helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

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



Autor: Terry Ogletree
Tłumaczenie: Jacek Baszkiewicz, Adam Balcerzak, Bartek Kruk
ISBN: 83-7197-266-0
Tytuł oryginału: Upgrading and Repairing Networks
Format: B5, stron: 472

Ta książka jest przede wszystkim przeznaczona dla doświadczonych techników i administratorów sieci. Wziąwszy pod uwagę tendencję do poszerzania sieci przy wykorzystaniu nowych technologii, protokołów i składników, książka ta okaże się nieocenioną pomocą podczas planowania i rozwiązywania problemów.

Nie znaczy to, że książki nie mogą przeczytać osoby zapoznające się dopiero z tematyką sieciową. W rzeczywistości książka stanowi wspaniałe narzędzie szkoleniowe zawierające rady dla tych, którzy zaznajamiają się z sieciami komputerowymi.

Do pracy nad książką zaproszono współautorów, z których każdy jest weteranem na polu publikacji komputerowych oraz ekspertem z dziedziny sieci komputerowych.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

O Autorze **15**

Podziękowania **17**

Wprowadzenie **19**

Rozdział 1. Narzędzia **21**

Podstawy: testowanie kabli 21
- Podręczne kontrolery kabli 22
- Próbniki kablowe 22
- Mierniki bitowej stopy błędów (BERT) 23

Czasowe mierniki odbić 24
- Sprawdzanie impedancji 24
- Ustawianie szerokości impulsu 25
- Porównywanie prędkości 25

Analizatory sieci i protokołów 26
- Ustalenie danych odniesienia 27
- Dane statystyczne 28
- Dekodowanie protokołów 28
- Filtrowanie 29
- Analizatory programowe 29
- Analizatory sprzętowe 33

Prosty protokół zarządzania siecią (SNMP) 34
- Operacje elementarne SNMP 35
- Obiekty sieciowe: baza informacji zarządzania (MIB) 36
- Agenty proxy 38
- SNMPv2 38
- RMON 38

Rozdział 2. Testowanie kabli **43**

Zgodność ze standardami 43
- Organizacje normalizacyjne 44
- CSMA/CD kontra Token-Ring 48
- Fizyczne rodzaje kabli 50

10Base-2 i 10Base-5 52

10Base-T 55
- Złącza i kable 56
- Kable skrośne 57
- Wymagania techniczne 10Base-T 58

100Base-T 58
- 100Base-TX 58
- 100Base-T4 59
- 100Base-FX 59

100VG-AnyLAN....60
Okablowanie....60
Dostęp priorytetowy na żądanie....61
Sprawy bezpieczeństwa....62
Światłowody....62
Światłowody jedno- i wielomodowe....63
Zalety światłowodu....64
Gigabit Ethernet....64
Niewłaściwe okablowanie....65
Długości kabli....66
Sprawdzanie zakończeń....66
Skrzyżowane kable....66
Gięcie, przerywanie oraz rozciąganie kabli....67
Mieszanie kabli o różnych typach....67
Złącza....67
Problemy z wtyczkami....68
Zakłócenia elektromagnetyczne i radiowe....68
Przesłuch zbliżny (NEXT)....68
Inne problemy....69

Rozdział 3. Karty sieciowe....71
Wybór rodzaju magistrali systemowej: PCI, ISA, CZY EISA?....71
Sterowniki programowe....72
Sterowniki pakietowe....72
ODI....72
NDIS....73
Systemy wieloportowe....74
Przerwania....74
Podstawowe porty wejścia-wyjścia....76
Rozwiązywanie problemów z kartami sieciowymi....77
Diody LED....77
Program diagnostyczny karty sieciowej....78
Konflikty konfiguracyjne....78
Kroki zapobiegawcze....78

Rozdział 4. Mosty, routery, przełączniki oraz wzmacniaki....81
Wzmacniaki....81
Mosty....83
Segmentacja sieci (dzielenie sieci na segmenty)....84
Algorytm rozpiętego drzewa....85
Kiedy stosować mosty....87
Przełączniki....88
Komunikacja dwustronna w sieci Ethernet....89
Rodzaje przełączników....90
Kiedy stosować przełączniki....91
Routery....93
Protokół RIP....93
OSPF....96
Kiedy stosować routery....96

Rozdział 5. Jednostki dostępu do medium oraz wieloterminalowe jednostki dostępu 99
MAUs, CAUs oraz LAMs....99
PORTY Ring-In oraz Ring-Out 101
Funkcje wstawiania i omijania....101
Konfiguracja i rozwiązywanie problemów związanych z MAUs....102

Rozdział 6. Koncentratory 103
Wybieranie właściwego rodzaju koncentratora 103
Zalety topologii gwiaździstej....104
Jakiego koncentratora potrzebujesz? 105
Klasyfikacja koncentratorów pod względem funkcjonalności 107
Porty koncentratora 108
Porty UTP, AUI oraz BNC 109
Porty przejściowe tzw. krosowe 109
Rozwiązywanie problemów z koncentratorem 110
Sprawdzanie diod LED....110
Sprawdzanie nowych połączeń 110
Sprawdzanie konfiguracji portu lub koncentratora....111
Używanie oprogramowania do zarządzania koncentratorem 111
Generalna awaria koncentratora 111

Rozdział 7. Ograniczenia topologii Ethernetu 113
Czynniki ograniczające 113
Urządzenia wzmacniające oraz długość kabla....114
Reguła 5-4-3....114
Topologia magistrali 115
Korzystanie z topologii gwiazdy....116
Topologie hybrydowe 117
Drzewo....117
Hierarchia gwiazdy 118
Tworzenie sieci szkieletowej 118
Użycie koncentratora przełączającego....119
Użycie routerów do połączenia sieci 120

Rozdział 8. FDDI 123
Topologia FDDI Dual-Ring 124
Porty i stacje....124
Przerwy w pierścieniach 125
Optyczne przełączniki pomijające 127
Dodatkowe wyposażenie ważnych urządzeń....127
Standardy protokołu FDDI....127
Transmisja danych w pierścieniu FDDI....129
Wykorzystanie światła do kodowania bitów 129
Ramki FDDI....129
TRT (Token Rotation Timer)....130
Beaconing 131
Najczęstsze problemy z FDDI....131
Przerwy w pierścieniu....132
Błędy inicjalizacji pierścienia i sekwencji sprawdzania ramek....132
Dokonywanie napraw 133

