Część IV
Praca w sieci lokalnej i Internecie

Linux jest podstawą w świecie serwerów sieciowych. System Red Hat Linux 6 umożliwia obsługę wielu mechanizmów, za które w systemach komercyjnych trzeba było by zapłacić tysiące dolarów.

W tej części pokażemy, w jaki sposób obsługuje się niektóre z ważniejszych elementów serwera opartego na systemie Red Hat Linux 6. Większość z tych mechanizmów można skonfigurować w środowisku graficznym, unikając bezpośredniej edycji plików konfiguracyjnych. Jeśli dostępny jest graficzny sposób konfiguracji danego elementu – skoncentruję się właśnie na nim, a nie na konfiguracji za pomocą wiersza poleceń.

Jeśli chcesz uruchomić sieć lokalną lub serwer internetowy, trudno o system lepiej nadający się do tego celu niż Red Hat Linux 6.

Rozdział trzynasty: Serwer linuxowy wyjaśnia, w jaki sposób skonfigurować różne funkcje serwera, takie jak FTP, NFS, DHCP czy SAMBA.

Rozdział czternasty: Serwer Apache zawiera informacje dotyczące serwera Apache – najpopularniejszego na świecie serwera stron WWW, rozprowadzanego wraz z systemem Red Hat Linux 6.

13 Serwer linuxowy

Dla wielu użytkowników system Red Hat Linux 6 jest przede wszystkim *serwerem*. Istnieje wiele różnych typów serwerów, ale praktyczna definicja mogłaby brzmieć: serwer pozwala wielu użytkownikom zdalnym na współdzielenie lub korzystanie z tych samych zasobów. Zgodnie z tą definicją serwer może pozwalać użytkownikom na korzystanie z plików i systemów plików. Idąc nieco dalej, serwer może również udostępniać mechanizmy obsługi baz danych i „serwować" strony WWW.

Linux jest doskonałą platformą dla serwera w wielu sytuacjach wymagających wysokiej niezawodności. Jak zapewne wiesz, jest to system wykorzystywany przez wielu dostawców Internetu (Internet Service Providers, czyli ISP) – firm, które oferują usługi, takie jak udostępnianie zasobów internetowych czy prowadzenie stron WWW. W mniejszych systemach Linux doskonale sprawdza się jako serwer drukarek i plików w sieciach biurowych lub domowych.

W tym rozdziale przedstawimy różne zagadnienia związane z wykorzystaniem systemu linuxowego jako serwera:

- Telnetowanie do serwera.
- Konfiguracja Linuxa jako serwera FTP.
- Serwer sieciowych systemów plików NFS.
- Dynamiczna konfiguracja komputerów za pomocą DHCP.
- Łączenie się klientów Windows z serwerem za pomocą programu SAMBA.
- Łączenie się z systemami Microsoft Windows za pomocą programu smbclient.
- Wykorzystanie Linuxa jako serwera poczty.
- Zagadnienia związane z bezpieczeństwem.

Należy zdawać sobie sprawę, że konfiguracja sieci jest czymś na pograniczu czarnej magii i nauki. Co więcej, każda konfiguracja sieci jest inna. Przedstawione tu informacje powinny wystarczyć do rozpoczęcia pracy, ale to wszystko.

Zasady działania TCP/IP

TCP/IP jest standardowym protokołem używanym do obsługi sieci w świecie linuxowym oraz w większości sieci UNIX-owych; na tym protokole oparta jest również sieć Internet.

Protokół to język używany przez komputery do komunikowania się. Nie ma on nic wspólnego z fizycznym połączeniem komputerów realizowanym zwykle w oparciu o jedną z technologii Ethernet. Innymi słowy, okablowanie łączące komputery może być na przykład typu 10-Base-T z wtyczkami RJ-45 podłączonymi do kart sieciowych. Połączenie może też być realizowane za pomocą szybkich łączy optycznych. Z punktu widzenia protokołu rodzaj połączenia nie odgrywa żadnej roli. Abstrakcyjna warstwa oprogramowania – czyli protokół TCP/IP – umożliwia rozważanie problemów związanych z siecią bez konieczności skupiania się na sprzęcie, podobnie jak można programować w języku Java, nie zawracając sobie głowy sprzętem, na jakim program będzie wykonywany.

Protokół TCP/IP

TCP to skrót od słów *Transmission Control Protocol*, czyli protokół kontroli transmisji, natomiast IP oznacza *Internet Protocol* – protokół internetowy.

Funkcją TCP w tym dwuelementowym protokole jest dzielenie danych na fragmenty nazywane *pakietami*. IP obsługuje mechanizmy transmisji takich pakietów i kierowania ich do adresata. IP zarządza również pakietami UDP – czyli User Datagram Protocol, protokołu zbliżonego do TCP.

IP nie ma żadnych informacji o danych, które są przesyłane w pakietach. Dla kontrastu, pakiety TCP nie „wiedzą" dokąd są przesyłane i w jaki sposób mają tam trafić. Takie rozwiązania przypomina prowadzenie niewidomego do celu – przewodnik jest niezbędny do pomyślnego zakończenia całej operacji.

Konfiguracja TCP/IP

Jeśli musisz skonfigurować sieć TCP/IP lub komputer podłączony do takiej sieci – nazywany *węzłem* – będziesz musiał zrozumieć kilka ważnych zagadnień związanych z tym protokołem. Dokładne zrozumienie sensu terminów używanych przy ich opisie na pewno ułatwi Ci zadanie. Najważniejsze terminy to:

- adres IP,
- podsieć i maska sieci,
- adres rozgłoszenia,
- adres bramki,
- serwer nazw.

Adresy IP i maski sieci

Adres IP (lub krócej IP) to czteroczęściowa liczba identyfikująca jednoznacznie komputer nazywany *hostem*. Każda z czterech części liczby oddzielona jest od pozostałych kropką. Poszczególny host posiadający bezpośrednie połączenie z siecią musi mieć własny, niepowtarzalny adres IP.

Każda z czterech części adresu IP może być liczbą z przedziału od 1 do 255, co daje około 4,2 miliarda adresów. Adresy te podzielone są w grupy, nazywane *sieciami*, i przyznawane organizacjom potrzebującym takich adresów. Istnieją trzy rodzaje sieci:

- Sieci klasy A, identyfikowane przez pierwszą część adresu; dostępnych jest do 16.777.216 adresów IP.
- Sieci klasy B, identyfikowane przez pierwsze dwie części adresu; dostępnych jest do 65536 adresów IP.
- Sieci klasy C, identyfikowane przez pierwsze trzy części adresu; dostępnych jest do 256 adresów IP.

Dla przykładu, adres IP 24.16.108.142 może być adresem komputera o numerze 142 w sieci klasy C, komputera o numerze 108.142 w sieci klasy B lub komputera o numerze 16.108.142 w sieci klasy A. Skąd taka biedna maszyna ma wiedzieć, w jakiej sieci się znajduje?

Z pomocą przychodzi *maska podsieci*, zwana również *maską sieci*. Po zastosowaniu iloczynu bitowego adresu maski i adresu IP otrzymujemy numer sieci. **Tabela 13.1** przedstawia znaczenie poszczególnych masek podsieci.

Tabela 13.1. *Maski podsieci i ich znaczenie.*

Maska	Znaczenie
255.0.0.0	Sieć klasy A
255.255.0.0	Sieć klasy B
255.255.255.0	Sieć klasy C

Zauważ, że jeśli wykonamy operację AND na bitach adresu IP, na przykład 24.16.108.142 oraz na masce podsieci klasy C, czyli 255.255.255.0, ostatnia część adresu zostanie wyzerowana – otrzymamy 24.16.108.0. Taki adres nazywa się adresem sieci i nie może być przypisany żadnemu komputerowi.

Adres rozgłaszania

Innym adresem IP m.ającym specjalne znaczenie jest adres rozgłoszenia używany do rozsyłania informacji do wszystkich komputerów w sieci. Jeśli zamiast wysyłać pakiet do konkretnego komputera wykorzystasz adres rozgłoszenia, zostanie on przesłany do wszystkich komputerów.

Adres rozgłoszenia to zwykle adres IP sieci po zastąpieniu części hosta liczbami 255. Dla sieci klasy C o adresie 24.16.108.0 byłby to więc adres 24.16.108.255.

Adres rozgłoszenia również nie może zostać przypisany żadnemu z komputerów. Oznacza to, że – po uwzględnieniu adresu sieci i adresu rozgłoszenia – w sieci klasy C mogą działać maksymalnie 254 komputery.

Adresy bramki

Adres bramki to adres komputera, który zapewnia łączność ze światem zewnętrznym. Taki komputer zwykle nazywany jest właśnie *bramką*.

Najczęściej bramka posiada dwa interfejsy sieciowe: jeden jest połączony z siecią lokalną, a drugi – z siecią zewnętrzną, zwykle z Internetem.

Aby host mógł połączyć się z siecią zewnętrzną, musi znać adres IP przynajmniej jednej bramki.

Serwery nazw

System DNS (Domain Name System) jest rozproszoną bazą danych umieszczoną na *serwerach nazw*, która pozwala na tłumaczenie adresów IP na nazwy domenowe. Jeśli znasz adres IP serwera, z którym chcesz się połączyć, nie potrzebujesz systemu DNS ani serwera nazw. Zwykle jednak większość aplikacji i sieci zakłada, że użytkownik woli zapamiętywać nazwy domenowe, takie jak **www.bearhome.com**, zamiast ich odpowiedniki IP, na przykład 204.0.134.135.

