

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

Rozbudowa i naprawa sieci. Wydanie V

Autorzy: Scott Mueller, Terry W. Ogletree,
Mark Edward Soper

Tłumaczenie: Piotr Pilch, Przemysław Szeremiota
ISBN: 83-246-0474-X

Tytuł oryginału: [Upgrading and Repairing
Networks \(5th Edition\)](#)

Format: B5, stron: 1440



Poznaj zasady działania sieci komputerowych i naucz się nimi administrować

- Projektowanie sieci komputerowych
- Protokoły komunikacyjne i urządzenia
- Przyłączanie komputerów do sieci
- Zarządzanie siecią

W ciągu ostatnich lat sieci komputerowe stały się niemal tak powszechne, jak telefony i telewizja. Wiedza dotycząca zasad ich działania, umiejętność zarządzania nimi lub chociażby korzystania z nich jest dziś niezbędna większości użytkowników komputerów — od korporacyjnych informatyków po entuzjastów technologii komputerowych, wdrażających je w swoich domach i małych biurach. Na szczęście wraz z rozwojem sieci ujednolicono protokoły komunikacyjne i zaimplementowano w systemach operacyjnych narzędzia niezbędne do podłączenia komputera do sieci. Nie oznacza to jednak, że korzystanie z sieci przestało być źródłem problemów.

Dzięki książce „Rozbudowa i naprawa sieci. Wydanie V” rozwiążesz wszystkie problemy, jakie kiedykolwiek napotkasz projektując sieć i administrując nią. Najnowsze wydanie tej książki, uzupełnione o wiadomości dotyczące sieci bezprzewodowych, technologii Bluetooth i Gigabit Internet oraz możliwości sieciowych systemu Windows XP, zawiera kompleksowe omówienie wszystkich zagadnień związanych z sieciami komputerowymi. Czytając tę książkę poznasz strategię projektowania sieci i doboru odpowiednich urządzeń oraz protokoły wykorzystywane do realizacji poszczególnych funkcji sieci. Nauczysz się administrować siecią, kontami użytkowników oraz dbać o bezpieczeństwo danych i komputerów.

- Topologie sieci
- Planowanie struktury sieci
- Okablowanie
- Dobór i konfiguracja urządzeń sieciowych
- Protokoły komunikacyjne
- Sieci bezprzewodowe Wi-Fi i Bluetooth
- Poczta elektroniczna
- Protokoły DNS i DHCP
- Zarządzanie użytkownikami w systemach Unix/Linux i Windows
- Drukowanie w sieci
- Ochrona sieci przed atakami z zewnątrz

Zostań administratorem doskonałym

Wydawnictwo Helion
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl



Spis treści

O autorach	27
Wprowadzenie	30
Część I Początek: planowanie i projektowanie sieci	35
Rozdział 1. Historia sieci komputerowych w pigułce	37
Rozdział 2. Przegląd topologii sieciowych	41
Topologie stosowane w sieciach lokalnych	41
Topologia magistrali	42
Topologia gwiazdy	43
Topologia pierścienia	45
Topologia siatki	47
Topologia hybrydowa	49
Topologie łączy wspólnego i łączy izolowanych	51
Porównanie topologii opartych na mostach i routerach	53
Tworzenie sieci wielosegmentowej i stosowane topologie	54
Łączenie segmentów sieci w obrębie budynku — sieć szkieletowa	55
Aspekty projektowania sieci wielosegmentowej	56
Skalowalność	57
Nadmiarowość	57
Topologia sieci wielowarstwowej	58
Skalowalność	59
Nadmiarowość	59
Odporność na awarie	59
Rozdział 3. Strategie projektowania sieci	61
Planowanie struktury logicznej sieci	62
Kim są Twoi klienci?	64
Jakiego typu usługi lub aplikacje powinny być udostępnione w sieci?	64
Jaki stopień niezawodności jest wymagany dla każdego połączenia sieciowego?	65
Dobór protokołu sieci lokalnej	66
Instrumenty planowania i projektowania	70
Pełna dokumentacja	71
Nigdy dosyć testowania	72
Tworzenie zasad i procedur używania sieci	72
Szkolenie personelu technicznego	74
Nie zapominaj o budżecie (chyba że możesz sobie na to pozwolić)	74
Struktura fizyczna sieci	75
Planowanie zasobów	75

Rozdział 4. Zarządzanie projektem i strategię modernizacji sieci	77
Od czego zacząć?	77
Analiza — stwierdzenie konieczności przeprowadzenia modernizacji	80
Określanie wymagań i oczekiwań użytkowników	83
Obsługa starszych aplikacji	85
Zasoby wymagane do przeprowadzenia modernizacji	86
Planowanie modernizacji	87
Dokumentowanie planu	88
Określenie stopnia zgodności planu z firmowymi zasadami i procedurami	88
Określanie celów	89
Planowanie czasu przestoju sieci	90
„Kamienie milowe” i kryteria	90
Procedury wycofywania	91
Testowanie planu	91
Sprawdzanie konkurencyjnych produktów	91
Projekt pilotażowy	92
Wdrażanie	93
Członkowie zespołu	93
Informowanie użytkowników	94
Śledzenie postępu prac	94
Szkolenie użytkowników	94
Na zakończenie: spis, co zostało wykonane i dlaczego	95
Inne zagadnienia dotyczące modernizacji	95
Rozdział 5. Ochrona sieci: metody zapobiegania zagrożeniom	97
Stabilizacja napięcia i zasilacze awaryjne UPS (Uninterruptible Power Supplies)	97
Energia to pieniądze	98
Interfejs ACPI (Advanced Configuration and Power Interface) a niezależne systemy zasilaczy awaryjnych UPS	100
Urządzenia sieciowe	102
Monitorowanie sieci	102
Kopie zapasowe stacji roboczych i serwerów	103
Nośniki archiwizujące — taśmy, dyski optyczne i twarde	105
Harmonogram wykonywania kopii zapasowych	107
Przechowywanie kopii zapasowej w innej fizycznej lokalizacji	109
Regularna konserwacja	110
Tworzenie nadmiarowości w sieci	111
Planowanie przywracania pracy sieci	111
Szacowanie kosztu metod ochrony	112
Część II Fizyczne komponenty sieci	113
Rozdział 6. Okablowanie sieciowe: kable, złącza, koncentratory i inne komponenty sieciowe	115
Okablowanie strukturalne	115
Obszar roboczy	116
Struktura okablowania szkieletowego	117
Struktura okablowania poziomego	119
Szafa telekomunikacyjna	119
Ważne definicje	119
Typy kabli	124
Skętki	124
Kable koncentryczne	129
Światłowody	133
Terminatory i połączenia	137
Zaciskanie	138
Styk uzyskany poprzez zdjęcie izolacji	138

Modularne gniazda i wtyczki	138
Konfiguracje par wtyczek modularnych	139
Typy powszechnie stosowanych gniazdek	139
Krosownice	141
Końcówki światłowodów	142
Łączenie światłowodów	144
Krosownice światłowodowe	145
Ogólne zalecenia dotyczące światłowodów	145
Złącza SFF (Small Form Factor)	146
Pomieszczenia telekomunikacyjne	146
Okablowanie „przenośnych” biur	147
Punkty konsolidacyjne	147
Ogólne specyfikacje podsystemu okablowania poziomego	147
Dokumentowanie i zarządzanie instalacją	147
Rekordy	148
Rysunki	149
Zlecenia	149
Raporty	149
Rozdział 7. Karty sieciowe	151
Wybór typu magistrali sprzętowej	151
ISA	153
PCI	154
PCMCIA	155
CardBus	156
Różne karty, inne szybkości	157
Terminatory i złącza kabli sieciowych	158
Założenia WfM (Wired for Management)	158
Universal Network Boot	159
Asset Management	159
Power Management	159
Remote Wake-Up	160
Czy warto stosować karty sieciowe zgodne z technologią WOL?	162
Systemy z wieloma kartami	162
Równoważenie obciążenia i nadmiarowe kontrolery sieci	163
Sterowniki programowe	164
Packet Driver	164
ODI (Open Data-Link Interface)	165
NDIS (Network Driver Interface Specification)	165
Sygnały IRQ i porty wejścia-wyjścia	166
Sygnały IRQ	166
Podstawowe porty I/O (wejścia-wyjścia)	169
Rozwiązywanie problemów z kartami sieciowymi	170
Sprawdzanie konfiguracji karty sieciowej w systemie Linux	171
Monitorowanie diod karty sieciowej — diody aktywności i diody połączenia	173
Zastosowanie programu diagnostycznego karty	175
Konflikty konfiguracji	175
Sprawdzanie konfiguracji sieciowej komputera	177
Konieczne kroki zapobiegawcze	177
Rozdział 8. Przełączniki sieciowe	179
Zasada działania przełączników	180
Dzielenie domeny kolizyjnej	182
Przełączniki sieci Ethernet działające w trybie pełnego duplexu	183
Tworzenie sieci szkieletowych przy użyciu przełączników	185
Rodzaje przełączników	188
Przełączniki bezzwłoczne	188
Przełączniki buforujące	188

Przełączniki warstwy trzeciej	189
Zastosowanie przełącznika w niewielkim biurze	191
Przełączniki piętrowe i modułarne	191
Diagnostyka i zarządzanie przełącznikami	191
Rozdział 9. Sieci wirtualne VLAN	193
Sieci wirtualne VLAN i topologie sieci	193
Przełączanie oparte na ramach sieciowych	195
Znakowanie niejawne i jawne	197
Znakowanie niejawne	197
Znakowanie jawne	198
Sieci wirtualne VLAN oparte na adresach MAC	199
Sieci wirtualne VLAN oparte na typie protokołu	199
Zastosowanie znakowania jawnego w sieciach szkieletowych	200
Standardy IEEE dla wirtualnych sieci lokalnych	202
Jakiego typu przełącznik zastosować?	204
Rozdział 10. Routery	207
Do czego służą routery?	207
Hierarchiczna organizacja sieci	208
Zastosowanie zabezpieczeń	209
Różnica pomiędzy protokołami routowalnymi i protokołami trasowania	210
Kiedy jest konieczne zastosowanie routera?	211
Zwiększanie rozmiarów sieci lokalnych	212
Delegowanie uprawnień administracyjnych dla sieci lokalnych	216
Łączenie oddziałów firmy	217
Zastosowanie routera do ochrony sieci — translacja adresów i filtrowanie pakietów	218
Porty routerów i połączenia z nimi	219
Konfigurowanie routerów	220
Typy obudów routerów	222
Zastosowanie routerów w sieciach rozległych WAN	224
Routery a internet	224
Rozdział 11. Urządzenia NAS i sieci SAN	227
Porównanie lokalnych i sieciowych urządzeń masowych	229
Zastosowanie technologii NAS (Network Attached Storage)	229
Zastosowanie sieci SAN (Storage Area Network)	230
Urządzenia NAS	231
Gotowe urządzenia sieciowe	232
Protokoły technologii NAS	233
Ograniczenia pojemnościowe technologii NAS — przepustowość i przestrzeń dyskowa	233
Sieci SAN	235
Technologie SAN i NAS — ich połączenie i podobieństwa	236
Zastosowanie protokołu Fibre Channel w roli protokołu transportowego	236
Rodzaje kodowania danych w sieciach opartych na protokole Fibre Channel	237
Podstawowe sieci SAN: pętla z arbitrażem	239
Inicjalizacja pętli	241
Arbitraż dostępu do pętli	243
Zastosowanie w sieciach SAN przełączników strukturalnych (ang. Fabric Switches)	244
Połączona topologia pętli i przełączników	247
Sieci IP SAN a iSCSI	249
Jakiego typu urządzenia NAS i sieci SAN powinno się stosować?	251

Część III Protokoły sieciowe niskiego poziomu	255
Rozdział 12. Przyjęte przez IEEE standardy sieci LAN i MAN	257
Czym jest komitet standardów sieci LAN i MAN?	258
Standardy IEEE 802: ogólne pojęcia i architektura	259
IEEE 802.1: mostkowanie i zarządzanie	261
IEEE 802.2: sterowanie łączem logicznym	262
IEEE 802.3: metoda dostępu CSMA/CD	262
IEEE 802.4: metoda dostępu Token-Bus oraz IEEE 802.5: metoda dostępu Token-Ring	263
IEEE 802.7: zalecane praktyki w szerokopasmowych sieciach lokalnych	264
IEEE 802.10: bezpieczeństwo	264
IEEE 802.11: sieci bezprzewodowe	264
Pozyskiwanie dokumentacji standardów IEEE 802 za darmo	265
Rozdział 13. Ethernet, uniwersalny standard	267
Krótka historia Ethernetu	268
Ile różnych rodzajów Ethernetu istnieje?	269
Kolizje: czym są CSMA/CA i CSMA/CD?	272
Algorytm oczekiwania	275
Definiowanie domen kolizyjnych — magistrale, koncentratory i przełączniki	276
Ograniczenia tradycyjnych topologii sieci Ethernet	277
Czynniki ograniczające możliwości technologii ethernetowych	278
Urządzenia połączeń międzysieciowych i długości segmentów przewodów	278
Reguła 5-4-3	279
Stosowanie topologii magistrali	279
Stosowanie topologii gwiazdy	280
Hybrydowe topologie sieci LAN	282
Drzewo	282
Gwiazda hierarchiczna	283
Stosowanie sieci szkieletowych na poziomie korporacji	284
Ramki sieci Ethernet	285
XEROX PARC Ethernet i Ethernet II	286
Standard 802.3	287
Standard sterowania łączem logicznym (LLC), 802.2	287
Standardy Fast Ethernet (IEEE 802.3u) i Gigabit Ethernet (IEEE 802.3z)	290
Fast Ethernet	290
Gigabit Ethernet	293
Standard 10Gigabit Ethernet (IEEE 802.3ae)	294
Problemy w sieciach Ethernet	296
Wskaźniki liczby kolizji	296
Typy kolizji	297
Odstępy próbkowania	298
Ograniczanie liczby kolizji	299
Błędy w sieci Ethernet	300
Wykrywanie prostych błędów	300
Zła wartość FCS lub niedopasowana ramka	301
Krótkie ramki	302
Olbrzymie i niezrozumiałe ramki	303
Błędy wielokrotne	304
Fala rozgłoszeń	304
Monitorowanie wystąpień błędów	304

