Cisco Systems

Софтпрес
издателство
www.soft-press.com

Компютърни мрежи

Пълно ръководство по теория, изграждане и съвместна работа между мрежите

ciscopress.com

Дебра Литълджон Шиндър

ъдържание

т 1 **Въведение в мрежите 25**

ва 1 Въведение в мрежите 27

Кратка история на компютърните мрежи 27
Първите комуникационни мрежи 28
Недостатъци на самостоятелните системи 32
Какво все пак означава мрежа? 32
Защо мрежови компютри? 33
Предимства на свързването към мрежа 34
Раждането на Интернет 35
Цената на технологията: Все повече и повече за все по-малко и по-малко 37

Днешните компютърни мрежи 38
Работа с компютър вкъщи 38
Присъствие в Web и електронна търговия 38
Високопроизводителни бизнес решения 38
Онлайн обучение 38

Мрежите на утрешния ден 39
„Интелигентни“ домакински електроуреди 39
Телефониране от вкъщи 40
Свързаното в мрежа работно място 41
Училищата на бъдещето 41
Грижа за здравето по мрежата 42
Технологията и законът 42
Интергалактически мрежи? 42

Кратък преглед на терминологията на мрежите 43
Терминология, свързана с концепциите 43
Терминология, свързана с мрежовия хардуер 44
Терминология, свързана със софтуера 45
Терминология на дизайна и топологията 45
Терминология, свързана с мерните единици 46

Какво обхваща книгата и какво – не 47

Сертификати по мрежи 47
Сертификати, специфични за производителя 47
Сертификати, необвързани с производител 48
Тази книга и сертифицирането 48

Обобщение 48

Допълнителни източници 49

Въпроси за преговор 49

Глава 2 Категоризиране на мрежите 53

Категоризация на мрежите според физическия обхват 53
Характеристики на LAN мрежата 54
Характеристики на MAN мрежата 55

Категоризация на мрежите по метод на администриране 58
Сървъри и клиенти 59
Сървъри, споделящи „споделени ресурси“ 60
Характеристики на мрежите, базирани на сървъри 66

Категоризация на мрежите по мрежова операционна система 68
Windows мрежи 69
NetWare мрежи 69
UNIX мрежи 69
Хибридни мрежи 70

Категоризиране на мрежите по протокол 70
NetBEUI мрежи 71
IPX/SPX мрежи 71
TCP/IP мрежи 71
Други LAN протоколи, използвани в мрежи 72

Категоризиране на мрежите по топология 73
Мрежи с линейна шина 73
Кръгови мрежи 74
Мрежи от тип звезда 76
Решетъчни мрежи 77
Хибридни топологии 77

Категоризация на мрежите по архитектура 79
Ethernet мрежи 79
Мрежи Token Ring 84
Мрежи AppleTalk 85
Мрежи ARCnet 85

Обобщение 86
Допълнителни източници 87
Въпроси за преговор 87

ава 3 Мрежови концепции, модели и стандарти 91

Концепции на компютърните комуникации 91
Езикът на машината 92
Разпространени бройни системи 92
Използване на пакети 96
Многослоен процес на комуникация 98
Мрежови модели 100
Целта на моделите 100
Моделът OSI 100
Моделът DoD 112
Специфични за производителите модели 113
Мрежови стандарти и спецификации 114
Защо трябва да се спазват стандарти? 114
Организации за стандартизация 115
Обобщение 118
Допълнителни източници 118
Въпроси за преговор 119

ава 4 Методи за комуникация по мрежи 123

Методи на предаване на сигнали и характеристики 123
Аналогови и цифрови 123
Теснолентови и широколентови 126
Мултиплексиране 127
Асинхронно и синхронно предаване 129
Симплексно, полудуплексно и пълнодуплексно предаване 130
Проблеми на комуникациите и предаването на сигнали 132
Електромагнитни смущения 132
Радиочестотни смущения 133
Смесване на сигнали (Crosstalk) 133
Затихване 133
Проблеми, свързани с пропускателната способност (честотната лента) 134
Методи за достъп до преносната среда 135
CSMA/CD 136
CSMA/CA 136
Предаване на маркер 137
Приоритет по заявка 138
Обобщение 139
Допълнителни източници 140
Въпроси за преговор 140

Глава 5 LAN връзки 145

Ethernet 145
10Base2 146
10Base5 147
10BaseT 149
100BaseX 150
1000BaseT 150
Структура на Ethernet фрейма 151
Обобщение на характеристиките на Ethernet 154
Token Ring 155
Топологията на Token Ring 155
Процес на комуникация в Token Ring 155
Хардуерни компоненти на Token Ring 156
Предимства на Token Ring 157
Недостатъци на Token Ring 158
Структура на Token Ring фрейма 158
Правила на кръга 159
Обобщение на характеристиките на Token Ring 159
FDDI 159
Как работи FDDI? 159
FDDI спецификации 160
Предимства на FDDI 161
Недостатъци на FDDI 161
Структура на FDDI фрейма 161
Обобщение на характеристиките на FDDI 161
AppleTalk 161
Спецификации на AppleTalk 162
Как работи AppleTalk 162
Предимства на AppleTalk 162
Недостатъци на AppleTalk 162

Предаване на данни с LocalTalk 163
Обобщение на характеристиките на AppleTalk 163
ARCnet 163
Как работи ARCnet 163
Спецификации на ARCnet 164
Предимства на ARCnet 164
Недостатъци на ARCnet 164
Структура на пакетите на ARCnet 165
Обобщение на характеристиките на ARCnet 165
Сравнение на мрежовите архитектури 165
Обобщение 166
Допълнителни източници 166
Въпроси за преговор 167

лава 6 WAN връзки 171

WAN хардуер 172
Модеми 172
ISDN и DSL адаптери 177
Оборудването от страната на клиента 177
WAN топологии 178
WAN от точка до точка 178
WAN кръг 179
WAN от тип звезда 179
Многослойни WAN мрежи 180
Типове мрежово комутиране 181
Мрежи с комутиране на вериги 182
Мрежи с комутиране на пакети 187
Перспективни WAN технологии 189
OC-SONET 189
Широколентов ISDN 190
CATV 190
SMDS 191
Безжични WAN мрежи 192
Връзки между LAN и WAN 192
Транслирани връзки 193
Прокси сървъри 195
Обобщение 198
Допълнителни източници 198
Въпроси за преговор 198

Част II Мрежов хардуер и софтуер 203

Глава 7 Физически компоненти на мрежата 205

Мрежови интерфейсни карти 205
Ролята на мрежовите карти в мрежовите комуникации 205
Избиране на мрежова карта 206
Конфигуриране и използване на мрежова карта 207
Мрежова преносна среда 209
Типове кабели 210
Безжична преносна среда 216
Устройства за свързване на мрежата 219
Прости конектори 219
Сложни конектори 221
Устройства за разделяне на сегменти и подмрежи 222
Обобщение 229
Допълнителни източници 229
Въпроси за преговор 229

Глава 8 Мрежови протоколи и услуги 233

NetBIOS/NetBEUI 233
IPX/SPX 234
Протоколът от мрежовия слой: IPX 235
Протоколът от транспортния слой: SPX 236
TCP/IP 236
Комплектът TCP/IP 237
Протоколът от мрежовия слой: IP 237
Протоколите от транспортния слой: TCP и UDP 249
Адресиране на плика: хедъри на пакети 252
Преобразуване на имена 253
TCP/IP помощни програми 257
Протоколи от приложния слой 264
Обобщение 264
Допълнителни източници 265
Въпроси за преговор 265

Глава 9 Най-широкомащабната мрежа: глобалният Интернет 269

Еволюцията на Интернет 269
Разработката на опорния гръбнак 270
Проектът Интернет2 271

Компонентите на Интернет 271
Локален компютър или LAN 272
Доставчик на Интернет 272
Регионална мрежа 272
NAP точки 273
Градски централи 273
Как Интернет компонентите работят заедно 273

Какво прави Интернет 275
Мрежата 276
Електронна поща и пощенски списъци 284
Нюзгрупи 288
Трансфер на файлове 289
Telnet 291
Поточна медия 291
Чат на живо 292
Аудио/видео конференции 292
Интернет телефония 293
Виртуални частни мрежи 294

TCP/IP маршрутизиране и Интернет 294
Как работи IP маршрутизирането 294
Пример за проста маршрутизирана мрежа 295
Типове маршрутизиращи интерфейси 296
Статично срещу динамично маршрутизиране 296
Дистанционно-векторни протоколи срещу протоколи за състояние на връзките 298
Общоизползвани протоколи за маршрутизиране 299

Кой притежава Интернет? 301
ISOC 301
IAB 302
IETF 302
IESG 302
IANA/ICANN 302
W3C 302

Обобщение 302
Допълнителни източници 303
Въпроси за преговор 303

Глава 10 Мрежови операционни системи 307

Общи принципи на мрежовата администрация 307
Средата клиент/сървър 308
Споделяне на мрежови ресурси 311

Преглед на мрежовите операционни системи 319
Windows NT и Windows 2000 мрежи 320
NetWare мрежи 325
UNIX и Linux мрежи 328
Други мрежови операционни системи 333

Обобщение 334
Допълнителни източници 334
Въпроси за преговор 335

Глава 11 Директорийни услуги 339

Какво представляват директориите и директорийните услуги? 339
Какво е директория? 340
Какво представляват директорийните услуги? 341

Стандарти за директорийни услуги 343
X.500 344
DAP и LDAP 344
Мрежи с използване на директории 346

Популярни директорийни услуги 346
Novell NDS 346
Други директорийни услуги 351

Обобщение 353
Допълнителни източници 354
Въпроси за преговор 354

Глава 12 Настолни операционни системи 357

Основи на операционната система 357
Интерфейси на операционните системи 358
Използване на команди 360
Файлове и файлови системи 363

Общоизползвани настолни операционни системи 374

MS-DOS и Windows 3.*x* 374
Windows 9*x* 376
Windows NT Workstation 382
Windows 2000 Professional 386
Linux/UNIX 389
Macintosh 393
OS/2 395
Обобщение 395
Допълнителни източници 396
Въпроси за преговор 396

Глава 13 Хибридни мрежи 401

Характеристики на хибридната мрежа 401
Невъзможността един производител да осигури всички желани възможности 402
Персонални предпочитания на потребителите 402
Бюджетни фактори 402
Случайно разрастване 403
Мрежи с множество протоколи 403
Мрежови/транспортни протоколи 403
Протоколи за споделяне на файлове 406
Мрежи с множество операционни системи 407
Множество сървърни операционни системи 407
Множество клиентски операционни системи 409
Множество сървърни и множество клиентски операционни системи 409
Многоплатформени мрежи 409
PC-към-Macintosh комуникации 409
PC-към-мейнфрейм комуникации 410
PDA-към-PC и хендхелд-към-PC комуникации 410
Шлюзове: решението за хибридно свързване 411
Windows-към-NetWare редиректори 411
Междуплатформени решения 412
SNA 412
Samba 414
Обобщение 415
Допълнителни източници 416
Въпроси за преговор 416

Част III Особености в областта на мрежите 421

Глава 14 Защита на мрежата 423

Мрежова сигурност 423
Определяне на нуждите за сигурност 424
Определяне на заплахите за сигурността 425
Реализиране на мерки за сигурност 433
Как работят компонентите на сигурността 439
Перспективни технологии за идентификация и автентикация 445
Разработка на политики на сигурност 448
Защита и възстановяване от сривове 454
Аварийно захранване 455
Архивиране на данните 456
Отказоустойчивост при дисковете 459
Технологии за клъстериране 460
Обобщение 461
Допълнителни източници 462
Въпроси за преговор 462

Глава 15 Отдалечен достъп 467

Защо да използваме отдалечен достъп? 468
Офиси на филиали 468
Възможност за връзка след работно време 468
Телекомютинг 469
Мобилни потребители 470
Осигуряване на достъп за клиенти и партньори 470
Как работи отдалеченият достъп 471
Протоколи, използвани за отдалечен достъп 471
Автентикация при отдалечен достъп 472
Назначаване на IP адреси 473
Обединяване на пропускателната способност по Dialup връзки 473
Контрол на използването на пропускателната способност 474
Устройства за свързване при отдалечен достъп 474
Модеми 474
ISDN терминални адаптери 481
Кабелни модеми 482
CSU/DSU 483
Конфигуриране на клиенти и услуги за отдалечен достъп 483

Конфигуриране на сървър за отдалечен достъп 485
Проблеми на сигурността при отдалечен достъп 485
RADIUS 486
Политики на отдалечен достъп 487
Заключване на акаунт 487
Хостове за сигурност 488
Обобщение 488
Допълнителни източници 489
Въпроси за преговор 489

Глава 16 Виртуални частни мрежи 493

Какво представлява VPN? 493
Виртуална мрежа 493
Частна мрежа 494
Как работи VPN 494
Прокопаване на тунела 495
Поддръжка на VPN мрежи от операционната система 497
Защо да използваме виртуална частна мрежа? 498
Сравнение между VPN и Dialup мрежи: предимства и недостатъци 498
Сценарии на изграждане на VPN мрежи 500
VPN протоколи 504
Тунелни протоколи 504
Протоколи за криптиране 507
Сигурност на VPN 507
Автентикация 508
Авторизация 508
Криптиране 508
Проблеми на производителността на VPN 508
Типове VPN мрежи 509
Софтуерно-базирани VPN 509
Хардуерно-базирани VPN 509
Конфигуриране на VPN връзка 509
Обобщение 512
Допълнителни източници 512
Въпроси за преговор 513

Глава 17 Мрежи за тънки клиенти 517

Еволюция на мрежите за тънки клиенти 518
Технологията тънък клиент 519
Предимства на технологията тънък клиент 520
Протоколи за тънки клиенти 521
RDP 521
ICA 522
X и X Display Manager Communication Protocol (XDMCP) 522
RFB 522
BOOTP, DHCP и TFTP 523
Хардуер на тънките клиенти 524
WBT-та 524
Мрежови компютри 525
Net PC-та 525
Настолни компютри 526
Най-тънките клиенти: Хендхелд PC-тата 526
Софтуер за тънки клиенти 526
Терминални услуги на Microsoft 527
Winframe/MetaFrame на Citrix 528
Системата X Window 529
Web-базирана компютърна обработка 529
Виртуалната машина JVM 530
ASP-та 530
Microsoft .NET 531
Обобщение 531
Допълнителни източници 532
Въпроси за преговор 532

Глава 18 Инструменти за наблюдение, управление и отстраняване на неизправности 537

Анализиране и оптимизиране на производителността на мрежата 53
Тесни места 538
Базови линии 539
Най-добри практики 540
Определяне скоростта на Интернет връзка 540
Инструменти за мониторинг и мениджмънт на мрежата 542
Софтуер за мониторинг на мрежи 542
Софтуер за мениджмънт на мрежи 547

Софтуер за мениджмънт на малки и средни мрежи 551
Доставчици на услуги за мениджмънт 552
Устройства за мониторинг на хардуера и отстраняване на проблеми 552
Отстраняване на проблеми в мрежите 553
Основи на отстраняването на проблеми 554
Използване на файловете-дневници на операционната система 556
Използване на помощни програми за TCP/IP 557
Указания за решаване на проблеми 563
Обобщение 564
Допълнителни източници 565
Въпроси за преговор 565

Част IV Бъдещето на мрежите 569

Глава 19 Технологиите на бъдещето 569
Компютри навсякъде 571
Мрежите в дома 572
Преодоляване на ограниченията на IP 572
Нови насоки в мрежовите технологии 574
Универсална свързаност 576
„Смарт“ уреди 576
Мрежа в семейството 577
Това е забавление 577
Въпроси за поверителността: Големият брат гледа 578
Мрежа в дома 578
Влиянието на мрежовите технологии върху правителството 579
Влиянието на мрежовите технологии върху закона 581
Влиянието на мрежовите технологии върху медицината 582
Влиянието на мрежовите технологии върху издателската дейност 583
Нови начини за обучение 584
Изкуствен интелект 584
Компютрите могат да мислят 584
Кибернетични форми на живот: абсолютната мрежа 585
Обобщение 585
Допълнителни източници 586
Въпроси 586

Приложение А Отговори на преговорните въпроси от главите 589

Речник 615

Въведение

Книгата *„Компютърни мрежи“* ви помага да разберете концепциите на компютърни
ната реализация. Тя също така ви въвежда в клиентските и сървърните операционни с
то работят мрежовите компютри.

