

IDŹ DO

PRZYKŁADOWY ROZDZIAŁ



SPIS TREŚCI

KATALOG KSIĄŻEK

KATALOG ONLINE

ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK

DODAJ DO KOSZYKA

CENNIK I INFORMACJE

ZAMÓW INFORMACJE
O NOWOŚCIACH

ZAMÓW CENNIK

CZYTELNIA

FRAGMENTY KSIĄŻEK ONLINE

Windows 2000 Professional. Księga eksperta

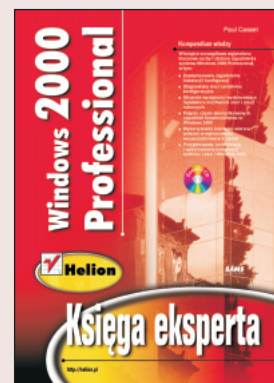
Autorzy: Paul Cassel, Glen Bergen, David Berry, Dave Bixler, Irfan Chaudhry, Chris Farnsworth, Edward Tetz, Rick Tempestini

Tłumaczenie: Sławomir Szymanowski

ISBN: 83-7197-203-2

Tytuł oryginału: [Windows 2000 Professional Unleashed](#)

Format: B5, stron: 838



Zastosuj w instalacji, administracji i obsłudze Windows 2000 Professional porady eksperta Paula Cassela.

W książce szczegółowo wyjaśniono kluczowe cechy i złożone zagadnienia systemu Windows 2000 Professional, w tym:

- Zaawansowane zagadnienia instalacji i konfiguracji.
- Diagnostykę sieci i problemy konfiguracyjne.
- Strojenie wydajności wydobywające największe możliwości sieci i stacji roboczych.
- Pojęcie często skomplikowanych zagadnień bezpieczeństwa w Windows 2000.
- Wykorzystanie interfejsu wiersza poleceń w wykonywaniu wyspecjalizowanych zadań.
- Przygotowanie, konfigurację i wykorzystanie kombinacji systemu Linux i Windows 2000.



Spis treści

O Autorach	21
Część I Definicja Windows 2000	23
Rozdział 1. Czym jest Windows 2000 Professional	25
Architektura Windows 2000	26
Skąd ten podział?.....	27
DOS oraz starsze aplikacje systemu Windows	28
Przenośność.....	32
Obsługa kilku procesorów	33
DirectX.....	33
Bezpieczeństwo w Windows 2000 Professional.....	34
Wielozadaniowość	34
Windows 3.x.....	35
Następcy Windows 3.x.....	35
Rodzina Windows 2000	37
Ulepszenia i zmiany w stosunku do poprzednich wersji Windows NT.....	38
Interfejs użytkownika	38
Interfejs użytkownika Windows 2000 Professional.....	39
Personalizowane menu	42
Panel sterowania.....	44
Sieć w Windows 2000.....	46
Odporność na uszkodzenia	48
Pojemność	48
Systemy plików	48
Nowe interesujące elementy Windows 2000 Professional.....	48
Rozdział 2. Przygotowanie do instalacji i analiza systemu.....	51
Inwentaryzacja	52
Zgodność sprzętowa	52
Dlaczego odrzucono starsze produkty?.....	52
Lista czynności kontrolnych	55
Możliwe utrudnienia.....	57
Proces inwentaryzacji.....	59
Wybór opcji konfiguracyjnych	60
Aplety Windows 2000.....	60
Opcje sieciowe	62
Usługa zdalnego dostępu.....	63

Udostępnianie równorzędne	63
Wirtualne sieci prywatne	64
Po instalacji	64
Wsparcie użytkowników	64
Szkolenie użytkowników	65
Metody szkolenia	67
Metoda sali wykładowej	67
Pokaz wideo	68
Aktualizacja istniejącego systemu operacyjnego lub czysta instalacja	68
Systemy plików	69
Windows 9x	69
Windows NT 4 i 3.51	71
Rozdział 3. Instalacja Windows 2000 Professional	73
Instalacja krok po kroku	74
Uruchomienie instalacji	74
Opcje instalacyjne	79
Instalacja w trybie tekstowym	80
Instalacja w trybie graficznym	85
Aktualizacja Windows 2000	88
Partycja startowa a partycja systemowa	88
Proces PnP	89
Konfiguracja sieci	90
Program Sysprep	90
Instalacje automatyczne	91
Remote Installation Services (RIS)	91
Opcje automatyzacji instalacji	92
Plik UNATTEND.TXT	92
Unikatowe pliki definicyjne UDF	94
Menedżer instalacji	94
Opcja Syspart	98
Zabiegi końcowe	98
Rozdział 4. Rozwiązywanie problemów instalacyjnych	99
Scenariusze idealnej instalacji	99
Identyczne stacje robocze	100
Cały sprzęt pochodzi od znanych producentów i nie jest starszy niż rok	101
Czysta instalacja zamiast aktualizacji	102
Ponowne uruchamianie instalacji z dodatkowymi opcjami	103
CHECKUPGRADEONLY	103
CMDCONS	104
DEBUG [POZIOM] [:NAZWA_PLIKU]	105
M:NAZWA_FOLDERU	105
MAKELOCALSOURCE	105
NOREBOOT	105
Poprawka czystej instalacji	106

W obliczu niepowodzenia instalacji.....	106
Sterowniki	107
ACPI (Advanced Configuration and Power Interface)	108
Płyta główna i BIOS.....	109
Przetaktowywane płyty główne.....	109
Wybór metody instalacji	110
Po przerwanej instalacji nowa instalacja zawiera kilka identycznych opcji startowych	110
Instalator albo system działa niestabilnie lub zawiesza się przy uruchamianiu, wyświetlając niebieski ekran	111
Awaria po udanej instalacji.....	113
Komputer nie startuje po pomyślnym teście POST (Power On Self Test)	114
Uruchomienie systemu Windows 2000 zawodzi po inicjalizacji programu ładującego.....	114
Błąd STOP 0x0000007B	115
Uruchamianie	116
Proces uruchamiania.....	116
Funkcja pliku BOOT.INI	117
Wywołanie startowe	117
Błędy startu.....	119
Konsola odzyskiwania systemu	122
Pomoc w pozostałych przypadkach	129
 Część II Dostrajanie systemu Windows 2000 Professional	 131
Rozdział 5. Dostrajanie wydajności Windows 2000	133
Podstawowe współczynniki	133
Prędkość dysku twardego.....	134
Prędkość procesora.....	135
Typ procesora	136
Pamięć fizyczna.....	137
Magistrala.....	138
Karta grafiki	139
Ogólne dostrajanie	140
Diagnozowanie „wąskich gardeł”	145
Pamięć	145
Problemy dyskowe	151
Procesor	153
Usuwanie problemów wydajnościowych.....	155
Kilka wydajnościowych znaków ostrzegawczych	156
Rozważania na temat aplikacji 16-bitowego systemu Windows	157
 Rozdział 6. Zaawansowane narzędzia panelu sterowania	 159
Nowe możliwości panelu sterowania.....	159
Korzystanie z panelu sterowania.....	161
Aplety Panelu sterowania.....	162
Łatwiejsza instalacja i konfiguracja	162
Łatwiejsze zarządzanie.....	173
Dostosowywanie menu Start.....	181

Rozdział 7. Dostrajanie zabezpieczeń Windows 2000	183
Przegląd zabezpieczeń Windows 2000	183
Użytkownicy i hasła	184
Wbudowane konta	184
Tworzenie nowych kont użytkowników	185
Dodatkowe właściwości kont	187
Grupy	189
Profile użytkowników	192
Inspekcja	195
Zasady	197
Bezpieczeństwo połączeń telefonicznych	198
Rejestr	200
Bezpieczeństwo systemu plików	201
Usuwanie uprawnień grupy Wszyscy (Everyone)	201
Usługa zdalnego dostępu (RAS)	203
Certyfikaty	204
Rozdział 8. Rejestr Windows 2000	207
Przeznaczenie rejestru	207
Narzędzia do edycji rejestru	208
REGEDT32	209
REGEDIT	209
Zasady Komputer lokalny	210
Bezpieczeństwo podczas edycji	212
Zmiany atomowe	212
Tryb tylko do odczytu	213
Zapisywanie i odtwarzanie kluczy	213
Elementy rejestru	215
Drzewa Windows 2000	217
HKEY_LOCAL_MACHINE	218
HKEY_CLASSES_ROOT	219
HKEY_CURRENT_USER	222
HKEY_USERS	224
HKEY_CURRENT_CONFIG	225
Korzystanie z programu REGEDIT	226
Korzystanie z programu REGEDT32	231
Dostosowywanie systemu za pomocą rejestru	235
Część III Praca z Windows 2000 Professional	237
Rozdział 9. System plików w Windows 2000	239
System plików FAT	240
Przegląd systemu NTFS (NT File System)	242
FAT a NTFS	244
Konwersja systemu FAT na NTFS	245
Zwłoczny i ostrożny zapis dyskowy	246

Zarządzanie dyskami.....	248
Tworzenie i przygotowywanie partycji.....	249
Dodawanie nowego dysku.....	249
Usuwanie partycji.....	249
Przeglądanie i monitorowanie.....	249
Zmiana litery napędu.....	252
Indeksowanie.....	253
Standardowe zadania zarządzania dyskami.....	254
Eksploreator Windows 2000.....	257
Skojarzenia plików.....	258
Manipulacja plikami.....	263
Widoki.....	266
Skróty.....	267
Zabezpieczenia.....	270
Udostępnianie i mapowanie plików.....	271
Udostępnianie plików.....	272
Mapowanie plików.....	274
Inne sztuczki menu podręcznego.....	276
Widoki i edycja.....	276
Drukowanie.....	278
Wysyłanie.....	278
Przydziały dyskowe.....	280
Rozdział 10. Instalacja aplikacji w Windows 2000.....	283
Systemy operacyjne i aplikacje.....	283
RegClean.....	284
Bezpieczne instalacje.....	286
Wprowadzanie zmian systemu Windows 2000.....	289
Dodawanie aplikacji.....	292
Aplikacje 32-bitowe.....	292
Dodawanie i usuwanie 16-bitowych aplikacji systemu Windows.....	293
Instalacja aplikacji systemu MS-DOS.....	295
Jakie zadania wykonują programy instalacyjne.....	296
CLSID i GUID.....	296
Wpisy rejestru.....	297
Rozwiązywanie problemów instalacji i deinstalacji programów.....	299
Rozdział 11. Interfejs wiersza poleceń.....	303
Co zawiera i czego nie zawiera CLI.....	303
Uruchamianie i konfiguracja wiersza poleceń.....	306
Uruchamianie wiersza poleceń.....	306
Konfiguracja skrótu lub programu.....	311
Posługiwanie się wierszem poleceń.....	313
Uzyskiwanie informacji o CLI.....	313
Ukośniki i myśluki.....	314
Potoki, przekierowanie i symbole warunkowe.....	316
Pliki wsadowe.....	318
CMD, Command i środowiska.....	319
Optymalizacja programu systemu DOS.....	319

Rozdział 12. Drukowanie i faksowanie w Windows 2000.....	323
Drukarki	323
Podstawy drukowania.....	323
Instalacja drukarki w Windows 2000.....	324
Drukowanie sieciowe	330
Sterowniki drukarek sieciowych	332
Porty drukarki.....	333
Drukowanie z poziomu aplikacji systemu DOS.....	333
Zarządzanie i rekonfiguracja drukarek.....	334
Zaawansowane opcje konfiguracji	335
Zabezpieczenia drukarek.....	336
Inspekcja drukarek	337
Faksowanie.....	338
Rozdział 13. Czcionki w Windows 2000	343
Czym jest czcionka?.....	343
Czcionki drukarkowe i ekranowe.....	346
Technologia Open	348
Zainstalowane czcionki	349
Użycie czcionek Open.....	353
Instalacja i usuwanie czcionek	354
Symbole dodatkowe i czcionki ozdobne.....	355
Klawiatura ekranowa.....	357
Edytor znaków prywatnych.....	358
Rozdział 14. Windows 2000 w komputerach przenośnych.....	361
Windows 2000 w komputerze przenośnym?	361
Instalacja systemu Windows 2000 w komputerze przenośnym.....	362
Instalacja.....	362
Dostrajanie wydajności	368
Konfiguracja profili sprzętowych	370
Praca zdalna	372
Obsługa trybu offline	372
Udostępnianie informacji w trybie offline	373
Powrót do biura	375
Zawartość zdalnej witryny	376
Zaawansowane zarządzanie energią	377
Część IV Windows 2000 wchodzi do Internetu	379
Rozdział 15. Łączność między komputerami — bezpośrednie połączenia kablowe.....	381
Porty	382
Kable modemu zerowego.....	384
Instalacja kabla modemu zerowego	386
Przygotowanie połączeń bezpośrednich	388
Komputery typu host	389
Komputery typu gość	391
Właściwości połączenia bezpośredniego	391

Logowanie.....	395
Uzyskiwanie dostępu do zasobów.....	396
Udostępnianie zasobów.....	397
Rozwiązywanie problemów połączeń bezpośrednich.....	398
Rozdział 16. Przygotowanie modemu	401
Instalacja modemu.....	402
Konfiguracja modemu.....	406
Zakładka Ogólne.....	406
Połączenie.....	407
Zakładka Zaawansowane.....	408
Zmiana preferencji domyślnych.....	409
Właściwości wybierania.....	409
ISDN i łącza alternatywne.....	414
Rozdział 17. Konfiguracja dostępu z użyciem TCP/IP	417
Warstwy protokołu.....	418
Warstwa aplikacji.....	418
Gniazda Windows.....	420
NetBIOS przez TCP/IP.....	425
Warstwa transportowa.....	428
Transmission Control Protocol (TCP).....	428
User Datagram Protocol (UDP).....	430
Warstwa internetowa.....	430
Internet Protocol (IP).....	431
Zabezpieczenie protokołu IP (IPSec).....	434
Internet Control Message Protocol (ICMP).....	438
Internet Group Management Protocol (IGMP).....	439
Warstwa dostępu do sieci.....	439
Adres internetowy, maska podsieci i brama domyślna.....	440
Podsieci.....	443
Rozwiązywanie problemów związanych z TCP/IP.....	447
Problemy kablowe.....	448
Karty sieciowe.....	448
ipconfig.....	449
ping.....	449
route.....	451
arp.....	453
tracert.....	453
netstat.....	454
nbtstat.....	454
nslookup.....	454
Monitor wydajności.....	455
Monitor sieci.....	455
Rozdział 18. Korzystanie z programu Microsoft Internet Explorer	457
Uruchamianie programu Internet Explorer 5.....	457
Interfejs użytkownika programu Internet Explorer 5.....	465
Pole listy Adres (Address).....	465
Pasek narzędzi.....	467