Część IV Połączenia wydzielone i protokoły sieci WAN 307**Rozdział 14. Połączenia telefoniczne 309**

Protokół punkt-punkt (PPP) oraz protokół IP dla łączy szeregowych (SLIP)	310
Protokół IP dla łączy szeregowych (SLIP)	312
Protokół punkt-punkt (PPP)	314
Ustanawianie połączenia: protokół sterowania łączem (LCP)	317
Protokoły kontroli sieci (NCP)	320
Konfigurowanie połączenia telefonicznego w Windows XP Professional	320
Kiedy połączenie telefoniczne jest zbyt wolne	322

Rozdział 15. Połączenia wydzielone 325

Linie dzierżawione	326
System T-carrier	328
Częściowe T1	329
Diagnozowanie problemów w usługach T-carrier	329
Sieci ATM	331
Ramki ATM	332
Połączenia ATM	334
Model architektury ATM (model B-ISDN/ATM)	335
Emulacja sieci LAN (LANE)	338
Kategorie usług ATM	339
Znaczenie interfejsów Frame Relay i X.25	341
Nagłówki w sieci Frame Relay	342
Sygnalizacja przeciążenia sieci	344
Mechanizm sygnalizacji lokalnego interfejsu zarządzającego (LMI)	345
Stosowanie wirtualnych obwodów komutowanych (SVC)	345
Możliwe problemy w sieciach Frame Relay	346

Rozdział 16. Technologie cyfrowych linii abonenckich (DSL) 349

Modemy DSL i modemy kablowe	350
Różnice topologiczne pomiędzy technologiami sieci kablowych i DSL	351
Krótkie wprowadzenie do publicznych komutowanych sieci telefonicznych	354
xDSL	355
Przyszłość technologii DSL	362

Rozdział 17. Stosowanie modemów kablowych 363

Działanie modemów kablowych	364
Przekazywanie adresów IP dla modemów kablowych	365
Systemy modemów kablowych pierwszej generacji	367
Różnice w działaniu modemów kablowych i szerokopasmowych modemów dostępowych xDSL	367
Specyfikacja DOCSIS (Data Over Cable Service and Interface Specification)	369
Modem kablowy czy DSL?	370

Część V Protokoły sieci bezprzewodowych 371**Rozdział 18. Wprowadzenie do sieci bezprzewodowych 373**

Przyczyny rozprzestrzeniania się sieci bezprzewodowych	375
Punkty dostępowe i sieci ad hoc	377
Sieci ad hoc	378
Stosowanie punktów dostępowych jako elementów pośredniczących w komunikacji bezprzewodowej	379
Technologie fizycznego przesyłania danych	382
Kluczowanie częstotliwości kontra widmo rozproszone	382

Standard sieci bezprzewodowych IEEE 802.11	384
Warstwa fizyczna	384
Warstwa MAC	385
Inne usługi realizowane w warstwie fizycznej	387
Źródła zakłóceń w sieciach bezprzewodowych	387
Rozdział 19. Pionier technologii Wi-Fi: standard IEEE 802.11b	389
Składniki bezprzewodowej sieci opartej na standardach 802.11	389
Standard 802.11b — pierwszy, lecz już przestarzały	390
Kanały 802.11b/g	390
Niestandardowe rozszerzenia standardu 802.11b	390
Czego wymagać od punktu dostępowego?	391
Ograniczenia zasięgu	395
Firewalle	395
Punkty dostępowe z obsługą technologii VPN	396
Czy potrzebujesz sieci bezprzewodowej?	396
Łączenie sieci bezprzewodowej z przewodową siecią LAN	397
Punkty dostępowe pracujące w trybie dualnym	398
Dlaczego technologia Wi-Fi?	399
Rozdział 20. Szybsza usługa: standard IEEE 802.11a	401
Przegląd standardu IEEE 802.11a	402
Zakłócenia powodowane przez inne urządzenia	402
Zwiększona przepustowość w paśmie 5,4 GHz	403
Modulacja sygnału w przypadku standardu 802.11a	404
Kanały standardu 802.11a	405
Niestandardowe rozszerzenia standardu 802.11a	405
Stosowanie sieci bezprzewodowych w miejscach publicznych	405
Problem bezpieczeństwa	407
Porównanie standardów 802.11a, 802.11b i 802.11g	407
Rozdział 21. Standard IEEE 802.11g	409
Przegląd standardu 802.11g	410
Instalacja routera Linksys Wireless-G Broadband Router	412
Instalacja i konfiguracja karty sieci bezprzewodowej	423
Zastosowanie instalacyjnego dysku CD	424
Zastosowanie narzędzia Kreator sieci bezprzewodowej systemu Windows XP z dodatkiem Service Pack 2	427
Niestandardowe rozszerzenia standardu IEEE 802.11g	430
Zwiększanie wydajności sieciowej	432
za pomocą dwupasmowej technologii bezprzewodowej	432
Który protokół bezprzewodowy jest przeznaczony dla Ciebie?	433
Rozdział 22. Bezprzewodowa technologia Bluetooth	435
Grupa Bluetooth SIG (Special Interest Group)	437
Ogólny przegląd technologii Bluetooth	437
Sieci piconet i scatternet	439
Sieci piconet	440
Sieci scatternet	441
Tryby pracy urządzeń Bluetooth	443
Łączy SCO i ACL	443
Łączy SCO	444
Łączy ACL	444
Pakiety Bluetooth	444
Czym są profile Bluetooth?	446
Profil podstawowy GAP	447
Profil Service Discovery Application	449

Profile telefonów bezprzewodowych oraz komunikacji wewnętrznej	449
Profil portu szeregowego	450
Profil słuchawki	450
Profil połączeń telefonicznych	450
Inne profile Bluetooth	451
Bluetooth to więcej niż protokół komunikacji bezprzewodowej	453
Rozdział 23. Zabezpieczenia i inne technologie bezprzewodowe	455
Komunikatory i urządzenia przenośne	455
Porównanie urządzeń mobilnych	456
Osobiste asystenty cyfrowe BlackBerry	457
Bezpieczeństwo komunikacji bezprzewodowej	458
WEP	458
Mechanizmy Wired Protected Access (WPA) i WPA2 oraz standard 802.11i	461
Jak dobrze znasz użytkowników swojej sieci?	465
Sieci osobiste (PAN)	466
Część VI Sieci LAN i WAN, usługi, protokoły i aplikacje	469
Rozdział 24. Przegląd zestawu protokołów TCP/IP	471
TCP/IP i referencyjny model OSI	472
TCP/IP: zbiór protokołów, usług i aplikacji	473
TCP/IP, IP i UDP	474
Inne protokoły pomocnicze	475
Internet Protocol (IP)	476
IP jest bezpołączeniowym protokołem transportowym	477
IP jest protokołem bez potwierdzeń	477
IP nie zapewnia niezawodności	478
IP zapewnia przestrzeń adresową dla sieci	478
Jakie funkcje realizuje IP?	479
Nagłówki datagramu IP	479
Adresowanie IP	482
Address Resolution Protocol — zamiana adresów IP na adresy sprzętowe	494
Proxy ARP	499
Reverse Address Resolution Protocol (RARP)	500
Transmission Control Protocol (TCP)	500
TCP tworzy niezawodne sesje połączeniowe	501
Zawartość nagłówka TCP	501
Sesje TCP	503
Problemy z bezpieczeństwem sesji TCP	510
User Datagram Protocol (UDP)	511
Dane nagłówka UDP	511
Współpraca pomiędzy UDP i ICMP	512
Porty, usługi i aplikacje	513
Porty zarezerwowane	514
Porty zarejestrowane	514
Internet Control Message Protocol (ICMP)	515
Typy komunikatów ICMP	515
Rozdział 25. Podstawowe usługi i aplikacje TCP/IP	519
File Transfer Protocol (FTP)	520
Porty i procesy FTP	521
Przesyłanie danych	522
Polecenia protokołu FTP	523
Odpowiedzi serwera na polecenia FTP	525
Użycie klienta FTP z wierszem poleceń w Windows	526

Użycie FTP w Red Hat Linux	532
Zastosowanie klienta FTP z wierszem poleceń w Red Hat Linux	533
Trivial File Transfer Protocol (TFTP)	536
Protokół Telnet	537
Czym jest wirtualny terminal sieciowy i NVT ASCII?	538
Polecenia protokołu Telnet i negocjacja opcji	539
Telnet a autoryzacja	543
Korzystanie z protokołów Telnet i FTP za firewallem	544
R-utilities	544
Sposób autoryzacji tradycyjnych R-utilities przy dostępie do zasobów sieciowych	545
Narzędzie rlogin	546
Użycie rsh	548
Użycie rcp	550
Użycie rwho	551
Użycie ruptime	551
Program finger	552
Inne usługi i aplikacje korzystające z TCP/IP	554
Bezpieczne usługi sieciowe	555
Rozdział 26. Protokoły poczty internetowej: POP3, SMTP oraz IMAP	557
Jak działa SMTP	558
Model SMTP	560
Rozszerzenia usługi SMTP	561
Polecenia SMTP i kody odpowiedzi	561
Kody odpowiedzi SMTP	564
Łączymy wszystko razem	565
Post Office Protocol (POP3)	566
Stan AUTORYZACJA	567
Stan TRANSAKCJA	567
Stan AKTUALIZACJA	568
Internet Message Access Protocol w wersji 4 (IMAP4)	568
Protokoły transportowe	569
Polecenia klienta	570
Znaczniki systemowe	570
Pobieranie nagłówka i treści przesyłki	570
Formatowanie danych	571
Nazwa skrzynki odbiorczej użytkownika i innych skrzynek	571
Polecenia uniwersalne	571
Pozostałe polecenia IMAP	572
Rozdział 27. Narzędzia diagnostyczne dla sieci TCP/IP	575
Sprawdzanie konfiguracji systemu komputera	575
Użycie polecenia hostname i poleceń pokrewnych	576
Kontrola konfiguracji za pomocą poleceń ipconfig i ifconfig	577
Użycie narzędzi ping i traceroute do sprawdzenia połączenia	582
Polecenie ping	582
Użycie ping w systemach uniksowych i w Linuksie	583
Polecenie traceroute	587
Polecenia netstat i route	591
Polecenie arp	598
Polecenie tcpdump	599
Program WinDump	601
Użycie polecenia nslookup do wyszukiwania problemów z tłumaczeniem nazw	603
Inne użyteczne polecenia	604
Naprawianie połączenia sieciowego w Windows XP	606

Rozdział 28. Protokoły BOOTP i Dynamic Host Configuration Protocol (DHCP)	607
Czym jest BOOTP?	607
Format pakietu BOOTP	608
Mechanizm żądań i odpowiedzi BOOTP	611
Informacje BOOTP specyficzne dla producenta	612
Pobieranie systemu operacyjnego	615
Krok dalej niż BOOTP — DHCP	615
Format pakietu DHCP oraz opcje dodatkowe	618
Wymiana komunikatów między klientem i serwerem DHCP	620
Instalacja i konfiguracja serwera DHCP w Windows 2000/2003	625
Instalacja usługi serwera DHCP w Windows 2000 lub Server 2003	625
Autoryzacja serwera	626
Użycie menu Akcja w MMC	627
Konfiguracja serwera DHCP i opcji zakresu	633
Obsługa klientów BOOTP	636
Uaktywnianie agenta pośredniczącego DHCP	637
Czym jest klastrer DHCP	639
Rozważania na temat DHCP w dużych sieciach lub w sieciach korzystających z routingu	640
Jak DHCP współpracuje z Microsoft Dynamic Domain Name Service (DNS)	640
Rezerwacje i wykluczenia	642
Co to jest APIPA?	644
Rozwiązywanie problemów z Microsoft DHCP	646
Zarządzanie rejestrowaniem	646
Użycie DHCP w Red Hat Linux	648
Demon serwera DHCP	648
Agent przekazujący DHCP	650
Konfigurowanie usług DHCP na routerach i punktach dostępowych WAP	650
Blokowanie połączeń nieautoryzowanych przez filtrowanie adresów fizycznych	652
Rozdział 29. Wyszukiwanie nazw sieciowych	655
Adresy fizyczne a adresy logiczne protokołów	656
NetBIOS	657
Plik lmhosts	657
Windows Internet Name Service	661
Instalacja i konfiguracja WINS w Windows 2000 i 2003 Server	667
Zarządzanie serwerem WINS w Windows 2000	668
Zarządzanie usługą WINS w Windows Server 2003	673
Korzystanie z polecenia netsh do zarządzania serwerem WINS	673
Nazwy w TCP/IP	675
Plik hosts	677
Domain Name System	678
Konfigurowanie klienta DNS	685
Wykorzystanie nslookup	686
Dynamiczny DNS	687
Instalowanie DNS na serwerze Windows	688
Network Information Service	689
Rozdział 30. Korzystanie z usług katalogowych Active Directory	691
Początki technologii katalogowych	692
Różnice pomiędzy katalogiem i usługą katalogową	692
Interesujące obiekty	693
Co umożliwia usługa Active Directory?	694
Rozwój usług katalogowych: od X.500 do LDAP	695
Schemat Active Directory	698
Obiekty i atrybuty	699
Standardowe obiekty Active Directory	700

