

1. Omów usługę Xen.
2. Jakim narzędziem tworzy się wirtualne maszyny Xen?

7.12. Skrypty

W systemie Linux skrypty mogą być tworzone w powłoce:

- bash.

Skrypty w systemach Linux mogę być tworzone w dowolnym edytorze, tu wykorzystamy np. edytor vi. Skrypty w Linuksie nie wymagają specjalnego rozszerzenia, tak jak w Windows *.cmd* lub *.bat*. Są również plikami wykonywalnymi, więc wymagają nadania uprawnienia `x`.

Pierwszy skrypt będzie wyświetlał komunikat w konsoli (rysunek 7.143).

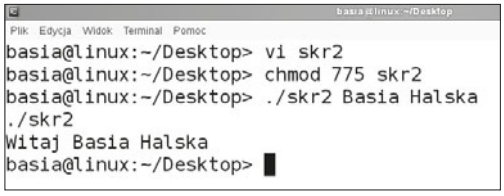
Rysunek 7.143. Skrypt nr 1

Przed uruchomieniem skryptu należy zmienić uprawnienia na 775 dla tego pliku, a następnie wywołać go, podając `./nazwa_skryptu` (rysunek 7.144).

Rysunek 7.144. Uruchamianie skryptu nr 1

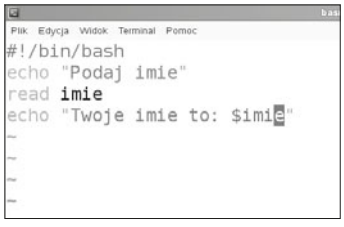
Parametry wywołania obsługuje się w ten sam sposób jak w skryptach windowsowych, czyli od `0` do `9`, przy czym `0` zawsze zwraca nazwę skryptu. W Linuksie, aby odczytać wartość z parametru bądź zmiennej, przed nazwą należy wstawić `$`.

Rysunek 7.145. Skrypt nr 2

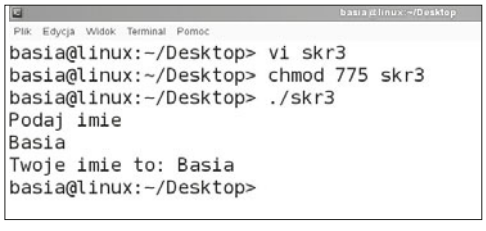


Rysunek 7.146. Uruchomienie skryptu nr 2

Poza parametrami w skryptach możemy również definiować zmienne.



Rysunek 7.147. Skrypt nr 3



Rysunek 7.148. Uruchomienie skryptu nr 3

W skryptach można również korzystać z instrukcji warunkowych.

Instrukcja warunkowa `if...` ma postać:

```
if warunek then
   instrukcja
fi

if warunek then
 instrukcja
else
   instrukcja
fi
if warunek then
   instrukcja
elif
   instrukcja
else
   instrukcja
fi
```

PORÓWNANIA LICZBOWE

- `-gt`: większy od,
- `-lt`: mniejszy od,
- `-ge`: większy od, równy,
- `-le`: mniejszy od, równy,
- `-eq`: równy,
- `-ne`: różny od.

PORÓWNANIA TEKSTOWE

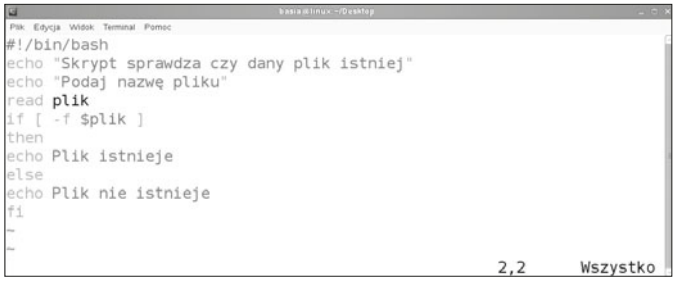
- `-z`: sprawdza, czy ciąg jest pusty,
- `-n`: sprawdza wartość ciągu,
- `=`: równy,
- `!=`: różny,
- `Str`: sprawdza, czy ciąg jest zerowy.

OPERACJE LOGICZNE

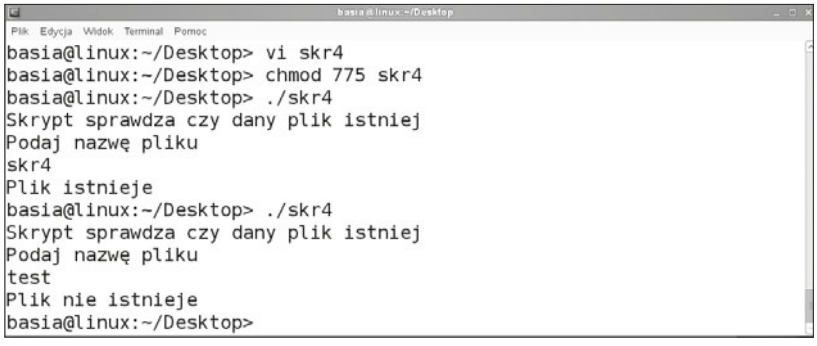
- `-a`: logiczne i (zamiast `-a` można stosować `&&`),
- `-o`: logiczne lub (można stosować też `||`),
- `!`: logiczne nie.

TESTY NA PLIKACH

- `-f`: plik istnieje i jest zwykłym plikiem,
- `-s`: plik nie jest pusty,
- `-r`: plik jest możliwy do odczytu,
- `-w`: plik może być modyfikowany,
- `-x`: plik może być uruchamiany,
- `-d`: jest katalogiem,
- `-h`: jest dowiązaniem symbolicznym,
- `-c`: nazwa odnosi się do urządzenia.



Rysunek 7.149. Skrypt nr 4



Rysunek 7.150. Uruchamianie skryptu nr 4

Pętle

- `while` *`warunek`* `do` *`akcja`* `done` — `while` wykonuje akcję (`akcja`), dopóki warunek (*`warunek`*) ma wartość `prawda` (`true`).
- `until` *`warunek`* `do` *`akcja`* `done` — `until` wykonuje akcję (`akcja`), dopóki warunek (*`warunek`*) ma wartość `fałsz` (`false`).
- `for` *`zmienna`* `in` *`lista-wartości`* `do` *`akcja`* `done` — pętla `for-in` została zaprojektowana do użytku z listami wartości. Są one kolejno przyporządkowywane do zmiennej (*`zmienna`*).
- `for` *`zmienna`* `do` *`akcja`* `done` — odnosi się do argumentów skryptu, przyporządkowując je kolejno do zmiennej (`zmienna`).

Rysunek 7.151. Skrypt nr 5

Rysunek 7.152. Uruchomienie skryptu nr 5

ĆWICZENIA

1. Utwórz wszystkie skrypty omówione w tym rozdziale i sprawdź ich działanie.

PYTANIA

1. Jaki wpis musi być na początku każdego skryptu?
2. W jakiej powłoce można pisać skrypty?
3. Jakie uprawnienia należy nadać dla skryptu, aby był wykonywalny?

7.13. Centralne zarządzanie stacjami roboczymi

7.13.1. SSH

DEFINICJA

SSH (ang. *Secure Shell*) to standard protokołów komunikacyjnych używanych w sieciach komputerowych TCP/IP, w architekturze klient-serwer.

Usługa SSH to następca protokołu Telnet, służąca do terminalowego łączenia się ze zdalnymi komputerami. Transfer wszelkich danych jest zaszyfrowany.

Protokół SSH opiera się na kryptografii klucza publicznego. Do korzystania z SSH są potrzebne dwa klucze: publiczny oraz prywatny. Klucz publiczny jest powszechnie dostępny, klucz prywatny musi być dobrze chroniony. Każda kombinacja klucz prywatny/klucz publiczny jest niepowtarzalna. Klucz prywatny nie jest przesyłany przez sieć. Gdy dane są zaszyfrowane za pomocą klucza publicznego, odszyfrować je można tylko za pomocą klucza prywatnego konkretnego użytkownika.

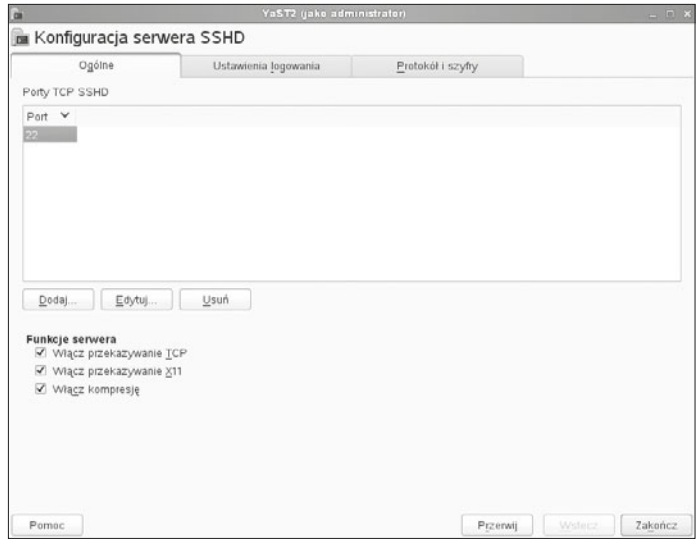
W wersji serwerowej Linuksa ta usługa jest już zainstalowana, natomiast nie jest skonfigurowana ani nawet uruchomiona. Aby przeprowadzić konfigurację, należy w YaST2 spośród usług sieciowych uruchomić konfigurację SSHD (rysunek 7.153).

Rysunek 7.153. Konfiguracja serwera SSHD

W pierwszej zakładce konfiguracji serwera (rysunek 7.154) należy zdefiniować port, na którym będzie pracowała usługa, można również włączyć dodatkowe funkcje serwera:

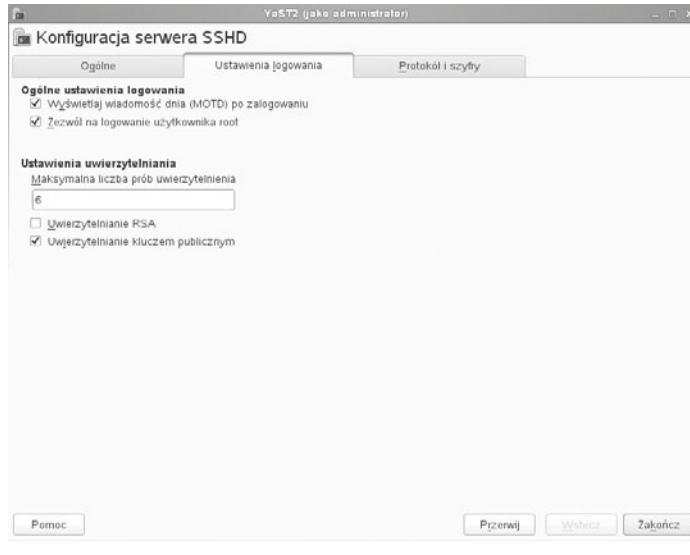
- przekazywanie TCP,
- przekazywanie X11,
- kompresję.

Rysunek 7.154. Konfiguracja portu oraz funkcji serwera



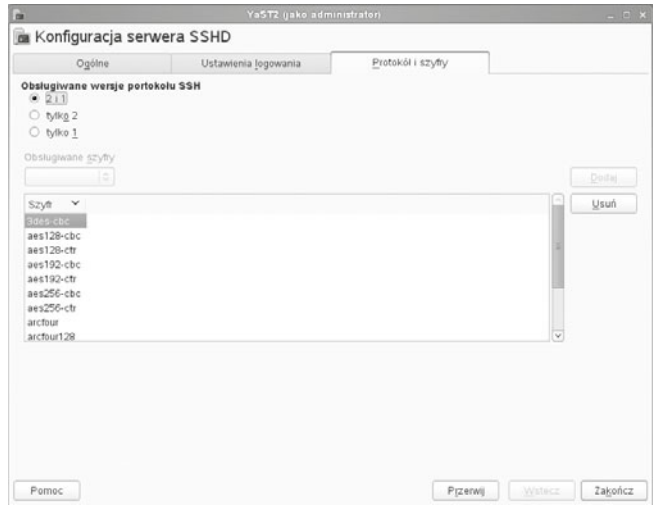
W kolejnej zakładce należy skonfigurować ustawienia logowania (rysunek 7.155). Jednym z nich jest umożliwienie logowania się użytkownika *root*.

Rysunek 7.155. Konfiguracja logowania



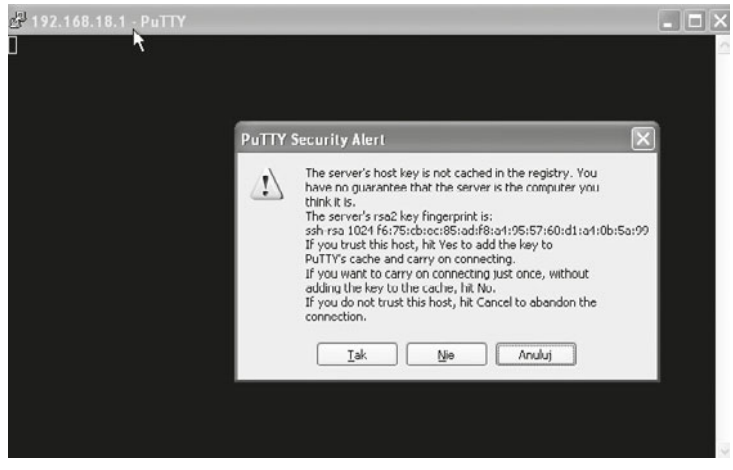
W ostatniej zakładce należy wybrać metodę szyfrowania (rysunek 7.156).

Rysunek 7.156.
Metody szyfrowania



Żeby połączyć się z serwerem z wykorzystaniem SSH, trzeba mieć klienta. Jednym z wielu klientów SSH dla różnych platform systemowych jest program PuTTY, który można pobrać ze strony (*http://www.putty.org/*) (rysunek 7.157).

Rysunek 7.157.
PuTTY



ĆWICZENIA

1. Zainstaluj i skonfiguruj serwer SSH, a następnie zaloguj się do niego z Windowsa.

PYTANIA

1. Omów usługę SSH.
2. Na jakim porcie pracuje usługa SSH?
3. W jaki sposób można się połączyć z serwerem SSH?

7.13.2. VNC

Do połączenia zdalnego służy narzędzie VNC (ang. *Virtual Network Computing*), które umożliwia przekazywanie graficznego obrazu z pulpitu maszyny odległej, do której się połączymy.

Serwer VNC jest składową usług sieciowych. W celu jego konfiguracji należy uruchomić narzędzie *Administracja zdalna (VNC)* (rysunek 7.158).

Rysunek 7.158. Administracja zdalna

W oknie konfiguracji należy uruchomić serwer zdalnej administracji oraz otworzyć port w zaporze sieciowej (rysunek 7.159). Po zakończeniu usługa zostanie uruchomiona.

Rysunek 7.159. Uruchamianie zdalnej administracji

ĆWICZENIA

1. Skonfiguruj połączenie z usługą VNC.

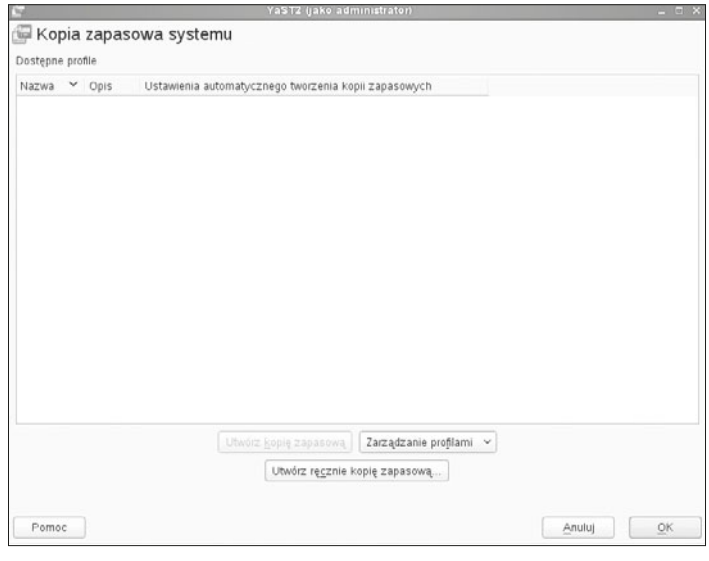
PYTANIA

1. Omów usługę VNC.
2. Do czego służy usługa VNC?
3. Za pomocą jakich programów można połączyć się z serwerem VNC?

7.14. Kopia zapasowa

Większość systemów operacyjnych dysponuje narzędziami służącymi do tworzenia kopii zapasowej. W SLES to narzędzie znajduje się w YaST2 (rysunek 7.160). *Kopia zapasowa systemu* umożliwia generowanie kopii na podstawie określonego wcześniej profilu. Jeżeli go nie ma, to w tym miejscu można go stworzyć lub też ręcznie wykonać kopię zapasową.

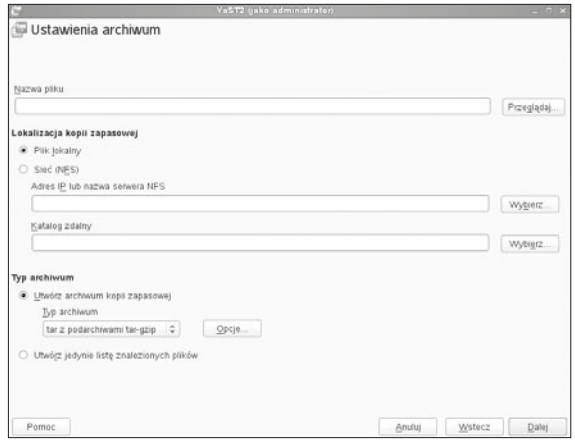
Rysunek 7.160. Kopia zapasowa



Aby ręcznie wykonać kopię zapasową, w następnym oknie (rysunek 7.161) należy:

- nadać nazwę dla pliku, pamiętając o podaniu pełnej ścieżki, np. */tmp/kopia.tar*,
- określić miejsce przechowywania pliku jako plik lokalny bądź serwer sieciowy NFS oraz wybrać typ archiwum.

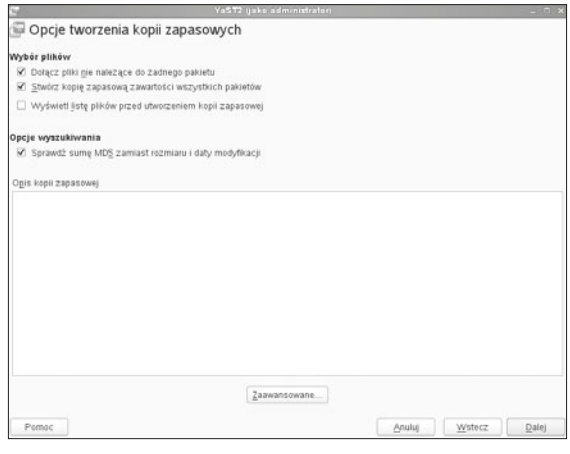
Rysunek 7.161.
Ustawienia archiwum



W kolejnym oknie kreatora (rysunek 7.162) można określić wybór plików do archiwum:

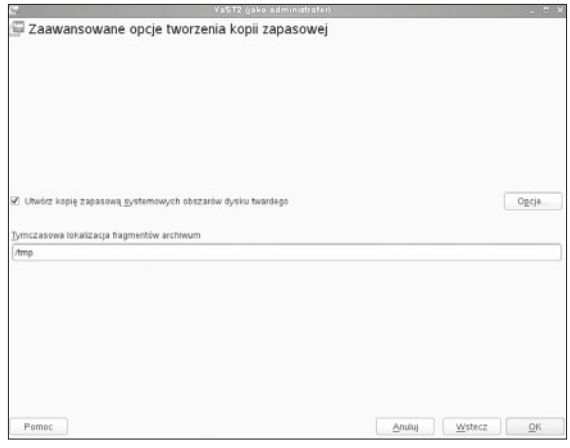
- *Dołącz pliki nie należące do żadnego pakietu* — zostaną dołączone pliki, które nie należą do żadnego z zainstalowanych pakietów.
- *Stwórz kopię zapasową zawartości wszystkich pakietów*.
- *Wyświetl listę plików przed utworzeniem kopii zapasowej* — bardzo przydatna opcja, która umożliwia wyświetlenie listy dołączanych plików przed zrobieniem kopii.
- *Sprawdź sumę MD5 zamiast rozmiaru i daty modyfikacji* — umożliwia wyszukiwanie zmienionych plików po analizie sumy kontrolnej.

Rysunek 7.162.
Opcje tworzenia kopii zapasowej



W ramach zaawansowanej konfiguracji (rysunek 7.163) można ustalić dodatkowe opcje dla tworzenia kopii, takie jak określenie lokalizacji pliku oraz możliwość utworzenia kopii zapasowej systemowych obszarów dysku twardego.

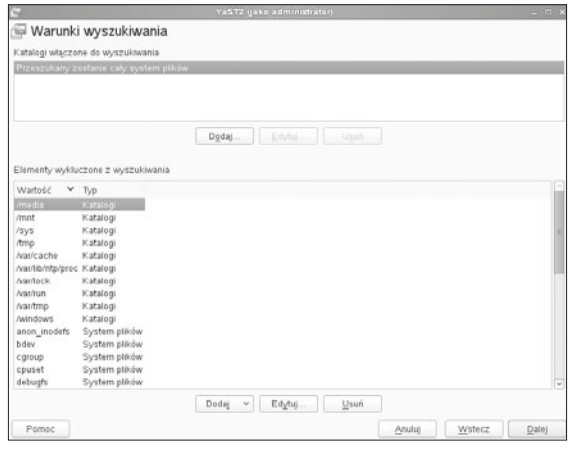
Rysunek 7.163. Zaawansowane opcje tworzenia kopii zapasowej



W kolejnym kroku (rysunek 7.164) jest wymagane określenie zasobów, które zostaną pominięte podczas tworzenia kopii, może być zdefiniowany w dwóch formach:

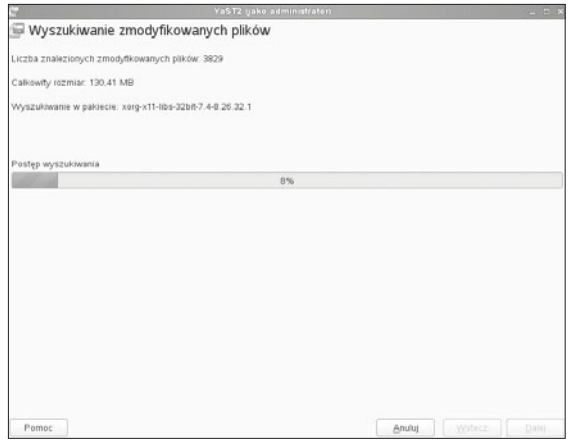
- *Katalog* — specyfikuje bezwzględnie ścieżkę do katalogu w systemie plików.
- *System plików* — określa rodzaje systemu plików.

Rysunek 7.164. Określenie warunków przeszukiwania



Po określeniu elementów, które zostaną pominięte podczas przeszukiwania zawartości dysku, i po przejściu *Dalej* rozpoczyna się proces gromadzenia informacji na temat plików, jakie mają wejść w skład kopii (rysunek 7.165).

Rysunek 7.165. Odczytywanie pakietów włączanych do tworzonej kopii



ĆWICZENIA

1. Wykonaj kopię zapasową plików znajdujących się w Twoim katalogu domowym.

PYTANIA

1. Do czego służy narzędzie *kopia zapasowa systemu*?
2. Czy możemy zrobić kopię zapasową pojedynczych plików?

8

Konfigurowanie urządzeń sieciowych

Zasady konfigurowania urządzeń sieciowych są podobne w przypadku wielu producentów oferujących sprzęt do zastosowań domowych i małego biznesu (ang. SOHO — *Small Office Home Office*) — zmiana parametrów konfiguracyjnych zazwyczaj odbywa się poprzez przeglądarkę WWW po uruchomieniu adresu wybranego urządzenia.

W zależności od producenta domyślny adres może być różny, przy czym zawsze jest to adres prywatny.

Domyślnie dostęp do konfiguracji urządzeń sieciowych przez przeglądarkę jest zabezpieczony przy użyciu loginu oraz hasła — każdy z producentów używa własnych loginów i haseł niezbędnych do konfiguracji. Są one dostarczane wraz z urządzeniem.

Konfiguracja poprzez przeglądarkę WWW pozwala na łatwą i intuicyjną pracę w trybie graficznym, gdzie najczęściej jest dostępny również system pomocy kontekstowej przydatny dla użytkowników.

Konfigurację urządzeń sieciowych w podręczniku zaprezentowano na przykładzie urządzeń firmy D-Link. Wybór ten został podyktowany popularnością tych urządzeń w zastosowaniach domowych.

Dodatkowo w celu zapoznania czytelników z konfiguracją urządzeń do zastosowań bardziej komercyjnych przedstawiono konfigurację urządzeń sieciowych firmy Cisco — lidera na rynku zastosowań biznesowych.

8.1. Konfigurowanie urządzeń sieciowych przez przeglądarkę WWW

W dalszej części rozdziału, jako przykład, został użyty router D-Link DIR-665.

Aby rozpocząć konfigurację urządzenia sieciowego poprzez przeglądarkę (w naszym przypadku użyty został router D-Link DIR-665), należy sprawdzić przypisany mu adres

IP. Przy zakupie nowych urządzeń wraz z dokumentacją są dostarczane: domyślny adres IP urządzenia oraz domyślny login i hasło. W przypadku gdy urządzenie było wcześniej konfigurowane i dane te zostały zmienione, istnieje możliwość przywrócenia fabrycznych ustawień poprzez przytrzymanie przycisku *reset* znajdującego się na obudowie urządzenia.

W przypadku urządzeń firmy D-Link urządzeniom sieciowym jest fabrycznie przypisywany adres *192.168.1.1* lub *192.168.0.1*, login użytkownika to *Admin*, hasło użytkownika *Admin*.

Aby rozpocząć konfigurację urządzenia, należy podłączyć kabel sieciowy do portu w komputerze oraz do portu w urządzeniu (w przypadku gdy urządzenie posiada porty zarówno LAN, jak i WAN, kabel wpinamy do jednego z portów LAN).

UWAGA

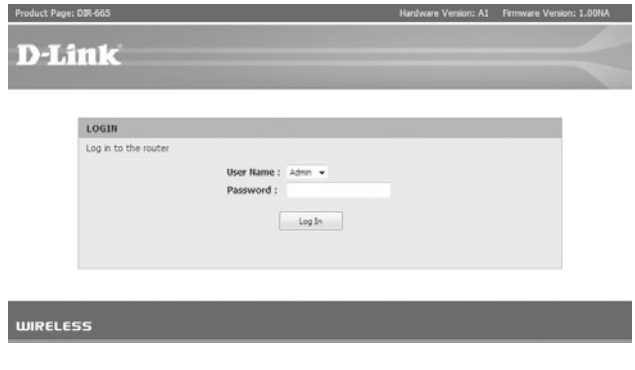
W przypadku urządzeń bezprzewodowych czasem istnieje możliwość podłączenia się do domyślnej sieci bezprzewodowej, co pozwala na konfigurację bez konieczności używania kabli.

Jeśli urządzenie ma skonfigurowany serwer DHCP nadający adresy IP, wówczas do komputera zostaje przypisany adres z właściwej sieci (o ile system operacyjny jest skonfigurowany do automatycznego pobierania adresu IP). Jeżeli urządzenie sieciowe nie ma możliwości nadania adresu IP dla komputera, wówczas należy skonfigurować adres IP karty sieciowej, aby znajdował się on we właściwej sieci. Dla domyślnego adresu urządzeń firmy D-Link przykładowe parametry konfiguracji protokołu IP wyglądają następująco:

Adres IP:	192.168.1.100
Maska podsieci:	255.255.255.0
Brama domyślna:	192.168.1.1

Po właściwej konfiguracji użytkownik może uruchomić dowolną przeglądarkę internetową i przejść do konfiguracji urządzenia poprzez wpisanie w pasku adresu przeglądarki adresu IP urządzenia sieciowego.

W naszym przypadku pojawi się monit o login i hasło użytkownika, widoczny na rysunku 8.1.



Rysunek 8.1. Logowanie do routera DIR-665

Po poprawnej weryfikacji nazwy użytkownika i hasła użytkownik jest przenoszony na właściwą stronę konfiguracji. Poszczególne parametry konfiguracyjne specyficzne dla urządzeń danego typu zostały omówione w dalszej części podręcznika.

8.2. Konfigurowanie urządzeń sieciowych firmy Cisco

Urządzenia sieciowe Cisco pracują pod kontrolą systemu operacyjnego IOS (ang. *Internetwork Operating System*), który działa w trybie tekstowym, obsługa jest więc podobna do obsługi wiersza poleceń systemu Windows bądź powłoki systemu Linux. Istnieje również możliwość uruchomienia konfiguracji poprzez stronę WWW, niemniej jednak zaawansowani użytkownicy preferują konfigurację w trybie tekstowym, która pozwala na szybsze wprowadzanie zmian.

Dostęp do konfiguracji urządzeń firmy Cisco może odbywać się przez protokół telnet lub SSH (w zależności od konfiguracji urządzenia), jednak podstawowym sposobem zmiany ustawień jest podłączenie komputera bezpośrednio do urządzenia sieciowego przez specjalny port konsolowy w urządzeniu (ang. *console*), do którego podłącza się kabel typu roll-over (zwany także kablem konsolowym lub kablem null modem). Oryginalny kabel firmy Cisco (zazwyczaj dołączony do sprzętu) dostarczany razem z zakupionym sprzętem jest płaski, z jednej strony zakończony wtykiem RJ-45, z drugiej wtykiem żeńskim DB9, i ma kolor jasnoniebieski.

Konfiguracja poprzez port konsolowy wymaga podłączenia kabla do portu szeregowego w komputerze oraz skonfigurowania oprogramowania typu emulator terminala, które pozwala na bezpośrednią komunikację poprzez port szeregowy (np. Putty — *www.putty.org*).

Domyślne parametry dostępu poprzez port konsoli dla urządzeń Cisco:

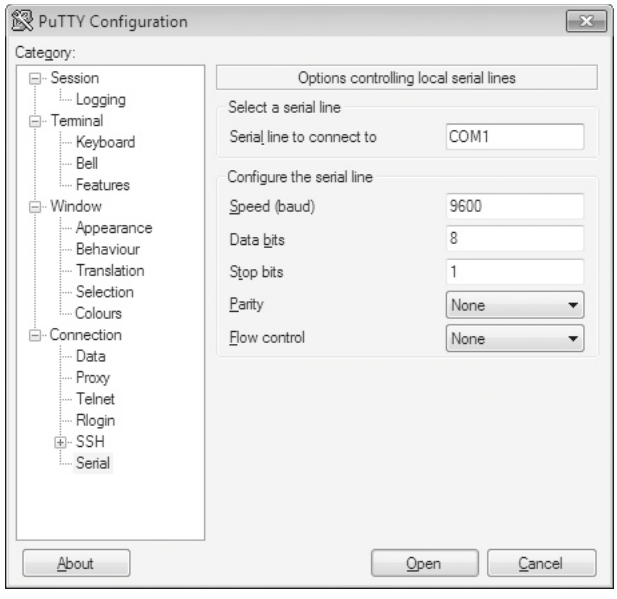
- prędkość: 9600,
- 8 bitów danych,
- bez parzystości,
- 1 bit stopu,
- kontrola przepływu: brak.

Konfiguracja programu Putty do komunikacji poprzez port szeregowy z portem konsoli urządzenia Cisco została przedstawiona na rysunku 8.2.

Domyślnie dostęp poprzez port konsolowy nie jest zabezpieczony hasłem — można je ustawić w konfiguracji urządzenia.

UWAGA

Połączenie przez port konsolowy jest realizowane bezpośrednio przez port szeregowy, tak więc nie wymaga konfiguracji protokołu IP na komputerze użytkownika.



Rysunek 8.2. Konfiguracja programu Putty do komunikacji z urządzeniami Cisco

Po poprawnym skonfigurowaniu połączenia konsolowego i uruchomieniu routera w oknie emulatora terminala można obserwować komunikaty przekazywane przez proces uruchamiania urządzenia (rysunek 8.2).

```
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
########################################################################
## [OK]
              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software — Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
Image text-base: 0x60080608, data-base: 0x6270CD50
```

Po uruchomieniu routera urządzenie zgłasza się w trybie użytkownika, na co wskazuje znak > po nazwie urządzenia, np.:

```
Router>
```

Tryb użytkownika (ang. *user exec mode*) pozwala tylko oglądać niektóre statystyki routera, bez możliwości zmian konfiguracji. Aby wprowadzić zmiany w ustawieniach urządzenia, należy zmienić tryb pracy na tryb uprzywilejowany (ang. *privileged exec mode*) komendą `enable`. Jeśli zostało skonfigurowane zabezpieczenie hasłem, wówczas użytkownik zostanie poproszony o podanie hasła dostępu, po czym urządzenie zmieni znak zachęty na #, np.:

```
Router#
```

Konfiguracja urządzenia jest dostępna po wejściu w tryb konfiguracji, co z poziomu połączenia konsolowego jest możliwe poprzez komendę `configure terminal`. Wykonanie komendy powoduje zmianę zgłoszenia routera:

```
Router (config)#
```

Wyjście z trybu konfiguracji jest możliwe poprzez kombinację *Ctrl+Z* lub przy użyciu komendy `exit`.

Tryb konfiguracji pozwala na ustawienie ogólnych parametrów urządzenia, takich jak jego nazwa, data, czas czy hasła dostępu. Konfiguracja poszczególnych interfejsów sieciowych odbywa się po wejściu w tryb konfiguracji wybranego interfejsu poprzez komendę `interface` *`nazwa_portu`*, np. `interface FastEthernet 0/0`, co zmienia zgłoszenie routera na:

```
Router (config-if)#
```

UWAGA

Urządzenia firmy Cisco pozwalają na testowanie konfiguracji bez ich zapisywania — zmiany w ustawieniach następują w momencie zaakceptowania polecenia klawiszem *Enter*, jednak zapisanie ich na stałe wymaga wprowadzenia dodatkowej komendy:

```
copy running-config startup-config
```

która zapisze bieżącą konfigurację (`running-config`) w miejsce konfiguracji startowej uruchamianej po włączeniu urządzenia (`startup-config`).

Aby zmienić nazwę urządzenia, która pojawia się po zalogowaniu, należy w trybie uprzywilejowanym wykonać następujące komendy:

```
Router# configure terminal
Router(config)# hostname Urzadzenie1
Urzadzenie1(config)#exit
```

W celu wprowadzenia hasła dostępu dla trybu uprzywilejowanego:

```
Router# configure terminal
Router(config)# enable password haslo
Router(config)# exit
```

Komenda `enable password haslo` ustawia hasło dostępu do trybu uprzywilejowanego, przy czym hasło to jest zapisane w pliku konfiguracyjnym tekstem niezaszyfrowanym. Aby zapisać w pliku konfiguracyjnym hasło zaszyfrowane, należy użyć komendy `enable secret haslo`.

Do ustawienia hasła dostępu dla połączenia konsolowego służą następujące komendy:

```
Router# configure terminal
Router(config)# line console 0
Router(config-line)# password haslo
Router(config-line)# login
Router(config-line)# exit
Router(config)# exit
```

Komenda `line console 0` powoduje przejście w tryb konfiguracji połączenia konsoli, komenda `password haslo` ustawia hasło wymagane do zalogowania na `haslo`, komenda `login` powoduje włączenie autoryzacji po podłączeniu przez konsolę.

Konfiguracja zabezpieczenia hasłem dla połączeń telnet jest przeprowadzana w taki sam sposób, przy czym konsole telnet w systemie IOS są oznaczane nazwą VTY. Tak więc w powyższym przykładzie należy linię `line console 0` zastąpić przez `line vty 0 5`, gdzie druga liczba wskazuje na liczbę jednoczesnych połączeń do konsoli telnet (najnowsze wersje oprogramowania pozwalają na obsługę równocześnie 15 połączeń; wówczas należy użyć komendy `line vty 0 15`).

8.3. Konfiguracja przełącznika

Głównym zadaniem przełącznika jest dzielenie sieci na segmenty w 2. warstwie modelu OSI na podstawie adresu MAC podłączonych urządzeń. Zaletą przełączników (w porównaniu z koncentratorami) jest podział sieci na domeny kolizyjne. Więcej informacji na ten temat można znaleźć w podrozdziale 5.3.

Podział przełączników pod względem ich funkcjonalności wygląda następująco:

- Przełączniki niezarządzalne — proste urządzenia typu włącz i używaj, które nie oferują użytkownikowi zaawansowanych funkcji, pełnią podstawową funkcję przełączania ramek. Są to urządzenia najczęściej używane w niewielkich sieciach, gdzie bezpieczeństwo i wydajność nie są kluczowe.
- Przełączniki zarządzalne — urządzania zaawansowane, pozwalające na zwiększenie bezpieczeństwa oraz wydajności sieci. Urządzenie tego typu umożliwia zmianę wielu parametrów przełączania, co pozwala łatwo rozbudowywać sieci i zarządzać nimi.
- Przełączniki warstwy trzeciej — to urządzenia, które oprócz przełączania na podstawie adresów MAC dodatkowo przełączają transmisje w oparciu o adres IP. Działanie

przełącznika warstwy trzeciej jest podobne do działania routera wyposażonego jedynie w porty Ethernet, przy czym przełącznik ze względu na architekturę sprzętową wykorzystującą układy ASIC (ang. *Application Specific Integrated Circuits*) działa szybciej. Dodatkowo przełączniki nie obsługują interfejsów innego typu oraz nie oferują wielu funkcji routera (np. NAT).

8.3.1. Parametry konfiguracyjne przełączników zarządzalnych

Przełączniki do zastosowań domowych i małego biznesu najczęściej są urządzeniami, które nie są zarządzalne, czyli nie mają możliwości konfiguracji. W zastosowaniach komercyjnych są używane urządzenia zarządzalne, które pozwalają zachować wyższy poziom bezpieczeństwa, a także dają możliwość wpływania na ruch sieciowy. Funkcje, które mogą być konfigurowane w zaawansowanych przełącznikach, to m.in.:

- *Protokół STP* (ang. *Spanning Tree Protocol*) — protokół zatwierdzony w dokumencie IEEE 802.1d pozwalający na kontrolę połączeń pomiędzy przełącznikami — jeśli między nimi występują zwielokrotnione połączenia, są one blokowane i uruchamiane jedynie w przypadku wystąpienia awarii połączenia podstawowego. W sieci wykorzystującej protokół STP istnieje główny przełącznik zarządzający, w którym są ustawiane łącza redundantne (zapasowe) w celu zachowania ciągłości pracy na wypadek awarii jednego z nich. Łącza zapasowe są blokowane przez protokół STP i uruchamiane jedynie w przypadku awarii. Istnieją modyfikacje protokołu: *RSTP* (ang. *Rapid Spanning Tree Protocol*) opisany w dokumencie IEEE 802.1w, pozwalający na szybsze wznowienie prawidłowej pracy sieci, oraz *MSTP* (ang. *Multiple Spanning Tree Protocol*) opisany w dokumencie IEEE 802.1s, który umożliwia równoważenie obciążenia pomiędzy przełącznikami i zapewnia równocześnie wiele ścieżek transmisji.
- *Protokół SNMP* (ang. *Simple Network Management Protocol*), opisany w dokumencie RFC 1157, to uniwersalny protokół służący do zarządzania urządzeniami sieciowymi i monitorowania ich. Działanie protokołu polega na rozsyłaniu zapytań przez oprogramowanie nadrzędne (ang. *manager*) do agentów SNMP pracujących na urządzeniach sieciowych w celu zdobycia informacji o ich aktualnym stanie. Dane te są gromadzone w bazie MIB (ang. *Management Information Base*). Przełączniki dodatkowo mogą zostać skonfigurowane tak, aby wysyłać informacje w przypadku określonych zdarzeń sieciowych, takich jak awaria łącza czy niewłaściwa próba połączenia.
- *Port Mirroring* funkcja pozwalająca na przesyłanie danych z wybranego portu lub wybranej sieci VLAN równocześnie do innego portu — tworzy się kopia przechodzących przez urządzenie danych (ten jeden port działa tak, jak całe urządzenie „poprzedniej generacji", czyli koncentrator, ruch jest powielany, a nie przekazywany pomiędzy wybranymi portami). Operacja taka daje możliwość monitorowania ruchu na wybranym segmencie sieci, na wybranym porcie lub na wybranej sieci VLAN. W przypadku urządzeń firmy Cisco funkcja ta nosi nazwę SPAN (ang. *Switched Port Analyzer*) lub RAP (ang. *Roving Analysis Port*) w przypadku urządzeń firmy 3Com.

- *QoS* (ang. *Quality of Service*) — usługa pozwalająca na kształtowanie ruchu w celu poprawienia jakości usług transmisji danych. Usługa QoS umożliwia ustawienie priorytetów dla wybranego typu ruchu sieciowego w celu zapewnienia jak najlepszej jakości dostarczanych usług (np. ruch VoIP powinien mieć wyższy priorytet przy transmisji niż inne przesyłane dane, przykładowo pliki pobierane protokołem FTP). Poziomy priorytetu ruchu opisane w dokumencie 802.1p zostały przedstawione w tabeli 8.1.

Tabela 8.1. Priorytety ruchu zdefiniowane w dokumencie IEEE 802.1p

Priorytet ruchu	Znaczenie	Rekomendowane zastosowanie
7	*Network Control*	Ruch krytyczny dla zarządzania siecią i jej działania
6	*Voice*	Aplikacje wrażliwe na opóźnienia, np. VoIP — opóźnienia mniejsze niż 10 ms
5	*Video*	Aplikacje wrażliwe na opóźnienia, np. telewizja interaktywna — opóźnienia mniejsze niż 100 ms
4	*Controlled Load*	Aplikacje wykorzystujące z góry określone pasmo, np. transmisje strumieniowe
3	*Excellent Effort*	Aplikacje transmitujące ważne dane
2	*Spare*	Ruch mało istotny
1	*Background*	Ruch masowy
0	*Best Effort*	Priorytet domyślny, gdy nie są ustawione inne wartości

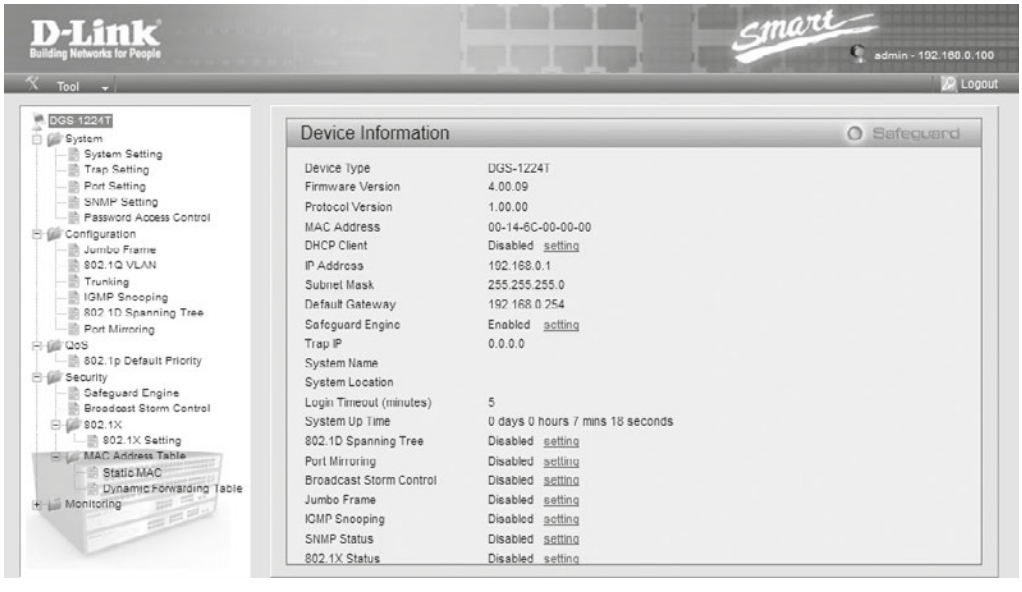
- *Zarządzanie pasmem* (ang. *bandwith control*) — usługa pozwalająca ograniczyć przepustowość na wybranym porcie.
- *Sieci wirtualne* (ang. *Virtual Local Area Network* — *VLAN*) — opisany w dokumencie IEEE 802.1Q standard pozwalający na podział urządzeń podłączonych do jednej fizycznej sieci na niezależne sieci logiczne. Komunikację pomiędzy sieciami VLAN zapewnia router. Przynależność urządzeń sieciowych do konkretnej sieci wirtualnej może być określana zarówno na podstawie portu przełącznika, do którego jest podłączone dane urządzenie, jak i na podstawie adresu MAC karty sieciowej tego urządzenia.
- *Agregacja łączy* (ang. *link agregation*) — usługa umożliwiająca łączenie przełączników równocześnie kilkoma połączeniami, co pozwala na utworzenie za pomocą wielu fizycznych połączeń jednego połączenia logicznego (wirtualnego kanału) charakteryzującego się większą przepustowością oraz większą niezawodnością.
- *Połączenie trunk* — zaawansowane urządzenia sieciowe pozwalają również na znakowanie identyfikatorem sieci VLAN ramek przesyłanych pomiędzy przełącznikami, co umożliwia transmisję jednym łączem ramek z wielu sieci wirtualnych. Specjalny znacznik (ang. *tag*) dodawany do ramki pozwala rozpoznać sieć VLAN, do której dana ramka powinna zostać skierowana.