Темите, разгледани в тази книга, включват история на мрежите, мрежова терминологи
мрежите и установените стандарти, както и реализация на локални и глобални мрежи.
мание е отделено на мрежовите протоколи и начина им на работа във всички слоеве на
дел. Също така се набляга и на съвместната работа между мрежи, работещи с различни
различни платформи и под различни операционни системи.

Разгледани са специални области, като сигурност, отдалечен достъп, виртуални частни
клиенти, мониторинг, мениджмънт и отстраняване на проблеми. Засегнати са техноло
разработват в момента и се очаква да се реализират в близкото бъдеще.

За кого е предназначена книгата

Тази книга е предназначена за професионалисти, които искат да започнат кариера в об
жовите технологии, както и за желаещите да овладеят основните концепции.

Това изчерпателно ръководство е особено подходящо за корпоративните центрове за о
нически кадри, както и за членове на бизнеса, които работят с персонал в сферата на и
технологии и се нуждаят от обширно въведение в концепциите, свързани с мрежите.

Като третостепенна аудитория се явява масовият потребител, който иска да знае повеч
компютрите си комуникират по мрежата. Подходът на книгата е съобразен с „дружелю
ребителя тон, а стилът е достъпен и за технически неграмотния читател, който не иска
гона, използван в техническата документация и ръководствата.

Как е организирана книгата

Тази книга е организирана в четири части и включва 19 глави, приложение и речник на
Следващите секции описват съдържанието на всяка част от книгата.

Част I: Въведение в мрежите

Глава 1, „Въведение в мрежите“, ви въвежда в основните концепции на PC мрежите, ка
кратка история на електронните комуникации и мрежи, както и обобщение на това, къ
мрежите днес.

Глава 2, „Категоризиране на мрежите“, дискутира категоризирането на мрежите според
обхват, административния модел, мрежовата операционна система, използваните прото
гията и архитектурата.

Глава 3, „Мрежови концепции, модели и стандарти“, разглежда двоичните комуникации
популярни мрежови модела: моделът DoD (Department of Defense), на който се базират TCP
и моделът OSI (Open Systems Interconnection), разработен от ISO (International Organization for
Дискутирани са и спецификациите, установени от IEEE (Institute of Electrical and Electronics
то и моделите на различните производители.

Глава 4, „Методи за комуникация по мрежи“, дискутира методите за предаване на сигнали
говите, цифровите, широколентовите, теснолентовите, асинхронните, синхронните, симплекс
те и мултиплексираните сигнали. Описани са методите за достъп до преносната среда, включ
CSMA/CD, CSMA/CA, предаване на маркер и приоритет по заявка.

Глава 5, „LAN връзки“, дискутира популярните LAN типове, включващи Ethernet, Toke
AppleTalk и ARCnet.

Глава 6, „WAN връзки“, осигурява преглед на WAN връзките, като PSTN, ISDN, T-носещи, Fra
кабелните телевизионни мрежи (CATV), както и на високоскоростните решения, като ATM,
Тази глава дискутира и LAN-към-WAN решенията, включващи ICS (Internet Connection Sh
(Network Address Translation), прокси сървъри и маршрутизирани връзки.

Част

Въведение в мрежите

Глава 1 Въведение в мрежите

Глава 2 Категоризиране на мрежите

Глава 3 Мрежови концепции, модели и стандарти

Глава 4 Методи за комуникация по мрежи

Глава 5 LAN връзки

Глава 6 WAN връзки

Глава 1

Въведение в мрежите

Добре дошли в света на мрежите от персонални компютри (PC-та). В този свят вече не е достатъчно просто да имате и да използвате персонален компютър; повелята на днешния ден е също да „сте свързани“. Реалната мощност и използваемост на компютрите се проявява само когато са свързани така, че да могат да комуникират един с друг. От простата домашна мрежа от два компютъра или малката локална компютърна мрежа (LAN) до постоянно нарастващата глобална мрежа Интернет, работата в мрежа *е бъдещето* на компютърната обработка и това бъдеще е тук днес и сега.

В много области на Съединените щати, търсенето на подготвени професионалисти по мрежи далече надхвърля предлагането. Според Министерството на труда на САЩ компютърните мрежи са професия със светло бъдеще. Търговските предприятия и отделни лица купуват компютри и тези компютри биват свързвани в локални компютърни мрежи (LAN) и глобални мрежи (WAN) с удивителни темпове. Ние буквално „свързваме света в мрежа“.

Тъй като мрежовите комуникации бързо стават част от нашия живот, дори тези хора, които не участват пряко в индустрията за информационни технологии (IT), трябва да знаят нещо за основите на мрежите. По същия начин, по който трудно бихте могли да функционирате в съвременния свят, ако не знаете нищо за телефона и неговите възможности, в едно не чак толкова далечно бъдеще познаването на начините за „свързване към мрежа“ ще бъде задължително за много хора, както в работата, така и вкъщи.

Кратка история на компютърните мрежи

Желанието за комуникация с други хора е движеща сила за всички човешки същества, а разработените от нас интелигентни средства за комуникация ни отличават от другите биологични видове. От момента, когато стана възможно свързването на два компютъра и провеждането на разговор между тях, концепцията за развитието на Интернет стана неизбежна.

В ранните дни на използването на компютри, те представляваха огромни машини, които изпълваха цели стаи — понякога цели градски квартали — и струваха стотици хиляди долари. Макар че тези скъпи хипопотами имаха много помалка мощност на обработка и памет от днешните тънки ръчни компютри, те бяха последен вик на технологията през 50-те и 60-те години. В свят, в който хората бяха бавни и предразположени към грешки, извършвайки ръчно всички изчисления, възможностите на компютъра бяха поразителни.

В средата на двадесети век компютрите все още бяха редки, екзотични и мистериозни машини, собственост само на големи компании, държавни и образователни институции. В по-голямата си част компютрите бяха самостоятелни (автономни) системи, изолирани една от друга.

През 40-те години Томас Уотсън – председател на IBM, казва, че тогавашният световен пазар е за около пет компютъра. Дори още по-скоро, през 1977 г., Кен Олсън – президент на Digital Equipment Corporation, каза: „Няма причина, поради която някой би поискал компютър вкъщи“ (ISBC [International Small Business Consortium], www.isbc.com/isbc/business/wisdom.cfm). Разбира се, и двамата са допуснали грешка, дори много голяма грешка. Но дори преди десет години никой не би могъл да предположи, че персоналните компютри могат да се размножат толкова, или че компютърните мрежи ще станат главна насока на развитие.

Първите комуникационни мрежи

Към средата на 20 век електронните комуникации съществуват вече повече от едно столетие и са реализирани както в Европа, така и в Съединените щати. Тези ранни мрежи приемат множество форми и по тях се изпращат само кодирани сигнали. По-късно те получават възможността за предаване на глас по кабела.

Тази секция дава свободен исторически преглед на начина на създаване на първите мрежи.

Телеграфни кабели

В началото на 19 век французите разработват първата оптическа телеграфна мрежа, която изпраща информация с поразителната скорост от 20 знака за секунда, а Самюъл Морз демонстрира електрическия телеграф, който слага началото на разработката на мрежовите комуникации в Съединените щати.

Телефонната мрежа: Технология с комутиране на електрически вериги

В края на 19 век започва изграждането на огромна телефонна мрежа. Но тогавашните технологични лидери не са били по-предвидливи от техните наследници от ранната компютърна ера. Едно вътрешно разпореждане в Western Union от 1876 г. твърди, че: „Този „телефон“ има прекалено много недостатъци, за да може да бъде възприет като средство за комуникация. Устройството няма никаква стойност за нас“. (www.isbc.com/isbc/business/wisdom.cfm).

Независимо от това становище, към 1880 г. в Съединените щати има повече от 50 000 телефонни линии, а към 1960 г. телефонните линии обхващат градските области и телефонната мрежа се превръща в световна комуникационна мрежа.

Телефонната система използва технология с комутиране на електрически вериги, при която се изгражда верига или виртуална пътека при всяко свързване на един телефон с друг по мрежата. Тази технология е подходяща за предаване на глас, защото звуците се пренасят по кабела с относително постоянна скорост.

При мрежата с комутиране на вериги една връзка се изгражда по начина, показан на фигура 1-1. Всички сигнали се предават по тази верига през цялата продължителност на сесията. Ако прекъснете връзката и я установите отново, може да бъде използвана друга верига, както е показано с пунктираната линия.

Фигура 1-1 *В мрежата с комутиране на вериги се изгражда връзка, както е показано с плътната линия.*

Технологията не е подходяща за трансфер на компютърни данни, които притежават тенденцията да бъдат изпращани на отделни пакети; т.е. периодите на висока активност са разредени с интервали на ниска активност или липса на активност.

Технология на комутиране на пакети

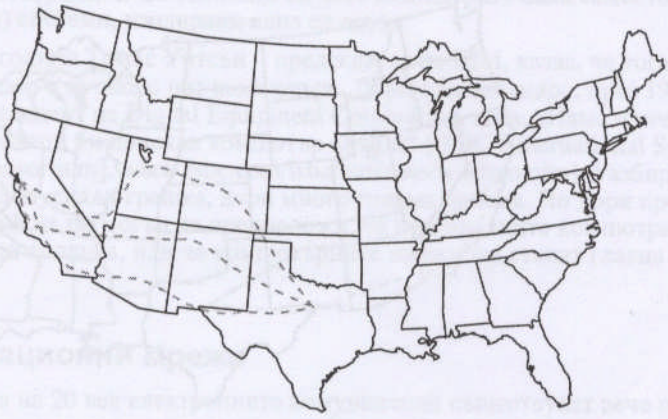
През 60-те години правителството на Съединените щати се заинтересува от разработването на компютърна мрежа, която би позволила на военните системи и на системите на главните образователни институции да комуникират едни с други. Тъй като това става в разгара на Студената война, те искат мрежата да притежава устойчивост, надеждност и достатъчен резерв, така че да може да оцелее при възможна ядрена война.

Изследователи от Масачузетския технологичен институт (MIT), института RAND и Националната физична лаборатория (NPL) във Великобритания изобретяват нова технология, наречена *комутиране на пакети* (packet switching), която при периодични пикови предавания работи по-добре, отколкото традиционните технологии с комутиране на вериги. Тяхната работа полага основата на комуникационните технологии, използвани в днешния Интернет.

В мрежата с комутиране на пакети, показана на фигура 1-2, не се изгражда една постоянна връзка (конекция) за цялото време на предаването. Вместо това всеки отделен пакет от данни може да пътува по различен път.

Комуникациите от различни източници могат да споделят една и съща линия, вместо линията да бъде заделяна специално само за една комуникация от едно крайно устройство до друго крайно устройство за цялото времетраене на сесията, какъвто е случаят с комутирането на вериги.

Фигура 1-2 *Свързаните в мрежа компютри използват общи данни, софтуер и хардуерни ресурси.*



Сравнение между комутирането на вериги и комутирането на пакети

Термините *комутиране на вериги* (circuit switching) и *комутиране на пакети* (packet switching) звучат близко, но имат различни значения.

Обществената телефонна система, означавана понякога като POTS (plain old telephone service – обикновена стара телефонна услуга), представлява комуникационна мрежа с комутиране на вериги. Когато провеждате телефонен разговор в този тип мрежа, за цялото времетраене на този разговор се използва само една физическа пътека от вашия телефон до телефона, който сте избрали. Тази пътека, или верига, се поддържа изключително за ваше ползване до момента, когато прекъснете връзката, поставяйки телефонната слушалка обратно на мястото ѝ.

Обърнете внимание, че ако се обадите на същия номер на следващия ден и направите това от същото място, от което сте провели днешния разговор, пътят няма да е непременно същият. Ето защо веригата се обозначава като комутирана (превключвана). Това обяснява също защо първия ден може да имате ясна връзка, а на другия – пълна с шумове.

При мрежата с комутиране на пакети не се изгражда специална пътека или верига. Комутирането на пакети понякога се означава като технология без установяване на конекции, поради липсата на специално изградена пътека. Ако прехвърляте данни, например текстов файл, от вашия компютър на друг с използване на мрежа с комутиране на пакети, всеки отделен пакет (т.е. всяко малко парче данни) може да поеме по различен маршрут. Макар че всички те пристигат на едно и също местоназначение, не всички пътуват по един и същ път, за да стигнат там. Технологията с комутиране на пакети по правило се използва за осъществяване на трафика по Интернет.