Czym jest drzewo domen, a czym las?	702
Modele domen — niech spoczywają w pokoju	702
Podział Active Directory na domeny	703
Domena wciąż jest domeną	704
Drzewa i lasy Active Directory	704
Active Directory i dynamiczny DNS	705
Dynamiczny DNS	706
Jak Active Directory korzysta z DNS?	706
Zarządzanie dużymi sieciami przedsiębiorstw za pomocą lokacji	707
Replikacja katalogu	708
Podsumowanie danych katalogowych w wykazie globalnym	709
Active Directory Service Interfaces (ADSI)	710
Programowanie aplikacji współpracujących z katalogiem	710
Zostały tylko kontrolery domen i serwery członkowskie	711
Schemat Active Directory	712
Modyfikacje schematu Active Directory	712
Znajdowanie obiektów w Active Directory	721
Znajdowanie konta użytkownika	722
Wyszukiwanie drukarki w Active Directory	725
Funkcja Wyszukaj w menu Start	726
Usługa Active Directory w Windows Server 2003	727
Nowe elementy Active Directory w Windows Server 2003	727
Instalacja Active Directory na komputerze z systemem Windows Server 2003	728
Rozdział 31. Protokoły serwera plików	735
Znaczenie protokołów serwerów plików	735
Server Message Block (SMB) i Common Internet File System (CIFS)	737
Typy komunikatów SMB	737
Mechanizmy zabezpieczeń w SMB	738
Negocjacja protokołu i nawiązanie sesji	740
Dostęp do plików	741
Polecenia NET	744
Monitorowanie i rozwiązywanie problemów z SMB	747
Protokół SMB/CIFS w klientach innych niż produkowanych przez Microsoft: Samba	750
Protokół CIFS	751
NetWare Core Protocol (NCP)	752
Ogólne żądania i odpowiedzi	753
Tryb strumieniowy	753
Trwa przetwarzanie żądania	754
Zakończenie połączenia	754
Network File System (NFS) w systemach Unix	754
Komponenty protokołu: protokół RPC	755
External Data Representation (XDR)	756
Protokoły NFS i Mount	757
Konfiguracja serwerów i klientów NFS	759
Demony klientów NFS	759
Demony serwerowe	762
Rozwiązywanie problemów z NFS	768
Rozproszony system plików DFS firmy Microsoft	770
Tworzenie katalogu głównego DFS	771
Dodawanie łącz do katalogu głównego DFS	772
Rozdział 32. Protokół HTTP	775
Początki protokołu HTTP	776
HTTP z bliska	777
Mechanika HTTP	777
Pola nagłówka HTTP	778
URL, URI i URN	778

Rozdział 33. Protokoły routingu	783
Podstawowe typy protokołów routingu	784
Protokół RIP	784
Protokół OSPF (Open Shortest Path First)	790
Multi-Protocol Label Switching (MPLS)	792
Połączenie routingu i przełączania	793
Etykietowanie	793
Współpraca Frame Relay i ATM z MPLS	794
Rozdział 34. Protokół SSL	795
Szyfrowanie symetryczne i asymetryczne	796
Certyfikaty cyfrowe	797
Procedura wymiany potwierdzeń SSL	797
Ochrona przed przechwyceniem dzięki certyfikatom	798
http:// i https://	799
Dodatkowa warstwa w stosie protokołów sieciowych	799
Czy SSL zapewnia wystarczające bezpieczeństwo transakcji internetowych?	800
Otwarte wersje SSL	800
Rozdział 35. Wprowadzenie do protokołu IPv6	801
Czym różnią się protokoły IPv4 i IPv6?	802
Nagłówki IPv6	803
Nagłówki dodatkowe IPv6	804
Pole „Typ opcji” dla nagłówków „Skok po skoku” i „Opcje odbiorcy”	806
Inne zagadnienia związane z IPv6	807
Przyszłość IPv6	807
Część VII Zarządzanie zasobami sieciowymi i użytkownikami	809
Rozdział 36. Domeny Windows NT	811
Grupy robocze i domeny	812
Międzydomenowe relacje zaufania	814
Kontrolery domen	817
Modele domen Windows NT	818
Grupy użytkowników Windows NT	821
Wbudowane grupy użytkowników	821
Tworzenie grup użytkowników	823
Specjalne grupy użytkowników	824
Zarządzanie kontami użytkowników	824
Dodawanie użytkownika do grupy	826
Profile użytkowników	826
Ograniczenie godzin logowania użytkownika	827
Ograniczanie stacji roboczych, do których użytkownik może się logować	827
Dane konta	828
Dopuszczenie dostępu przez łącza telefoniczne	829
Replikacja pomiędzy kontrolerami domen	829
Hasła i zasady	831
Wykrywanie nieudanych prób zalogowania	833
Strategie minimalizacji problemów z logowaniem	834
Rozdział 37. Narzędzia do zarządzania użytkownikami i komputerami w systemach Windows 2000 i Windows Server 2003	835
Microsoft Management Console	835
Zarządzanie użytkownikami	836
Tworzenie nowych kont użytkowników w Active Directory	836
Zarządzanie innymi informacjami w kontach użytkowników	839
Menu Action	842

Zarządzanie komputerami	843
Dodawanie komputera do domeny	844
Zarządzanie innymi danymi kont komputerów	845
Grupy użytkowników Windows 2000	847
Wybór grupy na podstawie zasięgu grupy	847
Grupy wbudowane	849
Tworzenie nowej grupy użytkowników	852
Co jeszcze można zrobić z przystawką Użytkownicy i komputery usługi Active Directory?	853
Rozdział 38. Zarządzanie użytkownikami systemów Unix i Linux	855
Zarządzanie użytkownikami	855
Plik /etc/passwd	856
Chroniony plik hasel	858
Plik /etc/groups	859
Dodawanie i usuwanie kont użytkowników	859
Zarządzanie użytkownikami w systemie Linux z GUI	862
Network Information Service (NIS)	867
Główne i podrzędne serwery NIS	867
Mapy NIS	867
Demon ypserve serwera NIS i lokalizacja map	869
Ustawienie nazwy domeny NIS za pomocą polecenia domainname	869
Uruchomienie NIS: ypinit, ypserve i ypxfrd	870
Serwery podrzędne NIS	871
Zmiany w mapach NIS	872
Wysyłanie modyfikacji do serwerów podrzędnych NIS	872
Inne przydatne polecenia YP usługi NIS	872
Klienty NIS	873
Najczęściej spotykane problemy z logowaniem	873
Rozdział 39. Prawa i uprawnienia	875
Zabezpieczenia na poziomie użytkownika i udziału	876
Zabezpieczenia na poziomie udziału w systemach Microsoft Windows	877
Przyznawanie praw użytkownika w Windows 2000, Server 2003 i XP	879
Zarządzanie zasadami hasel użytkowników	886
Standardowe i specjalne uprawnienia NTFS	888
Uprawnienia w systemie Windows są kumulatywne	892
Grupy użytkowników ułatwiają zarządzanie prawami użytkowników	892
Grupy użytkowników w Windows 2000 i Windows Server 2003	893
Grupy w Active Directory	895
NetWare	897
Dysponenci	897
Prawa w systemie plików	898
Prawa do obiektów i właściwości	898
Różnice pomiędzy prawami w NDS i prawami do systemu plików i katalogów	899
Dziedziczenie praw	900
Grupy Everyone i [Public]	901
Unix i Linux	902
Przeglądanie uprawnień do plików	903
Uprawnienia do plików SUID i SGID	904
Polecenie su	906
Rozdział 40. Sieciowe protokoły drukowania	907
Protokoły drukowania i języki drukowania	908
Korzystanie z lpr, lpd i protokołów strumieniowych TCP	909
Data Link Control Protocol (DLC)	909

Internet Printing Protocol (IPP)	910
Typy obiektów IPP	912
Operacje IPP	912
Co nowego w wersji 1.1?	913
Gdzie można znaleźć IPP?	914
Rozdział 41. Serwery druku	915
Drukowanie w systemach Unix i Linux	915
System kolejowania BSD	916
System drukowania SVR4	926
Konfiguracja serwerów druku Windows	933
Drukarki i urządzenia drukujące	933
Instalowanie i konfiguracja drukarek w serwerach Windows	935
Windows NT 4.0	935
Windows 2000 Server	943
Windows XP	957
Drukowanie w NetWare	961
Właściwości obiektu Print Queue	963
Właściwości obiektu Printer	964
Właściwości obiektu Print Server	965
PSEVER.NLM i NPRINTER.NLM	966
Narzędzie NetWare 6.x iPrint	966
Sprzętowe serwery drukarek	967
Część VIII Zabezpieczenia systemów i sieci	971
Rozdział 42. Podstawowe środki bezpieczeństwa,	
 które każdy administrator sieci znać powinien	973
Zasady i procedury	973
Zasady podłączania do sieci	974
Dopuszczalne zastosowania i wytyczne użytkowania	975
Procedury reagowania	978
Co powinno zostać uwzględnione w zasadach bezpieczeństwa	979
Zabezpieczenia fizyczne	981
Zamykanie drzwi	981
Zasilacze awaryjne (UPS)	982
Bezpieczna likwidacja sprzętu i nośników	982
Bezpieczeństwo z dwóch stron	982
Przed faktem: kontrola dostępu	983
Po fakcie: kontrole użytkowania	985
Hasła	986
Demony i usługi systemowe	988
Usuwanie zbędnego balastu	990
Delegowanie uprawnień	990
Konta użytkowników	991
Serwery aplikacji, serwery druku i serwery WWW	991
Nie zapominaj o firewallach	992
Rozdział 43. Inspekcje i inne środki monitorowania	993
Systemy Unix i Linux	994
Praca z narzędziem syslog	995
Pliki dziennika systemowego	998
Konfiguracja zasad inspekcji w Windows NT 4.0	999
Wybór zdarzeń do kontroli	999
Windows NT 4.0 Event Viewer	1002

Konfiguracja zasad inspekcji w Windows 2000 i Windows Server 2003	1003
Włączenie inspekcji dla plików i folderów	1005
Inspekcje drukarek	1008
Rejestrowanie zdarzeń zamknięcia i uruchomienia systemu Windows Server 2003	1009
Korzystanie z Podglądu zdarzeń	1010
Inspekcje komputerów Windows XP Professional	1012
Zabezpieczenia w systemach Novella	1014
SYSCON i AUDITCON	1014
Audyty w NetWare	1016
Rozdział 44. Zagadnienia bezpieczeństwa w sieciach rozległych	1019
Zostałeś namierzony!	1021
Wirusy komputerowe, konie trojańskie i inne niszczące programy	1022
Konie trojańskie	1023
Wirusy	1024
Jak dochodzi do infekcji	1025
Sieć pod ostrzałem — najczęstsze ataki	1026
Ataki typu „odmowa usługi”	1027
Rozproszony atak typu „odmowa usługi”	1027
Atak typu SYN flooding	1029
Przekierowania ICMP	1030
Ping of Death	1031
Fałszywe przesyłki pocztowe	1031
Ochrona haseł, SecurID oraz karty elektroniczne	1032
„Furtki” w sieci	1033
Sondy sieciowe	1034
Podszywanie i naśladownictwo	1035
Jeżeli coś jest zbyt dobre, aby było prawdziwe, na pewno takie nie jest	1035
Działania prewencyjne	1036
Zabezpieczanie routerów	1036
Sieć jako cel	1036
Zabezpieczanie komputerów — szyfrowanie i oprogramowanie antywirusowe	1037
Wykorzystanie Tripwire	1038
Świadomość i wyszkolenie użytkowników	1039
Stałe poznawanie zagadnień bezpieczeństwa	1040
Rozdział 45. Firewall	1041
Czym jest firewall?	1041
Filtrowanie pakietów	1043
Filtrowanie adresów IP	1044
Filtrowanie w oparciu o protokoły	1044
Filtrowanie oparte na numerach portów	1046
Filtrowanie z pamięcią stanu	1048
Filtrowanie bazujące na aplikacjach	1048
Zapora Windows kontra programowe firewalle firm trzecich	1049
Serwery pośredniczące	1051
Standardowe zastosowania serwera pośredniczącego	1055
Ukrywanie użytkowników końcowych:	
mechanizm translacji adresów sieciowych (NAT)	1058
Zalety i wady serwera pośredniczącego	1060
Rozbudowane firewalle	1060
Czego należy oczekiwać od firewalla?	1062
Tanie firewalle dla małych firm	1064
Rozwiązania sprzętowe	1065
Rozwiązania programowe	1066
Jednoczesne stosowanie firewalli sprzętowych i programowych	1067
Skąd wiadomo, że dany firewall jest bezpieczny?	1068