8.3.2. Konfiguracja podstawowa

Konfiguracja urządzenia sieciowego została przedstawiona na przykładzie modelu z serii DGS-1200 firmy D-Link. Jest to urządzenie przeznaczone do budowy małych, zarządzanych sieci komputerowych. W zależności od modelu może być wyposażone w 16, 24 lub 48 portów.

Panel konfiguracji urządzenia jest dostępny poprzez stronę WWW domyślnie pod adresem *192.168.0.1*. Po jego uruchomieniu użytkownik zostanie zapytany o hasło dostępu — domyślnie *Admin*.

Po lewej stronie panelu konfiguracyjnego znajduje się menu wyboru określonych parametrów konfiguracyjnych. Po wybraniu jednego z nich w głównej części okna pojawia się formularz pozwalający na zmianę oraz zapis ustawień (rysunek 8.3).



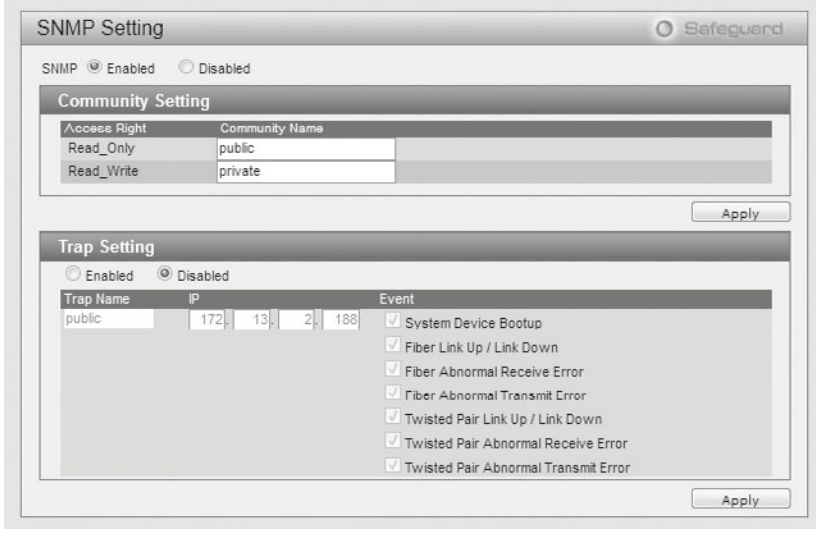
Rysunek 8.3. Panel konfiguracyjny przełącznika z serii DGS-1200

Konfiguracja podstawowych parametrów urządzenia jest dostępna w menu *System/System Setting*. Pozwala ono na ustawienie adresu IP, pod którym będzie dostępny panel konfiguracji urządzenia (adres statyczny lub automatyczne pobieranie adresu z serwera DHCP). Dodatkowo w panelu konfiguracji istnieje możliwość przypisania nazwy urządzenia wraz z opisem lokalizacji, co w przypadku rozbudowanych sieci pozwala administratorowi na łatwiejsze zarządzanie urządzeniami sieciowymi.

Włączanie oraz ustawianie prędkości działania poszczególnych interfejsów sieciowych jest możliwe w menu *System/Port Setting*.

8.3.3. Konfiguracja protokołu SNMP

Parametry konfiguracyjne protokołu SNMP są dostępne w menu *System/SNMP Setting* (rysunek 8.4).



Rysunek 8.4. Konfiguracja protokołu SNMP

Protokół SNMP w celu komunikacji z użytkownikami wymaga uwierzytelnienia, do którego są wykorzystywane wcześniej skonfigurowane hasła dostępu pozwalające na odczyt (tzw. *public_community*) oraz odczyt i zapis (*private_community*). Hasła te należy wprowadzić w polach *Read_Only* (dla odczytu) oraz *Read_Write* (dla odczytu i zapisu).

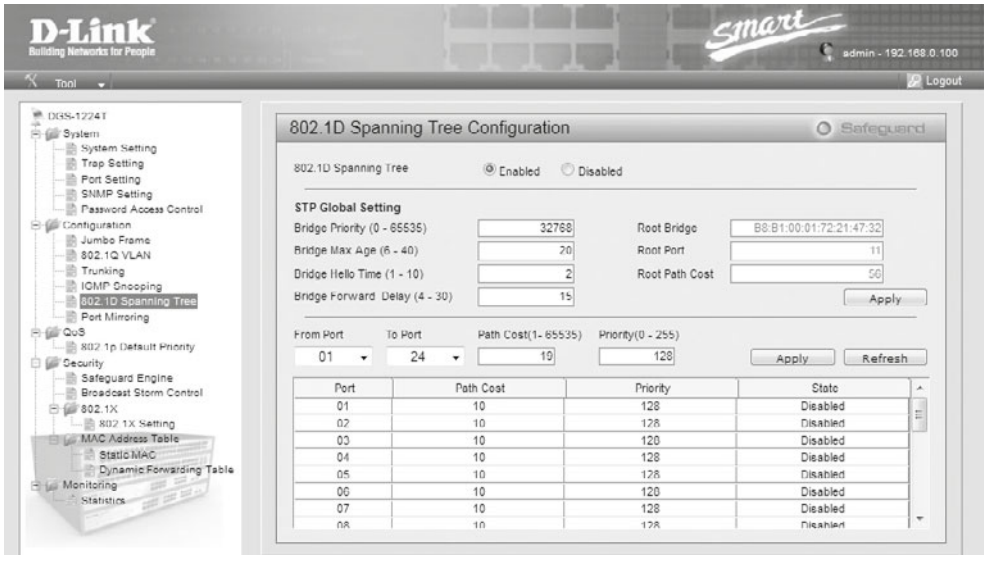
Ustawienia *Trap Setting* pozwalają na automatyczny zapis informacji o danym zdarzeniu, które wystąpiło w urządzeniu, do serwera SMTP (określa się go poprzez podanie jego adresu IP). Zdarzenia, które mogą być zapisywane, to:

- *System Device Bootup* (restart urządzenia);
- *Fiber Link Up/Link Down* (włączenie/wyłączenie portu światłowodowego, jeśli występuje);
- *Fiber Abnormal Receive Error* (błąd odbioru danych przez port światłowodowy, jeśli występuje);
- *Fiber Abnormal Transmit Error* (błąd wysyłki danych przez port światłowodowy, jeśli występuje);
- *Twisted Pair Link Up/Link Down* (włączenie/wyłączenie portu RJ-45);
- *Twisted Pair Abnormal Receive Error* (błąd odbioru danych przez port RJ-45);
- *Twisted Pair Abnormal Transmit Error* (błąd wysyłki danych przez port RJ-45).

Oprogramowanie pozwala użytkownikowi wybrać poszczególne typy zdarzeń poprzez zaznaczenie odpowiednich pól na formularzu.

8.3.4. Konfiguracja protokołu STP

Konfiguracja protokołu STP jest dostępna w menu *Configuration/802.1D Spanning Tree* (rysunek 8.5).



Rysunek 8.5. Konfiguracja protokołu STP

W przełącznikach protokół STP jest domyślnie wyłączony, aby nie obciążać dodatkowo sieci własnymi komunikatami (BPDU — *Bridge Protocol Data Unit*). W celu jego uruchomienia w oknie konfiguracji należy zmienić stan protokołu na włączony (ang. *Enabled*). Dodatkowo panel konfiguracyjny pozwala na zmianę następujących parametrów protokołu STP:

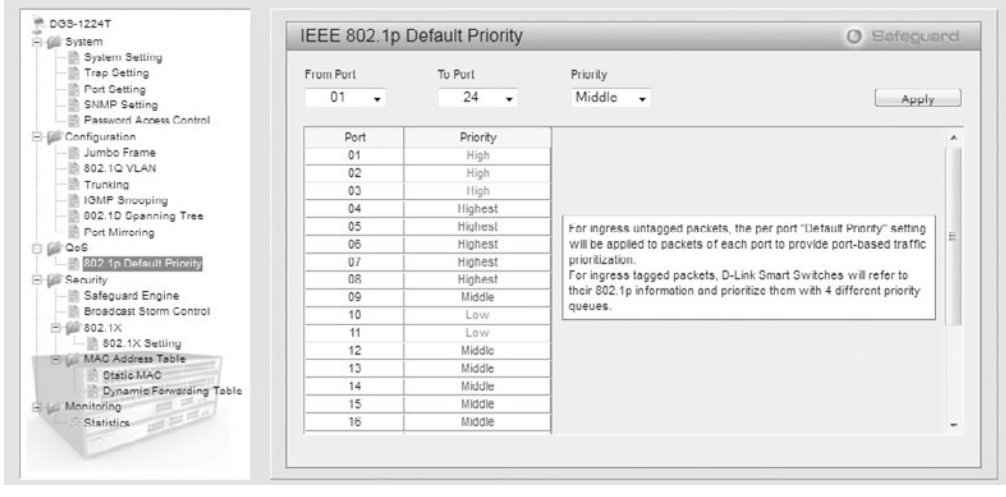
- *Bridge Priority* — priorytet urządzenia — to wartość z zakresu 0 – 65535 określająca priorytet przekazywanych ramek.
- *Bridge Max Age* — maksymalny czas życia komunikatów BPDU — to wartość pozwalająca ustawić maksymalny czas krążenia w sieci komunikatów protokołu BPDU w celu zabezpieczenia przed krążeniem danych w sieci w nieskończoność.
- *Bridge Hello Time* — czas pomiędzy wysyłaniem kolejnych komunikatów informujących, że urządzenie pracuje poprawnie.
- *Bridge Forward Delay* — maksymalny czas pomiędzy zmianami statusu łącza.

Dodatkowo istnieje możliwość ustawienia priorytetów oraz kosztów transmisji przez wybrany port, co pozwala na określenie, które z wielu łączy w danym momencie będzie wykorzystywane do transmisji. Im niższy koszt transmisji (ang. *path cost*) oraz priorytet (ang. *priority*), tym większe szanse, że port zostanie wybrany do przekazywania danych przez algorytm protokołu STP.

8.3.5. Konfiguracja QoS

Wybrany przełącznik w swojej konfiguracji oferuje jedynie proste zarządzanie jakością usług pozwalającą na określenie priorytetów transmisji dla każdego z portów. Standard IEEE 802.1p określający priorytety ruchu umożliwia dodawanie do przesyłanej ramki znacznika (ang. *tag*) wskazującego jego priorytet. Gdy urządzenie operuje na ramkach oznakowanych, korzysta z priorytetów określonych w przesyłanych danych, a kiedy ramki nie mają znacznika priorytetu, wykorzystywane są ustawienia priorytetów transmisji dla poszczególnych portów.

Aby ustawić priorytety transmisji pomiędzy poszczególnymi portami, należy w menu wybrać *QoS/802.1p Default Priority* (rysunek 8.6), a następnie dla wybranego portu ustawić jeden z 4 dostępnych priorytetów (najwyższy, wysoki, zwykły, niski — ang. *highest*, *high*, *middle*, *low*).

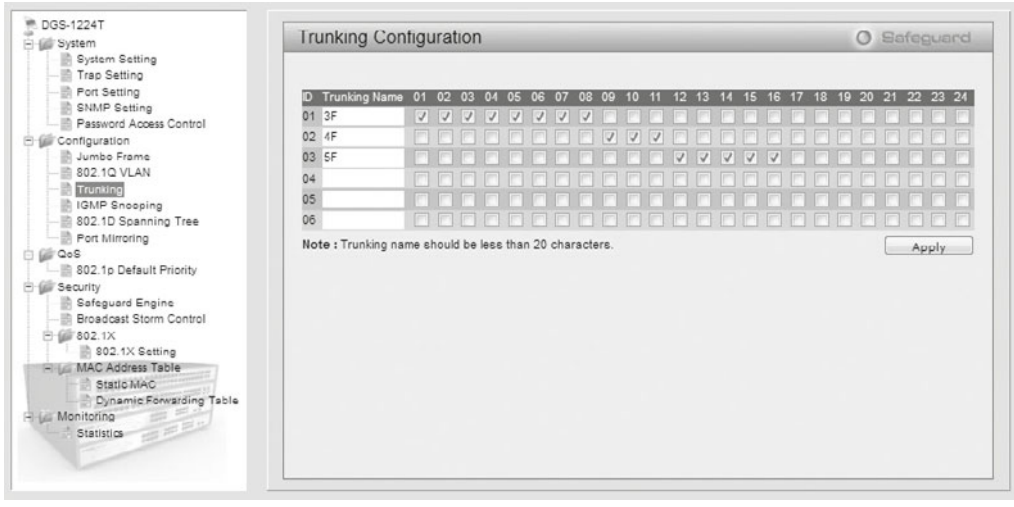


Rysunek 8.6. Konfiguracja QoS

8.3.6. Konfiguracja łącza typu trunk

Wybrane urządzenie pozwala na utworzenie 6 połączeń typu trunk, każde z nich może zawierać do 8 portów.

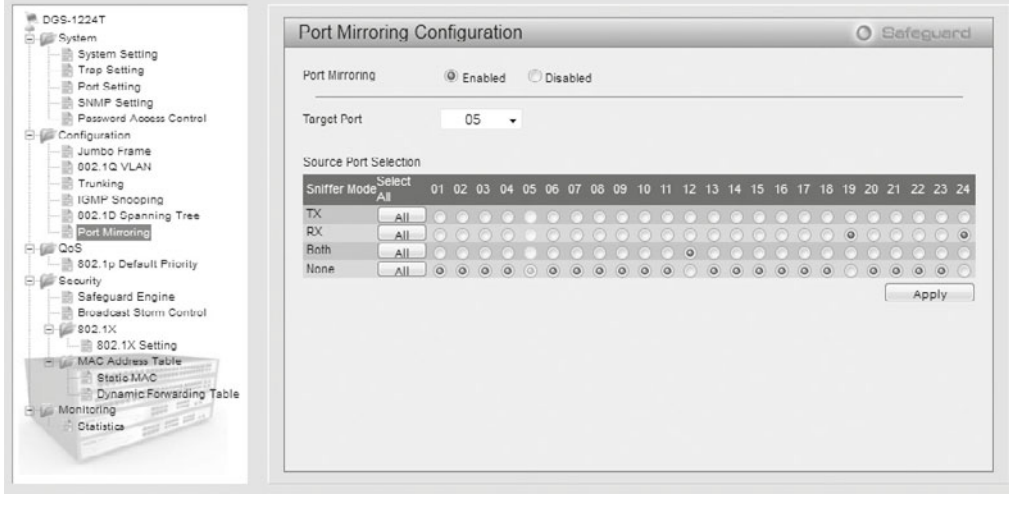
Aby utworzyć połączenie typu trunk, należy wybrać w menu *Configuration/Trunking* (rysunek 8.7), a następnie wprowadzić nazwę danego połączenia oraz wskazać porty, które mają do niego należeć.



Rysunek 8.7. Konfiguracja połączenia typu trunk

8.3.7. Konfiguracja usługi port mirroring

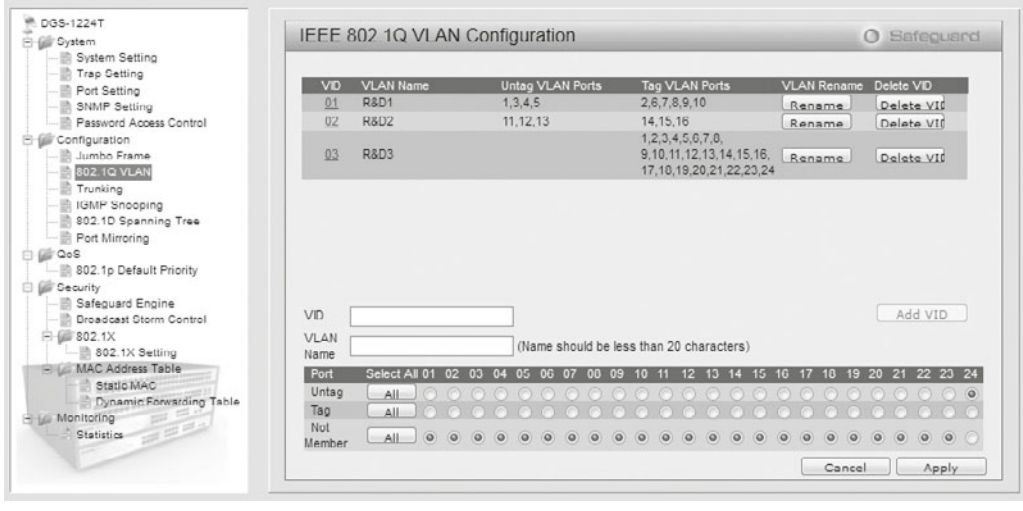
Konfiguracja usługi port mirroring jest dostępna w menu *Configuration/Port Mirroring* (rysunek 8.8). Aby uruchomić usługę w oknie konfiguracji, należy zmienić stan usługi na włączony (*Enabled*), wskazać port docelowy, do którego będą duplikowane dane (*Target port*) oraz porty źródłowe, skąd dane mają być przekazywane do portu docelowego (*Source Port Selection*). Oprogramowanie urządzenia pozwala wybrać, jakie dane z portu źródłowego mają być przekazywane do portu docelowego: *TX* — dane wysyłane, *RX* — dane odbierane, *Both* — zarówno dane wysyłane, jak i odbierane.



Rysunek 8.8. Konfiguracja usługi port mirroring

8.3.8. Konfiguracja sieci VLAN

Konfiguracja sieci wirtualnych VLAN jest dostępna w menu *Configuration/802.1Q VLAN* (rysunek 8.9). Po jego wybraniu pojawia się informacja dotycząca wszystkich skonfigurowanych sieci wirtualnych oraz przypisanych do nich portów. Urządzenie pozwala na przypisywanie do sieci VLAN portów działających w dwóch trybach — *Untag VLAN Ports* oraz *Tag VLAN Ports*. W pierwszym z nich urządzenie podłączone do portu nie musi znakować ramek identyfikatorem sieci VLAN, bo każda ramka przekazywana tym portem należy do jednej, wskazanej sieci VLAN. Drugi typ pozwala na przypisanie portu do wielu sieci VLAN, przy czym ramki muszą być znakowane identyfikatorem sieci VLAN.



Rysunek 8.9. Konfiguracja sieci VLAN

Aby utworzyć nową sieć VLAN, należy wybrać przycisk *Add VID*, podać identyfikator oraz nazwę, a następnie wskazać, które porty urządzenia i w jakim trybie mają należeć do nowej sieci.

Edycja poszczególnych sieci VLAN odbywa się w podobny sposób jak ich dodawanie; aby przejść do trybu edycji, należy wybrać link, na który wskazuje identyfikator wybranej sieci VLAN.

Zaprezentowane przykłady konfiguracji pokazują, w jaki sposób odnaleźć interesujące ustawienia w wybranym modelu urządzenia. Interfejsy graficzne różnych modeli lub innych producentów na ogół różnią się wyglądem, jednak zasada konfigurowania poszczególnych parametrów pozostaje zbliżona.

8.3.9. Konfiguracja przełącznika firmy Cisco

Konfiguracja adresu IP niezbędnego do zdalnego logowania się do urządzeń dla przełączników firmy Cisco może być określona dla urządzeń pracujących w tzw. administracyjnej

sieci VLAN. Domyślnie urządzenia mają tylko jedną sieć VLAN o identyfikatorze 1, dla której nie został przypisany żaden adres IP, w związku z czym dostęp do konfiguracji jest możliwy jedynie przez port konsoli.

Aby przypisać urządzeniu adres IP, należy w trybie uprzywilejowanym wykonać następujące komendy:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.0.5 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, przejście do konfiguracji wirtualnego interfejsu sieci VLAN 1, przypisanie adresu IP oraz maski podsieci dla wybranej sieci VLAN, uruchomienie sieci, opuszczenie trybu konfiguracji interfejsu, opuszczenie trybu konfiguracji.

Przypisanie adresu IP pozwala na komunikację pomiędzy zdalnymi urządzeniami a przełącznikiem. Aby możliwe było zalogowanie się i zdalna praca na urządzeniu, dostęp do konsoli telnet powinien być zabezpieczony hasłem.

Konfiguracja ustawień poszczególnych portów urządzenia odbywa się poprzez wejście w trybie uprzywilejowanym do konfiguracji wybranego interfejsu, a następnie wprowadzenie wybranych ustawień.

```
Switch# configure terminal
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, przejście do konfiguracji interfejsu o numerze 1, ustawienie automatycznej negocjacji prędkości portu, ustawienie automatycznej negocjacji trybu pracy portu, włączenie portu, opuszczenie trybu konfiguracji interfejsu, opuszczenie trybu konfiguracji.

Aby sprawdzić stan kolejnych interfejsów urządzenia, należy wprowadzić komendę:

```
Switch# show interfaces
```

lub gdy chce się sprawdzić stan konkretnego interfejsu, podać jego adres:

```
Switch# show interface FastEthernet 0/1
```

Ustawienie haseł dla protokołu SNMP jest możliwe w trybie uprzywilejowanym za pomocą następujących komend:

```
Switch# configure terminal
```

```
Switch(config)# snmp-server community public RO
Switch(config)# snmp-server community private RW
Switch(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, przypisanie hasła public dla odczytu (parametr `RO` — ang. *read only*), przypisanie hasła private dla zapisu i odczytu (parametr `RW` — ang. *read write*), wyjście z trybu konfiguracji.

Aby uruchomić protokół STP na urządzeniach firmy Cisco, należy wskazać tryb jego pracy w trybie konfiguracji poprzez następujące komendy:

```
Switch# configure terminal
Switch(config)# spanning-tree mode pvst
Switch(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, uruchomienie protokołu STP w trybie `pvst` (ang. *per-vlan spanning tree mode*), wyjście z trybu konfiguracji. Tryb pvst to standardowy protokół STP. Istnieje możliwość uruchomienia trybu *per-vlan rapid spanning tree mode* przez wybranie komendy `spanning-tree mode rapid-pvst`.

Aby na przełączniku firmy Cisco uruchomić priorytety transmisji na danych portach, należy włączyć globalnie priorytet wybranego portu następującymi komendami:

```
Switch# configure terminal
Switch(config)# mls qos
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# mls qos cos 0
Switch(config-if)# exit
Switch(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, uruchomienie usługi QoS na urządzeniu, wejście w tryb konfiguracji konkretnego interfejsu, przypisanie klasy usług na danym porcie, opuszczenie trybu konfiguracji interfejsu, opuszczenie trybu konfiguracji.

Poniższa konfiguracja pozwala na utworzenie łącza zagregowanego.

```
Switch# configure terminal
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# channel-group 1 mode auto
Switch(config-if)# interface FastEthernet 0/2
Switch(config-if)# channel-group 1 mode auto
Switch(config-if)# interface port-channel 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, wejście w tryb konfiguracji interfejsu `FastEthernet 0/1`, przypisanie portu do pierwszego kanału agregującego pracującego w trybie automatycznym, wejście w tryb konfiguracji interfejsu

`FastEthernet 0/2`, przypisanie portu do pierwszego kanału agregującego pracującego w trybie automatycznym, wejście w tryb konfiguracji wirtualnego interfejsu agregującego `port-channel 1`, ustawienie trybu pracy portu jako portu *trunk* (przekazuje dane z informacją, do której sieci VLAN one należą), opuszczenie trybu konfiguracji interfejsu, opuszczenie trybu konfiguracji.

Usługa port mirroring na urządzeniach firmy Cisco jest nazywana SPAN (ang. *Switched Port Analyzer*). Jej konfiguracja została przedstawiona poniżej.

```
Switch# configure terminal
Switch(config)# monitor session 1 source interface FastEthernet 0/1
Switch(config)# monitor session 1 destination interface FastEthernet 0/10
Switch(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, przypisanie do 1. sesji monitoringu portu źródłowego — `FastEthernet 0/1`, przypisanie do 1. sesji monitoringu portu docelowego — `FastEthernet 0/10`, opuszczenie trybu konfiguracji.

Aby dodać sieć VLAN i przypisać jej wybraną nazwę, należy użyć poniższej konfiguracji:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name siec-vlan20
Switch(config-vlan)# exit
Switch(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, wejście w tryb konfiguracji sieci VLAN o identyfikatorze `20`, przypisanie nazwy `siec-vlan20`, opuszczenie trybu konfiguracji sieci, opuszczenie trybu konfiguracji.

Aby przypisać dany port do wybranej sieci VLAN, należy użyć poniższej konfiguracji:

```
Switch# configure terminal
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
Switch(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, wejście w tryb konfiguracji interfejsu `FastEthernet 0/1`, ustawienie trybu pracy portu w sieci VLAN jako portu należącego do wybranej sieci, dołączenie portu do wirtualnej sieci VLAN 20, opuszczenie trybu konfiguracji interfejsu, opuszczenie trybu konfiguracji.

Przełączniki firmy Cisco pozwalają na uruchomienie pomiędzy routerami połączeń przekazujących informacje dotyczące sieci VLAN, do których należy przekazywana ramka — port pracujący w trybie *trunk* należy do wielu sieci VLAN. Poniższa konfiguracja prezentuje, w jaki sposób przypisać tryb pracy *trunk* do interfejsu `FastEthernet 0/24`.

```
Switch# configure terminal
Switch(config)# interface FastEthernet 0/24
```

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan all
Switch(config-if)# exit
Switch(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, wejście w tryb konfiguracji interfejsu `FastEthernet 0/24`, ustawienie trybu pracy portu w sieci VLAN jako portu *trunk*, przypisanie do portu *trunk* wszystkich sieci VLAN, opuszczenie trybu konfiguracji interfejsu, opuszczenie trybu konfiguracji.

Pokazane przykłady konfiguracji pozwalają na przygotowanie wydajnego środowiska pracy. Dostępność poszczególnych ustawień zależy od posiadanej konfiguracji sprzętowej oraz zainstalowanej wersji systemu IOS. Urządzenia firmy Cisco mają szereg zaawansowanych parametrów konfiguracyjnych, które wykraczają poza ramy niniejszej publikacji.

8.4. Konfiguracja routera

Głównym zadaniem routera jest zapewnienie połączeń między sieciami na podstawie propagowanych przez protokoły routingu informacji oraz przekazywanie pakietów IP pomiędzy sieciami. Szczegółowy opis funkcji routerów znajduje się w podrozdziale 5.4.

8.4.1. Parametry konfiguracyjne routerów

Routery do zastosowań domowych i małego biznesu najczęściej są urządzeniami mającymi jeden interfejs dostępu do sieci WAN (RJ-45 dla połączeń Ethernet lub RJ-11 dla połączeń ADSL) oraz interfejsy do podłączenia urządzeń sieci LAN (porty RJ-45 i opcjonalnie interfejs sieci WiFi). W profesjonalnych zastosowaniach w firmach zajmujących się transmisją danych routery są bardzo zaawansowanymi urządzeniami, pozwalającymi na łączenie wielu sieci WAN pracujących w różnych technologiach z wieloma sieciami LAN. Bardzo często są to urządzenia o budowie modularnej, które pozwalają w razie potrzeby na rozbudowę sprzętową przy zastosowaniu specjalnych kart rozszerzeń.

Najczęściej konfigurowane parametry routerów to m.in.:

- *Interfejs WAN* — tryb pracy interfejsu, mechanizm komunikacji z dostawcą internetu, adresacja IP.
- *Serwer DHCP* — większość routerów oferuje możliwość uruchomienia serwera DHCP, co pozwala na automatyczne przypisywanie adresów IP dla urządzeń w sieci lokalnej.
- *Protokół SNMP* (ang. *Simple Network Management Protocol*) — to uniwersalny protokół opisany w dokumencie RFC 1157, służący do zarządzania urządzeniami sieciowymi i monitorowania ich.
- *Technologia NAT* — routery oferują możliwość uruchomienia technologii translacji adresów, czyli zamiany prywatnych adresów urządzeń sieci LAN na adresy publiczne, co pozwala na dostęp do internetu w przypadku zbyt małej liczby publicznych adresów IP.

- *Przekierowanie portów* (ang. *Port Forwarding*) — usługa pozwalająca na przekierowanie danych z określonego portu routera na konkretny port urządzenia pracującego w wewnętrznej sieci LAN. Przekierowanie portów pozwala na uruchamianie tzw. serwerów wirtualnych — usług dostępnych z sieci zewnętrznej działających na komputerach, które nie mają publicznych adresów IP.
- *Strefa zdemilitaryzowana* (ang. *Demilitarized Zone*) — jest to obszar sieci komputerowej zwiększonego ryzyka włamania, w którym działają urządzenia i serwery świadczące usługi dla użytkowników sieci zewnętrznej, ale pracujące również w sieci wewnętrznej.
- *Routing statyczny* — możliwość ręcznego przypisania trasy kierującej pakiety do określonej sieci (poprzez wybrany interfejs lub adres IP).
- *Routing dynamiczny* — pozwala na automatyczną wymianę pomiędzy routerami informacji na temat tras dostępu do osiągalnych przez nie sieci.
- *QoS* (ang. *Quality of Service*) — usługa pozwalająca na kształtowanie ruchu w celu poprawienia jakości usług transmisji danych w routerach, działająca na poziomie pakietów IP.

Do zaprezentowania konfiguracji konkretnego urządzenia sieciowego został wybrany model z serii DSL-2640 firmy D-Link. Jest to urządzenie mające wiele parametrów konfiguracyjnych, pozwalające na połączenie lokalnej sieci LAN bezpośrednio z siecią internetową typu ADSL dzięki wbudowanemu modemowi.

8.4.2. Konfiguracja podstawowa

Panel konfiguracji urządzenia jest dostępny poprzez stronę WWW domyślnie pod adresem *192.168.1.1*. Po jego uruchomieniu użytkownik zostanie zapytany o login oraz hasło dostępu — domyślne ustawienia to: login *Admin*, hasło *Admin*.

Okno konfiguracji składa się ze stałego menu górnego oraz zmiennego menu znajdującego się po lewej stronie. Główna część ekranu zawiera edytor parametrów konfiguracyjnych z obszaru wybranego menu (rysunek 8.10).

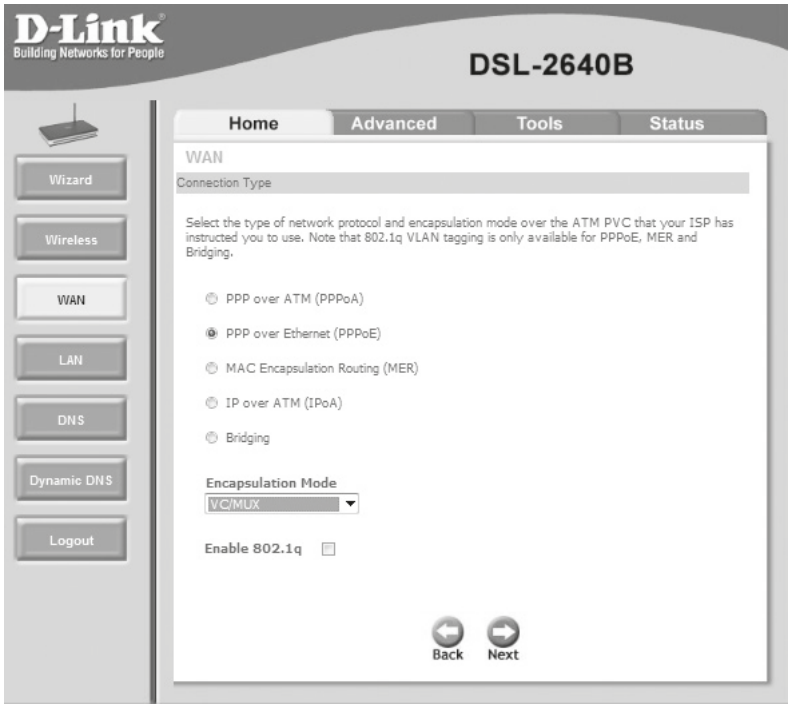
Rysunek 8.10. Główne okno konfiguracji routera

8.4.3. Konfiguracja interfejsu WAN

Konfiguracja interfejsu sieci rozległej pracującego w trybie ADSL polega na wprowadzeniu parametrów połączenia, które są dostarczane przez dostawcę usług internetowych (ang. *Internet Service Provider*). Połączenia ADSL są oferowane przez dostawców telekomunikacyjnych i powszechnie dostępne na terenie praktycznie całego kraju.

Aby skonfigurować parametry połączenia internetowego, należy na głównej stronie panelu konfiguracyjnego w menu po lewej stronie wybrać opcję WAN, która uruchomi kreator ustawień. Na kolejnych stronach użytkownik musi określić — zgodnie z parametrami otrzymanymi od usługodawcy — następujące wartości:

- VPI — *Virtual Path Identifier* (liczba z zakresu 0–255) — identyfikator wirtualnej ścieżki w wirtualnym obwodzie sieci telekomunikacyjnej pracującej w standardzie ATM (ang. *Asynchronous Transfer Mode*).
- VCI — *Virtual Channel Identifier* (liczba z zakresu 32–65535) — identyfikator wirtualnego kanału na danej ścieżce w sieci telekomunikacyjnej pracującej w standardzie ATM. Parametr jest zależny od konkretnego dostawcy usługi dostępu do internetu.
- Kategorię usług sieci ATM — do wyboru z listy: UBR Without PCR (*Unspecified Bit Rate without Peak Cell Rate*), UBR With PCR (*Unspecified Bit Rate with Peak Cell Rate*), CBR (*Constant Bit Rate*), Non Realtime VBR (*Non-Real-time Variable Bit Rate*), Realtime VBR (*Real-time Variable Bit Rate*).



Rysunek 8.11. Wybór typu sieci ATM w konfiguracji routera

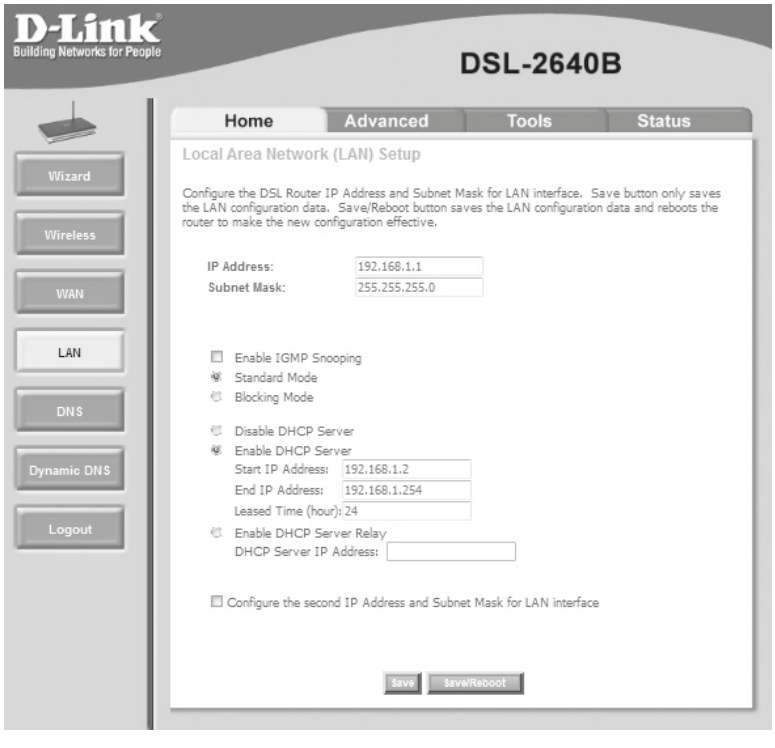
- Typ enkapsulacji w sieci ATM — *LLC/Snap-Bridging* lub *VC/MUX*.
- Typ protokołu sieciowego w sieci ATM — do wyboru z listy: *PPP over ATM* (PPPoA), *PPP over Ethernet* (PPPoE), *MAC Encapsulation Routing* (MER), *IP over ATM* (IpoA), *Bridging* (rysunek 8.11).
- W przypadku wyboru protokołu PPP używanego przez dostawców usług internetowych wymagane są: podanie loginu oraz hasła dostępu do sieci, a także wybór sposobu otrzymania adresu IP bramy domyślnej po połączeniu.

Kolejne okno kreatora pozwala na ustawienie hasła dostępu dla protokołu PPP, uruchomienie technologii translacji adresów oraz zapory ogniowej na routerze.

Po zapisaniu zmian router zostanie automatycznie zrestartowany, a połączenie z dostawcą internetowym powinno zostać nawiązane.

8.4.4. Konfiguracja sieci LAN — serwera DHCP oraz DNS

Konfiguracja ustawień dla sieci lokalnej jest dostępna poprzez wybór z menu po lewej stronie opcji *LAN* (rysunek 8.12).

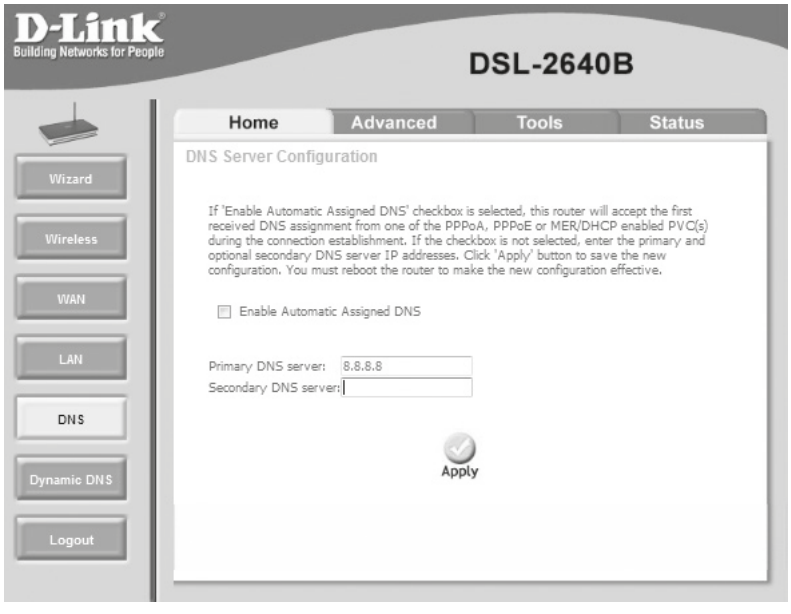


Rysunek 8.12. Konfiguracja ustawień sieci lokalnej oraz serwera DHCP

Aby poprawnie skonfigurować serwer DHCP, należy podać adres IP (*IP Address*), pod którym w sieci lokalnej będzie widoczny router (będzie on propagowany w sieci jako adres bramy domyślnej), maskę podsieci (*Subnet Mask*) oraz zakres adresów, jakie mają być nadawane przez protokół (pola *Start IP Address* oraz *End IP Address* są dostępne po uruchomieniu serwera po zaznaczeniu opcji *Enable DHCP Server*). Dodatkowo urządzenie pozwala na ustawienie czasu, na jaki jest nadawany adres IP przez serwer DHCP (*Leased Time*).

Wybrane urządzenie nie pozwala na zdefiniowanie adresu IP serwera DNS przekazywanego przez serwer DHCP — przekazywanym adresem IP serwera DNS jest zawsze adres routera.

Do poprawnego przekierowania zapytań DNS przez router niezbędne jest ustawienie adresu poprawnego serwera DNS, który będzie w stanie odpowiedzieć na zapytania kierowane z wewnątrz sieci. Aby to zrobić, należy wybrać w menu po lewej stronie opcję *DNS* (rysunek 8.13).

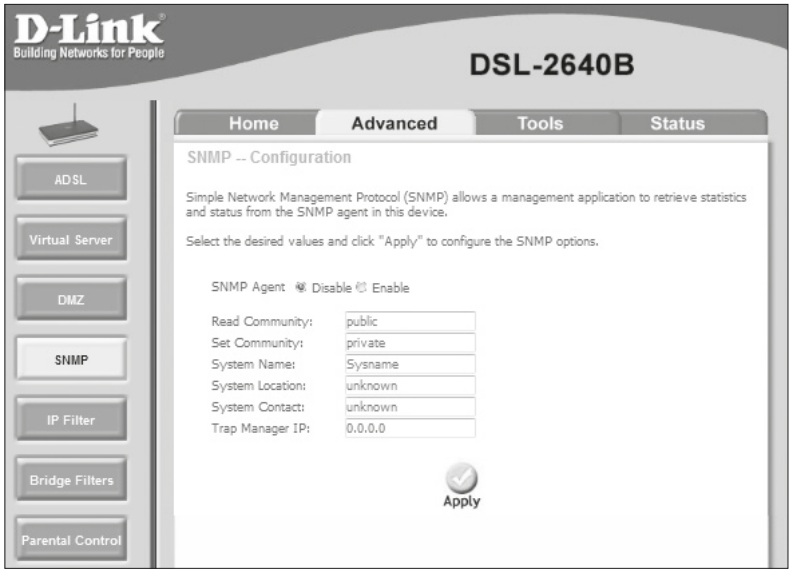


Rysunek 8.13. Konfiguracja adresu DNS

Wybór opcji *Enable Automatic Assigned DNS* pozwala na używanie adresu serwera DNS przypisanego przez dostawcę internetowego podczas nadawania adresu IP.

8.4.5. Konfiguracja protokołu SNMP

Konfiguracja protokołu SNMP jest dostępna po wybraniu w górnym menu opcji *Advanced*, a następnie w menu po lewej stronie *SNMP* (rysunek 8.14).



Rysunek 8.14. Konfiguracja protokołu SNMP

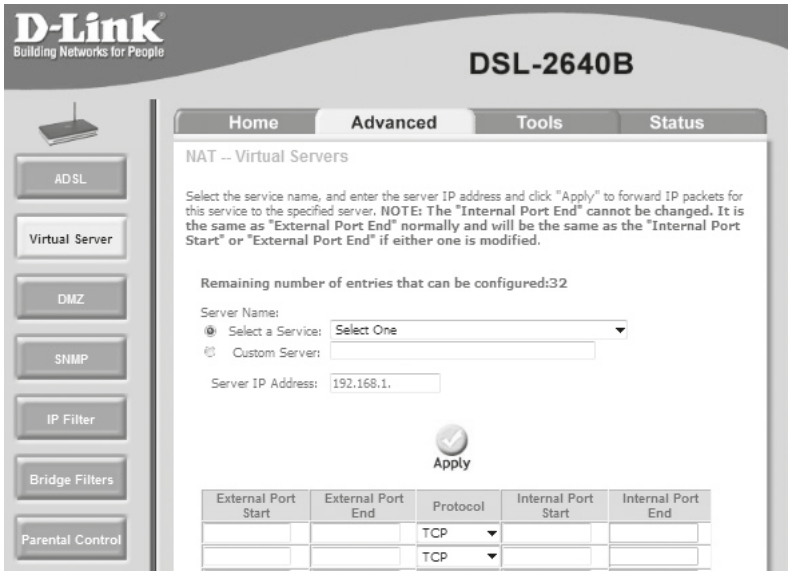
Aby uruchomić protokół SNMP, należy wybrać opcję *Enable* oraz skonfigurować hasła dla odczytu (*Read Community*), a także odczytu i zapisu (*Set Community*). Dodatkowo można ustawić nazwę, lokalizację oraz dane kontaktowe do osoby zarządzającej wybranym urządzeniem. Istnieje również możliwość określenia adresu IP serwera, który gromadzi dane dotyczące zdarzeń na urządzeniu (*Trap Manager IP*).

8.4.6. Konfiguracja technologii NAT, przekierowania portów oraz strefy zdemilitaryzowanej

Uruchomienie technologii NAT jest możliwe na etapie konfigurowania sieci WAN — w oknie kreatora ustawień należy zaznaczyć opcję *Enable NAT*, która uruchomi translacje adresów z sieci lokalnej na adres publiczny interfejsu WAN.

Przekierowanie portów pozwala na inicjację dostępu do usług sieciowych działających w sieci wewnętrznej poprzez stałe zdefiniowanie przekierowania portów interfejsu WAN na dany port wybranego urządzenia po stronie sieci LAN. Usługa ta umożliwia uruchamianie usług i serwerów dostępnych spoza sieci lokalnej, mimo że nie mają one publicznego adresu IP.

Tworzenie serwerów wirtualnych poprzez przekierowanie portów jest możliwe po wybraniu opcji *Virtual Server* dostępnej po kliknięciu opcji *Advanced* z górnego menu, gdzie są prezentowane wszystkie uruchomione przekierowania. Po wybraniu przycisku *Add* zostaje uruchomione okno pozwalające na dodanie kolejnego przekierowania (rysunek 8.15).



Rysunek 8.15. Konfiguracja przekierowania portów

Aby dołączyć kolejne przekierowanie, należy wybrać wcześniej zdefiniowaną usługę z listy (*Select a Service*) lub dodać własną poprzez podanie jej nazwy (*Custom Server*), zdefiniowanie zakresów portów do przekierowania z interfejsu WAN (*External Port*) oraz zakresu portów sieci wewnętrznej, na które dane mają zostać przekierowane (*Internal Port*), a także typu protokołów, które mają być przekierowywane (TCP, UDP, TCP/UDP).

Wymagane jest również zdefiniowanie adresu IP urządzenia w sieci wewnętrznej, do którego dane mają zostać przekierowane (*Server IP Address*).

Po zapisaniu ustawień wszystkie dane kierowane na adres interfejsu WAN na wybrany port zostaną przekierowane bezpośrednio na wskazany port urządzenia pracującego w sieci wewnętrznej.

Uruchomienie strefy zdemilitaryzowanej pozwala na przekierowanie całego ruchu przychodzącego, który nie jest kierowany do wcześniej zdefiniowanych serwerów wirtualnych, do wybranego adresu IP. Konfiguracja strefy zdemilitaryzowanej polega na przypisaniu adresu IP urządzenia; można to zrobić, wybierając w górnym menu opcję *Advanced*, a następnie w menu po lewej stronie opcję *DMZ*.

8.4.7. Konfiguracja routingu dynamicznego i statycznego

W rozbudowanych sieciach istnieje konieczność zapewnienia automatycznej wymiany pomiędzy routerami informacji o sieciach, które są osiągalne przez dany router. W tym celu zostały stworzone protokoły routingu, które przesyłają informacje pomiędzy

węzłami sieci. Na ich podstawie powstają tablice routingu pozwalające na wybór optymalnej trasy przesyłania danych.

W urządzeniach dla zastosowań domowych i małych firm najczęściej udostępniany jest protokół RIP (ang. *Routing Information Protocol*). W celu wybrania najlepszej ścieżki posługuje się on liczbą kolejnych routerów, przez które wędruje określony pakiet.

Konfiguracja protokołu RIP w wybranym urządzeniu jest dostępna po wybraniu opcji *RIP* z karty *Routing* po wskazaniu w górnym menu opcji *Advanced*. Aby uruchomić protokół RIP, należy zaznaczyć opcję *Enabled* przy polu *Global RIP Mode*. Dodatkowo można skonfigurować wersję używanego protokołu (wersja 1. lub 2.) oraz tryb pracy (aktywny albo pasywny).

Routing statyczny pozwala na ręczne przypisanie trasy do określonej sieci, co umożliwia konfigurację tras przesyłu danych.

Konfiguracja routingu statycznego polega na wskazaniu adresu sieci docelowej wraz z maską podsieci oraz podaniu adresu lub wybraniu interfejsu, przez który dane mają być przesyłane do wskazanej sieci. Jest ona dostępna po wybraniu opcji *Static Route* na karcie *Routing* po wskazaniu w górnym menu opcji *Advanced* (rysunek 8.16).

Rysunek 8.16. Konfiguracja routingu statycznego

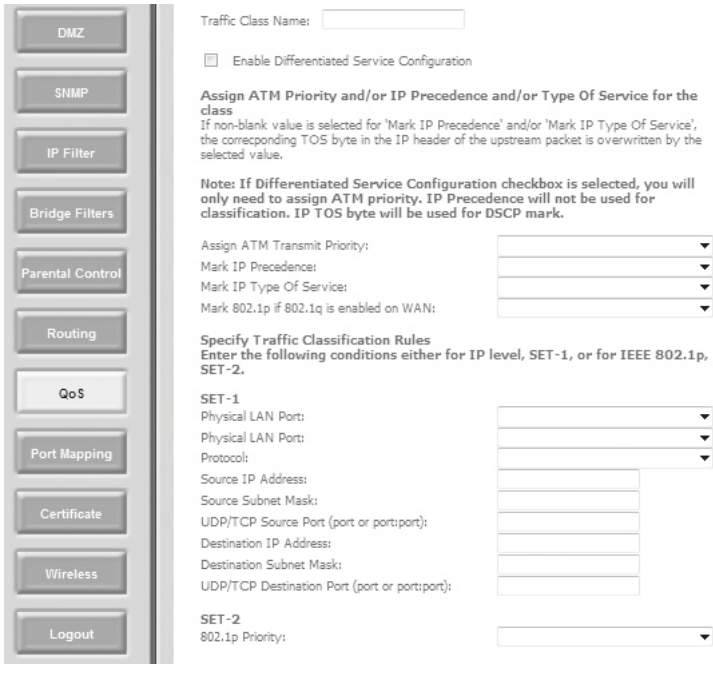
8.4.8. Konfiguracja usługi QoS

Usługa QoS pozwala na identyfikację, klasyfikację i przypisywanie priorytetów ruchu sieciowego przechodzącego przez router, aby zapewnić lepszą jakość transmisji dla danych wrażliwych na opóźnienia (np. transmisji wideo).

Ustawienia usługi QoS są dostępne w menu *QoS* po wybraniu górnej zakładki *Advanced*.

Konfiguracja usługi QoS na routerach polega na utworzeniu klas ruchu (rysunek 8.17), dla których są przypisywane konkretne — ustawione przez administratora — parametry ruchu:

- *ATM Transmit Priority* — priorytet transmisji na poziomie komunikacji sieci ATM,
- *IP Precedence* — priorytet transmisji określany w nagłówku pakietów IP na pierwszych 3 bitach pola TOS (*type of service*),
- *IP Type Of Service* — rodzaj transmitowanych danych określany w nagłówku pakietu IP na ostatnich 5 bitach pola TOS (*type of service*),
- priorytet 802.1p dla łącza WAN — ustawienie priorytetów na poziomie transmisji w sieci Ethernet (o ile łącze WAN używa znakowania ramek).



Rysunek 8.17. Ustawianie priorytetów ruchu

Po ustawieniu priorytetów należy wybrać, jaki ruch ma być znakowany zgodnie z powyższymi ustawieniami, na podstawie następujących kryteriów:

- Fizyczny port urządzenia (ang. *Physical LAN port*).
- Protokół (ang. *Protocol*) — *TCP/UDP*.
- Źródłowy adres IP (ang. *Source IP Address*).
- Źródłowa maska podsieci (ang. *Source Subnet Mask*).
- Źródłowy port UDP/TCP (ang. *UDP/TCP Source Port*).
- Docelowy adres IP (ang. *Destination IP Address*).
- Docelowa maska podsieci (ang. *Destination Subnet Mask*).
- Docelowy port UDP/TCP (ang. *Destination Port*).
- Źródłowy adres MAC (ang. *Source MAC Address*).

- Maska źródłowego adresu MAC (ang. *Source MAC Mask*).
- Docelowy adres MAC (ang. *Destination MAC Address*).
- Maska docelowego adresu MAC (ang. *Destination MAC Mask*).
- Priorytet ruchu w warstwie 2. — *802.1p Priority*.

Maska adresów MAC pozwala na wybór adresów spełniających określone kryteria — podobnie jak maska podsieci przypisywana w konfiguracji protokołu IP.

Dla każdej klasy wymagane jest również podanie jej nazwy. Po zapisaniu klasy przy użyciu przycisku *Apply* ruch sieciowy będzie wysyłany zgodnie z przypisanymi priorytetami.

Kształtowanie ruchu sieciowego przy użyciu usługi QoS jest bardzo rozległym zagadnieniem wykraczającym poza ramy podręcznika, w którym przedstawiono jedynie podstawowe i łatwe do zrozumienia zasady konfiguracji usługi.

8.4.9. Konfiguracja zabezpieczeń sieci — firewall

Routery to urządzenia pracujące na styku sieci wewnętrznej i zewnętrznej, w związku z czym są one często narażone na ataki z zewnątrz sieci. W celu wyeliminowania potencjalnych zagrożeń większość urządzeń ma wbudowane funkcje zabezpieczeń sieci — zaporę ogniową (ang. *firewall*). Funkcjonalność zapory ogniowej pozwala na filtrowanie ruchu przychodzącego i wychodzącego pod względem źródłowych i docelowych adresów IP oraz portów, a także protokołu warstwy czwartej.

Domyślnie prezentowane urządzenie blokuje cały ruch przychodzący, a wbudowany mechanizm pozwala na odblokowanie wybranego rodzaju ruchu przychodzącego. W przypadku ruchu wychodzącego domyślnie cały ruch jest dozwolony; filtrowanie pozwala na ograniczenie wybranego rodzaju ruchu.

Konfiguracja filtrowania adresów IP jest dostępna na karcie *IP Filter* po wybraniu z górnego menu opcji *Advanced*, gdzie można określić ustawienia dla ruchu przychodzącego (ang. *inbound filter*) oraz wychodzącego (ang. *outbound filter*) — rysunek 8.18.

Rysunek 8.18. Konfiguracja filtrów IP dla połączeń wychodzących

8.4.10. Konfiguracja routerów firmy Cisco

Przykładowa konfiguracja routera firmy Cisco odnosi się do urządzenia zapewniającego komunikację sieci lokalnej z dostawcą internetu poprzez łącze typu ADSL.

Łącza typu ADSL należą do łączy wdzwanianych (ang. *Dial-up*), czyli takich, które mogą działać jedynie wtedy, gdy połączenie zostanie nawiązane. Połączenia tego typu pozwalają na uruchamianie tzw. Routingu na żądanie (ang. *Routing on demand*), np. w przypadku awarii innego łącza, czy też umożliwiają łączenie się przy użyciu jednego interfejsu fizycznego z wieloma dostawcami internetu lub innymi lokalizacjami sieci. Aby poprawnie skonfigurować połączenie wdzwaniane, niezbędne są następujące elementy:

- Interfejs fizyczny (ang. *Physical interface*) — port routera, który będzie połączony z siecią dostawcy internetu lub siecią telekomunikacyjną.
- Interfejs logiczny (ang. *Dialer interface*) — to zestaw ustawień konkretnego wdzwanianego połączenia z siecią (takich jak numer telefonu, jeśli jest potrzebny, login i hasło niezbędne do podłączenia się do zdalnej sieci).
- Pula interfejsów wdzwanianych (ang. *Dialer pool*) — to przypisanie interfejsów fizycznych do interfejsów logicznych.

Interfejsy pozwalające na podłączenie do sieci ADSL w routerach Cisco są oznaczane nazwą ATM. Przykładowa konfiguracja routera do połączenia z siecią ADSL może wyglądać następująco:

```
Router# configure terminal
Router(config)# interface Dialer0
Router(config-if)# ip address negotiated
Router(config-if)# encapsulation ppp
Router(config-if)# dialer pool 1
Router(config-if)# ppp chap hostname login
Router(config-if)# ppp chap password haslo
Router(config-if)# interface ATM0/0
Router(config-if)# no ip address
Router(config-if)# pvc 0/35
Router(config-if)# encapsulation aal5mux ppp dialer
Router(config-if)# dialer pool-member 1
Router(config-if)# exit
Router(config)# exit
```

Kolejne komendy oznaczają uruchomienie trybu konfiguracji, wejście w tryb konfiguracji interfejsu logicznego `Dialer0` (numer interfejsu jest nadawany dowolnie), uruchomienie automatycznego pobierania adresu IP, włączenie protokołu PPP, przypisanie interfejsu do puli 1., ustawienie loginu do zdalnej sieci, ustawienie hasła dostępu do zdalnej sieci, przejście do konfiguracji interfejsu fizycznego, usunięcie przypisania adresu IP, ustawienie wirtualnej ścieżki i wirtualnego kanału połączenia ATM, wybór enkapsulacji dla połączenia ATM, przypisanie interfejsu do puli 1., wyjście z trybu konfiguracji interfejsu, wyjście z trybu konfiguracji.

Uruchomienie technologii NAT wymaga utworzenia listy dostępu (ang. *Access list*) — jest to lista reguł sprawdzająca adresy IP ruchu sieciowego, które są wykorzystywane przede wszystkim do filtrowania ruchu, ale również przy konfiguracji usług routera.

Urządzenia Cisco oferują trzy rodzaje list dostępu:

- Listy standardowe (ang. *standard list*) — pozwalają na sprawdzenie tylko źródłowego adresu IP.
- Listy rozszerzone (ang. *extended list*) — pozwalają na sprawdzenie źródłowego i docelowego adresu, a także portu i protokołu warstwy czwartej.
- Listy nazywane (ang. *named list*) — pozwalają na tworzenie list określanych nazwami, a nie liczbami. Mogą służyć zarówno do sprawdzania adresu źródłowego, jak również źródłowego i docelowego adresu oraz portu i protokołu warstwy czwartej.

Przetwarzanie listy dostępu odbywa się zgodnie z kolejnymi wpisami; jeśli przesyłany pakiet spełnia warunki określonego wpisu, kolejne wpisy nie są sprawdzane.

Określenie zakresu adresów w listach dostępu odbywa się przy użyciu maski odwrotnej (ang. *wildcard mask*). Jest to liczba 32-bitowa, wskazująca, które kolejne liczby w adresie IP muszą być zgodne z zapisem na liście dostępu — bity oznaczone w masce cyfrą 1 nie muszą być zgodne z zapisem na liście, bity oznaczone 0 muszą być równe, np.:

Adres IP:	192.168.1.1
Maska odwrotna:	0.0.0.255

oznacza zakres adresów 192.168.1.0–192.168.1.255.

Przy konfigurowaniu list dostępu można stosować specjalne słowa kluczowe:

- `any` zastępuje adres IP 0.0.0.0 oraz maskę 255.255.255.255 i oznacza dowolny adres sieciowy.
- `host` zastępuje maskę 0.0.0.0 i oznacza konkretny adres IP (dopasowanie wszystkich bitów adresu IP i adresu znajdującego się na liście).

Definiowanie list dostępu odbywa się w trybie konfiguracji urządzenia po słowie kluczowym `access-list`. Dla list standardowych przewidziane są numery 1–99; ich konfiguracja wygląda następująco:

```
Router# configure terminal
Router(config)# access-list 1 permit host 192.168.1.10
Router(config)# access-list 1 permit 192.168.2.0 0.0.0.255
Router(config)# exit
```

Kolejne polecenia oznaczają uruchomienie trybu konfiguracji, dołączenie do standardowej listy dostępu 1 zezwolenia dla adresu 192.168.1.10, dołączenie do standardowej listy dostępu 1 zezwolenia dla sieci 192.168.2.0, opuszczenie trybu konfiguracji. Taki zapis listy dostępu powoduje, że dopuszcza ona jedynie ruch pochodzący z adresu 192.168.1.10 oraz z sieci 192.168.2.0. Domyślnie każda lista na końcu zawiera niejawny zapis `deny any`, który oznacza, że żaden inny ruch nie zostanie zaakceptowany.

Konfiguracja list rozszerzonych wygląda następująco:

```
Router# configure terminal
Router(config)# access-list 100 permit tcp host 192.168.1.100 host
201.202.203.204 eq 22
Router(config)# access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 22
Router(config)# access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 25
Router(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255 any
Router(config)# exit
```

Kolejne polecenia oznaczają uruchomienie trybu konfiguracji, dołączenie do rozszerzonej listy dostępu 100 zezwolenia dla adresu 192.168.1.100 do komunikacji z adresem 201.202.203.204 na porcie 22, zabronienie dostępu z sieci 192.168.1.0 dla połączeń kierowanych na port 22, zabronienie dostępu z sieci 192.168.1.0 dla połączeń kierowanych na port 25, zezwolenie na dostęp z sieci 192.168.1.0 dla połączeń kierowanych na dowolne porty dowolnych adresów IP, opuszczenie trybu konfiguracji. Taki zapis listy dostępu pozwala na komunikację na porcie 22 jedynie urządzenia o adresie 192.168.1.100 z urządzeniem o adresie 201.202.203.204. Pozostałe połączenia na porcie 22 są zabronione, podobnie jak zabroniona jest komunikacja na porcie 25. Pozostała komunikacja z innymi portami pochodząca z sieci 192.168.1.0 jest dozwolona. Podobnie jak w przypadku listy standardowej, niejawny zapis `deny any` oznacza, że żaden inny ruch nie zostanie zaakceptowany.

Istnieje również możliwość utworzenia nazywanych list dostępu, dzięki czemu nie trzeba ograniczać się do dostępnych numerów przeznaczonych dla danego rodzaju listy. Konfiguracja zezwalająca na ruch pochodzący z adresu 192.168.1.10 oraz sieci 192.168.2.0 przy zastosowaniu list nazywanych wygląda następująco:

```
Router# configure terminal
Router(config)# ip access-list standard RuchZSieci
Router(config-std-nacl)# permit host 192.168.1.10
Router(config-std-nacl)# permit 192.168.2.0 0.0.0.255
Router(config-std-nacl)# exit
```

Konfiguracja translacji adresów na urządzeniach firmy Cisco odbywa się w trzech etapach:

- określenie interfejsu wewnętrznego oraz zewnętrznego;
- określenie puli adresów zewnętrznych, dla których ma być wykonywana translacja adresów;
- określenie ruchu, który ma mieć adresy tłumaczone za pomocą listy dostępu, oraz przypisanie listy do określonej puli adresów zewnętrznych.

Przykładowa konfiguracja translacji adresów ruchu pochodzącego z sieci 192.168.1.0 podłączonej do interfejsu `FastEthernet 0/0` na adres 201.202.203.204 przypisany na interfejsie `GigabitEthernet 0/0` wygląda następująco:

```
Router# configure terminal
Router(config)# interface FastEthernet 0/0
```

```
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# interface GigabitEthernet 0/0
Router(config-if)# ip address 201.202.203.204 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# exit
Router(config)# ip nat pool Pula1 201.202.203.204 201.202.203.204 netmask
255.255.255.255
Router(config)# ip access-list standard RuchZSieciLan
Router(config-std-nacl)# permit 192.168.1.0 0.0.0.255
Router(config-std-nacl)# exit
Router(config)# ip nat inside source list RuchZSieciLan pool Pula1
overload
Router(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, wejście w tryb konfiguracji interfejsu `FastEthernet 0/0`, przypisanie adresu 192.168.1.1, ustawienie interfejsu jako wewnętrznego dla technologii NAT, przejście do konfiguracji interfejsu `GigabitEthernet 0/0`, przypisanie adresu 201.202.203.204, ustawienie interfejsu jako zewnętrznego dla technologii NAT, opuszczenie konfiguracji interfejsu, utworzenie puli adresów zewnętrznych, na które będzie tworzone tłumaczenie, utworzenie standardowej nazywanej listy dostępu, dopuszczenie ruchu pochodzącego z sieci 192.168.1.0, opuszczenie konfiguracji nazywanej listy dostępu, przypisanie translacji adresów dla adresów wewnętrznych, które spełniają warunki listy `RuchZSieciLan`, tłumaczenie adresów na zdefiniowaną wcześniej pulę adresów zewnętrznych `Pula1`, opuszczenie trybu konfiguracji.

Urządzenia Cisco pozwalają również na przekierowanie portów lub całego ruchu na wskazany adres IP. Aby przekierować ruch z portu 8080 interfejsu zewnętrznego na port 80 urządzenia o adresie 192.168.1.50, należy użyć następującego polecenia:

```
Router# configure terminal
Router(config)# ip nat inside source static tcp 192.168.1.50
80 201.202.203.204 8080 extendable
Router(config)# exit
```

Aby uruchomić usługę serwera DHCP na routerze, należy zarezerwować adres IP interfejsu routera, który nie będzie przypisywany przez serwer DHCP, i zdefiniować pulę adresów wraz z parametrami, np.:

```
Router# configure terminal
Router(config)# ip dhcp excluded-address 192.168.1.1
Router(config)# ip dhcp pool PulaDHCP
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 192.168.1.50
Router(dhcp-config)# exit
Router(config)# exit
```

Kolejne komendy oznaczają wejście w tryb konfiguracji, wyłączenie adresu 192.168.1.1 z puli adresów przydzielanych przez serwer DHCP, utworzenie puli adresów DHCP o nazwie `PulaDHCP`, przypisanie sieci 192.168.1.0 do przydzielanych adresów, przypisanie adresu bramy domyślnej przekazywanego przez serwer DHCP, przypisanie adresu serwera DNS przekazywanego przez serwer DHCP, opuszczenie trybu konfiguracji puli DHCP, wyjście z trybu konfiguracji.

Konfiguracja parametrów protokołu SMTP w oprogramowaniu routera odbywa się w taki sam sposób jak w przypadku konfiguracji przełączników (punkt 8.3.9).

Urządzenia firmy Cisco pozwalają na bardzo zaawansowaną parametryzację jakości usług. Ze względu na złożoność tego zagadnienia, które wykracza poza ramy podręcznika, omówiona zostanie podstawowa funkcjonalność pozwalająca przypisywać wybrany ruch do kolejek o różnych priorytetach.

Podstawowa konfiguracja kolejkowania w urządzeniach Cisco pozwala na uruchomienie 4 kolejek o priorytetach wysokim, średnim, normalnym oraz niskim (`high`, `medium`, `normal`, `low`). Przypisanie ruchu, który ma być kierowany kolejką o wybranym priorytecie, odbywa się za pomocą omówionych wcześniej list dostępu. Ze względu na większe możliwości weryfikowania najczęściej używane są w tym celu listy rozszerzone.

Po utworzeniu list dostępu należy je przypisać do wybranej listy kolejek z odpowiednimi priorytetami, a następnie przypisać listę kolejek do określonego interfejsu, np.:

```
Router# configure terminal
Router(config)# access-list extended 100
Router(config-ext-nacl)# permit tcp any any eq 22
Router(config-ext-nacl)# permit tcp any any eq 23
Router(config-ext-nacl)# ip access-list extended 110
Router(config-ext-nacl)# permit tcp any any eq 25
Router(config-ext-nacl)# permit tcp any any eq 80
Router(config-ext-nacl)# permit tcp any any eq 110
Router(config-ext-nacl)# ip access-list extended 120
Router(config-ext-nacl)# permit tcp any any eq 21
Router(config-ext-nacl)# exit
Router(config)# priority-list 1 protocol ip high list 100
Router(config)# priority-list 1 protocol ip medium list 110
Router(config)# priority-list 1 protocol ip low list 120
Router(config)# priority-list 1 default normal
Router(config)# interface FastEthernet 0/0
Router(config-if)# priority-group 1
Router(config-if)# exit
Router# exit
```

W powyższym przykładzie po wejściu w tryb konfiguracji zostają skonfigurowane kolejne rozszerzone listy dostępu — lista 100 wskazująca dowolny ruch kierowany na porty 22 i 23 (usługi SSH i telnet), lista 110 wskazująca dowolny ruch kierowany na

porty 25, 80 i 110 (usługi SMTP, WWW, POP3) oraz lista 120 wskazująca dowolny ruch kierowany na port 21 (usługa FTP). Następnie zostaje utworzona lista kolejek nr 1 (ruch spełniający warunki listy 100 będzie kierowany z priorytetem wysokim, ruch spełniający warunki listy 110 z priorytetem średnim, ruch spełniający warunki listy 120 z priorytetem niskim, pozostały ruch ma domyślnie ustawiony priorytet normalny), po czym zostaje ona przypisana do interfejsu `FastEthernet 0/0`.

Konfiguracja protokołu RIP na urządzeniach firmy Cisco polega na uruchomieniu usługi oraz wskazaniu sieci, które mają być rozgłaszane przy użyciu protokołu RIP.

```
Router# configure terminal
Router(config)# router rip
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
Router(config-router)# exit
Router(config)# exit
```

Kolejne komendy konfiguracji oznaczają wejście w tryb konfiguracji, uruchomienie konfiguracji protokołu RIP, uruchomienie rozgłaszania informacji o sieciach 192.168.1.0 oraz 192.168.2.0 przy użyciu protokołu RIP, wyjście z trybu konfiguracji protokołu routingu, wyjście z trybu konfiguracji.

Aby sprawdzić tablicę routingu, w której znajdują się adresy dostępnych sieci wraz z informacją, w jaki sposób są one osiągalne, należy użyć komendy:

```
Router# show ip route
```

Konfiguracja filtrowania ruchu na urządzeniach firmy Cisco opiera się na utworzeniu listy dostępu oraz przypisaniu jej do określonego interfejsu dla połączeń przychodzących i (lub) wychodzących — samo utworzenie listy dostępu nie powoduje rozpoczęcia filtrowania ruchu, gdyż listy mogą być wykorzystywane również do konfiguracji innych usług (np. kolejkowania). Przykładowa konfiguracja tworzy listę dostępu zezwalającą jedynie na ruch WWW (port 80 i 443) do wszystkich urządzeń oraz ruch generowany przez serwery poczty (na porcie 25 i 110) kierowany do urządzenia o adresie 201.202.203.204, a następnie uruchamia filtrowanie ruchu wychodzącego zgodnie z utworzoną listą na interfejsie `FastEthernet 0/0`.

```
Router# configure terminal
Router(config)# ip access-list extended RuchWychodzacy
Router(config-ext-nacl)# permit tcp any any eq 80
Router(config-ext-nacl)# permit tcp any host 201.202.203.204 eq 25
Router(config-ext-nacl)# permit tcp any host 201.202.203.204 eq 110
Router(config-ext-nacl)# exit
Router(config)# interface FastEthernet0/0
Router(config-if)# ip access-group RuchWychodzacy out
Router(config-if)# exit
Router(config)# exit
```

Kolejne komendy konfiguracyjne oznaczają wejście w tryb konfiguracji, utworzenie rozszerzonej listy dostępu o nazwie `RuchWychodzacy`, zezwolenie na cały ruch wychodzący kierowany na port 80, zezwolenie na ruch wychodzący kierowany na port 25 serwera o adresie 201.202.203.204, zezwolenie na ruch wychodzący kierowany na port 110 serwera o adresie 201.202.203.204, opuszczenie konfiguracji listy dostępu, wejście w tryb konfiguracji interfejsu `FastEthernet 0/0`, przypisanie dla ruchu wychodzącego listy dostępu o nazwie `RuchWychodzacy`, opuszczenie trybu konfiguracji interfejsu, opuszczenie trybu konfiguracji.

8.5. Konfiguracja urządzeń bezprzewodowych

Najbardziej popularne urządzenia bezprzewodowe pozwalają na komunikację z siecią przy użyciu fal radiowych o częstotliwości 2,4 Ghz (w standardzie 802.11b, 802.11g oraz 802.11n) lub też 5 GHz (w standardzie 802.11a). Na infrastrukturę sieci bezprzewodowej składają się punkty dostępu (ang. *Access point*) z dołączanymi antenami oraz bezprzewodowe karty sieciowe montowane w urządzeniach. W segmencie urządzeń profesjonalnych występują dodatkowo kontrolery punktów dostępu (ang. *Access point controller*).

Sieci bezprzewodowe (ang. *Wireless Local Area Network* — WLAN) mogą pracować w dwóch trybach:

- w trybie ad hoc, w którym urządzenia łączą się bezpośrednio z sobą,
- w trybie infrastruktury, z wykorzystaniem punktów dostępowych (ang. *Access point*).

Punkt dostępowy to centralny punkt sieci bezprzewodowej. Przekazuje dane między urządzeniami, pozwala także na podłączenie sieci bezprzewodowej do sieci kablowej. Punkty dostępowe mają dwa interfejsy sieciowe: interfejs bezprzewodowy (gniazdo do podłączenia anteny) i interfejs sieci kablowej (najczęściej gniazdo RJ-45 do podłączenia sieci Ethernet).

Punkty dostępowe mogą komunikować się z sobą, co pozwala na budowę złożonej infrastruktury łączącej urządzenia znacznie od siebie oddalone.

8.5.1. Parametry konfiguracyjne urządzeń bezprzewodowych

Podstawowe parametry konfiguracyjne urządzeń dostępowych do sieci bezprzewodowych odnoszą się do nazwy sieci oraz opcjonalnych zabezpieczeń:

- Identyfikator sieci bezprzewodowej (ang. *Service Set IDentifier* — SSID) — nazwa sieci bezprzewodowej; urządzenia, które mają pracować w jednej sieci, muszą mieć ten sam identyfikator sieci.
- Rozgłaszanie identyfikatora sieci (ang. *SSID Broadcast*) — ustawienie pozwalające ukryć sieć bezprzewodową — nie będzie ona widoczna podczas przeglądania

dostępnych sieci WLAN, dostęp do niej będzie możliwy po wpisaniu jej nazwy. Do zmiany tych ustawień odnoszą się także ukrycie sieci (*Hide WLAN*) lub ukrycie punktu dostępu (*Hide Access Point*).

- Kanał działania sieci (ang. *channel*) — ustawienia pozwalające wybrać konkretny kanał transmisji — w obrębie wybranego zakresu częstotliwości jest wyodrębnionych kilkanaście kanałów (w Polsce jest to 13 kanałów). Ich wydzielanie ma za zadanie umożliwienie funkcjonowania na jednym obszarze kilku sieci bezprzewodowych działających w tym samym zakresie częstotliwości. Często ustawienia kanału są wybierane automatycznie, użytkownik musi określić tylko kraj, w którym działa urządzenie, gdyż kanały transmisji mogą się różnić w zależności od terytorium.
- Rodzaj zabezpieczenia sieci (*Network Autentication*) — ustawienie pozwalające określić sposób szyfrowania danych.
- Hasła dostępu do sieci.

Urządzenia bezprzewodowe mogą pracować bez szyfrowania danych (tryb niezalecany ze względów bezpieczeństwa) lub w jednym z następujących trybów szyfrowania danych:

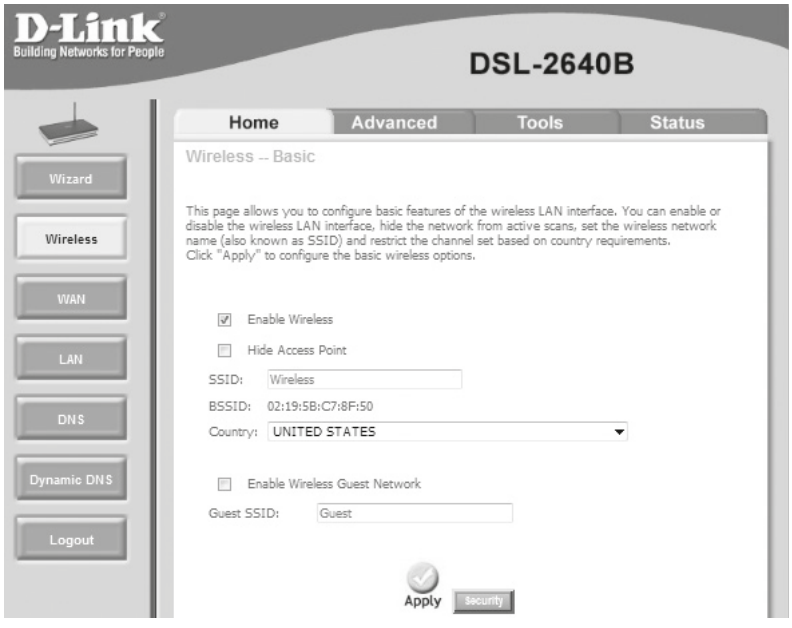
- WEP (ang. *Wired Equivalent Privacy*) — tryb pozwalający na używanie kluczy 64-bitowych lub 128-bitowych. Szyfrowanie WEP zostało złamane i nie jest uznawane za bezpieczne.
- WPA (ang. *WiFi Protected Access*) — zabezpieczenie wykorzystujące cykliczne zmiany klucza szyfrującego podczas transmisji; może działać w dwóch trybach: *Enterprise* (klucze są przydzielane przez serwer Radius dla każdego użytkownika sieci) lub *Personal* (wszyscy użytkownicy sieci korzystają z dzielonego klucza — ang. *Pre-Shared Key* — PSK).
- WPA2 — poprawiona wersja protokołu WPA, zalecana do zabezpieczeń sieci bezprzewodowych.

Konfiguracja urządzeń bezprzewodowych została przedstawiona na przykładzie wcześniej omawianego routera DSL-2640B firmy D-Link. Urządzenie to jest nazywane routerem bezprzewodowym. Oznacza to, że jest to router z wbudowanym punktem dostępu — interfejsem dla sieci bezprzewodowej. Dodatkowo została przedstawiona konfiguracja bezprzewodowej karty sieciowej zainstalowanej w systemie Windows w celu podłączenia do sieci WiFi.

8.5.2. Konfiguracja sieci bezprzewodowej

Ustawienie parametrów sieci bezprzewodowej jest dostępne na głównej stronie panelu konfiguracyjnego po wybraniu opcji *Wireless* z lewego menu.

Na głównej stronie konfiguracji interfejsu bezprzewodowego (rysunek 8.19) znajduje się opcja uruchomienia sieci bezprzewodowej (*Enable Wireless*), ukrycia rozgłaszania nazwy sieci (*Hide Access Point*), ustawienia identyfikatora sieci (*SSID*), a także wskazania kraju, w którym działa urządzenie, w celu poprawnego przypisania kanałów (*Country*).



Rysunek 8.19. Konfiguracja interfejsu bezprzewodowego

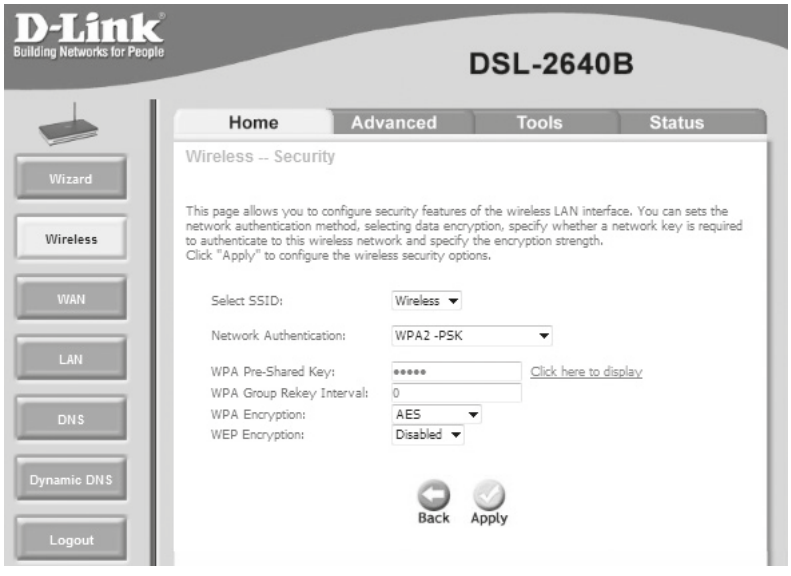
Wybrane urządzenie pozwala na skonfigurowanie dodatkowej — gościnnej — sieci WiFi (*Enable Wireless Guest Network*). Jest to niezależna sieć bezprzewodowa zapewniająca dostęp do intenetu, bez zabezpieczeń i możliwości połączenia do głównej — wcześniej skonfigurowanej sieci.

Konfiguracja zabezpieczeń sieci WiFi jest dostępna poprzez wybór opcji *Security* (rysunek 8.20). Pozwala ona ustawić rodzaj zabezpieczeń oraz ich parametry: klucz dla szyfrowania WEP, natomiast dla szyfrowania WPA i WPA2 należy wskazać klucz lub adres serwera Radius oraz rodzaj kodowania stosowanego przy zabezpieczeniach (TKIP, silniejsze AES oraz TKIP+AES).

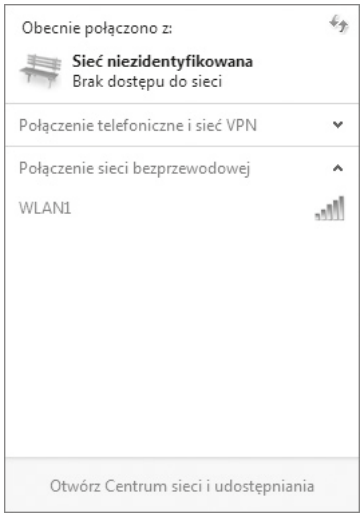
Aby uruchomić sieć bezprzewodową w systemie Windows 7, należy poprawnie zainstalować kartę sieciową oraz odpowiednio ustawić niezbędne parametry — nazwę sieci, do której użytkownik ma zostać podłączony (wybrać, jeśli jest rozgłaszana, lub wpisać, jeżeli jest ukryta), oraz hasło dostępu do sieci i skonfigurować protokół IP.

Aby podłączyć komputer do sieci bezprzewodowej, należy w Panelu sterowania wybrać *Sieć i internet/Centrum sieci i udostępniania*, a następnie wskazać opcję *Połącz lub rozłącz* lub wybrać w obszarze powiadamiania paska zadań (w prawym dolnym rogu obok zegara) ikonę  .

Wyświetlona zostanie lista dostępnych połączeń sieciowych, na której są widoczne działające i dostępne połączenia sieciowe (rysunek 8.21). W obszarze *Połączenia sieci bezprzewodowych* są wyświetlane wszystkie sieci WLAN, które rozgłaszają swoje nazwy.

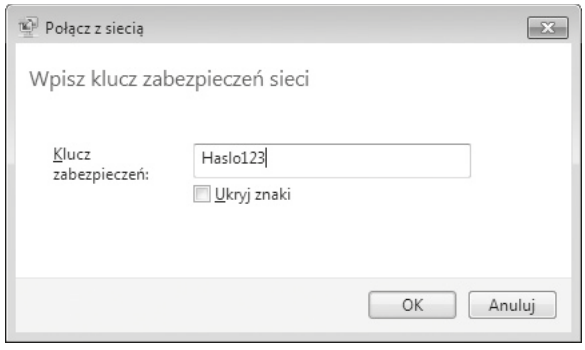


Rysunek 8.20. Konfiguracja zabezpieczeń sieci



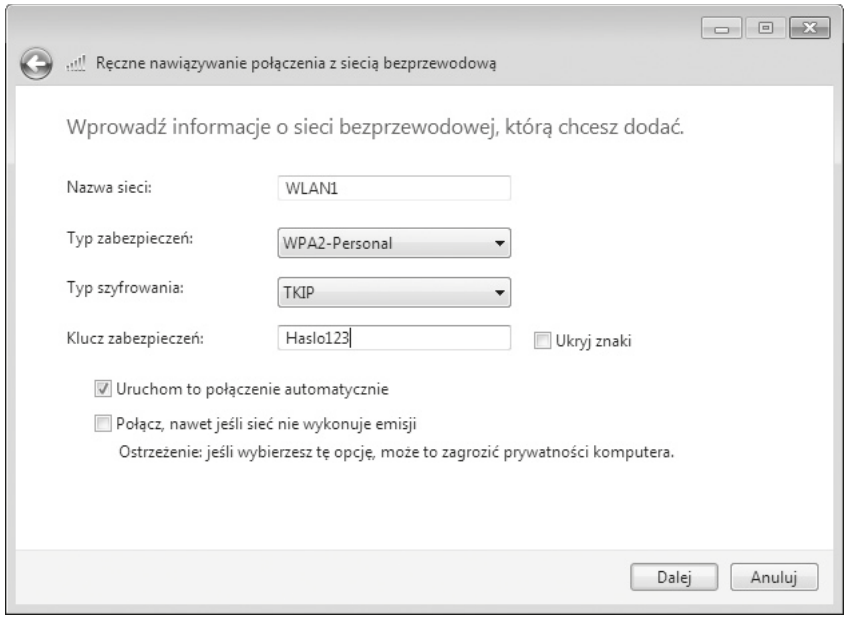
Rysunek 8.21. Okno dostępnych połączeń sieciowych

Po kliknięciu nazwy wybranej sieci pojawi się przycisk *Połącz*. Kliknięcie go automatycznie uruchomi połączenie sieciowe. Jeśli dostęp do sieci jest zabezpieczony, pojawi się monit o hasło dostępu do sieci (rysunek 8.22).



Rysunek 8.22. Monit o hasło dostępu do sieci bezprzewodowej

W przypadku gdy sieć nie rozgłasza swojej nazwy, nie pojawia się ona na liście dostępnych połączeń sieciowych. Aby podłączyć się do takiej sieci, należy w Panelu sterowania wybrać *Sieć i internet/Centrum sieci i udostępniania/Zarządzaj sieciami bezprzewodowymi*, a następnie przycisk *Dodaj*. W nowym oknie zostanie uruchomiony kreator dostępu do sieci bezprzewodowej, w którym należy wybrać opcję *Ręcznie utwórz profil sieciowy*, a następnie podać kryty identyfikator sieci, typ zabezpieczeń i rodzaj szyfrowania oraz klucz (rysunek 8.23).



Rysunek 8.23. Ręczne tworzenie profilu sieci bezprzewodowej

8.6. Konfiguracja usług telefonii internetowej (VoIP)

Telefonia internetowa, inaczej zwana VoIP (ang. *Voice over Internet Protocol*), pozwala na przesyłanie głosu przez sieć cyfrową działającą w oparciu o protokół IP. Standardowa telefonia umożliwia transmisję danych w postaci analogowej, przez co dane te potrzebują większej przepustowości łącza, a dodatkowo jakość tego rodzaju połączeń jest niższa niż w przypadku komunikacji cyfrowej.

Operatorzy VoIP oferują szereg usług pozwalających na wykorzystanie telefonii internetowej nie tylko do przesyłania rozmów pomiędzy komputerami, ale również na wykonywanie połączeń do publicznej sieci telefonicznej (ang. *Public Switched Telephone Network* — PSTN), wysyłanie i odbieranie faksów czy pozyskanie standardowego numeru telefonu z dowolnej strefy numeracyjnej.

8.6.1. Parametry konfiguracyjne VoIP

Technologia VoIP do komunikacji wykorzystuje protokół SIP (ang. *Session Initiation Protocol*), który jest odpowiedzialny za ustanawianie i kończenie połączeń. Jest to protokół warstwy aplikacji oparty na języku HTML.

Na sieć SIP składają się następujące elementy:

- Terminal końcowy — Agent SIP; może nim być telefon IP, telefon analogowy podłączony do bramki VoIP (*VoIP gateway*) lub aplikacja obsługująca protokół SIP.
- Serwer Proxy SIP — kieruje połączeniami pomiędzy rozmówcami. Jego adres musi być skonfigurowany na terminalu końcowym w celu nawiązywania połączeń. Pozwala nawiązywać połączenia z innymi terminalami końcowymi oraz numerami publicznej sieci telefonicznej.
- Serwer przekierowań (ang. *redirect server*) — zwraca adres odbiorcy rozmowy lub adres serwera proxy protokołu SIP, do którego rozmówca jest podłączony.
- Serwer rejestracji SIP — dokonuje mapowania nazw użytkowników SIP na adresy serwerów proxy, dla których są one dostępne.