Rozdział 9. Sieci bezprzewodowe 135
Zastosowania bezprzewodowych sieci lokalnych 135
Topologia bezprzewodowa 137
Metody komunikacji 138
Standardy bezprzewodowe 139
Warstwa fizyczna 140
Warstwa MAC 140
Zabezpieczenia w sieciach bezprzewodowych 141
Inne rozwiązania bezprzewodowe 141
WAP (Wireless Application Protocol) 141
Bluetooth 141

Rozdział 10. Współczynniki kolizji 145
Powody występowania kolizji — CSMA/CD 145
Algorytm wycofywania 146
Związek liczby kolizji z długością pakietów 147
Kolizje i wykorzystanie sieci 147
Wykrywanie kolizji 148
Rodzaje kolizji 148
Kolizje lokalne 148
Kolizje opóźnione 149
Okresy próbkowania 149
Redukowanie ilości kolizji 150
Niewłaściwa topologia sieci 150
Uszkodzone karty sieciowe 150
„Rozgadane" urządzenia 150

Rozdział 11. Błędy Ethernetu 153
Błędne FCS i niewyrównane ramki 154
Krótkie (karłowate) ramki 155
Zbyt duże ramki 155
Wielokrotne błędy 156
Burze rozgłaszania 156
Monitorowanie błędów 157

Rozdział 12. Ograniczenia topologii Token-Ring 159
Topologia gwiazdy 159
Jednostki dostępu do medium (MAU) 160
Łączenie kilku MAU w celu utworzenia większej sieci lokalnej 161
Topologie hierarchiczne 161
Wykorzystanie mostów 162
Bramy 164
Przełączniki Token-Ring 165
Rozwiązywanie problemów z mostami 166
Odmiany pierścienia: sieci Token-Bus 167

Rozdział 13. Monitorowanie wykorzystania sieci Token-Ring 169
Statystyki sieci Token-Ring 169
Wykrywanie błędów i ich źródeł 171
Monitor błędów pierścienia 171
Błędy sieci Token-Ring 172
Użycie analizatorów sieci i protokołu 174
Rozszerzenia Token-Ring dla zdalnego monitorowania sieci 174
Rady dotyczące rozwiązywania problemów 175

Rozdział 14. Połączenia dedykowane 177
Łącza dzierżawione 177
System T-Carrier 179
Fractional T1 180
Diagnozowanie problemów związanych z usługami T-Carrier 180
ATM 181
Połączenia ATM 181
Kategorie usług ATM 182
Emulacja sieci lokalnej (LANE) 183
Połączenia 183
X.25 i Frame Relay 183

Rozdział 15. Podstawowe zagadnienia bezpieczeństwa 187
Zasady i procedury 187
Zasady łączenia z siecią 188
Zasady korzystania z oprogramowania 188
Procedury reagowania 190
Tworzenie własnych zasad zabezpieczeń 191
Zabezpieczenia fizyczne 193
Zamknij drzwi 193
Utrzymanie zasilania 193
Pozbywanie się sprzętu i nośników 194
Dwie strony zabezpieczeń 194
Przed faktem: kontrola dostępu 194
Po fakcie: inspekcja 196
Hasła 197
Usługi i demony systemowe 199
Przeglądanie domyślnych ustawień 201
Delegowanie uprawnień 201
Konta użytkowników 202
Serwery aplikacji, serwery wydruku i serwery WWW 202
Wirusy komputerowe 203
Inne destrukcyjne programy 204
Jak dochodzi do infekcji 204
Kroki prewencyjne 205
Źródła informacji o wirusach 205

Rozdział 16. Firewalle 207
Co to jest firewall? 207
Czego można oczekiwać od firewalla? 209
Filtry pakietów 211
Udawanie adresów IP 212
Wykrywanie ataku 212
Serwery proxy 213
Translacja adresów sieciowych (NAT) 213
Zwiększanie przestrzeni adresowej 214
Bramy dla aplikacji 214
Wady i zalety serwerów proxy 216
Hybrydy 216
Skąd wiadomo, że firewall jest bezpieczny? 217

Rozdział 17. Inspekcja i inne zagadnienia monitorowania 219
Systemy Unix i Linux 220
Korzystanie z syslog 220
Plik dzienników systemowych 223
Systemy Windows NT 223
Ustawianie zdarzeń do inspekcji 224
Korzystanie z podglądu zdarzeń 227
Zabezpieczenia Novella 228
SYSCON i AUDITCON 228
Programy typu SATAN 231

Rozdział 18. Szyfrowanie 233
Komputery i prywatność 233
Szyfrowanie symetryczne 234
Szyfrowanie asymetryczne 235
PGP (Pretty Good Privacy) 236
Instalowanie PGP w systemach uniksowych 236
Instalowanie PGP w Windows NT 240

Rozdział 19. Przejście z Ethernetu 10 Mb/s do 1000 Mb/s 245
Istniejąca struktura okablowania 245
Sprawdzanie, czy istniejące kable wystarczą dla szybkości 100 Mb/s i większych 246
Gigabit Ethernet kable UTP 247
Najczęstsze przyczyny fizycznych problemów z Gigabit Ethernetem 248
Standardy dla Gigabit Ethernetu z użyciem przewodów i światłowodów 250
Przejście do Gigabit Ethernetu 251
Przyspieszanie Fast Ethernetu jako alternatywa dla Gigabit Ethernetu 252

Rozdział 20. Przejście z 10Base-2 do 10Base-T 253
Czynniki sprzętowe 253
Kable sieciowe 254
Karty sieciowe 255
Konektory 256
Mosty, koncentratory i routery 256
Inne możliwości 257

Rozdział 21. Przejście z Token-Ring do Ethernetu 259
Dlaczego Ethernet? 259
Dopasowanie Ethernetu do sieci Token-Ring 260
Różnice utrudniające przejście 261
Bity i ramki 261
Powiadamianie o dostarczeniu 262
Informacje o trasach 262
Wymiana całego sprzętu Token-Ring 263
Koncentratory, przełączniki i routery 263
Okablowanie i konektory sieciowe 263
Karty sieciowe 264
Scenariusz konwersji sieci 264