Разликата между комутирането на вериги и пакети може да бъде сравнена с различните начини, по които една голяма група от хора, пътуващи от Далас за Сан Франциско, могат да достигнат до крайната цел на тяхното пътуване. Например комутирането на вериги е подобно на това цялата група да се качи на един автобус, влак или самолет. Маршрутът е начертан и цялата група пътува по същия този маршрут.

Комутирането на пакети е подобно на това да накарате всяко лице да пътува в отделна кола. Групата се разделя на отделни компоненти, както комуникацията на данните се разделя на пакети. Някои пътници могат да поемат по междущатските магистрали, а други да използват черните пътища. Едни могат да карат направо, а други да изберат по-обиколни пътища. В крайна сметка всички те завършват пътуването си в едно и също местоназначение. Групата се събира отново точно както пакетите се подреждат в едно цяло в крайната точка на комуникацията.

ARPAnet

Началото на първата компютърна мрежа с комутиране на пакети е поставено в края на 60-те години под покровителството на Министерството на отбраната на САЩ. Тя е наречена ARPAnet (Advanced Research Projects Agency network). Първият *възел*, или точка на свързване, към ARPAnet е инсталиран в Калифорнийския университет в Лос Анджелис през 1969 г. Само за три години мрежата се разпростира през целите Съединени щати, а две години след това достига до Европа.

С нарастването на мрежата тя бива разделена на две части. Военните наричат своята част от интермрежата *Milnet*, а ARPAnet продължава да бъде използвана за описание на частта от мрежата, която свързва изследователските и университетските сайтове. През 80-те години ARPAnet е заменена от мрежите Defense Data Network (отделна военна мрежа) и NSFNet (мрежа от научни и академични сайтове, основана от Националната научна фондация). Впоследствие тази WAN мрежа се разраства в това, което днес наричаме Интернет.

Мрежите на вчерашния ден

Изграждането на компютърни мрежи не започва от такъв голям мащаб като проекта ARPAnet; т.е. локалните мрежи се появяват преди WAN. С поевтиняването на компютрите и с увеличаването на тяхната мощност, търговските организации от всички мащаби започнаха да ги използват все по-масово. Първите машини можеха да се използват само за ограничени видове обработка на данни, но с процъфтяването на разработката на софтуер новите програми позволиха на потребителите да правят много повече от простото събиране и сортиране на данни.

Например при ранните мейнфрейм системи множество потребители можеха да осъществяват достъп до едни и същи съхранени данни с помощта на *терминали*, представляващи станции с входни и изходни устройства (например клавиатури и монитори). Тези станции нямат собствена изчислителна мощност; те са просто точки, от които може да бъде осъществен достъп до мейнфрейм компютъра.

Използването на мейнфрейм компютри вършеше добра работа в много отношения, но те имаха няколко минуса в сравнение с по-малките компютри (наричани тогава микрокомпютри). Недостатък беше тяхната висока цена; големите мейнфрейм системи струваха много повече от така наречените „персонални“ компютри, проектирани така, че да бъдат поставени на бюрото и да функционират самостоятелно.

Друг недостатък на мейнфрейм компютрите беше концепцията за *единствена точка на отказ* (single point of failure). При работа с мейнфрейм компютър, ако компютърът бъде изключен, той е изключен за всички. Никой не може да осъществява достъп до данни и никой, който зависи от компютъра, не може да

свърши никаква работа. От друга страна, използването на отделни персонални компютри разрешава този проблем.

Персоналните компютри представляваха компютри, разработени като напълно функционални единици, които изпълняваха програми и извършваха работни задания напълно самостоятелно, без чужда помощ. Те осигуряваха известна *отказоустойчивост* – способността на системата да продължава да функционира и да осигурява цялост на данните при възникване на повреди. Ако компютърът на един от служителите прекъсне работа, той не влияе на възможността на останалите служители, които имат техни собствени персонални компютри, да продължат да работят. Реално, ако даден служител запише данните на дискета, той или тя могат да се преместят на функционираща машина и да продължат да работят.

Тези фактори допринесоха за нарастване на популярността на персоналните компютри като решение за малки, средни и големи търговски организации. Но след като всеки се сдоби с отделен компютър на бюрото си, компаниите се изправиха пред дилемата: как работниците да използват съвместно информация, както правеха това при стария модел на обработка с мейнфрейм компютри. Решението беше изграждането и работата в мрежи.

Недостатъци на самостоятелните системи

В ранните дни на настолните персонални компютри хардуерът и софтуерът за работа в мрежа не бяха лесно достъпни и много търговски компании използваха машините като самостоятелни системи. Ако се наложеше всички потребители да отпечатат документи при някакъв повод, съществуваха три начина за осигуряване на такава възможност:

- Към всяка машина можеше да бъде свързан принтер. Това беше скъпо решение, защото налагаше закупуването на множество принтери, макар че беше малко вероятно всички те да бъдат използвани едновременно.
- Файлът, който трябваше да бъде разпечатан, можеше да бъде записан на дискета и след това да бъде прехвърлен на машината, към която има свързан принтер. Това беше по-евтина опция, но беше неудобно както за лицето, което трябваше да моли за принтер, така и за лицето с принтера, работата на което биваше прекъсвана, докато някой друг използва неговата машина за печат.
- Принтерът можеше да бъде местен от една работна станция на друга в зависимост от това, кой се нуждае от печат. Това беше доста тежко решение; въпреки това то се прилагаше масово, като за целта се използваха колички за принтерите, които се търкаляха из офиса. Всяко преместване изискваше кабелите да бъдат изключвани и включвани отново; понякога преместването изискваше също и известно преконфигуриране на софтуера.

Високата цена, неудобството и допълнителната работа са главните недостатъци на самостоятелните или немрежовите решения.

Какво все пак означава мрежа?

Речникът *American Heritage Dictionary* дефинира *мрежата* като „система от линии или канали, които се пресичат или свързват едни с други". По-рано споменахме телеграфните и телефонните мрежи и, разбира се, всички сме чували

за телевизионните мрежи. Използвайки дефиницията от речника, можем да наречем мрежа дори пътищата или железопътните линии, които пресичат страната.

Като имаме всичко това предвид, какво в крайна сметка представлява една компютърна мрежа? Просто казано, това са две или повече устройства, свързани с цел общо използване на информация, ресурси или и двете. Връзката може да бъде чрез кабел (коаксиален, усукана двойка или оптично влакно, както ще научите по-късно в тази глава), или може да бъде безжична връзка, която използва радиовълни, лазерна или инфрачервена технология, или сателитно предаване. Споделената обща информация и ресурси могат да бъдат файлове с данни, приложни програми, принтери, модеми или други хардуерни устройства. За илюстрация вижте фигура 1-3.

Фигура 1-3 *Тази диаграма показва значимите събития в историята на мрежите от персонални компютри.*

Защо мрежови компютри?

При положение, че предимството на персоналните компютри се състои в това, че всеки потребител има независим компютър, защо да събираме и да ги свързваме отново в едно. Правим това, защото мрежовите персонални компютри ни дават, и то по много начини, най-доброто от двата свята. Всеки потребител има независима изчислителна мощност, но пак може да се радва на предимствата от общото използване (споделянето). От друга страна организацията може да реализира значителни спестявания, когато скъпи и рядко използвани периферни устройства бъдат споделени по мрежата. Например един скъп цветен лазерен принтер може да бъде използван само за специални проекти, но от време на време и други членове на организацията ще искат да печатат на него. При наличието на мрежов достъп до принтера те лесно могат да правят това.

Предимства на свързването към мрежа

Както бе описано в предишния пример, много собственици и мениджъри твърдят, че главната причина за свързването на техните персонални компютри в мрежа е била необходимостта от общо използване (споделяне) на принтери. Разбира се, след свързването на системите хората откриват ползата от споделянето на много други ресурси, освен принтерите.

Цената на свързването на компютрите в LAN – мрежовите интерфейсни карти (NIC) за компютрите, кабелната или безкабелната преносна среда, хъбовете (концентраторите) и други свързващи устройства – често се изплаща многократно с намаляване на разходите и на изгубеното производствено време.

Споделяне на изходни устройства

Както казахме, принтерите и другите изходни устройства могат да бъдат споделяни в мрежата, спестявайки време, пари и много главоболия. В елементите, които могат да бъдат споделяни, се включват плотерите – устройства за чертане на диаграми и графики. Те включват също линейни графични устройства, които използват писалки или електростатични заряди и тонер. Факс машините, които могат да бъдат входни или изходни устройства, също лесно могат да бъдат споделяни.

Споделяне на входни устройства

По мрежата можете да споделяте скенери, цифрови фотокамери и други входни устройства. Тъй като тези устройства, дори повече от принтерите, се използват най-общо в случаен ред и често са сравнително скъпи, има смисъл да ги конфигурирате за множество потребители в мрежата.

Споделяне на запаметяващи устройства

Свързаните в мрежа компютри могат да споделят използването на твърди дискове, флопидискови устройства и CD-ROM устройства. При този тип споделяне можете да записвате файлове на диска на друг компютър по мрежата, ако имате недостиг на пространство на твърдия диск на вашия компютър. Освен това, ако вашият компютър няма инсталирано CD-ROM устройство, можете да осъществите достъп до споделено CD-ROM устройство на друг компютър. Тази възможност за споделяне важи и за Zip и Jaz устройства, магнито-оптични устройства, лентови устройства и почти всеки друг тип запаметяващи устройства, които могат да бъдат включвани към PC.

Споделяне на модеми и Интернет връзки

Друго важно предимство при работа в мрежа е възможността на мрежовите PC-та да споделят модеми, ISDN линии, кабелни модеми и DSL адаптери. С помощта на подходящ софтуер – например прокси или NAT (Network Address Transition) софтуер, който ще разгледаме детайлно в Глава 9 – „Най-широкомащабната мрежа: глобалният Интернет“ – цялата локална мрежа може да се свързва към Интернет с помощта на една телефонна линия и един ISP акаунт.

Споделяне на данни и приложения

Хардуерните устройства не са единствените и дори не са най-важните ресурси, които могат да бъдат споделяни в една мрежа. Файловете с данни и приложни-

те програми също могат да бъдат направени достъпни за множество потребители. Резултатът от такъв тип споделяне е ефикасното използване на дисковото пространство и по-лесно сътрудничество при работа по многопотребителски проекти. Например, ако няколко мениджъра искат да имат достъп и да ревизират една електронна таблица, съдържаща бюджета на техния отдел, този файл може да бъде съхранен в едно централно (достъпно за всички) местоположение. След като всеки мениджър направи желаните промени, файлът може да бъде записан отново на това местоположение в мрежата, така че обновената версия да бъде достъпна за следващия мениджър.

Приложните програми (приложенията), например текстообработващи програми, могат да бъдат инсталирани на мрежов сървър. Потребителите могат да се свързват към сървъра и да изпълняват споделената програма на собствени си машини, без файловете на програмата да заемат място на техните твърди дискове.

Имайте предвид, че в лицензните договори разпространителите на софтуер могат да изискат от вас да закупите допълнителни лицензи за всяка работна станция, която използва дадено мрежово приложение, макар че реално е инсталирано само едно копие на програмата и всички потребители осъществяват достъп до това копие.

Раждането на Интернет

Както беше споменато по-рано, в края на 60-те години станаха достъпни полезни технологии за работа в мрежа, а в началото на 70-те години беше създадена мрежата ARPAnet – резултат от сътрудничеството между американското правителство (главно Министерството на отбраната) и няколко големи университета.

Ролята на Министерството на отбраната на САЩ

С разрастването на студената война между САЩ и СССР през 60-те години, Министерството на отбраната на САЩ установи нуждата от изграждането на комуникационни връзки между основните военни съоръжения. Главната мотивация беше продължаване на поддържането на комуникациите, при условие че ядрената война доведе до масово унищожение и прекъсване на традиционните комуникационни канали. По това време големите университети, като Калифорнийския университет и Масачузетския технологичен институт, също биват включени в процеса на изграждането на общата мрежа.

Министерството на отбраната на САЩ спонсорира изследователските центрове в САЩ и през 1968 г. ARPA сключва договор с частната компания BNN за изграждане на мрежа, базирана на технологията на комутиране на пакети, разработена с цел по-доброто предаване на компютри данни.

70-те години: Започват усилията за разрастване

Когато започва проекта ARPAnet, още никой не може да предвиди, че мрежата ще надрасне многократно първоначалния си обхват. През 70-те години биват добавени още възли, както в САЩ, така и в чужбина.

80-те години: Повече означава по-добре

През 1983 г. мрежата ARPAnet се разделя и 68 от съществуващите 113 възела биват поети от Milnet, която се интегрира с мрежата Defense Data Network. Defense Data Network е създадена предишната година.

Системата Domain Name System (DNS) беше представена през 1984 г., осигурявайки начин за асоцииране на „приятелски" имена на хостове и IP адреси, което е много по-ефикасно и удобно от предишните методи. Тези методи ще разгледаме в Глава 8 – „Мрежови протоколи и услуги". През 1984 г. в мрежата вече имаше повече от 1000 хост компютъра.

През втората половина на 80-те години мрежата нарасна значително. Например NSF създаде суперкомпютърни центрове в Принстън, Калифорнийския университет в Сан Диего, в Университета на Илиноис, в Урабана-Шампейн и в Корнел. По това време се появи и комитетът Internet Engineering Task Force (IETF). Към 1987 г. в мрежата вече имаше 10 000 хоста, а към 1989 този брой нарасна до над 100 000.