Każda zarejestrowana domena posiada przynajmniej dwa serwery DNS odpowiedzialne za obsługę zapytań odnoszących się do tej właśnie domeny.

Każdy host, który powinien móc zamieniać adresy domenowe na adresy IP, musi znać numer IP przynajmniej jednego serwera DNS mogący w razie konieczności połączyć się z innymi serwerami DNS, aby przetłumaczyć zadaną nazwę. Adres IP serwera DNS jest zwykle wymagany podczas konfiguracji protokołu TCP/IP.

Program Ping

Ping jest programem dostępnym zarówno w systemie Red Hat Linux 6, jak i Microsoft Windows i służy do testowania najbardziej podstawowej funkcji sieci, czyli łączności. Jeśli możesz **pingować** do hosta, masz pewność, że podstawowe mechanizmy komunikacji z nim działają prawidłowo (choć nadal nie wiesz nic o usługach wyższego poziomu).

Z drugiej strony, jeśli ping nie potrafi komunikować się z hostem, możesz być prawie pewny, że masz jakieś problemy z podstawową konfiguracją sieci.

Aby przetestować połączenie z komputerem w systemie Linux

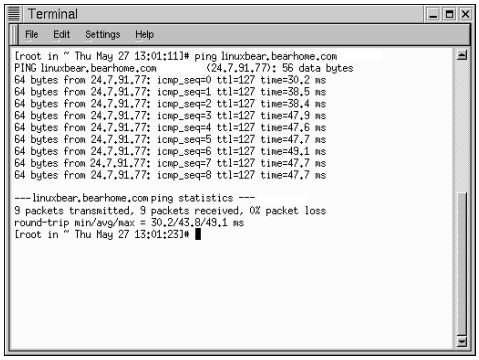
1. W wierszu poleceń wpisz `ping` i nazwę domenową lub numer IP komputera, do którego połączenie chcesz przetestować, na przykład **ping www.bearhome.com**
2. Wciśnij **Enter**. Jeśli nie wystąpią żadne problemy, uzyskasz komunikat zawierający dane o transmitowanych pakietach (**rysunek 13.1**).

Wskazówka

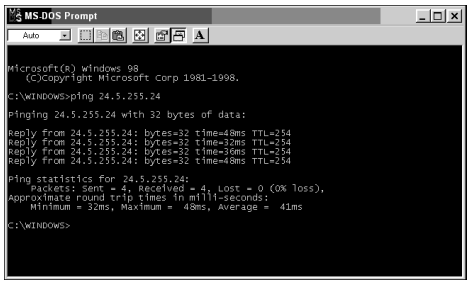
- Program ping dla systemu Linux nie kończy automatycznie swojego działania. Aby zakończyć „pingowanie" i uzyskać podsumowanie przedstawione na **rysunku 13.1**, wciśnij klawisze **Ctrl+C**.

Aby przetestować połączenie z komputerem w systemie Microsoft Windows

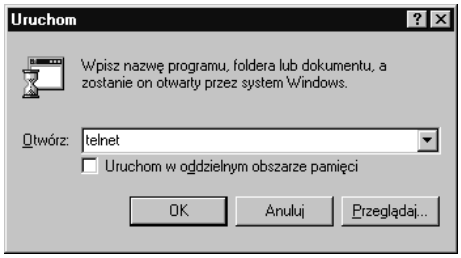
1. Kliknij na przycisk **Start**.
2. Z menu **Programy** wybierz **Tryb MS-DOS**. Otwarte zostanie okno MS-DOS.
3. W wierszu poleceń wpisz ping i nazwę domenową lub numer IP komputera linuxowego, z którym połączenie chcesz przetestować, na przykład **ping 204.0.134.135**. Jeśli nie wystąpią żadne problemy, uzyskasz komunikat zawierający dane o kilku transmitowanych pakietach (**rysunek 13.2**).



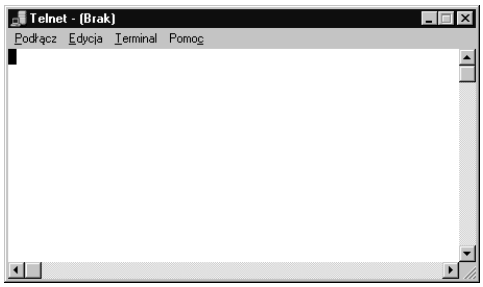
Rysunek 13.1. *Jeśli program ping wyświetla komunikaty o przesyłanych pakietach, podstawowa konfiguracja sieci jest prawidłowa.*



Rysunek 13.2. *Do systemu Linux można zapingować, korzystając z DOS-owego wiersza poleceń.*



Rysunek 13.3. *Aby uruchomić program telnet w systemie Microsoft Windows, otwórz najpierw okno dialogowe Uruchom.*



Rysunek 13.4. *Jeśli uruchomisz program telnet bez podania nazwy hosta, otwarte zostanie puste okno.*

Rysunek 13.5. *Okno dialogowe Połącz używane jest do określenia serwera, z którym należy się połączyć.*

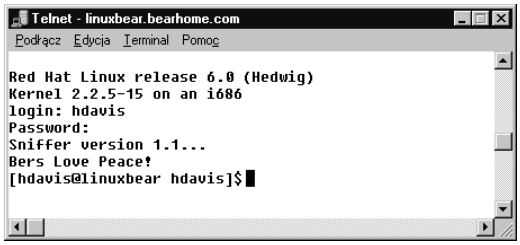
Łączenie się z serwerem za pomocą programu Telnet

Program Telnet umożliwia jeden z najłatwiejszych sposobów wykorzystania serwera linuxowego, którego w tym programie nazywa się hostem. To rozwiązanie redukuje w zasadzie rolę komputera do zwykłego terminala. Użytkownicy, którzy zetknęli się z większymi sieciami, w których działały zarówno systemy UNIX, jak i NT, zetknęli się na pewno z tym programem pracując zdalnie w systemach UNIX. Po uruchomieniu serwera linuxowego procedury są oczywiście dokładnie takie same.

Aby połączyć się z serwerem za pomocą programu telnet dla systemu Windows

1. Z menu **Start** sytemu Microsoft Windows wybierz polecenie **Uruchom**. Otwarte zostanie okno dialogowe **Uruchom**.
2. Wpisz **telnet**.
3. Kliknij na **OK**. Otwarte zostanie puste okno programu telnet (**rysunek 13.4**).
4. Z menu **Podłącz** programu Telnet wybierz polecenie **System zdalny**. Wyświetlone zostanie okno dialogowe **Połącz** (**rysunek 13.5**).
5. W polu **Nazwa hosta** wprowadź nazwę serwera, z którym chcesz się połączyć. Jest to nazwa hosta linuxowego, jak wyjaśniliśmy w rozdziałach 3. i 4., na przykład **linuxbear**. W zależności od połączenia pomiędzy Tobą i serwerem, możesz podać albo samą nazwę serwera, albo nazwę wraz z resztą adresu domenowego, na przykład **linuxbear.bearhome.com**. W niektórych przypadkach wykorzystanie adresu IP działa lepiej niż korzystanie z nazwy domenowej. *(dalej...)*

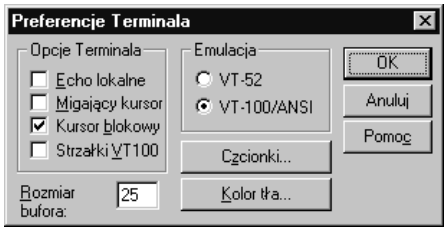
6. Wybierz przycisk **Połącz**. Zostaniesz zapytany o identyfikator użytkownika (**rysunek 13.6**).
7. Wprowadź identyfikator użytkownika.
8. Wciśnij **Enter**.
9. Podaj hasło.
10. Wciśnij **Enter**. Zostaniesz połączony z serwerem linuxowym i wyświetlony zostanie linuxowy znak zachęty w katalogu domowym odpowiedniego użytkownika. Teraz możesz korzystać z wiersza poleceń serwera tak, jak opisaliśmy to w rozdziałach od 10. do 12.



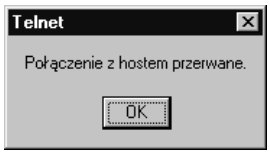
Rysunek 13.6. *Po połączeniu się z hostem zostaniesz zapytany o identyfikator użytkownika i hasło.*

Wskazówki

- Nazwa komputera, z którym chcesz się połączyć, może zostać podana przy uruchamianiu programu Telnet w oknie dialogowym **Uruchom**; można na przykład wpisać **telnet linuxbear**.
- Program Telnet zwykle przechowuje listę ostatnio używanych hostów w menu **Podłącz**. Dzięki temu można ponownie połączyć się z nimi bez konieczności wpisywania ich nazwy.
- Istnieje wiele wersji programu Telnet bardziej funkcjonalnych od programu rozprowadzanego wraz z systemem Windows. Na przykład, jeśli na stronie CNet pod adresem **http://www.download.com** spróbujesz poszukać programu Telnet, znajdziesz ponad 60 różnych wersji, które można pobrać.