Rozdział 46. Wirtualne sieci prywatne (VPN) i tunelowanie	1069
Co to jest VPN?	1069
Mobilna siła robocza	1070
Protokoły, protokoły, jeszcze więcej protokołów!	1071
Protokoły IPsec	1071
Internet Key Exchange (IKE)	1072
Authentication Header (AH)	1073
Encapsulation Security Payload (ESP)	1075
Point-to-Point Tunneling Protocol (PPTP)	1076
Layer Two Tunneling Protocol (L2TP)	1077
Wbudowywanie pakietów L2TP	1078
Tworzenie połączenia VPN w systemie Windows XP Professional	1078
Definiowanie i stosowanie połączenia VPN w systemie Windows XP	1079
Rozwiązywanie problemów z połączeniem VPN	1082
Wybieranie routera obsługującego połączenia VPN	1083
Rozdział 47. Technologie szyfrowania	1085
Komputery i prywatność	1085
Co to jest szyfrowanie?	1086
Szyfrowanie pojedynczym kluczem — szyfrowanie symetryczne	1086
Szyfrowanie kluczem publicznym	1088
Kryptografia klucza publicznego RSA	1090
Certyfikaty cyfrowe	1090
Pretty Good Privacy (PGP)	1092
Część IX Rozwiązywanie problemów z siecią	1093
Rozdział 48. Strategie rozwiązywania problemów w sieciach	1095
Dokumentacja sieci przydaje się przy rozwiązywaniu problemów	1095
Utrzymanie aktualności dokumentacji	1098
Techniki rozwiązywania problemów	1101
Cykl rozwiązywania problemu	1101
Monitorowanie sieci w celu lokalizacji źródeł problemów	1105
Pułapki przy rozwiązywaniu problemów	1105
Rozdział 49. Narzędzia do testowania i analizowania sieci	1107
Podstawy: testowanie kabli	1107
Ręczne testy połączeń	1108
Testery kabli	1109
Testery bitowej stopy błędów	1109
Reflektometria w domenie czasu	1110
Impedancja	1111
Szerokość impulsu	1111
Prędkość	1112
Analizatory sieci i protokołów	1112
Ustalenie poziomu odniesienia	1113
Dane statystyczne	1115
Dekodowanie protokołów	1115
Filtrowanie	1115
Analizatory programowe	1116
Inne programowe analizatory sieci	1120
Analizatory sprzętowe	1121
Protokół SNMP	1122
Operacje elementarne SNMP	1123
Obiekty sieciowe: baza MIB	1123
Agenty pośredniczące	1125
Wyboista droga do SNMPv2 i SNMPv3	1126
RMON	1128

Rozdział 50. Rozwiązywanie problemów w małych sieciach biurowych i domowych	1131
Kłopoty z zasilaniem	1132
Problemy z konfiguracją komputerów	1135
Problemy z komponentami	1140
Chroń kable!	1141
Problemy z firewallami	1142
Higiena sieci	1143
Problemy z sieciami bezprzewodowymi	1144
Gdy nic innego nie pomoże... ..	1146
Część X Modernizacja sprzętu sieciowego	1147
Rozdział 51. Modernizacja starszych sieci Ethernet	1149
Przejście z technologii 10BASE-2 lub 10BASE-T	1150
Elementy sprzętowe i programowe powiązane z technologiami 10BASE-2, 10BASE-T i 100BASE-T	1151
Kable sieciowe	1153
Karta sieciowa	1155
Złącza kabli sieciowych	1156
Mosty, koncentratory, repeatery i przełączniki	1157
Łączenie sieci opartych na różnym okablowaniu lub topologiach	1158
Inne rozwiązania	1159
Zastosowanie w sieci szkieletowej technologii Gigabit Ethernet	1159
Umieszczenie zaawansowanych serwerów w sieci Gigabit Ethernet	1160
Połączenie ze stacjami roboczymi oparte na technologii Gigabit Ethernet	1160
Zastosowanie technologii Gigabit Ethernet na dużych odległościach	1161
Technologia 10Gigabit Ethernet pod względem finansowym staje się coraz bardziej przystępna	1161
Rozdział 52. Zamiana mostów i koncentratorów na routery i przełączniki	1163
Zwiększanie rozmiaru sieci lokalnej	1164
Segmentacja sieci może zwiększyć jej wydajność	1166
Łączenie zdalnych lokacji	1167
Zamiana mostów na routery	1168
Zagadnienia dotyczące protokołu sieciowego	1169
Zagadnienia dotyczące adresów sieciowych	1169
Inne zagadnienia dotyczące zarządzania routerem	1170
Zastosowanie routera do segmentacji sieci	1171
Połączenie z większą siecią rozległą lub internetem	1172
Zamiana mostów na przełączniki	1173
Rozdział 53. Zastosowanie bezprzewodowych sieci lokalnych	1177
Dlaczego warto zastosować technologię sieci bezprzewodowych?	1178
Wybieranie lokalizacji dla punktów dostępowych	1180
Kwestie bezpieczeństwa	1182
Część XI Migracja i integracja	1185
Rozdział 54. Migracja z systemu NetWare do systemu Windows 2000 lub Windows 2003	1187
Protokoły i usługi systemu Windows	1188
Client Services for NetWare (CSNW)	1189
Gateway Services for NetWare (GSNW)	1190

Oprogramowanie Services for NetWare Version 5.0 (SFN)	1195
Porównanie uprawnień plików systemów Windows Server i NetWare	1196
Instalacja narzędzia File and Print Services for NetWare Version 5.0 (FPNW 5.0)	1198
Microsoft Directory Synchronization Services (MSDSS)	1202
Narzędzie File Migration Utility (FMU)	1208

Rozdział 55. Migracja między systemami Windows NT, Windows 2000, Windows 2003, Unix i Linux oraz integracja tych systemów1213

Protokoły i narzędzia uniksowe na serwerach Windows	1214
Protokoły TCP/IP	1215
Usługa Telnet	1216
Usługa FTP (File Transfer Protocol)	1224
Zarządzanie usługą FTP w systemie Windows Server 2003	1226
Protokoły DHCP (Dynamic Host Configuration Protocol) i BOOTP	1229
Usługa DNS	1231
Aplikacje	1232
Windows Services for Unix 3.0 firmy Microsoft	1233
Instalacja pakietu SFU 3.5	1235
Usługa NFS (Network File System)	1238
Powłoka Korn Shell	1239
Komponent Password Synchronization	1242
Komponent User Name Mapping	1243
Nowy serwer i klient usługi Telnet	1244
Komponent ActiveState ActivePerl 5.8	1245
Samba	1246
Network Information System	1246

Rozdział 56. Migracja z systemu Windows NT 4.0 do systemów Windows 2000, Windows 2003 i Windows XP1249

Czy konieczna jest aktualizacja systemu operacyjnego lub aplikacji?	1250
Aktualizacja do systemu Windows 2000 Server	1254
Zanim zaczniesz	1256
Kontrolery domeny Windows NT i serwery członkowskie	1256
Modelowanie struktury usługi katalogowej przy uwzględnieniu organizacji firmy	1258
Domeny będące partycjami usługi Active Directory	1259
Aspekty związane z migracją — porównanie administracji scentralizowanej ze zdecentralizowaną	1260
Wdrażanie usługi Active Directory	1262
Aktualizacja podstawowego kontrolera domeny	1263
Dodawanie innych domen do struktury usługi Active Directory	1265
Najpierw uaktualnij domenę główną	1266
Aktualizacja kolejnych zapasowych kontrolerów domeny	1269
Migracja z systemu Windows NT 4.0 lub systemu Windows 2000 do systemu Windows Server 2003	1270
Wymagania sprzętowe związane z aktualizacją do systemu Windows Server 2003	1271
Zestaw aplikacji sprawdzający zgodność oprogramowania	1273
Jaką rolę będzie spełniał serwer?	1274
Przykład aktualizacji systemu Windows 2000 Server do systemu Windows Server 2003 Enterprise Edition	1274
Zostać przy Windows 2000 Professional czy przejść na Windows XP Professional?	1278
Aktualizacja klientów stosowanych w małych biurach	1278

Rozdział 57. Migracja między systemami NetWare, Unix i Linux

oraz integracja tych systemów	1281
Dlaczego warto użyć systemu Unix lub Linux?	1281
Kluczowe różnice pomiędzy systemami Unix/Linux i NetWare	1282
Udostępnianie plików	1283
Udostępnianie drukarek	1283
Autoryzacja użytkowników	1284
Przenoszenie kont użytkowników	1284
Protokoły sieciowe	1285
Aplikacje	1285
Szukanie sterowników urządzeń dla systemu Linux	1288
Novell Open Enterprise Server	1289

Dodatki 1291**Dodatek A Siedmiowarstwowy referencyjny model sieci OSI 1293**

To tylko model!	1293
Kapsułkowanie	1294
Warstwa fizyczna	1295
Warstwa łącza danych	1295
Warstwa sieci	1295
Warstwa transportowa	1296
Warstwa sesji	1296
Warstwa prezentacji	1296
Warstwa aplikacji	1297

Dodatek B Słownik terminów sieciowych 1299**Dodatek C Zasoby internetu przydatne administratorom sieci 1337**

Organizacje standaryzujące	1337
Producenci sprzętu i oprogramowania sieciowego	1338
Sieci bezprzewodowe	1342
Bezpieczeństwo	1343

Dodatek D Protokół Lightweight Directory Access Protocol 1349

Wprowadzenie do LDAP	1349
Protokoły i standardy X.500	1350
Skróty, skróty, skróty!	1351
Schemat	1353
Lightweight Directory Access Protocol	1353
Protokół LDAP	1354
Podłączanie do serwera	1355
Przeszukiwanie bazy danych	1355
Dodawanie, modyfikowanie lub usuwanie informacji z katalogu	1356
Porównywanie danych w katalogu	1356
Katalogi LDAP	1356
Windows 2000 Server, Windows Server 2003 i NetWare	
nie są jedynymi produktami do wyboru	1357
Zgodność ze standardem: współpraca między katalogami	1357

Dodatek E Wprowadzenie do budowania sieci w małym biurze 1359

Definiowanie wymagań: czego potrzebujesz?	1360
Zakup sprzętu dla aplikacji	1362
Topologie małych sieci	1367
Archiwizacja dla małych firm	1370

Skorowidz 1373

Rozdział 5.

Ochrona sieci: metody zapobiegania zagrożeniom

W tym rozdziale przyjrzymy się kilku ważnym ochronnym metodom zapobiegawczym, które można zastosować w sieci. Wielkość i budowa sieci będą miały wpływ na wybór jednej z metod omawianych w niniejszym rozdziale. Nie wszystkie metody są odpowiednie dla każdej sieci. Niektóre z nich — ze względu na wysoki koszt — nie nadają się do niewielkich sieci. Ponadto należy pamiętać, że podobnie do planowania rozbudowy samej sieci można również planować modernizację procedur i urządzeń chroniących sieć przed awariami i utratą danych.

Stabilizacja napięcia i zasilacze awaryjne UPS (Uninterruptible Power Supplies)

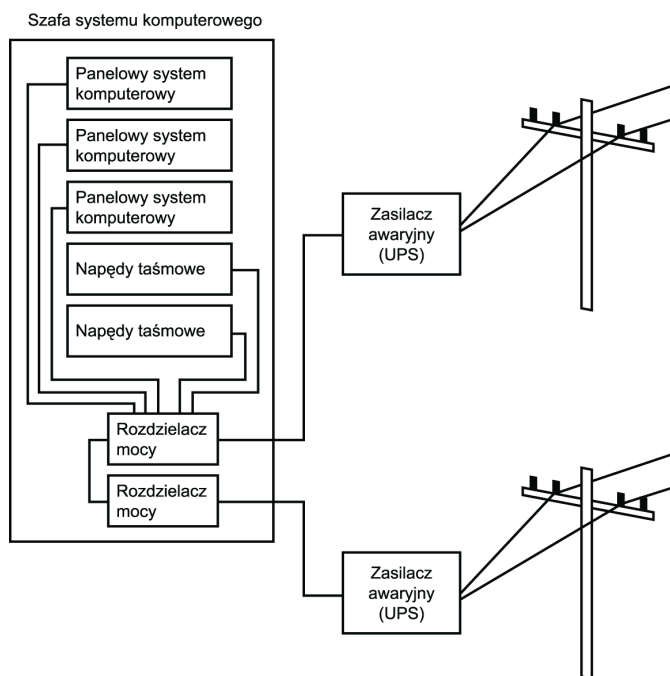
Bez prądu żadna sieć nie będzie w ogóle działała, natomiast w celu poprawnego funkcjonowania komputery wymagają stabilnego źródła napięcia. Zasilacz komputera może nie wytrzymać odebranego skoku napięcia, spowodowanego na przykład piorunem. Podobnie krótkotrwały spadek napięcia może doprowadzić do „zawieszenia się” komputera, a więc i utraty danych.

Duże systemy komputerowe stosowane w środowiskach korporacyjnych, takie jak średniej klasy serwery oraz komputery przemysłowe, również wymagają stabilnego źródła zasilania. W celu jego zapewnienia w większości dużych pomieszczeń komputerowych stosowane są duże zasilacze awaryjne UPS, których zadaniem jest pośredniczenie pomiędzy zewnętrznym źródłem zasilania a komputerami oraz innymi urządzeniami w serwerowni.

Przykładowo w większości przestronnych serwerowni komputery — niezależnie od tego, czy są to serwery PC czy większe systemy — są umieszczane w szafach panelowych wraz z napędami taśmowymi, dyskami oraz innymi urządzeniami peryferyjnymi. Szafa zawiera zazwyczaj jeden lub kilka rozdzielaczy mocy (PDU), zasilających zamontowane w niej urządzenia (rysunek 5.1).

Rysunek 5.1.