Menu Plik (File)	475
Menu Edycja (Edit)	478
Menu Widok (View)	478
Menu Narzędzia (Tools).....	478
Menu Ulubione (Favorites)	483
Łącza (Links).....	483
Sztuczki i wskazówki w programie Internet Explorer 5	484
Przemieszczanie na pasek Łącza (Links)	484
Menu podręczne	484
Drukowanie	485
Przenoszenie ulubionych adresów.....	486
Przyciski Wstecz (Back) i Dalej (Forward)	486
Przeciąganie pasków	486
Ekspresowe wyszukiwanie.....	486
Rozdział 19. Korzystanie z programu Microsoft Outlook Express	487
Interfejs programu Outlook Express	487
Zarządzanie folderami.....	488
Zarządzanie wiadomościami	489
Zarządzanie kontami	490
Konta grup dyskusyjnych.....	491
Opcje	492
Działanie programu Outlook Express	494
Wysyłanie i odbieranie wiadomości.....	495
Przeglądanie wiadomości pocztowych.....	495
Tworzenie nowej wiadomości.....	495
Odpowiadanie na wiadomość.....	496
Przekazywanie wiadomości	496
Korzystanie z grup dyskusyjnych	496
Pobieranie listy grup i subskrypcja	496
Czytanie wiadomości grup dyskusyjnych	497
Odpowiadanie na wiadomości grup dyskusyjnych i ich przekazywanie	499
Archiwizacja wiadomości	499
Książka adresowa.....	499
Dodawanie kontaktów	499
Grupy.....	500
Foldery.....	501
Reguły wiadomości.....	502
Blokowanie nadawców.....	502
Tożsamości.....	503
Rozdział 20. Praca zdalna za pomocą usługi zdalnego dostępu	505
Instalacja modemu	506
Tworzenie połączenia modemowego z Internetem.....	511
Tworzenie połączenia modemowego	512
Konfiguracja poczty elektronicznej.....	518
Inne możliwości usługi zdalnego dostępu.....	523
Inne rodzaje połączeń usługi RAS	523
Menedżer automatycznego połączenia dostępu zdalnego.....	525

Polecenie rasdial.....	526
Narzędzie do rozwiązywania problemów ze zdalnym dostępem.....	527
Dziennik modemu	527
Część V Sieć w systemie Windows 2000 Professional.....	529
Rozdział 21. Protokoły sieciowe w Windows 2000	531
Instalacja sieci	531
Kreator sprzętu	532
Instalacja karty sieciowej	534
Instalacja urządzenia podczerwieni	535
Połączenia sieciowe i telefoniczne	536
Identyfikacja sieciowa	537
Zakładka Identyfikacja sieciowa (Network Identification).....	539
Dodawanie składników sieciowych	541
Właściwości połączenia lokalnego	542
Opcje klienta sieci	544
Usługi	546
Instalacja i konfiguracja TCP/IP	546
Instalacja TCP/IP.....	547
Ogólne właściwości TCP/IP.....	547
DHCP	548
DNS	549
NetBIOS i WINS.....	551
Zabezpieczenia IP.....	553
Filtrowanie TCP/IP.....	554
Sprawdzanie łączności TCP/IP	555
NWLink.....	556
NetBEUI.....	557
Inne protokoły	558
Rozdział 22. Użytkownicy i grupy.....	559
Konta użytkowników	559
Administrator.....	560
Gość.....	560
Grupy.....	560
Grupy wbudowane	561
Aplet Użytkownicy i hasła	562
Użytkownicy i grupy lokalne	566
Tworzenie kont użytkowników i zarządzanie nimi.....	567
Tworzenie grup i zarządzanie nimi	571
Grupy systemowe	572
Uwagi o koncie Administrator	573
Profile	576
Ścieżki profili	576
Skrypty logowania.....	578
Foldery macierzyste	578

Zasady grupy	580
Zasady konta.....	582
Zasady lokalne.....	584
Prawa użytkowników	585
Szablony administracyjne.....	589
Przydziały dyskowe	594
Rozdział 23. Internetowe usługi informacyjne (IIS)	597
Składniki IIS.....	597
Instalacja IIS.....	600
Zarządzanie IIS	601
Zarządzanie domyślną witryną sieci Web.....	604
Zarządzanie domyślną witryną FTP.....	612
Konfiguracja i zarządzanie domyślnym serwerem wirtualnym SMTP.....	616
Rozdział 24. Przygotowanie intranetu	623
Pojęcie intranetu.....	623
Zalety intranetu.....	624
Przykładowe zastosowania intranetu.....	624
Intranet kontra publikacje papierowe	625
Planowanie intranetu	625
Administracja intranetem	626
Ustalenie odbiorców i zawartości intranetu	626
Ocena potrzeb sprzętowych i programowych	628
Projektowanie intranetu.....	630
Przygotowanie intranetu i dostęp do niego	631
Przygotowanie witryny sieci Web.....	631
Udzielanie użytkownikom dostępu do intranetu	632
Użycie gotowych dokumentów jako podstawy intranetu	632
Prosty przykład budowy intranetu z użyciem pakietu Office 2000	632
Umieszczanie plików w intranecie.....	634
Publikacja prezentacji programu PowerPoint	636
Publikacja arkuszy kalkulacyjnych programu Excel.....	637
Dostęp do baz danych poprzez intranet.....	640
Inne zastosowania intranetu	643
Oceny i ankiety.....	644
Witryna dyskusji.....	645
Witryna projektu.....	645
Witryna obsługi	645
Multimedia i konferencje	645
Obsługa intranetu	646
Administracja intranetem	646
Utrzymanie aktualności informacji	647
Odnosiniki i zalecana literatura	648
Office 2000.....	648
Intranet.....	648
Serwer sieci Web.....	649
Przeglądarka internetowa	649
Aplikacje baz danych w sieci Web.....	649
Zasady korzystania	649
Przykłady zastosowania intranetu	649

Rozdział 25. Współpraca systemów Linux i Windows 2000.....	651
Czym jest Linux?	652
Kluczowe różnice między Linuksem i Windows 2000 Professional.....	652
Dostępność kodu źródłowego	653
Linux nie ma właściciela.....	653
Linux opiera się na systemie UNIX	653
Microsoft posiada ustaloną bazę aplikacji.....	653
Kilka odmian jednego systemu operacyjnego.....	653
Z Linuksa wyciśniesz więcej.....	654
Instalacja Linuksa.....	654
Wymagania sprzętowe	655
Przygotowanie woluminu dla Linuksa.....	655
Problemy z uruchomieniem.....	655
Procedura instalacji	656
Powłoka Linuksa.....	661
Wybór powłoki.....	661
Podstawowe polecenia Linuksa.....	662
Procesy i potrzeba ich zabijania	664
System X Window	665
X Window systemem typu klient-serwer	666
Instalacja XFree86.....	666
Konfiguracja XFree86.....	666
Uruchamianie systemu X Window.....	669
Menedżer X Window	669
Pulpit w X Window.....	671
Pasek zadań	671
Aplikacje	671
Administracja systemem	672
Plik passwd.....	672
Dodawanie użytkowników	672
Dodawanie grupy	675
Usuwanie użytkowników	675
Zasoby internetowe dla systemu Linux.....	676
Zamykanie systemu Linux	676
Zamykanie systemu Linux z poziomu wiersza poleceń.....	677
Zamykanie Linuksa z poziomu X Window.....	677
Wymiana informacji między Linuksem i Windows 2000	678
FTP.....	678
SMB.....	678
 Część VI Administracja systemem Windows 2000 Professional.....	 679
Rozdział 26. Usuwanie skutków awarii	681
Obsługiwane technologie taśmowe.....	684
Interfejsy napędów taśmowych.....	684
Formaty taśm	685
Instalacja urządzenia taśmowego.....	685
Tworzenie kopii zapasowych plików, folderów i napędów	687

Program Kopia zapasowa.....	689
Kopia zapasowa rejestru systemu.....	689
Typy kopii zapasowych.....	690
Kopie zapasowe typu ojciec, syn i dziadek.....	691
Dziennik kopii zapasowej.....	692
Przywracanie kopii zapasowej.....	693
Opcje przywracania.....	693
Obsługa kopii zapasowych z poziomu wiersza poleceń.....	694
Planowanie automatycznych kopii zapasowych.....	694
Oprogramowanie innych firm.....	696
Awaryjny dysk naprawczy.....	696
Korzystanie z awaryjnego dysku naprawczego.....	697
Odtwarzanie rejestru systemu.....	698
Odtwarzanie sektora MBR.....	699
Rozdział 27. Podgląd zdarzeń.....	701
Podgląd zdarzeń.....	701
Podgląd zdarzeń spieszy z pomocą.....	704
Korzystanie z programu Podgląd zdarzeń.....	705
Jakie informacje są rejestrowane?.....	706
Dzienniki systemu i aplikacji.....	708
Dziennik zabezpieczeń.....	708
Przeglądanie dzienników lokalnych.....	712
Przeglądanie dzienników zdalnych.....	715
Zarządzanie dziennikami zdarzeń.....	716
Zapisywanie i odtwarzanie dzienników.....	717
Rozdział 28. Monitor wydajności.....	719
Monitor wydajności.....	719
Uruchamianie monitora wydajności.....	719
Zastosowania monitora wydajności.....	720
Liczniki, wystąpienia i obiekty.....	720
Wykres.....	721
Alerty.....	723
Jak ustawić alert.....	724
Monitorowanie zdalnych komputerów.....	726
Dzienniki śledzenia i liczników.....	726
Raport.....	728
Funkcje dodatkowe.....	729
Najważniejsze liczniki.....	729
Rozdział 29. Menedżer zadań.....	731
Uruchamianie Menedżera zadań.....	731
Aplikacje.....	732
Procesy.....	738
Wydajność.....	741

Rozdział 30. Diagnostyka systemu	745
Uruchamianie narzędzia Informacje o systemie	745
Korzystanie z narzędzia Informacje o systemie	747
Organizacja	748
Elementy zaawansowane.....	749
Podsumowanie systemu	749
Zasoby sprzętowe.....	749
Składniki	751
Środowisko oprogramowania.....	753
Aplikacje	755
Menedżer urządzeń	757
Zmiana sterowników i zasobów	758
Właściwości systemu	759
Rozdział 31. Usługi terminalowe i ich licencjonowanie	761
Charakterystyka usług terminalowych.....	761
Gruby i cienki klient.....	762
Zastosowania usług terminalowych	763
Zanim zaczniesz.....	763
Wymagania	763
Jakiego sprzętu potrzebuję?.....	764
Jakie aplikacje będą dostępne poprzez usługi terminalowe?	764
Ilu użytkowników będzie korzystać z usług terminalowych i jakie są ich wymagania?	764
Instalacja usług terminalowych.....	765
Instalacja klienta.....	767
Konfiguracja połączeń terminalowych	769
Zarządzanie użytkownikami i ich sesjami	771
Zarządzanie użytkownikami.....	771
Zarządzanie sesjami	772
Przeglądanie informacji o usługach terminalowych	773
Wysyłanie komunikatu do użytkownika usług terminalowych	773
Odłączanie użytkownika od serwera terminali	773
Zdalne sterowanie.....	774
Przeglądanie statystyk połączeń	774
Licencjonowanie usług terminalowych.....	775
Dodatki.....	777
Dodatek A Słowniczek terminów	779
Dodatek B Polecenia systemu Windows 2000.....	787
Uruchamianie interfejsu wiersza poleceń	787
Uzyskiwanie pomocy na temat poleceń.....	789
Polecenia, ich składnia i przykłady użycia	789
Polecenia plikowe i dyskowe	790
Append	790
Assoc	790
Attrib	791
CD lub Chdir	791

Chkdsk.....	792
Comp	792
Compact.....	793
Convert	794
Copy	795
Del i Erase	795
Dir.....	796
Diskcomp.....	796
Diskcopy.....	797
Expand.....	797
FC	798
Files	798
Findstr.....	799
Format	800
MD i Mkdir	800
Move.....	800
Print	800
RD i Rmdir	801
Ren i Rename	801
Xcopy	801
Polecenia Net	802
NBTStat.....	803
Net Accounts	803
Net Config	804
Net Continue, Pause, Start, Stop	805
Net File.....	805
Net Helpmsg.....	805
Net Print	806
Net Session	806
NetStat.....	807
Net Statistics.....	807
Net Time.....	808
Net Use	808
Polecenia związane z TCP/IP.....	809
Ftp.....	809
Ipconfig	810
Ping.....	811
Telnet.....	811
Polecenia sterujące środowiskiem wiersza poleceń.....	812
Exit	812
Path.....	812
Popd i Pushd.....	812
Prompt	813
Subst.....	813
Title	814
Pliki wsadowe	814
Call	815
Echo.....	815
For	815

Goto	815
If	816
Rem	816
Setlocal i Endlocal	816
Shift	817
Symbole stosowane w wierszu poleceń	817
<817	
>>	817
>818	
(potok)	818
818	
2>>	818
, (przecinek).....	819
^ (daszek).....	819
&	819
&&	819
()	819
Polecenie AT	820
Narzędzia usunięte z systemu	821
Przestarzałe polecenia plików wsadowych	823
Polecenia „zabytkowe”	823
Skorowidz	825

Rozdział 21.

Protokoły sieciowe w Windows 2000

W tym rozdziale:

- ◆ Instalacja sieci
- ◆ Połączenia sieciowe i telefoniczne
- ◆ Właściwości połączenia lokalnego
- ◆ Opcje *klienta* sieci
- ◆ Usługi
- ◆ Instalacja i konfiguracja TCP/IP
- ◆ NWLink
- ◆ NetBEUI
- ◆ Inne protokoły

Jednym z najważniejszych zadań administracyjnych w systemie Windows 2000 jest instalacja i konfiguracja składników sieciowych. Wszystkie projekty sieci obejmują unikatowe składniki sprzętowe i programowe, ponieważ to, co sprawdza się w jednym środowisku, niekoniecznie musi być idealne w innych. W bieżącym rozdziale omówione zostaną możliwości sieciowe systemu Windows 2000 Professional, począwszy od procedur instalacji karty sieciowej, poprzez szczegóły właściwości sieci, znacznie zmienione w porównaniu z poprzednimi wersjami systemu, aż po możliwości i instalację różnych protokołów sieciowych.