Rysunek 13.7. *Program Telnet można dostosować do własnych potrzeb za pomocą okna dialogowego Preferencje terminala.*



Rysunek 13.8. *Po wylogowaniu się z sesji programu Telnet połączenie jest przerywane.*

Aby skonfigurować program Telnet dla systemu Windows

1. Z menu **Terminal** programu Telnet wybierz pozycję **Preferencje**. Wyświetlone zostanie okno dialogowe **Preferencje terminala** (**rysunek 13.7**).
2. Wprowadź potrzebne modyfikacje.
3. Kliknij na **OK**.

Wskazówka

- Najczęstszą modyfikacją jest zwiększenie rozmiaru bufora (domyślnie jest to 25 wierszy). Dzięki temu można wrócić do wierszy wyświetlanych wcześniej.
- Możesz również zmienić czcionkę i kolory, aby poprawić czytelność.

Aby zakończyć połączenie

1. W wierszu poleceń wyświetlanym w oknie programu Telnet wpisz **logout** lub **exit**.
2. Wciśnij **Enter**. Otrzymasz komunikat o zakończeniu połączenia (**rysunek 13.8**).

Korzystanie z FTP

FTP, czyli File Transfer Protocol (protokół transmisji plików), jest jednym z najbardziej popularnych (i najszybszych) protokołów wykorzystywanych do transmisji plików pomiędzy systemami. Ponieważ programy klientów FTP są dostępne praktycznie dla wszystkich systemów operacyjnych, protokół ten jest chyba najbardziej zbliżony do uniwersalnego sposobu przesyłania danych.

Red Hat Linux 6 rozprowadzany jest wraz z serwerem FTP o nazwie Wu-ftpd. Jeśli chcesz umożliwić zdalny dostęp do Twojego serwera za pomocą FTP, program Wu-ftpd Ci w tym pomoże.

Najprawdopodobniej w Twoim systemie program Wu-ftpd został zainstalowany, choć zależy to od rodzaju instalacji i wybranych pakietów (Wu-ftpd jest częścią standardowej instalacji dla serwera). Jeśli nie, zainstaluj go z płyty CD-ROM rozprowadzanej wraz z książką za pomocą programu Gnome RPM, jak pokazaliśmy w rozdziale 2. oraz 3.

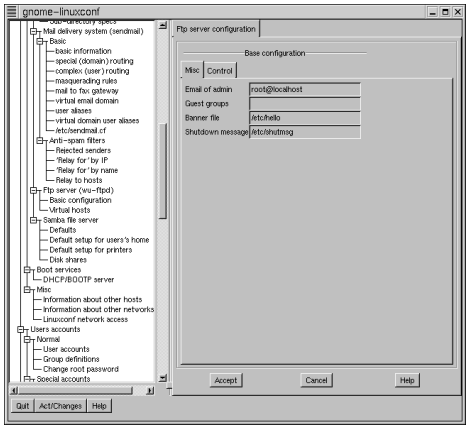
Jeśli program Wu-ftpd zainstalowano w systemie, usługa FTP jest uruchamiana automatycznie w chwili, gdy ktoś próbuje połączyć się z portem FTP (ponieważ może zdarzyć się, że program klienta FTP zapyta o tę informację, powinieneś wiedzieć, że port ma numer 21).

Ogólnie użytkowników serwera FTP można podzielić na dwie grupy:

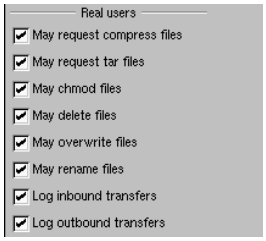
- posiadających własne konto oraz hasło;
- użytkowników anonimowych, nazywanych też gośćmi (ang. *guest*).

W tym kontekście *konto* rozumiane jest jako identyfikator użytkownika wraz z kontem shellowym. Oznacza to, że musisz przyznać każdemu użytkownikowi, który potrzebuje dostępu poprzez FTP, konto shellowe wraz z odpowiednim wpisem w pliku /etc/passwd.

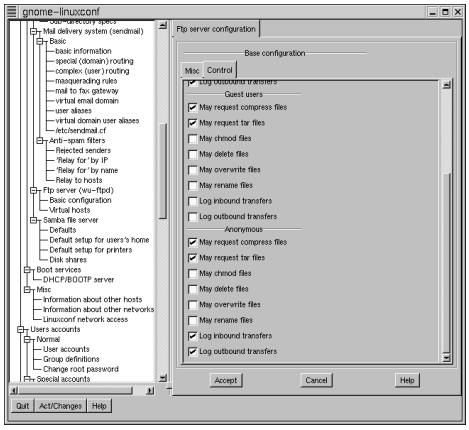
Anonimowe konto FTP używane jest wówczas, gdy chcesz zezwolić wszystkim użytkownikom na dostęp do niektórych plików na serwerze.



Rysunek 13.9. *Serwer Wu-ftpd można skonfigurować za pomocą programu Linux Configuration.*



Rysunek 13.10. *Domyślnie faktycznym użytkownikom systemu – posiadającym własny identyfikator i konto shellowe – przyznana jest większość uprawnień.*



Rysunek 13.11. *Użytkownicy guest i anonymous domyślnie nie mają zbyt dużych uprawnień.*

Choć można kontrolować dostęp do anonimowego FTP (zwykle wymaga się na przykład podania adresu e-mail) na pewno nie można sprawdzić, kto z niego korzysta, dlatego użytkownikom anonimowym trzeba przydzielać zasoby bardzo ostrożnie. Powinieneś również wiedzieć, że udostępnienie anonimowego FTP zawsze wiąże się z pewnym ryzykiem (patrz punkt **Bezpieczeństwo** w dalszej części tego rozdziału).

Aby skonfigurować program Wu-ftpd za pomocą programu Linux Configuration

1. Zaloguj się jako root.
2. Z podmenu **System** menu głównego środowiska Gnome wybierz pozycję **Linux Configuration**. Otwarte zostanie okno programu **Linux Configuration**.
3. Przewiń w dół listę wyświetlaną w lewej części okna i wybierz pozycję **Basic Configuration** z kategorii **Ftp Server**. W prawej części okna wyświetlona zostanie zakładka **Misc** okna dialogowego **FTP Server Configuration** (**rysunek 13.9**).
4. W zakładce **Misc** sprawdź, czy adres e-mail jest poprawny.
5. W polu **Banner file** wprowadź nazwę pliku, który będzie wyświetlany, zanim użytkownik się zaloguje. Tekst wiadomości zostanie zapisany właśnie do tego pliku. Można w nim umieścić na przykład listę plików dostępnych w systemie lub opis zabezpieczeń.
6. W podobny sposób wyznacz plik wyświetlany po zakończeniu sesji, wpisując jego nazwę w polu **Shutdown Message**.
7. Kliknij na zakładkę **Control**. Panel sterowania pozwala na elastyczną konfigurację uprawnień użytkowników (posiadających własne identyfikatory i konta – patrz **rysunek 13.10**) oraz użytkowników anonimowych (**rysunek 13.11**).
8. Określ uprawnienia poszczególnych użytkowników.
9. Kliknij na **Accept**.

Wskazówki

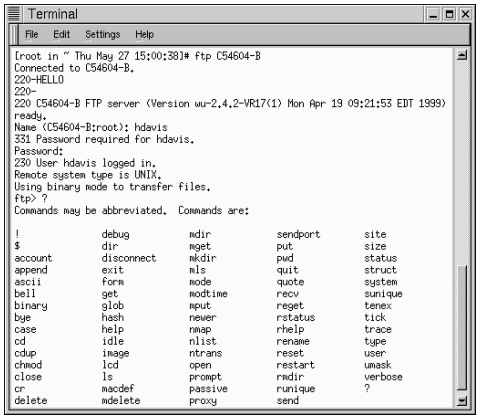
- Anonimowy dostęp do FTP jest ograniczony do katalogu **/home/ftp** i jego podkatalogów.
- Dokładniejsza konfiguracja programu Wu-ftpd możliwa jest poprzez edycję zawartości plików konfiguracyjnych:
  - /etc/ftpaccess
  - /etc/ftpconversions
  - /etc/ftphosts

Aby zalogować się do serwera FTP jako rzeczywisty użytkownik

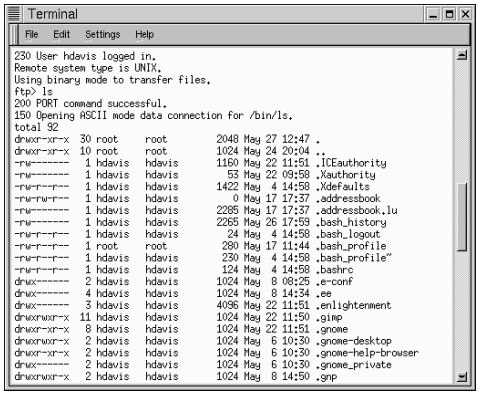
1. Otwórz okno terminala w środowisku Gnome.
2. W wierszu poleceń wpisz **ftp** i nazwę domenową serwera lub jego adres IP.
3. Wciśnij **Enter**. Wyświetlona zostanie zawartość pliku powitalnego.
4. Po znaku zachęty wprowadź identyfikator użytkownika (**rysunek 13.12**).
5. Wciśnij **Enter**.
6. Wprowadź swoje hasło.
7. Wciśnij **Enter**. Powinien zostać wyświetlony znak zachęty FTP: **ftp>**

Aby wyświetlić dostępne polecenia FTP

1. Po znaku zachęty FTP wpisz **?**
2. Wciśnij **Enter**. Na ekranie wyświetlona zostanie lista wszystkich dostępnych poleceń FTP.