90-те години: Мрежата става голям бизнес

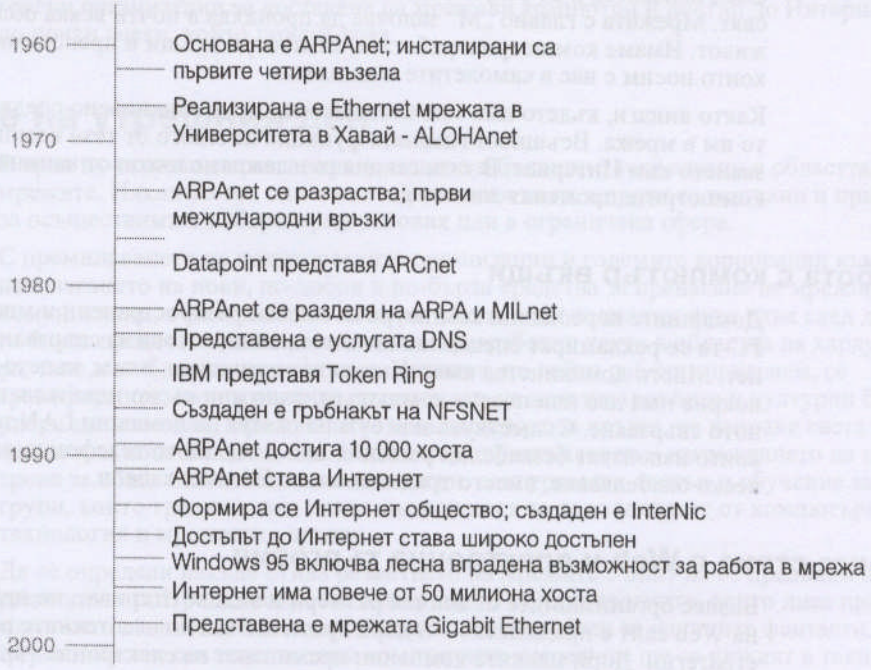
Феноменалната скорост на нарастване през 80-те години е нищо в сравнение с това, което стана през 90-те. ARPAnet прекрати своето съществуване и беше „измислена" мрежата Интернет, като американското правителство се включи в разработката на така наречената информационна супермагистрала. Гръбнакът на NSFnet беше обновен до скорост T3 (т.е. 44736 Mbps) и през 1991 г. предаваше повече от 1 трилион байта на месец. Формира се Интернет общността (Internet Society - ISOC), а през 1992 г. в Интернет вече съществуваха повече от 1 милион хоста.

90-те години бяха десетилетието, когато Интернет беше комерсиализиран. Със свързването към Интернет на все повече и повече студенти и университети, отделни домашни потребители и компании от всякакъв размер, светът на бизнеса откри възможността за достигане до голям и разрастващ се изобилен пазар. Към 1995 г. възникна рекламата в мрежата, онлайн банкирането и стана възможно дори поръчването на пица по Интернет.

През последната половина от последното десетилетие на века едва ли не всеки ден бяха въвеждани нови големи разработки. Поточното аудио и видео, „push" технологиите, Java и ActiveX скриптовете използваха предимството на високопроизводителната връзка, достъпна на все по-ниска цена. Имената на домейни станаха голям бизнес, като особено желаните имена се продаваха на цена до 1 милион долара. През декември 1999 г. в World Wide Web съществуваха почти 1 милиард сайта с повече от 50 милиона хост компютъра, участващи в това голямо свързване.

Фигура 1–4 показва времедиаграмата на значителните събития в историята на компютърните мрежи.

Фигура 1–4 *Глобалната мрежа води началото си от 60-те години и продължава да се разраства.*



Цената на технологията: Все повече и повече за все по-малко и по-малко

С напредъка на компютърната и мрежова технология в последните няколко десетилетия, цената на тази все по-интелигентна технология спадаше драматично. Тези непрекъснато намаляващи цени доведоха до нарастващата популярност на мрежовите решения в света на бизнеса и в личния живот на хората.

През 70-те и 80-те години персоналните компютри бяха считани за произведение на изкуството поради цените си от няколко хиляди долара. Съществуваха онлайн услуги, но при цени от 25 долара и повече *на час* за достъп, само големите бизнес организации и богатите такива можеха да се възползват от тях. PC ветераните още помнят предлаганите от Prodigy „приемливи цени" само от 9,95$ на час за онлайн достъп. Това ставаше при „поразителните" скорости от 1200 или 2400 бода.

Днес, разбира се, за по-малко от 1000$ можете да купите компютърна система, която може да прави много повече и да прави това много по-добре и по-бързо от един мейнфрейм компютър за 500 000 долара от преди 20 години. Достъпът до Интернет със скорости, еквивалентни на T1, е достъпен по DSL или кабелен модем за 30–40$ на месец, като цените падат непрекъснато. Основният достъп до Интернет на 56 kbps може да бъде получен и за много по-малко и дори безплатно, ако запазите малко толерантност и отделите на екрана си малко място за реклами.

Днешните компютърни мрежи

След влизането в 21 век, навлязохме в ерата на свързването в мрежа на целия свят. Мрежата с главно „М“ започва да прониква в почти всяка област от нашия живот. Имаме компютри в работата, компютри вкъщи и преносими компютри, които носим с нас в самолетите и на плажа.

Както винаги, където има множество компютри, обикновено следва свързването им в мрежа. Всъщност главната функция на много от тези компютри е свързването към Интернет. В тази секция разглеждаме някои от начините, по които компютрите променят живота ни.

Работа с компютър вкъщи

Домашните персонални компютри са масово разпространени и много от тези PC-та се рекламират специално като е-машини, готови за свързване към Интернет. Много домакинства имат множество компютри, а там, където под един покрив има два или повече компютъра, рано или късно идва желанието за тяхното свързване. Съществува нов бум на пазара на домашни LAN технологии, които използват безкабелни решения или домашното телефонно или електрическо окабеляване, вместо традиционните Ethernet кабели.

Присъствие в Web и електронна търговия

Бизнес организациите от всички размери и видове откриват, че притежаването на Web сайт е предимство – и дори критично важно – за техните рекламни стратегии. Дори малките компании преминават на електронна търговия (e-commerce) (т.е. започват да продават своите продукти или услуги директно по Интернет) като ценово ефективно решение. Големите корпорации пускат корпоративни мрежи (enterprise networks) (т.е. големи мрежи с множество сайтове), които свързват офисите по света към техните собствени вътрешни интранет мрежи, както и към Интернет.

Високопроизводителни бизнес решения

С масовото навлизане на високоскоростните връзки по оптични влакна и други бързи преносни среди, видеоконференциите на живо станаха реален заместител на работните съвещания, провеждани с личното присъствие на участващите. Ръководителите остават в близко взаимодействие със своите офиси дори когато пътуват, благодарение на възможността за отдалечен dial-up достъп и работа във виртуална частна мрежа. Служителите на всички нива на организацията могат да работят от разстояние (телекомютинг), което позволява по-голяма гъвкавост в техните работни разписания, а компанията се радва на икономии на помещения и офис оборудване. В допълнение сега може бързо и лесно да бъде осъществен трансфер на големи файлове с данни. Дори традиционните дейности, за които е необходима връзка с ниска скорост, като съставянето на разписания и достъпа до електронна поща, се подобряват с помощта на новите и достъпни високопроизводителни технологии.

Онлайн обучение

Обществените училища биват свързвани към мрежата и онлайн обучението става реалност, когато големите колежи и университети предлагат кредитни

курсове, които могат да бъдат завършени частично или изцяло по Интернет. В допълнение разпространителите на хардуер и софтуер, водени от големи играчи като Microsoft Corporation и Cisco Systems, партнират на търговски и нетърговски организации за доставяне на мрежови компютри и достъп до Интернет до почти всеки, който поиска това.

Мрежите на утрешния ден

В края на тази книга разглеждаме новите и бъдещите технологии в областта на мрежите. Някои то тях още са на чертожната маса, а други са тествани и приети за осъществими в лабораторни условия или в ограничена сфера.

С преминаването на политическите организации и големите корпорации към използването на нови, по-добри и по-бързи средства за пренасяне на мрежовите комуникации, в ежедневието на хората на всички социални нива една след друга биват представяни съвременни нови разработки както в областта на хардуера, така и в областта на софтуера. Начинът, по който работим и играем, се трансформира, а оптимистите предвиждат, че международните и културни бариери ще изчезнат, като глобалната възможност за връзка ще направи света по-малък или поне по-достъпен. Много хора пристъпват към изграждането на центрове за общо използване на технологии, осигуряващи достъп и обучение за групи, които традиционно нямат възможност да се възползват от компютърната технология и мрежовите връзки.

Да се определи накъде отива развитието на мрежите е опит да се предвиди непредвидимото. Преди двадесет години много от технологиите, които днес приемаме като даденост, бяха немислими за всички, освен за научните фантасти. Вероятно след двадесет години компютрите и мрежите ще се развият в такива направления, които днес дори не можем да си представим. Но на хоризонта има някои интересни възможности, разгледани в следващите секции.

„Интелигентни“ домакински електроуреди

Макар и не широко достъпна, концепцията за интелигентни домакински уреди и къщи е вече реалност. Днес можете да купите кухненски електроуреди с вградени микропроцесори или миниатюрни компютри, които контролират температурата, времето на печене и др. Следващата стъпка – и то не много голяма – е свързването на тези малки компютри в мрежа, така че да можете да ги командвате отдалеч. Вероятно в не твърде далечно бъдеще ще се свързваме онлайн от офиса, ще осъществяваме достъп до нашата фурна и ще указваме по кое време да започне подгряването, за да се подготви ястието за нашето пристигане.

Тази концепция логически води до следващата: интегрираната интелигентна къща, управлявана с компютър и свързана към централна мрежа. Основен пример за такава къща е имението за милиони долари на президента на Microsoft Бил Гейтс. Имението притежава компютъризиран климатичен контрол и специални музикални „зони“, които следват човека от стая в стая.

Много компании могат да направят вашата къща интелигентна, като я окабелят за свързване към Ethernet мрежа и интегрират вашите домашни компютри с вашия телефон, охранителна система, домашен кинотеатър, отопление и климатици, и осветителната система. Можете да контролирате тези системи с щракване на мишката или дори с гласова команда. Фигура 1–5 илюстрира някои възможности, които в момента са достъпни в интелигентната къща.

Къщата на бъдещето ще разгледаме малко по-подробно в Глава 19, „Технологиите на бъдещето".

Фигура 1–5 *Технологията на интелигентната къща пренася мрежата на бъдещето в днешния ден.*

Телефониране от вкъщи

В последните няколко десетилетия телефонната технология бързо напредна. Но разработките в тази област бяха предлагани на пазара и интегрирани в нашия живот толкова меко и постепенно, че тяхното въздействие не предизвиква никакви грижи, каквито би предизвикало в други случаи.

Операторите на мобилни телефони създадоха клетъчни и сателитно базирани мрежи, които сега предлагат интелигентни услуги като безжичен достъп до Интернет на приемливи цени. Технологията се подобрява непрекъснато.

Традиционните телефонни компании (означавани в индустрията като *телеко-ми*), подтиквани от конкуренцията с кабелните TV компании, реализират трансфер за високоскоростни услуги за данни като ADSL (Asynchronious Digital Subscriber Line) на достатъчно ниска цена за пазара на домашните потребители.

Приложенията за телефония интегрират персоналните компютри и телефона по най-различни начини, които позволяват даване на автоматичен отговор, съхранение на съобщения и приемане на съобщения с помощта на компютър.

ЗАБЕЛЕЖКА Приложенията за *телефония* са тези, които комбинират телекомуникационните технологии с компютърните технологии. Те включват реализации, отговарящи на спецификациите на Telephony Applications Programming Interface (TAPI) и стандартите на консорциума ITC (Internet and Telecoms Convergence Consortium).

Програмите за телефониране през Интернет, използващи глас по IP (voice over IP) ви позволяват да избегнете напълно телефонните линии (ако имате Интернет връзка по кабел, безжична или някаква друга преносна среда) и да провеждате международни разговори от вашия компютър, без да плащате високите такси.

Новите операционни системи, например последната версия на Microsoft Windows, включват поддръжка на IP телефония, която съчетава предаване на глас, видео и данни по TCP/IP връзки с подобрено качество на услугата.

По-подробен поглед на персоналните комуникационни системи на бъдещето ще направим в Глава 19.

Свързаното в мрежа работно място

Едно добро мерило, по което можем да преценим всяка бизнес сграда, в която влезем, е това дали на всяко бюро има по един (или няколко) компютъра, всичките свързани към вътрешна локална мрежа, Интернет и няколко отдалечени частни мрежи. Можем само да гадаем по какво работната среда на бъдещето може да бъде по-обвързана с мрежите, отколкото е днес.

Офисът на утрешния ден ще бъде още по-зависим от мрежовата технология. Когато бизнес средищата бъдат свързани посредством кабели с оптични влакна и други високопроизводителни преносни среди, увеличаването на пропускателната способност и видеото в реално време ще направи телеконферирането атрактивна алтернатива на работните срещи с лично присъствие на участниците. Вероятно все повече и повече служители ще работят от вкъщи. Но те няма да бъдат изолирани с техните собствени малки проекти. Вместо това те ще използват съвместно документи по мрежата, за да се чувстват в по-голяма степен обвързани с работната среда на целия екип.

Размерите на мощните компютри ще намаляват, а възможностите им ще се увеличават, поради което ще става по-лесно „да вземеш офиса си на път". Ръчните преносими системи, които днес интегрират електронна поща, достъп до Web, календари и управление на работни задачи, без съмнение в бъдеще ще осигуряват видео при поискване, гласови комуникации и услуги за уведомяване – комбинирайки функциите, изпълнявани днес от отделни устройства. Вече няма да бъде необходимо да носите палмтоп компютър, мобилен телефон и пейджър; една машина, достатъчно малка за носене на колана или в джоба, ще прави всичко това.

Тази универсална възможност за свързване и достъп притежава потенциал за увеличаване на продуктивността на всички типове бизнес организации.

Училищата на бъдещето

Бъдещето на образованието ще бъде силно повлияно от разработките в мрежовите технологии. Факт е, че вече стана нещо обикновено за библиотеките от елементарно до университетско ниво да включват един или повече свързани към Интернет компютри в помощ на студентите.

Най-драматичният ефект от технологията върху училищата е възможността за достъп до информация от такъв мащаб, който никога досега не е бил възможен. Със свързването в мрежи на все повече обществени и частни училища ще се промени начинът, по който учениците и студентите осъществяват достъп до научна информация. Фактически може да се промени дори самата същност на тези източници, които могат да изискват включване на мултимедиен материал.

Вероятно ще станат популярни нови методологии за обучение и учене, включващи участието на повече сетива. При по-малките ученици това означава използване на образователни интерактивни игри, които ангажират вниманието и способстват за изграждане на координацията ръка-око.