Instalacja sieci

Obsługa mechanizmu Plug and Play została zintegrowana z podstawowym kodem systemu Windows, a zarządza nią menedżer Plug and Play, należący do usług wykonawczych jądra systemu. Dzięki temu rozwiązaniu Windows 2000 Professional automatycznie rozpoznaje karty sieciowe zgodne z Plug and Play oraz konfiguruje ich ustawienia podczas instalacji. Jeżeli karta sieciowa nie obsługuje Plug and Play, lecz jej sterowniki są

zgodne z tym mechanizmem, Windows 2000 nie rozpozna automatycznie nowego urządzenia, ale poradzi sobie z obsługą jego zasobów. Dzięki temu konflikty przerwań sprzętowych zostaną znacznie zredukowane. Więcej informacji o mechanizmie Plug and Play przedstawiono w rozdziale 3., *Instalacja Windows 2000 Professional*.

W bieżącym rozdziale przedstawiono, krok po kroku, ręczną instalację karty sieciowej, jednak w większości przypadków Windows 2000 automatycznie rozpozna nowe urządzenie podczas instalacji i uruchamiania systemu lub w wyniku zdarzeń sprzętowych, zaistniałych w trakcie pracy systemu (dokowanie komputera przenośnego). Sytuacje wymagające ręcznej instalacji wynikają z użycia starszych urządzeń i sterowników lub kart sieciowych nieobsługujących mechanizmu Plug and Play — w połączeniu ze sterownikami zgodnymi z tym mechanizmem.

Ważne jest, by kupując karty sieciowe przeznaczone do pracy w Windows 2000, upewnić się, że wymieniono je na *liście zgodności sprzętowej* (HCL — Hardware Compatibility List), publikowanej kwartalnie przez Microsoft. Jeżeli kart nie ma na liście HCL, należy sprawdzić w witrynie ich producenta, czy istnieją dla nich sterowniki Plug and Play przeznaczone do pracy w Windows 2000. Pozwoli to zaoszczędzić sobie kłopotów podczas instalacji składników sieciowych.



Lista zgodności sprzętowej (HCL — Hardware Compatibility List) jest dostępna pod adresem www.microsoft.com/hcl.

Kolejnym dodatkiem w Windows 2000 są *podpisy cyfrowe*. Producent sterownika przeznaczonego do pracy w Windows 2000 może poddać swój produkt procesowi testów zgodności przeprowadzanemu przez Microsoft. W procesie tym sterowniki są poddawane *testowi WHQL* (Windows Hardware Quality Labs), potwierdzającemu spełnienie przez nich określonego poziomu standardów. Jeżeli testy zakończą się pomyślnie, dla sterownika tworzony jest plik katalogowy (*.cat), zawierający podpis cyfrowy Microsoftu. Podczas instalacji nowego urządzenia w systemie Windows 2000 plik *.inf (zawierający informacje o konfiguracji urządzenia w systemie operacyjnym) informuje system o istnieniu pliku katalogowego tego urządzenia. Informacje te są wykorzystywane przez system przy dalszym używaniu sterowników urządzenia. Powyższy proces gwarantuje, że pliki sterownika nie zostaną w przyszłości zastąpione lub zmodyfikowane przez instalację innego urządzenia lub programu.



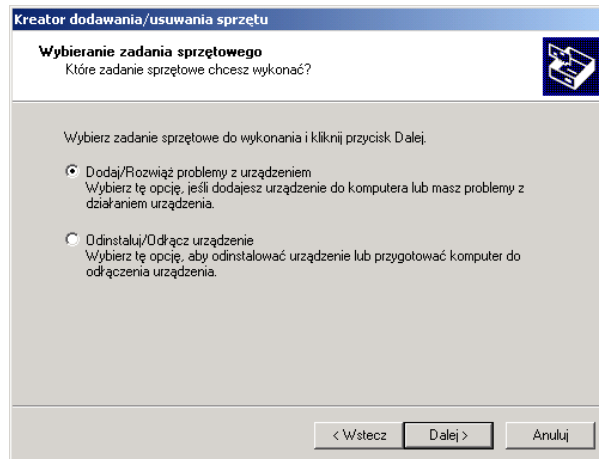
Gdy uczeń kończy szkołę, otrzymuje świadectwo podpisane przez jej władze. Podpis poświadczający, że uczeń uczęszczał na zajęcia i spełnił wymagania programu nauczania. Podpisy cyfrowe pełnią tę samą rolę, tyle że występują w postaci elektronicznej. Poświadczają one, że urządzenie spełnia pewien poziom jakości. Podpisy cyfrowe wykorzystuje się także w technologii szyfrowania (metoda kodowania danych przesyłanych pomiędzy komputerem wysyłającym i odbierającym) do wzajemnej weryfikacji tożsamości komputerów.

Kreator sprzętu

Windows 2000 korzysta przy instalacji nowego sprzętu z kreatora znanego z systemów Windows 95 i 98. Instalację nowego sprzętu może przeprowadzić tylko użytkownik posiadający uprawnienia administratorskie. *Kreator dodawania/usuwania sprzętu* (Add/Remove

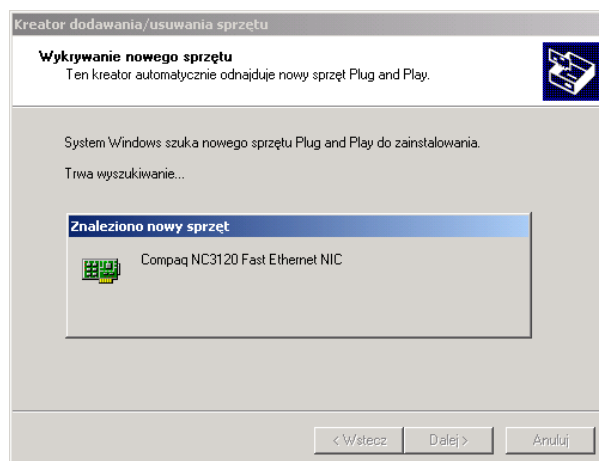
Hardware Wizard) dostępny poprzez aplet *Dodaj/Usuń sprzęt* (Add/Remove Hardware) w *Panelu sterowania* (Control Panel), służy dwóm celom — dodawaniu urządzeń lub rozwiązywaniu związanych z nimi problemów oraz ich deinstalacji lub wyłączeniu (rysunek 21.1). Windows 2000 skupia zatem w pojedynczym obszarze całe zarządzanie urządzeniami.

Rysunek 21.1.
Wybieranie zadania sprzętowego w Kreatorze dodawania/usuwania sprzętu (Add/Remove Hardware Wizard)



Windows 2000 rozpoznaje nowe urządzenia zgodne z mechanizmem Plug and Play podczas instalacji i uruchamiania systemu. Po poprawnym uruchomieniu system przeprowadza instalację urządzeń bez żadnych dodatkowych informacji ze strony instalatora. Kreator sieci wykonuje procedurę tego kroku zaraz po uruchomieniu. Rysunek 21.2 przedstawia okno kreatora sprzętu w trakcie instalacji nowej karty sieciowej. W kolejnym kroku kreator zatwierdza wszystkie nowo zainstalowane urządzenia. Windows 2000 konfiguruje także ustawienia protokołów zainstalowanej karty sieciowej, co bardziej szczegółowo przedstawiono w podrozdziałach dotyczących protokołów TCP/IP, NWLink i NetBEUI, w dalszej części bieżącego rozdziału. W większości środowisk sieciowych będą to jedyne wymagane kroki.

Rysunek 21.2.
Zadanie sprzętowe wykrywające nową kartę sieciową

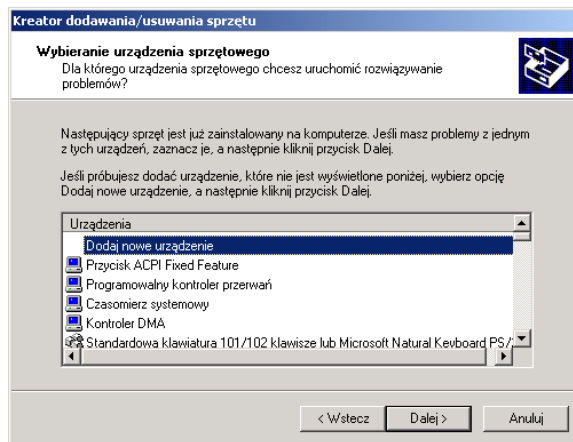


W przypadku kart sieciowych niezgodnych z mechanizmem Plug and Play (korzystających ze sterowników obsługujących Plug and Play lub z nich niekorzystające) *Kreator dodawania/usuwania sprzętu* (Add/Remove Hardware Wizard) przeprowadza proces ręcznej instalacji.

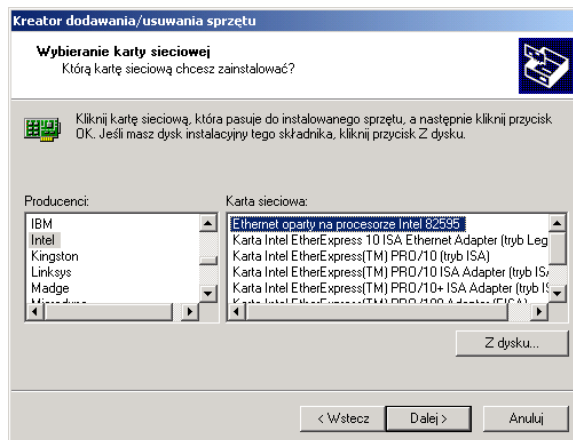
Instalacja karty sieciowej

Jeśli *Kreator dodawania/usuwania sprzętu* (Add/Remove Hardware Wizard) nie rozpozna żadnego nowego urządzenia, wyświetli urządzenia zainstalowane obecnie w systemie w celu rozwiązania problemów któregoś z nich. Jedną z opcji znajdujących się na liście urządzeń umożliwia dodanie nowego urządzenia (rysunek 21.3). Wybierz *Dodaj nowe urządzenie* (Add a new device) i kliknij *Dalej* (Next). Zostaniesz poproszony o potwierdzenie wykrywania nowych urządzeń. Wybierz *Nie* (No) i kliknij *Dalej* (Next). System przygotuje listę wszystkich rozpoznanych kart sieciowych, co zazwyczaj zajmuje dłuższą chwilę. Kolejne okno kreatora prezentuje listę wszystkich kart sieciowych i ich producentów (rysunek 21.4). Wybierz z listy właściwą kartę i kliknij *Dalej* (Next). Kreator zainstaluje teraz kartę w systemie.

Rysunek 21.3.
Kreator dodawania/usuwania sprzętu (Add/Remove Hardware Wizard) prezentujący listę zainstalowanych urządzeń wraz z opcją dodania nowego urządzenia



Rysunek 21.4.
Kreator dodawania/usuwania sprzętu (Add/Remove Hardware Wizard) prezentujący listę kart sieciowych i ich producentów. Opcja 'Z dysku' (Have Disk) przydaje się przy instalacji najnowszych sterowników dostarczonych na dyskietce lub płycie CD-ROM





Jedną z opcji powyższego punktu procesu instalacji oferuje przycisk *Z dysku* (Have Disk), widoczny na rysunku 21.4. Jeśli to tylko możliwe, korzystaj z tej opcji przy instalacji najnowszych wersji sterowników karty sieciowej. Sklepy komputerowe często sprzedają karty sieciowe bez sterowników, pozostawiając rozpoznanie i instalację karty systemowi Windows 2000. Mimo to, kupując kartę sieciową, poproś o aktualne jej sterowniki. Producenci kart zazwyczaj publikują informacje o sterownikach w swoich witrynach internetowych.

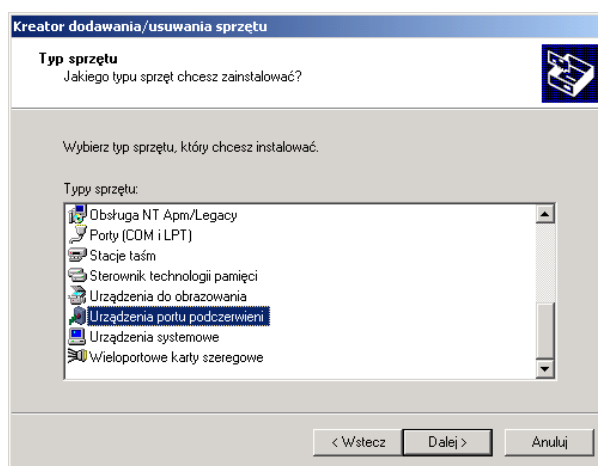
Korzystając ze sterowników dostępnych na liście lub dostarczonych za pomocą opcji *Z dysku* (Have Disk), *Kreator dodawania/usuwania sprzętu* (Add/Remove Hardware Wizard) zainstaluje teraz i skonfiguruje nową kartę sieciową. Proces ten zazwyczaj nie wymaga zastosowania instalacyjnej płyty Windows 2000 Professional ani ponownego uruchomienia systemu.

Instalacja urządzenia podczerwieni

Cenną opcją komunikacji sieciowej jest wykorzystanie technologii podczerwieni. Chociaż podczerwień w sieciach komputerowych rozpatruje się jedynie w szczególnych sytuacjach — ze względu na koszt sprzętu — technologia ta stała się bardziej popularna wówczas, gdy mamy do czynienia z łączeniem dwóch urządzeń. Komunikacja z zastosowaniem podczerwieni nie zastąpi tradycyjnego okablowania, jednak znajdzie zastosowanie w miejscach, w których nie stosuje się kabli ze względów estetycznych. Przykładem są tu zabytkowe budynki, w których instalacja okablowania jest niedopuszczalna.

Podobnie jak w przypadku kart sieciowych, do instalacji urządzenia podczerwieni służy *Kreator dodawania/usuwania sprzętu* (Add/Remove Hardware Wizard). Poszczególne kroki są podobne, z tą różnicą, że zamiast karty sieciowej wybiera się urządzenie podczerwieni. Rysunek 21.5 przedstawia okno *Kreatora dodawania/usuwania sprzętu* (Add/Remove Hardware Wizard) podczas wyboru typu urządzenia.

Rysunek 21.5.
Kreator dodawania/usuwania sprzętu (Add/Remove Hardware Wizard) podczas wyboru instalowanego urządzenia



Kreator dodawania/usuwania sprzętu (Add/Remove Hardware Wizard) stosuje domyślne ustawienia, aby automatycznie skonfigurować urządzenie podczerwieni.