Rysunek 13.12. *Jeżeli logujesz się jako rzeczywisty użytkownik, musisz podać swój identyfikator i hasło.*



Rysunek 13.13. *Aby wyświetlić listę plików w katalogu bieżącym, wydaj polecenie* ls.

Aby wyświetlić listę plików dostępnych na serwerze

1. Po znaku zachęty FTP wpisz **ls**.
2. Wciśnij **Enter**. Wyświetlona zostanie lista plików znajdujących się w katalogu bieżącym (**rysunek 13.13**).

Wskazówka

- Polecenia FTP są podzbiorem poleceń służących do manipulowania plikami dostępnych w systemie Linux, opisanych w rozdziale 11. Więcej informacji o poleceniach FTP znajdziesz w dodatku A.

Aby pobrać plik

1. W wierszu poleceń FTP wydaj polecenie **cd**, aby przejść do katalogu, w którym znajduje się interesujący Cię plik.
2. Za pomocą polecenia **lcd** zmień katalog lokalny na ten, w którym pobrany plik ma zostać zapisany.
3. Wydaj polecenie **binary**, aby uaktywnić binarny transfer plików.
4. Wciśnij **Enter**.
5. Wpisz **hash**, aby klient FTP wyświetlał symbole pokazujące postęp w ładowaniu plików.
6. Wciśnij **Enter**.
7. Wpisz **get nazwapliku**, gdzie *nazwapliku* jest nazwą pliku, który chcesz załadować.
8. Wciśnij **Enter**.

Aby zakończyć pracę klienta FTP

1. W wierszu poleceń FTP wpisz **quit**.
2. Wciśnij **Enter**.

Aby zalogować się jako anonimowy użytkownik FTP

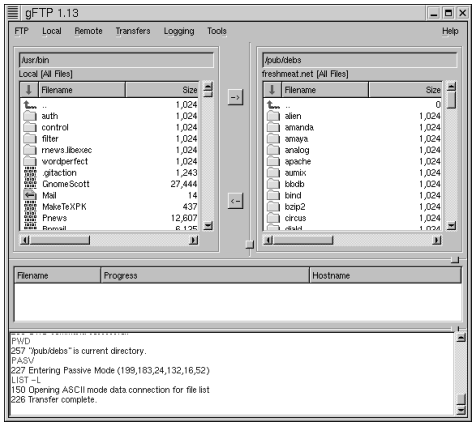
1. Wpisz **ftp** i nazwę serwera, z którym chcesz się połączyć.
2. Wciśnij **Enter**.
3. W odpowiedzi na prośbę o podanie identyfikatora użytkownika, wpisz **anonymous**.
4. Wciśnij **Enter**.
5. Jako hasło podaj swój adres e-mail.

Korzystanie z programu Gnome FTP

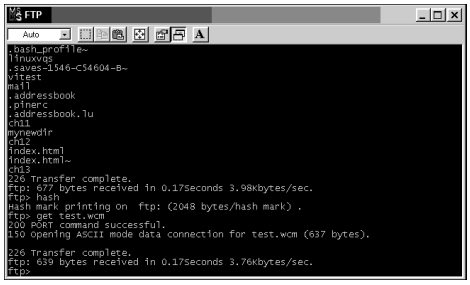
Program Gnome FTP – gFTP – jest graficznym klientem FTP, rozprowadzanym wraz z systemem Red Hat Linux 6 (**rysunek 13.14**). Graficzny klient FTP pozwala na obsługę całego procesu połączenia oraz pobierania plików za pomocą menu i techniki przeciągania i upuszczania plików. Wiele osób woli takie podejście od interfejsu tekstowego.

Aby uruchomić gFTP

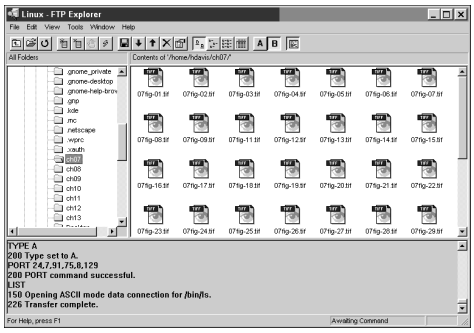
1. Z menu głównego środowiska Gnome wybierz pozycję **File Manager**.
2. Za pomocą programu File Manager zlokalizuj katalog **/usr/bin**.
3. Kliknij na katalog **/usr/bin**, aby wyświetlić jego zawartość w prawej części okna.
4. Przewiń zawartość prawej części okna, aż zobaczysz plik o nazwie gftp.
5. Kliknij dwukrotnie na plik gftp. Uruchomiony zostanie program Gnome FTP.



Rysunek 13.14. *Gnome FTP – gFTP – pozwala na korzystanie z funkcji FTP bez znajomości składni poszczególnych poleceń.*



Rysunek 13.15. *Klient FTP dla systemu Windows działa podobnie jak analogiczny program linuxowy.*



Rysunek 13.16. *FTP Explorer jest graficznym klientem FTP dla systemu Microsoft Windows.*

Korzystanie z klientów FTP dla systemu Windows

Z serwerem FTP działającym pod kontrolą systemu Linux możesz również połączyć się z łatwością za pomocą jednego z klientów FTP dla systemu Windows. Klient FTP pracujący w trybie tekstowym obsługuje takie same polecenia, jak jego linuxowy odpowiednik.

Aby zalogować się do serwera FTP za pomocą klienta działającego w trybie tekstowym dla systemu Windows

1. Kliknij na przycisk **Start** na pulpicie systemu Microsoft Windows.
2. Z menu **Programy** wybierz pozycję **Tryb MS-DOS**. Otwarte zostanie okno trybu MS-DOS.
3. W DOS-owym wierszu poleceń wpisz **ftp** i nazwę lub adres IP serwera, z którym chcesz się połączyć.
4. Wciśnij **Enter**. Po zalogowaniu się będziesz mógł korzystać z poleceń FTP, podobnie jak w wersji linuxowej tego programu (**rysunek 13.15**).

Wskazówka

- Dla systemu Microsoft Windows dostępnych jest wiele dobrych, graficznych klientów FTP. Na **rysunku 13.16** przedstawiony jest program FTP Explorer firmy FTPx Corporation.

Korzystanie z NFS

NFS, czyli Network File System, sieciowy system plików, pozwala dzielić pliki pomiędzy systemami linuxowymi (i UNIX-owymi) za pośrednictwem sieci opartej na TCP/IP.

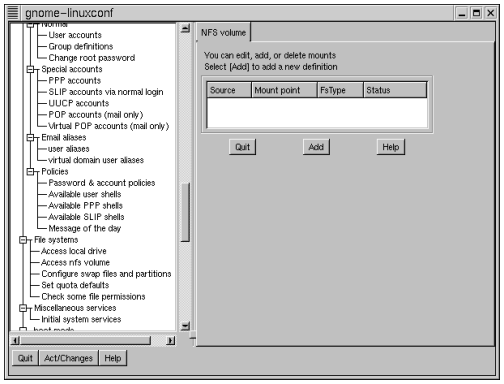
W zasadzie NFS działa bardzo podobnie jak dyski CD-ROM czy dyskietki dodawane do systemu plików. Inaczej mówiąc, aby uzyskać dostęp jako klient do sieciowego systemu plików NFS, trzeba go najpierw *zamontować*. Następnie staje się on integralną częścią systemu plików, do którego jest dołączony w punkcie zamontowania.

Aby jednak klient mógł zamontować system plików z serwera NFS, serwer musi na to zezwolić (ma to oczywiście konsekwencje dla bezpieczeństwa systemu – zagadnienie to poruszymy jeszcze w punkcie **Bezpieczeństwo**).

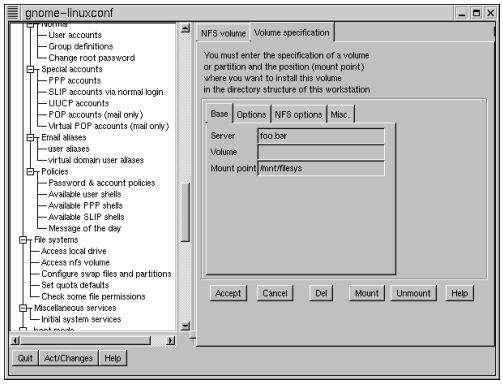
Kiedy umożliwiasz montowanie swojego systemu plików, musisz określić, która jego część może być montowana. Jeśli zdecydujesz się udostępnić wszystko, rozpoczynając od katalogu głównego, użytkownicy będą mieli dostęp do całego systemu plików. Częściej jednak będziesz chciał udostępnić tylko fragment systemu plików, dzięki czemu dostępne będą tylko pliki znajdujące się w podkatalogach udostępnionych katalogów.

Możliwe jest zezwolenie wszystkim użytkownikom na montowanie systemu NFS udostępnianego przez Twój serwer (a przynajmniej tym użytkownikom, którzy mogą połączyć się z Twoim hostem). Zwykle jednak na montowanie systemów plików zezwala się tylko poszczególnym hostom.