W celu zapobieżenia awarii zasilania sieci elementy zasilające są dublowane



Na rysunku można zauważyć, że kilka używanych systemów komputerowych i napędów taśmowych umieszczono w jednej szafie. Dwa rozdzielacze mocy znajdujące się na dole szafy doprowadzają napięcie do wszystkich urządzeń w niej umieszczonych. Rozdzielacze są wzajemnie nadmiarowe, dzięki czemu w sytuacji, gdy jeden z nich ulegnie awarii, drugi będzie w dalszym ciągu doprowadzać napięcie do urządzeń. Każdy z rozdzielaczy mocy jest podłączony do oddzielnego zasilacza awaryjnego UPS, znajdującego się w pomieszczeniu. Jest to ważne z kilku powodów. Po pierwsze, nie wszystkie awarie zasilania wynikają z zewnętrznych problemów, takich jak wyłączona linia przesyłowa. Czasem awarii ulegnie sam zasilacz awaryjny. W trakcie rutynowych czynności konserwacyjnych lub instalacyjnych elektryk może odłączyć niewłaściwy kabel. Mysz może przegryźć przewody, powodując zwarcie. Mogą się zdarzyć przeróżne rzeczy, dlatego powinniśmy „oczekiwać nieoczekiwanego”.

Aby nadmiarowość sięgała dalej, każdy zasilacz awaryjny znajdujący się w serwerowni i używany przez systemy jest podłączony do niezależnego zewnętrznego źródła zasilania. A zatem jeśli złamie się drzewo i uszkodzona zostanie w ten sposób jedna linia zasilania, to w dalszym ciągu będzie dostępna dodatkowa linia, która za pośrednictwem drugiego zasilacza awaryjnego doprowadzi napięcie do urządzeń. Dzięki zapasowemu źródłu zasilania komputery i inne urządzenia podłączone do sieci nadal będą działały.

Energia to pieniądze

Istnieje takie stare powiedzenie: „pieniądze dają władzę”¹. Odwrotna sytuacja również jest prawdziwa.

¹ W oryginale („power is money” i „money is power”) gra słów, polegająca na wieloznaczności słowa „power”, które oznacza zarówno władzę, jak i energię elektryczną — *przyp. tłum.*

Schemat przytoczony w poprzednim podrozdziale może wydać się przesadny dla administratora niewielkiej sieci złożonej z kilku komputerów PC, w której przestoje są dopuszczalne. Jednak w przypadku środowiska komputerowego, w którym wymagana jest bardzo wysoka dostępność — takiego, jak sieć dużej korporacji — koszt przestoju może być wyjątkowo wysoki z kilku powodów:

- ♦ Setki, a nawet tysiące pracowników stanie się bezproduktywnych, gdy komputery, których używają, będą pozbawione zasilania. Pracownicy w dalszym ciągu będą opłacani, nawet gdy nie będą mogli wykonywać swoich obowiązków. Dodaj złotówkę do złotówki i dojdiesz do wniosku, że każda minuta przestoju jest dość kosztowna.
- ♦ Klienci mogą nie być w stanie składać zamówień lub sprawdzać stanu realizacji zamówień już istniejących. Mniej lojalni klienci mogą po prostu zadzwonić do kogoś innego. Nikt nie lubi słyszeć: „właśnie teraz nasz serwer jest odłączony, proszę zadzwonić później”. Po tym, jak klient skontaktuje się z innym dostawcą, możesz nawet już nigdy więcej się z nim nie spotkać. W efekcie stracisz nie tylko aktualne zamówienia, ale i wszystkie te, które mogły pojawić się w przyszłości.
- ♦ Niespodziewana awaria systemu spowodowana zanikiem zasilania może doprowadzić do uszkodzenia danych. Po przywróceniu zasilania identyfikacja uszkodzonych plików, a następnie ich przywrócenie do poprzedniego stanu z kopii zapasowych zapisanych na taśmach może czasem zająć wiele godzin, a nawet dni. Obecnie wiele dużych sieci, takich jak te należące do dostawców usług internetowych, zawiera dane o wielkości wyrażanej w terabajtach. Przywrócenie całej bazy danych może być bardzo kosztowne i czasochłonne. Taki dodatkowy przestój prawdopodobnie może kosztować więcej niż sama awaria zasilania, która do niego doprowadziła.

Jeśli masz do czynienia z tak wielkim środowiskiem, prawdopodobnie jesteś już świadom znaczenia gwarantowania ciągłej dostępności systemów komputerowych. Jeśli nie zadbasz o stabilne i pewne źródło zasilania, to wszystkie inne ochronne metody zapobiegawcze mogą przedstawiać niewielką wartość, gdy następnym razem dojdzie do zaniku napięcia.

Zasilacz awaryjny nie jest nieskończonym źródłem zasilania. Spełnia on rolę przewodu, przez który zewnętrzne źródło zasilania przesyła napięcie do systemów komputerowych. Działanie zasilaczy awaryjnych UPS polega na magazynowaniu energii w jednej lub kilku bateriach, dzięki czemu po nieoczekiwanej awarii zewnętrznego źródła zasilania w ciągu kilku milisekund mogą one przejść na zasilanie z baterii. Jednak baterie mogą być używane tylko przez określony czas. Jeśli jest używany tylko jeden zasilacz awaryjny, podłączony do jedynego źródła zasilania, pozwoli on na powiadomienie użytkowników o konieczności wylogowania się z systemów przez niego zasilanych oraz wyłączenie ich w sposób nie zagrażający uszkodzeniu danych. Co prawda nadal spowoduje to bezproduktywne oczekiwanie pracowników, ale nie pojawi się konieczność przywracania danych po usunięciu awarii zasilania.

W przypadku dużych sieci należy zaplanować dodatkowy poziom zabezpieczenia na wypadek zaniku zasilania, czyli generatory prądu oparte na silniku Diesla. Co prawda zasilanie przy ich użyciu dużej liczby stacji roboczych użytkowników byłoby zbyt kosztowne, ale mogą one posłużyć do podtrzymania pracy serwerów oraz rezerwowej pracowni, do której użytkownicy (przynajmniej najważniejsi) powinni się przenieść na czas awarii.

Przykładowo w większości sytuacji nie wszystkie aplikacje sieciowe odgrywają krytyczną rolę i muszą być dostępne przez 24 godziny na dobę i siedem dni w tygodniu. A zatem w zapasowe zasilanie powinny być wyposażone wyłącznie serwery o bardzo dużym znaczeniu. Jeśli masz do czynienia przykładowo z firmą handlową, to będzie Ci zależało na utrzymaniu dostępności serwerów (np. serwer WWW), które obsługują klientów. Inne aplikacje, takie jak edytor tekstu używany przez dział prawny czy dział realizujący inne zadania, mogą zostać przywrócone do działania później.

Interfejs ACPI (Advanced Configuration and Power Interface) a niezależne systemy zasilaczy awaryjnych UPS

W przypadku komputerów PC i niewielkich serwerów wystarczający będzie zakup niedrogich zasilaczy awaryjnych UPS, wartych kilkaset złotych. Mogą one być zastosowane w środowisku, w którym przestój jest dopuszczalny, ale uszkodzenie danych już nie. Konfiguracja typowego zasilacza awaryjnego, produkowanego np. przez firmę APC (American Power Conversion Corp), zajmuje zaledwie kilka minut. W zależności od modelu może on oferować zarówno zasilanie z baterii, jak i wybrane funkcje stabilizacji napięcia.

Trzeba wziąć pod uwagę, że stabilizatory i listwy przeciwprzebiegowe, choć mają uniemożliwiać przenikanie przebiegów do chronionych systemów, nie zawsze działają zgodnie z zapewnieniami producenta. Tanie modele nabywane w niespecjalistycznych sklepach zazwyczaj nie oferują ochrony, o której wspominają producenci. Jeśli całe zabezpieczenie ma się opierać na prostym bezpieczniku, to przy jego zakupie należy odłożyć pieniądze na zakup nowego komputera — będzie potrzebny po najbliższym silnym wyładowaniu atmosferycznym. Tam gdzie nie ma miejsca dla rozbudowanych systemów UPS, realnym zabezpieczeniem może być jedynie prosty zasilacz awaryjny chroniący serwer czy inne ważne urządzenia sieciowe.



Należy mieć świadomość, że wszystkie urządzenia podłączone do komputera również muszą być chronione przed przebiegami itp. Jeśli Twój komputer został podłączony do zasilacza UPS oferującego taką ochronę, ale monitor i modem kablowy są podłączone bezpośrednio do gniazdka, a dopiero potem do komputera, to będziesz miał jedynie fałszywe poczucie bezpieczeństwa. W domu czy małym biurze z kablowym dostępem do internetu uderzenie pioruna w zewnętrzną instalację kablową może spowodować przeniesienie udaru przez okablowanie, a potem przez modem kablowy wprost do wnętrza komputera. Innymi słowy, wszystkie urządzenia podłączone do komputera wszelkimi sposobami powinny również być chronione zasilaczami awaryjnymi albo innymi porządnymi zabezpieczeniami.

Aby po zaniku napięcia i przejściu na zasilanie z baterii możliwe było poprawne zamknięcie systemu operacyjnego, kilka firm (najważniejsze z nich to Intel, Microsoft, a także inni producenci) opracowało interfejs ACPI (ang. *Advanced Configuration and Power Interface*). Interfejs ACPI jest dość obszerny i swoim zakresem obejmuje zarządzanie energią w laptopach i innego typu komputerach. Jednak interfejs ten oferuje też standardową metodę komunikacji niezależnego zasilacza awaryjnego z komputerem i w chwili, gdy UPS przełącza się na zasilanie z baterii, wymuszane jest wyłączenie systemu w sposób bezpieczny dla danych.



W celu uzyskania dodatkowych informacji na temat specyfikacji i innych danych dotyczących sposobu współpracy interfejsu ACPI z BIOS-em komputerów należy zajrzeć na stronę internetową znajdującą się pod adresem <http://acpi.info>. Na stronie zawarto też kilka narzędzi, takich jak kompilatory, które umożliwiają zastosowanie języka ASL (*ACPI Source Language*), służącego do tworzenia kodu zapisywanego w układach instalowanych na płycie głównej komputera. Co prawda czytanie informacji zawartych na stronie nie należy do przyjemności, ale zalecane jest to dla osób, które lubią wiedzieć, jak dane urządzenie działa. Na stronie zawarto też dekompilekator, który może posłużyć do zamiany kodu maszynowego zapisanego w układzie z powrotem na kod języka ASL, co ma na celu uproszczenie jego analizy. Interfejs ACPI jest też dostosowywany do komputerów pracujących pod kontrolą systemu Linux. Dodatkowe informacje na ten temat można znaleźć na stronie <http://acpi.sourceforge.net/>.

Interfejs ACPI nie jest ograniczony wyłącznie do zewnętrznych zasilaczy awaryjnych. Specyfikacja uwzględnia też inne funkcje związane z zarządzaniem energią, które obecnie są standardowo obsługiwane przez większość systemów operacyjnych. Przykładowo jeśli w panelu sterowania systemów Windows 2000/XP/Server 2003 zostanie otwarte okno *Opcje zasilania*, to ustawienia, które można tam modyfikować, są powiązane z interfejsem ACPI. Kolejna interesująca funkcja zapewniana przez ACPI to uruchamianie komputera poprzez naciśnięcie dowolnego klawisza.

Komunikacja ta realizowana jest przez przyłączenie kabla zasilającego komputera do zasilacza awaryjnego, a także przez połączenie zasilacza i komputera specjalnym kablem szeregowym (albo kablem USB), a potem uruchomienie obsługi zasilacza awaryjnego w systemie operacyjnym. W systemach Windows 2000 i Windows Server 2003 tego typu usługa współpracuje z podłączonymi zasilaczami awaryjnymi, obsługującymi interfejs ACPI. Usługa taka jest też oferowana przez takie systemy, jak Windows 2000 Professional, Windows XP oraz niektóre wersje systemów Unix i Linux. Zasilacz awaryjny komunikuje się z usługą i nakazuje systemowi, aby zakończył działanie w standardowy sposób, gdy zostanie stwierdzony zanik napięcia i przejście na zasilanie z baterii. W niewielkich zasilaczach awaryjnych należy sprawdzić obecność następujących elementów:

- ♦ **Alarmy dźwiękowe.** Pamiętam, jak kilka lat temu obudził mnie alarm zasilacza awaryjnego. Okazało się, że spałem w trakcie huraganu. Cieszyłem się wówczas, że miałem zasilacz UPS — ocalił mój komputer i, przy okazji, być może mnie.
- ♦ **Wiele gniazd.** Większość małych zasilaczy awaryjnych pozwala na podłączenie do niego od dwóch do czterech urządzeń, dzięki czemu nie trzeba kupować oddzielnych zasilaczy UPS dla komputera, drukarki, routera itd. Takie rozwiązanie może być przydatne w środowisku małego biura SOHO (ang. *Small Office/Home Office*), w którym urządzenia wymagające ochrony znajdują się blisko siebie. Dodatkowo przy zakupie zasilacza UPS należy szukać modeli umożliwiających ochronę podłączanych do komputera przewodów innych niż napięciowe, jak na przykład linia telefoniczna. Pamiętaj, że niektóre gniazdzka zasilaczy UPS oferują tylko ochronę przeciwprzepięciową. Urządzenia mniej istotne dla sieci, takie jak drukarki, powinny być podłączane właśnie do tych gniazdek zasilacza.
- ♦ **Wskaźnik baterii.** Należy sprawdzić, czy zasilacz UPS zawiera mechanizm powiadamiania (zazwyczaj dioda sygnalizacyjna) o sytuacji, gdy bateria zostanie całkowicie naładowana lub jest w trakcie ładowania. Baterie nie podtrzymują napięcia w nieskończoność. Dodatkowo dioda powinna wskazywać, czy UPS doprowadza napięcie przy użyciu baterii czy zewnętrznego źródła prądu.