Komunikacja w sieciach VoIP polega na przesyłaniu za pomocą protokołu RTP (ang. *Real-time Transport Protocol*) zakodowanego i często również skompresowanego dźwięku. Za kodowanie dźwięku do postaci cyfrowej odpowiedzialne są tzw. kodeki (ang. *codec*). Ich użycie zależy od dostawcy usług telefonii internetowej — na ogół sieci pozwalają na używanie kilku z nich w zależności od możliwości łącza internetowego oraz oczekiwanej jakości połączenia. Tabela 8.2 prezentuje zestawienie używanych w technologii VoIP kodeków — jak wynika z zawartych danych, im lepsza jakość połączenia, tym większa jego wymagana przepustowość.

Tabela 8.2. Zestawienie kodeków VoIP wraz z parametrami

Nazwa kodeka	Próbkowanie	Częstotliwość wysyłania pakietów z dźwiękiem	Wymagana przepustowość
G.711u	64,0 kbit/s	20 ms	87,2 kbit/s
G.711a	64,0 kbit/s	20 ms	87,2 kbit/s
G.726-32	32,0 kbit/s	20 ms	55,2 kbit/s
iLBC	15,0 kbit/s	20 ms	37,5 kbit/s
GSM	13,0 kbit/s	20 ms	32,5 kbit/s
G.729	8,0 kbit/s	20 ms	31,2 kbit/s
G.723.1 MPMLQ	6,3 kbit/s	30 ms	21,9 kbit/s
G.723.1 ACELP	5,3 kbit/s	30 ms	20,8 kbit/s

Dostęp do sieci VoIP powinien być skonfigurowany na terminalu końcowym, którym może być komputer z odpowiednim oprogramowaniem (ang. *softphone*), telefon IP lub bramka VoIP (urządzenie pozwalające na podłączenie sieci VoIP poprzez port RJ-45, telefonów analogowych przez porty RJ-11).

W celu uruchomienia telefonii internetowej jest wymagana konfiguracja protokołu SIP (nazwa serwera proxy, nazwa użytkownika SIP, nazwa domeny SIP, hasło dostępu) oraz wybranie kodeków dostępnych w sieci, do której jest podłączane urządzenie.

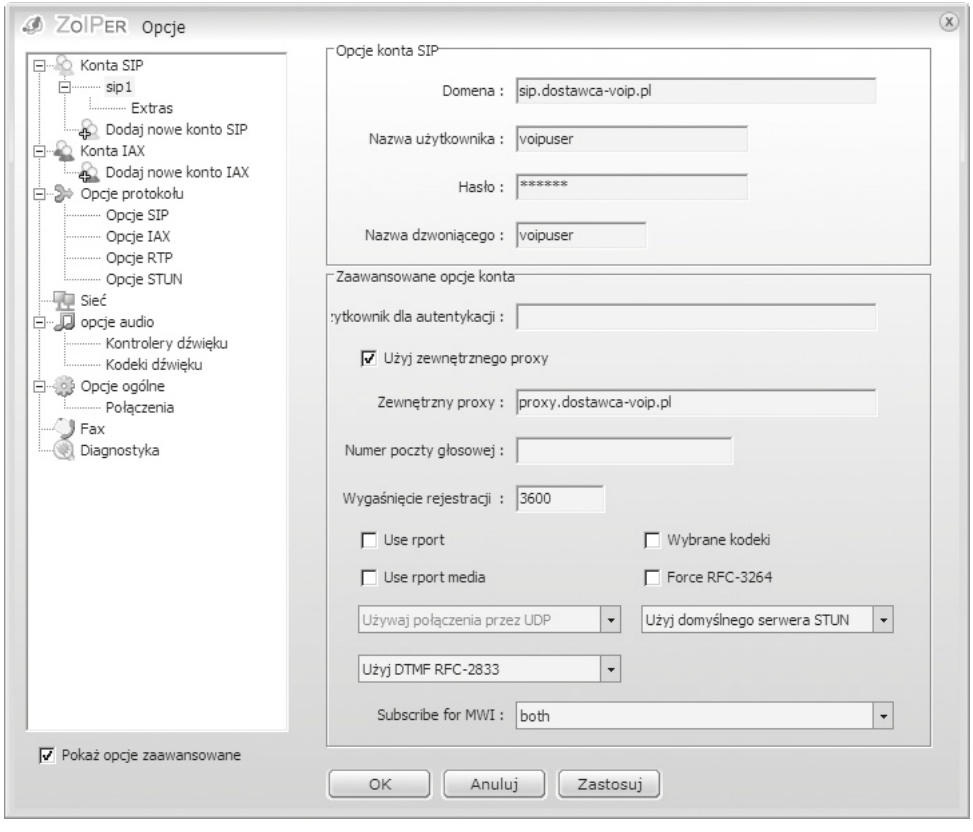
8.6.2. Konfiguracja oprogramowania — klienta SIP

Konfiguracja oprogramowania do komunikacji VoIP przy użyciu protokołu SIP została przedstawiona na przykładzie programu *ZoIPer (www.zoiper.com)*. Parametry protokołu SIP powinny zostać dostarczone przez dostawcę usług.

Domyślnie program instaluje się w języku angielskim. Aby to zmienić, należy kliknąć prawym przyciskiem myszy ikonę programu, a następnie wybrać *Language/Polski*.

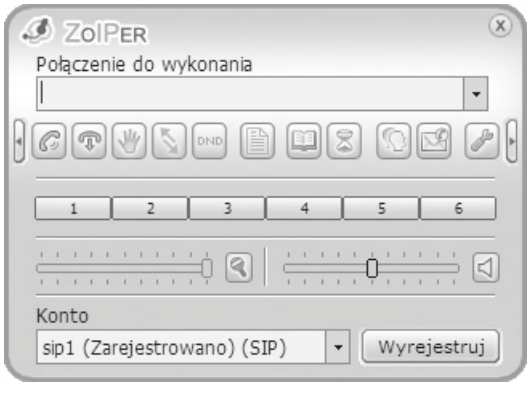
Żeby podłączyć oprogramowanie do sieci SIP, należy w głównym oknie programu wybrać ikonę *Opcje*, a następnie *Dodaj nowe konto SIP*, po czym wybrać nazwę profilu połączenia — po wykonaniu tych kroków na liście kont SIP pojawi się nowa pozycja. Po jej wskazaniu zostanie wyświetlone okno konfiguracji parametrów dla wybranego konta SIP (rysunek 8.24).

Podstawowe parametry konfiguracji to domena, nazwa użytkownika oraz hasło. Przełącznik *Pokaż opcje zaawansowane* pozwala na ustawienie dodatkowych parametrów połączenia, które mogą być wymagane przez dostawcę usług (m.in. często wymagany parametr *Zewnętrzny proxy*).



Rysunek 8.24. Konfiguracja połączenia SIP w programie ZoIPer

Po poprawnym skonfigurowaniu usługi istnieje możliwość korzystania z telefonii internetowej. Aby wybrać połączenie, należy w głównym oknie programu (rysunek 8.25) wprowadzić numer telefonu lub nazwę użytkownika SIP osoby, z którą ma być nawiązane połączenie, a następnie wybrać ikonę oznaczoną zieloną słuchawką.



Rysunek 8.25. Główne okno programu ZoIPer

Aby możliwe było odbieranie połączeń przychodzących z publicznej sieci telefonicznej, konto SIP na serwerze powinno być odpowiednio skonfigurowane przez dostawcę usług VoIP (przypisany publiczny numer z sieci PSTN).

8.6.3. Konfiguracja bramki VoIP

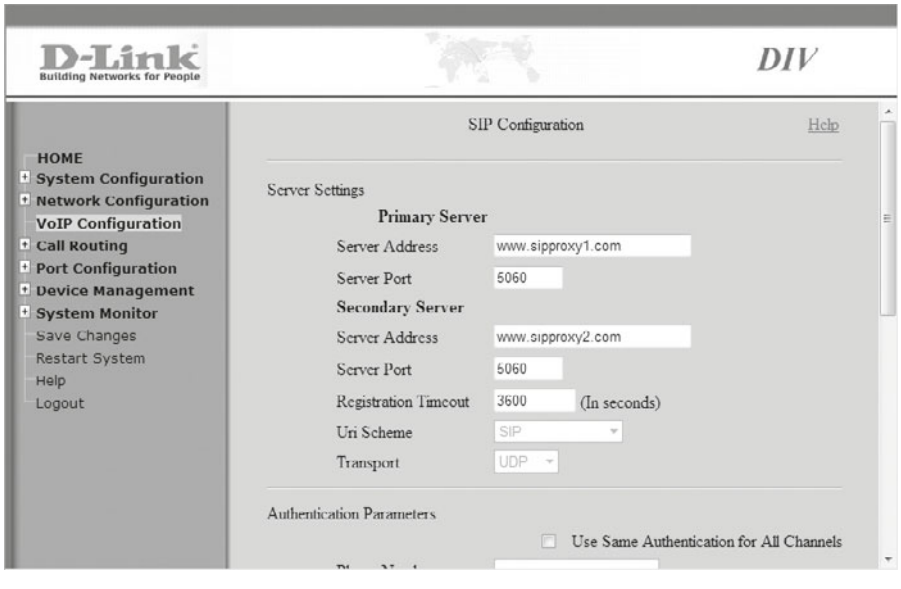
Przykładowa konfiguracja bramki VoIP została przedstawiona na przykładzie bramki DIV-140 firmy D-Link. Jest to urządzenie pozwalające na podłączenie 4 telefonów analogowych i skonfigurowanie dla każdego z nich niezależnego połączenia SIP. Dodatkowe funkcje urządzenia pozwalają na grupowanie numerów telefonicznych, do których może być równocześnie kierowane połączenie, a także automatycznych przekierowań połączeń, książki adresowej czy szybkich połączeń pod wybranymi numerami telefonicznymi.

Domyślnie panel konfiguracyjny urządzenia jest dostępny pod adresem 10.0.0.1 jedynie przez protokół HTTPS przy użyciu nazwy użytkownika *admin* oraz hasła *password*.

Okno konfiguracji jest podzielone na dwie części — po lewej stronie znajduje się menu pozwalające wybrać grupę parametrów konfiguracyjnych, których edycja będzie się odbywać w głównej części okna.

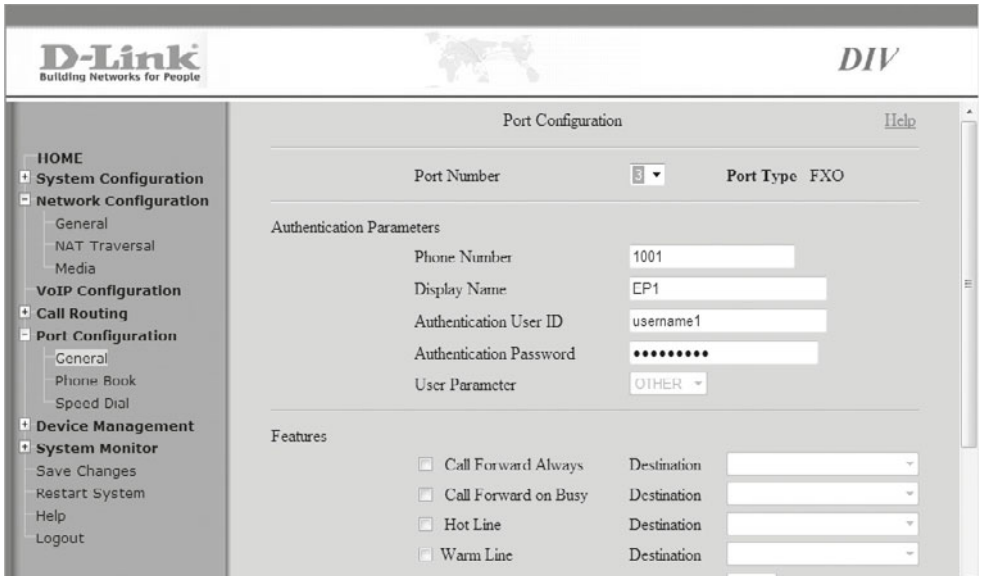
Konfiguracja adresacji IP i sposobu podłączenia do sieci lokalnej jest możliwa za pośrednictwem menu *Network Configuration/General*.

Podstawowe ustawienia SIP są dostępne w menu *VoIP Configuration* — można ustawić adresy serwerów SIP oraz porty, na których działają. Dodatkowo istnieje możliwość ustawienia wspólnej autentykacji dla poszczególnych usług SIP (rysunek 8.26).



Rysunek 8.26. Konfiguracja adresów serwerów SIP

Konfiguracja parametrów poszczególnych portów telefonicznych jest dostępna w menu *Port Configuration/General* (rysunek 8.27).



Rysunek 8.27. Konfiguracja ustawień portu telefonicznego

Parametry dla poszczególnych portów pozwalają na ustawienie numerów wewnętrznych dostępnych z pozostałych linii, autentykacji dla protokołu SIP oraz przekierowań połączeń (zawsze gdy zajęte, po określonej liczbie sygnałów dzwonka).

Po zapisaniu ustawień dla wybranego portu telefon podłączony do niego może korzystać z usług dostawcy VoIP. Aby poszczególne linie były dostępne przez numery publicznej sieci telefonicznej, trzeba je przypisać do poszczególnych kont użytkowników SIP przez dostawcę usług.

8.7. Monitoring sieci i urządzeń sieciowych

Ważnym elementem zarządzania siecią komputerową jest bieżący monitoring jej działania. Pozwala on na wczesne wykrycie nieprawidłowości i przywrócenie sieci do właściwego stanu, co umożliwia zapobieganie awariom. W zależności od rodzaju sieci i oczekiwanej dostępności usług sieciowych monitorowane są różne aspekty jej funkcjonowania, takie jak:

- dostępność węzłów sieci,
- dostępność wybranych usług sieciowych,
- obciążenie łączy internetowych,
- obciążenie serwerów sieciowych,
- zdarzenia na urządzeniach sieciowych (np. wyłączenie interfejsu sieciowego, zmiana trasy routingu) i serwerach (np. wyłączenie usługi, próba logowania).

Dodatkowo w dużych serwerowniach monitoruje się również infrastrukturę powiązaną z sieciami, np. napięcie w urządzeniach UPS czy działanie klimatyzacji w serwerowni.

Termin monitoring sieci może wiązać się również z monitorowaniem przesyłanych przez sieć danych w celu ich analizy (np. próby włamań, wyciek danych itp.).

8.7.1. Monitoring działania sieci — program NetTools Professional

Dostępnych jest wiele programów pozwalających na monitoring działania sieci — zarówno w wersji komercyjnej, jak i bezpłatnej; mogą one działać na różnych platformach.

Dla systemów Linux jednym z najpopularniejszych programów do monitoringu jest rozpowszechniany na licencji GPL **Nagios**, który pozwala na monitorowanie dostępności węzłów sieciowych, usług sieciowych działających w sieci, a także użycia zasobów systemowych na serwerach. W przypadku wykrycia nieprawidłowości system może wysłać powiadomienie za pomocą poczty elektronicznej lub wiadomości SMS.

Dla systemu Windows również istnieje szereg programów do monitoringu sieci. Do zaprezentowania działania tego rodzaju aplikacji zostało wybrane oprogramowanie **NetTools Professional** firmy **Axence** (*www.axencesoftware.com*). Jest to pakiet oprogramowania pozwalający na monitoring dostępności urządzeń sieciowych wraz z powiadamianiem, a także na weryfikowanie usług działających na określonych serwerach, skanowanie sieci w celu wykrycia uruchomionych urządzeń czy przeglądanie bazy SNMP.

Na główne okno programu NetTools Professional składa się górny pasek nawigacji, który pozwala na uruchomienie wybranego narzędzia do monitoringu, pasek adresu, w którym podawany jest adres IP lub nazwa urządzenia, jakie ma zostać zdiagnozowane, oraz główny obszar roboczy zależny od wybranego narzędzia.

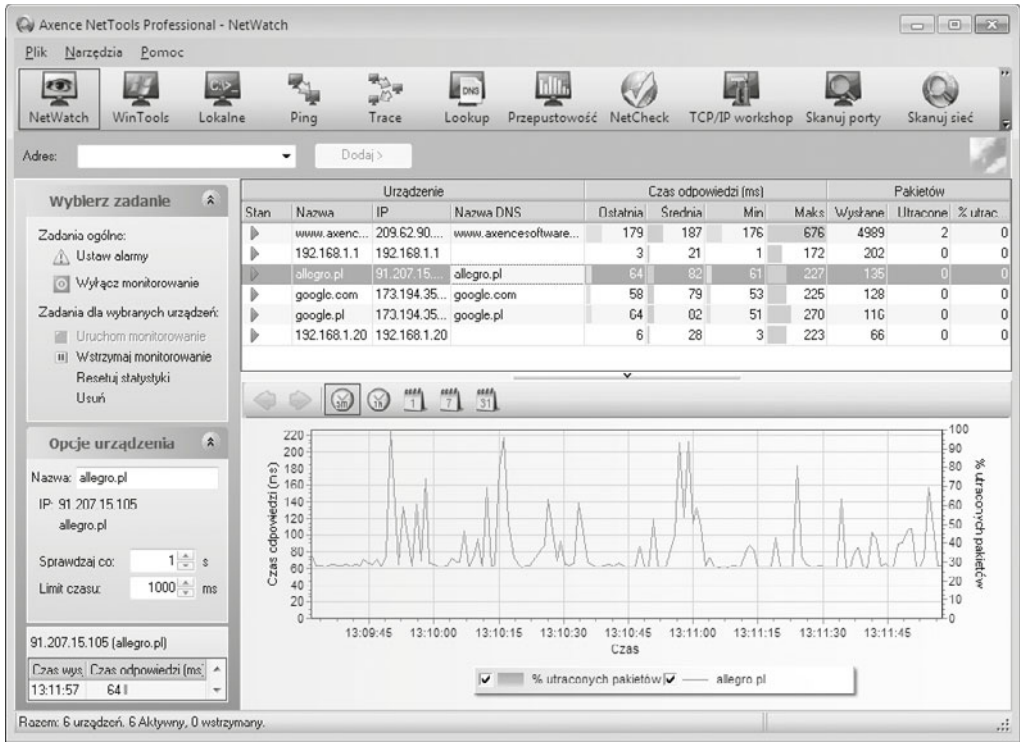
Narzędzie *NetWatch* pozwala na monitorowanie dostępności wybranego urządzenia (rysunek 8.28). Aby rozpocząć monitorowanie, należy w pasku adresu podać nazwę lub adres IP urządzenia, a następnie kliknąć przycisk *Dodaj*.

Parametry monitorowania — limit czasu na odpowiedź oraz częstotliwość wysyłania zapytań — mogą być ustawione w obszarze *Opcje urządzenia*.

Monitoring dostępności na bieżąco aktualizuje dane w głównej tabeli: nazwę DNS i adres IP, czasy odpowiedzi (min/max/średni), a także liczbę pakietów wysłanych i utraconych.

Na głównym wykresie poniżej tabeli można zobaczyć czasy odpowiedzi oraz procent utraconych pakietów w wybranym czasie. Aby wyświetlić dane historyczne w różnych okresach czasu (np. ostatnie 5 minut, godzina, dzień, tydzień, miesiąc), należy wybrać dany okres czasu, klikając odpowiadającą mu ikonę na pasku narzędziowym wykresu.

Aby ustawić parametry powiadamiania o występujących problemach z dostępnością, należy wybrać opcję *Ustaw alarmy* (rysunek 8.28), gdzie istnieje możliwość wskazania warunków oraz sposobu powiadamiania.



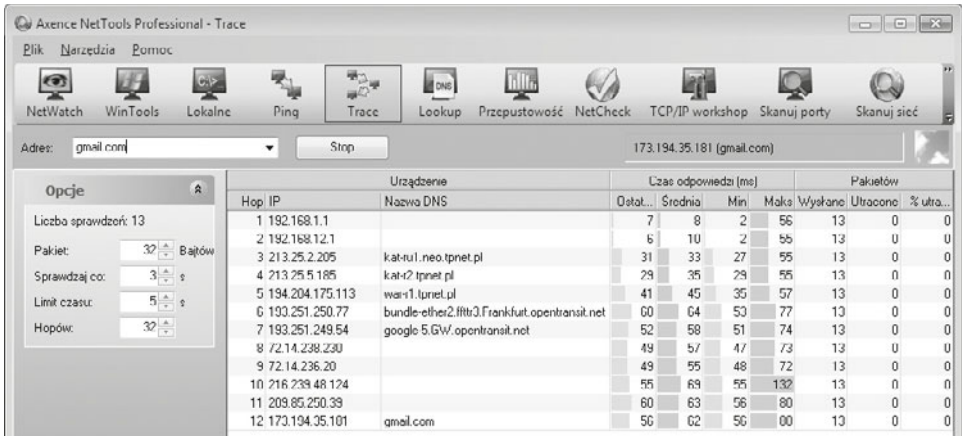
Rysunek 8.28. Monitorowanie dostępności urządzeń sieciowych

Narzędzie *WinTools* pozwala odczytywać informacje udostępniane przez usługę WMI (ang. *Windows Management Instrumentation*), która umożliwia zarządzanie zasobami komputerów pracujących w systemie Windows, takimi jak dostępne usługi, informacje o dyskach, zapisy w dziennikach systemowych itp.

Narzędzie *Lokalne* przedstawia informacje dotyczące sieci na lokalnym komputerze (m.in. tabelę adresów IP, tabelę ARP, tabelę routingu, otwarte porty, dane o kartach sieciowych, statystyki dla TCP/UDP i ICMP).

Narzędzie *Ping* pozwala na wizualną prezentację wyników działania komendy `ping`, dodatkowo zawiera 5-minutową historię, dzięki czemu można zaobserwować zmiany w dostępie do wybranego komputera czy urządzenia.

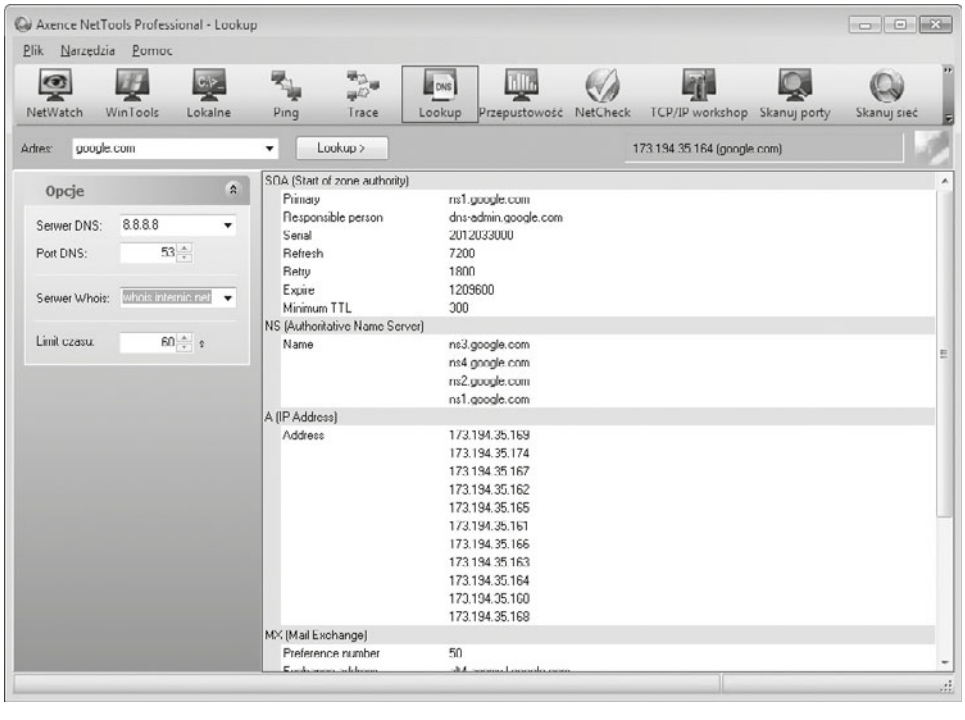
Trace to narzędzie prezentujące kolejne routery na trasie wędrówki pakietu IP do adresu docelowego (rysunek 8.29). Dodatkowo są podawane czasy odpowiedzi oraz liczba pakietów utraconych, co pozwala określić miejsce powstawania zatorów w sieci, dzięki lokalizacji wolno działających lub przeciążonych routerów. Jest to odpowiednik polecenia `tracert` w systemie Windows.



Rysunek 8.29. Narzędzie trace

Narzędzie *Lookup* pozwala na zbadanie rekordów DNS określonej domeny. Działa podobnie jak komenda `nslookup` systemu Windows, przy czym automatycznie podaje wszystkie wpisy dotyczące wybranej domeny oraz informację z bazy WHOIS, która zawiera dodatkowe dane o domenie, takie jak właściciel, dane kontaktowe, czas wygaśnięcia itp.

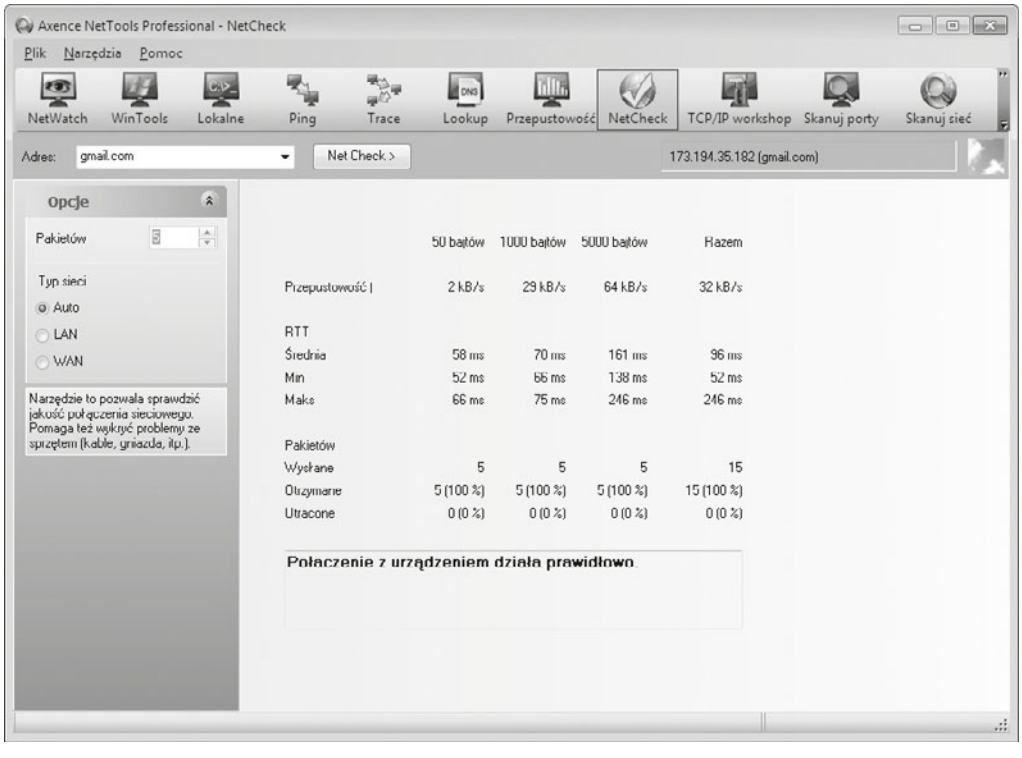
Rysunek 8.30 przedstawia wynik działania narzędzia *Lookup* dla domeny *google.com*.



Rysunek 8.30. Wynik działania narzędzia nslookup

Prędkość łącza pozwala zbadać narzędzie *Przepustowość*. Wysyła ono określoną wielkość danych pod wskazany adres i bada czas odpowiedzi, co pozwala na oszacowanie przepustowości łącza.

Narzędzie *NetCheck* pozwala na sprawdzenie jakości połączenia z wybranym urządzeniem — za pomocą transmisji różnej wielkości pakietów sprawdzana jest dostępność i parametry połączenia (rysunek 8.31).

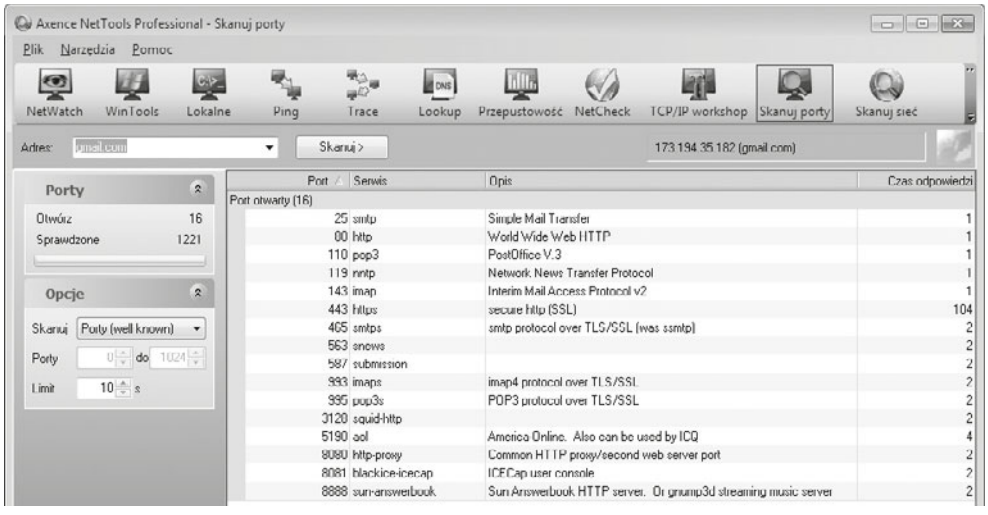


Rysunek 8.31. Wynik działania narzędzia NetCheck

TCP/IP workshop to narzędzie pozwalające na nawiązanie bezpośredniego połączenia z wybranym portem TCP/UDP. Narzędzie pozwala tworzyć i wysyłać zapytania kierowane bezpośrednio na wybrany port oraz śledzić odpowiedzi przekazywane przez serwer.

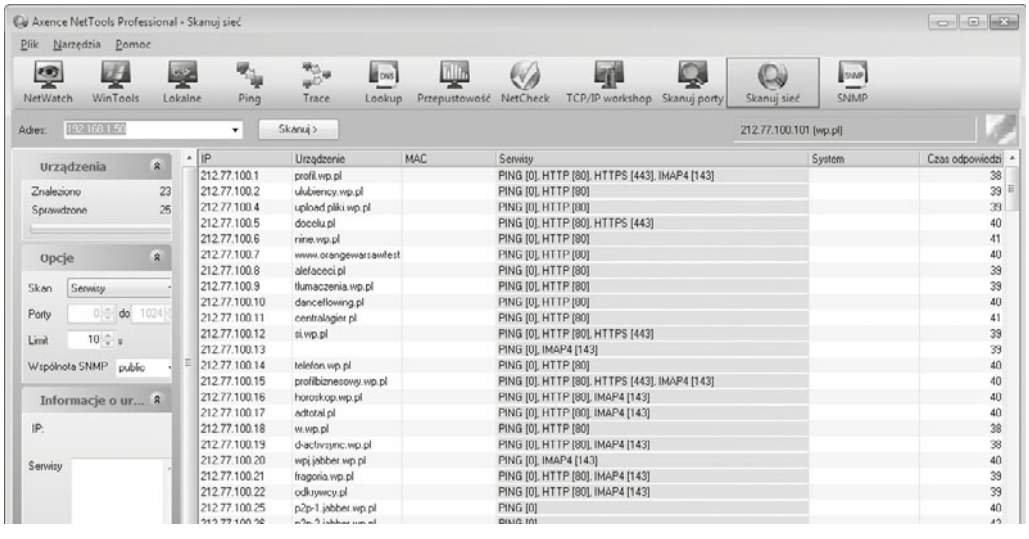
Dodatkowo istnieje też możliwość uruchomienia nasłuchiwania na wybranym porcie i kontroli zapytań otrzymywanych od innych urządzeń sieciowych.

Narzędzie *Skanuj porty* pozwala na sprawdzenie dostępnych usług (portów nasłuchujących) na wskazanym urządzeniu. Narzędzie umożliwia wybranie zakresu skanowanych portów oraz określenie limitu czasu na odpowiedź. Wyniki działania skanowania portów zostały przedstawione na rysunku 8.32.



Rysunek 8.32. Wynik działania narzędzia Skanuj porty

Narzędzie *Skaner sieci* pozwala na skanowanie urządzeń działających w wybranej sieci. Po podaniu adresu narzędzie za pomocą polecenia ping sprawdza dostępność wszystkich urządzeń pracujących w sieci, do której należy podany adres. Dodatkowo użytkownik ma możliwość skanowania portów na wszystkich komputerach, co pozwala na łatwe zdiagnozowanie usług działających w obrębie całej sieci. Wynik działania skanera sieci został przedstawiony na rysunku 8.33.



Rysunek 8.33. Wynik działania narzędzia Skaner sieci

Ostatnim narzędziem oferowanym przez pakiet NetTools Professional jest przeglądarka protokołu SNMP, która pozwala przeglądać dane udostępniane przez urządzenia sieciowe.

8.7.2. Monitoring i analiza transmitowanych danych — program Wireshark

Do analizy danych przesyłanych siecią niezbędny jest program pozwalający na ich przechwytywanie, czyli pobieranie i zapis w celu przetwarzania. Istnieje wiele programów, które spełniają tę funkcję. Są one nazywane snifferami (od ang. *sniffer*).

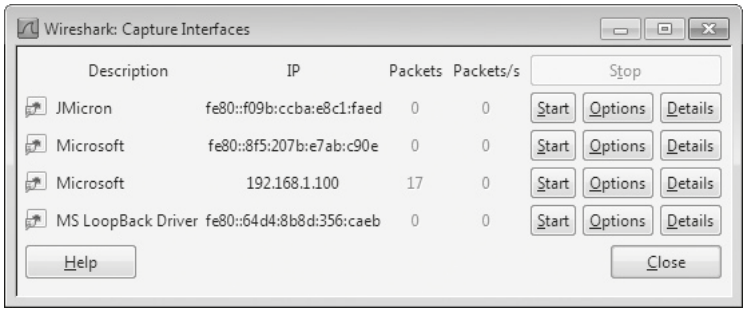
Sniffer to program, który zapisuje cały ruch krążący w sieci — zarówno dane właściwe bezpośrednio przetwarzane przez oprogramowanie, jak i dane służące do sterowania ruchem (np. potwierdzenia otrzymania pakietów, zapytania DNS czy nawiązywanie sesji szyfrowanej), które na ogół nie są dostępne dla użytkowników.

Przechwytywanie danych stosuje się zarówno do rozwiązywania problemów z siecią, analizy ruchu oraz danych, jak i w celu poznania zasad działania protokołów komunikacyjnych czy oprogramowania sieciowego — zapisane dane mogą być analizowane na wszystkich warstwach modelu OSI, co pozwala dokładnie zapoznać się z mechanizmem przygotowania danych do transmisji.

Użycie programu typu sniffer zostało przedstawione na przykładzie programu Wireshark (*http://www.wireshark.org/*) rozpowszechnianego na licencji GNU GPL2.

Należy zwrócić uwagę, że przechwytywanie w sieciach zbudowanych z wykorzystaniem przełączników jest możliwe jedynie dla danych wysyłanych przez komputer użytkownika oraz adresowanych do tego komputera, a także danych kierowanych do wszystkich w danej sieci (ang. *broadcast*). Aby możliwe było przechwytywanie danych ze wszystkich urządzeń sieciowych, powinny być one podłączone do koncentratora lub do przełącznika pozwalającego na uruchomienie usługi port mirroring. Gdy chce się analizować ruch sieciowy kierowany do internetu, należy podłączyć koncentrator pomiędzy przełącznik a interfejs routera.

Aby rozpocząć pobieranie ruchu sieciowego, należy wskazać interfejs sieciowy, z którego dane mają być pobierane, i opcjonalnie ustawić parametry pobierania, takie jak filtry dotyczące zapisywanego ruchu, czas zapisu lub ilość zapisanych danych, rozpoznawanie nazw itp. Wybór interfejsu do pobierania danych odbywa się w menu *Capture Interfaces* (rysunek 8.34).

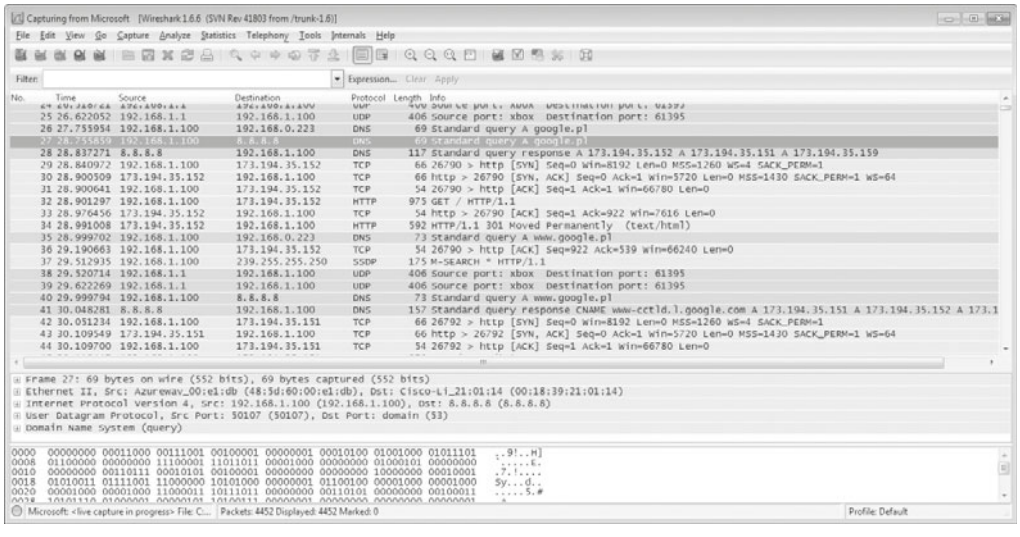


Rysunek 8.34. Wybór interfejsu do pobierania danych

Po kliknięciu opcji *Start* rozpocznie się zapisywanie ruchu sieciowego zgodnie z ustalonymi opcjami. W głównym oknie programu zostanie wyświetlona tabela z informacją o pobranych pakietach (rysunek 8.35). Standardowo wyświetlane są: kolejny numer pobranego pakietu, czas, adres źródłowy, adres docelowy, protokół, wielkość danych oraz informacja o pobranych danych.

WSKAZÓWKA

Aby uświadomić sobie, jak wiele pakietów jest transmitowanych w sieci, warto rozpocząć pobieranie ruchu bez żadnych ograniczeń i uruchomić przeglądarkę internetową lub klienta poczty elektronicznej.



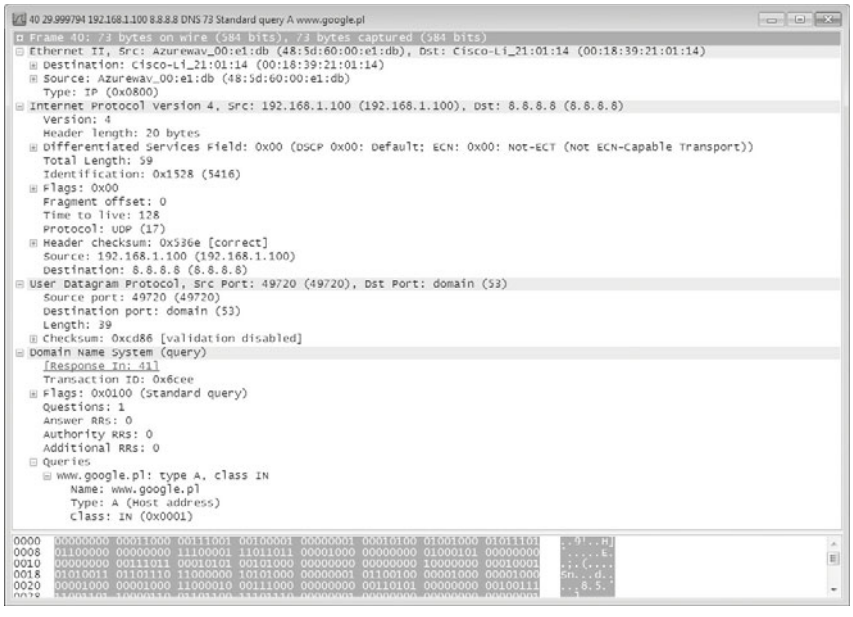
Rysunek 8.35. Pobieranie danych

Pod tabelą są wyświetlane informacje dotyczące transmisji danych w różnych warstwach modelu OSI, m.in.:

- bity w ramce dla warstwy fizycznej,
- źródłowy i docelowy adres MAC oraz rodzaj przesyłanych danych dla warstwy łącza danych,
- źródłowy i docelowy adres IP, suma kontrolna dla warstwy sieci,
- źródłowy i docelowy port dla warstwy transportowej,
- dane właściwe dla protokołu warstwy aplikacji.

Poniżej został zaprezentowany zapis binarny lub heksadecymalny transmitowanych danych.

Po dwukrotnym kliknięciu wybranego pakietu dane dotyczące transmisji oraz zapis binarny zostaną wyświetlone w nowym oknie. Na rysunku 8.36 zostało przedstawione



Rysunek 8.36. Analiza transmisji zapytania kierowanego do serwera DNS

przykładowe zapytanie kierowane z komputera o adresie 192.168.1.100 z portu 49720 do serwera DNS o adresie 8.8.8.8 na port 53 dotyczące nazwy *www.google.pl*.

Analiza transmisji danych została przedstawiona w sposób pozwalający zobrazować, jak ważne jest używanie w transmisji sieciowej połączeń szyfrowanych. Na przykładzie pobranych danych został przeanalizowany niezaszyfrowany ruch kierowany do serwera FTP, dzięki czemu możliwe jest odczytanie loginu i hasła przesyłanego nieszyfrowanym tekstem.

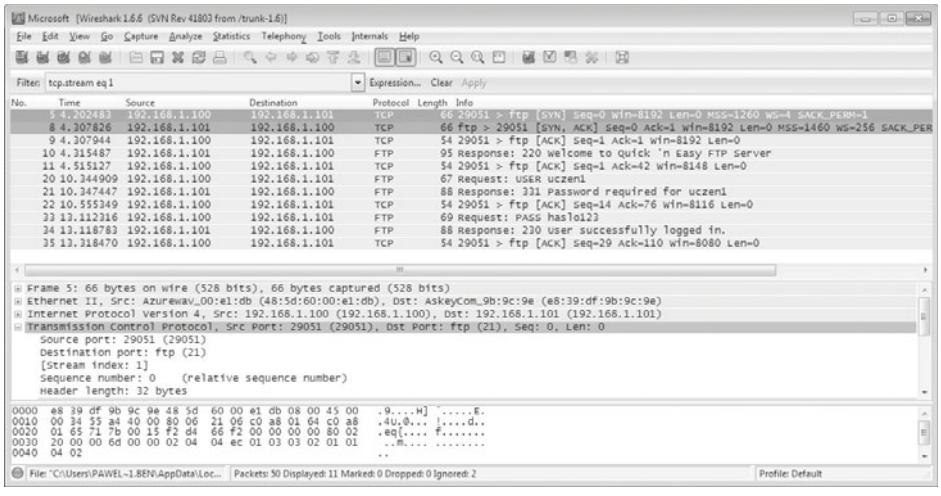
Aby rozpocząć analizę danych, należy uruchomić przechwytywanie danych, a następnie klienta usługi FTP, spróbować zalogować się do serwera i zatrzymać przechwytywanie danych.

Pobrane dane są zależne od ruchu generowanego przez aplikacje działające na komputerze oraz transmisje sieciowe. Aby wyświetlić jedynie transmisje związane z analizowanym ruchem, można użyć filtrów, podając nazwę konkretnego protokołu (FTP) lub klikając pakiet prawym przyciskiem myszy i wybierając opcję *Follow TCP Stream* — wówczas program automatycznie ustawi filtr na wszystkie pakiety związane z wybraną transmisją.