Uwaga

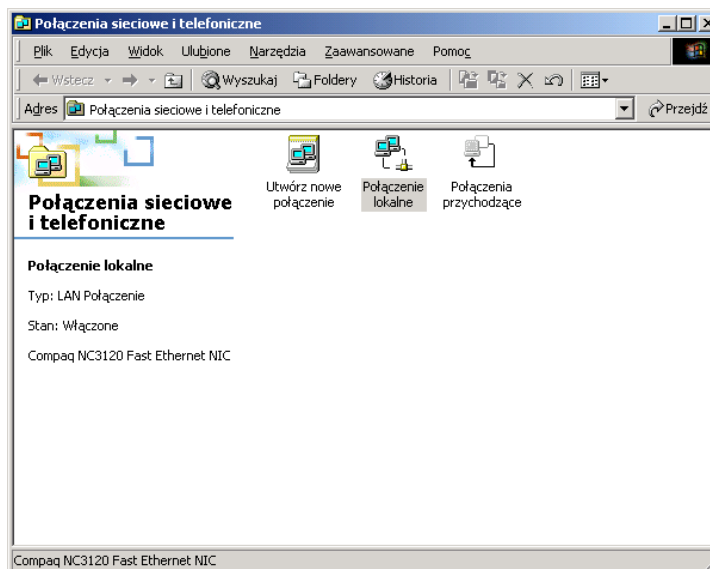
Urządzenia podczerwieni wykorzystują do komunikacji protokół *IrDA* (Infrared Data Association). Jeśli komputer posiada wbudowany sprzęt IrDA, Windows 2000 automatycznie rozpozna go i zainstaluje z ustawieniami domyślnymi. Żadne inne ustawienia nie wymagają konfiguracji. Windows 2000 zawiera dodatkowe programy, takie jak *Łącze bezprzewodowe* (Wireless Link) do przesyłu plików i możliwość drukowania oraz przesyłu obrazów za pośrednictwem podczerwieni. Jeśli komputer nie posiada sprzętu IrDA, do portu COM można podłączyć nadajnik-odbiorcę IrDA i dzięki niemu zainstalować urządzenie IrDA.

Połączenia sieciowe i telefoniczne

Windows 2000 posiada pojedynczy centralny punkt, skupiający wszystkie połączenia sieciowe. W ten sposób wszystkie połączenia — za pośrednictwem modemu, karty sieciowej lub urządzenia podczerwieni — są zarządzane z jednego miejsca, co ułatwia odświadczenie ustawień konfiguracyjnych. Aplet *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections) w *Panelu sterowania* (Control Panel) prezentuje różne metody komunikacji komputera z innymi urządzeniami. Informacje o połączeniach znajdują się w lewej części okna apletu. Każda karta sieciowa posiada własny obiekt połączenia, widoczny w oknie tego apletu. Rysunek 21.6 przedstawia typowe okno *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections).

Rysunek 21.6.

Okno
Połączenia sieciowe i telefoniczne
(*Network and Dial-up Connections*)

**Uwaga**

Ustawienia sieci są dostępne z poziomu Panelu sterowania (Control Panel) lub też po kliknięciu prawym przyciskiem myszy ikony *Moje miejsca sieciowe* (My Network Places), umieszczonej na pulpicie, i wybraniu pozycji *Właściwości* (Properties).

Okno *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections) oferuje wiele opcji. Jedną z nich jest utworzenie nowego połączenia w oparciu o wcześniej zainstalowane urządzenie. Podobnie jak w przypadku kart sieciowych, czynność tej opcji jest automatycznie wykonywana przez system operacyjny. Aby utworzyć nowe połączenie

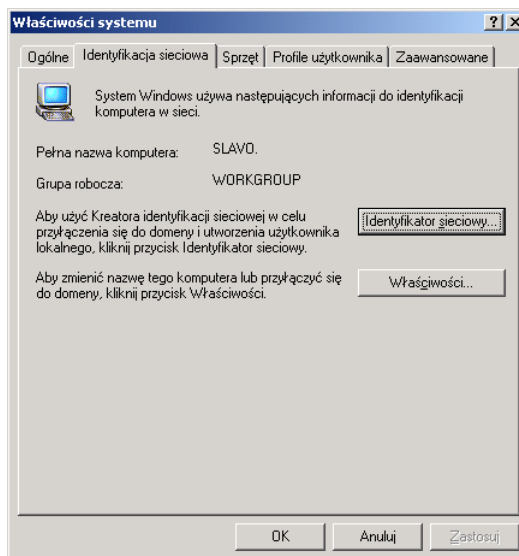
za pośrednictwem modemu, portu komunikacyjnego, sieci ISDN lub *wirtualnej sieci prywatnej* (VPN — Virtual Private Network; metoda łączenia komputerów poprzez Internet), należy dwukrotnie kliknąć ikonę *Utwórz nowe połączenie* (Make New Connection), co spowoduje *uruchomienie Kreatora połączeń sieciowych* (Network Connection Wizard), przeprowadzającego proces łączenia. Inną opcją dostępną w oknie *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections) jest sprawdzenie właściwości połączenia sieciowego. Okno to służy również do identyfikacji komputera w sieci oraz dodawania składników sieciowych. Opcje te opisano bardziej szczegółowo w kolejnych podrozdziałach.

Identyfikacja sieciowa

Kliknięcie opcji *Identyfikacja sieciowa* (Network Identification) w lewym panelu okna *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections) powoduje wyświetlenie zakładki *Identyfikacja sieciowa* (Network Identification) okna dialogowego *Właściwości systemu* (System Properties), przedstawionej na rysunku 21.7. Nie należy zaznaczać żadnego połączenia, ponieważ wówczas w lewym panelu okna *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections) wyświetlone zostaną informacje na jego temat. Okno dialogowe *Właściwości systemu* (System Properties) jest również dostępne po kliknięciu prawym przyciskiem myszy ikony *Mój komputer* (My Computer), umieszczonej na pulpicie, lub z poziomu Panelu sterowania (Control Panel). Zakładka *Identyfikacja sieciowa* (Network Identification) okna *Właściwości systemu* (System Properties) przedstawia pełną nazwę komputera (wprowadzaną ręcznie lub generowaną losowo podczas instalacji systemu) oraz nazwę grupy roboczej lub domeny, do której należy komputer. Nazwa komputera może się składać maksymalnie z 63 znaków, o ile zainstalowano TCP/IP lub w przeciwnym razie z 15 znaków. Może ona zawierać znaki A – Z, a – z, 0 – 9 oraz łączniki. Można użyć również innych znaków, jednak nie zostaną one rozpoznane przez wszystkie komputery w sieci. Zmiana pełnej nazwy komputera albo informacji o grupie roboczej lub domenie odbywa się przy użyciu *Kreatora identyfikacji sieciowej* (Network Identification Wizard).

Rysunek 21.7.

Zakładka
*Identyfikacja
sieciowa* (Network
Identification)
okna dialogowego
Właściwości systemu
(System Properties)



Omówienie tego kreatora wymaga wcześniejszego przedstawienia grup roboczych i domen w środowisku sieci systemu Windows 2000.

Grupy robocze

Windows 2000 Professional może pracować w grupie roboczej lub w domenie, logicznie pełniąc tę samą rolę. Grupy robocze i domeny operują w środowisku sieciowym, w którym komputery komunikują się ze sobą. Obydwa te mechanizmy posiadają pewien rodzaj zabezpieczeń, chociaż informacje o logowaniu mogą zostać wyłączone w przypadku grup roboczych (więcej na temat logowania i użytkowników znajdziesz w rozdziale 22., *Użytkownicy i grupy*). Jeśli jednak chodzi o zabezpieczenia i uwierzytelnianie użytkowników, administracja siecią opartą o grupy robocze różni się dalece od administracji siecią z domenami.

Grupa robocza to zazwyczaj mała grupa komputerów wykonujących podobne zadania lub w jakimś celu związanych ze sobą. Komputery te są zazwyczaj położone blisko siebie, choć nie jest to konieczne. Istotna różnica pomiędzy grupami roboczymi i domenami wynika z zarządzania kontami użytkowników i grup. W środowisku grup roboczych każdy komputer przechowuje własne konta użytkowników i grup. Jeśli na przykład w jednym z komputerów należących do grupy roboczej utworzono konto dla Janice, będzie ona mogła logować się tylko do tego jednego komputera, ponieważ wyłącznie w nim znajduje się jej konto. Nie będzie mogła też korzystać z zasobów innych komputerów, na przykład plików i drukarek, ponieważ nie będzie *uwierzytelniana* w tych komputerach. Każdy komputer w takim środowisku musi być zarządzany oddzielnie i będzie on uwierzytelniał tylko własnych użytkowników.

Ze względu na wysoką złożoność utrzymania związaną z administracją grupy robocze są przydatne w niewielkich środowiskach, składających się zazwyczaj z nie więcej niż dziesięciu komputerów, lub w rzadko spotykanych stałych środowiskach. Bardziej złożonym sieciom środowisko domenowe oferuje o wiele prostsze metody zarządzania uwierzytelnianiem i bezpieczeństwem.

Domeny

Domeny stosuje się w przypadku dużych środowisk sieciowych. W rzeczywistości środowisko takie może obejmować wszystkie komputery w jakimś celu połączone ze sobą logicznie za pośrednictwem sieci, choć fizycznie umieszczone gdziekolwiek na świecie. W domenie, podobnie jak w przypadku grup roboczych, komputery nie muszą być fizycznie umieszczone blisko siebie — i zazwyczaj nie są. W systemie Windows 2000 teoretycznie rozmiar osiągnięty przez domenę nie jest ograniczony.

Struktura domenowa oznacza, że wszystkie konta użytkowników i grup są zarządzane centralnie, nie zaś lokalnie w każdym komputerze. Gdyby konto Janice utworzono w środowisku domenowym, byłaby ona w stanie logować się do sieci z dowolnego komputera w domenie. Ponadto, po uwierzytelnieniu, mogłaby ona korzystać z dowolnych zasobów domeny — pod warunkiem posiadania właściwych uprawnień.

W systemie Windows 2000 znacznie rozszerzono strukturę domenową, wprowadzając usługi *Active Directory* (ADS — Active Directory Services). W strukturze ADS konta użytkowników, grup i komputerów są grupowane w jednostkach organizacyjnych, co ułatwia administrację. Struktura domenowa dzieli się także na lasy i drzewa, co również ułatwia administrację.

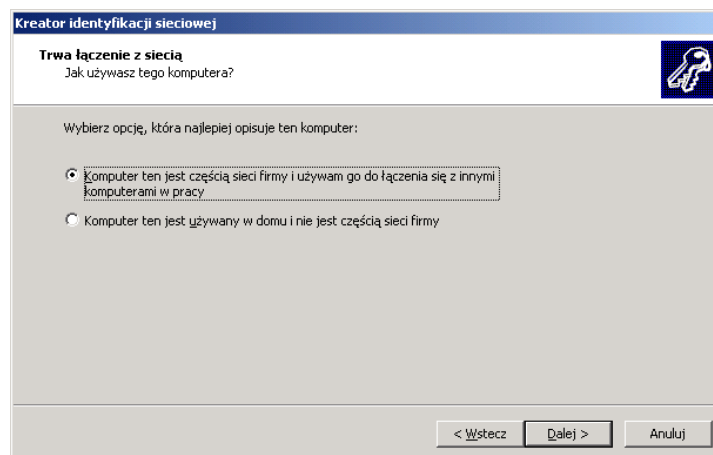
Użytkownicy Windows 2000 Professional mogą logować się do kontrolera domeny. Kontroler domeny pełni dodatkową rolę, przechowując kopie wszystkich kont użytkowników logujących się do domeny. W ten sposób podczas logowania Janice do domeny podane przez nią informacje logowania są przekazywane do kontrolera domeny. Kontroler domeny sprawdza istnienie konta użytkownika Janice w bazie danych katalogu ADS oraz poprawność podanego hasła, a następnie zezwala na zalogowanie się do domeny. W przeciwieństwie do Windows NT, w Windows 2000 żaden komputer nie pełni roli podstawowego kontrolera domeny. Wszystkie kontrolery domeny w Windows 2000 przechowują modyfikowalne kopie bazy danych katalogu. Tylko serwery Windows 2000 mogą działać jako kontrolery domeny.

Zakładka Identyfikacja sieciowa (Network Identification)

Zakładka *Identyfikacja sieciowa* (Network Identification) oferuje dwie możliwości zmiany właściwości komputera oraz grupy roboczej lub domeny. Kliknięcie przycisku *Identyfikator sieciowy* (Network ID) uruchamia *Kreator identyfikacji sieciowej* (Network Identification Wizard), w trakcie działania którego użytkownik jest proszony o określenie charakteru pracy komputera. Drugą opcję udostępnia przycisk *Właściwości* (Properties), którego kliknięcie powoduje bezpośrednie wyświetlenie informacji o komputerze i grupie roboczej lub domenie. W tym podrozdziale najpierw zostanie przedstawiony *Kreator identyfikacji sieciowej* (Network Identification Wizard), a następnie właściwości zaawansowane.

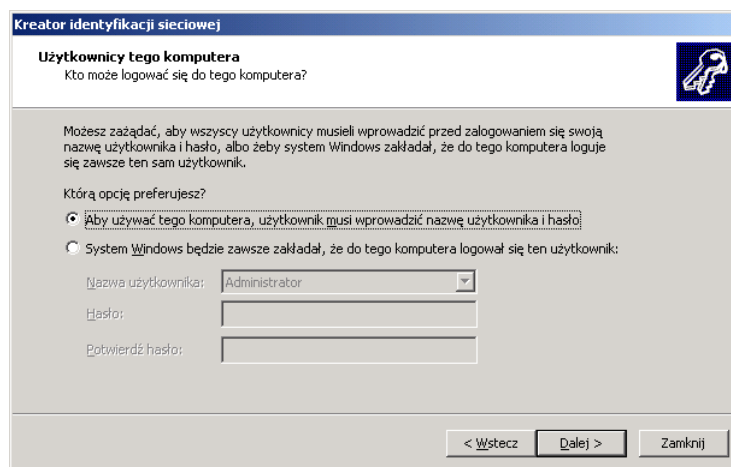
Kreator identyfikacji sieciowej (Network Identification Wizard) ma za zadanie określić funkcję komputera. Na początku użytkownik jest pytany o to, czy jego komputer jest częścią środowiska sieci firmy, czy też służy zastosowaniom domowym (rysunek 21.8).

Rysunek 21.8.
Kreator identyfikacji sieciowej (Network Identification Wizard)



Wybranie opcji komputera domowego powoduje umieszczenie go w grupie roboczej, a następnie użytkownik określa, kto może się do niego logować. Jedną z opcji zakłada, że każdy użytkownik korzysta z oddzielnego konta. Kont użytkowników nie można utworzyć korzystając z *Kreatora identyfikacji sieciowej* (Network Identification Wizard), do tego celu służy aplet *Użytkownicy i hasła* (Users and Passwords) w *Panelu sterowania* (Control Panel). Stosowanie oddzielnych kont użytkowników zapewnia bezpieczeństwo komputera, ponieważ każda osoba musi się zalogować, a baza danych zabezpieczeń komputera musi ją uwierzytelnić. Metoda ta przypomina system operacyjny Windows NT Workstation. Rysunek 21.9 przedstawia etap działania *Kreatora identyfikacji sieciowej* (Network Identification Wizard), w którym określa się sposób logowania do komputera.