Rozdział 22. Przejście od mostów do routerów i przełączników 267
Rozbudowa poza małą sieć lokalną 267
Podział sieci na segmenty 268
Łączenie odległych miejsc 269

Kiedy należy użyć routera 269
Kiedy należy użyć przełącznika? 269
Przejście od mostów do routerów 269
Zagadnienia protokołów sieciowych 270
Zagadnienia adresów sieciowych 270
Inne zagadnienia zarządzania routerem 271
Użycie routera do podziału sieci na segmenty 271
Łączenie z większą siecią WAN 272
Przejście od mostów do przełączników 272

Rozdział 23. Przejście z sieci ARCnet do Ethernetu 275
Omówienie sieci ARCnet 275
Koncentratory i okablowanie 276
Karty sieciowe 278
Współpraca nowego i starego sprzętu 278
Aktualizacja do Ethernetu 278
Kable sieciowe 279
Wybór rozwiązania ethernetowego 279
Układ nowej sieci 280
Rozwiązywanie problemów z wydajnością 282

Rozdział 24. Przejście z Novell NetWare do Windows NT 4.0 283
Protokoły 284
Usługi dla NetWare 284
CSNW (Client Services for NetWare) 284
GSNW (Gateway Services for NetWare) 285
Usługi plików i drukarek dla NetWare (FPNW) 286
Narzędzie migracji do Windows NT 286
Opis szczegółowy 287
Opcje użytkownika 288
Opcje haseł 289
Konflikty nazw użytkowników 289
Konflikty nazw grup 290
Ograniczenia konta 290
Uprawnienia administratora 290
Odwzorowywanie kont 290
Opcje plików 291
Wybór woluminów do przeniesienia 291
Określanie docelowych udziałów 292
Wybór folderów i plików do przeniesienia 292
Przenoszenie plików ukrytych i systemowych 292
Skrypty logowania 292
Próbne przejście 292
Przeglądanie plików dzienników 292
Rozpoczęcie przejścia 293
Ograniczenia folderów i plików 295
Udostępniane pliki 296
Kolejność uprawnień 297
Konflikty uprawnień plików i kartotek 298
Uprawnienia przejmowania na własność 298
Udostępnianie drukarki 298
Aplikacje 299
Aplikacje administracyjne 299
Aplikacje użytkowników 303

Narzędzia konwersji 303
Szkolenie 303

Rozdział 25. Przejście z Uniksa do Windows NT 4.0 305
Przeniesienie kont użytkowników 306
Logowanie do systemu 306
Konta użytkowników 308
Skrypty logowania 315
Tworzenie skryptów logowania 316
Tworzenie udostępnianych plików i drukarek w serwerze Windows NT 4.0 317
Udostępniane pliki 317
Uprawnienia dostępu do plików 318
Udostępnianie plików 318
Tworzenie udostępnionych drukarek 320
Inspekcja użytkowników drukarek 322
Aplikacje 322
Narzędzia 323
Procesory tekstu 324
Aplikacje baz danych 325
Arkusze kalkulacyjne 325
Programy graficzne 325
Aplikacje poczty elektronicznej 326
Wiadomości i grupy dyskusyjne 327
Aplikacje sieciowe 328
Narzędzia konwersji Microsoftu 332
Usługi plików 332
Usługi połączeń 332
Usługi użytkowe 332
Inne narzędzia konwersji 333

Rozdział 26. Migracja z Windows NT 4.0 do NetWare 335
Dodawanie użytkowników w NetWare 338
Używanie grup 338
Tworzenie obiektu typu liść 339
Skrypty logowania 340
Tworzenie skryptów logowania 342
Stosowanie NetWare Administratora do tworzenia skryptów logowania 342
Tworzenie zasobów plikowych i drukowania w NetWare 344
Udostępnianie drukarek 344
Tworzenie zasobów plikowych 346
Aplikacje 347
Corel WordPerfect Suite 348
Oprogramowanie do przetwarzania tekstu 348
Oprogramowanie do archiwizacji 348

Rozdział 27. Przejście z Windows NT 4.0 do Windows 2000 349
Active Directory 349
Kartoteka i usługi katalogowe 350
Interesujące obiekty 350
Czego dostarcza Active Directory? 351
Od X.500 i DAP do LDAP 352
Czym jest schemat? 354
Obiekty i atrybuty 355
Standardowe obiekty kartoteki 357

Nazywanie obiektów kartoteki 358
Modyfikowanie schematu 359
Co to jest drzewo domeny? Co to jest las? 361
Modele domen — niech spoczywają w spokoju! 361
Kartoteka jest podzielona na domeny 362
Domena pozostaje domeną 363
Drzewa i lasy 363
Active Directory i Dynamiczny DNS 364
Szkielet Internetu a Active Directory 365
Dynamiczny DNS 365
Jak Active Directory korzysta z DNS 365
Używanie witryn do zarządzania dużymi przedsiębiorstwami 366
Replikacja kartoteki 367
Podsumowanie danych kartoteki z użyciem katalogu globalnego 369
Interfejsy usług Active Directory (ADSI) 369
Programowanie aplikacji zgodnych z Active Directory 370
Przygotowanie do przejścia do Windows 2000 371
Kontrolery domen i serwery składowe 372
Odtworzenie struktury kartoteki dla firmy lub organizacji 373
Domeny — część przestrzeni nazw 374
Zagadnienia związane z przejściem: zarządzanie scentralizowane i zdecentralizowane 375
Implementowanie przejścia do Active Directory 376
Najpierw zaktualizuj podstawowy kontroler domeny 377
Inne domeny mogą dołączyć do istniejącego drzewa 379
Domena główna jako pierwsza 379

Rozdział 28. Integrowanie Windows NT 4.0 z Linuksem 383

Konwertowanie kont użytkowników 383
Prawa do plików 384
Grupy 384
Praca z użytkownikami w Linuksie 384
Format i położenie kont użytkowników 385
Informacje o użytkowniku 386
Dodawanie użytkownika ręcznie 386
Przypisywanie użytkownika do grupy 388
Kopiowanie profili 389
Usuwanie użytkowników 389
Zasoby plików i drukarek 389
Rodzaje plików w Linuksie 390
I-węzły 391
Prawa dostępu do plików 391
Drukarki 394
Aplikacje 396
Przetwarzanie tekstu 397
Arkusze kalkulacyjne 398
Bazy danych 399
Transfer plików 399
DNS 401
Konfigurowanie resolvera 401
Demon named 402
Sprawy sprzętowe 405
Płyty główne 405
Procesory 405
Pamięć 406