Przykładowa analiza transmisji dotyczyć będzie połączenia o następujących parametrach:

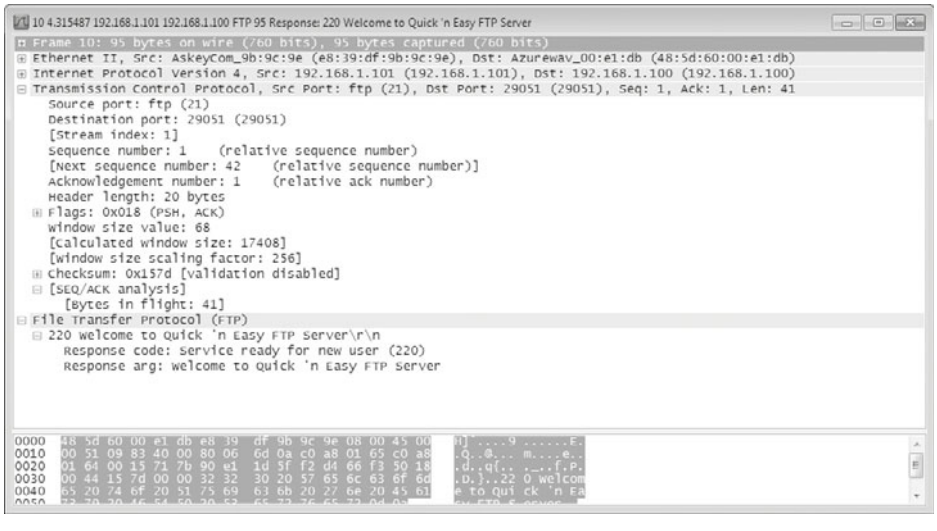
- Adres serwera FTP: 192.168.1.101
- Adres klienta FTP: 192.168.1.100
- Nazwa użytkownika FTP: uczen1
- Hasło użytkownika FTP: haslo123

W celu pełnej analizy zaleca się odnalezienie pierwszego pakietu kierowanego pod adres serwera FTP oraz wybranie opcji *Follow TCP Stream* (rysunek 8.37).



Rysunek 8.37. Analiza nawiązania połączenia do serwera FTP

Przeglądając dane wysyłane w kolejnych pakietach, można zaobserwować komunikaty, które są przesyłane pomiędzy klientem (lokalną aplikacją FTP) a serwerem (oprogramowaniem udostępniającym pliki). Pierwszy pakiet (nr 5) nawiązuje połączenie z portem 21 serwera, przesyłane są pakiety synchronizacji i potwierdzające odbiór danych i serwer wysyła powitanie (pakiet nr 10), które można obserwować w oknie programu klienckiego (rysunek 8.38).



Rysunek 8.38. Analiza protokołu FTP — zgłoszenie serwera

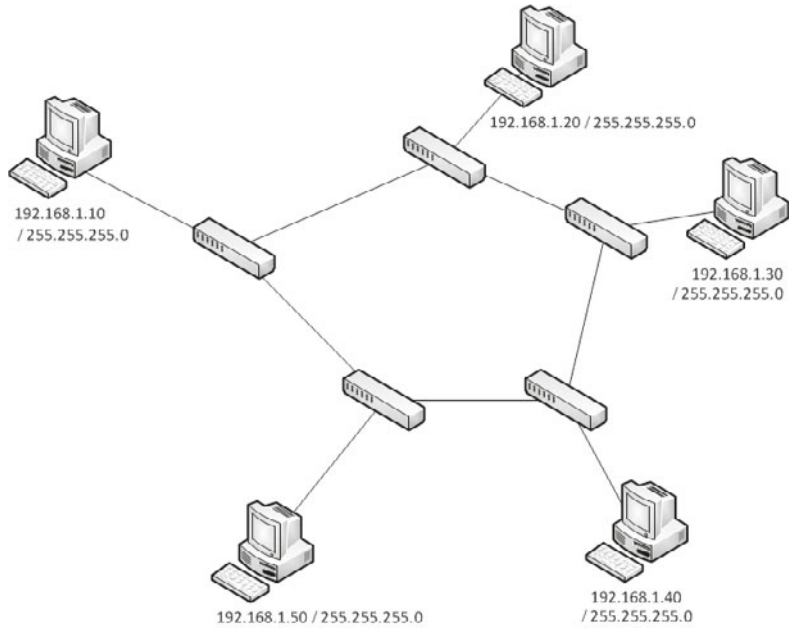
W pakiecie nr 20 klient FTP wysyła nazwę użytkownika — *Request: USER uczen1*, serwer FTP odpowiada (pakiet 21) prośbą o hasło — *Response: 331 Password required for uczen1*. Pakiet 33 — *Request: PASS haslo123* zawiera hasło użytkownika *uczen1*, na które serwer odpowiada pakietem 34 — *Response: 230 User successfully logged in*, co oznacza poprawne zalogowanie.

Analiza tych danych pokazuje, jak łatwo i w krótkim czasie można odczytać informacje transmitowane przez nieszyfrowane połączenia, takie jak FTP, telnet, POP3, SMTP czy HTTP.

Analizie danych mogą być poddane wszystkie protokoły, co pozwala sprawdzić, jakie dane są transmitowane, może być również przydatne podczas odzyskiwania haseł zapamiętanych w programach komputerowych, np. w kliencie poczty elektronicznej.

ĆWICZENIA

1. Sprawdź dostępne urządzenia sieci komputerowej. W jaki sposób można je skonfigurować? Zapoznaj się z ich dokumentacją.
2. Zbuduj sieć o topologii jak na rysunku 8.39. W konfiguracji przełączników wyłącz protokół STP. Sprawdź poprawność połączenia przy użyciu komendy `ping`. Czy pojawiają się problemy w transmisji? Wyjaśnij dlaczego.

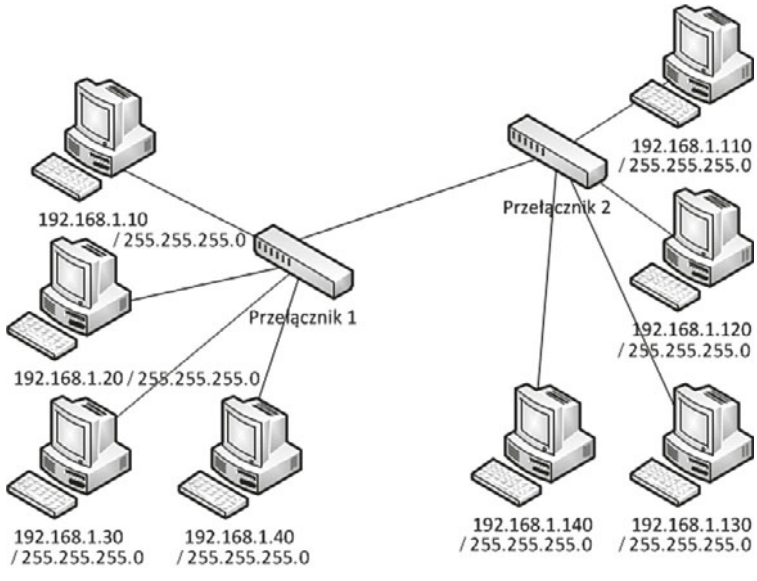


Rysunek 8.39. Topologia wykorzystująca przełączniki, zawierająca pętlę

ĆWICZENIA cd.

3. Zbuduj sieć na podstawie rysunku 8.39 z uruchomionym protokołem STP. Sprawdź poprawność połączenia pomiędzy komputerami 192.168.1.10 a 192.168.1.20 przy użyciu komendy ping. Jak zachowa się połączenie w przypadku rozłączenia go pomiędzy komputerami o adresach 192.168.1.10 oraz 192.168.1.20?

4. Zbuduj sieć o topologii jak na rysunku 8.40. Sprawdź dostępność połączeń pomiędzy poszczególnymi komputerami. Rozpocznij równoczesną transmisję dużych plików (powyżej 500 MB) pomiędzy komputerami 192.168.1.10 a 192.168.1.110, 192.168.1.20 a 192.168.1.120, 192.168.1.30 a 192.168.1.130 oraz 192.168.1.40 a 192.168.1.140. Sprawdź, jak w zależności od obciążenia spada wydajność łącza.



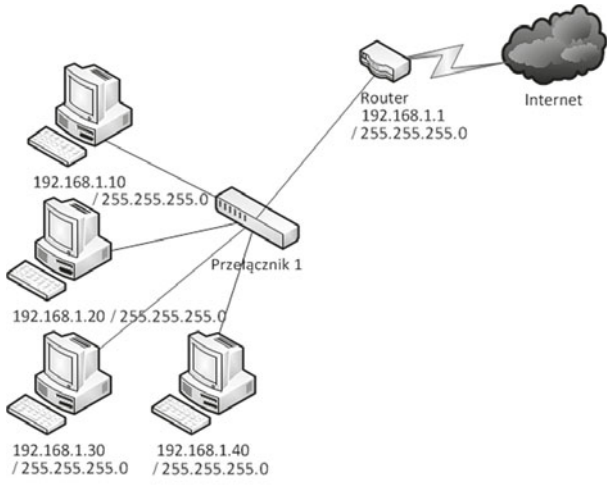
Rysunek 8.40. Topologia zbudowana z wykorzystaniem przełączników

5. W sieci zbudowanej na podstawie rysunku 8.40 uruchom zwielokrotnione łącze, a następnie równoczesną transmisję plików jak w ćwiczeniu 4. Sprawdź, jak zmienia się czas transmisji przy uruchamianiu dodatkowych połączeń pomiędzy przełącznikami.

ĆWICZENIA cd.

6. Zbuduj sieć na podstawie topologii przedstawionej na rysunku 8.41. Uruchom dowolną transmisję do internetu na wszystkich komputerach, a następnie za pomocą oprogramowania typu sniffer zbadaj ruch w sieci. Czy możliwe jest podejrzenie transmisji z innych komputerów?

7. W sieci zbudowanej na podstawie rysunku 8.41 w przełączniku uruchom usługę port mirroring i przekieruj cały ruch do i z routera na port, do którego jest podłączony Twój komputer. Za pomocą oprogramowania typu sniffer sprawdź przesyłane dane.



Rysunek 8.41. Topologia dostępu do internetu

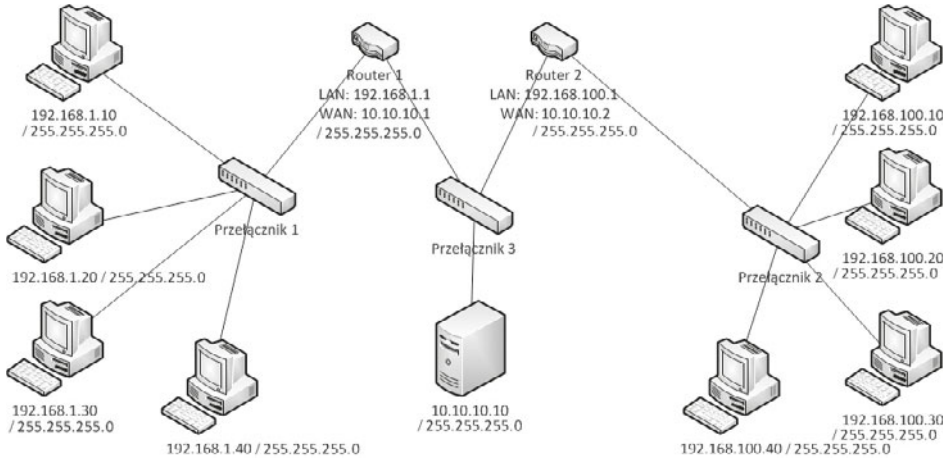
8. Zbuduj sieć na podstawie topologii przedstawionej na rysunku 8.40. Sprawdź dostępność poszczególnych połączeń między komputerami przy użyciu komendy `ping`. Utwórz sieci VLAN, do których zostaną przypisane następujące komputery:

- **a)** VLAN10: 192.168.1.10 oraz 192.168.1.110
- **b)** VLAN20: 192.168.1.20 oraz 192.168.1.120
- **c)** VLAN30: 192.168.1.30 oraz 192.168.1.130
- **d)** VLAN40: 192.168.1.40 oraz 192.168.1.140

Sprawdź dostępność połączeń pomiędzy poszczególnymi komputerami. Które z połączeń przestały działać? Wyjaśnij dlaczego.

ĆWICZENIA cd.

9. Zbuduj sieć na podstawie topologii przedstawionej na rysunku 8.42. Uruchom na serwerze o adresie 10.10.10.10 serwer WWW.



Rysunek 8.42. Topologia symulująca działanie internetu

Sprawdź dostępność serwera z poszczególnych komputerów w sieciach podłączonych do routerów 1. oraz 2.

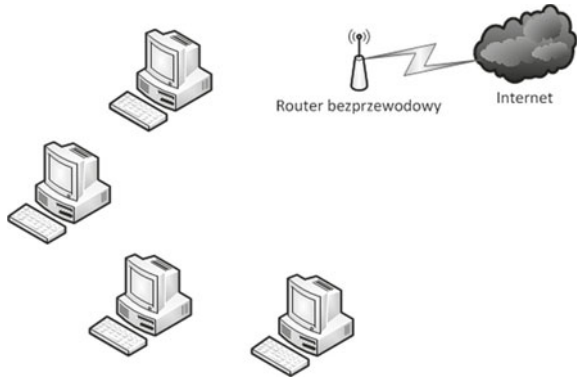
10. Na komputerze o adresie 192.168.1.10 uruchom serwer stron WWW, a następnie przekierowanie portu 80 na port 80 serwera WWW. Sprawdź działanie przekierowania z drugiej sieci poprzez uruchomienie w przeglądarce adresu routera 1.: 10.10.10.1.

11. Na routerze 2. uruchom firewall zabraniający dostępu do stron WWW (port 80) dla komputera o adresie 192.168.100.10.

12. Uruchom na routerze 1. serwer SNMP. Sprawdź za pomocą dowolnego oprogramowania korzystającego z tego protokołu parametry urządzenia.

ĆWICZENIA cd.

13. Zbuduj sieć na podstawie topologii przedstawionej na rysunku 8.43 oraz skonfiguruj dostęp do sieci bezprzewodowej z wykorzystaniem szyfrowania WPA2. Skonfiguruj poszczególne komputery, aby uzyskiwały dostęp do sieci bezprzewodowej. Uruchom serwer DHCP na routerze bezprzewodowym, tak by przypisywał urządzeniom w sieci wewnętrznej adresy z sieci 176.16.1.0.



Rysunek 8.43. Topologia z wykorzystaniem routera bezprzewodowego

14. Znajdź w internecie dostawcę usług VoIP, który oferuje darmowe połączenia pomiędzy swoimi abonentami. Utwórz konto użytkownika usługi, a następnie skonfiguruj zgodnie z zaleceniami usługodawcy oprogramowanie pozwalające na korzystanie z usług VoIP. Sprawdź możliwość połączenia z innym użytkownikiem sieci.

15. Przy użyciu oprogramowania Wireshark przechwyć login i hasło przesyłane protokołem FTP.

16. Przy użyciu oprogramowania Wireshark spróbuj przechwycić ruch związany ze stronami WWW wygenerowany przez innego użytkownika sieci.

PYTANIA

1. Jakie są domyślne parametry konfiguracyjne połączenia z portem konsoli dla urządzeń firmy Cisco?
2. Jaka komenda w systemie operacyjnym urządzeń Cisco pozwala na wejście w tryb uprzywilejowany?
3. Jaka komenda w systemie operacyjnym urządzeń Cisco pozwala na zapisanie konfiguracji?
4. Czym różni się przełącznik warstwy trzeciej od routera?
5. Czym różni się przełącznik zarządzalny od niezarządzalnego?
6. W której warstwie modelu OSI działa router?
7. Do czego służy Spanning Tree Protocol (STP)?
8. Jak nazywa się protokół pozwalający na monitorowanie pracy urządzeń sieciowych i zdalne zarządzanie nimi?
9. Jak nazywa się usługa pozwalająca na przesyłanie danych transmitowanych wybranym portem przełącznika do innego portu, np. w celu analizy danych?
10. Co oznacza skrót QoS? Do czego służy ta usługa?
11. Co oznacza skrót VLAN?
12. Do czego służą wirtualne sieci lokalne?
13. Na jakiej podstawie urządzenia mogą być podłączane do wybranej sieci VLAN?
14. Co jest niezbędne, aby umożliwić komunikację pomiędzy różnymi sieciami VLAN?
15. Do czego służy agregacja łącza?
16. Jak nazywa się połączenie pozwalające na przekazywanie ruchu z sieci VLAN pomiędzy przełącznikami?
17. Do czego używany jest serwer DHCP uruchamiany na routerach?
18. Czym jest technologia translacji adresów? Do czego służy?
19. Na czym polega usługa przekierowania portów? Do czego może być stosowana?
20. Co oznacza strefa zdemilitaryzowana w odniesieniu do sieci komputerowych?
21. Czym różni się routing statyczny od routingu dynamicznego?
22. Na podstawie jakich parametrów transmisji TCP/IP ruch sieciowy może być filtrowany w urządzeniach zabezpieczających transmisję (firewall)?
23. Do czego mogą być wykorzystane listy dostępu (ang. *access list*) w urządzeniach Cisco?

PYTANIA cd.

24. Jakiego rodzaju listy dostępu występują w urządzeniach firmy Cisco? Czym różnią się od siebie?

25. Co oznacza skrót WLAN?

26. W jakim trybie mogą pracować urządzenia sieci bezprzewodowych?

27. Co w konfiguracji urządzenia sieciowego oznacza skrót SSID?

28. Wymień rodzaje szyfrowania stosowane w zabezpieczeniach sieci bezprzewodowych.

29. Co oznacza skrót VoIP?

30. Do czego służy protokół SIP?

31. Co oznacza termin softphone w odniesieniu do telefonii internetowej?

32. Czy w sieci VoIP istnieje możliwość uzyskania standardowego numeru telefonicznego dostępnego z sieci telefonicznej?

33. Do czego służy oprogramowanie typu sniffer?

34. Wymień znane Ci protokoły przesyłające niezaszyfrowane dane, które mogą być podglądane w sieci.

9

Projektowanie i wykonanie sieci komputerowych

Projektowanie sieci komputerowych to złożony proces, na który składa się opracowanie wielu aspektów, takich jak:

- Projekt sieci fizycznej:
  - » dobór medium transmisyjnego,
  - » dobór urządzeń sieciowych,
  - » wybór lokalizacji gniazdek sieciowych, punktów dystrybucji, umieszczenia okablowania sieciowego.
- Projekt sieci logicznej:
  - » model adresacji IP,
  - » podział na sieci VLAN,
  - » routing wewnątrz sieci,
  - » miejsca styku z innymi sieciami, strefy zdemilitaryzowane,
  - » uruchamiane usługi,
  - » zabezpieczenia.

Wszystkie plany powinny opierać się na założeniach biznesowych — zdiagnozowanych i spisanych potrzebach użytkowników sieci, a także uwzględniać budżet przeznaczony przez zleceniodawcę na wykonanie sieci.

Dobrze zaprojektowana sieć powinna:

- spełniać oczekiwania użytkowników,
- zapewniać wymaganą przepustowość,
- zapewniać wymagany poziom bezpieczeństwa i ochrony danych na etapie ich transmisji i przechowywania,
- zapewniać wymaganą dostępność sieci (ang. *availability*) — ciągłość pracy,

- zapewniać skalowalność (ang. *scalability*) — umożliwiać łatwą rozbudowę,
- umożliwiać łatwą diagnozę usterek oraz szybką — najlepiej automatyczną — rekonfigurację w przypadku wystąpienia awarii.

9.1. Normy i zalecenia związane z projektowaniem sieci komputerowych

Normy związane z budową sieci komputerowych dotyczą samego okablowania strukturalnego, ale również jego testowania, kanałów telekomunikacyjnych czy administracji infrastrukturą telekomunikacyjną w biurowcach.

Pierwsza norma — *EIA/TIA 568A* — Standardy okablowania strukturalnego budynków (ang. *Building Telecommunications Wiring Standards*) — została wydana w 1995 roku w Stanach Zjednoczonych. Na jej podstawie powstało wiele norm towarzyszących:

- *EIA/TIA 569 Commercial Building Telecommunications for Pathways and Spaces* (kanały telekomunikacyjne w biurowcach);
- *EIA/TIA 570 Residential Telecommunications Cabling Standard* (kanały telekomunikacyjne w budynkach mieszkalnych);
- *EIA/TIA 606 The Administration Standard for the Telecommunications Infrastructure of Commercial Building* (administracja infrastruktury telekomunikacyjnej w biurowcach);
- *EIA/TIA 607 Commercial Building Grounding and Bonding Requirements for Telecommunications* (uziemienia w budynkach biurowych);
- *TSB 67 Transmission Performance Specification for Field Testing of Unshielded Twisted-Pair Cabling Systems* (pomiary systemów okablowania strukturalnego);
- *TSB 72 Centralized Optical Fiber Cabling Guidelines* (scentralizowane okablowanie światłowodowe);
- *TSB 75 Horizontal Cabling for Open Office* (okablowanie poziome dla biur o zmiennej aranżacji wnętrz);
- *TSB 95 Additional Transmission Performance Guidelines for 4-Pair 100 W Category 5 Cabling* (dodatkowa wydajność w transmisji dla okablowania typu skrętka 5. kategorii).

Normy amerykańskie były podstawą utworzenia norm międzynarodowych zatwierdzonych przez Międzynarodową Organizację Normalizacyjną (ang. *International Organization for Standardization* — ISO) — *ISO/IEC 11801* — oraz norm europejskich określonych w dokumencie *EN 50173*. Normy obowiązujące w Polsce są implementacją norm europejskich i są zapisane w dokumentacji *PN-EN 50173 (Technika informatyczna. Systemy okablowania strukturalnego*), która składa się z następujących części:

1. Wymagania ogólne.
2. Pomieszczenia biurowe.
3. Zabudowania przemysłowe.
4. Zabudowania mieszkalne.
5. Centra danych.

W dokumentacji *PN-EN 50174* (*Technika informatyczna. Instalacja okablowania*) podzielonej na następujące części:

1. Specyfikacja i zapewnienie jakości.
2. Planowanie i wykonawstwo instalacji wewnątrz budynków.
3. Planowanie i wykonawstwo instalacji na zewnątrz budynków.
4. Badanie zainstalowanego okablowania.

Oraz w dokumentacji *PN-EN 50310* (*Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym*).

Oprócz norm związanych z techniką informatyczną wskazana jest znajomość norm *PN-IEC 60364* (*Instalacje elektryczne w obiektach budowlanych*) i *PN-HD 60364* (*Instalacje elektryczne niskiego napięcia*), najważniejszymi z tych norm częściami są:

- *PN-IEC 60364-4-442* — Ochrona dla zapewnienia bezpieczeństwa — Ochrona przed przepięciami.
- *PN-IEC 60364-7-707* — Wymagania dotyczące specjalnych instalacji lub lokalizacji — Wymagania dotyczące uziemień instalacji urządzeń przetwarzania danych.
- *PN-HD 60364-4-41* — Ochrona dla zapewnienia bezpieczeństwa — Ochrona przed porażeniem elektrycznym.
- *PN-HD 60364-4-444* — Ochrona dla zapewnienia bezpieczeństwa — Ochrona przed zaburzeniami napięciowymi i zaburzeniami elektromagnetycznymi.
- *PN-HD 60364-5-551* — Dobór i montaż wyposażenia elektrycznego — Inne wyposażenie — Niskonapięciowe zespoły prądotwórcze.

Normy określające parametry okablowania strukturalnego przypisują mu odpowiednie kategorie (norma amerykańska) lub klasy (norma międzynarodowa i europejska). Różnica pomiędzy nimi polega na tym, że kategoria dotyczy jedynie okablowania, a klasa określa wymagania, jakie musi spełniać kompleksowe łącze transmisyjne złożone z okablowania, osprzętu transmisyjnego, gniazdek itp.

Zestaw klas okablowania strukturalnego przedstawia się następująco:

- Klasa A — pozwala na realizację usług telefonicznych z pasmem częstotliwości do 100 kHz.
- Klasa B — pozwala na realizację usług telefonicznych oraz usług terminalowych z pasmem częstotliwości do 1 MHz.
- Klasa C (kategoria 3) — podstawowe usługi sieci lokalnych wykorzystujące pasmo częstotliwości do 16 MHz.
- Klasa D (kategoria 5) — dla szybkich sieci lokalnych wykorzystujących pasmo częstotliwości do 100 MHz. W roku 1998 powstało rozszerzenie klasy D (zwane też kategorią 5e) definiujące bardziej restrykcyjne wymagania.
- Klasa E (kategoria 6) — realizacja usług w paśmie częstotliwości do 250 MHz (dla aplikacji wymagających pasma 200 MHz). Okablowanie kategorii 6. jest wykorzystywane w sieci Gigabit Ethernet — wymaga stosowania zmodyfikowanych złączy RJ-45.
- Klasa F (kategoria 7) — do realizacji usług w paśmie częstotliwości do 600 MHz. Wymaga stosowania okablowania podwójnie ekranowanego S-STP (każda para otoczona jest ekranem, dodatkowo występuje ekran obejmujący cztery pary). Dla tej klasy okablowania będzie możliwa realizacja transmisji z szybkością przekraczającą 1 Gb/s.

9.1.1. Elementy okablowania strukturalnego

Normy projektowania sieci dotyczą budowy bardzo rozbudowanych sieci obejmujących wiele budynków — taki obszar jest nazywany kampusem (ang. *campus*).

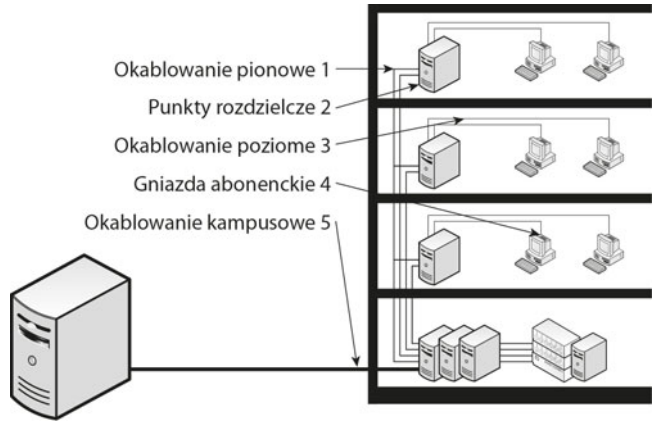
Normy określają następujące elementy sieci okablowania strukturalnego:

- *Kampusowy punkt dystrybucyjny* (ang. *campus distributor* — CD) — centralny punkt sieci, z którego jest rozprowadzane kampusowe okablowanie szkieletowe.
- *Kampusowy kabel szkieletowy* (ang. *campus backbone cable*) — to okablowanie łączące kampusowy punkt dystrybucyjny z punktami budynkowymi. Powinien to być kabel światłowodowy, dopuszcza się jednak stosowanie okablowania miedzianego. Gdy okablowanie jest prowadzone na zewnątrz budynku, rekomenduje się stosowanie połączeń światłowodowych ze względu na ich odporność na warunki zewnętrzne.
- *Budynkowy punkt dystrybucyjny* (ang. *building distributor*) — punkt, w którym są zakończone budynkowe kable szkieletowe. Jest on również określany jako MDF (ang. *Main Distribution Facility*).
- *Budynkowy kabel szkieletowy* (ang. *building backbone cable* — główny punkt dystrybucyjny) — kabel łączący budynkowy punkt dystrybucyjny z piętrowym punktem dystrybucyjnym lub łączący ze sobą piętrowe punkty dystrybucyjne.
- *Piętrowy punkt dystrybucyjny* (ang. *floor distributor*) — jest centralnym punktem sieci na piętrze, od którego jest rozprowadzane okablowanie poziome. Jest on również określany jako IDF (ang. *Intermediate Distribution Facility* — pośredni punkt dystrybucyjny).
- *Kabel poziomy* — łączy punkt piętrowy dystrybucyjny z gniazdem telekomunikacyjnym lub punktem pośrednim, o ile taki występuje. Może być kablem miedzianym lub światłowodowym.
- *Punkt pośredni* (ang. *consolidation point*) — opcjonalny punkt połączenia w okablowaniu poziomym tworzony pomiędzy piętrowym punktem dystrybucji a gniazdem telekomunikacyjnym.
- *Kable punktu pośredniego* (ang. *consolidation point cable*) — kabel łączący punkt pośredni z gniazdem telekomunikacyjnym.
- *Gniazdo telekomunikacyjne* (ang. *telecommunications outlet*) — gniazdo sieci komputerowej będące zakończeniem okablowania poziomego. Pozwala na podłączenie urządzeń poprzez kabel połączeniowy (ang. *work area cord*). Gniazda telekomunikacyjne montuje się w obszarach roboczych (ang. *work area*) — miejscach, w których pracują użytkownicy sieci.
- *Zespół gniazd telekomunikacyjnych przeznaczony dla wielu użytkowników* (ang. *Multi-user Telecommunication Outlet*) — zgrupowane gniazdo telekomunikacyjne, często stosowane w otwartych obszarach roboczych, takich jak sale konferencyjne czy otwarte przestrzenie biurowe.

Rozmieszczenie elementów okablowania strukturalnego zostało przedstawione na rysunku 9.1.

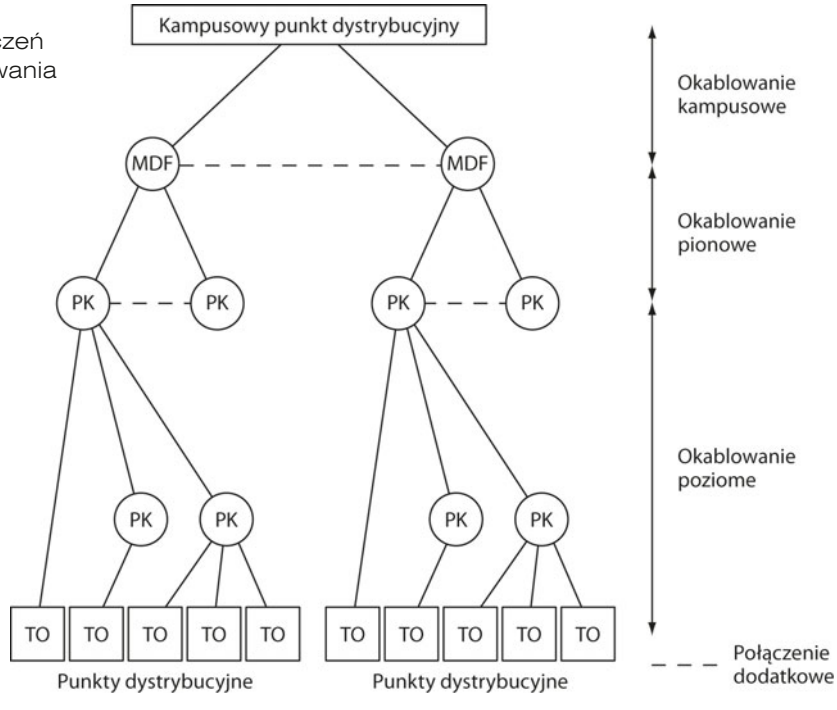
Jak wynika z przedstawionej terminologii, normy mówią o budowie sieci w topologii gwiazdy bądź rozszerzonej gwiazdy. Dodatkowo normy dopuszczają zastosowanie połączeń zapasowych (redundantnych), które zmieniają czystą strukturę gwiazdy, niemniej jednak pozwalają zapewnić większą wydajność lub mniejszą awaryjność sieci.

Rysunek 9.1.
Elementy okablowania strukturalnego w przykładowej sieci



Rysunek 9.2 przedstawia strukturę połączeń w sieci okablowania strukturalnego.

Rysunek 9.2.
Struktura połączeń w sieci okablowania strukturalnego



WSKAZÓWKA

Nie wszystkie przedstawione elementy muszą występować w każdej projektowanej sieci. Projekt powinien zakładać ich dopasowanie do konkretnych warunków, w których sieć będzie działać, np. sieć budowana na obszarze 2 pokoi nie będzie zawierała budynkowego i piętrowego punktu dystrybucji, ale tylko jeden z nich, będący głównym punktem dystrybucji całej sieci.

9.1.2. Zalecenia dotyczące projektowania sieci

Normy określają szereg czynników, które mają wpływ na jakość transmisji w sieci oraz na jej skalowalność. Najważniejsze z nich zostały przedstawione poniżej:

- Na każde 1000 m² powierzchni biurowej powinien przypadać jeden piętrowy punkt rozdzielczy.
- Na każdym piętrze powinien zostać zaprojektowany co najmniej jeden punkt rozdzielczy — jeżeli na danym piętrze jest przewidywane małe nasycenie punktami abonenckimi, obszary robocze mogą być obsłużone z innego piętrowego punktu rozdzielczego.
- Na każde 10 m² powierzchni biurowej powinno przypadać jedno gniazdo telekomunikacyjne (punkt abonencki) wyposażone w 2 gniazda RJ-45 i gniazdo sieci elektrycznej (najlepiej dedykowanej jedynie dla urządzeń komputerowych, co pozwoli zapewnić odpowiednią jakość dostarczanego prądu).
- W obrębie całej sieci powinna być wprowadzona jednolita numeracja elementów sieci — wszystkie elementy okablowania powinny być czytelnie oznaczone unikalnym numerem; po wykonaniu instalacji należy wykonać dokumentację sieci, która powinna być przechowywana i aktualizowana przez administratora sieci.
- Przewody zasilające i teleinformatyczne muszą przecinać się pod kątem 90°.
- Promień zgięcia kabla miedzianego powinien być przynajmniej 8-krotnie większy od średnicy kabla.
- Promień zgięcia kabla światłowodowego w zależności od jego rodzaju wynosi zazwyczaj 30, 15 i 7,5 mm.
- Kable teleinformatyczne muszą przebiegać minimum 0,9 m od silników, sprzętu przemysłowego oraz minimum 30 cm od opraw świetlówkowych (mogą one zaburzać transmisję danych poprzez wytwarzane pole elektromagnetyczne).
- Jeżeli kable zasilające i teleinformatyczne są prowadzone w rurkach (podtynkowo lub natynkowo), muszą to być oddzielne rurki.
- Sieci zasilające i komputerowe mogą być prowadzone w jednym kanale kablowym; w takim przypadku kable teleinformatyczne powinny być oddzielone przegrodą i znajdować się poniżej kabli zasilających.
- Jeśli sieci są prowadzone w podniesionej podłodze lub podwieszanym suficie, kanały kablowe powinny być montowane z zachowaniem minimum 5 cm dystansu.

9.1.3. Zalecenia dotyczące okablowania

Aby zapewnić łatwe zarządzanie elementami okablowania strukturalnego, wszelkie kable, które stanowią stałą część infrastruktury — nie są podłączane do urządzeń końcowych — są zakańczane na tzw. panelach krosowych (ang. *patch panel*) lub na gniazdach. Kable służące do podłączenia urządzeń do paneli są nazywane kablami krosowymi (ang. *patch cord*), kable do podłączenia gniazd z urządzeniami — kablami połączeniowymi (ang. *work area cord*). Tabela 9.1 pokazuje całkowite dopuszczalne długości okablowania (włącznie z kablami krosowymi oraz połączeniowymi) oraz zalecany rodzaj kabla dla poszczególnych podsystemów okablowania strukturalnego.

Tabela 9.1. Dopuszczalne długości okablowania w poszczególnych segmentach sieci okablowania strukturalnego

Podsystem	Zalecany rodzaj okablowania	Dopuszczalna długość
Okablowanie poziome	Skrętka UTP Skrętka STP Skrętka FTP Skrętka S-STP	100 m (włącznie z kablami krosowymi oraz połączeniowymi)
Okablowanie pionowe	Skrętka UTP Skrętka STP Skrętka FTP Skrętka S-STP	100 m
Okablowanie kampusowe	Światłowód jednomodowy	W zależności od użytego typu światłowodu i urządzeń nadawczo-odbiorczych, na chwilę obecną nawet do 100 km.
	Światłowód wielomodowy	
	Skrętka UTP Skrętka STP Skrętka FTP Skrętka S-STP	100 m

9.2. Metodologia tworzenia projektu

Nie istnieje jeden prawidłowy sposób tworzenia projektu sieci komputerowej — jest on zależny od wymagań zamawiającego, wielkości sieci czy też wcześniejszych doświadczeń projektanta. Zaproponowana metodologia zawiera etapy, które — zrealizowane w odpowiedniej kolejności — pozwolą na bezproblemowe stworzenie projektu sieci. Zakładana metodologia składa się z następujących etapów:

1. Analizy biznesowej potrzeb zamawiającego.
2. Projektu logicznego sieci.
3. Projektu fizycznego sieci.
4. Doboru urządzeń sieciowych.
5. Kosztorysowania.
6. Dokumentacji.

9.2.1. Analiza biznesowa potrzeb zamawiającego

Najważniejszym aspektem projektowania sieci jest jej dostosowanie do potrzeb zamawiającego. Jeśli stworzony projekt nie będzie uwzględniał wszystkich zaleceń klienta, stanie się bezużyteczny. Jeżeli na jego podstawie zostanie zbudowana sieć, nie będzie ona pełnić swojej roli i będzie wymagać zmian, co pociągnie za sobą dodatkowe koszty.

Na podstawie informacji uzyskanych podczas analizy biznesowej projektant podejmuje szereg ważnych decyzji, takich jak:

- wybór aplikacji sieciowych — systemów finansowo-księgowych, systemów operacyjnych dla stacji roboczych i serwerów,
- wybór sprzętu komputerowego (stacje robocze i serwery),
- wybór topologii sieci i używanych protokołów komunikacyjnych,
- wybór urządzeń sieciowych (przełączniki, routery, firewall),
- wybór elementów okablowania strukturalnego (przewody, panele krosowe, szafy dystrybucyjne),
- sposób połączenia z siecią internet,
- wybór poziomu bezpieczeństwa.

Analiza potrzeb zamawiającego powinna zdefiniować wymagania funkcjonalne dotyczące sieci (używane aplikacje, działające usługi) oraz strukturę organizacyjną zamawiającego wraz z zakresem dostępu do danych i usług sieciowych. Na etapie analizy należy również zapoznać się z infrastrukturą, w której sieć ma powstać, w celu odpowiedniego zaplanowania tras przebiegu okablowania, umieszczenia punktów dystrybucji sieci czy gniazdek sieciowych.

Analizę biznesową potrzeb klienta należy rozpocząć od zebrania informacji dotyczących zamawiającego — trzeba określić wielkość firmy, rodzaj prowadzonej działalności, potencjał rozwoju firmy (oznaczający możliwą rozbudowę sieci).

Kolejnym etapem analizy powinno być zapoznanie się ze strukturą organizacyjną firmy, liczbą osób zatrudnionych w poszczególnych działach czy realizowanymi przez dane komórki zadaniami. Wiedza ta pozwala na zaplanowanie usług, jakie będą wykorzystywane na poszczególnych stanowiskach, oraz rodzaju sprzętu i oprogramowania wymaganego na danych stacjach roboczych. Znajomość struktury organizacyjnej pozwala również zaplanować logiczny podział sieci na podsieci czy wirtualne sieci VLAN, tak aby zapewnić niezbędny poziom bezpieczeństwa danych.

Następnym krokiem w przygotowaniu do projektowania sieci jest zebranie informacji o infrastrukturze — lokalizacjach, w jakich ma działać sieć komputerowa. Należy określić położenie pomieszczeń oraz budynków, rozmieszczenie pracowników poszczególnych działów oraz przewidywane zapotrzebowanie na punkty abonenckie w konkretnych pomieszczeniach (tzw. nasycenie).

Na tym etapie niezbędne jest pozyskanie planów budynków wraz z wymiarami, a także odległościami pomiędzy budynkami, w przypadku gdy budowana sieć ma obejmować swoim działaniem wiele lokalizacji. Dane te są niezbędne w celu zaprojektowania właściwego rozmieszczenia punktów dystrybucji sieci oraz okablowania. Warto sprawdzić, czy zamawiający ma jakieś wytyczne dotyczące rozmieszczenia punktów dystrybucji, i zweryfikować je pod kątem wymagań projektowania tego typu pomieszczeń (patrz punkt 9.2.3).

Istotne jest również uwzględnienie specyficznych parametrów pracy sieci, np. tego, że transformatory w pobliżu działającej sieci mogą zakłócać jej pracę, przeszkody pomiędzy antenami sieci bezprzewodowej mogą wpływać na jej wydajność itp.

Zbierając informacje na temat infrastruktury, warto sprawdzić dostępną instalację elektryczną, która jest niezbędna do poprawnego działania sieci. Gdy nie ma instalacji o właściwych parametrach, należy uwzględnić jej przygotowanie w planowanych pracach.

Istotne jest również pozyskanie informacji o istniejącej instalacji klimatyzacji. Jest ona niezbędna do chłodzenia serwerowni w celu zapewnienia optymalnych warunków pracy zainstalowanych tam urządzeń. Jeśli w budynkach klimatyzacja była wcześniej uruchamiana, należy sprawdzić możliwość jej rozbudowy. Jeżeli takiej instalacji nie ma, trzeba zbadać warunki jej uruchomienia.

Po zbadaniu infrastruktury należy określić wymagania funkcjonalne dotyczące sieci, przede wszystkim to, do czego sieć będzie wykorzystywana, jakie usługi będą w niej uruchamiane, jakie oprogramowanie ma być użyte, gdzie i w jaki sposób powinien być dostępny internet, na ile jest on kluczowy w działalności firmy. Warto również sprawdzić, czy zamawiający korzysta obecnie z usług jakiegoś dostawcy internetowego, czy zamierza kontynuować współpracę, czy też przewiduje jego zmianę — często zamawiający może nie być świadomy tego, że są inni usługodawcy. Jeśli został określony dostawca usług internetowych, należy zbadać ofertę pod kątem potrzeb budowanej sieci — sprawdzić oferowane prędkości, interfejsy dostępu do sieci, publiczne adresy IP, łącza zapasowe itp.

Podczas analizy trzeba także określić, jakie kluczowe usługi sieciowe będą realizowane wewnętrznie (na własnych serwerach w obrębie projektowanej sieci), a jakie zewnętrznie (na serwerach poza siecią).

Podane zagadnienia pokazują zakres koniecznych do zebrania informacji, które pozwolą na stworzenie wstępnego zakresu prac i kosztorysu. Dokumenty te powinny być przedstawione do akceptacji zamawiającemu w celu uniknięcia nieporozumień wynikających z błędnej interpretacji przedstawionych informacji. Właściwe prace projektowe powinny rozpocząć się dopiero po zaakceptowaniu przez klienta spisanych wymagań.

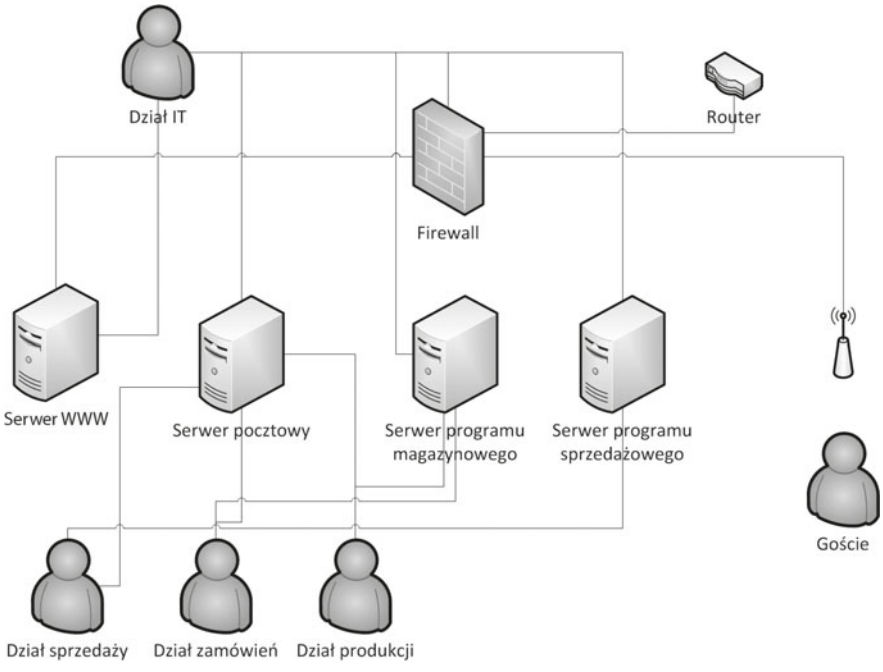
Przedstawione zagadnienia ustalane z zamawiającym są bardzo ogólne, dzięki czemu mogą być wykorzystywane w wielu przypadkach, niemniej jednak nie należy traktować ich jako ostatecznych. Każdy projekt jest indywidualny, związany z różnymi wymaganiami klienta czy infrastrukturą, w której ma być tworzony. W procesie analizy powinno się jak najlepiej określić wszelkie wymogi i ograniczenia stawiane budowanej sieci, w związku z czym należy go dostosować do konkretnych warunków.