При по-големите ученици от колежите и студентите в университетите изглежда, че тенденцията ще бъде дистанционното обучение. Студентите могат да провеждат учебните занятия посредством компютър, като свалят преподавания материал за четене, изпращат изпълнените задания по електронна поща и участват в учебни дискусии чрез чат на живо. Вече има малък процент учебни курсове, предлагани по този начин; очакваме, че в следващото десетилетие това ще стане стандартен начин за получаване на диплома от колеж и дори придобиване на дипломи за висше образование и следващи степени.

Грижа за здравето по мрежата

Напредъкът в компютърната и мрежова технология ще упражни огромно въздействие върху медицината и грижата за здравето. Най-очевидното предимство на мрежите за здравната индустрия е възможността на лекарите да обменят записи за пациенти и диагностична и терапевтична информация.

Други амбициозни разработки вече заемат своето място или се очакват да станат реалност в близко бъдеще. Например дистанционната хирургия – в която лекарят, извършващ операцията, контролира от отдалечено местоположение роботизирано устройство, което реално оперира пациента – вече показва успешни резултати при експериментални ситуации.

Друга подобна концепция е телепрегледът (дистанционният преглед), при който лекарят провежда подготвителен физически преглед по двупосочно видео с помощта на посредник – помощник-лекар или медицинска сестра – който реално се намира при пациента. Идеята на телемедицината е особено привлекателна за селските области и слаборазвитите страни, където лекарите не достигат.

Технологията и законът

Следователските и съдебните процедури станаха по-ефикасни с въвеждането на мрежите и последвалото подобрение на съхраняването и споделения достъп до информацията.

Изпълнителната власт също възприе работата с новите технологии. Сега много полицейски управления имат мобилни терминали за данни (MDT), инсталирани в полицейските коли; те позволяват на полицаите да извършват бърз и директен достъп до криминални досиета, шофьорски книжки, различни ведомствени данни и ресурси. MDT също така дава на полицаите възможност да комуникират помежду си по мрежата по начин, който е по-сигурен от обмена на съобщения по открити радиоканали. Полицейските отдели използват също технологията на глобалната система за позициониране (GPS), комбинирана с компютърно подпомагано проследяване, за да осигурят точна информация на диспечерите и супервайзерите в полицейското управление за местоположението на всяка една подвижна полицейска единица по всяко време. Това дава на командващия щаб по-голям контрол и позволява по-добро разполагане на полицаите.

Интергалактически мрежи?

Сега, когато връзката към Интернет обхваща почти всеки ъгъл на света, следващата логическа стъпка е свързването в мрежа на крайната граница – външният космос. Идеята не е толкова футуристична, колкото изглежда; фактически компютърните комуникации вече изпращат сигнали до спътниците на околоземна орбита. На път са проекти за предаване на сигнали в далечния космос с

надежда за улавяне на признаци на живот, ако съществува такъв, на други планети.

Компютрите на земята вече контролират действията на космически мисии без участие на хора и играят огромна роля в пътуванията на космическите совалки. Мрежовите комуникации правят възможни изследванията на други планети.

Кратък преглед на терминологията на мрежите

Когато посещавате друга страна, първата задача, с която трябва да се преборите, е да научите езика. Същото е валидно и при навлизане в нова област на обучение или нова професионална сфера.

Компютърните мрежи, подобно на повечето професионални сфери, има свой собствен жаргон, съставен от технически термини, съкращения и акроними, които могат на пръв поглед да изглеждат чужди на непосветения подобно на азбуката на държава на другия края на света.

Без добро познаване на терминологията трудно можете да разберете концепциите и процесите в тази книга. Тази секция ще ви даде начален старт в дешифрирането на някои от техническите обяснения в книгата, а също и в други въвеждащи ръководства по мрежи и мрежови операционни системи.

Секцията не е изчерпателен речник на мрежови термини, а по-скоро е предназначена за бързи справки, които дефинират някои от най-важните и най-основни думи, фрази и съкращения, позволяващи ви да преминете без проблеми през следващите няколко глави.

Всяка дефиниция е разширена в следващите глави. За по-изчерпателен списък от дефиниции се обърнете към речника в края на книгата.

Терминология, свързана с концепциите

мрежов модел – Мрежовият модел е графично представяне на процесите на мрежовите комуникации. Разпространените модели представят тези процеси като слоеве или нива; затова те се наричат слоести модели. Най-често споменаваните са седемслойният модел OSI (Open System Interconnection), четирислойният DoD модел (понякога наричан мрежов модел TCP/IP) и мрежовия модел на Microsoft Windows. Всеки от тях ще разгледаме подробно в Глава 2, „Категоризиране на мрежите“.

мрежа клиент/сървър – В терминологията на компютърните мрежи *клиентският* компютър е този, който изпраща запитване към друг компютър за достъп до неговите данни или ресурси. Компютърът, който отговаря на това запитване и споделя своите данни или ресурси по мрежата, се нарича *сървър*. В *равноправна мрежа* (*peer to peer*), наричана също *работна група* (*workgroup*), всички компютри в мрежата действат и като клиенти, и като сървъри. В *базираните на сървър мрежи* (понякога наричани мрежи клиент/сървър) и в Microsoft Windows мрежите, наричани *домейни*, има компютър, назначен за сървър, който работи със специален сървърен софтуер, изпълняващ функции по автентикация/управление на сигурността на потребителите. Равноправните мрежи и базираните на сървър мрежи ще разгледаме в Глава 2.

Терминология, свързана с мрежовия хардуер

NIC – Произнася се „ник“ и означава мрежовата интерфейсна карта, наричана също мрежов адаптер (но поради неизвестна причина никога не се нарича NAC) или просто мрежовия интерфейс. Тази карта обикновено се поставя в ISA, PCI или PCMCIA (PC card) слот в компютъра и се свързва към мрежовата *преносна среда*, която от своя страна се свързва към други компютри в мрежата.

преносна среда (media) – Преносната среда представлява съвкупност от средства, с помощта на които сигналите биват изпращани от един компютър на друг по кабел или чрез *безжични* (*wireless*) методи.

безжична преносна среда (wireless media) – Безжичната преносна среда, например радио, лазерни, инфрачервени и сателитни/микровълнови технологии, пренася сигналите от един компютър на друг без постоянно установена физическа връзка (кабел).

коаксиален кабел (coax) – Коаксиалният кабел е подобен на телевизионния кабел; той има медно ядро, обвито със солиден защитен екран и се използва за свързване на компютрите в мрежа. Може да бъде използван тънък или дебел коаксиален кабел.

усукана двойка (twisted pair) – Усуканата двойка е тип кабел, използван също за телефонни комуникации. Той се състои от двойка медни проводници, усукани във вътрешността на външна защитна обвивка. Съществуват два основни типа: UTP (неекранирана усукана двойка) и STP (екранирана усукана двойка). UTP се използва най-често за окабеляване на съвременни Ethernet мрежи. Той се разделя на различни категории в зависимост от това, дали е предназначен за предаване на глас или данни, както и по скоростта на предаване, която поддържа. „Cat 5“ означава категория 5, което ще рече, че може да бъде използван за глас (телефон) или данни и поддържа скорости до 100 Mbps.

пленум (plenum) – Пленумът в една сграда представлява пространството между висящите тавани и намиращата се над тях етажна плоча; през пленума могат да бъдат прокарани кабелите. Кабелът за прокарване през пленум, наричан често огнеупорен кабел, има външна обвивка, направена от тефлон или друг материал, който издържа на огън и отговаря на противопожарните правила на сградата за инсталиране на кабели.

PVC – В контекста на мрежовия хардуер и кабелите, PVC означава поливинилхлорид – материалът, от който се правят обвивките на кабелите, предназначени за обикновени инсталации. Той е по-евтин от устойчивите на огън материали, но не отговаря на противопожарните правила за инсталиране в сгради, защото при горене отделя отровен газ.

оптични влакна (fiber optics) – Често се използва и съкратеното наименовани *оптичен кабел*; оптичните влакна по същество са кабели с ядро, представляващо стъклена или пластмасова нишка (вместо медна), по която светлинни импулси пренасят сигнали. Оптичните влакна имат много предимства пред медните проводници по отношение на скоростта на предаване и запазване на целостта на сигнала на големи разстояния; но те са по-скъпи и с тях се работи по-трудно.

устройства за свързване (connectivity devices) – С този термин се означават няколко различни типа устройства, които се използват за свързване на кабелни сегменти, за свързване на две или повече по-малки мрежи (или подмрежи) в една по-голяма, или за разделяне на голямата мрежа на по-малки такива. Терминът обхваща повторителите, хъбовете, суичовете, мостовете, маршрутизаторите и b-маршрутизаторите. Всяко от тези устройства е разгледано детайлно в Глава 7 – „Физически компоненти на мрежата“.

Терминология, свързана със софтуера

протокол (protocol) – Мрежовият протокол представлява набор от правила, по които комуникират компютрите. Понякога протоколите се сравняват с езици, но по-добрата аналогия е, че протоколът е подобен на синтаксиса на един език, т.е. редът, в който възникват процесите. Има множество различни компютърни протоколи. *Протоколният стек* описва набор от два или повече протокола, работещи заедно. Терминът *протоколен пакет* (protocol suite) описва набор от няколко протокола, извършващи различни функции, свързани с различни аспекти на комуникационния процес.

NOS – Съкращението NOS, което означава мрежова операционна система (от Network Operation System), обикновено се използва за сървърен софтуер, например Windows NT, Windows 2000 Server, Novel NetWare и UNIX. Терминът понякога означава и мрежови компоненти на клиентската операционна система, като Windows 95 или Macintosh OS.

клиентска операционна система (client operation system) – Означавана също като настолна операционна система, клиентската операционна система представлява софтуерът на операционната система, с който работят работните станции в мрежата и осъществяват достъп до сървъра и/или влизат в мрежата като клиенти.

хибридна мрежа (hybrid network) – Хибридната мрежа е такава, при която софтуерните продукти на различни производители на мрежи работят съвместно, особено по отношение на сървърните операционни системи. Например мрежа, която има Windows NT домейн контролери, NetWare файлови сървъри и UNIX Web сървър, представлява хибридна мрежа.

Терминология на дизайна и топологията

LAN (local area network) – Локалната компютърна мрежа (LAN) представлява мрежа, която обхваща само ограничена географска област. Това може да бъде стая, етаж, сграда или дори цял университет.

WAN (wide area network) – Глобалната компютърна мрежа (WAN) е изградена от свързани една с друга локални мрежи. Тя обхваща широки географски области, като използва WAN връзки, например телефонни линии или сателитна технология за свързване на компютри в различни градове, държави и дори в различни континенти.

MAN (metropolitan-area network) – Градската компютърна мрежа (MAN) представлява мрежа с размер, по-голям от локална мрежа и по-малък от глобална мрежа. Това е мрежа, която обхваща приблизително областта на голям град или централна градска област.

физическа топология (physical topology) – Разположението или физическата форма на мрежата, т.е. дали компютрите са подредени така, че кабелът да върви от една машина към друга в линеен ред (линейна шинна топология), дали последният компютър се свързва обратно към първия за формиране на кръг (кръгова топология), дали системите „се срещат в средата“ чрез свързването им към централен хъб (топология звезда) или пък множество допълнителни конекции изграждат пътеки (решетъчна топология). Характеристиките на всяка от тези топологии са разгледани в Глава 3, „Мрежови концепции, модели и стандарти“.

логическа топология (logical topology) – Логическата топология представлява пътят, по който се предават сигналите от един компютър до друг. Тя може да

отговаря на физическата топология. Например мрежата може да бъде физическа *звезда (star)*, в която всеки компютър е свързан към централен хъб, но вътре в хъба данните могат да пътуват в кръг, което я превръщат в *логически кръг* (*logical ring*). Разликата между физическата и логическата топология е разгледана в Глава 3.

Терминология, свързана с мерните единици

бит (bit) – Най-малката единица данни в компютъра. Битът е равен на 1 или 0 и представлява двоичен формат, в който данните биват обработвани от компютрите.

байт (byte) – Байтът е мерна единица, използвана за описание на размера на файл с данни, количеството пространство на диск или друг запаметяващ носител, или количеството данни, изпращани по мрежа. 1 байт е равен на 8 бита данни.

килобайт (kilobyte – KB) – Килобайтът е приблизително равен на 1000 байта (по-точно 1024 байта). Може да бъде записан съкратено с „K".

килобайта в секунда (kilobytes per second - KBps) – Това е стандартна мерна единица за количеството данни, предавани по дадена мрежова връзка.

килобита в секунда (kilobits per second - kbps) – Това е стандартна мерна единица за количеството данни, предавани по дадена мрежова връзка.

мегабайт (megabyte - MB) – Мегабайтът е приблизително равен на 1 милион байта (точно 1 048 576). Понякога мегабайтът се означава като „meg".

мегабайта в секунда (megabytes per second - MBps) – Това е стандартна мерна единица за количеството данни, предавани по дадена мрежова връзка.

мегабита в секунда (megabits per second - Mbps) – Това е стандартна мерна единица за количеството данни, предавани по дадена мрежова връзка.

херц (Hertz – Hz) – Мерна единица за честота. Това е скоростта на промяна на състоянието или цикъл в звукова вълна, променлив ток или друга циклична вълнова форма. Означава един цикъл (такт, тактов период) в секунда и се използва за описание на скоростта на микропроцесора на компютъра.

мегахерц (megahertz – MHz) – Един милион такта в секунда. Това е общоприета мерна единица за скоростта на изчислителна обработка на даден чип, като например микропроцесора на компютъра.

гигахерц (gigahertz – GHz) – Един милиард такта в секунда. Това е общоприета мерна единица за скоростта на изчислителна обработка на даден чип, като например микропроцесора на компютъра.

ЗАБЕЛЕЖКА Всеобща грешка е объркването на KB с kb и на MB с mb. Помнете, че трябва да направите правилни изчисления, когато сравнявате скоростите, измерени в KB, с тези, измерени в kb. Например софтуерът на модема обикновено показва скоростта на вашата връзка като килобита за секунда (например 45 kbps). Но популярните браузъри показват скоростите за сваляне (download) на файлове в килобайти за секунда, което означава, че при връзка с 45 kbps вашата скорост на сваляне ще бъде максимум 5,76 KBps. На практика не можете да достигнете тази скорост на сваляне поради другите фактори, които консумират пропускателна способност в същото време. Скоростите за трансфер на данни ще разгледаме по-детайлно в Глава 7.