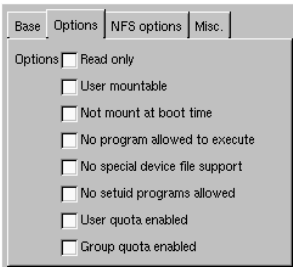
Po wyeksportowaniu systemu NFS i zamontowaniu go na komputerze zdalnym z punktu widzenia tego komputera staje się on częścią jego systemu plików i jest obsługiwany tak samo, jak pozostałe części tego systemu.



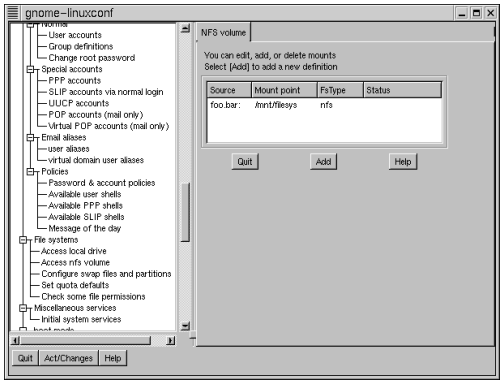
Rysunek 13.17. *Zakładka NFS Volume pozwala na montowanie eksportowanych przez systemy zdalne systemów NFS.*



Rysunek 13.18. *Okno dialogowe Volume* ***Specification*** *pozwala podać informacje dotyczące montowania systemu zdalnego.*



Rysunek 13.19. *Można ustalić wartości opcji montowania zdalnego systemu plików, takich jak zezwolenie na wykonywanie plików oraz montowanie go przy uruchamianiu systemu.*



Rysunek 13.20. *Zdalne systemy plików montowane przy starcie systemu są wyświetlane na zakładce NFS Volume.*

Montowanie zdalnych systemów plików

Do montowania eksportowanych przez serwer systemów NFS służy polecenie mount; aby montować je podczas uruchamiania systemu, można dodać odpowiednie wpisy do pliku /etc/fstab. Mimo to w systemie Red Hat Linux 6 łatwiej jest do tego celu wykorzystać graficzne narzędzia środowiska Gnome.

Aby zamontować zdalny system plików

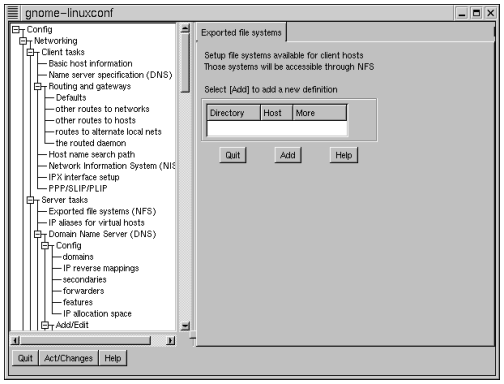
1. Zaloguj się jako root.
2. Uruchom program Linux Configuration.
3. Przewiń listę wyświetlaną w lewej części okna, aż znajdziesz kategorię **Network File Systems**.
4. Wybierz pozycję **Access NFS Volume**. Wyświetlona zostanie zakładka **NFS Volume** (**rysunek 13.17**).
5. Kliknij na przycisk **Add**. Otwarte zostanie okno dialogowe **Volume Specification** (**rysunek 13.18**).
6. Wprowadź nazwę serwera, który eksportuje sieciowy system plików oraz punkt zamontowania.
7. Aby określić dodatkowe opcje, kliknij na zakładkę **Options** (**rysunek 13.19**). Możesz na przykład nie chcieć zezwolić na wykonywanie plików zapisanych w systemie zdalnym. Jeśli zaznaczysz opcję **Not Mount at Boot Time**, zdalny system plików nie będzie montowany automatycznie podczas startu systemu.
8. Aby zamontować zdalny system plików, kliknij na **Mount**.
9. Aby dodać system plików do listy zdalnych systemów plików montowanych podczas startu systemu, kliknij na **Accept**. System zostanie wyświetlony w zakładce **NFS Volume** (**rysunek 13.20**).

Eksportowanie systemów plików

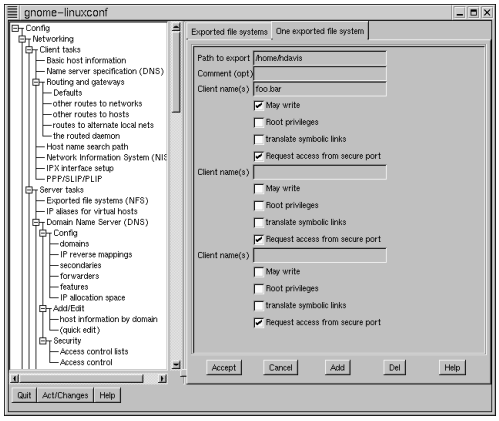
Aby wyeksportować gałąź systemu plików (lub cały system plików, jeśli jako punkt początkowy wpisana zostanie nazwa katalogu głównego, czyli /) w tradycyjny sposób, możesz zmodyfikować zawartość pliku /etc/exports. Jednak również tu łatwiej jest posłużyć się graficznymi narzędziami konfiguracyjnymi.

Aby wyeksportować system plików

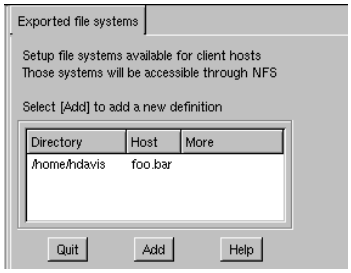
1. Zaloguj się jako root.
2. Uruchom program Linux Configuration.
3. Przewiń listę wyświetlaną w lewej części okna, aż znajdziesz kategorię **Server Tasks**.
4. Kliknij na pozycję **Exported File Systems (NFS)**. Wyświetlona zostanie zakładka **Exported File Systems** (**rysunek 13.21**).
5. Kliknij na przycisk **Add**. Wyświetlona zostanie zakładka **One Exported File System** (**rysunek 13.22**).
6. Wprowadź ścieżkę dostępu do katalogu, który ma zostać wyeksportowany, na przykład
   /exports
   lub
   /home/hdavis
   Oczywiście / oznacza katalog główny, czyli cały system plików.
7. Wprowadź nazwę klienta. *Nazwa klienta* to nazwa hosta, czyli komputera, który będzie korzystał z systemu plików, a nie nazwa użytkownika. Jeśli pole to pozostanie puste, każdy host będzie mógł zamontować eksportowany system plików.
8. Określ wartości odpowiednich opcji (poniżej przedstawiamy wskazówki).
9. Kliknij na przycisk **Add**. Eksportowany system plików pojawi się w liście systemów dostępnych poprzez NFS (**rysunek 13.23**).



Rysunek 13.21. *Zakładka Exported File Systems służy do eksportowania gałęzi systemu plików.*



Rysunek 13.22. *Informacje o eksportowanym systemie należy w prowadzić w zakładce One Exported File System.*



Rysunek 13.23. *Systemy plików, które są dostępne dla innych komputerów poprzez NFS, wyświetlane są w liście Exported File Systems.*

Wskazówki

- Opcje ustawiane w obrębie zakładki **One Exported File System** mają poważne konsekwencje dla bezpieczeństwa systemu.
- Zezwolenie na dostęp do głównego systemu plików jest potencjalnie niebezpieczne. Zezwolenie zdalnemu użytkownikowi na posiadanie uprawnień administratora to ryzyko – takie rozwiązanie wchodzi w grę tylko w niektórych sytuacjach.
- Zezwolenie na zapis jest również potencjalną luką w bezpieczeństwie – użytkownicy zdalni mogą usunąć ważne pliki i zaatakować system przeciążając go.
- Dobrym pomysłem jest wymaganie dostępu poprzez bezpieczny port.

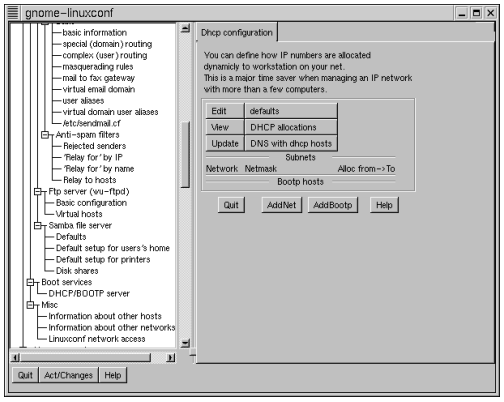
Korzystanie z DHCP

DHCP – Dynamic Host Configuration Protocol, czyli protokół dynamicznej konfiguracji komputerów – pozwala na automatyczne przyznawanie *dynamicznych adresów IP* hostom i sieciom. Jeśli musisz administrować siecią klasy C – lub większą – dynamiczne przydzielanie adresów IP może bardzo ułatwić Ci pracę.