9.2.2. Projekt logiczny sieci

Na podstawie danych zebranych podczas analizy można rozpocząć projektowanie logiczne sieci. Na projekt logiczny składa się ogólna koncepcja sieci, adresacja IP, sieci VLAN czy podział sieci na segmenty wraz z połączeniami między nimi. Na tym etapie nie przedstawia się konkretnych rozwiązań sprzętowych, ale jedynie funkcje i usługi sieciowe uruchamiane na serwerach — urządzenia dobiera się na podstawie logicznego projektu sieci.

Logiczny projekt tworzy się metodą zstępującą — od ogółu do szczegółu (ang. *top-down*). Pierwszym etapem prac jest stworzenie ogólnego schematu sieci obejmującego strukturę

organizacyjną oraz usługi sieciowe (rysunek 9.3). Taki wstępny plan powinien zostać rozbudowany o informacje na temat urządzeń sieciowych uwzględniające połączenia pomiędzy poszczególnymi lokalizacjami oraz ogólną liczbę podłączanych urządzeń sieciowych.



Rysunek 9.3. Szkic logicznego schematu sieci

Następnie dla każdego obszaru sieci powinna zostać zaproponowana adresacja IP — dla interfejsów konkretnych urządzeń sieciowych można przypisać stałe adresy, a dla urządzeń końcowych wskazać adres sieci.

WSKAZÓWKA

Ze względu na elastyczność i łatwość konfigurowania dla urządzeń końcowych (stacji roboczych) zaleca się automatyczną konfigurację protokołu IP za pomocą protokołu DHCP, natomiast dla urządzeń sieciowych oraz serwerów zaleca się konfigurację statyczną.

Projekt adresacji IP powinien uwzględniać publiczne adresy IP, które przekaże dostawca sieci internet — będą one przeznaczone do zapewniania dostępu do internetu czy uruchamiania niezbędnych usług sieciowych — oraz adresy prywatne zaproponowane przez projektanta.

Aby opracować schemat adresacji dla projektowanej sieci, należy określić liczbę potrzebnych adresów IP zarówno na etapie projektowania, jak i w przyszłości, podczas rozwoju sieci. Adresy IP powinny być przypisane dla takich urządzeń, jak:

- urządzenia końcowe — komputery użytkowników, komputery administratorów, serwery, drukarki sieciowe, telefony oraz kamery IP itp.;
- urządzenia sieciowe — interfejsy LAN i WAN routera, interfejsy administracyjne urządzeń sieciowych — przełączników, punktów dostępu sieci bezprzewodowej itp.

Po określeniu wszystkich urządzeń, które do prawidłowego działania potrzebują adresów IP, należy podjąć decyzję dotyczącą podziału sieci na niezależne podsieci.

Dzielenie sieci na podsieci ma na celu:

- Zarządzanie ruchem rozgłoszeniowym — podział na podsieci ogranicza transmisje rozgłoszeniowe.
- Zwiększenie bezpieczeństwa — poszczególne usługi mogą być dostępne w różnych, niezależnych podsieciach.
- Spełnienie specyficznych wymagań sieciowych.

Gdy zna się wymagania odnośnie do podziału na podsieci IP, należy podjąć decyzję o zakresie i użytych klasach adresów IP.

WSKAZÓWKA

Na etapie projektowania warto również stworzyć ogólny schemat nadawania adresów IP w obrębie poszczególnych sieci. Np.:

- Pierwszy adres IP danej sieci jest zarezerwowany dla bramy domyślnej.
- Adresy IP serwerów w sieci są przypisywane z zakresu X.X.X.10 – X.X.X.49.
- Adresy IP urządzeń końcowych zawierają się w zakresie X.X.X.100 – X.X.X.199.
- Adresy IP urządzeń sieciowych w danej sieci mieszczą się w zakresie X.X.X.210 – X.X.X.230.

Przyjęty schemat powinien zostać opisany w dokumentacji sieci.

Następnym krokiem w przygotowywaniu logicznego projektu jest stworzenie sieci VLAN oraz przypisanie do nich poszczególnych portów w urządzeniach sieciowych. Sieci VLAN powinny uwzględniać zakres dostępu do poszczególnych usług sieciowych, strukturę organizacyjną oraz dostęp do poszczególnych danych.

Na tym etapie ze względów bezpieczeństwa warto rozważyć osobną sieć na potrzeby administracji urządzeniami komputerowymi. Jest to wyodrębniona sieć, w której są dozwolone procedury zdalnego logowania na urządzenia sieciowe (np. SSH, RDP). Wydzielenie takiej sieci pozwoli na łatwą kontrolę dostępu do kluczowych elementów infrastruktury sieciowej i zminimalizowanie ryzyka podłączenia się do nich z wnętrza sieci osobom nieupoważnionym.

Ostatnim etapem projektowania logicznego jest dobór oprogramowania. Na podstawie założeń zebranych podczas analizy należy określić oprogramowanie, które będzie działać w sieci na poszczególnych serwerach. Dotyczy to zarówno oprogramowania

bezpośrednio związanego z usługami działającymi na rzecz użytkowników, jak i oprogramowania narzędziowego na potrzeby diagnozowania czy monitoringu sieci oraz bezpieczeństwa sieciowego.

Podczas projektowania sieci, na etapie analizy, zamawiający często przedstawia własną koncepcję używanego oprogramowania — czy to programów użytkowych, czy też serwerów sieciowych. Jest to podyktowane posiadanymi licencjami lub wykształconą w danej technologii kadrą. Projektowana sieć powinna zawsze spełniać wymagania zamawiającego, w związku z czym w przypadku, gdy oprogramowanie jest jasno określone, ten zakres projektu może zostać pominięty.

WSKAZÓWKA

Zdarza się, że zamawiający wymaga dostosowania projektu sieci do istniejących w firmie rozwiązań sprzętowych bądź programowych. Dobry projekt powinien uwzględniać wymagania zamawiającego, lecz nic nie stoi na przeszkodzie, by wprowadzić do projektu sugestie czy zalecenia, które pozwolą — zdaniem projektanta — na zwiększenie wydajności sieci.

9.2.3. Projekt fizyczny sieci

Na podstawie projektu logicznego należy utworzyć projekt fizyczny sieci. Projekt fizyczny powinien zawierać opis wybranego okablowania, konkretnych urządzeń sieciowych (włącznie ze wskazaniem modeli i ich parametrów technicznych), a także plan ułożenia okablowania strukturalnego wraz z punktami dystrybucji w poszczególnych budynkach. Projekt ten powinien opierać się na założeniach projektu logicznego, obowiązujących normach (patrz podrozdział 9.1), a także zaleceniach oraz wymaganiach producentów sprzętu.

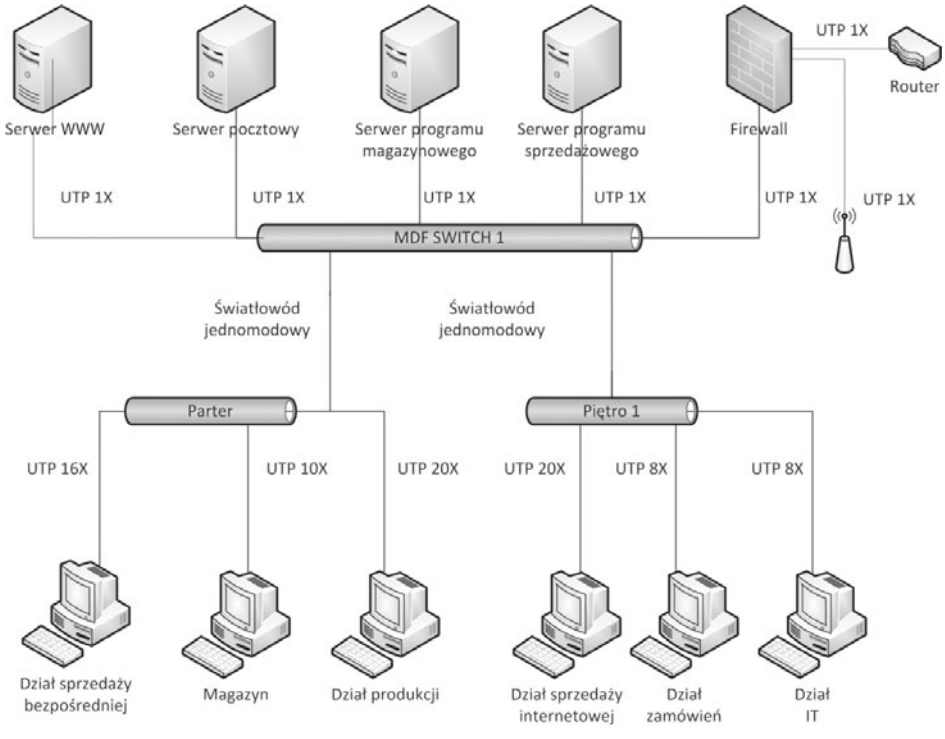
Na podstawie projektu logicznego oraz planów budynków należy wybrać okablowanie sieci dla poszczególnych jej segmentów — okablowania poziomego, pionowego oraz kampusowego.

WSKAZÓWKA

Wielu producentów elementów okablowania strukturalnego oferuje kompleksowe rozwiązania dla całej infrastruktury okablowania — od kabli, przez panele krosowe, gniazda, po zaciskarki do kabli. Używanie w obrębie całej projektowanej sieci części jednego producenta często jest warunkiem uzyskania bądź przedłużenia gwarancji na pojedyncze elementy.

Projektowanie rozmieszczenia okablowania należy rozpocząć od analizy projektów infrastruktury — jeśli istnieje konieczność utworzenia sieci pomiędzy budynkami, trzeba sprawdzić odległości między nimi oraz wymagania dotyczące przepustowości. Normy

dotyczące okablowania strukturalnego pozwalają na stosowanie między budynkami światłowodów jedno- i wielomodowych oraz skrętki. Wybór konkretnego rozwiązania zależy od warunków w miejscu instalacji oraz wymaganych parametrów łącza.



Rysunek 9.4. Projekt sieci uwzględniający lokalizacje oraz urządzenia sieciowe

Kolejnym etapem tworzenia fizycznego projektu sieci jest rozmieszczenie punktów dystrybucji sieci w obrębie poszczególnych budynków (rysunek 9.4). Najczęściej większość najważniejszego sprzętu sieciowego (serwery, macierze dyskowe) jest umieszczona w głównym punkcie dystrybucji — budynkowym lub w przypadku większych sieci kampusowym. Przy wyborze lokalizacji punktu dystrybucyjnego należy uwzględnić następujące czynniki:

- Pomieszczenie nie powinno znajdować się przy zewnętrznej, południowej ścianie budynku — nasłonecznienie i przenikanie ciepła powoduje wzrost temperatury w pomieszczeniu. Dodatkowo na ścianach nasłonecznionych nie można montować wymienników ciepła klimatyzacji. Konieczne staje się więc przedłużanie przebiegów instalacji klimatyzacji, co z kolei ma wpływ na jej wydajność.
- Pomieszczenie nie powinno mieć okien, które mogą powodować przenikanie ciepła z zewnątrz budynku. Jeśli ma, powinny one zostać zamurowane lub w razie braku takiej możliwości przysłonięte żaluzjami odbijającymi ciepło. Każde okno powoduje konieczność zwiększenia mocy projektowanej instalacji klimatyzacji, co przekłada się na wyższe koszty jej założenia i eksploatacji.

- Ze względu na ryzyko zalania serwerownia nie powinna się znajdować w najniższym miejscu budynku.
- W pomieszczeniu nie powinno być żadnych rur, które stanowią potencjalne źródło wycieku. Jeżeli nie ma możliwości usunięcia rur z wybranego pomieszczenia, należy pod każdą z nich zastosować okap lub rynnę, która odprowadzi wodę, a wewnątrz rynny umieścić czujnik zalania.
- Powinna istnieć możliwość łatwego transportu sprzętu do punktu dystrybucji.
- Droga transportowa od wejścia do budynku aż do drzwi do serwerowni powinna mieć szerokość 120 cm, wysokość minimum 2,5 m i wytrzymałość na obciążenie do 1000 kg/m^2. Na drodze transportowej, nie mogą znajdować się żadne progi ani stopnie. Cała droga musi być możliwa do pokonania przez wózek do transportu palet. Wymagania te są podyktowane koniecznością transportu urządzeń — niektóre z nich (np. wybrane macierze dyskowe) nie mogą być przechylane podczas transportu, gdyż grozi to ich uszkodzeniem.

Należy również wziąć pod uwagę konieczność doprowadzenia do głównego punktu dystrybucji odpowiedniej instalacji elektrycznej, pozwalającej na zapewnienie wystarczającej energii dla pracy wszystkich urządzeń. W przypadku gdy system komputerowy i działająca sieć są kluczowe dla pracy organizacji (np. sterowanie ciągłą produkcją), może istnieć konieczność doprowadzenia zapasowego łącza elektrycznego czy też uwzględnienia podłączenia agregatów prądotwórczych oraz zaprojektowania układów samoczynnie przełączających źródła energii.

UWAGA

Projekt zasilania powinien zostać wykonany przez osoby posiadające odpowiednie uprawnienia. W zależności od wymagań zamawiającego może on stanowić część projektu sieci komputerowej lub też być osobnym projektem opracowanym niezależnie — wówczas w projekcie sieci należy wskazać zapotrzebowanie na energię elektryczną generowaną przez poszczególne urządzenia sieciowe.

Projekt instalacji elektrycznej powinien uwzględniać nie tylko moc urządzeń komputerowych, ale również energię niezbędną do ładowania akumulatorów systemów podtrzymujących napięcie (UPS), oświetlenie oraz inne obwody elektryczne, energię do zasilania urządzeń klimatyzacji oraz rezerwę na wypadek wzrostu zapotrzebowania, np. po instalacji dodatkowego serwera.

Serwery i inne aktywne urządzenia sieciowe podczas pracy generują ciepło. Ze względu na ich stosunkowo dużą liczbę w punktach dystrybucji sieci ilość generowanego ciepła zagraża poprawnej pracy urządzeń i konieczne jest jego odprowadzenie. W tym celu projektuje się układy klimatyzacji, które mają za zadanie zapewnienie optymalnej temperatury pracy urządzeń.

W przypadku mniejszych punktów dystrybucji, w których pracuje mniejsza liczba urządzeń (np. piętrowy punkt dystrybucji, gdzie działa jeden przełącznik), ilość generowanego ciepła może nie wymagać dodatkowego chłodzenia.

UWAGA

Projekt klimatyzacji powinien zostać sporządzony przez osoby do tego uprawnione. Odpowiedni dobór urządzeń ma duży wpływ na koszty eksploatacji takiej instalacji — zapotrzebowanie tego typu urządzeń na energię elektryczną jest znaczne, a ich odpowiedni dobór pozwala te koszty zminimalizować.

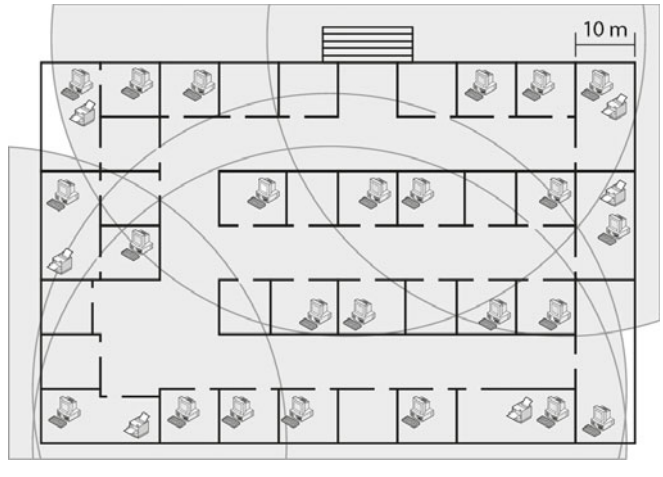
Podobnie jak w przypadku instalacji elektrycznej, plan instalacji klimatyzacji nie musi być częścią projektu sieci komputerowej — w takim przypadku w projekcie sieci powinny zostać zapisane wyraźne wytyczne dotyczące jej budowy.

Budynkowe oraz kampusowe punkty dystrybucji powinny zostać określone na podstawie planów budynków oraz wytycznych zamawiającego zebranych podczas analizy.

Podczas przeprowadzania analizy dobrze jest wskazać kilka potencjalnych lokalizacji, w których mogą mieścić się punkty dystrybucji. Na ich podstawie wybiera się najlepsze, które pokryją jak największy obszar roboczy — pozwolą na obsługę możliwie dużej liczby użytkowników sieci pracujących we wskazanych przez zamawiającego pomieszczeniach.

Okablowanie poziome wykonuje się najczęściej przy użyciu kabla typu skrętka — maksymalna długość okablowania poziomego bez kabli krosowych i połączeniowych wynosi 90 m. Należy wziąć pod uwagę, że nie jest to maksymalna odległość w linii prostej od punktu dystrybucji do punktu abonenckiego — trzeba uwzględnić konieczność prowadzenia kabli wzdłuż ścian oraz ewentualne doprowadzenie okablowania z głównego kanału kablowego do gniazdka telekomunikacyjnego.

Wyboru najlepszej lokalizacji piętrowych punktów dystrybucji dokonuje się na podstawie planów budynków, na które są nanoszone okręgi o promieniu 50 m (w skali odpowiadającej skali planów budynku). Środek okręgu stanowi potencjalną lokalizację punktu dystrybucji, okręgi zaś wskazują obszar, który może być pokryty okablowaniem z danego punktu dystrybucji (rysunek 9.5). Jeśli nie istnieje możliwość umieszczenia punktu w wybranym miejscu, należy powtórzyć wyznaczanie lokalizacji.



Rysunek 9.5. Wyznaczanie pokrycia obszarów roboczych przez piętrowe punkty dystrybucji

Pokrycie obszarów roboczych pozwala na wybór najbardziej korzystnej lokalizacji dla punktów dystrybucji.

Kiedy zostały wybrane lokalizacje punktów dystrybucji, należy wybrać drogi prowadzenia kanałów kablowych do gniazd abonenckich.

Okablowanie strukturalne powinno być prowadzone w kanałach wzdłuż ścian w plastikowych korytach umieszczanych na dowolnej wysokości ściany lub w rynnach umieszczonych pod sufitem. Dopuszczalne jest również prowadzenie okablowania powyżej podwieszanego sufitu lub pod podwyższoną podłogą, niemniej jednak okablowanie powinno znajdować się w korytach lub rynnach zamocowanych w odległości co najmniej 5 cm od innych elementów.

Na podstawie określonych punktów dystrybucji, wybranego okablowania oraz sposobu jego montażu należy nanieść na plany budynków wyznaczone przebiegi kablowe wraz z gniazdami abonenckimi. Każdy rodzaj okablowania powinien być oznaczony innym kolorem (lub stylem linii), aby łatwo można go było odróżnić.

Należy również przedstawić przebiegi kanałów kablowych, w których poprowadzone będzie okablowanie. W zależności od złożoności projektu i wymagań zamawiającego projekt może być prosty, pokazujący jedynie przebieg kanałów bez rozbicia na poszczególne elementy, lub dokładny, uwzględniający każdy użyty element, taki jak trójnik, narożnik, łącznik, reduktor, zakończenie kanału, puszki czy obudowy oraz użyte gniazda telekomunikacyjne. W tym drugim przypadku należy dokładnie zapoznać się z ofertą elementów systemu kanałów wybranego producenta, aby sprawdzić i dobrać odpowiednie części, a następnie nanieść je na rysunek. Pod każdym rysunkiem powinna znaleźć się legenda wskazująca, co oznaczają poszczególne symbole użyte na rysunkach.

9.2.4. Symbole używane w projektowaniu sieci

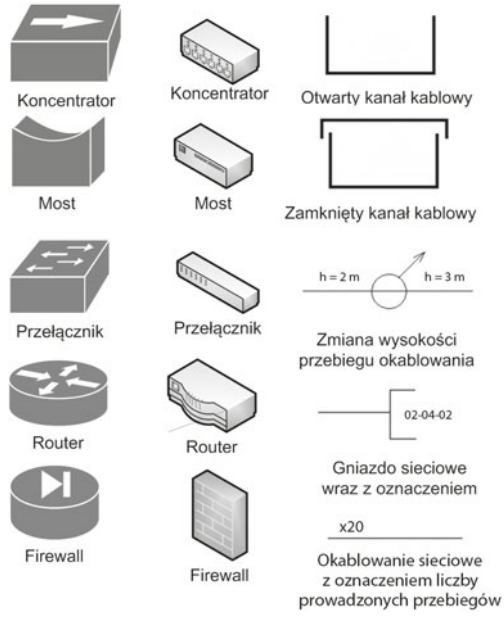
Polskie normy nie określają dokładnie symboli dla poszczególnych elementów sieci komputerowych, w związku z czym trudno jednoznacznie wskazać, jakie oznaczenia powinny być używane na etapie projektowania. Rysunek 9.6 przedstawia ogólnie przyjęte symbole urządzeń sieciowych oraz proponowane symbole używane w fizycznych projektach okablowania strukturalnego.

9.2.5. Dobór urządzeń sieciowych

Częścią projektu fizycznego sieci jest dobór odpowiednich urządzeń sieciowych do realizacji założonych zadań.

Okablowanie

Dobór okablowania sieciowego ma kluczowe znaczenie dla prędkości i jakości działania sieci. Źle dobrane lub źle ułożone okablowanie może spowodować, że nawet najlepszy aktywny sprzęt sieciowy nie będzie mógł osiągnąć oczekiwanej wydajności ze względu na błędy pojawiające się podczas przesyłania sygnałów.



Rysunek 9.6.
Proponowane symbole do użycia w projektach sieci komputerowych

Normy określają, jaki rodzaj kabla może być stosowany w kolejnych odcinkach okablowania strukturalnego. Poza parametrami dynamicznymi określającymi cechy samej transmisji przy wyborze konkretnego okablowania należy brać pod uwagę również parametry mechaniczne:

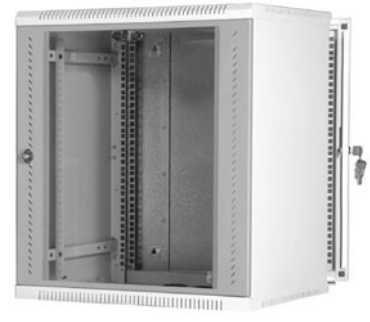
- Rodzaj przewodnika — w przypadku okablowania miedzianego występują kable typu drut (do układania przebiegów kablowych; są bardziej sztywne, dzięki czemu łatwiej się je układa w korytkach i są bardziej odporne na zagięcia) lub kable typu linka (stosowane jako kable krosowe; są bardziej elastyczne i łatwiej poddają się przy układaniu np. w szafach dystrybucyjnych).
- Średnicę przewodnika — jest podawana w jednostkach AWG (ang. *American Wire Gauge*) — musi być dopasowana do zacisków w panelach krosowych i gniazdach abonenckich.
- Średnicę zewnętrzną kabla — informacja niezbędna w celu poprawnego obliczenia wielkości koryt kablowych.
- Rodzaj ekranowania — w przypadku budowy sieci w miejscach narażonych na działanie fal elektromagnetycznych w celu eliminacji zakłóceń są stosowane kable z ekranowaniem.
- Dopuszczalne temperatury pracy oraz temperaturę podczas instalacji okablowania.
- Dopuszczalne promienie zagięcia kabla przy instalacji i podczas pracy — przekroczenie zalecanych wartości powoduje, że okablowanie nie zachowuje parametrów transmisji — skręcone pary ulegają rozkręceniu.
- Tworzywo izolacji zewnętrznej — występują dwa rodzaje: standardowa PCV oraz niepalna LSZH (ang. *Low Smoke Zero Halogen*), która jest stosowana w instalacjach podwyższonego ryzyka pożaru.

- Masę właściwą kabla — informacja niezbędna do projektowania wytrzymałości kanałów kablowych oraz obliczania obciążenia stropów.
- Dostępne długości kabla w jednostkowych opakowaniach — najczęściej okablowanie jest sprzedawane w opakowaniach po 100 lub 305 metrów.

Szafy dystrybucyjne

Punktami dystrybucyjnymi w sieci, w zależności od potrzeb, mogą być osobne pomieszczenia, wyodrębnione części pomieszczeń bądź szafy dystrybucyjne umieszczone w obszarach roboczych. Osprzęt sieciowy w punktach dystrybucyjnych powinien być montowany w szafach dystrybucyjnych typu rack (rysunki 9.7 i 9.8).

Rysunek 9.7.
Szafa dystrybucyjna stojąca



Rysunek 9.8.
Szafa dystrybucyjna dwusekcyjna wisząca

Jest to standard szaf, stojaków oraz urządzeń stosowany w przemyśle, zatwierdzony przez organizację EIA (ang. *Electronic Industries Association*) w dokumencie EIA-310-D. Wysokość elementów typu rack określa się w wielokrotności tzw. jednostek (U) — 1 U to wysokość pojedynczego elementu montażowego w szafie (wynosi 4,445 cm — 1,75 cala). Jednostka ta służy do określania wysokości szaf oraz zamontowanych w nich urządzeń.

Najczęściej spotykane szafy dystrybucyjne pozwalają na montaż urządzeń o szerokości 19 cali, ich wysokość wynosi od 10 do 45 U, głębokość od 60 do 100 cm; dostępne są w wersjach stojącej lub wiszącej.

Wysokość sprzętu sieciowego zależy od jego rodzaju, funkcjonalności czy liczby gniazd.

Stojące szafy dystrybucyjne mają budowę modularną, która pozwala na ich rozbudowę i łączenie w razie potrzeby instalacji większej ilości sprzętu sieciowego. Najczęściej mają one demontowane boczne ściany, dzięki czemu jest możliwy łatwy dostęp do zainstalowanych urządzeń. W górnej ścianie szaf dystrybucyjnych montuje się wentylatory, które zapewniają wymianę powietrza w szafie oraz chłodzenie sprzętu.

Aby ograniczyć dostawanie się kurzu do wnętrza szafy, wszelkie przewody są wprowadzane przez tzw. szczotkowe przepusty kablowe.

Dobierając wielkość szafy, należy mieć na uwadze następujące czynniki:

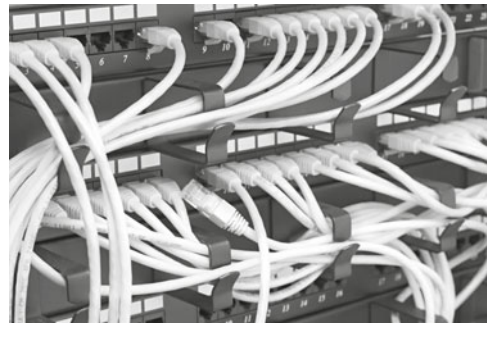
- Serwery w obudowach typu rack powinny być montowane w szafach o głębokości 100 cm w celu zapewnienia odpowiedniej wentylacji wewnątrz szafy.
- Wysokość szafy powinna uwzględniać nie tylko wysokość zainstalowanych wewnątrz urządzeń, ale również przestrzeń pomiędzy urządzeniami aktywnymi — w celu zapewnienia lepszej cyrkulacji powietrza zalecane jest pozostawienie wolnej przestrzeni o wysokości 1 U pomiędzy elementami aktywnymi, takimi jak serwery, routery i przełączniki.
- Jeśli w szafie dystrybucyjnej trzeba będzie zamontować wiele pionowych połączeń pomiędzy urządzeniami, należy rozważyć zakup szerszej szafy, która pozwala na montaż specjalnych pionowych elementów porządkujących.
- Przy wyborze szafy należy również rozważyć rozwój projektowanej sieci, a co za tym idzie, możliwość instalacji dodatkowych urządzeń w przyszłości.

Panele krosowe i organizery okablowania

Okablowanie sieciowe w szafach dystrybucyjnych jest zakańczane na tzw. panelach krosowych (ang. *patch panel*). Są to pasywne elementy sieci, które składają się z szeregu gniazd (najczęściej RJ-45 lub gniazd światłowodowych), do nich zaś są podłączane kable tworzonej sieci. Wyprowadzenie zakończeń kabli do paneli krosowych pozwala je w łatwy sposób zorganizować oraz, w razie potrzeby, zreorganizować — każde gniazdo w panelu powinno być opisane, w dokumentacji sieci powinien znajdować się schemat połączeń pomiędzy poszczególnymi gniazdami a urządzeniami sieciowymi w szafie.

W zależności od liczby gniazd (najczęściej 12, 24 lub 48) panele są różnej wysokości: 1, 2 oraz 3 U.

Dobrym zwyczajem jest stosowanie organizerów kabli (rysunek 9.9), które pozwalają na uporządkowanie okablowania wewnątrz szafy, dzięki zgrupowaniu kabli w jednym obszarze. Dostępne są zarówno organizery poziome montowane najczęściej pomiędzy przełącznikiem a panelem krosowym, jak i organizery pionowe pozwalające na poprowadzenie szeregu kabli wzdłuż szafy.



Rysunek 9.9. Poziome organizery kabli do szaf dystrybucyjnych

Przełączniki

Przełączniki działające w sieciach można podzielić na dwa rodzaje: przełączniki szkieletowe, służące do łączenia innych przełączników, stanowiące szkielet sieci, oraz przełączniki grup roboczych, które pozwalają na podłączenie końcowych użytkowników.

Przełączniki szkieletowe powinny być wydajnymi urządzeniami, które będą w stanie zapewnić wymaganą jakość ruchu sieciowego oraz oczekiwany poziom bezpieczeństwa. Najczęściej stosuje się tutaj przełączniki warstwy trzeciej, które działają z prędkościami co najmniej 1 Gb/s. Pozwalają one na kształtowanie ruchu za pomocą list kontroli dostępu czy przełączania na podstawie adresów IP, dzięki czemu sieć pracuje wydajniej.

Przełączniki grup roboczych działają najczęściej w piętrowych punktach dystrybucji i służą głównie do podłączenia użytkowników. Nie muszą zapewniać aż takiej wydajności oraz dodatkowych funkcji, jakie oferują przełączniki szkieletowe, dlatego najczęściej stosuje się w tym przypadku przełączniki warstwy drugiej, z obsługą sieci VLAN, jeśli jest to wymagane.

Niektóre modele przełączników do zastosowań profesjonalnych mają budowę modularną, która w razie potrzeby pozwala na rozbudowę urządzenia o dodatkowe porty — zarówno światłowodowe, jak i RJ-45. Wybór tego typu urządzeń pozwala na łatwą konfigurację sieci w celu dopasowania jej do zmieniających się potrzeb.

Jeśli istnieje konieczność podłączenia w obrębie jednego punktu dystrybucji większej liczby użytkowników (niemodularne przełączniki mają maksymalnie 48 portów + 4 dodatkowe gniazda GBIC), trzeba połączyć przełączniki między sobą. Połączenie to może zostać zrealizowane w jeden z następujących sposobów:

- Bezpośrednie połączenie port – port — przy użyciu kabla krosowego łączy się porty kolejnych urządzeń. Wadą takiego rozwiązania jest niska wydajność oraz potencjalne zagrożenie awarią — gdy połączonych jest kilka urządzeń, przerwanie jednego z połączeń powoduje zerwanie komunikacji pomiędzy kolejnymi urządzeniami. Zaletą są niskie koszty oraz łatwa rozbudowa o następne przełączniki.
- Bezpośrednie połączenie port – port z redundancją — przy użyciu kabla krosowego łączy się porty kolejnych urządzeń, dodatkowo tworząc pętlę. Rozwiązanie to nie zwiększy wydajności, ale w razie problemów z jednym z łączy protokół drzewa opinającego (ang. *Spanning Tree Protocol* — STP) uruchomi połączenie nadmiarowe, które pozwoli zachować ciągłość transmisji.
- Agregacja portów — przy użyciu kabli krosowych wielokrotnie łączy się te same przełączniki. Pozwala to na stworzenie logicznego połączenia pracującego z większą prędkością.
- Połączenie przełączników w stos (ang. *stacking*) — jest to specjalne połączenie pomiędzy urządzeniami realizowane przez dedykowany do tego celu port o bardzo dużej przepustowości. Urządzenia połączone w ten sposób mają jeden adres IP, co ułatwia administrację. Wadą takiego rozwiązania jest konieczność stosowania urządzeń tego samego producenta (brak standardów tego typu rozwiązań) oraz wysokie koszty — nie wszystkie przełączniki mają taką funkcjonalność.

Wydajność przełączników jest określana przez przepustowość (podawana w milionach pakietów na sekundę — mpps), szybkość szyny (Gb/s), szybkość procesora oraz ilość pamięci operacyjnej.

Oprócz wydajności przy wyborze przełącznika należy uwzględnić następujące czynniki:

- dostępne interfejsy sieciowe — Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, realizowane za pomocą skrętki i światłowodu;
- architekturę przełączania — przełączanie w warstwie drugiej (dostępność sieci VLAN, możliwość uruchomienia usługi QoS, przystosowanie do obsługi VoIP), przełączanie w warstwie trzeciej;
- wymaganą liczbę portów;
- dostępne funkcje bezpieczeństwa.

Istotny wpływ na wybór konkretnego urządzenia mogą mieć również warunki napraw i gwarancji. Należy przy tym starać się utrzymać jednolite środowisko sieci, a więc używać sprzętu jednego producenta — pozwoli to na oszczędności przy administrowaniu siecią oraz wyeliminuje niektóre problemy z niekompatybilnością niestandardowych rozwiązań (np. agregacja portów).

W okablowaniu pionowym oraz okablowaniu kampusowym można wykorzystać kabel typu skrętka lub światłowody, należy zatem odpowiednio dobrać porty w urządzeniu.

Istnieje możliwość podłączenia kabla światłowodowego do portu RJ-45 za pomocą specjalnych konwerterów (ang. *transceiver*). Oferują one zalety transmisji światłowodem bez konieczności zakupu przełączników z portami światłowodowymi.

Routery

Podstawowe zadanie routerów to przełączanie pakietów pomiędzy sieciami/interfejsami sieciowymi oraz wyznaczanie trasy do innych sieci.

W sieciach lokalnych działają dwa rodzaje routerów — router brzegowy zapewniający dostęp do internetu oraz routery szkieletowe odpowiedzialne za przełączanie pomiędzy wewnętrznymi sieciami. Dodatkowo routery mogą oferować szereg innych usług, takich jak kształtowanie ruchu (usługa QoS), kontrola dostępu czy połączenia VPN.

Routery można podzielić ze względu na ich mechanizm działania na:

- Routery sprzętowe — specjalne dedykowane urządzenia zbudowane z wykorzystaniem sprzętu zapewniającego wysoką wydajność przełączania pakietów. Do zastosowań profesjonalnych używa się urządzeń o budowie modularnej, pozwalającej na podłączanie wielu różnych typów interfejsów.
- Routery programowe — to komputer z uruchomionym odpowiednim oprogramowaniem zapewniającym przełączanie pakietów. Takie rozwiązania często można spotkać w małych sieciach, które nie wymagają wysokiej wydajności lub w których generowany ruch nie jest zbyt duży. Przykładem wykorzystania routera programowego jest udostępnianie połączenia sieciowego w systemie Windows — komputer z dwoma kartami sieciowymi zapewnia routing pomiędzy nimi.

Projektant przy wyborze routera powinien uwzględnić następujące czynniki:

- Wydajność — jest określana w pakietach na sekundę (pps); mówi o maksymalnej liczbie pakietów, które router jest w stanie przeanalizować w ciągu sekundy.
- Liczbę i rodzaj zainstalowanych portów — routery (zwłaszcza do zastosowań komercyjnych) oprócz standardowych łączy sieci Ethernet (do podłączenia mediów miedzianych, światłowodowych i bezprzewodowych) mogą mieć również interfejsy do podłączenia sieci WAN — porty szeregowe, porty ISDN, porty xDSL itd.
- Modularną budowę oraz dostępne karty rozszerzeń — w przypadku budowy dużych sieci lub sieci, dla których ważna jest skalowalność, należy wybierać urządzenia możliwe do ewentualnej przyszłej rozbudowy. Dotyczy to zarówno kart z interfejsami, jak i elementów mających wpływ na wydajność urządzenia (np. pamięć RAM).
- System operacyjny urządzenia — funkcjonalność routerów zależy od oprogramowania, które steruje sprzętem. Urządzenia do zastosowań komercyjnych działają pod kontrolą specjalnych dedykowanych systemów operacyjnych. Często funkcjonalność, a co za tym idzie, cena urządzenia jest zależna od zainstalowanej wersji systemu operacyjnego.

Serwery

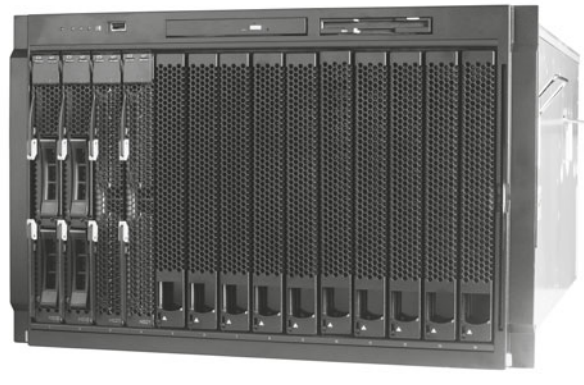
Sieci komputerowe są tworzone w celu udostępniania usług sieciowych, które działają na dedykowanych do tego celu komputerach — serwerach. W zależności od wymagań oprogramowania usługi te potrzebują różnej wielkości zasobów serwerowych — mocy procesora, wielkości pamięci RAM, wielkości przestrzeni dyskowej czy prędkości zapisu na dyskach. Właściwy dobór serwera ma kluczowe znaczenie dla wydajności uruchomionego na nim oprogramowania.

Aby dobrać odpowiedni serwer, należy znać wymagania stawiane przez aplikacje, które będą na nim uruchamiane, oczekiwany poziom niezawodności i bezpieczeństwa uruchamianych usług czy przewidywany wzrost zapotrzebowania na zasoby. Przy wyborze serwerów należy kierować się następującymi parametrami:

- Wymaganiami sprzętowymi uruchamianych aplikacji — ilością pamięci operacyjnej, ilością miejsca na dysku, liczbą oraz szybkością zainstalowanych procesorów, prędkością zapisu na dyskach.
- Obsługiwanymi macierzami RAID (ang. *Redundant Array of Independent Disks*) oraz rodzajem używanych dysków (SCSI/SATA).
- Oczekiwaną niezawodnością działających usług — stosowaniem redundantnych wentylatorów, zasilaczy itp., możliwością instalacji elementów typu HOT SWAP (wentylatorów, zasilaczy, dysków), które pozwalają na rozbudowę bez konieczności wyłączania serwera.
- Możliwością rozbudowy — liczbą wolnych gniazd dla instalacji dodatkowych procesorów, rozszerzeniami pamięci RAM, możliwością podłączenia dodatkowych dysków.
- Architekturą rozwiązania — aktualnie najczęściej spotykane są serwery 64-bitowe. (Należy pamiętać, że aby w pełni wykorzystać możliwości, jakie daje architektura sprzętowa, trzeba używać 64-bitowych aplikacji).

- Obudową serwera — serwery sieciowe są dostępne w następujących obudowach:
  - » obudowa typu wieża (ang. *tower*) — wolnostojąca, do uruchamiania poza szafami dystrybucyjnymi;
  - » obudowa typu rack — do montażu w szafach dystrybucyjnych, ma wysokość od 1 do 6 U, wewnątrz jest zamontowany jeden serwer sprzętowy i wszystkie niezbędne elementy, takie jak zasilacze, wentylatory, interfejsy sieciowe itp. Serwery tego typu mają zwartą i kompaktową konstrukcję, dzięki czemu miejsce w szafach dystrybucyjnych jest lepiej wykorzystywane. Każdy serwer typu rack montowany w szafie ma niezależny zasilacz, wentylację, interfejsy komunikacyjne oraz podłączenie klawiatury, myszy i ekranu;
  - » obudowa kasetowa typu blade — jest to obudowa zawierająca wspólny zasilacz, wentylację, interfejsy komunikacyjne oraz podłączenie klawiatury, myszy i ekranu dla właściwych serwerów w postaci karty podłączanej do obudowy poprzez specjalne dedykowane łącze (rysunek 9.10). Tego typu rozwiązania charakteryzują się dużą skalowalnością — istnieje możliwość łatwej rozbudowy o kolejny serwer poprzez podłączenie karty do obudowy blade.
- Oferowanym wsparciem dla systemów operacyjnych — w zależności od planowanych usług należy określić wsparcie producenta urządzenia dla wybranych systemów operacyjnych.
- Wsparciem technicznym oraz serwisem oferowanym przez producenta — w zależności od potrzeb można zakupić dodatkowe wsparcie techniczne oraz usługi naprawcze realizowane w określonym przez zamawiającego czasie (np. naprawa w ciągu 4 godzin od momentu zgłoszenia usterki). Takie pakiety serwisowe często znacznie zwiększają koszty użycia wybranego serwera, jednak gwarantują szybkie reakcje w przypadku wystąpienia awarii.

Rysunek 9.10.
Obudowa serwerowa typu blade



Zaleca się montowanie serwerów w szafach dystrybucyjnych o głębokości 100 cm, co pozwala na swobodną cyrkulację powietrza z tyłu urządzenia. Serwery typu rack są montowane na specjalnych szynach umożliwiających ich wysunięcie w celu konserwacji czy rozbudowy. Serwery typu blade montowane są na stałe do wewnętrznych elementów konstrukcyjnych.

Często w przypadku konieczności uruchomienia wielu serwerów w jednej organizacji w celu zmniejszenia kosztów zakupu sprzętu oraz jego utrzymania, a także oszczędzenia miejsca w szafach dystrybucyjnych, stosuje się serwery wirtualne. Wirtualizacja serwerów pozwala na uruchomienie na jednym fizycznym serwerze wielu serwerów wirtualnych. Serwer wirtualny jest niezależną instancją sieciowego systemu operacyjnego, pracującego na zasobach, które zostały mu przydzielone przez oprogramowanie obsługujące wirtualizację. Najczęściej stosowane oprogramowanie do wirtualizacji to:

- Microsoft Hyper-V — dostępny jako komponent Microsoft Windows Server 2008 oraz jako osobny produkt — Hyper-V Server 2008. Umożliwia instalowanie w wirtualnej maszynie systemów x86 i x64 z rodziny Windows, ale też SUSE Linux Enterprise od wersji 10.3 i Red Hat Linux Enterprise od wersji 5.2.
- VMware ESX Server — oprogramowanie firmy VMware pozwalające na uruchamianie wielu systemów operacyjnych, m.in. Windows, Linux, Solaris, FreeBSD. Oprogramowanie jest oferowane w darmowej wersji z ograniczoną funkcjonalnością.
- XenServer — oprogramowanie firmy Citrix, które pozwala na uruchomienie wielu systemów operacyjnych, m.in. Windows, Linux, Solaris, FreeBSD. Oferowana jest również darmowa wersja.

Stosowanie serwerów wirtualnych ma szereg zalet związanych z bezpieczeństwem i dostępnością usług. Dane dotyczące konkretnego serwera wirtualnego mogą być z łatwością przenoszone pomiędzy innymi serwerami fizycznymi, na których działa ta sama wersja oprogramowania do wirtualizacji. Dodatkowo mogą być tworzone obrazy stanu serwera (tzw. *snapshot*), które zapisują wszelkie parametry jego pracy (przetwarzane dane, zawartość pamięci RAM, otwarte pliki) w konkretnej chwili, co pozwala odtworzyć stan urządzenia z określonego czasu.