Karty graficzne....406
Kontrolery dysku twardego....406
Kontrolery SCSI....406
Kontrolery wejścia-wyjścia....407
Karty sieciowe....407
Karty dźwiękowe....407
Napędy taśmowe....408
Napędy CD-ROM oraz nagrywarki....408
Myszy....408
Modemy....408
Drukarki....409
Skanery....409
Inne urządzenia....409
Pozostałe narzędzia konwersji....409

Rozdział 29. Integracja Novell NetWare i Linuksa....411
Po co migrować do Linuksa?....411
Najważniejsze różnice między Linuksem i NetWare....412
Dzielenie plików....412
Dzielenie drukarek....413
Uwierzytelnianie użytkownika....413
Przenoszenie kont użytkowników....413
Sieć....413
Aplikacje....414
Pozostałe narzędzia....414

Rozdział 30. Integracja NetWare z Windows NT....417
Narzędzia klientów Microsoft....417
Usługi plikowe i drukowania dla NetWare (FPNW)....418
Usługi bram dla NetWare (GSNW)....422
Menedżer usług katalogowych dla NetWare (DSMN)....425
Usługi klientów dla NetWare (CSNW)....427
Narzędzia NetWare....428
Klient Novell dla Windows NT....428
NDS dla NT....432

Rozdział 31. Integracja Uniksa, Linuksa i Windows NT....435
Obsługa protokołów oraz narzędzi Uniksa przez Windows NT....436
TCP/IP....436
Protokół dynamicznego konfigurowania hostów (DHCP) oraz BOOTP....437
DNS....438
Pakiet Microsoft Windows NT usług dodatkowych dla Uniksa....439
SAMBA....441
Edycja serwera terminalowego Windows NT....441

Rozdział 32. Integracja Uniksa, Linuksa, NetWare oraz Windows NT....443
Konta użytkowników....443
NetWare i Windows NT....444
Dostęp do Windows NT z systemu NetWare....444
Unix i konta użytkowników systemu Windows NT....445
Zrozumienie praw dostępu i uprawnień systemowych....445
Pełna kontrola (Full Controla)....445
Odczyt....447
Uprawnienie do zmiany....448

Dodawanie 448
Przejęcie posiadania 449
Inne prawa 450
Protokoły sieciowe 451
Instalacja TCP/IP w Windows NT 452
NetWare TCP/IP 452
Udostępnianie plików oraz drukarek wszystkim użytkownikom 452
Protokół SMB 453
Intranet 454

Dodatek A Siedmiowarstwowy model sieciowy OSI 455
Przegląd modelu OSI 455
Warstwa fizyczna 456
Warstwa łącza danych 456
Warstwa sieci 457
Warstwa transportu 457
Warstwa sesji 458
Warstwa prezentacji 458
Warstwa aplikacji 458
Jak podstawowe protokoły sieciowe odnoszą się do modelu OSI? 458

Skorowidz 461

Rozdział 3.

Karty sieciowe

Główne tematy omawiane w tym rozdziale:

- Wybór rodzaju magistrali sprzętowej: PCI, ISA czy EISA?
- Sterowniki programowe
- Stosowanie kilku kart sieciowych w jednym komputerze
- Przerwania IRQ
- Podstawowe porty wejścia-wyjścia
- Rozwiązywanie problemów związanych z kartami sieciowymi

NIC, czyli interfejs sieciowy (*Network Interface Card*) jest to urządzenie łączące komputer z medium transmisyjnym. Karta sieciowa działa wykorzystując warstwę fizyczną siedmiowarstwowego modelu referencyjnego OSI i jest odpowiedzialna za dostosowanie danych do transmisji w sieci poprzez medium transmisyjne. Mimo że w wielu produkowanych kartach stosowana jest technologia Plug and Play, to niestety, nie we wszystkich. Chociaż instalowanie nowej karty w komputerze lub wymiana starej na nową nie wydają się skomplikowanym zadaniem, to jednak czasami sprawiają trudność. W tym rozdziale zajmiemy się zagadnieniami konfiguracyjnymi kart sieciowych oraz wymienimy sposoby rozwiązywania problemów z kartami, które nie działają tak, jak powinny.

Wybór rodzaju magistrali systemowej: PCI, ISA, CZY EISA?

Magistrala *ISA* reprezentuje starszy typ architektury, który powoli wychodzi z użycia, jako że producenci proponują obecnie komputery z magistralą typu *EISA*. Najnowszą magistralą jest *PCI* (Peripherial Component Interconnect). Ma ona więcej zalet niż poprzednie (ISA, EISA) modele (włącznie z szybszym transferem informacji oraz 32- lub 64-bitowym kanałem danych). Urządzenia wykorzystujące PCI mogą także użyć funkcji zwanej „przejęciem szyny" (Bus Mastering), co pozwala im przechwytywać kontrolę nad magistralą i bezpośrednio, bez ingerencji procesora, przetransferować duże ilości danych do pamięci systemu. Microsoft i inni wiodący dostawcy oprogramowania są skłonni w ciągu 2 lat zaprzestać obsługi sprzętu wykorzystującego ISA i EISA. Z tego względu warto raczej rozważyć zakup karty sieciowej o standardzie PCI niż starszych, „przeterminowanych", jak niedługo będą nazywane karty ISA i EISA.

Sterowniki programowe

W czasach kiedy sieci tworzone były na zamówienia indywidualnych klientów i składały się z rozwiązań opracowanych dla ich specyficznych systemów, sprzedawca tworzył prosty sterownik, który obsługiwał wszystkie funkcje tych protokołów, które zaimplementował na karcie. Obecnie zazwyczaj zachodzi konieczność korzystania z kilku różnych protokołów w sieci, tak więc współczesne sterowniki muszą obsługiwać kilka lub większość protokołów powszechnie stosowanych.