ЗАБЕЛЕЖКА Процесорите на персоналните компютри стават все по-бързи. Микропроцесорите, използвани в персоналните компютри през 80-те години, обикновено работеха със скорост под 10 MHz (оригиналният IBM PC беше с честота 4,77 MHz). През 2000 година процесорите на компютрите достигнаха скорост 1 GHz, която продължава да нараства.

Какво обхваща книгата и какво – не

Тази книга представя общ преглед на основите на компютърните мрежи и популярните операционни системи клиент-сървър, които се използват днес. Тъй като обхват е широк, нямаме възможност да се впускаме в дълбочина или в детайли по отделните въпроси по начина, по който правим това в по-специализираните заглавия.

В книгата в края на всяка глава предоставяме списък от ресурси, които могат да ви насочат към източници с по-подробна информация по всеки от представените въпроси.

Сертификати по мрежи

Поради недостига на квалифицирани професионалисти и високата необходимост от персонал в мрежовата индустрия, сертифицирането стана популярно средство за измерване на основните знания и квалификации, особено за работни места на входно ниво. Много организации предлагат изпити за сертифициране, за да тестват вашите знания по мрежови технологии.

Сертификати, специфични за производителя

Някои сертификационни програми са специфични за производителя (vendor-specific); кандидатите биват тествани по техните възможности за работа с конкретни хардуерни или софтуерни продукти и от тях се очаква да знаят официалната позиция на производителя, както и да отговарят на изпитните въпроси, спазвайки конкретната философия и гледна точка на производителя. Много от тези сертификати, например Cisco CCIE и Microsoft MCSE, се приемат много добре от индустрията.

ЗАБЕЛЕЖКА Специфичните за производителя сертификати са полезни за демонстриране на конкретни способности с конкретни продукти на компанията и в много случаи са желани и дори задължителни за работодателите.

Някои от най-популярните специфични за производителите сертификационни програми са следните:

- Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP) и Cisco Certified Internetwork Expert (CCIE)
- Microsoft Certified Professional (MCP) и Microsoft Certified Systems Engineer (MCSE)
- Novel Certified NetWare Administrator (CNA) и Novel Certified NetWare Engineer (CNE)

Други компании, като Sun, Lotus, IBM, RedHat и други разпространители на Linux, също предлагат сертификационни изпити за техния мрежов софтуер. Съществуват също специфични за производителите на хардуер сертификати, предлагани от IBM, Compaq Computers, Digital Equipment Corporation и други.

Сертификати, необвързани с производител

Необвързаните с даден производител програми за сертифициране целят да определят общите познания и умения, прилагани при работата с мрежови продукти на широк обхват от производители.

Най-популярният сертификат за определяне на уменията по мрежи, необвързан с конкретен производител, е Network+, предлаган от Computing Technology Industry Association (CompTIA). Тази асоциация е разработила и неутралния спрямо производителите изпит за хардуерни техници по персонални компютри, наречен A+.

Сертификатите, които не са свързани с конкретни производители, са полезни за демонстриране на широка база от знания и умения, отнасящи се до основни мрежови концепции, практики и терминология.

Тази книга и сертифицирането

Тази книга е проектирана така, че да ви даде обща представа за основните елементи на мрежите от персонални компютри. Тя може да послужи като встъпително ръководство за тези от вас, които сега навлизат в IT индустрията, и тези, които планират да се явят на изпит за сертифициране като CCNA, MCSE или CAN.

Заедно с друг предварително подготвен материал, тази книга може да бъде използвана и като учебник за изпита Network+. Обхванали сме всички въпроси, включени в задачите от изпита.

ЗАБЕЛЕЖКА Сертификатът Network+ се поддържа и спонсорира от компании като Microsoft, Novell, IBM, Lotus и много други.

Макар че новият сертификат Windows 2000 MCSE не включва изпит, посветен изключително на основите на мрежите, много от материала в тази книга е полезен за изучаване за основния изпит по Windows 2000, а именно изпит 70-216.

Обобщение

Тази глава ви представи света на компютърните мрежи и начините, по които отделни самостоятелни системи започват да бъдат свързани в мрежи. Научихте за ранните локални мрежи и разработката на ARPAnet, която е общ проект между Министерството на отбраната на САЩ и техническите университети, превърнал се в днешния Интернет.

Тази глава се докосна до някои от начините, по които технологиите влияят на нашия живот, и предостави общ преглед на някои от концепциите, изложени в дълбочина в следващите глави на книгата. Научихте някои общоизползвани термини, свързани с мрежите, както и за ролята на техническите сертификати в мрежовата индустрия.

В следващите глави ще допълните тази информация, като изучите моделите и стандартите, по които се изграждат съвременните мрежи. Ще преминем от малки локални мрежи до сложни глобални мрежи и ще се запознаем с методите на предаване на сигнали, архитектурите, хардуера, протоколите, операционните системи и услугите, които осигуряват основите на модерните мрежи.

Ще изучите такива горещи теми като сигурността и отстраняването на неизправности; ще разгледаме такива специални области, като отдалечения достъп, виртуалните частни мрежи и мрежите с тънки клиенти. Ще дискутираме зараждащите се технологии, които обещават, че мрежите на бъдещето ще бъдат още по-интересни и по-полезни на практика, отколкото днешните мрежи.

Допълнителни източници

Един чудесен Web-базиран ресурс за дефиниции на мрежови термини и съкращения е www.whatis.com.

Добър източник за допълнителна информация за историята на мрежите е www.silkroad.com/net-history.html.

Повече информация за сертификационните програми CompTIA и Network+ можете да намерите на Web сайта на CompTIA на адрес www.comptia.com.

За повече информация относно обучението и изпитите за специфични за производителите сертификати вижте следните Web сайтове:

- Cisco: www.cisco.com/warp/public/10/wwtraining/certprog
- Microsoft: www.Microsoft.com/train_cert
- Novell: education.novell.com/certinfo

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Каква е ранната реализация на мрежовата технология, разработена от французите в началото на 19-ти век?

   a Телефонната мрежа
   b Оптичната телеграфна мрежа
   c Мрежата Ethernet
   d ARPAnet

2 Какво е името на технологията, която използва телефонната мрежа?

   a Комутиране на пакети
   b Комутиране на слой 2
   c Комутиране на слой 3
   d Комутиране на вериги

3 Каква е технологията, която е най-подходяща за предавания на данни, предавани на пикове?

a Комутиране на пакети
b Аналогово предаване
c Комутиране на вериги
d Технология switchboard

4 Кое от следните е недостатък на мрежите, базирани на мейнфрейм компютри? (Изберете всички верни отговори)

a Хардуерът на мейнфрейм компютрите е по-скъп от хардуера на персоналните компютри.
b Мейнфрейм компютрите не могат да обработват големи количества данни, които се обработват от PC сървърите.
c Мейнфрейм компютрите представят единична точка на отказ
d Мейнфрейм терминалите са по-малко сигурни от мрежовите персонални компютри.

5 Кое от следните може да бъде споделено по компютърна мрежа? (Изберете всички верни отговори)

a Данни
b Приложения
c Принтери
d Модеми

6 Кое от следните се класифицира като входно устройство? (Изберете всички верни отговори)

a Плотер
b Факс-машина
c Цифрова камера
d Принтер

7 Какво е името на метода, представен през 80-те години, за осигуряване на средства за асоцииране на дружелюбни имена на хостове с IP адреси?

a DoD
b DHCP
c DSL
d DNS

8 Как се наричат приложенията, които комбинират телекомуникационните и компютърните технологии?

a Компютърни технологии
b Телефония
c TPI технологии
d ITC технологии

9 Какъв тип компютър изпраща запитване към друг компютър за достъп до неговите данни или ресурси?

a Сървър
b Работна станция
c Клиент
d Терминал

10 Какъв е наборът от правила, по които комуникират компютрите?

a Протокол
b Тип медия
c Байт
d Топология

Глава 2

Категоризиране на мрежите

Професионалистите по технологии разделят мрежите на категории на базата на характеристиките, необходими за администрирането или отстраняването на неизправности на конкретна мрежа. Можете да класифицирате типовете мрежи в зависимост от физическите свойства или характеристиките на софтуера, който се изпълнява на тях. Например категоризацията може да бъде базирана на слените характеристики:

- Физически обхват
- Метод на администриране
- Мрежова операционна система
- Мрежови протоколи
- Топология
- Архитектура

В следващите секции ще разгледаме всеки от методите за класификация.

Категоризация на мрежите според физическия обхват

Един от методите за категоризация на мрежите е базиран на физическия обхват, който включва географската област, която се обхваща от мрежата, и в помалка степен размера на мрежата. Използвайки този метод можем да класифицираме дадена мрежа в една от следните три категории:

- Локална мрежа (LAN)
- Градска мрежа (MAN)
- Глобална мрежа (WAN)

Тези категоризации са свързани донякъде с размера на мрежата, представляващ броя на компютрите и потребителите (обикновено LAN мрежите са помалки от MAN, които от своя страна са по-малки от WAN). Те са свързани също до известна степен с финансовите ресурси (изобщо WAN е много по-скъпа за инсталиране и поддръжка от LAN), но най-важният определящ фактор е географската област, която мрежата покрива.

Характеристики на LAN мрежата

Речникът American Heritage Dictionary дефинира думата *local* като „свързан със или характерен за конкретно място, а не за по-голяма област". Подобно на това терминът *LAN* описва мрежа, която обхваща ограничена област; компютрите, принадлежащи към мрежата във физическа близост един до друг. Но LAN мрежите могат да варират драстично по броя на компютрите и потребителите. Например една локална мрежа може да се състои от два компютъра, разположени на разстояние няколко метра в офиса или вкъщи, или да включва стотици компютри, обхващайки няколко етажа от небостъргач, или в някои случаи дори множество сгради, разположени близо една до друга. Фигура 2-1 показва графично представяне на разположението на проста локална мрежа.

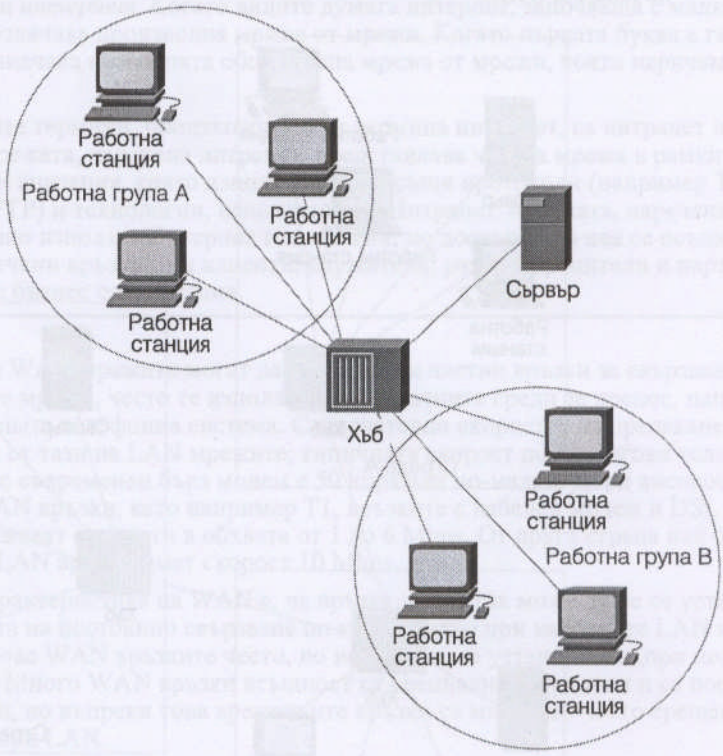
Фигура 2-1 *LAN мрежата е ограничена до конкретна географска област.*

ЗАБЕЛЕЖКА Мрежовата архитектура и типът на кабела могат да ограничат броя на компютрите, съдържащи се в една LAN мрежа. Повече за тези ограничения ще научите по-късно в тази глава, в секцията „Категоризация на мрежите по архитектура".

Големите локални мрежи могат да бъдат разделени на *работни групи* с цел полесното им управление. В този контекст работната група се състои от потребители, които споделят едни и същи ресурси, като файлове, принтери и приложения. Например в локалната мрежа на една организация можете да създадете работни групи за различните отдели – Продажби, Финанси и Личен състав. Фигура 2-2 показва как LAN мрежата може да бъде разделена на работни групи.

Локалните мрежи образуват основата за по-големи мрежи (MAN и WAN), които се създават чрез свързване на две или повече локални мрежи.

Фигура 2-2 *LAN мрежите могат да бъдат разделени на работни групи.*

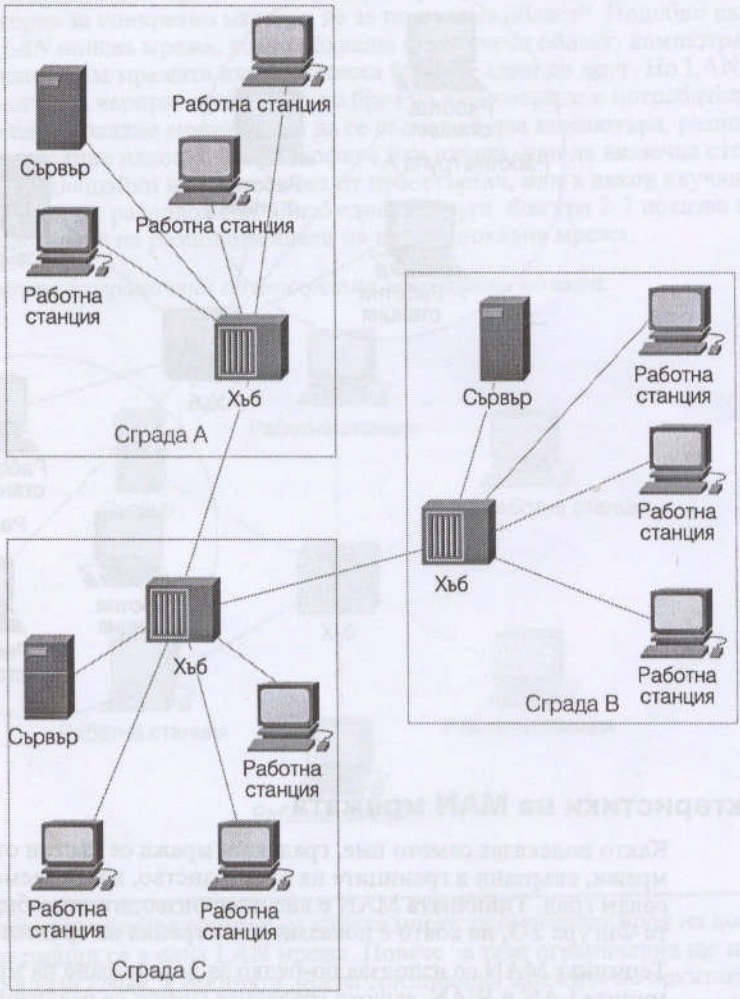


Характеристики на MAN мрежата

Както подсказва самото име, градската мрежа се състои от две или повече LAN мрежи, свързани в границите на пространство, което заема приблизително един голям град. Типичната MAN е високопроизводителна обществена мрежа. Вижте Фигура 2-3, на която е показана илюстрация на градска мрежа.