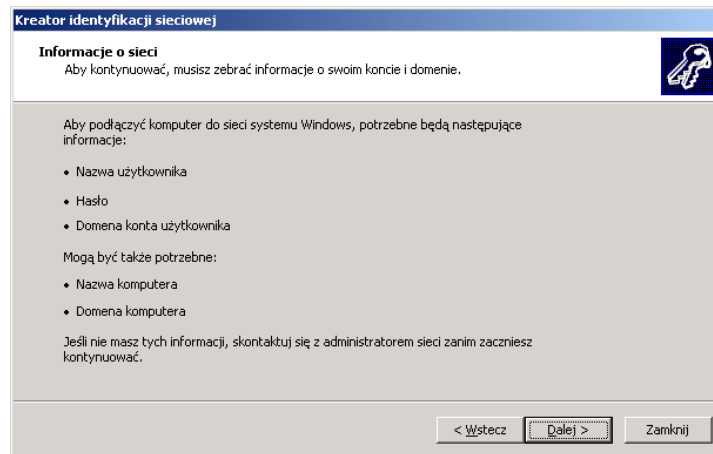
Rysunek 21.9.
Kreator identyfikacji sieciowej (Network Identification Wizard) z widoczną opcją określania sposobu logowania do komputera



Druga opcja tego kroku kreatora przypomina schemat logowania do systemu Windows 95 lub Windows 98, w którym wszyscy użytkownicy korzystają z tego samego konta. Proces logowania można całkowicie wyłączyć w aplecie *Użytkownicy i hasła* (Users and Passwords) w *Panelu sterowania* (Control Panel). Po wybraniu jednej z powyższych opcji komputer musi być ponownie uruchomiony, aby zainicjalizować nowe ustawienia sieciowe.

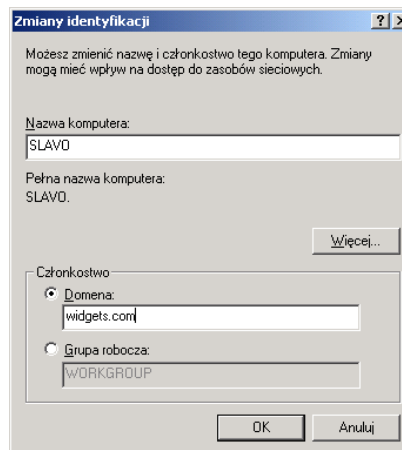
Jeśli określono, że komputer służy celom biznesowym, użytkownik zostanie poproszony o potwierdzenie jego uczestnictwa w domenie lub w grupie roboczej. Jeżeli komputer nie należy do domeny, użytkownik zostanie poproszony o podanie nazwy grupy roboczej, po czym *Kreator identyfikacji sieciowej* (Network Identification Wizard) zakończy działanie. Jeśli komputer należy do domeny, kreator poprosi o podanie informacji niezbędnych do połączenia się z nią (rysunek 21.10). Do przyłączenia komputera do domeny wymagane jest konto i hasło użytkownika posiadającego uprawnienia administratora. Potrzebna będzie również nazwa domeny i być może nazwa komputera. Po podaniu tych informacji kreator skontaktuje się z kontrolerem danej domeny, aby określić, czy użytkownik posiada uprawnienia do utworzenia konta komputera. Jeżeli podane przez użytkownika informacje są prawidłowe i poprawnie uwierzytelnione, kreator kończy działanie. Zanim wprowadzone zmiany zaczną obowiązywać, wymagane jest ponowne uruchomienie systemu.

Rysunek 21.10.
Kreator identyfikacji sieciowej (Network Identification Wizard) w trakcie procesu przyłączania do domeny



Opcja *Właściwości* (Properties) zakłada, że przeznaczenie komputera się nie zmieniło. Służy ona do zmiany nazwy komputera, grupy roboczej lub domeny (rysunek 21.11). Niezbędne procedury uwierzytelniania stosowane w kreatorze identyfikacji sieciowej dotyczą również wszelkich zmian w oknie *Zmiany identyfikacji* (Identification Changes).

Rysunek 21.11.
Okno Zmiany identyfikacji (Identification Changes)



Kliknięcie przycisku *Więcej* (More) w oknie *Zmiany identyfikacji* (Identification Changes) powoduje wyświetlenie kolejnego okna służącego do wprowadzenia informacji związanych z systemem DNS. *Serwery nazw* (DNS — Domain Name System) w środowisku domenowym mogą być zintegrowane z kontami komputerów. System DNS szerzej omówiono w podrozdziale *Instalacja i konfiguracja TCP/IP*, w dalszej części bieżącego rozdziału.

Dodawanie składników sieciowych

Kolejną opcją w oknie *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections) jest dodawanie składników sieciowych. Składniki te nie są wymagane przy typowym korzystaniu z sieci i powinno się je instalować jedynie w określonych celach. Składniki dodatkowe dzielą się na następujące cztery kategorie:

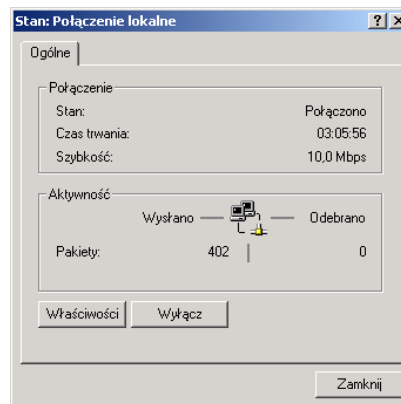
- ♦ *Narzędzia zarządzania i monitorowania* (Management and Monitoring Tools), protokół Simple Management Network Protocol — *SNMP* jest protokołem używanym do zarządzania urządzeniami w sieci. W Windows 2000 Professional opcja ta instaluje *agenta* raportującego menedżerowi SNMP szczegóły na temat sieci. Przykładem takiej przekazywanej informacji byłby adres IP karty sieciowej.
- ♦ *Usługi sieciowe* (Network Services), *Odbiornik RIP* (RIP Listener)
— Windows 2000 Server korzysta z dwóch protokołów wyboru trasy: RIP i OSPF. Komputery i routery przechowują tabele tras zawierające informacje sieciowe wykorzystywane do kierowania danych do innych komputerów i sieci. Obydwa te protokoły wyboru trasy umożliwiają routerom współdzielenie informacji zawartych w tabelach tras. RIP (Routing Information Protocol) jest protokołem typu *wektor odległości* (distance vector), używanym do dynamicznego wyboru trasy w małych i średnich sieciach. *OSPF* (Open Shortest Path First) jest protokołem wyboru trasy typu *stan łącza* (link state), używanym w sieciach o dużych rozmiarach. Komputer z systemem Windows 2000 Professional może nasłuchiwać aktualizacji tras korzystając z protokołu RIP w wersji 1, o ile zainstalowano tę opcję.
- ♦ *Usługi sieciowe* (Network Services), *usługi Simple TCP/IP* (Simple TCP/IP Services) — opcja ta dostarcza pięć dodatkowych usług TCP/IP: *Generator znaków* (Character Generator), *Daytime*, *Discard*, *Echo* i *Cytat dnia* (Quote of the Day). Usługi te nie należą do standardowego zestawu protokołów TCP/IP i określa się je jako *obieralne*, czyli instalowane samodzielnie przez użytkownika.
- ♦ *Inne usługi plików i drukowania w sieci* (Other Network File and Print Services), *usługi drukowania dla systemu Unix* (Print services for Unix)
— opcja ta umożliwia *klientom* systemu Unix wysyłanie poleceń LPR i LPQ do komputera z systemem Windows 2000 Professional.

Właściwości połączenia lokalnego

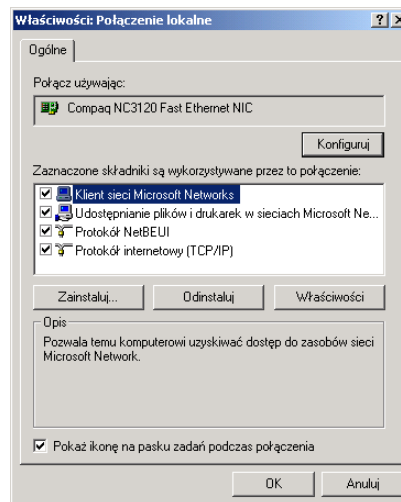
Okno *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections) zawiera obiekty właściwości połączeń każdej zainstalowanej karty sieciowej. Nazwy tych obiektów można łatwo zmienić dla łatwiejszej ich identyfikacji, a także dowolnie je podłączać i odłączać. Okno stanu dostarcza informacji na temat połączenia. Są to: czas trwania, prędkość oraz liczba wysłanych i odebranych pakietów w danym połączeniu (rysunek 21.12). We właściwościach połączenia lokalnego można zaznaczyć opcję wyświetlania ikony połączenia w prawym dolnym rogu paska narzędzi (rysunek 21.13). Nową, wygodną funkcją każdego okna dialogowego właściwości jest pomocny opis każdego wybranego elementu. Chociaż niektóre opisy składają się tylko z jednego zdania, streszczają jednak znaczenie funkcji bez potrzeby otwierania okna pomocy. Aby skonfigurować *Połączenie lokalne* (Local Area Connection), należy kliknąć jego obiekt prawym przyciskiem myszy i wybrać pozycję *Właściwości* (Properties).

Okno dialogowe *Właściwości: Połączenie lokalne* (Local Area Connection Properties) przedstawia wszystkie informacje o karcie sieciowej, *klientach*, usługach i protokołach połączenia lokalnego. Dodanie jednego składnika połączenia lokalnego, z wyjątkiem informacji o karcie sieciowej, spowoduje jego dodanie do wszystkich połączeń lokalnych.

Rysunek 21.12.
Okno stanu
połączenia lokalnego



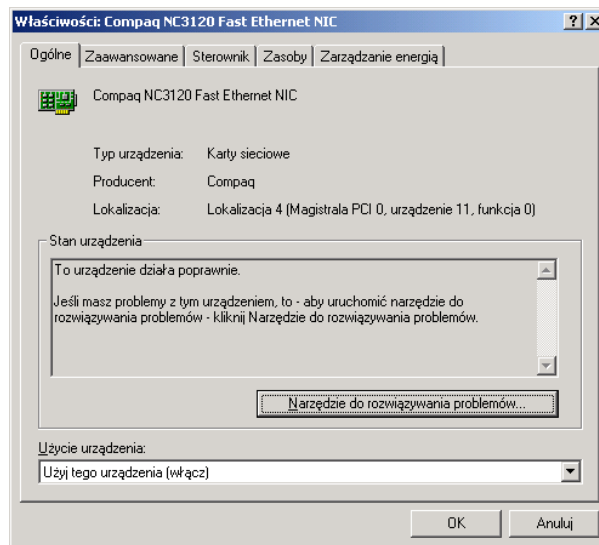
Rysunek 21.13.
Okno dialogowe
Właściwości:
Połączenie lokalne
(Local Area
Connection
Properties)



W oknie dialogowym *Właściwości: Połączenie lokalne* (Local Area Connection Properties) dostępna jest opcja konfiguracji kart sieciowych. Rysunek 21.14 przedstawia okno właściwości sieciowych zawierające następujące cztery zakładki:

- ♦ *Ogólne* (General) — zakładka ta przedstawia typ urządzenia, jego producenta i lokalizację. Jeśli urządzenie napotka jakiegokolwiek trudności, w polu jego stanu wyświetlone zostaną stosowne informacje. Zakładka udostępnia narzędzie do rozwiązywania problemów, którego uruchomienie powoduje wyświetlenie ekranu pomocy systemu Windows 2000 zawierającego w formie kreatora określone szczegóły dotyczące urządzenia. Zakładka *Ogólne* (General) zawiera też opcję włączania lub wyłączania karty sieciowej.
- ♦ *Zaawansowane* (Advanced) — zakładka ta zawiera ustawienia charakterystyczne dla urządzenia, takie jak tryb duplexowy, rodzaj medium i adres sieciowy. Ustawienia te nie powinny być zmieniane, chyba że istnieją ku temu powody. W zależności od zainstalowanego urządzenia, zakładka ta może się pojawić.

Rysunek 21.14.
Okno dialogowe
konfiguracji sieci



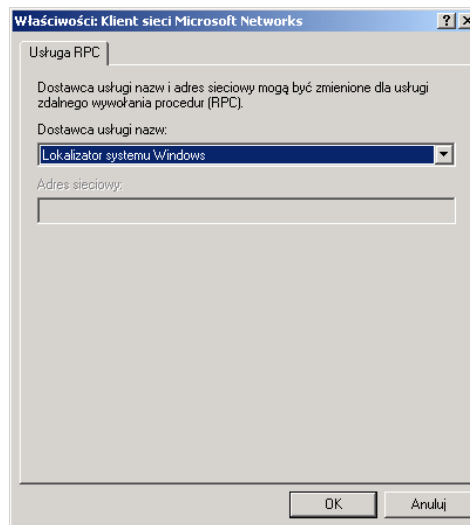
- ♦ *Sterownik* (Driver) — zakładka przedstawia takie informacje o sterowniku jak jego data, wersja i podpis cyfrowy. Na ich podstawie ustala się potrzebę aktualizacji sterowników. Kliknięcie przycisku *Szczegóły sterownika* (Driver Details) powoduje wyświetlenie szczegółów plików sterownika. Zakładka *Sterownik* (Driver) umożliwia także przeprowadzanie aktualizacji sterownika.
- ♦ *Zasoby* (Resources) — podobnie jak w Windows 95 i Windows 98, zakładka ta zawiera ustawienia takich zasobów jak zakresy wejścia-wyjścia i żądania przerwań IRQ. Ustawienia te można modyfikować ręcznie, o ile urządzenie jest zgodne z mechanizmem Plug and Play, w przeciwnym razie konfigurację przeprowadza się za pomocą programu dostarczonego przez producenta.

Opcje klienta sieci

Klient umożliwia komputerowi komunikację z innymi komputerami i ich zasobami w sieci lokalnej; reprezentuje go ikona komputera wyświetlana w oknie dialogowym właściwości połączenia. W ramach połączeń lokalnych domyślnie instalowany jest *Klient sieci Microsoft Networks* (Client for Microsoft Networks). Opcja instalacji w oknie właściwości połączenia lokalnego umożliwia dodanie *Usługi klientów dla systemu NetWare* (Client Service for NetWare). Ta usługa jest niezbędna do uzyskania dostępu do zasobów serwera NetWare i zastępuje usługi *klienta* systemu NetWare, obecne w Windows NT Workstation.