- ♦ **Wskaźnik przeciążenia.** Nawet pomimo tego, że UPS jest wyposażony w wiele gniazd, może nie być w stanie dostarczać wystarczającej mocy do podłączonych urządzeń. Dobrej jakości zasilacz awaryjny powiadomi (znów zazwyczaj przy użyciu diody) o zbliżeniu się do jego maksymalnych możliwości. W takiej sytuacji konieczne będzie zastosowanie więcej niż jednego zasilacza. W dokumentacji dołączonej do UPS powinno być podane natężenie prądu, jakie może być zapewniane przez urządzenie. Podobnie w dokumentacji dołączonej do komputerów i urządzeń peryferyjnych powinna się znajdować informacja dotycząca pobieranej przez nie energii. W celu sprawdzenia, czy zasilacz UPS jest w stanie spełnić wymagania, należy obliczyć całkowity pobór mocy.
- ♦ **Wyłącznik obwodu.** Jeśli zignorujesz wskaźnik przeciążenia, zasilacz powinien być wyposażony w automatyczny wyłącznik, który zwykle ma postać niewielkiego przycisku, który można ponownie włączać. Jeśli mimo powiadomienia o przeciążeniu w dalszym ciągu próbujesz uzyskać więcej mocy, niż zasilacz na to pozwala, UPS uruchomi wyłącznik i tym samym odetnie zewnętrzne źródło zasilania. Zasilacz przejdzie na pracę przy wykorzystaniu baterii, a podłączone urządzenia otrzymają sygnał do zakończenia pracy.

Co prawda duża liczba wytwórców produkuje i sprzedaje niewielkie zasilacze UPS, ale w celu uzyskania informacji na temat produktów (wraz z dokumentacją), które można zastosować w różnych przypadkach — począwszy od stacji roboczej, a skończywszy na w pełni wyposażonej serwerowni opartej na systemach zasilaczy UPS — warto zajrzeć na stronę internetową firmy American Power Conversion (www.apc.pl).

Przy podejmowaniu decyzji o zakupie zasilacza awaryjnego trzeba pamiętać, że możliwości tych produktów mocno windują ich ceny. Koszt zakupu zasilacza UPS należy porównać z kosztem wymiany urządzeń, które mają być chronione, ale także z kosztem przestoju, uszkodzenia danych itp.

Urządzenia sieciowe

Systemy zasilania awaryjnego nie są przeznaczone wyłącznie dla komputerów — w końcu niniejsza książka jest poświęcona sieciom. Nie zapomnij o routerach, przełącznikach i innych urządzeniach podłączonych do sieci. Co prawda w trakcie awarii zasilania dopuszczalny może być brak dostępu do drukarki, ale w przypadku komputerów nie będzie to miało większego znaczenia, czy działają, jeśli użytkownicy nie mogą się z nimi połączyć za pośrednictwem sieci. Tam gdzie ciągle działanie sieci jest ważne dla działalności korporacji, routery i inne tego rodzaju urządzenia należy podłączać do tych gniazdek zasilaczy awaryjnych, na których UPS podtrzymuje zasilanie. Z kolei w domu czy małym biurze do podtrzymywanych gniazdek zasilacza awaryjnego można podłączyć nie tylko komputer, ale i router czy modem szerokopasmowy (kablowy, satelitarny, DSL itd.).

Monitorowanie sieci

Protokoły SNMP (ang. *Simple Network Management Protocol*) i RMON (ang. *Remote Monitoring*) są przydatnymi technologiami, służącymi do zarządzania nośnikiem danych stosowanym w dużych sieciach. W przypadku niewielkich sieci lokalnych, używanych

na przykład w domu, takie rozwiązania nie są wymagane. Jeśli urządzenie takie, jak modem kablowy lub modem DSL bądź router przestanie działać, to prawdopodobnie będzie możliwe szybkie stwierdzenie tego faktu. Dotyczy to również drukarki (może zabraknąć w niej tonera lub tuszu) i komputera lub komputerów (mogą się „zawiesić” lub ulec awarii). Jednak gdy sieć swoim zasięgiem obejmuje duży obszar geograficzny lub składa się z dużej liczby urządzeń i komputerów, to oba wymienione protokoły mogą być — wraz z konsolami zarządzania — użyte w celu ułatwienia zdalnego diagnozowania problemów i gromadzenia danych statystycznych dotyczących sieci. Protokoły SNMP i RMON mogą też okazać się przydatne do wykrycia usterki, zanim jeszcze stanie się ona powodem rzeczywistego problemu.

Podstawowym zadaniem protokołu SNMP jest zbieranie danych na temat komputerów i innych urządzeń podłączonych do sieci. Protokół jest używany wraz z konsolą zarządzania, spełniającą rolę centrum generowania raportów. Co prawda protokół RMON jest podobny do protokołu SNMP, ale oferuje dodatkowe funkcje, powiązane szczególnie ze zdalnymi urządzeniami. Poprzez wybranie odpowiedniej konsoli zarządzania można określić wartości progowe wybranych zdarzeń, takich jak obciążenie sieci, błędy i inne dane statystyczne, dzięki czemu po wystąpieniu jakichkolwiek anomalii automatycznie zostaną wygenerowane ostrzegawcze alarmy.

- ▶ ▶ Protokoły SNMP i RMON szczegółowo omówiono w rozdziale 49. — „Narzędzia do testowania i analizowania sieci”. Jeśli zarządzasz dużą siecią za pomocą aplikacji służących do centralnego zarządzania, to wykorzystują one właśnie te protokoły do zbierania informacji o urządzeniach sieciowych oraz, w przypadku RMON, do ustawiania zmiennych w bazach MIB (ang. *Management Information Base*) tych urządzeń.

Kopie zapasowe stacji roboczych i serwerów

Czy kiedykolwiek zdarzyło Ci się stracić książkę adresową? Czy posiadałeś jej kopię? Jeśli korzystasz z laptopa lub urządzenia PDA (ang. *personal digital assistant*), pozwolę sobie na zadanie zmodyfikowanego pytania. Czy zdarzyło Ci się kiedyś stracić dane zapisane na komputerze PC? Czy wykonałeś wcześniej kopię zapasową? Może się to wydawać trywialne, ale jest to związane z najważniejszym zagadnieniem poruszonym w tym rozdziale.

Nic nie będzie bardziej dla Ciebie wartościowe niż poprawnie wykonana kopia zapasowa danych przechowywanych na wszystkich systemach komputerowych podłączonych do sieci. Nie ma znaczenia, czy wydałeś setki tysięcy złotych (lub nawet miliony) na zakup najnowocześniejszych macierzy dyskowych RAID (ang. *Redundant Array of Independent Disk*), gdzie na oddzielnych dyskach jest przechowywanych wiele kopii danych. Aby zapobiec klęsce żywiołowej spowodowanej utratą danych, wiele instytucji finansowych korzysta nawet z mechanizmu wykonywania lustrzanych kopii danych pomiędzy odległymi oddziałami, umieszczonymi w różnych miejscach kuli ziemskiej. Niezależnie od stopnia nadmiarowości w lokalnym systemie przechowywania danych istnieją inne powody, dla których należy utworzyć właściwy harmonogram regularnego wykonywania kopii zapasowych ważnych danych zapisanych na komputerach podłączonych do sieci.

Oto RAID!

Pierwotnie technologia RAID nosiła nazwę *Redundant Array of Inexpensive Disks* (*nadmiarowa macierz niedrogich dysków*). Zmiana nazwy została spowodowana tym, że większość dysków stosowanych w systemach RAID dużej skali może być kojarzona ze wszystkim, ale nie z niską ceną! Jeśli chcesz uzyskać więcej informacji na temat technologii RAID — począwszy od prostej konfiguracji dysków lustrzanych, a skończywszy na zestawach paskowych i kombinacji tych dwóch rozwiązań — zajrzyj na te strony: <http://SearchStorage.techtarget.com> (poszukaj tam artykułów z cyklu „The Essential RAID Primer”); www.acnc.com/04_01_07.html to adres witryny Advanced Computer and Network Corporation’s z przewodnikiem „Get to Know RAID”; witryna AAA Data Recovery’s publikuje pod adresem www.aaa-datarecovery.com/raid_tutorial.htm kolejny elementarz: „RAID Tutorial”. To znakomite źródła informacji o rozmaitych odmianach macierzy RAID. Technologia RAID może być stosowana na dyskach ATE/IDE, SATA, SCSI i SAS.

Przy zakupie technologii RAID należy być świadomym, że termin RAID niekoniecznie musi oznaczać, że oferowane rozwiązanie posłuży do ochrony danych. Termin RAID swoim zasięgiem obejmuje kilka technologii dyskowych. Niektóre z nich umożliwiają utrzymywanie wielu kopii danych (np. zestawy lustrzane), natomiast pozostałe przyspieszają operacje odczytu i zapisu danych (np. zestawy paskowe). Jednocześnie obie technologie są stosowane w środowisku wymagającym krótkiego czasu dostępu do magazynów danych oraz zaawansowanych metod ich ochrony.

Co prawda technologia RAID zazwyczaj jest omawiana w takich książkach, jak *Naprawa i rozbudowa komputerów PC*. Wydanie drugie autorstwa Scotta Muellera, ale wspomniano też o niej w niniejszej publikacji, co wynika z ważnej roli, jaką odgrywa ona w obecnie spotykanych większych sieciach. Więcej informacji na temat technologii RAID zawarto w rozdziale 11. — „Urządzenia NAS i sieci SAN”.

Nawet jeśli zastosujesz na przykład zestaw lustrzany lub inną technologię RAID, co zrobisz, gdy z nieba spadnie meteoryt, w dodatku dokładnie na Twoją serwerownię? Bum! Stracisz wszystkie komputery, dane i oczywiście kilku administratorów. Można kupić nowe komputery i zatrudnić nowych pracowników (oczywiście po odpowiednim szkoleniu), ale czy możesz odzyskać dane?

- ▶▶ Dostępna jest jeszcze jedna technologia, która może okazać się przydatna, gdy awarii ulegnie cały system magazynowania danych znajdujący się w lokalnym oddziale. Sieci SAN (ang. *Storage Area Networks*) mogą posłużyć do replikacji danych pomiędzy lokacjami oddalonymi od siebie o kilka kilometrów. Istnieje również możliwość rozmieszczenia sieci SAN na znacznie większym obszarze geograficznym. Polega to na tunelowaniu danych przesyłanych w sieciach SAN przy użyciu takich protokołów sieci rozległych, jak ATM lub Frame Relay. W celu uzyskania dodatkowych informacji na temat sieci SAN należy zajrzeć do rozdziału 11.

W celu znalezienia bardziej praktycznego powodu, dla którego warto często wykonywać kopie zapasowe, wystarczy pomyśleć o użytkownikach. Kiedy ostatnio użytkownik usunął plik lub, co gorsza, cały katalog i prosił Cię o jego przywrócenie? Kopie zapasowe mogą Cię uchronić nie tylko przed skutkami awarii komputera i kataklizmów o charakterze naturalnym lub sztucznym. Czy naprawdę ufasz swoim użytkownikom? To duży błąd. Jak mówi stare powiedzenie, „ufaj każdemu, ale najpierw go sprawdź”. W dużych organizacjach trudno zadowolić wszystkich pracowników. Badania wykazały, że większość awarii poszczególnych komputerów lub sieci jest spowodowanych przez lokalnych użytkowników. Sieć powinna być chroniona zarówno przed wewnętrznymi, jak i zewnętrznymi źródłami problemów.

Nic nie jest w stanie zastąpić dobrej kopii zapasowej, może z wyjątkiem nowej pracy. Utrata danych będących wynikiem miesiący pracy, a nawet jednego dnia (zależnie od branży) bardzo podważa Twoje kompetencje i w prostej linii prowadzi do zmiany pracownika na Twoim stanowisku.

Nośniki archiwizujące — taśmy, dyski optyczne i twarde

Standardowa metoda wykonywania kopii zapasowych, stosowana przez większość firm, bazuje na taśmach o magnetycznym zapisie danych. Można się spotkać z każdego typu archiwizującym napędem obsługującym różne rodzaje taśm — począwszy od kasetowego formatu Travan, a skończywszy na bardziej nowoczesnych i pojemnych taśmach formatu DLT (ang. *Digital Linear Tape*). W niektórych instalacjach można się jeszcze natknąć na przestarzałe szpule 9-ścieżkowe. Przy wyborze nośnika archiwizującego należy kierować się następującymi kryteriami:

- ♦ Czy kopia zapasowa będzie przechowywana przez długi czy krótki okres czasu?
- ♦ Jeśli konieczna będzie operacja przywracania, to czy nośnik jest odpowiednio wydajny?
- ♦ Jaki jest koszt nośnika archiwizującego?
- ♦ Czy konieczna jest wymiana danych z innymi ośrodkami, takimi jak firmy zajmujące się przywracaniem danych po awarii i oferujące własne pomieszczenia?

Jeśli posiadasz dane tymczasowe i zależy Ci jedynie na przywróceniu systemów do poprzedniego stanu, niezbyt odległego w czasie, to można zastosować wiele typów nośników archiwizujących. Najprawdopodobniej Twój wybór będzie uzależniony od szybkości, z jaką będą tworzone kopie zapasowe, a następnie z jaką będą przywracane z nich dane. W takim przypadku prawdopodobnie taśma jest najlepszą propozycją. Dostępne są rozwiązania oparte na taśmach magnetycznych, oferujące bardzo dużą szybkość, które pozwalają na archiwizowanie i przywracanie danych w tempie kilku gigabajtów na godzinę. Taśma magnetyczna jest także odpowiednia do krótko- i długoterminowego przechowywania danych — przy założeniu, że jest przechowywana zgodnie z zaleceniami producenta. W przypadku długotrwałego składowania danych należy pamiętać o wybraniu nośnika obsługiwanego przez standardowe urządzenia. Przykładowo przez długi czas do wykonywania kopii zapasowych danych komputerowych używano 9-ścieżkowych taśm, traktowanych jako standard. Jednak jeśli na przykład ze względu na ustalenia ogórne konieczne jest przechowywanie kopii zapasowych przez wiele lat, należy również przechowywać napędy umożliwiające odczytanie danych na nich zapisanych.