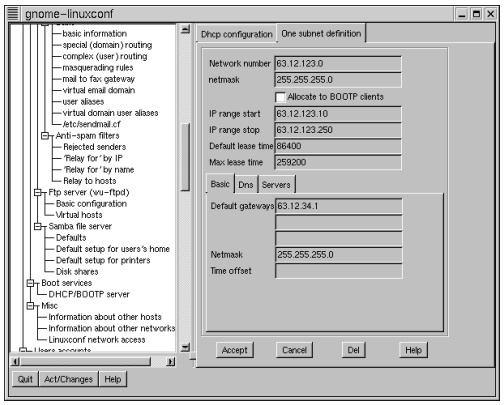
Aby wykorzystać DHCP do przypisywania adresów IP komputerom, w sieci musi działać serwer DHCP. System linuxowy może zostać skonfigurowany jako taki serwer, ale należy wziąć pod uwagę, że nie można przyznawać adresów z dowolnej puli. Adresy IP komputerów w sieci klasy C muszą należeć do Ciebie, abyś mógł je przydzielać. Co więcej, konfiguracji takiej nie należy uważać za trywialną. Często spotykana porada „zapytaj administratora sieci", w tym przypadku raczej nie jest zbyt pomocna, ponieważ jeśli decydujesz się na konfigurację serwera DHCP, prawdopodobnie to właśnie Ty jesteś administratorem. Aby poprawnie skonfigurować DHCP, będziesz musiał skontaktować się z dostawcą, który zapewnia Ci adresy IP sieci klasy C.

Aby skonfigurować serwer DHCP w systemie linuxowym

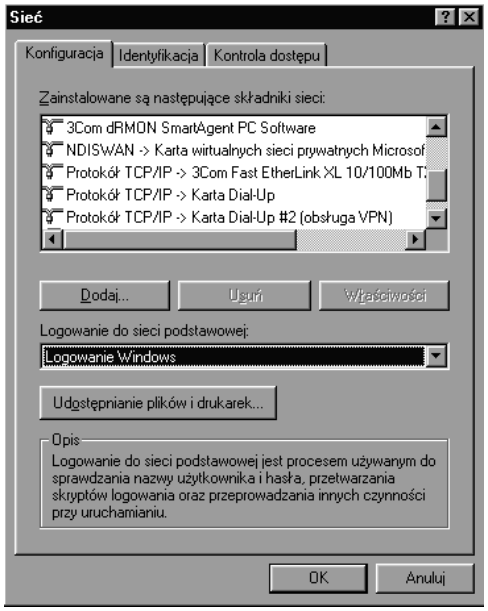
1. Zaloguj się jako root.
2. Uruchom program Linux Configuration.
3. Przewiń listę wyświetlaną w lewej części okna, aż znajdziesz kategorię **Boot Services**.
4. Kliknij na pozycję **DHCP/BOOTP Server**. Wyświetlona zostanie zakładka **DHCP Configuration** (**rysunek 13.24**).
5. Kliknij na przycisk **Add Net**. Wyświetlona zostanie zakładka **One Subnet Definition** (**rysunek 13.25**).
6. W polu **Network Number** wprowadź numer IP sieci.
7. W polu **Netmask** wprowadź maskę sieci.



Rysunek 13.24. *Zakładka DHCP Configuration pozwala na dynamiczne przypisywanie adresów IP komputerom w sieci.*



Rysunek 13.25. *Każdej z podsieci można przypisać inny zakres numerów IP.*



Rysunek 13.26. *Za pomocą okna dialogowego Network Properities systemu Microsoft Windows można skonfigurować system, tak by korzystał z serwera DHCP.*

8. W polach **IP Range Start** i **IP Range Stop** wprowadź pierwszy i ostatni z przydzielanych adresów.
9. W polu **Default Lease Time** wprowadź wartość **86400** (wartość w sekundach, oznaczająca cały dzień). Jest to czas, przez jaki serwer może utrzymywać adres IP bez konieczności odnowienia go w porozumieniu z serwerem.
10. W polu **Max Lease Time** wprowadź wartość **259200** (maksymalny czas, przez jaki host może zajmować adres IP).
11. Określa przynajmniej jedną bramkę domyślną oraz maskę sieci.
12. Kliknij na **Accept**.

Wskazówki

- Ustawienia serwera DHCP można zmienić, edytując zawartość pliku /etc/dhcpd.conf.
- Jeśli zdecydujesz się na ręczną edycję pliku /etc/dhcpd.conf, musisz utworzyć pusty plik o nazwie /etc/dhcpd.leases.
- Aby ręcznie uruchomić usługę DHCP, wydaj następujące polecenie: **/etc/rc.d/init.d/dhcpd restart**

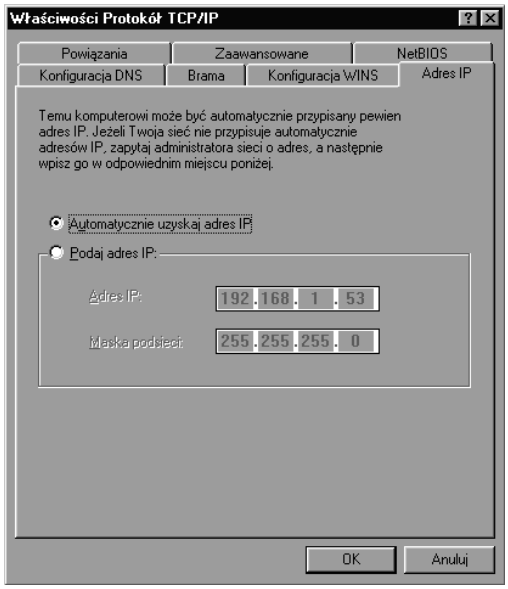
Aby skonfigurować klienta Microsoft Windows, tak by korzystał z serwera DHCP

1. Kliknij prawym klawiszem myszy na ikonę **Otoczenie sieciowe** i z menu kontekstowego wybierz pozycję **Właściwości**. Otwarte zostanie okno dialogowe **Sieć** (**rysunek 13.26**).
2. Przewiń listę zainstalowanych składników, aż znajdziesz wpis dotyczący protokołu TCP/IP powiązanego z Twoją kartą sieciową.
3. Wybierz pozycję TCP/IP.

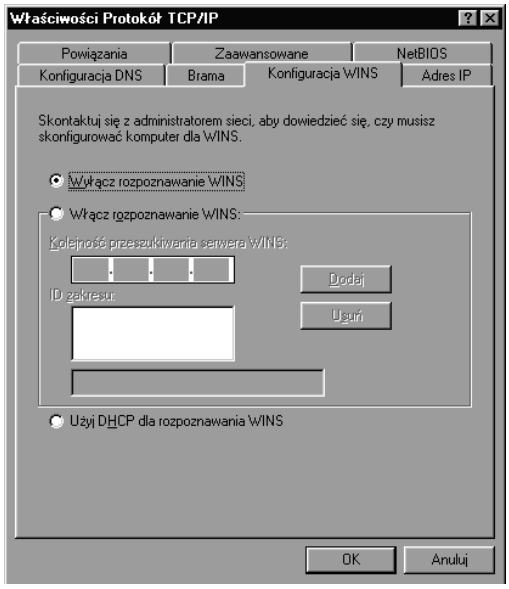
4. Kliknij na przycisk **Właściwości**. Wyświetlone zostanie okno dialogowe **Właściwości: TCP/IP** (**rysunek 13.27**).
5. Przejdź do zakładki **Adres IP** i zaznacz opcję **Uzyskaj adres IP z serwera DHCP**.
6. Przejdź do zakładki **Konfiguracja WINS** i załącz opcję **Użyj DHCP do rozpoznawania WINS** (**rysunek 13.28**).
7. Przejdź do zakładki **Bramka** i upewnij się, że nie zdefiniowano żadnych bramek.
8. W zakładce **Konfiguracja DNS** wyłącz obsługę tego mechanizmu (wartości DNS są dostarczane przez DHCP).
9. Kliknij na **OK**, aby powrócić do okna dialogowego **Sieć**.
10. Kliknij na **OK**, aby zaakceptować wprowadzone zmiany.
11. Po wyświetleniu odpowiedniego pytania, kliknij na klawisz **Tak**, zezwalając na restart komputera.

Wskazówka

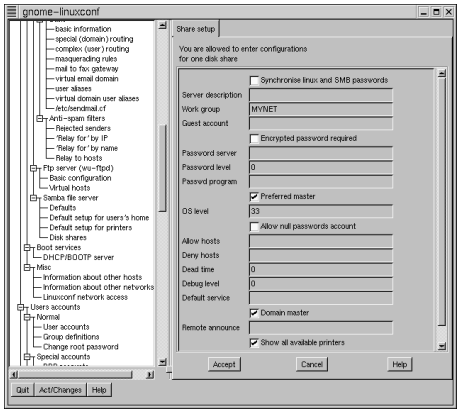
- W zależności od dostępnych w systemie plików po restarcie systemu może być konieczne włożenie do napędu dysku CD-ROM z wersją instalacyjną systemu Windows.



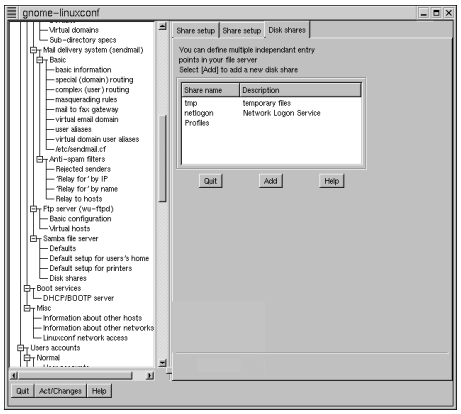
Rysunek 13.27. *Zaznacz opcję Uzyskaj adres IP z serwera DHCP.*



Rysunek 13.28. *Opcja Użyj DHCP do rozpoznawania WINS powinna być aktywna.*



Rysunek 13.29. *W zakładce Share Setup należy podać nazwę grupy roboczej Windows.*



Rysunek 13.30. *Zakładka Disk Shares pozwala na definiowanie wielu udziałów dla systemów Windows.*

SAMBA

Protokół sieciowy używany przez komputery z systemem Microsoft Windows nazywa się SMB, czyli Server Message Block. Choć firma Microsoft określa takie rozwiązanie jako sieć Microsoft Windows, w rzeczywistości jest ono wykorzystywane w wielu systemach operacyjnych.