Przedstawione na rysunku 21.15 okno właściwości *klienta* sieci Microsoft Networks umożliwia wybór nazwy dostawcy usługi zdalnego wywołania procedur RPC (Remote Procedure Call). Aplikacje rozproszone wykorzystują mechanizm zdalnego wywołania procedur do przekazywania wiadomości pomiędzy komputerami w sieci. Zasadniczo wywołują one wykonanie funkcji w zdalnym komputerze. Domyślnie powinien być wybrany

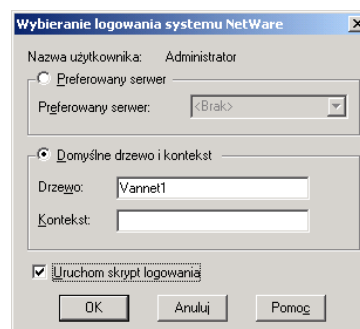
Rysunek 21.15.
Okno dialogowe
Właściwości:
Klient sieci Microsoft
Networks (Client for
Microsoft Networks
Properties)



Lokalizator systemu Windows (Windows Locator), poza pewnymi okolicznościami, w których określa się urządzenie pośredniczące w przekazywaniu wiadomości, stosując na przykład *Usługę katalogu komórkowego DCE* (DCE Cell Directory Service).

Interesujące jest, że po zainstalowaniu *klienta* sieci NetWare jego właściwości konfiguruje się korzystając z apletu CSNW w *Panelu sterowania* (Control Panel), a nie w oknie *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections). Opcje podłączania do serwera NetWare, dostępne w aplecie CSNW, wyświetlane są także podczas instalacji *klienta*; widać je w oknie przedstawionym na rysunku 21.16. W oknie tym określa się preferowany serwer NetWare 3.x lub wpisuje domyślne drzewo i kontekst — w przypadku serwerów NetWare 4.x. Dostępna jest także opcja przetwarzania skryptu logowania, zawierającego polecenia wykonywane podczas logowania się użytkownika. System Windows również posiada tę możliwość, uaktywnianą w aplecie *Użytkownicy i hasła* (Users and Passwords).

Rysunek 21.16.
Okno dialogowe
Wybieranie logowania
systemu NetWare
(Select NetWare
Logon)



Instalacja *klienta* w jednym połączeniu lokalnym pociąga za sobą jego instalację w pozostałych połączeniach lokalnych. Składniki połączenia widoczne w oknie jego właściwości posiadają jednak pola wyboru, których zaznaczenie określa *klientów*, usługi i protokoły wykorzystywane przez konkretne połączenie sieci lokalnej.

Usługi

W oknie dialogowym właściwości połączenia lokalnego dostępne są trzy usługi. Pierwsza z nich, *Udostępnianie plików i drukarek w sieciach Microsoft Networks* (File and Printer Sharing for Microsoft Networks), jest instalowana domyślnie. Dwie pozostałe są dostępne po kliknięciu przycisku *Zainstaluj* (Install) w oknie dialogowym właściwości połączenia lokalnego. Usługi te opisano poniżej.

- ♦ *Udostępnianie plików i drukarek w sieciach Microsoft Networks* (File and Printer Sharing for Microsoft Networks) — usługa ta umożliwia dostęp do zasobów komputera, na którym ją zainstalowano. Usługi udostępniania plików i drukarek odpowiadające usłudze *Server* muszą być włączone, jeśli zasoby mają być dostępne w sieci. Folder może wyglądać na udostępniony bez względu na to ustawienie, jednak łączący się użytkownicy otrzymają komunikat informujący o tym, że usługa *Server* nie została uruchomiona. Po wyłączeniu tej usługi nowe połączenia nie zostaną nawiązane, jednak połączenia istniejące pozostaną aktywne. Aktywne sesje zamyka się korzystając z węzła *Foldery udostępnione* (Shared Folders) w konsoli *Zarządzanie komputerem* (Computer Management).
- ♦ *Harmonogram pakietów QoS* (QoS Packet Scheduler) — technologia Quality of Service jest wykorzystywana do zarządzania aplikacjami znacznie obciążającymi sieć. Wraz z nastaniem strumieni wideo i dźwięku w czasie rzeczywistym QoS umożliwia administratorom sieci całkowite panowanie nad wykorzystaniem pasma, zapewniając w ten sposób, że jedna aplikacja nie „zapcha” sieci. Usługa harmonogramu pakietów pobiera pakiety z sieci, stosuje w odniesieniu do nich parametry QoS i przekazuje je dalej.
- ♦ *Agent SAP* (SAP Agent) — usługa zapewnia obsługę protokołu Service Advertising Protocol, charakterystycznego dla sieci NetWare. Protokół ten *rozglasza* takie zasoby jak udostępnione w sieci foldery, pliki i drukarki. Agent SAP określa dostępne w sieci zasoby i jest stosowany głównie w przypadku sieci opartych na protokole IPX, przy dostępie do zasobów serwerów Novell NetWare.

Wszystkie zainstalowane usługi są obrazuje ikona przedstawiająca komputer z charakterystyczną otwartą dłońią. Pełną listę usług i ich bieżących stanów uzyskuje się po wybraniu z menu *Narzędzia administracyjne* (Administrative Tools) pozycji *Zarządzanie komputerem* (Computer Management), a następnie otwarciu węzła *Usługi* (Services).

Instalacja i konfiguracja TCP/IP

W obecnych czasach administratorzy sieci stają w obliczu zadań zarządzania różnymi systemami operacyjnymi stale wymagającymi reorganizacji i integracji bez utraty wydajności. Na szczęście pojawił się elastyczny i niezawodny protokół TCP/IP, działający w prawie wszystkich środowiskach i w większości technologii. Dużą część popularności TCP/IP można przypisać rozwojowi Internetu i standardów tego otwartego protokołu. Implementacja TCP/IP w Windows 2000 zawiera wiele nowych możliwości znacznie ulepszających bezpieczeństwo, niezawodność i wydajność tego protokołu.

W bieżącym podrozdziale zostanie przedstawiony proces instalacji i definicja wszystkich właściwości konfiguracyjnych TCP/IP. Bardziej szczegółową definicję TCP/IP zaprezentowano w rozdziale 17., *Konfiguracja dostępu z zastosowaniem TCP/IP*.

Instalacja TCP/IP

Protokół TCP/IP jest instalowany automatycznie podczas instalacji systemu i można go skonfigurować, usunąć lub ponownie zainstalować w dowolnym momencie. Ustawienia konfiguracyjne znajdują się w oknach dialogowych właściwości wszystkich połączeń lokalnych. Poniższe kroki opisują instalację TCP/IP:

1. Z menu *Start* wybierz *Ustawienia* (Settings), *Panel sterowania* (Control Panel).
2. W *Panelu sterowania* (Control Panel) kliknij dwukrotnie ikonę *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections).
3. W oknie *Połączenia sieciowe i telefoniczne* (Network and Dial-up Connections) kliknij prawym przyciskiem myszy obiekt *Połączenie lokalne* (Local Area Connection) i wybierz z menu podręcznego pozycję *Właściwości* (Properties).
4. W oknie właściwości kliknij *Zainstaluj* (Install), a następnie *Protokół* (Protocol). Kliknij *Dodaj* (Add).
5. Z listy protokołów wybierz TCP/IP i kliknij *OK*. TCP/IP instaluje się bez potrzeby ponownego uruchamiania komputera.

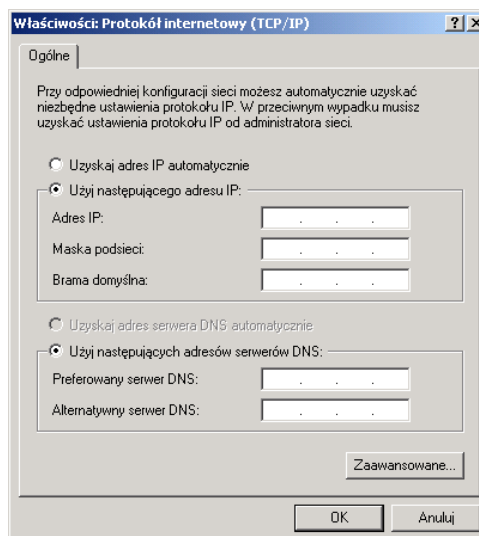
TCP/IP nie wymaga konfiguracji adresu IP, ponieważ domyślnie protokół ten jest ustawiony do korzystania z mechanizmu DHCP, bardziej szczegółowo opisanego w dalszej części bieżącego rozdziału, w podrozdziale *DHCP*. Po zainstalowaniu TCP/IP użytkownicy mogą ręcznie dodać adres IP i maskę podsieci. W tym celu należy wybrać zakładkę *Sieć* (Network) w oknie dialogowym właściwości dowolnego połączenia sieciowego. Jeżeli z systemu usunięto TCP/IP, Windows 2000 Professional będzie wymagał ponownego uruchomienia, inicjalizującego nowe ustawienia.

Ogólne właściwości TCP/IP

Okno ogólnych właściwości protokołu TCP/IP umożliwia ręczną konfigurację ustawień adresu IP, maski podsieci i bramy domyślnej (rysunek 21.17). Domyślnie adres IP jest automatycznie uzyskiwany z serwera DHCP, jednak przyciskiem opcji przełącza się adres IP z dynamicznego na statyczny.

Nowością w systemach Windows jest automatyczne uzyskiwanie adresu serwera DNS. System DNS odgrywa bardziej znaczącą rolę w rodzinie Windows 2000 i opisano go w dalszej części bieżącego rozdziału, w podrozdziale zatytułowanym *DNS*. Protokół TCP/IP może automatycznie przydzielić adres serwera DNS lub też można ręcznie wprowadzić adresy podstawowego i zapasowego serwera DNS. Dalsze ustawienia protokołu TCP/IP wprowadza się po kliknięciu przycisku *Zaawansowane* (Advanced). Dostępne są wówczas ustawienia systemów DNS i WINS oraz zabezpieczeń IP i TCP/IP, opisane pod koniec rozdziału.

Rysunek 21.17.
Ogólne właściwości
TCP/IP



DHCP

Protokół dynamicznej konfiguracji *hosta* (DHCP — Dynamic Host Configuration Protocol) odgrywa jedną z najważniejszych ról w TCP/IP. Zamiast ręcznego nadawania adresów IP i pozostałych ustawień TCP/IP każdemu komputerowi w sieci, wszystkie informacje IP mogą być centralnie zarządzane z serwera DHCP. Serwer DHCP przechowuje pulę adresów IP (zwaną zakresem) przekazywanych wszystkim komputerom działającym jako klienci DHCP. Informacje przekazywane stacjom *klienckim* z serwera DHCP obejmują adres IP, maskę podsieci, adres IP bramy domyślnej oraz adresy IP serwerów DNS i WINS. Stacja uzyskuje zatem z serwera DHCP wszystkie informacje potrzebne do komunikacji w sieci opartej na protokole TCP/IP.

Klient DHCP w trakcie uruchamiania żąda nadania adresu IP przez serwer DHCP. System Windows 2000 Professional instaluje się jako *klient* DHCP. Serwer DHCP oferuje *klientowi* dzierżawę adresu IP, maski podsieci i innych ustawień na ustalony okres czasu. Dzierżawiąc adres IP, *klient* otrzymuje informacje IP na określony czas, po którym następuje żądanie odświeżenia dzierżawy. *Klient* przyjmuje informacje konfiguracji z serwera DHCP i od tej chwili może komunikować się z innymi urządzeniami, korzystając lokalnie lub zdalnie z protokołu TCP/IP. Serwer DHCP potwierdza następnie akceptację ustawień TCP/IP przez *klienta* i przestaje oferować nadany adres IP pozostałym komputerom.



Serwer DHCP może działać w ramach podsieci lub być serwerem zdalnym, co oznacza, że może on być usytuowany za jednym lub kilkoma routerami. Przekazujący agent DHCP przesyła żądania przez routery do serwera DHCP.

Nową możliwością w Windows 2000 jest automatyczna konfiguracja *klienta*. Podczas uruchamiania komputer żąda informacji o adresie IP od serwera DHCP poprzez *rozglądanie* w sieci. Jeżeli żaden serwer DHCP na to nie zareaguje, klient DHCP automatycznie skonfiguruje adres, korzystając z zarezerwowanego przez Microsoft zakresu

klasy B 169.254.0.0 o masce podsieci 255.255.0.0. *Klient* DHCP upewni się, że dany adres nie jest używany, wydając polecenie ARP. Jeżeli dany adres jest już używany w sieci, automatyczna konfiguracja *klienta* wybiera inny adres i powtarza cały proces.

Automatyczna konfiguracja *klienta* sprawdza co pięć minut od chwili przydzielenia adresu IP z puli 169.254.0.0, czy przypadkiem serwer DHCP nie stał się już dostępny. Jeżeli serwer DHCP odpowie na żądanie, uprzednio przydzielone ustawienia zostają anulowane i *klient* akceptuje ofertę serwera DHCP.



Aby wyłączyć funkcję automatycznej konfiguracji *klienta* w Windows 2000 Professional, należy dodać w rejestrze systemu wpis IPAutoconfigurationEnabled z wartością false. Wpisy IPAutoconfigurationSubnet i IPAutoconfigurationMask sterują podsiecią i maską podsieci w tej funkcji. Wartości te mieszczą się w kluczu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCP/IP\Parameters

DNS

Komputery korzystające z TCP/IP komunikują się z innymi urządzeniami w oparciu o adres IP, jednak adresy IP są trudne do zapamiętania i z tego względu utworzono bardziej przyjazną użytkownikowi metodę nazw węzłów. Nazwa węzła to powszechnie rozpoznawana nazwa komputera, jak na przykład „Sprzedaż1” lub „ZuzannaP”. System DNS (Domain Name System) jest usługą tłumaczącą nazwy węzłów na adresy IP.



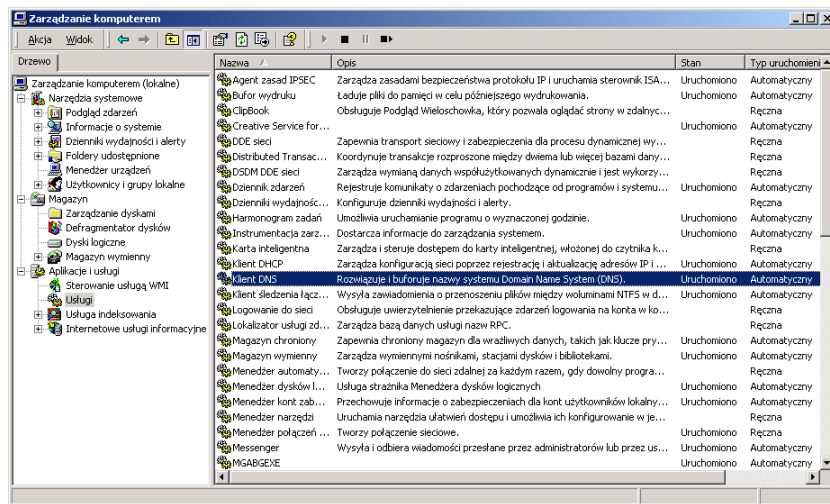
W nomenklaturze firmy Microsoft scentralizowana grupa komputerów w sieci nazywana jest domeną. Pojęcie to jest całkowicie niezależne od nazwy domeny TCP/IP, odzwierciedlanej przez serwer DNS. Nazwy domeny TCP/IP są stosowane w Internecie w takich programach jak Internet Explorer, a domeny w pojęciu Microsoftu są „tworami wewnętrznymi” przedsiębiorstwa.