Czynnikiem, który należy rozważyć, biorąc pod uwagę serwery lub routery, jest system posiadający więcej niż jeden typ zainstalowanych kart sieciowych. W tym wypadku sterownik musi być zdolny do rozróżnienia zarówno odmiennych interfejsów sieciowych, jak i wykorzystywanych na nich protokołów.

Dwa główne rodzaje programowych sterowników interfejsów sieciowych, które można obecnie spotkać, to ODI oraz NDIS. Wcześniej pojawił się inny rodzaj sterownika, zwany Packet Driver (sterownik pakietowy), który został wynaleziony przez FTP Software w 1986 roku. Ponieważ różne systemy operacyjne, lub oprogramowanie sieciowe, mogą pracować tylko z określonym sterownikiem, należy zwracać uwagę na jego rodzaj w kontekście współpracy z karta sieciową; zwłaszcza jeśli planuje się wymianę karty na nowszą lub zmianę systemu operacyjnego. Na przykład w sieci Novella potrzebne są karty wykorzystujące sterowniki ODI. Natomiast w środowisku sieciowym Microsoftu wymagane są karty obsługujące NDIS.

Sterowniki pakietowe

We wczesnych stadiach rozwoju sieci komputerowych główny problem z kartami sieciowymi i stosami protokołu polegał na tym, że były one zbyt ściśle powiązane ze sobą; kupno właściwego oprogramowania gwarantowało obsługę posiadanej karty. Kod programu, który współpracował z daną kartą, był dostarczany przez odpowiedni pakiet protokołu zamiast przez system operacyjny. To oczywiście oznacza, że projektanci stosów protokołu musieli spędzać dużo czasu nad stworzeniem kodu, który zapewniałby obsługę wszystkich rodzajów kart sieciowych znajdujących się aktualnie w sprzedaży.

Sterownik pakietowy został wynaleziony przez FTP Software po to, by stworzyć taki interfejs, który mógłby być wykorzystywany przez protokoły w celu uzyskania dostępu do funkcji dostarczanych przez kartę sieciową. Stosy protokołu, które używały tego sterownika, mogły istnieć w komputerze oraz jednocześnie używać karty sieciowej. Wcześniej sterowniki były mocno związane z kartą sieciową już od samego startu systemu i trzeba było restartować komputer za każdym razem, kiedy zaistniała potrzeba użycia innego protokołu sieciowego.

ODI

Otwarty interfejs łącza danych (Open Data-Link Interface, ODI) został zaprojektowany przez firmę Novell i Apple Computers w 1989 roku w celu zapewnienia połączenia z warstwą sieciową, transportową i łącza danych, jak pokazuje model referencyjny OSI. Specyfikacja ODI może być podzielona na trzy główne komponenty:

- *Sterownik interfejsu wielopołączeniowego* (Multi-Link Interface Driver MLID) — ten składnik kontroluje komunikację pomiędzy kartą sieciową a warstwą obsługi połączenia (link support layer, LSL). Zawiera on części z kodem napisanym przez firmę Novell, zwanym *modułem wspomagania medium* (Media Support Module, MSM) oraz *modułem specyfikacji sprzętowej* (Hardware-Specific Module, HSM), stworzonym przez producenta karty sieciowej. Moduł MSM umożliwia uruchamianie standardowych funkcji sieciowych dla medium sieciowego obsługiwanego przez ODI.
- *Warstwa wspomagania połączenia* (LSL) — ta warstwa pozwala na przypisanie wielu protokołów do jednej karty sieciowej. LSL jest bramką, która określa, do kogo należy dany pakiet stosu protokołu, i tam go wysyła.
- *Stos protokołu* (Protocol Stack) — ten komponent otrzymuje pakiety od LSL i wysyła je do protokołu wyższego poziomu lub aplikacji.

Ze względu na swą modularną budowę ODI sprawia, że pisanie stosów protokołu lub sterowników jest dużo łatwiejsze dla sprzedających podzespoły komputerowe. Programista, który pracuje nad oprogramowaniem, aby zaimplementować protokół, musi jedynie stosować się do specyfikacji interfejsu ODI, bez przyglądania się konkretnej karcie lub medium sieciowemu. Producent karty musi po prostu dbać o to, aby program, który komunikuje się z MSM, umożliwiał korzystanie z funkcji dostępnych na karcie sieciowej.

NDIS

Specyfikacja interfejsu sterownika sieciowego (Network Driver Interface Specification, NDIS) została początkowo zaprojektowana przez firmy Microsoft i 3Com (nowsze wersje zostały rozwinięte przez Microsoft). NDIS służy mniej więcej do tych samych celów co ODI, z tym że umożliwia istnienie wielu stosów protokołu na wielu kartach sieciowych w jednym komputerze. Jednakże szczegóły aktualnej implementacji są trochę inne.

W Windows NT protokoły transportowe łączą część warstwy transportu, warstwy sieci oraz część warstwy łącza danych. Protokoły transportowe takie jak Ramka NetBEUI (NBF) czy TCP są wprowadzane przez wywołanie odpowiednich serwisów w interfejsie NDIS. Sterownik ten nie ukrywa do końca medium sieciowego przed stosem protokołu, tak jak to robi ODI. Sytuacja ta ogranicza sterowniki do korzystania ze specyfikacji Ethernet 802.3 lub Token Ring 802.5. Dla przykładu, sterowniki dla sieci ARCnet są tak napisane, że uwzględniają powyższe ograniczenie i powodują, że dla warstwy oprogramowania sieć wygląda jak Ethernet lub Token Ring.

Obydwa sterowniki (ODI i NDIS) wzajemnie ze sobą współpracują. ODI dostarcza program zwany ODINSUP przeznaczony do współpracy ze sterownikiem NDIS. Windows NT oferuje program NWLink, który jest Microsoftową implementacją protokołów IPX/SPX. System ten zawiera też usługę klienta dla NetWare, która pozwala stacjom roboczym Windows NT na dostęp do danych umieszczonych na serwerach NetWare. Usługi Bramy (Gateway Services) dla NetWare spełniają podobne funkcje, używając pojedynczego komputera Windows NT jako bramy dla usług Novell NetWare. Osobnym pakietem firmy Microsoft są Usługi plikowe i drukowania (FILE and Print Services) dla Netware, który umożliwia klientowi Netware dostęp do zasobów sieci Windows NT.