Klienci Microsoft Windows podłączeni do sieci opartej na SMB mogą komunikować się z serwerem linuxowym dzięki linuxowej implementacji SMB o nazwie SAMBA. Więcej informacji na ten temat znajdziesz pod adresem **http://www.samba.org**.

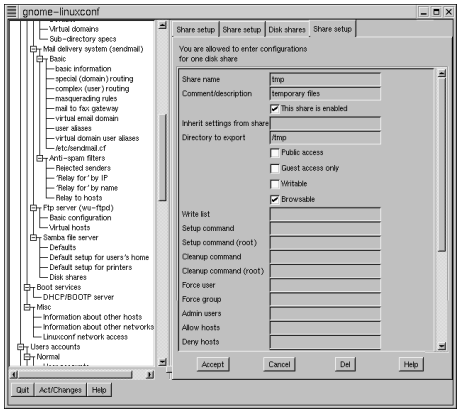
Trzeba wyraźnie powiedzieć, że SAMBA to nie to samo, co NFS. Jeśli Twój serwer działa w sieci mieszanej wraz z komputerami pracującymi pod kontrolą systemów Windows i UNIX, możesz zezwolić klientom UNIX-owym na korzystanie z NFS, a klientom Windows na łączenie się z serwerem SAMBA –zarządzać tymi usługami trzeba jednak oddzielnie.

Aby skonfigurować serwer SAMBA

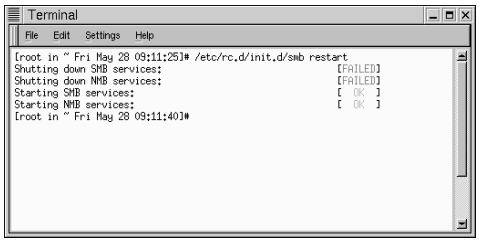
1. Zaloguj się jako root.
2. Uruchom program Linux Configuration.
3. Przewiń listę wyświetlaną w lewej części okna, aż znajdziesz kategorię **Samba File Server**.
4. Kliknij na pozycję **Defaults**. Wyświetlona zostanie zakładka **Share Setup** (**rysunek 13.29**).
5. W polu **Work Group** wprowadź nazwę grupy roboczej Microsoft Windows, do której należą pozostałe komputery, na przykład **MYNET**.
6. Kliknij na **Accept**.
7. Przejdź do zakładki **Disk Shares** (**rysunek 13.30**).

(dalej...)

8. Kliknij na przycisk **Add**, aby zdefiniować nowe udziały. Wyświetlona zostanie zakładka **Share Setup** (**rysunek 13.31**).
9. Wprowadź nazwę udziału, na przykład **tmp**.
10. Wprowadź ścieżkę dostępu do katalogu, który ma być widoczny jako udział, na przykład **/tmp**.
11. Zaznacz opcję **This Share Is Enabled**.
12. Zaznacz opcję **Browsable**.
13. Kliknij na przycisk **Accept**.
14. Po wyświetleniu odpowiedniej prośby zatwierdź wprowadzone zmiany.
15. Uruchom okno terminala.
16. W wierszu poleceń wpisz **/etc/rc.d/init.d/smb restart**. Uruchomiony zostanie serwer SAMBA (**rysunek 13.32**). Ponieważ nie działał on wcześniej, za pierwszym nie powiedzie się razem jego zamykanie– stąd komunikaty FAILED. Uruchomienie serwera nie powinno jednak stanowić problemu.



Rysunek 13.31. *Udostępniane katalogi są wyświetlane po wybraniu opcji Share Setup.*



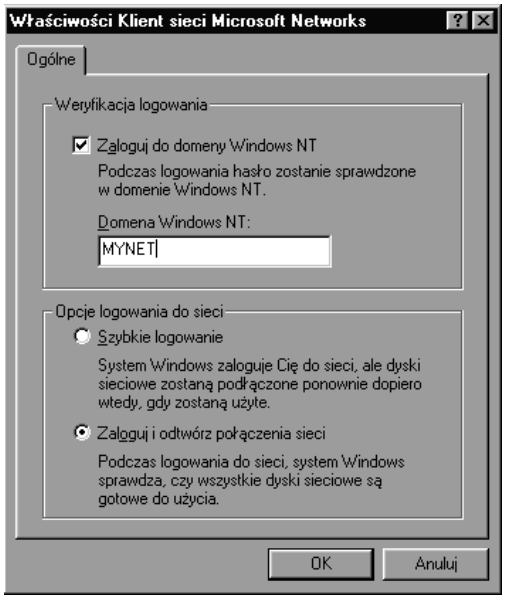
Rysunek 13.32. *Serwer SAMBA został uruchomiony.*

Wskazówka

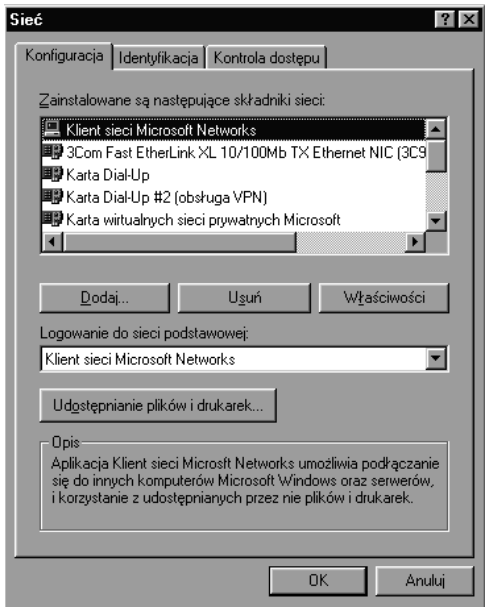
- Serwer SAMBA można skonfigurować z wiersza poleceń, edytując zawartość pliku /etc/smb.conf. Plik ten zawiera dużą liczbę komentarzy oraz przykładowe wpisy.

Aby skonfigurować klienta Windows

1. Kliknij prawym klawiszem myszy na ikonę **Otoczenie sieciowe** i z menu kontekstowego wybierz pozycję **Właściwości**. Otwarte zostanie okno dialogowe **Sieć**.
2. Jeśli serwer SAMBA korzysta z DHCP, uruchom opcję dynamicznego DHCP zgodnie ze wskazówkami w punkcie „Aby skonfigurować klienta Microsoft Windows tak, by korzystał z serwera DHCP”.
3. Z listy składników sieci wybierz pozycję **Klient sieci Microsoft Networks**.



Rysunek 13.33. *Informacja o domenie Windows NT jest ustawiana za pomocą zakładki Właściwości: Klient sieci Microsoft Networks.*



Rysunek 13.34. *Upewnij się, że podstawową siecią jest Klient sieci Microsoft Networks.*

4. Kliknij na przycisk **Właściwości**. Wyświetlone zostanie okno dialogowe **Właściwości: Klient sieci Microsoft Networks** (**rysunek 13.33**).
5. Zaznacz opcję **Zaloguj do domeny Windows NT**. Z punktu widzenia klienta Windows serwer SAMBA jest serwerem Windows NT.
6. Upewnij się, że nazwa domeny jest taka sama, jak nazwa grupy roboczej wprowadzona w konfiguracji serwera SAMBA, na przykład MYNET.
7. Kliknij na **OK**.
8. W oknie dialogowym **Sieć** upewnij się, że podstawową siecią jest **Klient sieci Microsoft Networks** (**rysunek 13.34**).
9. Kliknij na **OK**.
10. Po wyświetleniu zapytania odpowiedz **Tak**, zezwalając na restart komputera.
11. Zaloguj się do systemu Windows za pomocą identyfikatora i hasła obowiązującego na serwerze linuxowym.

Wskazówki

- W zależności od tego, jakie pliki znajdują się na dysku twardym, po restarcie komputera może być potrzebna płyta CD-ROM z wersją instalacyjną systemu Windows.
- Rozwiązywanie problemów z konfiguracją serwera SAMBA opisano krok po kroku w dokumencie autorstwa Andrew Tridgella, który opracował oprogramowanie SAMBA dla systemu Linux. Dokument ten można znaleźć w katalogu **/samba/docs/DIAGNOSIS.html** pod adresem **http://www.samba.org**.

Program SMB Client

Program SMB Client, o nazwie smbclient, służy do łączenia komputera linuxowego z serwerem SMB, na przykład działającym w systemie Windows NT.

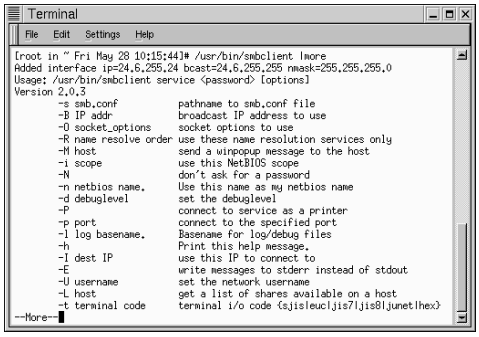
Smbclient to program działający w wierszu poleceń i posiadający wiele opcji.