W Windows 2000 ulepszono DNS, wprowadzając dynamiczne aktualizacje z zastosowaniem serwera DHCP. Gdy serwer DHCP (Windows 2000) wydierżawia adres IP *klientowi* DHCP (Windows 2000), ten wysyła swoją *w pełni kwalifikowaną* nazwę domeny (FQDN — Fully Qualified Domain Name) do tegoż serwera żądając jej rejestracji w serwerze DNS. *W pełni kwalifikowana* nazwa domeny to nazwa węzła komputera wraz z nazwą domeny, do której on należy. Serwer DHCP rejestruje następnie w serwerze DNS rekord węzła komputera oraz rekord PTR przeszukiwania wstecznego. Rekord PTR służy do przeprowadzania przeszukiwań wstecznych, polegających na tym, że serwer dostarcza nazwę węzła na podstawie podanego adresu IP. Takie rodzaje rekordów są zazwyczaj używane przez serwery poczty elektronicznej. Dzięki wykorzystaniu serwera DHCP do rejestracji nazw FQDN, baza danych systemu DNS jest spójna i zawiera wszystkie adresy wydierżawione klientom DHCP. Ta sama procedura dotyczy także odświeżania adresów IP.

Jeśli klient DHCP z systemem Windows 2000 dzierżawi adres IP z serwera DHCP, który nie obsługuje dynamicznej aktualizacji, *klient* ten samodzielnie zarejestruje się w serwerze DNS. Wpisy statycznych adresów IP klientów niekorzystających z DHCP nadal są wpisywane ręcznie w serwerze DNS.

Inną funkcją w Windows 2000 jest usługa buforowania odpowiedzi systemu DNS. Gdy komputer z systemem Windows 2000 Professional wymaga od serwera DNS określenia adresu IP na podstawie nazwy FQDN, wynik wyszukiwania jest zapamiętywany w buforze odpowiedzi systemu DNS tego komputera. Wynik wyszukiwania zawiera parametr *TTL* (Time to Live), określający, jak długo dany wpis będzie przechowywany w lokalnym buforze. Wszelkie przyszłe zapytania komputera o dany adres IP nie wymagają już komunikacji z serwerem DNS, co obniża tym samym stopień wykorzystania sieci. Usługa buforowania odpowiedzi systemu DNS zapamiętuje również negatywne odpowiedzi, które nie zwróciły adresu IP danej nazwy węzła, lub na które w ogóle nie było żadnej odpowiedzi; w ten sposób unika się przyszłych opóźnień związanych z oczekiwaniem na odpowiedzi odmowne. Usługa buforowania systemu DNS działa jako usługa systemu Windows 2000 Professional i jak każdą inną usługę można ją uruchomić, wstrzymać i zatrzymać. Rysunek 21.18 przedstawia tę usługę.

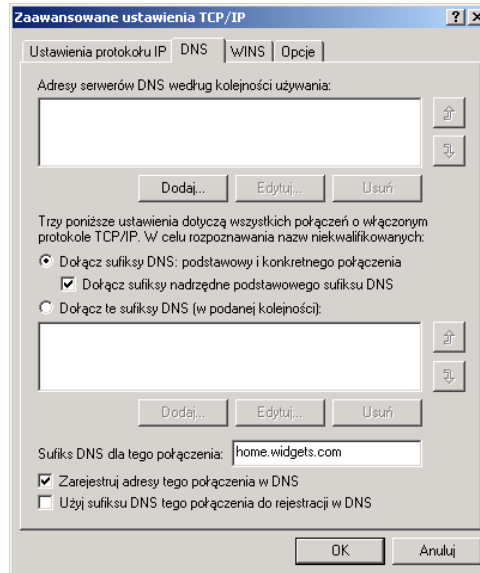
Rysunek 21.18.
Usługa pamięci podręcznej DNS



Serwer DHCP domyślnie dostarcza informacje o adresach IP serwerów DNS i żadne dalsze dane nie są wymagane, jednak po kliknięciu przycisku *Zaawansowane* (Advanced) w oknie właściwości TCP/IP dostępne są pewne konfigurowalne ustawienia systemu DNS. Rysunek 21.19 prezentuje te ustawienia, a poniżej przedstawiono opis poszczególnych opcji:

- ◆ Pierwsze pole zawiera listę serwerów DNS w kolejności ich przeszukiwania w zapytaniach o adres IP.
- ◆ Kolejna opcja zmienia parametry przeszukiwania systemu DNS. Gdy aplikacja wywołuje wyszukiwanie adresu IP na podstawie nazwy węzła, zapytanie dołącza do nazwy węzła nazwę domeny nadrzędnej. Przykładowo wpisanie polecenia ftp sprzedaż1 spowoduje skierowanie do serwera DNS żądania określenia adresu IP na podstawie podanej nazwy. Przed wysłaniem zapytania komputer *kliencki* uzupełni nazwę węzła sprzedaż1 nazwą domeny; jeśli nazwa domeny komputera sprzedaż1 brzmi *popkey.com*, zapytanie będzie zawierać nazwę sprzedaż1.popkey.com. Nazwę domeny może dostarczać dzierżawa DHCP

Rysunek 21.19.
Zakładka DNS
zaawansowanych
ustawień TCP/IP



lub można ją wpisać w polu *Sufiks DNS dla tego połączenia* (DNS suffix for this connection) w zakładce *DNS*. Zakładka ta zawiera opcje dodawania nazwy domeny do nazwy węzła lub odpytywania serwera DNS przy użyciu wymienionych nazw domen.

- ♦ Pozostałe opcje dotyczą rejestracji przez serwer DHCP nazwy węzła i nazwy domeny w serwerze DNS.

NetBIOS i WINS

We wcześniejszych systemach operacyjnych Windows każdy komputer potrzebował nazwy NetBIOS (Network Input/Output System) do komunikacji z zastosowaniem takich mechanizmów jak *Otoczenie sieciowe* (Network Neighborhood) lub polecenie Net View. Nazwy NetBIOS są wykorzystywane przez aplikacje systemu Windows do komunikacji z innymi komputerami. Podobnie jak nazwy węzłów, nazwy NetBIOS były odzwierciedlane adresami IP, jednak proces określania adresów IP odbywał się w oparciu o *rozgłaszanie*, co powodowało „zapychanie” większych sieci. Usługa WINS (Windows Internet Name Service) zmniejsza „burze rozgłaszania”, odzwierciedlając nazwy NetBIOS adresami IP, bezpośrednio komunikując się z klientami zamiast stosować *rozgłaszanie*. WINS jest bazą danych nazw NetBIOS i odpowiadających im adresów IP, przechowywaną w serwerze Windows 2000, w którym działa usługa WINS. Zakres funkcji nazw NetBIOS i usługi WINS został rozszerzony w porównaniu z poprzednimi wersjami systemu Windows NT.

Nową funkcją systemu Windows 2000 związaną z nazwami NetBIOS jest *mechanizm węzłów bezpośrednich*

(direct hosting). Umożliwia on aplikacjom poprzednio stosującym rozgłaszanie NetBIOS bezpośrednią komunikację w sposób podobny do gniazd Windows. Mechanizm

ten do odzwierciedlania nazw wykorzystuje system DNS zamiast *rozglaszania*, co upraszcza protokół i udostępnia aplikacjom większe pasmo sieci, jednak metoda węzłów bezpośrednich działa wyłącznie w komunikacji pomiędzy komputerami wyposażonymi w system Windows 2000. Komunikacja z wcześniejszymi systemami, takimi jak Windows NT 4 lub Windows 98, wykorzystuje *rozglaszanie* i system WINS.

Uwaga

Gniazdo systemu Windows jest metodą bezpośredniej komunikacji z innym komputerem z zastosowaniem adresu IP i numeru portu. Adres IP określa, w której sieci znajduje się komputer i jaki posiada numer w jej obrębie. Posłużmy się analogią — przykładem ludzi mieszkających w domach usytuowanych przy różnych ulicach. Każdy dom musi posiadać numer wyróżniający go w ramach ulicy, a każda ulica musi mieć unikatową w mieście nazwę. Adres IP odpowiada nazwie ulicy i numerowi domu. Gniazda korzystają również z portów. Port określa proces komputera docelowego, z którym komunikuje się komputer nadający. Niech za przykład posłuży komputer pełniący funkcję serwera FTP i serwera internetowego. Pozostałe komputery muszą *wiedzieć*, z którą usługą mają się komunikować — FTP lub HTTP. Porty wyróżniają każdą usługę w ramach komputera (port 21 dla FTP i port 80 dla HTTP). Port odpowiada numerowi apartamentu w budynku położonym przy ulicy. Adres IP i numer portu składają się na gniazdo. W ten sposób komputery komunikują się z określoną usługą innego komputera.

W Windows 2000 zaciera się linia oddzielająca aplikacje opierające się na nazwach węzłów od aplikacji stosujących nazwy NetBIOS. Nowe funkcje obejmują łączenie się z poziomu poleceń NetBIOS z urządzeniami stosującymi TCP/IP i nazwy FQDN. Polecenie `net use`, na przykład, mapuje literę napędu do zasobu udostępnianego w innym komputerze. Litery napędów można teraz mapować stosując nazwy FQDN. Oto przykład:

- ◆ `Net use x: \\www.Microsoft.com\windows2000`
- ◆ `Net use v: \\10.16.0.10\home`

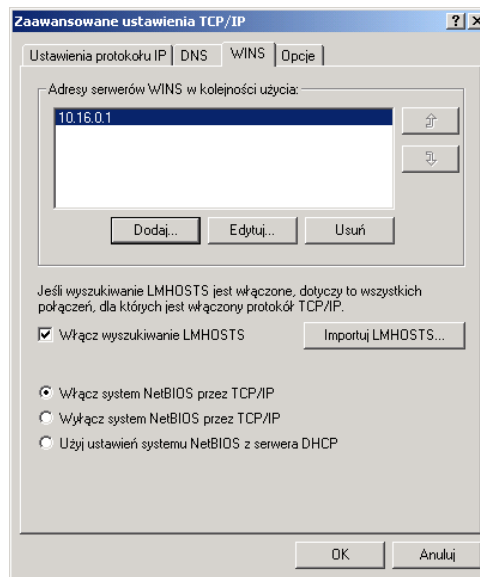
Inne polecenia, takie jak `dir` czy `net view` i wiele programów administracyjnych może korzystać z *w pełni kwalifikowanych* nazw domen. Jeżeli administrator nie chce korzystać z NetBIOS-u, może go całkowicie wyłączyć w oknie dialogowym właściwości połączenia.

Usługa WINS w Windows 2000 również charakteryzuje się poszerzonym zestawem funkcji zarówno serwera, jak i *klienta*. Windows 2000 Professional może korzystać maksymalnie z dwunastu serwerów WINS w celu zwiększenia odporności na awarie, a zmiany właściwości WINS nie wymagają ponownego uruchamiania komputera. Zmiany ustawień dotyczących systemu WINS wprowadza się w zakładce *WINS*, dostępnej po kliknięciu przycisku *Zaawansowane* (Advanced) w oknie właściwości TCP/IP. Zakładkę tę przedstawiono na rysunku 21.20.

Zakładka *WINS* zawiera następujące opcje:

- ◆ *Ręczne wprowadzenie adresów serwerów WINS* — komputery z systemem Windows 2000 Professional wymagają adresu IP serwera WINS. Adres ten wprowadza się ręcznie lub jest on dostarczany wraz z dzierżawą DHCP.
- ◆ *Włączenie korzystania z pliku Lmhosts* — plik *Lmhosts* działa podobnie jak plik *hosts*. Również zawiera listę nazw i odpowiadających im adresów IP, z tym że odzwierciedla on nazwy NetBIOS.
- ◆ *Zmiana ustawień NetBIOS* — NetBIOS można całkowicie wyłączyć w sieciach korzystających z nazw węzłów i nie używać aplikacji opartych na tym protokole.

Rysunek 21.20.
Zakładka
właściwości WINS



Zabezpieczenia IP

IPSec (IP Security) jest opartą na kryptografii usługą uwierzytelniania i szyfrowania, działającą w warstwie internetowej stosu protokołów TCP/IP. Jest to nowa funkcja w systemie Windows 2000, wypełniająca lukę w wielu sieciach, które dopuszczały przesyłanie otwartego tekstu w intranecie lub ekstranecie. Użytkownik o złych zamiarach musiał jedynie uzyskać dostęp do fizycznego komputera w sieci, aby przechwycić informacje o hasle. Dwie metody chroniące przed wyłomami w bezpieczeństwie to uwierzytelnianie i szyfrowanie danych. Każdy komputer może teraz korzystać z następujących metod uwierzytelniania:

- ♦ *Wymiana certyfikatów autentyczności* — użytkownicy w celu uwierzytelnienia muszą przedstawić certyfikat zawierający *klucz publiczny*. Certyfikat potwierdza, że użytkownik rzeczywiście jest tym, za kogo się podaje i nie jest oszustem. *Klucze publiczne* w połączeniu z *kluczami prywatnymi* są stosowane jako metoda szyfrowania i deszyfrowania haseł.
- ♦ *Uwierzytelnianie Kerberos* — jest to domyślna opcja uwierzytelniania. Protokół Kerberos V5 szyfruje hasła przesyłane w sieci podczas uwierzytelniania.
- ♦ *Wymiana kluczy* — ta metoda uwierzytelniania szyfruje hasła przy użyciu współdzielonego, wcześniej ustalonego tajnego klucza. Użytkownik musi posiadać ten klucz, aby system mógł go uwierzytelnić.

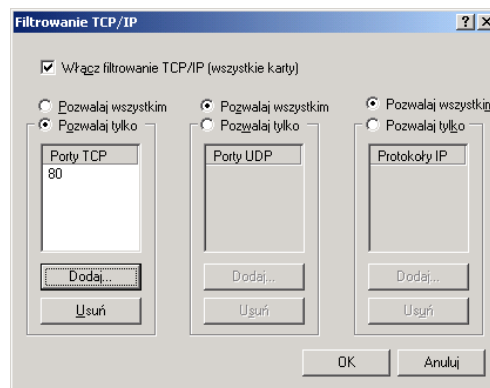
IPSec korzysta z szyfrowania danych, stosując odmianę standardu DES (Data Encryption Standard). Szyfrowanie spowalnia ruch w sieci i powinno być stosowane rozważnie. Inne opcje, takie jak przeniesienie procesu szyfrowania na urządzenie sprzętowe, mogą obniżyć ten efekt spowolnienia.