Systemy wieloportowe

Niektóre komputery wymagają więcej niż jednej karty sieciowej. Na przykład, jeśli w danej sieci LAN istnieją dwie podsieci, które muszą łączyć się z tym samym serwerem, to serwer ten będzie musiał używać więcej niż jednej karty sieciowej. Niektóre systemy operacyjne pozwalają serwerowi na przekazywanie pakietów pomiędzy podsieciami, jeśli komputer taki ma zainstalowaną więcej niż jedną kartę. Zależnie od rodzaju komputera, możliwe jest również przyłączenie więcej niż jednej karty obsługującą jedną podsieć. Zawsze jednak do każdej karty należy przypisać właściwy adres sieciowy i nazwę serwera.

Na przykład wysoko wydajny serwer może zostać wykorzystany w intranecie do udostępniania usług WWW oraz FTP. Jeśli serwer jest w stanie obsłużyć wszystkie żądania użytkowników z wymaganą szybkością, ale karta sieciowa jest czynnikiem ograniczającym wykonywanie tych zadań, można zainstalować kilka kart i nadać każdemu serwisowi (WWW, ftp) odrębną nazwę serwera i unikalny adres sieciowy.

Przerwania

Pomimo że w wielu nowych kartach zastosowano technologię Plug and Play, to jednak ta właściwość nie jest obsługiwana przez wszystkie systemy (np. liczne odmiany Uniksa). Z tego powodu może się zdarzyć, że trzeba będzie samodzielnie skonfigurować kartę, w przypadku jej wymiany na nowszą lub w sytuacji, kiedy dodając nową, spowoduje się konflikt z kartą już zainstalowaną. Dwa główne parametry, które zazwyczaj są modyfikowane, to wartości *Obsługi żądania przerwania* (Interrupt ReQuest Line) oraz *podstawowego portu wejścia-wyjścia* (base I/O port).

Kiedy urządzenie podłączone do magistrali komputera stara się „zwrócić na siebie uwagę" procesora, używa mechanizmu zwanego IRQ. Przerwania te są realizowane przez sygnały wysyłane do procesora poprzez warstwę sprzętu. Jest to połączenie bezpośrednie. Ze względu na fakt, że istnieje wiele urządzeń żądających obsługi w tym samym czasie, jedno IRQ (żądanie przerwania) nie wystarczy. Zamiast tego w większości przypadków każde urządzenie ma własny zakres przerwań. Kiedy urządzenie zgłasza procesorowi potrzebę obsługi, to sygnalizuje mu, że ma on do rozpatrzenia żądanie obsługi przerwania i że musi ono zostać spełnione najszybciej, jak to tylko jest możliwe.

Gdy tylko CPU otrzyma żądanie przerwania, to oddaje swoje zasoby właściwemu urządzeniu na taki czas, przez jaki nie będzie musiał obsługiwać przerwania o wyższym priorytecie. Jest również możliwa taka sytuacja, że procesor wykonuje aktualnie jakieś krytyczne zadanie i nie odpowiada na przerwanie. W tym wypadku CPU nie przerywa wykonywanego zadania. Takie przerwanie jest nazywane przerwaniem maskowalnym. Oznacza to, że procesor może wejść w stan, w którym maskuje wszystkie przerwania, podczas gdy jest zajęty wykonywaniem bardzo ważnego zadania, a później, kiedy jest w stanie wykonywać inne funkcje, przywraca obsługę przerwań.

Ilość IRQ, które są dostępne w systemie, zależy od rodzaju magistrali systemowej. Wczesne pecety, które bazowały na magistrali ISA, miały tylko osiem sprzętowych przerwań, ponumerowanych od 0 do 7, pokazanych w tabeli 3.1.

Tabela 3.1. *Przerwania magistrali ISA*

IRQ	Funkcje
0	System Timer — zegar systemowy
1	Keyboard Controller — kontroler klawiatury
2	Available — dostępne
3	Serial Port 2 and 4 — port szeregowy 2 i 4
4	Serial Port 1 and 3 — port szeregowy 1 i 3
5	Hard Disk Drive Controller — kontroler dysku twardego
6	Floppy Diskette Drive Controller — kontroler stacji dyskietek
7	Parallel Port — port równoległy

Ten mały zestaw przerwań wystarczał dla niewielkiego systemu zawierającego jedynie kilka urządzeń. Jak można zauważyć, tylko jedno przerwanie — 2 — jest dostępne dla dodatkowego urządzenia. Kiedy została wprowadzona magistrala EISA, podwoiła się liczba przerwań. Jednakże, aby to było możliwe, potrzebne były dwa kontrolery przerwań, jeden z nich przesyłał swoje przerwania poprzez kanał, którym był IRQ2. Oznaczało to, że faktycznie dla urządzeń w systemie dostępnych było 15 przerwań. Tabela 3.2 pokazuje, jakie urządzenia korzystają zazwyczaj z poszczególnych przerwań.

Tabela 3.2. *Urządzenia korzystające z przerwań magistrali ISA*

IRQ	Funkcje
0	System timer — zegar systemowy
1	Keyboard controller — kontroler klawiatury
2	Second Interrupt controller — kontroler drugiego przerwania
8	Real-time clock — zegar czasu rzeczywistego
9	Network Card — karta sieciowa
10	Available — dostępne
11	SCSI Card
12	Motherboard mouse port — port myszy
13	Math coprocessor — koprocesor matematyczny
14	Primary IDE (Hard Disk Drive) controller — kontroler głównego kanału IDE
15	Secondary IDE (Hard Disk Drive) controller — drugi kontroler IDE
3	Serial port 2 and 4 (COM2; COM4) — port szeregowy drugi i czwarty
4	Serial port 1 and 3 (COM1; COM3) — port szeregowy pierwszy i trzeci
5	Sound card or paraller port 2 — karta dźwiękowa lub port równoległy drugi
6	Floppy Diskette Drive controller — kontroler stacji dyskietek
7	Parallel Port — port równoległy