Aby wyświetlić informacje o składni programu smbclient

1. Uruchom okno terminala.
2. W wierszu poleceń wpisz **/usr/bin/smbclient | more**
   Wyświetlone zostaną wszystkie dostępne polecenia i opcje podzielone na porcje mieszczące się jednorazowo na ekranie za pomocą programu more.

Wskazówki

- W **tabeli 13.2** przedstawiamy niektóre z częściej używanych opcji programu smbclient.
- Po uzyskaniu dostępu do zasobu można korzystać z wielu poleceń do manipulowania plikami i katalogami. Są one podobne do poleceń klienta FTP (patrz podrozdział **Korzystanie z FTP** we wcześniejszej części tego rozdziału). Niektóre z częściej używanych poleceń zostały zebrane w **tabeli 13.3**.



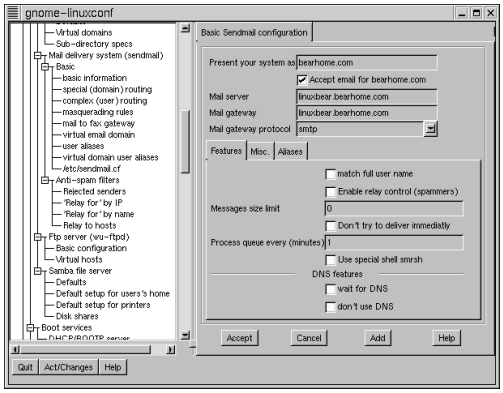
Rysunek 13.35. *Program smbclient może być uruchomiony z wiersza poleceń z różnymi opcjami.*

Tabela 13.2. *Ważniejsze opcje polecenia smbclient.*

Opcja	Komentarz
-L host	Wyświetla listę wszystkich zasobów udostępnianych przez danego hosta
-I adres_IP	Powoduje, że program smbclient będzie wyszukiwał host na podstawie adresu IP, a nie nazwy
-N	Używana, kiedy nie jest wymagane hasło
-U nazwa_użytkownika	Używana, aby podać identyfikator użytkownika w przypadku, gdy jest on inny niż identyfikator użytkownika systemu Linux. Hasło podaje się po symbolu procenta. Jeśli na przykład jesteś zalogowany jako root, możesz wydać następujące polecenie, aby połączyć się jako juser: **smbclient \\\\serwer\\tmp –U juser%haslo**
-W grupa_robocza	Określa grupę roboczą, w której znajduje się serwer SMB

Tabela 13.3. *Polecenia do obsługi plików.*

Polecenie	Komentarz
cd	Pozwala zmienić katalog
del	Usuwa plik
dir	Wyświetla zawartość katalogu
get	Pobiera plik z serwera i zapisuje go w katalogu lokalnym
lcd	Pozwala zmienić katalog lokalny
mkdir	Tworzy katalog w zdalnym systemie plików
put	Wysyła plik lokalny do systemu zdalnego
quit	Kończy pracę programu smbclient



Rysunek 13.36. *Podstawowa konfiguracja programu sendmail zwykle wystarcza, aby poczta działała prawidłowo.*

Serwer poczty

Prawdopodobnie przywykłeś do obsługi poczty za pomocą programu, takiego jak na przykład Eudora, Netscape Messenger czy Outlook. Programy te są klientami pocztowymi – aby mogły działać, pocztę musi dostarczyć im program serwera działający w sieci, nazywany również agentem transportu poczty (Mail Transport Agent, MTA).

Sendmail jest najczęściej używanym programem MTA dla systemów UNIX-owych i, prawdopodobnie, najpopularniejszym ze wszystkich programów tego typu. Sendmail rozprowadza się wraz z systemem Red Hat Linux 6. Jeśli podczas instalacji wybrałeś opcję Server, program sendmail zainstalowano również w Twoim systemie. W przeciwnym przypadku możesz zainstalować go z dysku CD-ROM dołączonego do książki za pomocą programu Gnome RPM, zgodnie z instrukcjami z rozdziału 2. i 3.

W tym podrozdziale pokażemy, jak skonfigurować podstawowe opcje programu sendmail (nie jest ich zbyt wiele). Informacje o bardziej zaawansowanych możliwościach znajdziesz pod adresem **http://www.sendmail.org**.

Aby utworzyć podstawową konfigurację programu sendmail

1. Zaloguj się jako root.
2. Uruchom program Linux Configuration.
3. Przewiń listę wyświetlaną w lewej części okna, aż znajdziesz kategorię **Mail Delivery System** (**Sendmail**).
4. Wybierz pozycję **Basic Information**. Wyświetlona zostanie zakładka **Basic Sendmail Configuration** (**rysunek 13.36**).
5. Wprowadź nazwę, która będzie używana przy wysyłaniu poczty. Wszystkie wiadomości pochodzące z Twojej organizacji będą prezentowane za pomocą tej nazwy, która należy do domeny, bez względu na nazwę hosta, z którego faktycznie pochodzą. *(dalej...)*

6. Zaznacz opcję **Accept Mail for the Domain**.
7. Wprowadź nazwę serwera poczty, który będzie przechowywał pocztę użytkowników oraz bramki pocztowej (zwykle jest nią serwer poczty).
7. Określ protokół używany przez bramkę poczty, domyślnie jest to SMTP.
8. Kliknij na **Accept**.
9. Po wyświetleniu monitu zaakceptuj wprowadzone zmiany.

Wskazówki

- Pliki pomocy, które są dostępne po kliknięciu na przycisk **Help**, zawierają dokładniejsze informacje o konfigurowaniu systemu poczty (w przeciwieństwie do plików pomocy na inne tematy, które zwykle nie są jeszcze gotowe).
- Możesz załączyć opcję **Relay Control**, która zabezpieczy Cię przed wykorzystaniem Twojego serwera do rozsyłania poczty przez nieproszonych gości i zaśmiecania Sieci reklamami czy łańcuszkami szczęścia.

Bezpieczeństwo

Truizmem jest stwierdzenie, że systemy UNIX i Linux nie zostały zaprojektowane z myślą o bezpieczeństwie. Linux stworzono po to, aby ułatwić manipulowanie danymi i plikami w środowisku sieciowym i wielodostępnym. Taki system jest z definicji podatny na ataki, szczególnie jeśli ma połączenie z Internetem.

Co więcej:

- zabezpieczenia w systemie Linux są załączone albo wyłączone (jeśli jesteś administratorem);
- wiele istotnych funkcji administracyjnych jest wykonywanych na zewnątrz jądra systemu – na przykład poprzez edycję plików konfiguracyjnych – w związku z czym łatwo nimi manipulować.

Trzeba więc zdawać sobie sprawę z faktu, że serwer linuxowy nigdy nie będzie całkowicie bezpieczny. Poza tym, im bezpieczniejszy serwer, tym mniej wygodne korzystanie z niego.

Pamiętając o powyższych uwagach, spróbujmy zastanowić się, jakie zabezpieczenia należy wprowadzić w niewielkim systemie.

Na początek zawsze warto zadbać o przestrzeganie kilku prostych reguł:

- W systemie podłączonym do Internetu nie należy przechowywać plików, które mogą być potencjalnym celem ataku włamywaczy czy nieuczciwej konkurencji. Jeśli musisz przechowywać takie pliki, rozważ nadanie im jakichś niezbyt oczywistych nazw oraz ich zaszyfrowanie.
- Zapoznaj się z narzędziami służącymi do podniesienia poziomu bezpieczeństwa. W szczególności, korzystaj z programów dostępnych bezpłatnie pod adresem **http://www.cern.org**, takich jak tripwire, crack czy COPS (ich opis znajdziesz w ramce **Programy zabezpieczające**), pozwalających na diagnozowanie ewentualnych luk w bezpieczeństwie.
- Dokładnie badaj dane o nietypowych działaniach.
- Upewnij się, że każdy użytkownik ma własny identyfikator i że nie dzieli go z żadnym innym.
- Wymagaj stosowania haseł użytkowników.
- Używaj bezpiecznego hasła użytkownika root i zmieniaj je regularnie.
- Upewnij się, że pliki **/etc/passwd** i **/etc/group** są własnością użytkownika root i że tylko on może wpisywać do nich dane.

Programy zabezpieczające

Tripwire, którego autorami są Gene Kim i Gene Spafford, kontroluje prawa dostępu i sumy kontrolne najważniejszych plików systemowych, dzięki czemu można łatwo stwierdzić, czy pliki te zostały podmienione, uszkodzone czy zmodyfikowane.

Crack, autorstwa Aleca D. E. Muffeta, potrafi wskazać słabe hasła użytkowników.

COPS, którego autorem jest Dan Farmer, wyszukuje potencjalne luki w bezpieczeństwie i informuje o nich pocztą elektroniczną wraz ze szczegółowym opisem problemu.

Podsumowanie

W tym rozdziale nauczyłeś się:

- Rozumieć podstawowe pojęcia związane z protokołem TCP/IP.
- Korzystać z programu ping.
- Łączyć się z serwerem za pomocą programu Telnet.
- Konfigurować program Wu-ftpd.
- Korzystać z klienta FTP.
- Montować zdalny system plików NFS.
- Eksportować system plików NFS.
- Konfigurować DHCP.
- Konfigurować serwer SAMBA.
- Korzystać z programu smbclient.
- Tworzyć podstawową konfigurację programu sendmail.