Przełączniki oraz konsole KVM

W przypadku używania serwerów sieciowych niezbędne jest podłączenie do nich urządzeń wejścia-wyjścia, takich jak klawiatura, mysz oraz monitor. Oczywiście po zainstalowaniu systemu operacyjnego istnieje możliwość zdalnego logowania na serwer oraz zarządzania nim, niemniej jednak w przypadku awarii urządzenia lub usługi niezbędne jest bezpośrednie podłączenie klawiatury i monitora (ewentualnie myszy) w celu zdiagnozowania występujących problemów.

W przypadku punktów dystrybucji, w których jest uruchamianych wiele serwerów, często niemożliwe jest podłączenie osobnych urządzeń wejścia-wyjścia do każdego z nich. Przełączniki KVM (od ang. *Keyboard*, *Video*, *Mouse* — klawiatura, monitor, mysz) pozwalają na podłączenie jednego zestawu (monitor, klawiatura i mysz) do wielu fizycznych serwerów. Przełącznik KVM pozwala wybrać, który serwer jest aktualnie obsługiwany przez urządzenia wejścia-wyjścia.

Do podłączenia serwerów z przełącznikiem KVM wykorzystuje się standardowe kable zakończone wtykami typu PS/2 dla myszy i klawiatury oraz standardowy kabel D-SUB do podłączenia monitorów. Urządzenia wejścia-wyjścia zamiast bezpośrednio do serwera są podłączane do przełącznika KVM.

Aby optymalnie wykorzystać miejsce w punktach dystrybucji, istnieje możliwość instalacji konsoli KVM wewnątrz szafy dystrybucyjnej (rysunek 9.11). Na ogół jest to monitor LCD 15″, 17″ lub 19″, który składa się podobnie jak ekran laptopa, oraz klawiatura wraz z panelem dotykowym (ang. *touch pad*) zastępującym mysz. Całość najczęściej mieści się w kompaktowej obudowie o wysokości 1 U, często zawiera również wbudowany przełącznik KVM.

Rysunek 9.11. Konsola KVM

Zasilanie awaryjne

Aby zapewnić ciągłość pracy i dostępność usług sieciowych, stosuje się zasilanie awaryjne, które w przypadku zaniku czy też skoków napięcia w sieci elektrycznej umożliwi dalszą pracę lub poprawne zamknięcie aplikacji, usług oraz systemów operacyjnych.

Urządzenia podtrzymujące napięcie przez krótki czas to UPS (od ang. *Uninterruptible Power Supply*). Są one wyposażone w akumulatory, które dostarczają napięcia podczas zaniku zasilania sieciowego lub gdy przekroczy ono dopuszczalny zakres. Ich stosowanie ma umożliwić poprawne zapisanie danych i zamknięcie systemu komputerowego lub podtrzymanie zasilania do czasu przełączenia na inne źródło zasilania (inny dostawca energii lub agregat prądotwórczy).

Aby właściwie dobrać moc zasilacza UPS, należy zsumować moc wszystkich odbiorników, które mają być zasilane z wybranego urządzenia. Moc urządzeń można odczytać z tabliczki znamionowej urządzenia — jest wyrażana w woltoamperach (VA) lub w watach (W). Jeśli moc urządzenia nie jest podana, wówczas można ją obliczyć ze wzoru:

$P = U \cdot I$,

gdzie:

U — natężenie prądu wyrażone w amperach (A),

I — napięcie prądu wyrażone w woltach (V).

Dla zasilaczy UPS podaje się ich moc pozorną wyrażoną w woltoamperach. Moc ta jest sumą mocy czynnej (która jest oddawana do podłączanych urządzeń) oraz mocy biernej (która jest wykorzystywana na pracę urządzenia).

Aby przeliczyć moc czynną urządzenia podłączanego do UPS na moc pozorną dla urządzeń komputerowych, przyjmuje się iloczyn mocy czynnej oraz przelicznika 1,4.

UWAGA

Zaleca się, aby moc zasilacza awaryjnego była większa od mocy podłączanych urządzeń o około 20% dla urządzeń sieciowych i 30–40% dla serwerów.

PRZYKŁAD

Aby obliczyć moc zasilacza UPS niezbędną do podtrzymania pracy serwera pobierającego 400 W, monitora LCD o mocy 80 W, przełącznika o mocy 100 W oraz routera o mocy 70 W, należy:

1. Obliczyć wymaganą moc dla urządzeń:
   - **a)** Serwer: 400 W · 1,4 = 560 VA
   - **b)** Monitor: 80 W · 1,4 = 112 VA
   - **c)** Przełącznik: 100 W · 1,4 = 140 VA
   - **d)** Router: 70 W · 1,4 = 98 VA
3. Obliczyć moc nadmiarową dla poszczególnych urządzeń, przyjmując 40% zapas dla serwerów sieciowych i 20% zapas dla pozostałych urządzeń:
   - **a)** Serwer: 560 VA · 1,4 = 784 VA
   - **b)** Monitor: 112 VA · 1,2 = 134,4 VA
   - **c)** Przełącznik: 140 VA · 1,2 = 168 VA
   - **d)** Router: 98 VA · 1,2 = 117,6 VA
2. Suma obliczonych mocy nadmiarowych (1204 VA) wskazuje na minimalną moc pozorną zasilacza UPS odpowiednią dla urządzeń o wskazanych parametrach.

Wybierając zasilacz awaryjny dla sieci, należy brać pod uwagę następujące parametry:

- Moc zasilacza, która pozwala określić moc podłączanych urządzeń.
- Czas pracy na akumulatorze — określa czas podtrzymania energii w podłączanych urządzeniach przy maksymalnym lub procentowym obciążeniu.

- Liczbę gniazd wyjściowych.
- Możliwość montażu w szafie typu rack.
- Możliwość wyprowadzenia gniazd na listwę zasilającą montowaną w szafie — pozwala na łatwiejsze zarządzanie przewodami zasilającymi.
- Złącza komunikacyjne — są to złącza, które mogą sterować podłączanymi urządzeniami — w przypadku przełączenia na tryb pracy na baterii lub osiągnięcia poziomu wyczerpania baterii wysyłany jest sygnał do podłączanego urządzenia, które może rozpocząć pracę w trybie oszczędzania energii lub rozpocząć procedurę wyłączenia. Typy oraz liczba złączy komunikacyjnych występujących w zasilaczach awaryjnych zależą od modelu urządzenia; najczęściej są to złącza **RS232 (DB9)**, **USB** lub **RJ-45**.
- Dołączone oprogramowanie sterujące — w celu zapewnienia poprawnej komunikacji zasilacza UPS z urządzeniem niezbędne jest zainstalowanie oprogramowania, które reaguje na odbierane sygnały. Wybierając urządzenie, należy zwrócić uwagę, czy dostarczone oprogramowanie jest kompatybilne z systemami operacyjnymi, które mają pracować na chronionych serwerach. Warto również zapoznać się z jego możliwościami w zakresie powiadamiania administratorów — część z nich pozwala na wyświetlanie informacji na ekranie serwera, część potrafi wysłać wiadomość pocztą elektroniczną lub nawet przy użyciu SMS-a.

9.2.6. Rozmieszczenie elementów w szafach dystrybucyjnych

Jeśli do całej sieci został dobrany sprzęt — zarówno aktywny, jak przełączniki, routery czy serwery, jak również pasywny, tj. panele krosowe, listwy zasilające czy prowadnice kabli — należy zaprojektować rozmieszczenie tych elementów wewnątrz szaf dystrybucyjnych. Nie istnieją żadne normy określające układ elementów w szafach. Poniżej przedstawione zostały dobre praktyki pozwalające na zachowanie lepszej ergonomii pracy ze sprzętem instalowanym wewnątrz szaf.

Gdy zna się liczbę oraz moc poszczególnych urządzeń, można dobrać odpowiednie panele chłodzące do szaf (wentylatory). Najczęściej wentylatory są montowane w górnej ścianie szafy. W przypadku większej ilości generowanego ciepła stosuje się specjalne cokoły, w których montuje się wentylatory. Górne wentylatory odprowadzają gorące powietrze z wnętrza szafy, dolne zasysają chłodne powietrze z pomieszczenia.

Zasady montażu elementów sieci wewnątrz szafy określają umiejscowienie elementów od najcięższych (na dole szafy) do najlżejszych (na górze szafy).

Na dole najczęściej są montowane zasilacze awaryjne ze względu na ich wagę, powyżej montuje się serwery w obudowach typu rack na specjalnych szynach lub półki, na których mogą być ustawione serwery w obudowach typu tower.

Należy pamiętać, że pomiędzy urządzeniami aktywnymi, takimi jak serwery czy przełączniki, które generują dużo ciepła, należy zostawiać przestrzeń o wysokości co najmniej 1 U w celu zapewnienia odpowiedniej cyrkulacji powietrza. Producenci szaf

dystrybucyjnych w swojej ofercie mają specjalne panele maskujące, które pozwalają zakryć występujące przerwy między urządzeniami oraz zapewniają estetyczny i przejrzysty wygląd całości.

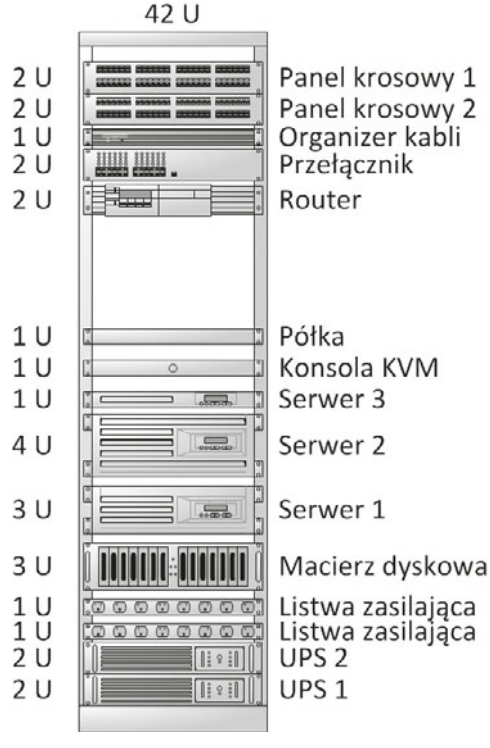
Jeżeli istnieje konieczność instalacji konsoli KVM, zaleca się zainstalowanie jej na wygodnej do pracy wysokości. Jeśli zamiast konsoli KVM wewnątrz szafy ma się znaleźć monitor i klawiatura, zaleca się montaż wysuwanej półki (na wysokości zgiętych w łokciach rąk), na której zostanie umieszczona klawiatura, oraz stałej półki przymocowanej do wewnętrznej konstrukcji, gdzie zostanie usytuowany monitor.

Na górze szafy montuje się panele krosowe, poziome organizery kabli oraz aktywne urządzenia sieciowe — przełączniki, routery czy sprzętowe firewalle.

Dobrą praktyką jest montaż paneli światłowodowych na samej górze szafy. Pozwala to nie narażać delikatnych światłowodowych kabli krosowych na przypadkowe uszkodzenia.

Do tylnej konstrukcji szafy najczęściej montowane są listwy zasilające — pozwalają one na podłączanie zasilania do poszczególnych urządzeń bezpośrednio w szafie dystrybucyjnej.

Rysunek 9.12 przedstawia przykładowe ułożenie elementów wewnątrz szafy dystrybucyjnej, zapewniające wygodną pracę i swobodny przepływ generowanego ciepła wewnątrz szafy.



Rysunek 9.12. Przykładowe ułożenie elementów wewnątrz szafy dystrybucyjnej

9.2.7. Kosztorysowanie projektowanych sieci komputerowych

Kosztorys jest dokumentem finansowym określającym koszty przedsięwzięcia. Kosztorys sieci komputerowych może być sporządzony na etapie składania oferty (szacunkowy kosztorys powstały na podstawie przekazanego zapytania ofertowego), na etapie tworzenia projektu (kosztorys wyceniający użyte materiały oraz szacowany koszt nakładu prac) lub po wykonaniu wszystkich założonych prac (kosztorys powykonawczy).

Różnice występujące pomiędzy poszczególnymi kosztorysami dotyczą dokładności wyliczeń — kosztorys ofertowy powstaje najczęściej na bazie niezweryfikowanych założeń przekazanych przez zamawiającego, a więc często kosztorysant nie jest w stanie precyzyjnie określić całkowitego nakładu pracy oraz dokładnej ilości okablowania, kanałów czy innego sprzętu niezbędnego do zbudowania poprawnie działającej sieci zgodnej z wymaganiami zamawiającego.

Kosztorys powstający na podstawie projektu zawiera zdecydowanie dokładniejsze dane — poszczególne elementy są wyceniane na podstawie dokładnego projektu sieci, więc projektant powinien być w stanie przewidzieć wszystkie materiały i prace niezbędne do wykonania prawidłowo działającej sieci.

Kosztorys powykonawczy jest sporządzany w celu określenia całości wydatków poniesionych na zbudowanie sieci. Zawiera on najczęściej całość kosztów z dokładnym rozbiciem na użyte materiały, sprzęt oraz zasoby ludzkie.

Kosztorys tworzony przy projekcie sieci może składać się jedynie z wykazu wszystkich planowanych elementów sieci (okablowanie strukturalne, urządzenia sieciowe), jak również z wykazu prac niezbędnych do wykonania wraz z cenami. Zakres kosztorysu zależy od wymagań zamawiającego — projekt sieci może być tworzony np. w celu wystosowania zapytania do potencjalnych instalatorów — wówczas koszty prac nie są elementem kosztorysu.

Kosztorys składa się z wykazu planowanych elementów, które mają być użyte — nazwy elementu, producenta, modelu urządzenia wraz z jednostką miary, ilością, kosztem jednostkowym oraz kosztem całkowitym.

W celu zwiększenia przejrzystości kosztorys może zostać podzielony na części odpowiadające kolejnym elementom budowanej sieci lub ich lokalizacji czy też funkcji, np. punktom dystrybucyjnym albo budynkom, piętrom lub pomieszczeniom.

Jeżeli kosztorys tworzy inwestor, powinien w nim umieścić informację o źródłach cen oraz dacie ich pozyskania.

WSKAZÓWKA

Określenie dat przy oferowanych cenach pozwoli zabezpieczyć się przed roszczeniami zamawiającego — ceny sprzętu komputerowego podlegają dużym wahaniom w czasie.

Fragment przykładowego kosztorysu sieci komputerowej został przedstawiony w tabeli 9.2.

Tabela 9.2. Fragment przykładowego kosztorysu sieci komputerowej

Okablowanie strukturalne							
Lp.	**Nazwa**	**Producent**	**Symbol producenta**	**Jednostka miary**	**Ilość**	**Cena netto (PLN)**	**Wartość**
1	PatchCord 0,5 m	ABC	PC 3202-05	szt.	20,00	3,00	60,00
2	PatchCord 2 m	ABC	PC 3202-20	szt.	25,00	5,00	125,00
3	Puszka n/t 80 2 mod	ABC	PC 34nt2-80	szt.	20,00	1,00	20,00
4	Ramka do puszki 80	ABC	RC 34nt2-80	szt.	20,00	1,00	20,00
5	Moduł 2xRJ-45	ABC	MC RJ-2x	szt.	10,00	5,00	50,00
6	Okablowanie UTP 305 m	ABC	CC UTP305	opak.	2,00	309,00	618,00
7	Patch Panel 24 porty 1 U	ABC	PP C5-24	szt.	1,00	134,00	134,00
8	Szafa dystrybucyjna 32 U	ABC	SD 32U-GL	szt.	1,00	1450,00	1450,00
9	Organizer pionowy 1 U	ABC	SO 1U	szt.	1,00	44,00	44,00
10	Półka do szafy 19″	ABC	SD P13	szt.	2,00	89,00	178,00
11	Panel chłodzący 19″	ABC	SC C1500-2	szt.	2,00	398,00	796,00
						Razem	**3495,00**
Oferta z 14.04.2012 r.							

Przy wycenie prac niezbędnych do wykonania sieci można korzystać z norm określonych na podstawie publikowanych cyklicznie katalogów norm rzeczowych (tzw. KNR) stanowiących zestawienie opisujące m.in. ceny dla określonych prac. Tego typu rozwiązania są stosowane głównie przy dużych projektach i najczęściej przez kosztorysantów budowlanych. Przy projektach niewielkich sieci lokalnych częściej stosuje się przyjęte ceny wykonania większego zakresu prac, np. montażu gniazda abonenckiego, który obejmuje przeciągnięcie kabla do punktu dystrybucji, zaszycie w panelu krosowym oraz gnieździe, przymocowanie gniazda do ściany, opisanie gniazda i portu w panelu krosowym i późniejsze testy. Przy wycenach większych sieci konieczne jest wykorzystanie katalogów norm rzeczowych.

Tworzenie kosztorysów sieci komputerowych jest zadaniem odpowiedzialnym, gdyż zaproponowane w kosztorysie ceny mają bezpośrednie przeliczenie na ponoszone koszty zamawiającego czy też zyski wykonawcy. O ile stworzenie kosztorysu użytych

elementów i materiałów jest stosunkowo proste, o tyle kosztorysowanie prac wymaga więcej doświadczenia, najlepiej zdobytego podczas prac instalacyjnych — pozwala to uniknąć błędnych kalkulacji i założeń dla wykonywanych prac. Dla przykładu montaż gniazd na ścianach kartonowo-gipsowych jest zdecydowanie prostszy i szybszy niż w przypadku ścian z gazobetonu; przewiert w ścianie działowej wymaga mniej nakładów niż przewiert w zbrojonym stropie itp.

WSKAZÓWKA

Przy tworzeniu kosztorysu prac należy wziąć pod uwagę również konieczność używania (zakupu/wypożyczania/amortyzacji) niezbędnego sprzętu, np. wiertarki do wykonywania przewiertów, testera okablowania czy spawarki do światłowodów.

9.2.8. Dokumentacja powykonawcza sieci

Dokumentacja powykonawcza sieci stanowi pełny opis przyjętych założeń projektowych, zastosowanych rozwiązań oraz przeprowadzonych testów. Nie istnieją wytyczne dotyczące wyglądu dokumentacji sieciowej, niemniej jednak pewne stałe elementy powinny być w niej zawarte. Przykładowa struktura dokumentacji wraz z opisem poszczególnych zagadnień przedstawiona została poniżej.

1. Informacje ogólne — rozdział zawierający wstępne informacje dotyczące sieci — kto jest zleceniodawcą projektu, gdzie dana sieć jest projektowana, jakie są podstawowe wymagania stawiane projektowanej sieci oraz jakie założenia w związku z tym zostały przyjęte.
2. Normy i zalecenia techniczne — w tym rozdziale należy wskazać normy, na podstawie których sieć została zaprojektowana, zarówno polskie, jak i międzynarodowe.
3. Ogólna struktura sieci — rozdział powinien zawierać opis logicznej struktury sieci wraz z uzasadnieniem przyjętych rozwiązań. Należy pokazać logiczne projekty sieci, podział na sieci wirtualne, główne elementy systemu.
4. Okablowanie — rozdział dotyczący okablowania powinien zawierać opis przyjętych rozwiązań dla poszczególnych elementów sieci — okablowania kampusowego, pionowego oraz poziomego. Dla każdego z nich należy określić wybranego producenta, parametry użytego medium, sposoby jego zakańczania, sposoby montażu i oznaczania. Należy też wskazać przyjęte założenia dotyczące kanałów kablowych oraz sposobów realizacji przebiegów między budynkami (na powierzchni, w dzierżawionych studzienkach telekomunikacyjnych itp.). W tym rozdziale należy przedstawić schemat dotyczący identyfikacji poszczególnych przebiegów kablowych.
5. Punkty dystrybucyjne — rozdział powinien zawierać opis poszczególnych punktów dystrybucji — szaf wraz z wyposażeniem, rodzaju sprzętu, użytych zabezpieczeń, wymagań dotyczących chłodzenia itp. Należy również dołączyć informacje dotyczące poszczególnych przebiegów kablowych zakończonych w konkretnych punktach dystrybucyjnych.

6. Opis instalacji zasilającej — przy tworzeniu sieci zasilającej ten rozdział powinien zawierać projekt sieci elektrycznej lub w innym przypadku wymagania stawiane dla sieci energetycznej w poszczególnych jej obszarach.
7. Elementy sieci — ten rozdział dokumentacji zawiera wykaz sprzętu użytego w projekcie wraz z jego parametrami technicznymi. Dotyczy to zarówno urządzeń aktywnych, tj. przełączników, routerów, serwerów (ze wskazaną wersją oprogramowania), jak również elementów pasywnych — szaf dystrybucyjnych, paneli krosowych, gniazd itp.
8. Wyniki testów — ten rozdział powinien zawierać opis przyjętej metodologii testowania sieci, opis narzędzi testujących oraz wyniki testów poszczególnych przebiegów kablowych oraz urządzeń.
9. Rysunki i schematy — ten rozdział powinien zawierać niezbędne rysunki i schematy wyjaśniające rozmieszczenie i działanie sieci, np. schemat rozmieszczenia gniazd w panelach, schemat połączeń między punktami dystrybucyjnymi, schematy poszczególnych kondygnacji wraz z rozmieszczeniem i numeracją gniazd, oznaczonymi przebiegami okablowania, przebiciami między piętrami. Ze względu na brak ogólnie przyjętych oznaczeń elementów sieci na rysunkach każdy z nich powinien być opatrzony legendą wyjaśniającą użyte na rysunku symbole.

Dobrze zrobiona dokumentacja stanowi bardzo istotną część sieci — pozwala administratorom na sprawne i szybkie wyszukanie niezbędnych informacji dotyczących charakterystyki sieci, a także umożliwia nowym pracownikom poznanie szczegółów jej budowy.

Podczas użytkowania sieci dokumentacja powinna być aktualizowana — informacje o wszelkich zmianach w sieci, czy to wymianie urządzenia, czy przepięciu kabla krosowego, należy dołączyć do dokumentacji.

WSKAZÓWKA

W celu łatwiejszego zarządzania zmianami w dokumentacji sieci warto do elektronicznego dokumentu wprowadzić tabelę informującą o wersji dokumentu, dacie i autorze aktualizacji oraz zakresie wprowadzonych zmian.

9.2.9. Montaż elementów okablowania oraz urządzeń sieciowych

Instalacja większości sprzętu sieciowego nie wymaga specjalnych narzędzi — wyjątkiem są przyrządy do zakańczania okablowania (gniazda, panele krosowe, wtyki RJ-45). Aby zamontować urządzenia w szafie dystrybucyjnej, potrzebny jest jedynie śrubokręt oraz ewentualnie opaski zaciskowe do łączenia przewodów.

Instalacja okablowania

Właściwa instalacja okablowania składa się z tzw. etapu surowego, który obejmuje montowanie kabli w stropach, ścianach i kanałach, oraz etapu przycinania, podczas którego następuje przycinanie, zakańczanie przewodów i układanie ich w organizerach.

Etap surowy

Na etapie surowym montuje się okablowanie. Najczęściej jest ono montowane w plastikowych korytach lub metalowych rynnach kablowych. Dobór koryt i rynien powinien uwzględniać ilość oraz średnicę okablowania, które ma być prowadzone danym kanałem, a także jego wagę. W sprzedaży jest dostępny szereg systemów kanałów kablowych wielu producentów — w ofercie znajdują się kanały i kształtki (trójniki, narożniki) o różnej szerokości oraz grubości, które pozwalają na upakowanie różnej ilości kabli. Dodatkowo oferowane są różnego rodzaju gniazda montowane na kanałach lub poza nimi, co pozwala na lepszą aranżację i dostosowanie przebiegów okablowania do wymagań zamawiającego.

Montując pionowe przebiegi okablowania między piętrami, należy korzystać z szybów lub rękawów zabezpieczających otwory w stropach. W przypadku montażu nad podwieszanym sufitem lub pod podniesioną podłogą dopuszcza się możliwość mocowania okablowania do uchwytów kablowych rozmieszczonych w odległości 120 – 150 cm, niedopuszczalne jest natomiast mocowanie kabli do konstrukcji nośnej podwieszanego sufitu lub podniesionej podłogi.

Po przygotowaniu kanałów kablowych odpowiedniej wielkości i zamocowaniu ich zgodnie z zaleceniami producenta można rozpocząć właściwe układanie kabli. Należy pamiętać, że każdy pojedynczy przebieg powinien być oznakowany informacją, dokąd okablowanie prowadzi na każdym końcu — ułatwi to identyfikację poszczególnych kabli w szafach dystrybucyjnych.

WSKAZÓWKA

Aby zapewnić łatwiejszą identyfikację i montaż okablowania w panelu krosowym, najlepiej prowadzić okablowanie z jednego obszaru roboczego, następnie pogrupować przewody wewnątrz szafy dystrybucyjnej i dopiero po tym etapie rozpocząć pracę nad okablowaniem kolejnego obszaru roboczego.

Do grupowania okablowania doskonale nadają się plastikowe opaski zaciskowe, należy jednak pamiętać, aby nie zaciągać ich zbyt mocno, gdyż może to spowodować zgniecenie wewnętrznej struktury kabla, a co za tym idzie, negatywnie wpłynąć na parametry transmisji.

Okablowanie prowadzone wewnątrz szafy do panelów krosowych może być montowane w specjalnych pionowych organizerach kabli lub mocowane do tylnej części ramy wewnątrz szafy rack.

Najważniejsze wytyczne dotyczące montażu okablowania zostały przedstawione poniżej:

- Wszystkie przebiegi kablowe powinny kończyć się w szafach dystrybucyjnych lub w gniazdach.
- Należy przestrzegać wymagań producenta w zakresie minimalnego promienia zgięcia okablowania — dla kabla typu skrętka przyjmuje się promień skrętu równy ośmiokrotności średnicy, dla światłowodu — dwudziestokrotność.
- Należy przestrzegać maksymalnej dopuszczalnej długości rozplotu kabla, wynoszącej w przypadku skrętki 13 mm.
- Należy przestrzegać dopuszczanej przez producenta maksymalnej siły naciągu kabla podczas instalacji.
- Należy zachować zalecane odległości od źródeł zakłóceń, takich jak źródła ciepła czy urządzenia elektryczne. Dopuszcza się montaż okablowania w odległości 30 cm od wysokonapięciowych źródeł światła (świetlówek), 90 cm od przewodów elektrycznych o mocy 5 kVA (lub większej) oraz 100 cm od transformatorów i silników.
- Na zewnątrz budynków należy używać specjalnego okablowania przeznaczonego do tego celu.

WSKAZÓWKA

Aby możliwa była łatwa identyfikacja okablowania wyprowadzonego w kanałach kablowych oraz w szafach dystrybucyjnych, należy stworzyć spójny schemat oznaczania okablowania, kanałów kablowych oraz gniazd. Warto opracować jednolity sposób oznaczenia, który będzie jednoznacznie wskazywał budynek (w sieciach obejmujących wiele budynków), numer punktu dystrybucji, numer panelu krosowego w punkcie dystrybucji oraz numer portu na panelu lub numer pomieszczenia, gniazda telekomunikacyjnego i portu, np.:

- B1-PD04-PK1_23 — oznacza połączenie zakończone w budynku nr 1, punkt dystrybucji nr 4, panel krosowy nr 1, port nr 23;
- B3-P12-G4_2 — oznacza gniazdo zakończone w budynku nr 3, pokój nr 12, gniazdo nr 4, port nr 2.

W projektach fizycznych konieczne jest dokładne oznaczenie przebiegów kablowych, co pozwoli wyliczyć niezbędną ilość okablowania oraz koryt kablowych wraz z dodatkowymi akcesoriami. Na całkowitą długość kabla składają się następujące odcinki:

- od panelu krosowego do podstawy szafy;
- od podstawy szafy do ściany;
- odcinki poziome wzdłuż ścian;
- odcinki pionowe rozprowadzające okablowanie na ścianach;
- grubość stropów oraz ścian, przez które jest prowadzone okablowanie;
- około 50 cm nadmiaru okablowania w gnieździe telekomunikacyjnym;
- około 50 cm nadmiaru w szafie telekomunikacyjnej.

Przyjmuje się, że na etapie zamawiania okablowania należy powiększyć jego ilość o 10–30% względem wyliczeń wynikających z obliczeń odcinków nanoszonych na plany budynków.

UWAGA

Podczas montażu wszelkich urządzeń należy stosować się do zaleceń producenta oraz bezwzględnie przestrzegać zasad BHP, które pozwolą zmniejszyć ryzyko utraty zdrowia i życia podczas pracy.

Etap przycinania

Na etapie przycinania tworzy się zakończenia okablowania — prowadzone wcześniej przebiegi kablowe są mocowane w gniazdach lub panelach (rysunek 9.13), dodatkowo są układane w organizerach kabli.

Rysunek 9.13.
Urządzenie do zaciskania okablowania we wtykach typu 110

UWAGA

Aby zabezpieczyć przed zniszczeniem aktywny sprzęt sieciowy, podczas zakańczania okablowania należy bezwzględnie odłączyć drugi koniec okablowania z urządzenia.

Zaciskanie wtyków typu 110

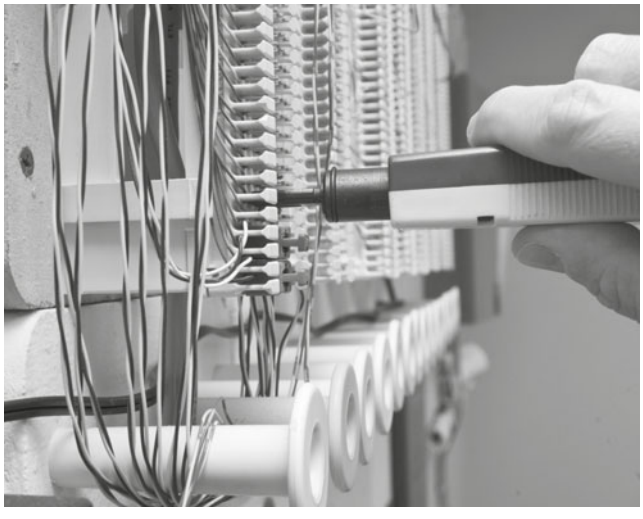
Gniazda telekomunikacyjne oraz panele krosowe są wyposażone we wtyki typu 110, które do poprawnego montażu wymagają specjalnego narzędzia — noża krosowniczego, zwanego także nożem krone lub nożem uderzeniowym (ang. *punch down tool*), służącego do wciskania i przycinania poszczególnych żył okablowania.

Aby rozpocząć zakańczanie przewodów miedzianych, należy ustalić przyjęty standard układu przewodów dla całej sieci (TIA/EIA 568A lub TIA/EIA 568B). Mówią one o kolejności poszczególnych żył (kolorów) w gnieździe. Panele na tylnych złączach mają zaciski oznaczone kolorami właściwymi dla jednego lub obydwu standardów, co pozwala na właściwe zaszycie przewodów.

Po ustaleniu używanego standardu należy:

1. Zdjąć około 5 cm izolacji zewnętrznej przewodu.
2. Rozpleść poszczególne przewody.
3. Ułożyć poszczególne przewody na właściwych zaciskach przy zachowaniu minimalnej odległości od zakończenia izolacji do zacisku.
4. Przy użyciu noża krosowniczego wcisnąć przewody do zacisków.
5. Jeżeli nóż krosowniczy nie ma elementu tnącego nadmiarowe okablowanie, należy je usunąć za pomocą innego narzędzia.

Kolejne kroki zaciskania wtyków typu 110 pokazuje rysunek 9.14.



Rysunek 9.14. Zaciskanie wtyków typu 110

Zaciskanie wtyków RJ-45

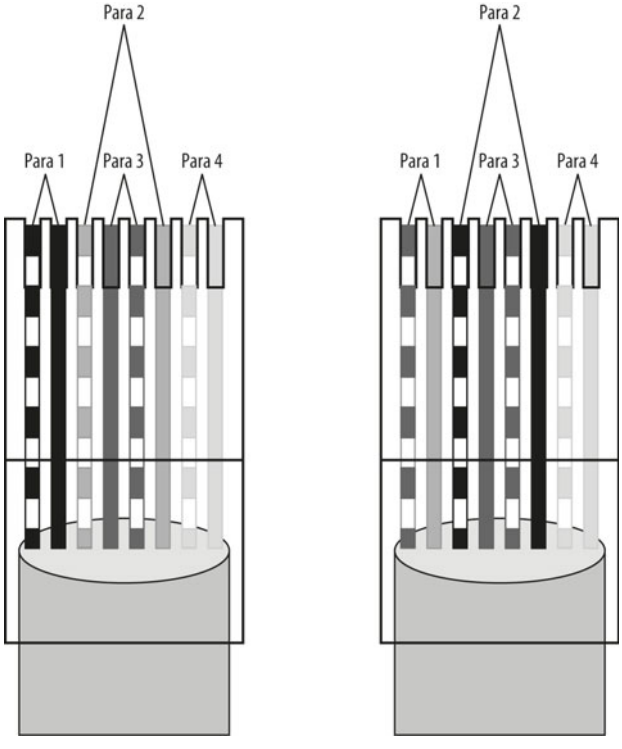
Do utworzenia połączenia pomiędzy elementami sieci (panelami krosowymi, przełącznikami, gniazdem telekomunikacyjnym) jest potrzebny kabel krosujący lub kabel połączeniowy. W tym typie okablowania najczęściej wykorzystuje się kabel typu skrętka; na obu końcach jest on zakończony gniazdem RJ-45.

Standard Ethernet określa, że każdy ze styków złącza RJ-45 ma specyficzne zadanie. Karta sieciowa wysyła sygnały przez styki 1. i 2., a odbiera na stykach 3. i 6. Przewody w skrętce muszą być podłączone do odpowiednich styków na obu końcach kabla (rysunek 9.15).

Standard TIA/EIA 568A definiuje następujący układ kolorów:

Biało-zielony, zielony, biało-pomarańczowy, niebieski, biało-niebieski, pomarańczowy, biało-brązowy, brązowy; z kolei standard TIA/EIA 568B wymienia kolory: biało-pomarańczowy, pomarańczowy, biało-zielony, niebieski, biało-niebieski, zielony,

biało-brązowy, brązowy. Kolejność kolorów jest podana dla wtyczki odwróconej zatrzaskiem w dół.



Rysunek 9.15. Standardy układu przewodów we wtyczce RJ-45 (TIA/EIA 568A oraz TIA/EIA 568B)

Przy budowie sieci z wykorzystaniem technologii Ethernet stosuje się dwa rodzaje kabli:

- prosty (ang. *straight-through*),
- skrosowany (ang. *crossover*).

Wersja **prosta** służy do łączenia urządzenia końcowego (np. komputera, drukarki itp.) z koncentratorem lub przełącznikiem. Obie końcówki kabla mają taki sam układ przewodów.

Wersja **skrosowana** służy do łączenia komputerów bez pośrednictwa koncentratora/przełącznika lub do łączenia koncentratorów/przełączników. W tym przypadku na końcach kabli zamienione są miejscami przewody 1. i 2. z 3. i 6.

W celu utworzenia kabla krosującego lub połączeniowego niezbędne są:

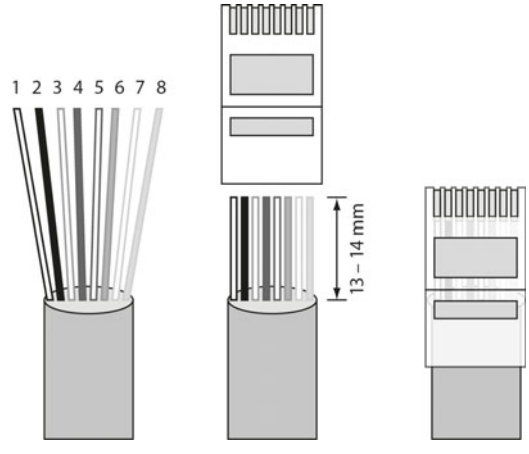
- kabel typu skrętka,
- wtyczki RJ-45,
- urządzenie do zaciskania wtyków RJ-45 (ang. *crimping tool*),

W celu uzyskania poprawnego kabla należy:

1. Odciąć wymaganą długość przewodu z zachowaniem kilku centymetrów zapasu.
2. Zdjąć izolację zewnętrzną kabla na długości 5 cm.
3. Rozpleść poszczególne splecione pary i wyprostować skręcenia poszczególnych przewodów.
4. Ułożyć kolejność przewodów zgodnie z wybranym schematem. Dla kabla prostego — dwa końce powinny być zaciśnięte w tym samym standardzie (TIA/EIA 568A lub TIA/EIA 568B), dla kabla skrosowanego — jeden koniec powinien być zakończony zgodnie ze standardem TIA/EIA 568A, a drugi zgodnie ze standardem TIA/EIA 568B.
5. Ułożone przewody wyprostować, chwytając jak najbliżej izolacji i przesuwając po nich zaciśnięty kciuk oraz palec wskazujący drugiej dłoni.
6. Należy skrócić rozplecione przewody do maksymalnie 13 mm — dopuszczalnego rozplotu kabla dla tego rodzaju przewodu oraz zapewnić, że podczas zaciskania element trzymający izolację zaciskany we wtyczce zostanie właściwie umieszczony, co pozwoli chronić tworzony kabel przed przypadkowym wyciągnięciem go z wtyczki.
7. Tak przycięte przewody należy wsunąć do niezaciśniętej wtyczki RJ-45. Należy pamiętać, że układ kolorów wybranego schematu mówi o ułożeniu kolorów dla wtyczki odwróconej zatrzaskiem zabezpieczającym w dół. Wewnątrz wtyczki znajdują się rowki, które pozwalają równo prowadzić poszczególne przewody oraz zapobiegają przypadkowej zmianie ich kolejności. Przewody powinny być maksymalnie dociśnięte do przedniej (czołowej) ściany wtyczki.
8. Przed właściwym zaciśnięciem należy sprawdzić poprawność ułożenia kolorów przewodów wewnątrz wtyczki oraz dosunięcie przewodów do czoła wtyczki.
9. Należy wsunąć wtyczkę w odpowiednie miejsce w zaciskarce i mocno ścisnąć.
10. Po wyjęciu wystarczy odgiąć dolny zatrzask zabezpieczający.

Kolejne etapy zaciskania pokazuje rysunek 9.16.

Rysunek 9.16.
Kolejne etapy zaciskania wtyczki RJ-45



WSKAZÓWKA

Aby ułatwić sobie pracę, izolacje zewnętrzne można zdejmować przy użyciu specjalnych nacinarek izolacji.

Większość zaciskarek ma noże tnące do przycinania i wyrównywania kabli umieszczone w rączkach; pozwalają one na szybkie i sprawne skrócenie kabli i przewodów.

W sprzedaży są oferowane osłony na wtyczki RJ-45, które mogą, ale nie muszą, być zamontowane na okablowaniu. Ich użycie pozwala ochronić przed złamaniem dolny zatrzask zabezpieczający.

Łączenie światłowodów

Łączenie światłowodów może odbywać się na dwa sposoby — za pomocą złączek lub specjalnej spawarki. W przypadku połączeń na krótkie odległości są stosowane złącza mechaniczne. Dla długich odcinków, gdzie kluczowa jest minimalizacja strat, najczęściej stosuje się połączenia spawane.

Połączenia przy użyciu złączy mechanicznych nie są wykonywane na stałe — podłączone końcówki mogą być przełączane do innych przewodów inaczej niż w przypadku stałych połączeń spawanych.

Rysunek 9.17.
Złącza światłowodowe typu ST

Instalacja urządzeń w szafach telekomunikacyjnych

Urządzenia wewnątrz szaf telekomunikacyjnych są montowane do ramy montażowej — specjalnej konstrukcji wewnątrz szafy, na której są wykonane kwadratowe otwory. Na jednostkę 1 U składają się 4 otwory rozmieszczone na tej samej wysokości po lewej i prawej części ramy.

Urządzenia są mocowane w szafie za pomocą śrub i specjalnych koszyków. Wewnątrz tych ostatnich na stałe montuje się nakrętki, na których są wkręcane śruby (rysunek 9.18). Koszyki wkłada się w otwory wewnątrz ramy montażowej. Poprawnie zamontowane urządzenie przymocowane jest 4 śrubami.

Rysunek 9.18.
Zestaw montażowy do szaf typu rack

Większość sprzętu pasywnego, takiego jak panele krosowe, półki czy zasilacze awaryjne, jest wyposażona w specjalne uchwyty dostosowane do montażu na szynach montażowych w szafach typu rack. Obudowy urządzeń aktywnych, takich jak routery, przełączniki czy serwery, nie mają takich uchwytów — aby je poprawnie zamontować, należy wykorzystać specjalne uchwyty (przełączniki, routery) bądź szyny (serwery) przykręcane do bocznych ścian urządzenia.

Po właściwym zamocowaniu urządzeń w szafie, zaszyciu okablowania i opisaniu poszczególnych gniazd w panelach krosowych można przystąpić do łączenia okablowania z urządzeniami.

Podłączenie najlepiej rozpocząć od podłączenia klawiatury, myszy oraz monitora lub przełącznika KVM do serwerów. W następnej kolejności można podłączyć zasilanie do zasilaczy awaryjnych lub do listew zasilanych bezpośrednio z sieci elektrycznej. W przypadku serwerów należy również podłączyć okablowanie zapewniające komunikację pomiędzy zasilaczami awaryjnymi a serwerami, tak by w razie potrzeby można je było wyłączyć.

Ze względu na ergonomię pracy okablowanie sieciowe powinno być podłączane na końcu — przewody zasilające oraz przewody łączące klawiaturę, monitor i myszkę są montowane na stałe i najczęściej nie wymagają przełączania, tak jak ma to miejsce w przypadku okablowania sieciowego.

Okablowanie sieci strukturalnej może być podłączane do włączonych (działających) urządzeń sieciowych; pozwala to na rekonfigurację sieci bez konieczności zakłócania jej pracy.

9.2.10. Pomiary i certyfikacja sieci

Testowanie okablowania jest bardzo ważnym etapem budowy sieci komputerowej. Pozwala ono na weryfikację poprawnego działania poszczególnych przebiegów kablowych.

Normy mówią o wykonaniu dwóch rodzajów testów — testów statycznych dotyczących fizycznych połączeń przewodów oraz testów dynamicznych weryfikujących parametry transmisji.

Testy statyczne pozwalają na zdiagnozowanie następujących uszkodzeń:

- Przerw w obwodzie — polegających na przerwaniu ciągłości przewodu w kablu, spowodowanych najczęściej błędami przy jego zakańczaniu lub uszkodzeniem kabla na etapie instalacji.
- Zwarć — polegających na zetknięciu przewodów wewnątrz kabla, którym mają być przesyłane dane.
- Rozdzielenia par — polegającego na pomieszaniu przewodów pomiędzy parami.
- Błędów mapowania połączeń — polegających na zamianie kolejności poszczególnych przewodów na jednym końcu względem drugiego zakończenia.

Do przeprowadzenia testów statycznych wystarczą proste mierniki, które badają jedynie przepływ prądu pomiędzy zakończeniami. Do przeprowadzenia kompletnych testów

okablowania są potrzebne zaawansowane urządzenia testujące, które pozwalają na testowanie mechaniczne i dynamiczne takich parametrów jak:

- Mapowanie połączeń — określenie przebiegów poszczególnych przewodów w kablu.
- Tłumienie — wskazanie strat sygnału w torze transmisyjnym. Parametr jest określany w dB.
- Straty odbiciowe (ang. *return loss*) — to miara pokazująca niedopasowanie impedancyjne i niejednorodności całego odcinka kablowego. W przypadku niejednorodności nośnika sygnały mogą zostać odbite i niekorzystnie wpływać na przesyłane dane.
- Opóźnienie propagacji sygnału (ang. *delay*) — wskazuje czas, w jakim impuls jest przenoszony z jednego końca kabla na drugi. Parametr jest określany w ns.
- Różnica opóźnień (ang. *delay skew*) — jest to różnica między najmniejszą i największą wartością opóźnienia w torze transmisyjnym mierzona na każdej z par w kablu.
- Długość kabla — pozwala określić długość mierzonego kabla oraz poszczególnych par — każda para ma inny skręt, co zmienia długości poszczególnych par na całej długości kabla. Najczęściej parametr ten jest określany w metrach.
- Impedancja — parametr związany z właściwościami geometrii kabla (grubość drutów, odległość pomiędzy nimi, izolacja) i właściwościami dielektryka stanowiącego izolację w przewodach. Niedopuszczalne jest stosowanie kabli o różnych impedancjach charakterystycznych w jednym systemie okablowania.
- Przesłuchy — jest to zjawisko przenikania sygnału pomiędzy sąsiadującymi w kablu parami przewodów. Zbyt duży przesłuch powoduje zakłócenia komunikacji w sieci.