Терминът MAN се използва по-рядко за дефиниране на мрежи, отколкото термините LAN и WAN, защото градските мрежи се реализират много по-рядко. Повечето мрежи са в рамките на сграда или комплекс от сгради (например университетски комплекс) и поради това попадат в категорията на LAN, или пък обхващат по-големи разстояния с възли, разположени в различни градове, щати и дори държави, като по този начин могат да бъдат квалифицирани като WAN мрежи. Максималното разстояние, дефиниращо една MAN мрежа, е приблизително 50 мили (80 км).

Фигура 2-3 *MAN мрежата покрива по-обширна област от LAN, но е географски по-ограничена от WAN.*



Характеристики на WAN мрежата

WAN представлява мрежа, която обхваща голяма географска област. Най-добрият и най-популярният пример за WAN е Интернет. Но WAN може да бъде и частна мрежа. Например организация с офиси в много страни може да има корпоративна WAN мрежа, свързваща отделните местоположения посредством телефонни линии, сателити или други технологии. Глобалната мрежа най-общо се състои от множество взаимосвързани локални мрежи.

ЗАБЕЛЕЖКА Резултатът от свързването на мрежите една с друга се означава като *интермрежа*, или *интернет*. Когато видите думата интернет, започваща с малка буква, това означава произволна мрежа от мрежи. Когато първата буква е главна, думата означава глобалната обществена мрежа от мрежи, която наричаме Интернет.

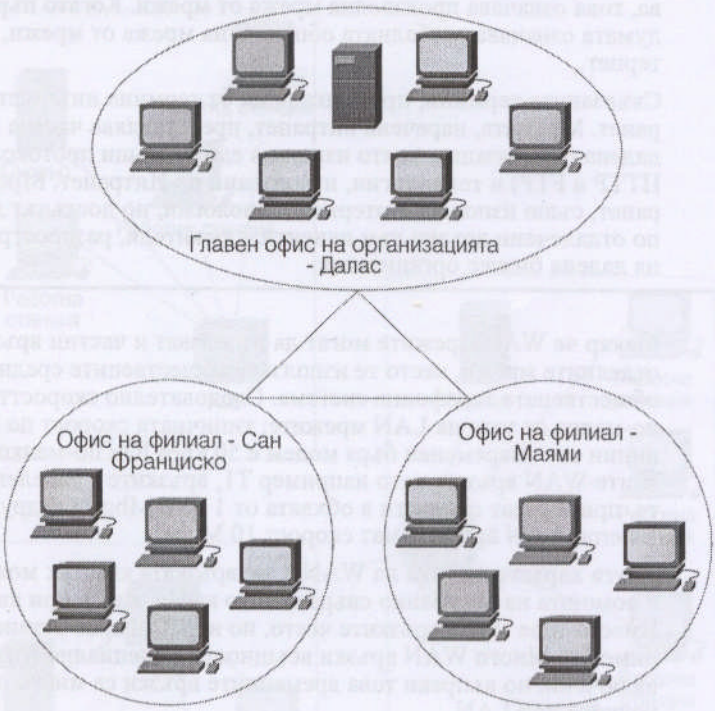
Свързаните термини, произхождащи от термина интернет, са интранет и екстранет. Мрежата, наречена интранет, представлява частна мрежа в рамките на дадена организация, която използва едни и същи протоколи (например TCP, HTTP и FTP) и технологии, използвани по Интранет. Мрежата, наречена екстранет, също използва Интернет технологии, но достъпът до нея се осъществява по отдалечени връзки към клиенти, служители, разпространители и партньори на дадена бизнес организация.

Макар че WAN мрежите могат да използват и частни връзки за свързване на отделните мрежи, често те използват обществените среди за пренос, например обществената телефонна система. Следователно скоростта на предаване често е по-малка от тази на LAN мрежите; типичната скорост по аналогови телефонни линии със съвременен бърз модем е 50 kbps или по-малко. Дори високоскоростните WAN връзки, като например T1, връзките с кабелен модем и DSL линиите, притежават скорости в обхвата от 1 до 6 Mbps. От друга страна най-бавните Ethernet LAN връзки имат скорост 10 Mbps.

Друга характеристика на WAN е, че връзката към тях може да не се установява с помощта на постоянно свързване по кабел, както при кабелните LAN мрежи. Вместо това WAN връзките често, но не винаги, се установяват „при необходимост". Много WAN връзки всъщност са специално изградени и са постоянно включени, но въпреки това временните връзки са много по-често срещани, отколкото при LAN.

В обобщение, WAN мрежите могат да използват частни или обществени преносни среди и могат да се състоят от постоянно изградени връзки или dial-up конекции (установявани при необходимост). WAN връзките обикновено са по-бавни в сравнение с LAN връзките. WAN мрежите се разделят на разпределени или централизирани. *Разпределените* WAN, например Интернет, нямат централна точка на управление. От друга страна, централизираните WAN са базирани на централен сървър или централизирано място (например главния офис на организация), към което се свързват всички други компютри. Фигура 2-4 показва централизирана WAN мрежа.

Фигура 2-4 *Централизираната WAN мрежа е изградена около „главен" компютър или място, към което са свързани останалите компютри.*



WAN мрежите са *маршрутизирани* мрежи, което означава, че за да могат съобщенията да преминават от една LAN мрежа в друга, пакетите трябва да преминават през *шлюз* (*gateway*). Шлюзът представлява *маршрутизатор* (*router*) – компютър, конфигуриран за изпълнение на маршрутизиращи функции. Ще разгледаме по-детайлно работата на маршрутизаторите в Глава 9 – „Най-широкомащабната мрежа: глобалният Интернет".

Категоризация на мрежите по метод на администриране

Можете да категоризирате мрежите на базата на метода на тяхното администриране, т.е. как и от кого се управляват ресурсите. Мрежата може да бъде организирана както следва:

- Като равноправна (peer to peer) работна група, в която всеки компютър функционира и като клиент, и като сървър, и всеки потребител администрира ресурсите на своя компютър.
- Като клиент/сървър или сървърно базирана мрежа, в която администрирането е централизирано на компютър, работещ със специален сървърен софтуер и мрежова операционна система (NOS). Този компютър автентицира информацията за името на потребителя и паролата, за да позволи на оторизираните потребители да влизат в мрежата и да осъществяват достъп до ресурсите.

Кой от двата метода е по-добър? Това зависи от ситуацията. Всеки от тях има предимства и недостатъци, обобщени в таблица 2-1.

Таблица 2-1 *Предимства и недостатъци на равноправните мрежи и на мрежите клиент/сървър.*

Предимства на равноправната мрежа	Предимства на мрежата клиент/сървър
По-евтина за реализация.	Предоставят по-добра сигурност.
Не изискват NOS сървърен софтуер.	По-лесни за администриране, когато мрежата е по-голяма, защото администрирането е централизирано.
Не изискват специално назначен мрежов администратор.	Всички данни могат да бъдат архивирани в едно централно място.
Недостатъци на равноправната мрежа	**Недостатъци на мрежата клиент/сървър**
Не може да бъде мащабирана добре за разрастване до големи мрежи; администрирането става неуправляемо.	Изисква скъп NOS софтуер, например NT или Windows 2000 Server, или пък Novell Net Ware.
Всеки потребител трябва да бъде обучаван да изпълнява задачи по администриране на мрежата.	Изисква скъп, по-мощен хардуер за сървърната машина.
По-несигурна е.	Изисква професионален администратор.
Всички машини, обменящи ресурси, влияят отрицателно на производителността.	Има само една точка на отказ, ако има един-единствен сървър; данните на потребителите могат да станат недостъпни, ако сървърът спре работа.

Както виждате, изборът на метода за организация на администрирането зависи от такива фактори, като броя на компютрите и потребителите, изискванията за сигурност, хардуера, персонала и достъпния бюджет.

Сървъри и клиенти

Преди да разгледаме по-отблизо характеристиките на всеки тип мрежа и начина за тяхното реализиране, нека да направим преглед на термините, използвани за описание на ролите, които могат да играят компютрите в мрежата.

Сървърът представлява компютър, който прави своите ресурси (данни, софтуер или свързаните към него периферни устройства, като например принтери) достъпни за други компютри в мрежата. От друга страна *клиентът* представлява компютър, който осъществява достъп до ресурсите на сървъра.

СЪВЕТ Можете да запомните двата по следния начин: Сървърите дават (т.е. споделят техни ресурси), а клиентите взимат (т.е. осъществяват достъп до ресурсите на сървърите).

Лесно можем да объркаме тези термини – макар че понякога използваме думата сървър, за да опишем компютър, специално предназначен за сървър, който обикновено е по-мощен, работи със софтуера на мрежова операционна система

и позволява централизирано управление на мрежата, всъщност *всеки* компютър, споделящ свои ресурси по мрежата, действа като сървър.

Сървъри, споделящи „споделени ресурси“

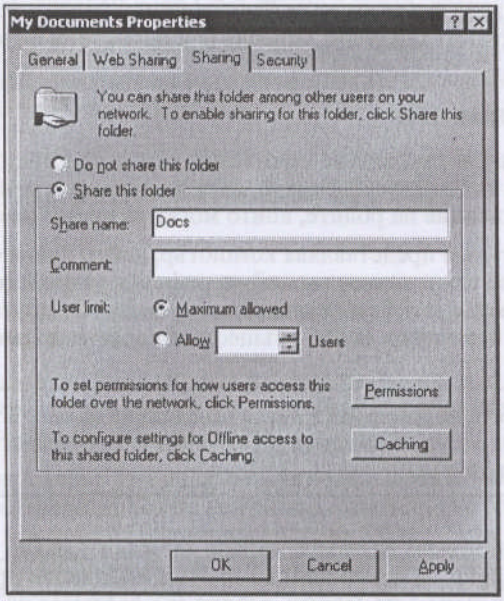
Операционните системи, които приемаме за клиентски или настолни операционни системи – например Windows 95/98, NT Workstation и Windows 2000 Professional – могат, и реално функционират като сървъри, когато създавате *споделени ресурси (shares)* на тях, за да позволите на други компютри да използват техни ресурси.

ЗАБЕЛЕЖКА Производителите на някои операционни системи използват термина *share*, за да опишат ресурсите, които са направени достъпни за други компютри, а други разпространители използват по-традиционната терминология *shared resource* (на български обаче и двата термина са приети като *споделен ресурс* – б.р.).

За да разрешите осъществяването на достъп до ресурси от страна на други компютри, трябва специално да установите ресурса като *споделен* (*shared*) и да му дадете *споделено име* (*share name*), което да го идентифицира в мрежата. Това име не е задължително да бъде същото като името на самия ресурс. Например ако имате папка, наречена Administration, която искате да споделите по мрежата, можете да наречете споделения ресурс „Admin“. Admin е името, което другите ще виждат, когато разглеждат мрежата. Също така те ще използват това име, когато установяват връзка към вашия споделен ресурс.

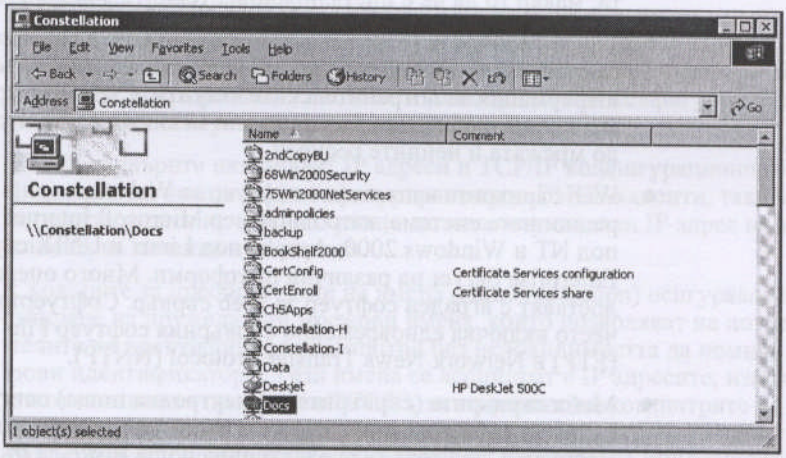
Фигура 2-5 показва диалоговия прозорец, използван в Windows 2000 за създаване на споделен ресурс за папката с име My Documents.

Фигура 2-5 *Създаване на споделен ресурс в Windows 2000.*



Обърнете внимание, че името на папката се появява в заглавната лента, но споделеният ресурс е именуван Docs. Когато друг компютър в мрежата направи справка в *списъка за преглед* (*browse list*), представляващ списък от достъпни споделени ресурси, ресурсът се появява, както е показано на Фигура 2-6.

Фигура 2-6 *Споделяният ресурс с име Docs се появява в списъка за преглед за сървъра с име Constellation.*



ЗАБЕЛЕЖКА Някои мрежови операционни системи позволяват споделените ресурси да бъдат „публикувани" в директорията (например споделените папки и принтери могат да бъдат публикувани в Active Directory в Windows 2000 и в NDS дървото в Novell NetWare). Това позволява на потребителите да откриват споделените ресурси без необходимостта да знаят точно на кой сървър физически е разположен ресурсът.

Специализирани сървъри

Всеки компютър, който споделя своите ресурси, е сървър. Но терминът често се използва за означаване на машини, които са специално предназначени за споделяне на техните файлове, приложения или периферни устройства. *Специализираният сървър (dedicated server)* обикновено е мощна машина с бърз процесор и голямо количество памет, и не се използва за изпълнение на ежедневни производствени задачи; той е специално предназначен за сървър. Достъпът до него обикновено е ограничен само до администраторите, които използват сървъра за управление, наблюдение и поддръжка на мрежата.