W jednym z miejsc, w którym pracowałem, miałem do czynienia z firmą, która wydała ogromną sumę pieniędzy na przeniesienie danych ze sporej liczby starych, 9-ścieżkowych taśm na nowszy nośnik DLT. Od czasu do czasu napotymano na taśmę, której odczyt nie był możliwy. Większość danych odzyskano i teraz są one przechowywane w oczekiwaniu na następną kosztowną operację konwersji. Cóż, takie są wymagania rządu!

Gdy zamierzasz przechowywać dane przez dłuższy czas, to ze względu na szybki postęp technologiczny nie masz zbyt dużego wyboru. Jednak pamiętaj o wybieraniu technologii archiwizacji opracowanej przez zaufanego producenta, co do którego możesz być pewny, że będzie istniał na rynku przez następne kilka lat.

W sytuacjach awaryjnych czas wymagany do przywrócenia danych z kopii zapasowej może być bardziej istotny od ilości czasu potrzebnego do jej stworzenia.

Przykładowo istnieje możliwość poprawnego rozbicia zestawu lustrzanego i użycia jednego z jego dysków do stworzenia kopii zapasowej, a następnie ponownego przywrócenia tego zestawu przy wykorzystaniu oprogramowania systemu RAID. Takie rozwiązanie tego zestawu przy wykorzystaniu nieprzerwanie korzystając z systemu, który w minimalnym stopniu będzie ulegnie wpływowi wykonywanej operacji archiwizacji. Jeśli zostanie stworzony zestaw lustrzany złożony z trzech lub większej liczby dysków, to w trakcie wykonywania kopii zapasowej w dalszym ciągu będzie możliwe działanie mechanizmu odporności na awarie, ponieważ kopia aktualnych danych będzie znajdowała się na wielu dyskach.

W systemie RAID przywracanie danych może trwać tak samo jak operacja archiwizacji lub dłużej. Jest to uzależnione od zastosowanych kontrolerów dysków, oprogramowania sprzętowego i innych czynników. Przy wybieraniu technologii tworzenia kopii zapasowych nie należy zapomnieć o konieczności uwzględnienia operacji przeciwnej, czyli przywracania danych. Można nabyć zaawansowany i szybki podsystem dyskowy, oferujący wiele różnych poziomów technologii RAID, łącznie z archiwizacją w trybie *online*. Jeśli jednak przywracanie danych z wielu dysków trwa znacząco dłużej niż w przypadku pojedynczego dysku, to można się zastanowić nad rozwiązaniem alternatywnym.

Gdy dojdzie do najgorszego, czyli gdy nie tylko komputery, ale cały oddział padnie ofiarą jakiegoś kataklizmu, takiego jak pożar, należy mieć wtedy pewność, że używany nośnik archiwizujący jest kompatybilny z urządzeniami, które zostaną użyte w trakcie wykonywania procedury przywracania. Z łatwością można to przeoczyć podczas szukania dostawcy systemów czy pracowni awaryjnych. Nie należy do końca ufać dostawcy. Trzeba samemu wszystko sprawdzić. Weź taśmę z kopią zapasową i wykonaj w pracowni operację przywracania. Zmierz czas jej trwania. Upewnij się, że stosowany nośnik jest kompatybilny ze sprzętem dostawcy, a także sprawdź, czy napędy taśmowe (lub napędy innego typu) są wystarczająco szybkie, aby w krótkim czasie można było przeprowadzić operację odtwarzania.

Obecnie taśma magnetyczna nie jest jedynym typem nośnika archiwizującego. Dostępny jest bogaty asortyment nośników, począwszy od dysków magneto-optycznych, a skończywszy na dyskach CD i DVD. Problem z zapisywalnymi (jednokrotnie i wielokrotnie) dyskami CD i DVD polega na tym, że w dalszym ciągu w porównaniu z szybkością stosowanych taśm magnetycznych są zbyt wolne (nawet jeśli dysponujesz jednym z szybszych napędów), aby mogły być użyte na potrzeby operacji archiwizacji i przywracania. Pomimo to technologia zapisywalnych dysków CD i DVD jest stosunkowo niedrogim rozwiązaniem, które może posłużyć do wykonywania kopii zapasowych danych zapisanych na dyskach niewielkiego komputera, stosowanego w małym biurze SOHO. Ze względu na to, że pojemność dysków twardych jest wyrażana w gigabajtach, natomiast zapisywalnych dysków CD-R w megabajtach, powinno się je stosować w przypadku niewielkiej sieci firmowej lub domowej, gdzie zależy Ci jedynie na archiwizacji niewielkiej ilości danych. Z kolei na dysku DVD można nagrać 4,7 gigabajta (zapis jednowarstwowy) albo nawet 8,5 gigabajta (zapis dwuwarstwowy), przez co taki dysk lepiej nadaje się do archiwizowania większej ilości danych (co prawda, nie na potrzeby wykonywania pełnej kopii zapasowej dysków twardych, w przypadku których nadal najlepiej sprawdzają się napędy taśmowe).

Dyski wielokrotnego zapisu (RW), użyte do wykonania kopii zapasowej, pozwalają na dodawanie danych, wymazywanie ich i ponowne zastosowanie nośnika. W tym celu należy użyć jednego z wielu dostępnych obecnie na rynku programów służących do nagrywania danych na dyski CD i DVD (Nero Ultra Edition, Easy Media Creator itd.). W systemach Windows XP i Windows Vista można też korzystać z wbudowanych funkcji zapisu płyt CD. Ale oprogramowanie obsługujące te wbudowane funkcje nie jest ani tak wygodne, ani tak proste w obsłudze jak niektóre specjalizowane aplikacje; przede wszystkim zaś wbudowane oprogramowanie Windows XP nie pozwala zapisywać nośników DVD (nagrywarki DVD funkcjonują tak, jakby były nagrywarkami CD). Przy dostępności nagrywarek dwuwarstwowych dysków DVD w cenie poniżej 300 złotych modernizacja posiadanej nagrywarki nie stanowi wyzwania ekonomicznego. A trzeba pamiętać, że nagrywarki płyt DVD radzą sobie świetnie z zapisywaniem płyt CD-R i CD-RW, a do niektórych urządzeń tej klasy dołączane jest gotowe oprogramowanie do archiwizacji danych.

Ostatnio środkiem archiwizacji danych jest coraz częściej zewnętrzny dysk twardy. Wielu producentów oferuje takie dyski, podłączane do komputera za pośrednictwem złączy USB albo IEEE-1394 (niektóre dyski obsługują oba interfejsy). Najnowsze zewnętrzne napędy mają pojemności do 500 GB, a do większości z nich dołączane jest oprogramowanie archiwizujące. Niektóre oferują nawet automatyzację wykonywania kopii zapasowych — inicjuje się je przyciskiem na obudowie dysku zewnętrznego. Takie wykonywanie kopii zapasowych, z utrwalaniem starszych danych na dwuwarstwowych płytach DVD, to niezłe rozwiązanie problemu szybkiego wykonywania częstych kopii w połączeniu z koniecznością długotrwałego ich przechowywania.

Harmonogram wykonywania kopii zapasowych

Zanim zostanie wykonana kopia zapasowa, należy określić, jakie dane wymagają archiwizacji i przez jak długi okres czasu kopie muszą być dostępne na potrzeby operacji przywracania. Jeśli masz do czynienia z ciągle zmieniającym się środowiskiem pracy, w którym dane mające więcej niż kilka tygodni lub miesięcy są już bezwartościowe, nie będzie konieczne długotrwałe przechowywanie danych na taśmach lub innych nośnikach. Jednak w przypadku większości firm duże znaczenie ma możliwość odzyskania danych sprzed wielu miesięcy lub nawet lat, co ma na celu spełnienie określonych przez przepisy prawa wymagań finansowych lub proceduralnych. W takiej sytuacji należy stworzyć odpowiedni do potrzeb harmonogram wykonywania kopii zapasowych.

Można na przykład każdej nocy wykonywać pełną kopię zapasową danych przechowywanych na wszystkich systemach. Można też wykonywać pełną kopię zapasową raz w tygodniu, a w pozostałe dni kopie przyrostowe, czyli zawierające tylko te pliki, które uległy zmianie od czasu wykonywania ostatniej pełnej archiwizacji. Kombinacja pełnej kopii i przyrostowych kopii zapasowych pozwala na przywrócenie systemu do stanu, w którym się znajdował w dowolnej chwili wykonywania archiwizacji.

W tym przypadku, gdy zostanie wykonana kolejna pełna kopia zapasowa, kopie przyrostowe mogą być już niepotrzebne. Dzięki temu można wielokrotnie używać tych samych taśm. Częstotliwość, z jaką taśmy lub inne nośniki danych mogą być ponownie stosowane, jest określana mianem *częstości rotacji*. Ogólnie sprawdzająca się podstawowa procedura archiwizacji (której użycie zależy oczywiście od konkretnego środowiska) polega na cotygodniowym wykonywaniu kopii zapasowej wszystkich danych, a w pozostałe dni tygodnia

— kopii przyrostowych. Taka metoda archiwizacji umożliwia wykonywanie pełnej kopii zapasowej w czasie mniejszej aktywności użytkowników (np. w weekend). Taśmy przeznaczone na kopie przyrostowe mogą być ponownie użyte w kolejnym tygodniu, jeśli poprawnie wykonano pełną kopię zapasową.

Taśmy z pełnymi kopiami zapasowymi wykonywanymi co tydzień mogą być przechowywane przez miesiąc, a następnie ponownie wykorzystywane. Dodatkowo można przez dłuższy okres czasu przechowywać jedną z pełnych kopii zapasowych z danego miesiąca, ale zależy to od Twoich wymagań z tym związanych.

Metoda wykonywania pełnych i przyrostowych kopii zapasowych ma na celu zmniejszenie *okna archiwizacji*. Termin ten oznacza okres, podczas którego działa program archiwizujący, a użytkownicy nie wymagają dostępu do systemu. Jednak ze względu na ciągły wzrost zapotrzebowania na przestrzeń dyskową i całodobowy dostęp do danych można skorzystać z kolejnej technologii, która w takich sytuacjach może być przydatna. Jak już wcześniej w rozdziale wspomniano, w celu przeniesienia magazynów danych z serwerów mogą zostać użyte sieci SAN. Sieci te rozwiązują wiele problemów związanych ze standardowymi urządzeniami SCSI. Po pierwsze, interfejs SCSI pozwala na podłączenie do magistrali ograniczonej liczby urządzeń. Kolejnym ograniczeniem interfejsu jest też niewielka odległość, obsługiwana przez urządzenia SCSI. Sieci SAN pozwalają na podłączenie magazynów danych — zarówno dyskowych, jak i taśmowych — które znajdują się w znacznie większych odległościach od siebie, co nie powoduje zwiększenia czasu dostępu do danych. Sieci SAN mogą też posłużyć do odciążenia procesora serwera od zadań związanych z archiwizacją danych. Sieci SAN mogą zostać użyte do archiwizacji na taśmach danych przechowywanych na dyskach, bez konieczności interwencji serwerów, których ta operacja dotyczy.

Niezależnie od zastosowanej metody archiwizacji należy się upewnić, że spełnia ona wymagania użytkowników i aplikacji, z których oni korzystają. Ponadto należy zastosować określony typ mechanizmu, taki jak baza danych przechowująca informacje o każdej taśmie, dzięki czemu będziesz w stanie wyeliminować taśmę, której użyto już ustaloną liczbę razy. Taśmy magnetyczne zużywają się z każdym kolejnym ich wykorzystaniem i mogą nawet ulec uszkodzeniu, gdy są przechowywane w miejscu, którego temperatura i wilgotność przekraczają wartości graniczne zalecane przez producenta.

Przy użyciu kodów kreskowych lub poprzez zwykłe umieszczanie na taśmach etykiet z numerami seryjnymi można zidentyfikować taśmy w bazie danych i uaktualniać jej zawartość po każdorazowym użyciu taśmy. Kody kreskowe wykorzystywane są jako mechanizm identyfikacji taśm przez zautomatyzowane podajniki, ale warto o nich pomyśleć również wtedy, kiedy zmiana taśm w napędzie archiwizującym wykonywana jest ręcznie. Gdy czas eksploatacji taśmy osiągnął czas określony przez producenta jako maksymalny, to przy użyciu specjalnego narzędzia należy wymazać jej zawartość, tak aby odczytanie danych było niemożliwe, i wyrzucić ją do kosza. Ze względów bezpieczeństwa zaleca się stworzenie firmowej procedury dotyczącej pozbywania się wszystkich materiałów, np. wydruków i taśm. Kto będzie grzebał w Twoim śmietniku? Lepiej być pewnym niż przekazać komuś innemu wartościowe dane, należące do Twojej firmy.