Istnieje możliwość zdiagnozowania następujących rodzajów przesłuchów:

- NEXT (ang. *Near End Crosstalk* — przesłuch zbliżny) — występuje, gdy sygnały z jednej pary zakłócają sygnał innej pary na bliższym końcu kabla.
- PSNEXT (ang. *Power Sum NEXT* — przesłuch zbliżny skumulowany w jednej parze) — występuje, gdy w kablu są wykorzystywane wszystkie przewody, sygnały w jednej parze interferują z przesłuchami z innych par.
- ELFEXT (ang. *Equal Level Far-End Crosstalk* — wyrównany współczynnik przesłuchu zdalnego) — określany podobnie jak NEXT, ale poziom sygnału jest mierzony na odległym końcu toru.
- PSELFEXT (ang. *Power Sum Equal Level Far-End Crosstalk* — wyrównany współczynnik przesłuchu zdalnego skumulowany w jednej parze) — skumulowany współczynnik ELFEXT.

Istnieje możliwość uzyskania certyfikatu producenta gwarantującego spełnianie określonych wymagań przez budowaną sieć. W tym celu należy przeprowadzić testy sieci z użyciem certyfikowanego testera, który przeprowadza wszystkie wymagane testy wydajnościowe sieci. Jeśli uzyskane wartości nie przekraczają poziomów dopuszczalnych przez normy, świadczy to o spełnianiu określonych parametrów, co pozwala wydać certyfikat danej normy.

Ważnym elementem certyfikacji sieci jest jej dokumentacja. Mierniki certyfikowane mają wewnętrzną pamięć, w której są zapisywane wyniki przeprowadzonych testów, a dołączane oprogramowanie pozwala na generowanie raportów, wykresów i innych danych w celu przygotowania wysokiej jakości dokumentacji.

9.3. Modernizacja sieci komputerowej

Modernizacja sieci komputerowej ma za zadanie dostosowanie jej do nowych wymagań. Mogą to być modyfikacje związane z wprowadzeniem nowych usług sieciowych, zmianą lokalizacji, dołączeniem kolejnego obszaru roboczego czy zwiększeniem przepustowości sieci. Projekt modernizacji sieci można wykonać w sposób zbliżony do projektu nowej sieci, przy czym urządzenia, technologia i funkcjonalności muszą być kompatybilne z istniejącą siecią.

Po przeprowadzeniu analizy biznesowej należy przeprowadzić diagnozę istniejącej sieci. O ile jest dostępna aktualna dokumentacja sieci, prace te nie stanowią większego utrudnienia. Jeśli dokumentacja nie jest prowadzona, należy przeprowadzić inspekcję (inwentaryzację) sieci lub jej fragmentu, w którym będzie modernizowana. Na tej podstawie trzeba określić elementy infrastruktury, działające protokoły sieciowe, użyty sprzęt, liczbę wolnych portów w urządzeniach sieciowych, ilość wolnego miejsca w kanałach kablowych, działające serwery i usługi sieciowe oraz zasoby dostępne na serwerach.

9.3.1. Rozbudowa serwerów

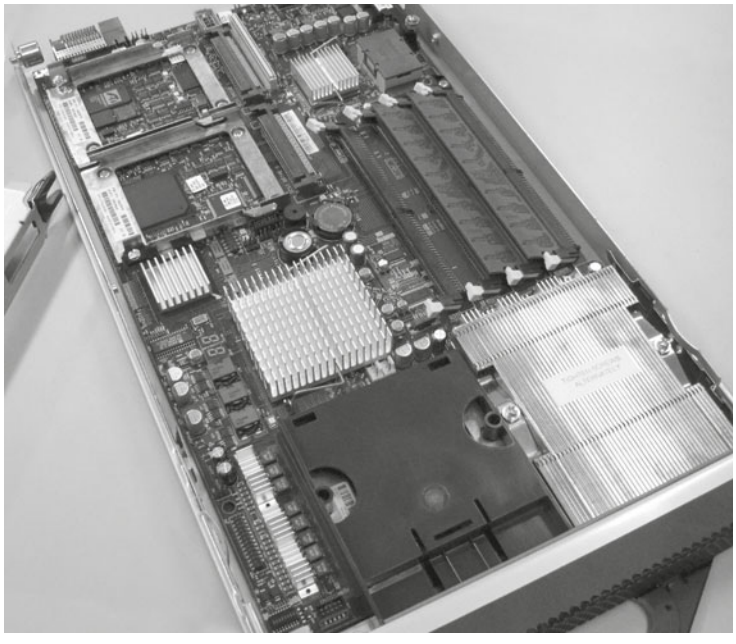
Możliwość rozbudowy serwerów sieciowych najczęściej ogranicza się do zwiększenia pamięci operacyjnej, pojemności dysków czy dołączenia dodatkowej karty sieciowej. Niektóre płyty główne serwerów sieciowych umożliwiają instalację dodatkowych procesorów, co zwiększa możliwości obliczeniowe urządzenia.

Aby zwiększyć dostępną pamięć lub dodać nową kartę sieciową czy procesor do serwera typu rack, należy wysunąć serwer z szafy oraz zdjąć górną obudowę w celu odsłonięcia płyty głównej (rysunek 9.19), a następnie znaleźć odpowiedni port dla elementu wybranego do rozbudowania. Po poprawnym zamocowaniu elementu można ponownie złożyć obudowę.

Instalacja dodatkowego dysku nie wymaga zdejmowania obudowy. Serwery typu rack najczęściej mają z przodu obudowy specjalne wysuwane szuflady, w których montuje się dyski.

UWAGA

Prace związane z rozbudową serwerów powinny być wykonywane przy wyłączonym zasilaniu, chyba że rozbudowa dotyczy elementów typu hot plug, które mogą być instalowane przy włączonym zasilaniu (np. wentylatory, zasilacze zapasowe, dyski).



Rysunek 9.19. Wnętrze serwera typu rack

Rozbudowa o dodatkową pamięć czy procesor nie pociąga za sobą konieczności instalacji dodatkowego oprogramowania w przeciwieństwie do montażu dodatkowej karty sieciowej, w przypadku którego może być niezbędna instalacja sterowników.

Montaż dodatkowych dysków może wymagać działań w systemie operacyjnym pracującym na serwerze, które pozwolą zainicjować dyski i udostępnić je aplikacjom. Poprawne działanie wymienionego dysku pracującego w macierzy RAID może wymagać dodatkowego czasu niezbędnego na odbudowanie danych.

UWAGA

Elementy serwerów do rozbudowy powinny być zgodne z wymaganiami producenta urządzenia. Zainstalowanie urządzeń, które nie mają rekomendacji producenta sprzętu, może spowodować utratę gwarancji.

Używanie w infrastrukturze sieci serwerów wirtualnych pozwala na znaczne zmniejszenie kosztów zarządzania serwerami oraz skrócenie czasu potrzebnego do ich uruchamiania czy przenoszenia. Serwery te są programowo konfigurowalnymi, niezależnymi od siebie instancjami działającymi w obrębie przypisanych przez administratora wspólnych fizycznych zasobów sprzętowych, takich jak dysk, czas procesora czy pamięć operacyjna.

Możliwości serwera wirtualnego może zwiększyć administrator, zmieniając jego konfigurację.

9.3.2. Rozbudowa infrastruktury

Zmiana infrastruktury sieciowej może pociągać za sobą konieczność prowadzenia dodatkowego okablowania. Normy projektowania sieci zakładają uwzględnienie już na etapie tworzenia projektu pewnej nadmiarowości w celu przyszłej rozbudowy. Niestety nie zawsze istnieje możliwość przewidywania przyszłych kierunków rozwoju, co powoduje konieczność zwiększonych nakładów przy późniejszej rozbudowie sieci.

Aby rozbudować obszar roboczy o dodatkowe gniazda abonenckie, trzeba doprowadzić okablowanie z określonego miejsca do punktu dystrybucji obsługującego wybrany obszar. Prace te powinny być wykonane zgodnie z wcześniej przyjętymi założeniami (określonym schematem kabli, określonym rodzajem okablowania) w celu zachowania jednolitej budowy sieci.

Jeżeli dostępne kanały kablowe nie pozwalają na instalację dodatkowego okablowania, należy rozważyć montaż dodatkowych kanałów, które zapewnią miejsce wystarczające dla aktualnych prac oraz przyszłego rozwoju infrastruktury.

W przypadku braku miejsca w panelach krosowych należy w szafach dystrybucyjnych zamontować dodatkowe urządzenia pozwalające na poprawne zaszycie okablowania.

Przy braku wolnych portów w przełącznikach grupy roboczej można rozważyć dołożenie dodatkowego urządzenia w szafie dystrybucyjnej, wymianę urządzenia na większe (zawierające większą liczbę portów) lub jego rozbudowę, o ile jest wykorzystywany przełącznik o budowie modularnej. Jeśli urządzenie jest przystosowane do łączenia w stos, pozwoli to na zwiększenie wydajności transmisji między łączonymi urządzeniami.

9.3.3. Zwiększenie przepustowości

Zwiększenie przepustowości sieci najczęściej jest wymagane w szkielecie sieci (okablowanie kampusowe oraz okablowanie pionowe). W zależności od planowanego zakresu zmian można rozważyć zmianę medium transmisyjnego na światłowód. Taka modyfikacja wymaga dodatkowo dostosowania przełączników łączących poszczególne odcinki. Jeśli urządzenia te nie mają portów światłowodowych, można użyć konwerterów pozwalających na podłączenie mediów światłowodowych do portu RJ-45. W przypadku urządzeń o budowie modularnej można rozbudować urządzenie o właściwy moduł.

Jeśli nie ma możliwości zainstalowania okablowania światłowodowego, można rozważyć zwiększenie przepustowości za pomocą technologii agregacji łącza — pozwala ona na połączenie przełączników z wykorzystaniem maksymalnie 8 połączeń przy odpowiednim zwielokrotnieniu prędkości. Połączenie to z punktu widzenia infrastruktury sieciowej stanowi jeden logiczny kanał transmisji. Fizycznie jest on realizowany na wielu portach.

9.4. Projekt bezpieczeństwa systemów i sieci komputerowych

System komputerowy jest bezpieczny, jeśli działa zgodnie ze specyfikacją (zgodnie z oczekiwaniami użytkownika) oraz zapewnia:

1. Poufność — dostępność danych tylko dla osób uprawnionych.
2. Integralność — pewność, że dane nie zostały naruszone/zmienione przez osoby trzecie.
3. Wiarygodność — pewność, że dane zostały udostępnione przez właściwe osoby i dla właściwych osób.
4. Dostępność — osiągalność danych w określonym czasie.

Aby to zapewnić, należy przewidzieć potencjalne zagrożenia i ograniczyć ich wpływ na system czy sieć komputerową. Koszty bezpieczeństwa systemu komputerowego zależą od wybranych technik i narzędzi — inne będą stosowane do zabezpieczenia danych w banku, inne w małej firmie, a jeszcze inne na prywatnych komputerach.

Aby wybrać właściwe mechanizmy zabezpieczeń, należy określić, co w sieci komputerowej powinno podlegać ochronie:

- stacje robocze oraz komputery przenośne, na których są przetwarzane dane,
- urządzenia sieciowe,
- infrastruktura sieciowa,
- instalowane oprogramowanie,
- nośniki danych,
- kopie zapasowe.

Zagrożenia, przed jakimi należy chronić systemy komputerowe, to między innymi:

- włamania do systemów komputerowych,
- wirusy komputerowe,
- błędy w oprogramowaniu,
- kradzież sprzętu komputerowego — dysków, komputerów stacjonarnych i przenośnych,
- nieuczciwi pracownicy/współpracownicy,
- nieobecność osób zarządzających siecią,
- zdarzenia losowe, np. powódź, pożar.

Wszystkie te aspekty mają istotny wpływ na prawidłowe funkcjonowanie sieci.

Tworząc mechanizmy zabezpieczeń sieci, należy wziąć pod uwagę ochronę stacji roboczych, ochronę sieci oraz ochronę usług sieciowych.

9.4.1. Ochrona stacji roboczych

Stacje robocze to urządzenia, na których są przetwarzane dane. Ich ochrona powinna polegać zarówno na ograniczeniu fizycznej dostępności dla osób trzecich, jak i możliwości pracy na urządzeniach osób do tego nieuprawnionych.

W zależności od założonego poziomu bezpieczeństwa należy rozważyć wprowadzenie następujących zabezpieczeń:

- Dostępu do urządzeń zabezpieczonego hasłem.
- Ograniczenia dotyczącego uruchamianych/instalowanych aplikacji.
- Wymuszenia działania określonych programów chroniących pracę komputera, np. programów antywirusowych, firewalla itp.
- Ograniczenia możliwości usunięcia/wyłączenia określonych aplikacji (np. programów antywirusowych).
- Blokady uruchomienia komputera z nośników wymiennych.
- Ograniczenia wykorzystywania nośników wymiennych (nagrywarek CD/DVD, pamięci flash).
- Ograniczenia wykorzystywania zasobów dyskowych.
- Rejestracji i kontroli prób dostępu do komputera.
- Bezpiecznego kasowania poufnych informacji.
- Zmiany haseł w określonych odstępach czasu.
- Tworzenia haseł spełniających określone wymagania co do złożoności.

Zabezpieczenia te mogą być wdrażane przy użyciu oprogramowania zainstalowanego na komputerach lub w przypadku mniejszych systemów komputerowych w postaci procedur wdrażanych w danej organizacji.

Często istotna może być również kontrola dostępu do pomieszczeń, gdzie są zainstalowane stanowiska pracy — pozwala to na zabezpieczenie się przed kradzieżą sprzętu czy nieuprawnionym dostępem do danych.

Wybór konkretnego instalowanego oprogramowania zabezpieczającego zależy od administratora sieci — trudno jednoznacznie wskazać najlepszy program typu osobisty firewall czy też program antywirusowy. Na rynku istnieje wiele programów tego typu różniących się prędkościami działania, skutecznością wykrywania zagrożeń czy też ceną, niemniej jednak różnice te są na tyle mało znaczące, że trudno wskazać jednoznacznie najlepsze rozwiązanie. Najważniejsze różnice mogą dotyczyć funkcjonalności zarządzania oprogramowaniem przez sieć.

9.4.2. Ochrona sieci i urządzeń sieciowych

Aby właściwie zabezpieczyć zasoby sieciowe, należy zapewnić zarówno bezpieczeństwo fizyczne urządzeń sieciowych, jak również rozważyć zabezpieczenia logiczne danych — filtrowanie ruchu, kopie bezpieczeństwa danych, oprogramowanie antywirusowe na serwerach, szyfrowanie danych na dyskach czy kontrolę dostępu do danych.

Przy tworzeniu zabezpieczeń sieci należy wziąć pod uwagę:

- Fizyczny dostęp do punktów dystrybucji, w których pracują serwery oraz zasoby dyskowe.
- Zdefiniowanie listy stanowisk lub wydzielenie specjalnej sieci, z której istnieje możliwość zarządzania urządzeniami sieciowymi.
- Zdefiniowanie ruchu sieciowego i ograniczanie zbędnych protokołów sieciowych.
- Usunięcie lub wyłączenie zbędnych usług sieciowych.
- Wykorzystywanie w miarę możliwości szyfrowanych protokołów danych (np. https, sftp, ssh).
- Stosowanie szyfrowanych zapisów na dyskach.
- Uruchomienie mechanizmów tworzenia kopii bezpieczeństwa danych, aplikacji i ustawień programów, serwerów i urządzeń sieciowych.
- Wybór odpowiednich zasobów dyskowych zapewniający wymagany poziom niezawodności (technologia RAID, macierze dyskowe).
- Wykorzystanie technologii wirtualizacji serwerów, która pozwala na przenoszenie kopii całych serwerów wirtualnych pomiędzy fizycznymi serwerami.
- Wybór odpowiedniego sprzętu zapewniającego możliwość wymiany/instalacji elementów bez konieczności wyłączania urządzenia (tzw. *hot plug*).
- Wybór urządzeń zapewniających zwielokrotnione (redundantne) elementy, takie jak zasilacz, wentylator itp.
- Zapewnienie odpowiednich zabezpieczeń przeciwpożarowych.
- Zapewnienie odpowiedniej temperatury pracy urządzeń.

Podana powyżej przykładowa lista zabezpieczeń sieci nie jest listą kompletną — istnieje szereg innych technik pozwalających na zminimalizowanie ryzyka wystąpienia awarii systemów komputerowych, niemniej jednak wskazany zbiór definiuje szeroki zakres najbardziej popularnych rodzajów zabezpieczeń. Projektując bezpieczną sieć komputerową, należy rozważyć sens stosowania poszczególnych typów zabezpieczeń, możliwości ich wprowadzenia oraz niezbędne do poniesienia koszty. Im wyższy poziom zabezpieczeń, tym wyższe stają się koszty ich wdrożenia. Często osiągnięcie wymaganego poziomu bezpieczeństwa stanowi kompromis pomiędzy dostępnymi technologiami a budżetem przeznaczonym na ten cel.

WSKAZÓWKA

Aby zapewnienić maksymalne bezpieczeństwo użytkownikom należy udzielać tylko i wyłącznie takich uprawnień, które są im niezbędne do pracy. Zmiana zakresu obowiązków użytkownika powinna pociągać za sobą modyfikację zakresu uprawnień.

Należy stosować regułę domyślnej odmowy dostępu — jeśli coś nie jest jawnie dozwolone, to znaczy, że jest zabronione.

9.4.3. Ochrona danych osobowych

Budując bezpieczną sieć komputerową przetwarzającą dane osobowe, należy zwrócić uwagę na wymagania stawiane tego typu rozwiązaniom przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Zgodnie z polskim prawem za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby, a więc imię, nazwisko, numer pesel, zdjęcie, ale również adres e-mail zawierający imię i nazwisko.

Gdy przetwarza się dane osobowe, należy zgłosić ten fakt do Generalnego Inspektora Ochrony Danych Osobowych. Rejestracji nie podlegają dane przetwarzane przez osoby prywatne oraz dane zbierane w celach księgowych (wystawianie faktur), kadrowych (dane pracowników), dane uczniów i studentów, kartoteki lekarskie, akta klientów kancelarii prawnych, doradców podatkowych oraz dane powszechnie dostępne, np. dane firm.

UWAGA

Zgodnie z ustawą przetwarzanie danych niezbędnych do wystawiania faktur jest zwolnione z rejestracji, lecz użycie tych samych danych do realizacji zamówienia (np. wysyłki) takiej rejestracji wymaga.

Wyłączenie zbioru z konieczności rejestracji nie oznacza, że zbiór może nie być zabezpieczony — powinien on spełniać określone wymagania, ale nie musi być zgłaszany do biura GIODO.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w zakresie ochrony danych osobowych definiuje trzy poziomy bezpieczeństwa przetwarzania danych osobowych: podstawowy, podwyższony oraz wysoki. Za bezpieczeństwo danych odpowiada powołany w tym celu Administrator Bezpieczeństwa Informacji, który powinien czuwać nad zakresem dostępu do danych dla poszczególnych pracowników, nadzorować sposób przetwarzania danych osobowych w systemach informatycznych, kontrolować zgodność systemu informatycznego z wymaganiami określonymi w przepisach oraz reagować na incydenty naruszenia bezpieczeństwa danych osobowych.

Poziom podstawowy dotyczy sytuacji, gdy system nie przetwarza danych wrażliwych (np. pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych, danych o stanie zdrowia itp.) i kiedy system komputerowy nie jest podłączony do sieci publicznej.

Na poziomie podstawowym wymagane są następujące środki ochrony:

1. Fizyczna kontrola dostępu do obszaru przetwarzania danych osobowych — ograniczenie dostępu do pomieszczeń, komputerów, serwerów.
2. Logiczna kontrola dostępu do danych — stosowanie mechanizmu autoryzacji użytkowników.
3. Złożoność haseł użytkowników: co najmniej 6 znaków zmieniane nie rzadziej niż co 30 dni.

4. Zabezpieczenia systemów komputerowych przed działaniem szkodliwego oprogramowania — stosowanie oprogramowania typu firewall, antywirus itp.
5. Zabezpieczenia systemów komputerowych spowodowane awarią zasilania lub zakłóceniami w sieci zasilającej — poprzez stosowanie zasilaczy awaryjnych.
6. Cykliczne tworzenie kopii zapasowych zarówno danych, jak i przetwarzających je programów. Kopie powinny być przechowywane w miejscach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem, z dala od miejsca ich przetwarzania.
7. Nośniki danych przeznaczone do likwidacji lub przekazania osobom nieuprawnionym powinny zostać wyczyszczone z zapisanych danych osobowych.
8. Kryptograficzna ochrona danych (zapis szyfrowany) dla danych na urządzeniach mobilnych i dostępnych poza obszarem przetwarzania.

Poziom podwyższony jest stosowany, gdy w systemie informatycznym są przetwarzane dane wrażliwe oraz żadne z urządzeń nie jest połączone z siecią publiczną. Wymagane są środki ochrony z poziomu podstawowego przy zwiększonej złożoności haseł uwierzytelniających (co najmniej 8 znaków, składające się z małych i dużych liter, cyfr oraz znaków specjalnych), a także zabezpieczenie kryptograficzne dla nośników danych przekazywanych poza obszar przetwarzania danych. Dodatkowo jest wymagane utworzenie dokumentów: polityki bezpieczeństwa danych osobowych oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego jest połączone z siecią publiczną. Na wysoki poziom zabezpieczeń składają się takie środki ochrony, jak dla poziomu podwyższonego, a dodatkowo należy chronić system informatyczny przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń przed nieuprawnionym dostępem.

Zabezpieczenia logiczne powinny zapewnić kontrolę przepływu informacji pomiędzy systemem informatycznym przetwarzającym dane a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego (np. poprzez zastosowanie zapory ogniowej). W przypadku gdy dane do uwierzytelniania użytkowników systemu są przesyłane w sieci publicznej, należy zastosować środki ochrony kryptograficznej.

Polityka bezpieczeństwa danych osobowych powinna zawierać:

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, gdzie są przetwarzane dane osobowe.
2. Wykaz zbiorów danych (baz danych) osobowych wraz ze wskazaniem programów do ich przetwarzania.
3. Opis struktury zbiorów danych wraz z powiązaniami między nimi.
4. Sposób przepływu danych pomiędzy poszczególnymi systemami przetwarzającymi dane osobowe.
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych powinna opisywać:

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.
2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z zarządzaniem nimi i ich użytkowaniem.
3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.
4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.
5. Sposób, miejsce i okres przechowywania nośników zawierających dane osobowe oraz kopie zapasowych zbiorów danych.
6. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.
7. Sposób odnotowywania informacji o odbiorcach, którym zostały udostępnione dane osobowe, dacie i zakresie udostępnienia, chyba że system informatyczny jest używany do przetwarzania danych w zbiorach jawnych.

ĆWICZENIA

Założenia projektu sieci komputerowej

Przygotuj projekt sieci komputerowej dla swojej szkoły. W ramach sieci powinny działać:

1. Sieć szkolna z dostępem do wspólnej przestrzeni dyskowej.
2. Sieć nauczycielska z dostępem do wewnętrznego serwera nauczycielskiego oraz serwera z sieci szkolnej.
3. Sieć biblioteczna z dostępem do serwera, na którym działa oprogramowanie do zarządzania biblioteką.
4. Sieć zarządzania szkołą z dostępem do serwera z oprogramowaniem do zarządzania szkołą.
5. Ogólnodostępna sieć bezprzewodowa pozwalająca na przeglądanie stron WWW.

Założenia, które powinna spełniać sieć:

- W każdej sali, gdzie odbywają się zajęcia, powinno zostać zamontowanych 8 gniazd sieciowych z dostępem do sieci szkolnej oraz 2 gniazda z dostępem do sieci nauczycielskiej.

ĆWICZENIA cd.

- W bibliotece powinno znaleźć się 20 gniazd z dostępem do sieci bibliotecznej.
- W pokoju nauczycielskim powinno znaleźć się 20 gniazd z dostępem do sieci nauczycielskiej.
- Sieć bezprzewodowa powinna być dostępna na korytarzach oraz na sali gimnastycznej.
- Dostęp do części usług (strony WWW) na serwerze nauczycielskim powinien być możliwy z internetu.

Jeśli nie ma dokładnych planów budynku, powinien je stworzyć autor projektu.

Założenia i ograniczenia związane z tworzeniem sieci należy uwzględnić w projekcie.

Podczas tworzenia projektu trzeba rozważyć potencjalne lokalizacje punktów dystrybucji, uzasadnić wybór konkretnych miejsc.

W projekcie należy wybrać sposób prowadzenia okablowania zarówno na kolejnych kondygnacjach, jak i pomiędzy nimi. Należy zastanowić się nad sposobem i miejscem prowadzenia okablowania między piętrami.

Dobór kanałów kablowych powinien uwzględniać liczbę prowadzonych w nich kabli.

Sprzęt sieciowy w projektowanej sieci powinien zapewniać odpowiednią dostępność usług. Należy uwzględnić możliwości przyszłego rozwoju.

Kosztorys sieci powinien obejmować zarówno ceny użytego sprzętu, jak i koszty niezbędnych prac. W celu uproszczenia kosztorysu należy przyjąć stawki za większy obszar prac.

PYTANIA

1. Jakie klasy miedzianego okablowania są stosowane przy budowie sieci strukturalnych?
2. Wymień znane Ci elementy okablowania strukturalnego.
3. Czym różni się budynkowy punkt dystrybucji od piętrowego punktu dystrybucji?
4. Jaka jest różnica pomiędzy okablowaniem pionowym a okablowaniem poziomym?
5. Jaki rodzaj okablowania jest zalecany do okablowania poziomego, pionowego oraz kampusowego?

PYTANIA cd.

6. Jakie maksymalne długości kabli światłowodowych jedno- i wielomodowych dopuszczają normy?
7. Wymień kolejne etapy tworzenia projektu sieci.
8. Jakie informacje powinny być zebrane na etapie analizy potrzeb zamawiającego podczas tworzenia projektu sieci? Dlaczego ten etap jest kluczowy przy budowaniu dobrego projektu?
9. W jakim celu tworzy się logiczny projekt sieci? Czym różni się on od projektu fizycznego?
10. Jakie warunki należy wziąć pod uwagę przy projektowaniu adresacji IP dla sieci?
11. Wymień, jakie urządzenia powinny być uwzględnione przy planowaniu adresacji IP dla sieci.
12. W jakim celu dzieli się sieci na podsieci?
13. Do czego służy wydzielona sieć administracyjna? Dlaczego warto zaprojektować taką sieć?
14. Jakie ograniczenia są uwzględniane przy wyborze lokalizacji punktów dystrybucji?
15. Jakie parametry mechaniczne dotyczące okablowania powinny być brane pod uwagę podczas wyboru konkretnego produktu?
16. W jakich jednostkach są podawane wysokości szaf dystrybucyjnych?
17. Do czego służy panel krosowy?
18. Dlaczego warto stosować organizery kabli?
19. Czym różni się przełącznik szkieletowy od przełącznika grupy roboczej?
20. W jaki sposób można połączyć przełączniki między sobą w celu zwiększenia liczby dostępnych portów w określonej lokalizacji?
21. Czym różni się router sprzętowy od routera programowego?
22. Jakie czynniki należy uwzględnić przy wyborze routera?
23. Jakie parametry mają wpływ na wybór serwera do projektowanej sieci?
24. Czym różni się obudowa serwerowa typu rack od obudowy blade?
25. Czym jest serwer wirtualny?
26. Wymień zalety stosowania serwerów wirtualnych.
27. Wymień oprogramowanie stosowane do wirtualizacji zasobów serwerowych.
28. Do czego służy przełącznik KVM?
29. Z czego jest zbudowana konsola KVM?
30. Do czego służą urządzenia UPS?

PYTANIA cd.

31. W jakich jednostkach jest podawana moc zasilaczy awaryjnych?

32. Jakie parametry decydują o doborze zasilacza awaryjnego?

33. Podaj optymalny sposób ułożenia elementów w szafie dystrybucyjnej. Z czego on wynika?

34. W jaki sposób wycenia się w kosztorysie sieci komputerowych prace związane z budową sieci?

35. Jakie elementy powinna zawierać dokumentacja sieci komputerowej?

36. Do czego służy nóż krosowniczy (ang. *punch down tool*)?

37. W jakich elementach stosowane są złącza typu 110?

38. Czym różni się kabel prosty od kabla skrosowanego?

39. Wymień kolejność kolorów w dwóch standardach układania przewodów we wtyczkach RJ-45.

40. W jaki sposób są łączone światłowody?

41. Jakie parametry mechaniczne i dynamiczne mogą być testowane przy użyciu certyfikowanych testerów okablowania?

42. Na czym polega zjawisko przesłuchu występujące w sieciach komputerowych?

43. Jakie cechy ma bezpieczny system komputerowy?

44. Kiedy stosuje się podstawowy poziom zabezpieczeń, kiedy poziom podwyższony, a kiedy poziom wysoki w systemach przetwarzających dane osobowe?

45. Czym różnią się poziomy podstawowy, podwyższony i wysoki stosowane przy ochronie zbiorów danych osobowych?

46. Jakie elementy powinna zawierać polityka bezpieczeństwa?

47. Co powinna opisywać instrukcja zarządzania systemem informatycznym?

Wykaz skrótów

AAL (ang. *ATM Adaptation Layer*)
ACL (ang. *Access Control List*)
APIPA (ang. *Automatic Private IP Addressing*)
ARP (ang. *Address Resolution Protocol*)
ASIC (ang. *Application Specific Integrated Circuits*)
ATM (ang. *Asynchronous Transfer Mode*)
AWG (ang. *American Wire Gauge*)
BGP (ang. *Border Gateway Protocol*)
BIND (ang. *Berkeley Internet Name Domain*)
BOOTP (ang. *BOOTstrap Protocol*)
BPDU (ang. *Bridge Protocol Data Unit*)
BSS (ang. *Basic Service Set*)
CA (ang. *certification authority*)
CIR (ang. *Committed Information Rate*)
CSMA/CD (ang. *Carrier Sense Multiple Access/Collision Detection*)
CUPS (ang. *Common UNIX Printing System*)
DFS (ang. *Distributed File System*)
DHCP (ang. *Dynamic Host Configuration Protocol*)
DN (ang. *Distinguished Name*)
DNS (ang. *Domain Name System*)
EFS (ang. *Encrypting File System*)
EIA (ang. *Electronic Industries Association*)
EIGRP (ang. *Enhanced Interior Gateway Routing Protocol*)
ELFEXT (ang. *Equal Level FarEnd Crosstalk*)
ESS (ang. *Extended Service Set*)
F/UTP (ang. *Foiled/Unshielded Twisted Pair*)
FDDI (ang. *Fiber Distributed Data Interface*)
FIFO (ang. *first in first out*)
FQDN (ang. *Fully Qualified Domain Name*)
FSMO (ang. *Flexible Single Operations Masters*)
FSRM (ang. *File Server Resource Manager*)
FTP (ang. *File Transfer Protocol*)
GID (ang. *Group Id*)
GPO (ang. *Group Policy Objects*)
HTTP (ang. *Hypertext Transfer Protocol*)
HTTPS (ang. *Hypertext Transfer Protocol Secure*)
IAPP (ang. *Inter-Access Point Protocol*)
ICMP (ang. *Internet Control Message Protocol*)
IDF (ang. *Intermediate Distribution Facility*)
IGRP (ang. *Interior Gateway Routing Protocol*)
IIS (ang. *Internet Information Services*)
IOS (ang. *Internetwork Operating System*)
IP (ang. *Internet Protocol*)
IPNG (ang. *Internet Protocol Next Generation*)
IPv4 (ang. *Internet Protocol version 4*)
IPv6 (ang. *Internet Protocol version 6*)
IPX (ang. *Internet Packet Exchange*)
KVM (ang. *Keyboard*, *Video*, *Mouse*)
L2TP (ang. *Layer Two Tunneling Protocol*)
LAN (ang. *Local Area Network*)
LD (ang. *laser diode*)
LDAP (ang. *Lightweight Directory Access Protocol*)
LED (ang. *light-emitting diode*)
LSZH (ang. *Low Smoke Zero Halogen*)
MAC (ang. *Media Access Control*)
MAN (ang. *Metropolitan Area Network*)
MDA (ang. *Mail Delivery Agent*)
MDF (ang. *Main Distribution Facility*)
MIB (ang. *Management Information Base*)
MSTP (ang. *Multiple Spanning Tree Protocol*)
MTA (ang. *Mail Transfer Agent*)

MUA (ang. *Mail User Agent*)
NAT (ang. *Network Address Translation*)
NEXT (ang. *Near End Crosstalk*)
NFS (ang. *Network File System*)
NIC (ang. *Network Interface Card*)
NIS (ang. *Network Information Service*)
NNI (ang. *Network-to-Network Interface*)
NTP (ang. *Network Time Protocol*)
OSPF (ang. *Open Shortest Path First*)
PDC (ang. *Primary domain controller*)
PID (ang. *Process IDentifier*)
POP3 (ang. *Post Office Protocol*)
PPTP (ang. *Point to Point Tunneling Protocol*)
PSELFEXT (ang. *Power Sum Equal Level FarEnd Crosstalk*)
PSK (ang. *Pre-Shared Key*)
PSNEXT (ang. *Power Sum NEXT*)
PSTN (ang. *Public Switched Telephone Network*)
PVC (ang. *Permanent Virtual Circuits*)
QM (ang. *Queue Manager*)
QoS (ang. *Quality of Service*)
RADIUS (ang. *Remote Authentication Dial-In User Service*)
RAID (ang. *Redundant Array of Independent Disks*)
RAP (ang. *Roving Analysis Port*)
RARP (ang. *Reverse Address Resolution Protocol*)
RIP (ang. *Routing Information Protocol*)
RO (ang. *read only*)
RRAS (ang. *Routing and Remote Access*)
RSTP (ang. *Rapid Spanning Tree Protocol*)
RTP (ang. *Real-time Transport Protocol*)
RW (ang. *read write*)
S/FTP (ang. *Shielded/Foiled Twisted Pair*)
SF/UTP (ang. *Shielded Foil/Unshielded Twisted Pair*)
SFD (ang. *Start Frame Delimiter*)
SID (ang. *Security ID*)
SIP (ang. *Session Initiation Protocol*)
SLP (ang. *Service Locator Protocol*)
SMB (ang. *Server Message Block*)
SMTP (ang. *Simple Mail Transfer Protocol*)
SNMP (ang. *Simple Network Management Protocol*)
SOHO (ang. *Small Office Home Office*)
SPAN (ang. *Switched Port Analyzer*)
SPX (ang. *Sequenced Packet Exchange*)
SSH (ang. *Secure Shell*)
SSID (ang. *Service Set IDentifier*)
SSO (ang. *Single Sign On*)
STP (ang. *Spanning Tree Protocol*)
SVC (ang. *Switched Virtual Circuits*)
TCP/IP (ang. *Transmission Control Protocol/Internet Protocol*)
ToS (ang. *Type of Service*)
TTL (ang. *Time To Live*)
U/UTP (ang. *Unshielded/Unshielded Twisted Pair*)
UCE (ang. *Unsolicited Commercial Email*)
UDP (ang. *User Datagram Protocol*)
UID (ang. *User Id*)
UNC (ang. *Universal Naming Convention*)
UNI (ang. *User Network Interface*)
UPS (ang. *Uninterruptible Power Supply*)
VLAN (ang. *Virtual Local Area Network*)
VNC (ang. *Virtual Network Computing*)
VoIP (ang. *Voice over Internet Protocol*)
VPN (ang. *Virtual Private Network*)
WAN (ang. *Wide Area Network*)
WDS (ang. *Windows Deployment Services*)
WEP (ang. *Wired Equivalent Privacy*)
WLAN (ang. *Wireless Local Area Network*)
WMI (ang. *Windows Management Instrumentation*)
WPA (ang. *WiFi Protected Access*)

Słowniczek

Ang.	Pol.
access point	punkt dostępowy
access point controllers	kontrolery punktów dostępu
active directory	usługa katalogowa
application layer	warstwa aplikacji
asynchronous transfer mode	asynchroniczny tryb przesyłania
availability	dostępność sieci
background	tło
backslash	ukośnik wsteczny
bandwith control	zarządzanie pasmem
basic service set	podstawowy zestaw usługowy
batch files	pliki wsadowe
broadcast	adres rozgłoszeniowy
building backbone cable	budynkowy kabel szkieletowy
building distributor	budynkowy punkt dystrybucyjny
bus	szyna danych (topologia magistrali)
campus	kampus
campus backbone cable	kampusowy kabel szkieletowy
campus distributor	kampusowy punkt dystrybucyjny
channel	kanał (np. działania sieci)
child process	proces potomny
codec	kodek
consolidation point	punkt pośredni
consolidation point cable	kabel punktu pośredniego
crossover cable	kabel skrosowany
daemon	demon
data link layer	warstwa łącza danych
debug logging	rejestracja uruchomieniowa
default gateway	brama domyślna
delay	opóźnienie
delay skew	różnica opóźnień
demilitarized zone	strefa zdemilitaryzowana

Ang.	Pol.
destination IP Address	docelowy adres IP
destination port	port docelowy
destination subnet mask	docelowa maska podsieci
dialer interface	interfejs logiczny
dialer pool	pula interfejsów wdzwanianych
distance vector protocols	protokoły wektora odległości
distribution	dystrybucja
domain local	lokalne domenowe
domain naming master	wzorzec nazw domen
done	zakończony
event log	dziennik zdarzeń
exclusions	wykluczenia
extended file system	rozszerzony system plików
extended list	lista rozszerzona
extended service set	rozszerzony zestaw usług
extended star topology	topologia gwiazdy rozszerzonej
false	fałsz
file server	serwer plików
file services	usługi serwera plików
firewall	zapora ogniowa
floor distributor	piętrowy punkt dystrybucyjny
foreground	pierwszy plan
forwarders	serwery przekazujące
forward lookup zone	strefa wyszukiwania do przodu
global	globalne
global catalog	wykaz globalny
help desk	zespół pomocy technicznej
hub	koncentrator
inbound filter	filtr ruchu przychodzącego
infrastructure master	wzorzec infrastruktury
intermediate distribution facility	pośredni punkt dystrybucyjny
internet service provider	dostawca usług internetowych
kernel	jądro systemu operacyjnego
laser diode	dioda laserowa

Ang.	Pol.
layer	warstwa
light-emitting diode	dioda elektroluminescencyjna
link agregation	agregacja łączy
link state protocols	protokoły stanu łącza
loopback	pętla zwrotna
manual	podręcznik systemowy
mesh topology	topologia siatki
mixed mesh topology	topologia siatki mieszanej
modulator-demodulator	modem
monitoring	monitorowanie
mount	montowanie
named list	lista nazywana
named pipe	nazwany potok
namespace	obszar nazw
network address	adres sieci
network layer	warstwa sieciowa
optical receiver	odbiornik optyczny
optical transmitter	nadajnik optyczny
outbound filter	filtr ruchu wychodzącego
parent process	proces rodzicielski
patch cord	kabel krosowy
patch panel	panel krosowy
performance monitor	monitor wydajności
physical interface	interfejs fizyczny
physical LAN port	fizyczny port urządzenia
physical layer	warstwa fizyczna
port forwarding	przekierowanie portów
presentation layer	warstwa prezentacji
print server	serwer wydruku
privileged exec mode	tryb uprzywilejowany
protocol	protokół
records	rekordy
redirect server	serwer przekierowań
reduced down time	zredukowany czas przestoju

Ang.	Pol.
return loss	straty odbiciowe
ring topology	topologia pierścienia
routed protocol	protokół rutowalny
routing table	tablica routingu
running	działający
scalability	skalowalność
schema master	wzorzec schematu
security	zabezpieczenia
session layer	warstwa sesji
shell	powłoka systemu operacyjnego
shielded	ekranowany
snapshot	migawka
sniffer	sniffer („program węszący”)
socket	gniazdo
softphone	program służący do wykonywania połączeń telefonicznych przez internet (np. Skype)
Source IP Address	źródłowy adres IP
source port	port źródłowy
source subnet mask	źródłowa maska podsieci
SSID broadcast	rozgłaszanie identyfikatora sieci
stacking	połączenie w stos
standard list	lista standardowa
star topology	topologia gwiazdy
stopped	zatrzymany
straightthrough cable	kabel prosty
subnet mask	maska podsieci
suspend	zamrozić
switch	przełącznik
task manager	menedżer zadań
telecommunications outlet	gniazdo telekomunikacyjne
terminal services	usługi terminalowe
time to live	czas życia
token	żeton

Ang.	Pol.
topdown	rozumowanie dedukcyjne (dosł. „od ogółu do szczegółu”)
touchpad	panel dotykowy
tower	wieża (typ obudowy)
transceiver	urządzenie nadawczo-odbiorcze
transport layer	warstwa transportowa
true	prawda
type of service	typ usługi
universal	uniwersalne
unshielded	nieekranowany
user exec mode	tryb użytkownika
validate	weryfikacja
VoIP gateway	bramka VoIP
work area	obszar roboczy
work area cord	kabel połączeniowy
workgroup	grupa robocza
zone	strefa

Bibliografia

[1] Ball Bill, *Poznaj Linux*, Mikom, Warszawa 1999

[2] Bensel Paweł, *Systemy i sieci komputerowe. Podręcznik do nauki zawodu technik informatyk*, Helion, Gliwice 2010

[3] Derfler Frank, Freed Les, *Okablowanie sieciowe w praktyce. Księga eksperta*, Helion, Gliwice 2000

[4] Empson Scott, *Akademia sieci Cisco. CCNA. Pełny przegląd poleceń*, Wydawnictwo Naukowe PWN, Warszawa 2008.

[5] Foster-Johnson Eric, Welch John C., Anderson Micah, *Skrypty powłoki. Od podstaw*, Helion, Gliwice 2006

[6] Józefiok Adam, *Budowa sieci komputerowych na przełącznikach i routerach Cisco*, Helion, Gliwice 2009.

[7] Komar Brian, *Administracja sieci TCP/IP dla każdego*, Helion, Gliwice 2000

[8] Krysiak Karol, *Sieci komputerowe. Kompendium*, wydanie II, Helion, Gliwice 2005.

[6] Morimoto Rand, Noel Michael, Droubi Omar, Mistry Ross, Amaris Chris, *Windows Server 2008 PL. Księga eksperta*, Helion, Gliwice 2009.

[9] Oppenheimer Priscilla, *Cisco. Projektowanie sieci metodą Top-Down*, Wydawnictwo Naukowe PWN, Warszawa 2007.

[10] Parker Tim, *Linux. Księga eksperta*, Helion, Gliwice 1999.

[11] Pawlak Rafał, *Okablowanie strukturalne sieci. Teoria i praktyka. Wydanie III*, Helion, Gliwice 2011

[12] Serafin Marek, *Sieci VPN. Zdalna praca i bezpieczeństwo danych. Wydanie II rozszerzone*, Helion, Gliwice 2009

[13] Sosinsky Barrie, *Sieci komputerowe. Biblia*, Helion, Gliwice 2011.

Źródła internetowe

[1] *http://www.microsoftvirtualacademy.com*

[2] *http://www.slow7.pl/*

[3] *https://www.suse.com/pl-pl/documentation/sles11/*

[4] *http://technet.microsoft.com*

[5] *http://www.wikipedia.org*

[6] *http://www.wss.pl*

W podręczniku wykorzystano fotografie pochodzące z następujących stron internetowych:

http://commons.wikimedia.org — rysunki 2.2, 3.7, 5.9, 5.10, 9.12, 9.17

http://www. shutterstock.com — rysunki 3.2, 3.5, 5.1, 5.2, 5.3, 5.4, 5.6, 5.8, 5.11, 9.7, 9.8, 9.9, 9.10, 9.13, 9.16

Skorowidz

E

F

G

H

I

J

K

O

P

Q

R

S

Ś

T

U

V

W

X

Y

Z

Ż