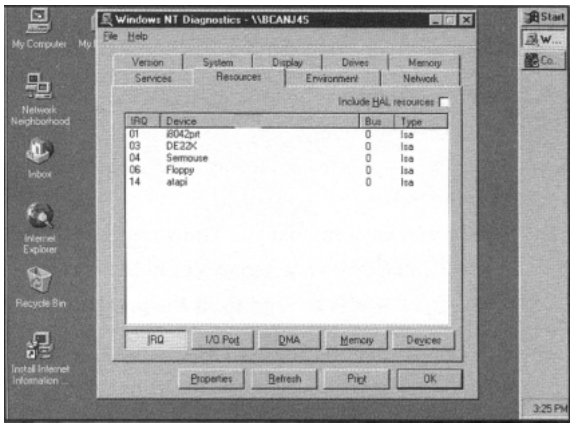
Warto zauważyć, że numery przerwań opisane w tabeli 4.2 nie są ułożone po kolei. Zamiast tego ustawione są w porządku priorytetowym; te u góry tabeli mają wyższy priorytet niż te na dole. Ponieważ osiem kolejnych przerwań zostało dodanych przez mechanizm, który używa oryginalnego IRQ2, przerwania te mają wyższy priorytet niż IRQ 3 – 7. W niektórych systemach IRQ9 jest używany do zapewnienia tych samych funkcje co IRQ2 we wcześniejszej wersji magistrali. Dlatego na niektórych kartach można znaleźć to IRQ oznaczone jako 2, 9 lub też IRQ2/9.

Jeśli dany komputer wykorzystuje technologię Plug and Play, może się okazać, że nie trzeba wprowadzać żadnych zmian wartości IRQ bezpośrednio na karcie sieciowej lub w systemie operacyjnym. Jeśli jednak jest inaczej, należy się upewnić (w dokumentacji karty), jakich można użyć przerwań i jak je ustawić. Przerwania zazwyczaj wybiera się, ustawiając odpowiednie zworki na karcie sieciowej.

Podstawowe porty wejścia-wyjścia

Podobnie w sytuacji, kiedy system operacyjny danego komputera nie obsługuje technologii Plug and Play, trzeba będzie ręcznie skonfigurować wartości adresu pamięci, który to adres jest wykorzystywany przez kartę sieciową do transferu danych do systemu i z powrotem. Wysyłając do procesora żądanie obsługi przerwania, karta sieciowa używa adresu pamięci zwanego podstawowym portem wejścia-wyjścia. Ponieważ wiele urządzeń używa adresów pamięci, ważne jest, aby skonfigurować każde urządzenie tak, żeby używało innego adresu pamięci; żaden transfer danych nie będzie wtedy kolidował z innymi.

W większości systemów 64 kB pamięci jest przypisywane do wykorzystania przez porty wejścia-wyjścia, a więc nie są to tak ograniczone zasoby jak w przypadku IRQ. Warto sprawdzić w dokumentacji systemu operacyjnego, jak wyświetlić zajęte obecnie adresy pamięci dla tego obszaru (64 kB). Na przykład w Microsoft Windows NT istnieje program zwany Microsoft Diagnostic (narzędzie diagnostyczne), który służy do wyświetlania różnorodnych konfiguracji sprzętowych i programowych. Rysunek 3.1 przedstawia okno, na którym widać porty wejścia-wyjścia na serwerze Windows NT. Proszę zauważyć, że na dole okna znajdują się przyciski, których należy użyć w celu obejrzenia innych związanych z urządzeniem informacji takich jak IRQ oraz alokacje pamięci.



Rysunek 3.1. *Narzędzie Microsoft Diagnostic pokazuje, jak przypisane są porty wejścia i wyjścia*

W dodatku niektóre urządzenia używają zasobów pamięci do tymczasowego buforowania danych. W tym celu wymagają określenia podstawowego adresu pamięci, który wskazuje na początek bufora. Dana karta sieciowa może, ale nie musi, używać pamięci RAM komputera, więc w sytuacji gdy powstaną jakieś kłopoty należy dokładnie przeczytać dokumentację.

Rozwiązywanie problemów z kartami sieciowymi

Kiedy w czasie instalacji lub wymiany karty sieciowej okazuje się, że coś nie działa tak, jak powinno, można wykonać kilka czynności umożliwiających wykrycie problemu. Przyczyną może być uszkodzona karta sieciowa, komputer, koncentrator lub kabel, który łączy kartę z koncentratorem, a także prosty problem przy zmianie konfiguracji urządzenia.

Dodając nową kartę sieciową do stacji roboczej, należy najpierw przejrzeć dokumentację dostarczoną wraz z urządzeniem, aby określić, jakich wartości należy używać dla IRQ, podstawowego portu wejścia-wyjścia itd. Trzeba również przeczytać dokumentację pozostałych urządzeń znajdujących się w systemie, ponieważ w trakcie rozwiązywania konfliktu sprzętowego może się okazać, że należy zmienić parametry innego urządzenia, a nie karty sieciowej.

Diody LED

Karty sieciowe mają zazwyczaj jedną diodę LED (dioda elektroluminescencyjna — light emitting diode) widoczną na zewnątrz komputera. Generalnie dioda taka powinna świecić, gdy karta jest w stanie komunikować się z siecią. Większość koncentratorów posiada diody określające stan każdego portu, więc dobrze jest sprawdzić za ich pomocą także koncentrator. Przyczyna może leżeć po stronie koncentratora, karty sieciowej lub także w kablu łączącym obydwa urządzenia. Oczywiście należy najpierw sprawdzić w dokumentacji karty przeznaczenie każdej z diod. Na przykład niektóre karty firmy 3Com mają jedną diodę wskazującą status połączenia. Jeśli świeci, to znaczy, że połączenie jest prawidłowe; jeśli miga, oznacza to trudności w transmisji i odbiorze (odwrotna polaryzacja). Inna dioda LED służy do określania wysyłania i odbioru danych przez kartę.

Jeśli okaże się, że występuje problem z połączeniem, trzeba spróbować go zlokalizować i określić jego przyczynę, wykonując następujące czynności:

- Sprawdzić wszystkie wtyczki, czy na pewno są wpięte w odpowiednie gniazda.
- Wypróbować inny port w koncentratorze.
- Wypróbować inny kabel, najlepiej taki, o którym wiadomo, że działa.
- Przełożyć kartę sieciową do innego slotu w komputerze.
- Zamienić kartę sieciową na taką, która działa i sprawdzić, czy problem nadal występuje.