Przechowywanie kopii zapasowej w innej fizycznej lokalizacji

Kopia zapasowa jest przydatna tylko wtedy, gdy jest przechowywana w bezpiecznym miejscu. Jeśli zależy Ci na przywróceniu tylko jednego pliku, ponieważ użytkownik popełnił błąd i usunął go, to — dysponując taśmą przechowywaną w serwerowni — możesz operację tę wykonać szybko i łatwo. Wystarczy umieścić taśmę w napędzie, przywrócić plik, a następnie powiadomić użytkownika. Jednak przechowywanie taśm archiwizujących w tym samym miejscu, w którym znajdują się komputery, nie zawsze jest dobrym rozwiązaniem. Przykładowo w przypadku jakiegokolwiek kataklizmu, takiego jak pożar, takie postępowanie może spowodować, że pozostaniesz bez kopii zapasowej. Zostaną stracone nie tylko komputery, ale również zarchiwizowane dane.

W przypadku danych o dużej wartości nośnik archiwizujący powinien zostać przewieziony do innej fizycznej lokalizacji jak najszybciej po wykonaniu kopii zapasowej. W takiej sytuacji, gdy dojdzie do kataklizmu, taśmy będą bezpiecznie przechowywane w innym miejscu i będą mogły zostać użyte do przywracania danych przy użyciu awaryjnego sprzętu lub po wymianie zniszczonego wyposażenia firmy.

Jakie są wymagania związane z przechowywaniem kopii w innej fizycznej lokalizacji? W zależności od potrzeb można przechowywać kopie zapasowe w kilku miejscach. Zastanów się najpierw, jak bezpieczne jest dodatkowe miejsce przechowywania kopii zapasowej, a następnie ile czasu będzie wymagane na dostarczenie nośnika archiwizującego. Na końcu należy określić koszt takiego rozwiązania. Oto kilka propozycji dodatkowych miejsc przechowywania:

- ♦ Skorzystaj z oferty firmy, która zajmuje się odbieraniem, przechowywaniem i dostarczaniem nośników archiwizujących. Istnieje wiele firm specjalizujących się w tym. W celu sprawdzenia, czy warunki oferowane przez wybraną firmę są odpowiednie do długotrwałego przechowywania wrażliwych nośników archiwizujących, należy osobiście się do niej wybrać. Poprzez zażądanie w różnych terminach próbnego dostarczenia taśm sprawdź, czy spełniany jest zadeklarowany czas reakcji. Upewnij się, że firma oferuje 24-godzinny dostęp do Twoich danych.
- ♦ Jeśli w przypadku wystąpienia jakiegoś kataklizmu będziesz korzystał z usług firmy udostępniającej awaryjne pracownie, może ona zaoferować również przechowywanie nośników archiwizujących w swoich pomieszczeniach. Dzięki temu w razie sytuacji awaryjnej można zaoszczędzić czas, ponieważ przed uaktywnieniem zapasowego środowiska roboczego nie będzie konieczne sprowadzanie taśm z innego miejsca.
- ♦ Jeśli pracujesz w dużej firmie, to praktyczniejsze może być przechowywanie nośników archiwizujących w jej innym oddziale. Pod uwagę powinna być brana szansa wystąpienia kataklizmu jednocześnie w kilku miejscach, a także warunki przechowywania w innej lokalizacji. Przykładowo jeśli oddziały znajdują się blisko siebie, może nie być to dobrym pomysłem — naturalny kataklizm, taki jak huragan lub powódź, mogą spowodować zniszczenie obu miejsc. Należy też uwzględnić koszt regularnego przesyłania taśm do innego oddziału firmy. Może się okazać, że tańsze będzie wynajęcie specjalistycznej firmy zajmującej się przechowywaniem taśm niż angażowanie pracowników w przewożenie ich z jednego oddziału do innego.

- ◆ Weź nośnik kopii albo zewnętrzny dysk twardy do domu i schowaj go pod łóżkiem. To nie jest żart! Miałem okazję pracować w niewielkiej firmie, w której menedżer ds. systemów zabierał comiesięczną kopię zapasową do domu i tam, pod łóżkiem, przechowywał ją do następnego miesiąca. To samo dotyczy małego biura prowadzonego w domu. Należy wziąć pod uwagę możliwość umieszczania cotygodniowej lub comiesięcznej taśmy z kopią zapasową w skrzynce depozytowej w lokalnym banku i traktować to jako metodę przechowywania danych w innym miejscu. Celem takich działań jest uzyskanie pewności, że dane są przechowywane z dala od systemu, na którym się znajdują. Dzięki temu zmniejsza się ryzyko wystąpienia kataklizmu, który zniszczy zarówno komputery, jak i kopie zapasowe zapisanych na nich danych.

Regularna konserwacja

Co prawda w rozdziale tym skupiłem się przede wszystkim na metodach zapobiegania zagrożeniom, ale ważne jest też regularne wykonywanie konserwacji komputerów i urządzeń sieciowych. Tego typu konserwacja zapobiega występowaniu awarii sprzętowych, spowodowanych intensywnie eksploatowanym lub przestarzałym sprzętem, który się psuje. Oto przykład: ponieważ wszystkie komputery — począwszy od niewielkich stacji roboczych, a skończywszy na dużych systemach montowanych w szafach — w celu zagwarantowania swobodnego przepływu powietrza wewnątrz systemu zapobiegającego przegrzaniu układów używają wentylatorów, to dodatkowo co jakiś czas powinno się sprawdzać, czy kurz i inne zanieczyszczenia nie są zasysane do środka obudowy i czy dzięki ładunkom elektrycznym nie przyczepiają do podzespołów.

Raz lub dwa razy w ciągu roku warto zdjąć obudowę i przy użyciu skompresowanego powietrza usunąć wszelkie zanieczyszczenia. Jest to zalecana metoda zapobiegawcza. W przypadku biura prowadzonego w domu dość łatwo o tym zapomnieć. Jeśli w domu znajduje się osoba paląca, to na przykład po jakimś czasie możesz stwierdzić, że dym papierosów może przyczynić się do powstania cienkiej warstwy kurzu nagromadzonego na komponentach komputera. Z własnego doświadczenia wiem, że powodem tego może też być kocia sierść. Co jakiś czas zdejmuj obudowę komputera. Zdejmij ją teraz i zajrzyj do środka, a następnie usuń brud. Nawet większe serwery, które znajdują się w zamkniętym pomieszczeniu, mogą wymagać czyszczenia co jakiś czas. Niezależnie od stopnia czystości pomieszczenia z komputerami należy sprawdzić, jaka ilość kurzu gromadzi się po upływie pewnego okresu czasu. Możesz być tym zaskoczony. Jest to jeden z problemów posiadania serwerowni, do której nikt nie zagląda. Warto więc od czasu do czasu odwiedzić takie pomieszczenie i skontrolować sytuację. Zawsze najlepiej wykryć problem, zanim w poważnym stopniu wpłynie on na używany sprzęt.

Napędy taśmowe wymagają okresowego czyszczenia, ponieważ taśma magnetyczna styka się z głowicami znajdującymi się wewnątrz urządzenia. Taśma czyszcząca powinna być stosowana z częstotliwością zalecaną przez producenta. Napędy taśm DLT zazwyczaj są wyposażone we wskaźnik świetlny, który zapala się, gdy na głowicy nagromadzi się taka ilość zanieczyszczeń, która może powodować występowanie błędów zapisu i odczytu. Jeśli taśma czyszcząca musi być używana częściej niż zaleca to producent, może się okazać

konieczne sprawdzenie, jakie taśmy były używane, zanim taki problem się pojawił. Możesz być w posiadaniu zużytej taśmy albo nawet napędu taśmowego, który należy ponownie skalibrować lub wymienić.

Tworzenie nadmiarowości w sieci

Bez znaczenia będzie rodzaj umowy serwisowej podpisanej z producentem, jeśli na sprostanie części zamiennych lub nowych urządzeń w miejsce uszkodzonych będzie on potrzebował wielu godzin lub dni. Z tego też powodu warto już na etapie projektowania zapewnić sieci nadmiarowość. Przykładowo jeśli awarii ulegnie router, to dodatkowa ścieżka sieci umożliwi użytkownikom uzyskanie w dalszym ciągu dostępu do wymaganych przez nich danych. W celu maksymalizacji dostępności systemów o dużym znaczeniu można zastosować serwery wyposażone w nadmiarowość bazującą na technologii klastrów.

- ◀◀ W rozdziale 2. — „Przegląd topologii sieciowych” — zawarto godne uwagi omówienie zastosowania topologii częściowej siatki, która może posłużyć do wyposażenia sieci w nadmiarowość. Zobacz punkt „Topologia siatki”, a także podrozdziały „Tworzenie sieci wielosegmentowej i stosowane topologie” i „Topologia sieci wielowarstwowej”.

Jeśli nie dysponujemy wystarczającą ilością czasu przeznaczoną na wymianę sprzętu (w porównaniu z kosztem związanym z opłacaniem użytkowników nie mogących wykonywać swoich zadań, kosztami powierzchni biurowej itp.), wartym rozważenia jest posiadanie na miejscu zapasowych urządzeń, które będą mogły szybko zastąpić ich uszkodzone odpowiedniki. W przypadku routera lub przełącznika operacja wymiany uszkodzonego urządzenia jest prosta. W tym celu należy — zgodnie z wcześniej przygotowaną szczegółową procedurą — dokonać ponownej konfiguracji, co pozwoli ponownie udostępnić sieć.

Planowanie przywracania pracy sieci

W sytuacji awaryjnej nic nie jest bardziej wartościowe (poza kopią zapasową) niż dobrze przemyślany plan przywracania pracy sieci. Tak naprawdę jest to ogólne określenie, ponieważ należy przygotować plany dotyczące awarii sieci lub serwera — począwszy od uszkodzenia pojedynczego dysku, poprzez niedostępność systemu komputerowego, a skończywszy na awarii całej sieci. W rozdziale 3. — „Strategie projektowania sieci” — zwrócono uwagę na to, że zawsze należy tworzyć dokumentację sieci i jej komponentów. W skład takiej dokumentacji powinny wchodzić procedury przywracania pracy sieci.

Cały problem z kataklizmami polega na tym, że nie można ich przewidzieć. Nie zawsze mają one miejsce w czasie normalnych godzin pracy, gdy jesteś w pełnej gotowości i sprawności. W środku nocy, po ciężkim dniu pracy, możesz zostać wezwany do przywracania systemu, co oznacza, że czeka Cię nieprzespana noc. Dobry plan przywracania pracy sieci po awarii jest przydatny dlatego, że dzięki niemu w trakcie całej operacji nie popełnisz błędów.

Dobry plan przywracania pracy sieci powinien uwzględniać następujące elementy:

- ♦ Dane kontaktowe pracowników, którzy będą odpowiedzialni za wykonywanie operacji przywracania oraz personelu, który powinien zostać o tym poinformowany. Należy tu wspomnieć o przedstawicielach klientów korzystających z przywracanego systemu. Pamiętaj o uaktualnianiu tego typu informacji.
- ♦ Dane kontaktowe producentów — zarówno sprzętu, jak i oprogramowania wchodzącego w skład systemu lub sieci. Należy w nich uwzględnić numery telefonów pomocy technicznej oraz dane kontaktowe pracowników lokalnego oddziału, którzy mogą być potrzebni przy odbudowie systemu i usuwaniu awarii.
- ♦ Szczegółowe procedury umożliwiające wyjście z sytuacji awaryjnej. Swoim zakresem mogą one obejmować całkowitą przebudowę określonego systemu poprzez ponowną instalację systemu operacyjnego i przywrócenie danych z kopii zapasowej zapisanej na taśmie. Plan przywracania pracy sieci powinien zawierać konfigurację routerów i innych urządzeń.
- ♦ Po usunięciu skutków kataklizmu zgodnie z opracowanym planem konieczne jest przeprowadzenie na systemie operacyjnym, urządzeniach i aplikacjach zestawu testów, mających na celu sprawdzenie, czy operacja przywracania pracy sieci została wykonana poprawnie.

Szacowanie kosztu metod ochrony

Niektóre z metod omówionych w niniejszym rozdziale są kosztowne. Z tego też powodu możesz mieć problemy z uzyskaniem od kierownictwa środków finansowych na ich zastosowanie. Aby sobie poradzić w takich sytuacjach, można wykonać kilka czynności.

Należy pamiętać o dokumentowaniu wszystkich przestoju każdego systemu znajdującego się w sieci i próbować określić ich koszt. Co prawda możesz nie być w stanie uzyskać informacji pozwalających określić, jaki wpływ przestoje mają na użytkowników, ale zazwyczaj jest możliwe ustalenie liczby tych przestoju. Zakładając, że użytkownicy pozbawieni dostępu do komputera lub sieci są w stanie wykonywać tylko pewien procent swoich codziennych obowiązków, spróbuj ustalić liczbę godzin straconych na skutek przestoju i pomnożyć ją przez średnią stawkę godzinową pracowników, którzy przez to ucierpieli. Najprawdopodobniej nie będziesz miał dostępu do wysokości stawek godzinowych innych pracowników. Jednak można sobie z tym poradzić poprzez pomnożenie liczby godzin przez minimalną średnią stawkę godzinową, a następnie — w przypadku uzyskania znacznej kwoty — poinformować o tym kierownictwo. Należy wspomnieć, że przy obliczeniach bazowano na minimalnej stawce. Ze względu na to, że osoby z kierownictwa najprawdopodobniej będą znały średnie zarobki używających komputera pracowników z dużym stażem, przekazany im wynik nadal będzie wiarygodnym oszacowaniem kosztu przestoju. Innymi słowy, jeśli w wyniku obliczeń opartych na stawce minimalnej uzyska się sporą wartość, to osoby z kierownictwa szybko dojdą do wniosku, że rzeczywista wartość będzie znacznie wyższa, dlatego też możesz liczyć na uzyskanie środków potrzebnych na zastosowanie metod zapobiegawczych.