Zasady zabezpieczeń IP tworzy się w konsoli *Zarządzanie komputerem* (Computer Management), w węzle zasad grup serwera Windows 2000, a następnie aktywuje je w zakładce *Opcje* (Options) okna zaawansowanych ustawień TCP/IP. Włączenie tej opcji umożliwia systemowi Windows 2000 Professional działanie w trybie odpowiedzi na negocjacje zabezpieczeń IP.

Filtrowanie TCP/IP

Funkcja filtrowania protokołu TCP/IP stosuje filtr na poziomie pakietów protokołów TCP, UDP i IP do określania portów, w obrębie których dopuszczalna jest transmisja informacji do komputera. Domyślne ustawienia zezwalają na transmisję danych przez wszystkie porty, jednak kliknięcie przycisku opcji *Pozwalaj tylko* (Permit Only) i wpisanie dopuszczalnych portów zmienia tę konfigurację. Rysunek 21.21 przedstawia okno dialogowe *Filtrowanie TCP/IP* (TCP/IP Filtering), w którym zezwolono jedynie na komunikację przez port 80 protokołu HTTP.

Rysunek 21.21.
Okno dialogowe
filtrowania TCP/IP



Uwaga

UDP (User Datagram Protocol) jest protokołem transportowym, zapewniającym bezpołączeniowe dostarczanie danych do komputera odbierającego. Oznacza to, że nie gwarantuje on nadejścia danych w stanie nienaruszonym (w przeciwieństwie do TCP). Z tego powodu charakteryzuje się on jednak mniejszym obciążeniem niż TCP i dzięki temu jest szybszym protokołem. Przykładem użycia UDP w roli protokołu transportowego jest polecenie ping.

Filtrowanie TCP/IP stanowi świetny środek przeciwko atakom w obrębie nielegalnych portów lub ogranicznik dostępu do wybranych programów.

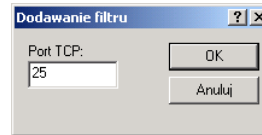
Uwaga

Numerzy portów od 1 do 1023 są zarezerwowane jako „dobrze znane” numery. Numery portów protokołów TCP i UDP opierają się na pliku *Winnt\System32\Drivers\Etc\Services*, zawierającym listę dobrze znanych numerów portów i ich nazw. Numery portów protokołu IP znajdują się w pliku *\systemroot\system32\drivers\etc\protocols*. Na podstawie zawartości tych plików można określić numery dopuszczonych do transmisji portów.

Aby określić, które porty będą blokowane, należy kliknąć przycisk *Dodaj* (Add) dla jednego z protokołów TCP, UDP lub IP. Następnie wpisuje się numer portu, który ma być filtrowany. Rysunek 21.22 przedstawia ustalenie filtrowania portu 25 protokołu TCP, używanego do wysyłania poczty elektronicznej pomiędzy serwerami SMTP.

Rysunek 21.22.

Okno dialogowe Dodawanie filtra (Add Filter), w którym odfiltrowuje się niedopuszczalne porty



Sprawdzanie łączności TCP/IP

Polecenie ping jest najskuteczniejszym i najprostszym narzędziem do rozwiązywania problemów z połączeniami TCP/IP. *Packet Internet Groper (PING)* wysyła cztery pakiety ICMP (protokół przesyłania komunikatów działający w warstwie internetowej) do komputera docelowego i w przypadku powodzenia odbiera cztery zwrotne komunikaty echa. Do sprawdzenia komunikacji pomiędzy dwoma komputerami używa się czterech rodzajów sprawdzeń z zastosowaniem polecenia ping. Więcej informacji o używaniu polecenia ping umieszczono podrozdziale *Rozwiązywanie problemów związanych z TCP/IP*, w rozdziale 17., *Konfiguracja dostępu z zastosowaniem TCP/IP*. Oto cztery odrębne typy sprawdzeń przy użyciu polecenia ping wraz z opisem:

- ♦ *Użycie polecenia ping w odniesieniu do adresu pętli zwrotnej* — jak wcześniej wspomniano, adres 127.0.0.1 służy do testowania działania kart sieciowych. Sprawdzenie tego adresu poleceniem ping dostarcza informacji o poprawności zainstalowania karty sieciowej, choć adres IP i maska podsieci mogą wymagać modyfikacji.
- ♦ *Użycie polecenia ping w odniesieniu do najbliższego routera* — informuje o poprawności konfiguracji adresu IP i maski podsieci. Adres IP bramy domyślnej zazwyczaj nigdy się nie zmienia ani nie jest wyłączany, a zatem świetnie nadaje się do testów.
- ♦ *Użycie polecenia ping w odniesieniu do adresu położonego po drugiej stronie routera* — administratorzy zawsze znają jeden lub dwa adresy, o których wiedzą, że są stale aktywne i używają ich jako adresów testowych. Odpowiedzi zwrotne spod tych adresów informują o poprawności działania bramy domyślnej.
- ♦ *Użycie polecenia ping w odniesieniu do nazwy innego komputera* — poprzednie trzy sprawdzenia testowały komunikację między dwoma komputerami. To ostatnie sprawdzenie testuje, czy komputer potrafi odzwierciedlić nazwę węzła jego adresem IP. Windows 2000 najpierw sprawdza nazwę węzła lokalnego, sprawdzając, czy polecenie ping nie dotyczy macierzystej stacji, następnie „zagląda” do pliku *hosts* i na zakończenie sprawdza system DNS. Jeśli odpowiedź od zdalnego węzła nie pojawia się, oznacza to, że jeden z tych trzech obszarów rozpoznawania nazw nie działa. Jak wcześniej wspomniano, Windows 2000 zawiera również usługę buforowania odpowiedzi systemu DNS, przechowującą zapytania przez pewien okres czasu. Przyszłe zapytania rozpoznawania nazw mogą być obsługane w oparciu o bufor.

Oczywiście wielu administratorów od razu posłuży się ostatnim z czterech sprawdzeń, ponieważ jego powodzenie oznacza poprawność trzech wcześniejszych.

Oto przykład użycia polecenia ping w odniesieniu do adresu IP:

```
C:\>ping 10.16.10.15
```

```
Badanie 10.16.10.15 z zastosowaniem 32 bajtów danych:
```

```
Odpowiedź z 10.16.10.15: bajtów=32 czas<10ms TTL=128
Odpowiedź z 10.16.10.15: bajtów=32 czas<10ms TTL=128
Odpowiedź z 10.16.10.15: bajtów=32 czas<10ms TTL=128
Odpowiedź z 10.16.10.15: bajtów=32 czas<10ms TTL=128
```

```
Statystyka badania dla 10.16.10.15:
```

```
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% utraconych),
Szacunkowy czas błędzenia pakietów w millisekundach:
Minimum = 0ms, Maksimum = 0ms, Średnia = 0ms
```

NWLink

NWLink to wprowadzona przez Microsoft implementacja protokołu IPX/SPX firmy Novell. IPX/SPX w tym przypomina TCP/IP, że jest niezawodnym 32-bitowym protokołem podlegającym *trasowaniu*. Zestaw protokołów IPX/SPX jest jednak wyłączną własnością firmy Novell i z tego powodu nie rozpowszechnił się tak szeroko jak TCP/IP. W sieciach, które nie wymagają dostępu do Internetu albo są zaopatrzone w zaporę sieciową (firewall) lub serwer pośredniczący (proxy), NWLink jest dobrą alternatywą wobec opartego na *rozglaszaniu* protokołu NetBEUI. NWLink często wykorzystuje się w dużych instalacjach *klienckich* jako protokół wstępnie łączący się z serwerem dystrybucyjnym.

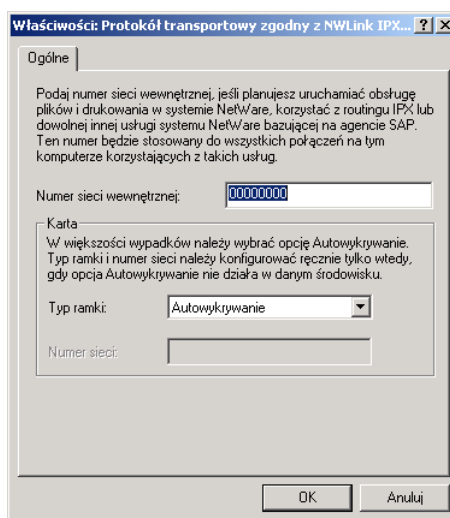
Oto metoda instalacji protokołu NWLink w systemie Windows 2000 Professional:

1. W oknie dialogowym *Właściwości: Połączenie lokalne* (Local Area Connection Properties) wybierz *Zainstaluj* (Install) (rysunek 21.13).
2. Wybierz *Protokół* (Protocol) i kliknij *Dodaj* (Add).
3. Z listy niezainstalowanych protokołów wybierz *Protokół transportowy zgodny z NWLink IPX/SPX/NetBIOS* (NWLink IPX/SPX/NetBIOS Compatible Transport Protocol) i kliknij *OK*.

Właściwości protokołu NWLink określają używany w sieci typ ramki. Serwery Novell NetWare 3.11 i wersji wcześniejszych korzystały z ramki typu 802.3; Novell NetWare 3.12 i późniejsze wersje stosują ramkę typu 802.2. *Typ ramki* określa format informacji wysyłanych w sieci. Komunikujące się urządzenia muszą używać tego samego typu ramki. Domyślne ustawienie typu ramki protokołu NWLink to *Autowykrywanie* (Auto Detect), co oznacza, że komputer wybiera odpowiednie ustawienie typu ramki. Jeśli NWLink wykryje w sieci kilka typów ramek, wybierze 802.2. Okno właściwości protokołu NWLink umożliwia ręczny wybór typu ramki, jeśli domyślnie wybrany typ nie jest odpowiedni.

Kolejne ustawienie okna właściwości protokołu NWLink to wybór numeru sieci wewnętrznej. Numer sieci wewnętrznej, często nazywany *numerem wirtualnym*, określa unikatowy numer w komputerze posiadającym kilka kart sieciowych, podłączonych do różnych sieci. Rysunek 21.23 przedstawia ustawienia właściwości protokołu NWLink.

Rysunek 21.23.
Okno dialogowe
Właściwości:
Protokół transportowy
zgodny z NWLink
IPX/SPX/NetBIOS
(NWLink IPX/SPX
/NetBIOS Compatible
Transport Protocol)



Po zainstalowaniu protokołu NWLink w oknie *Właściwości: Połączenie lokalne* (Local Area Connection Properties) pojawiają się dwie pozycje składników. NWLink NetBIOS konfiguruje NetBIOS przez IPX. Ustawienie to zapewnia obsługę nazw NetBIOS i aplikacji w komputerach z systemami Microsoftu i firmy Novell.

NetBEUI

NetBEUI (NetBIOS Enhanced User Interface) to niewielki, szybki i wydajny protokół, znajdujący zastosowanie w małych i domowych sieciach, które nie komunikują się ze światem zewnętrznym lub robią to poprzez serwer pośredniczący (proxy). Z powodu ograniczeń wynikających z architektury protokół ten nigdy nie wyjdzie poza obszar małych sieci, pomimo swego niskiego obciążenia i braku potrzeby administracji. NetBEUI jest protokołem niepodlegającym *trasowaniu*, z wyjątkiem pewnych mało popularnych sieci, i opiera się na *rozglaszaniu*.



NetBEUI często jest mylony ze specyfikacją NetBIOS. NetBIOS to zbiór poleceń i standardów określających transmisję informacji pomiędzy różnymi systemami. Pierwotnie zaprojektowany przez firmę IBM, NetBIOS działa jako *interfejs programowy aplikacji* (API — Application Programming Interface) wywołujący niskopoziomowe usługi do realizacji poleceń. NetBEUI jest protokołem, który wykonuje 17 spośród poleceń, jakie zawiera NetBIOS, i stanowi wprowadzoną przez Microsoft implementację standardów NetBIOS firmy IBM.

NetBEUI przeznaczono do pracy w sieciach połączonych *mostami* (bridge), a nie routernami. Współczesne sieci prawie zawsze wymagają pewnej formy *trasowania* i dlatego nie stosuje się w nich protokołu NetBEUI. Urządzenia używające protokołu NetBEUI komunikują się w oparciu o *rozglaszanie* i w rezultacie każdy komputer w sieci musi przetworzyć informacje wysyłane przez inny komputer. Proces ten powoduje „zapychanie” większych sieci — trzeba w nich stosować mosty lub przejść do protokołu bezpośredniej komunikacji typu punkt-punkt, taki jak TCP lub IPX/SPX.

Inne protokoły

Windows 2000 oferuje jeszcze kilka protokołów, używanych zazwyczaj jako dodatkowe funkcje jednego z trzech omówionych w bieżącym rozdziale podstawowych protokołów. Kluczową zasadą stosowania protokołów sieciowych jest instalacja możliwie najmniejszej ich liczby. Komputer wysyłający próbuje zestawzić sesję z komputerem odbierającym, korzystając ze wszystkich zainstalowanych protokołów. Zainstalowanie tylko niezbędnych protokołów likwiduje dodatkowe obciążenie spowodowane tymi próbami ustanowienia sesji. Zbędne protokoły dodatkowo obciążają pamięć i procesor komputera. Oto wspomniane dodatkowe protokoły:

- ♦ *Protokół AppleTalk* — protokół wykorzystywany do komunikacji z komputerami Apple Macintosh.
- ♦ *Protokół DLC (Data Link Control)* — niepodlegający *trasowaniu* protokół używany do komunikacji z drukarkami sieciowymi i komputerami typu mainframe firmy IBM.
- ♦ *Protokół OSI-LAN* — instaluje sterowniki mapujące warstwę transportową i sieciową modelu OSI; powszechnie używany w integracji poczty i x.400.
- ♦ *Sterownik monitora sieci (Network Monitor Driver)* — dzięki niemu zostaje zainstalowany agent monitorowania sieci, umożliwiający odbieranie i przeglądanie ramek w programie *Monitor sieci (Network Monitor)*.
- ♦ *Środowisko strumieni (Streams Environment)* — używane do aktywacji sterowników transportowych środowiska strumieni, które jest oparte na systemie Unix, do Windows.

Więcej informacji o powyższych protokołach można znaleźć w bazie informacji technicznej Microsoft Technet — Technical Information Library.