Jeśli żadna z powyższych operacji nie rozwiąże problemu, trzeba kartę sieciową zainstalować w komputerze, w którym taki problem nie występuje. Jeżeli karta będzie działać prawidłowo, to znaczy, że problem nie jej dotyczy.

Program diagnostyczny karty sieciowej

Większość kart, nawet te oznaczone jako Plug and Play, jest sprzedawanych z dyskietką zawierającą sterowniki oraz program diagnostyczny. Często niezbędne okazuje się wystartowanie komputera w trybie MS-DOS i uruchomienie programu diagnostycznego. W praktyce niektóre karty dostarczane są także z dyskietką do uruchomienia w trybie MS-DOS. Kiedy używa się takiego programu diagnostycznego, należy się upewnić, że żaden inny sterownik nie jest załadowany, ponieważ mogłoby to wpłynąć na wyniki przeprowadzanych testów. Proszę zauważyć, że MS-DOS nie oznacza okna trybu MS-DOS w systemie Windows98 czy NT, ale oznacza uruchomienie komputera w systemie operacyjnym MS-DOS.

Rodzaje testów, które można przeprowadzić, są różne, ale prawdopodobnie wyświetlone zostanie menu, które umożliwi przeprowadzenie jednego lub równocześnie wszystkich testów, jakie udostępnia program diagnostyczny. Mogą to być testy sprawdzające sprzęt oraz testy pętli zwrotnej. Niektóre karty umożliwiają także testy echa, w którym dwie karty tego samego producenta dla celów diagnostycznych mogą wysyłać do siebie nawzajem i otrzymywać od siebie pakiety danych. Jeśli karty nie mogą przejść pozytywnie wszystkich testów udostępnionych przez producenta i jeśli jest pewne, że nie występuje żaden inny problem (np. niewłaściwy slot na magistrali systemowej), to prawdopodobnie uszkodzona jest karta sieciowa i trzeba ją wymienić.

Konflikty konfiguracyjne

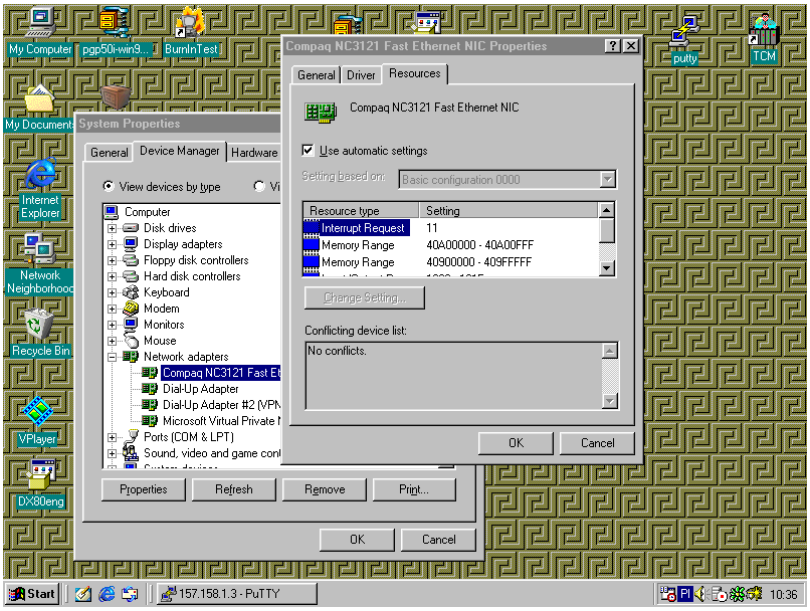
Jeżeli karta przejdzie pomyślnie wszystkie testy diagnostyczne i nie ma żadnych uszkodzeń w jej fizycznych komponentach, w systemie operacyjnym czy też koncentratorze, to trzeba sprawdzić ustawienia konfiguracyjne karty. Wcześniej przedstawiono narzędzie Microsoft Diagnostic dla Windows NT, które może zostać użyte do określenia zasobów adresów pamięci, dla jakich karta została skonfigurowana. Program ten może być użyty do ustalenia, jakiego IRQ używa zainstalowana karta, oraz innych informacji konfiguracyjnych. Na rysunku 3.2 widać ten program działający w systemie Windows 98.

W dolnej części zakładki *Resources* znajduje się pole *Conflicting device list*. W tym przypadku żadne urządzenia nie są na niej wymienione. Gdyby jednak lista zawierała jakieś urządzenia, można podjąć odpowiednie kroki i przypisać inne wartości IRQ oraz adresów pamięci, żeby żadne urządzenia nie powodowały konfliktów zasobów.

Dla użytkowników Uniksa sytuacja jest bardziej skomplikowana. W wielu przypadkach dodanie nowego sprzętu wymaga rekompilacji jądra i restartu systemu. Wiele systemów właściwie rozpozna sprzęt i skonfiguruje go automatycznie, ale nie zawsze tak będzie. Zależnie od wersji systemu Unix będziesz musiał sprawdzić pliki konfiguracyjne w celu określenia przerwań i adresów pamięci używanych przez dane urządzenie.

Kroki zapobiegawcze

Bieżące gromadzenie informacji systemowych dla komputerów w danej sieci może bardzo pomóc w rozwiązywaniu problemów. Na przykład arkusz, w którym znajduje się lista wszystkich węzłów sieci wraz z informacjami konfiguracyjnymi, może okazać się



Rysunek 3.2. *W systemie Windows 98 można sprawdzić, czy występują konflikty sprzętowe, przy użyciu narzędzia Microsoft Diagnostic*

przydatny, kiedy trzeba będzie zmienić lub wymienić na nowszy określony komponent. Posiadanie tych informacji pozwala zaoszczędzić sporo czasu przy rozwiązywaniu problemu w momencie, kiedy ten się pojawi.

Taki rodzaj informacji może być również użyteczny podczas podejmowania decyzji o zakupie sprzętu. Na przykład, jeśli wiadomo, ile magistrali ISA i PCI dostępnych jest w danej stacji roboczej i które z nich są już zajęte, to nie popełni się błędu polegającego na zakupie karty przeznaczonej dla magistrali ISA, na którą już nie ma miejsca, bo wszystkie sloty ISA są już zajęte.