В голяма мрежа специализираният сървър може да изпълнява само една функция, както при следните ситуации:

- Файловите сървъри са сървъри, на които се съхраняват файлове с данни. Потребителите записват своите приложни данни на твърд диск на сървъра, вместо да ги записват на локалните твърди дискове на машините на техните работни станции. Файловете на сървъра са по-лесни за намиране, защото всички те са в едно централно местоположение; също така те лесно могат да бъдат архивирани.

- Принт сървърите представляват машини, които управляват един или няколко принтера, към които потребителите могат да изпращат по мрежата документи за отпечатване.
- Приложните сървъри са компютри, на които са инсталирани мрежови приложения. Потребителите могат да изпълняват приложението (например текстообработваща програма или програма за база данни) по мрежата, макар то да не е инсталирано на техните локални машини.
- Logon сървърите (наричани домейн контролери в Windows мрежите) съхраняват *база данни за сигурността* (*security database*), която съдържа информация за потребителските акаунти. Сървърът проверява акредитивите на потребителя в базата данни за сигурността и контролира достъпа до мрежата и нейните ресурси.
- Web сървърите изпълняват софтуер за Web сървъри в комбинация с операционната система, като например Microsoft Internet Information Server под NT и Windows 2000, Apache под Linux и UNIX сървъри и Netscape Enterprise Server на различни платформи. Много операционни системи се доставят с вграден софтуер за Web сървър. Софтуерът за Web сървър често включва едновременно сървърния софтуер File Transfer Protocol (FTP) и Network News Transfer Protocol (NNTP).
- Мейл сървърите (сървърите за електронна поща) осигуряват пощенски кутии за събиране на електронна поща, изпратена към потребители на мрежата. След това тази електронна поща може да бъде свалена от софтуер за мейл клиент на отделните машини на потребителите. Примери за мейл сървъри са Microsoft Exchange за Windows мрежи и sendmail – популярен демон за поща в UNIX.

ЗАБЕЛЕЖКА В терминологията на UNIX, *демонът (daemon)* е програма, която се изпълнява непрекъснато и управлява периодични заявки за дадена услуга.

- Сървърите за отдалечен достъп позволяват установяване на dial-up връзки, с помощта на които други компютри могат да осъществяват достъп до сървъра или до цялата мрежа от отдалечено местоположение по телефонна линия.
- Терминалните сървъри изпълняват софтуер, който позволява клиентски приложения да бъдат изпълнявани на сървъра, така че „тънките клиенти“ (маломощни, евтини системи) да могат да функционират като терминали, вместо като независими системи. Сървърът осигурява многосесийна среда и изпълнява приложните програми, които се използват на клиентските машини.
- Сървърите за телефония осигуряват услуги за телефонен секретар и гласова поща, а също и маршрутизиране на разговори.
- Клъстерните сървъри изпълняват софтуер, който позволява множество сървъри да бъдат свързвани в *клъстери (clusters)*, представляващи групи от независими компютърни системи, познати също като *възли (nodes)*. Те работят заедно като една система, за да осигурят непрекъснат достъп на клиентите до критично важни приложения и ресурси.

- Прокси сървърите действат като посредници между потребителите с работни станции и Интернет, за да осигурят сигурност и да предоставят услуги за административен контрол и кеширане на Интернет съдържание.
- Факс сървърите осигуряват централна точка в мрежата за изпращане и получаване на факсове и за разпределяне на входящите факсове до съответните потребители.
- BOOTP сървърите използват bootstrap протокол (протокол за първоначално зареждане), давайки възможност на клиентските компютри да стартират операционната система и да получават IP конфигурационна информация по мрежата.
- DHCP сървърите назначават IP адреси и TCP/IP конфигурационна информация на компютри, конфигурирани като DHCP клиенти, така че администраторите не е нужно ръчно да задават уникален IP адрес на всяка клиентска машина по мрежата.
- Сървърите за преобразуване на имена (name resolution) осигуряват асоцииране на дружелюбни мрежови имена, които позволяват на потребителите да идентифицират компютри без необходимостта да помнят цифрови идентификатори. Тези имена се асоциират с IP адресите, използвани от комплекта протоколи TCP/IP, за откриване на компютрите по мрежата. Сървърите за преобразуване на имена включват *DNS (Domain Name System) сървърите*, които асоциират йерархично структурирани имена на хостове с IP адреси, и *NetBIOS Name сървъри* (като WINS сървъра на Microsoft), които асоциират прости NetBIOS имена с IP адреси.

ЗАБЕЛЕЖКА Услугите BOOTP, DHCP и преобразуването на имена ще разгледаме по-детайлно в Глава 8, „Мрежови протоколи и услуги“, в секцията „Комплектът TCP/IP“.

Клиенти, работни станции, хостове и възли

Както научихте, клиентът в мрежата представлява компютър или друго мрежово устройство, отправящо заявки за достъп до мрежови ресурси. Клиентът обикновено, но не винаги, е компютър. Обърнете внимание, че принтер или друго мрежово устройство, което може да изисква ресурси, технически също е клиент.

С термина *клиент* могат също да се означават софтуерни програми, осъществяващи достъп до сървърни програми. Например програмата за електронна поща, която се изпълнява на екрана на вашия компютър и която изпраща заявка за сваляне на вашите нови съобщения от сървърен компютър, изпълняващ сървърен софтуер за електронна поща, се нарича *мейл клиент* (*mail client*).

Клиентска операционна система се инсталира най-често на настолните компютри, т.е. *работните станции*, които са свързани в мрежа като равноправни членове на работна група или се логват чрез сървър за автентикация при влизане, за да осъществят достъп до мрежата. Примерите на клиентски операционни системи са Windows 95/98 и Windows NT Workstation.

Терминът *работна станция* се използва по много начини. Той означава клиентската операционната система NT, а понякога се използва и за означаване на настолен компютър, работещ под произволна клиентска операционна система.

Терминът *работна станция* има и второ значение: мощен компютър, използван за изпълнение на приложен софтуер, който интензивно използва ресурси. Такива компютри са графичните работни станции или работните станции за проектиране с помощта на компютър (CAD станциите).

Друг термин, който чувате, е, че някои от компютрите в мрежата са *хостове*. Този термин често се използва за означаване на мрежи, базирани на TCP/IP, и може да включва всяко мрежово устройство, на което е зададен IP адрес.

ЗАБЕЛЕЖКА Когато се използва като глагол, *хостването* най-общо означава осигуряване на услуга на друго устройство или компютър. Например Web сървърът хоства Web страниците на потребителите.

Възелът представлява точка на свързване към мрежата. В някои случаи думата означава всеки компютър или друго мрежово устройство. В други случаи тя индицира точката на преразпределяне, или устройство, което е програмирано или конструирано да разпознава и обработва предавания към други възли.

Характеристики на равноправните мрежи

Структурата на равноправните мрежи (peer to peer) е подходяща за малки мрежи, където не се изисква стриктна сигурност. Повечето книги за мрежи препоръчват максимум десет компютъра за този тип модел на администриране.

Реализирането на малка равноправна мрежа не е скъпо и е относително лесно с помощта на модерни операционни системи като Windows 95/98, NT Workstation, Windows 2000 и различни версии на Linux, които имат вградени мрежови компоненти.

Ако искате да участвате в равноправна мрежа, трябва да конфигурирате компютъра за присъединяване към *работна група*. Това става чрез настройка на свойствата за работа в мрежа (networking properties) в Windows 9x, Windows NT и Windows 2000. Всички компютри, които споделят един с друг ресурси, в това поле трябва да имат въведено едно и също име на работна група.

Администриране на равноправни мрежи

Администрирането на потребители и ресурси в равноправните мрежи е *децентрализирано*. Всеки компютър в мрежата може да действа и като клиент, и като сървър; т.е. всеки компютър може да споделя собствени ресурси с останалата мрежа и да осъществява достъп до ресурсите на другите.

Потребителят на всеки компютър отговаря за администрирането на ресурсите на своя компютър (създаване на потребителски акаунти, създаване на споделени ресурси и задаването на позволения за достъп до тези ресурси). Всеки потребител отговаря също за архивирането на данните на своя компютър. За нещастие, откриването на търсен ресурс може да бъде трудно в равноправна мрежа, в която има повече от няколко компютъра.

Сигурност в равноправните мрежи

Равноправната мрежа няма централна база данни, където се пази информация за потребителските акаунти. Цялата сигурност е локална. Потребителските акаунти и пароли трябва да бъдат създавани и поддържани на всяка отделна

машина. Това е хем неудобно, хем значително по-несигурно в сравнение с централизирания модел на сигурността, използван в мрежите клиент/сървър.

Да разгледаме например работна група, състояща се от четири машини с NT Workstation, принадлежащи на Мери, Джо, Джон и Дейн. За да може Мери да осъществява достъп до файловете, съхранени на машината на Джо, Джо трябва да създаде потребителски акаунт за нейния компютър. Ако тя иска достъп и до споделения принтер, свързан към компютъра на Джейн, Джейн трябва да създаде потребителски акаунт за Мери, и т.н.

Ако Джо, Джейн и Джон зададат различни потребителски имена и пароли на тези акаунти, Мери може да се окаже в положението задължително да помни името *maryjohnson* и паролата *tree*, когато осъществява достъп до ресурси на машината на Джо, потребителското име *maryj* и паролата Shelton, когато осъществява достъп до ресурси, разположени на компютъра на Джон. Можете да си представите колко неуправляеми могат да станат всичките тези акаунти с нарастването на мрежата.

Сигурност на ниво споделен ресурс, сравнена със сигурност на ниво потребител

В Windows for Workgroups или в работна група на Windows 95/98, сигурността се реализира на *ниво споделен ресурс*, вместо на *ниво потребител*. Таблица 2-2 очертава разликите между сигурността на ниво споделен ресурс и на ниво потребител.

Таблица 2-2 *Характеристики на сигурността на ниво споделен ресурс и на ниво потребител*

Сигурност на ниво споделен ресурс	Сигурност на ниво потребител
Използва се от Windows for Workgroups 3.11, Windows 95 и Windows 98.	Използва се от Windows NT и Windows 2000.
На всеки споделен ресурс се задава парола.	Парола се задава за всеки отделен потребител.
За достъп до ресурс по мрежата потребителят трябва да въведе паролата за този ресурс.	За да осъществи достъп до ресурс по мрежата, потребителският акаунт трябва да има зададени позволения за достъп до този ресурс.
Потребителите трябва да помнят множество пароли.	Потребителите трябва да помнят само една парола.

В нашия предишен пример за малка работна група, ако Мери, Джо, Джейн и Джон изпълняват на своите компютри Windows 95, те не трябва да създават потребителски акаунти за всяко лице, което ще осъществява достъп до техните ресурси. Вместо това те задават парола на всеки споделен ресурс. Това означава, че ако Мери иска Джейн да има достъп до папката Documents, но не иска Джо или Джон да има достъп до тази папка, тя трябва да зададе парола за папката (например „health“) и да каже паролата само на Джейн. Когато Джейн се опита да осъществи достъп до папката, ще ѝ бъде изведена покана за въвеждане на парола.

Ако Мери има друга папка с име Pix, която тя иска да предостави за достъп на Джон и Джейн, но не на Джо, тя трябва да зададе на тази папка различна парола (да кажем, „crate“) и да даде тази парола само на Джон и Джейн.

Да предположим, че Мери има 20 споделени папки на нейния твърд диск. Тя трябва да запомни 20 различни пароли, които разрешават достъп до тези папки, а другите потребители трябва да запомнят множество пароли *и* да следят коя парола на коя папка отговаря. (А си мислехте, че сценарият с множество потребителски акаунти на NT workgroup е лош!) Фигура 2-7 илюстрира тази ситуация.

Фигура 2-7 *При сигурност на ниво споделен ресурс броят на паролите, които трябва да бъдат запомняни, може бързо да излезе от контрол.*

Тъй като тази ситуация става нетърпима с разрастване на мрежата, повечето потребители в работни групи с Windows 9x скоро започват да се обръщат към по-простото решение – не реализират никаква сигурност на ресурсите. Очевидно е, че оставянето на ресурсите без сигурност не е подходящо за мрежова среда, съдържаща поверителни данни, достъпът до които трябва да бъде ограничен. По-добре е да се използва сървърно-базирана технология, както е описано в следващата секция.

Характеристики на мрежите, базирани на сървъри

Определящата характеристика на сървърно-базираната мрежа (наричана още мрежа клиент/сървър) е *централизираното управление*. В такава мрежа поне една от машините работи под мрежова операционна система, като например Windows NT, Windows 2000 Server или NetWare. Потребителските акаунти се създават на сървъра, а мрежовият администратор може да контролира цялата мрежа от това централно местоположение.

Изграждането на сървърно-базирана мрежа решава проблема със снижаването на производителността, настъпващо с компютрите от работната група, когато други потребители осъществяват достъп до системен ресурс в същото време, когато потребителят работи на станцията, на която се намира този ресурс. Като цяло производителността и скоростта са по-добри в мрежите, базирани на сървъри.

Сървърните операционни системи по принцип осигуряват допълнителни интелигентни услуги. Например Windows NT/2000 сървър може да функционира като сървър за отдалечен достъп (dial-up) сървър, към който множество потребители могат да се свързват по телефонни линии. Обърнете внимание, че Windows 9x и NT Workstation позволяват само една входяща връзка в даден момент. Сървърът притежава също други вградени услуги, като възможността да осигурява услуги за преобразуване на имена, да назначава IP адреси като DHCP

сървър и да хоства Web сайтове с помощта на добавен или вграден софтуер за Web сървър.

Администриране в сървърно-базирани мрежи

Моделът на организиране на мрежи, базирани на сървър, опростява администрирането, особено за мрежи с много компютри и голям брой споделени ресурси. Споделените файлове се съхраняват на сървъра, така че да могат лесно да бъдат откривани и архивирани.

Една важна характеристика на компютърната обработка, базирана на сървър, която може да бъде окачествена или като недостатък, или като предимство, е необходимостта от специално назначен професионален мрежов администратор. Макар че това може да повиши цената на поддръжката на мрежата, упражняването на контрол върху всички мрежови операции от обучен администратор, вместо задължаването на крайните потребители да управляват техните собствени ресурси, може реално да намали общите разходи в един по-дългосрочен период от време.

Сигурност в сървърно-базираните мрежи

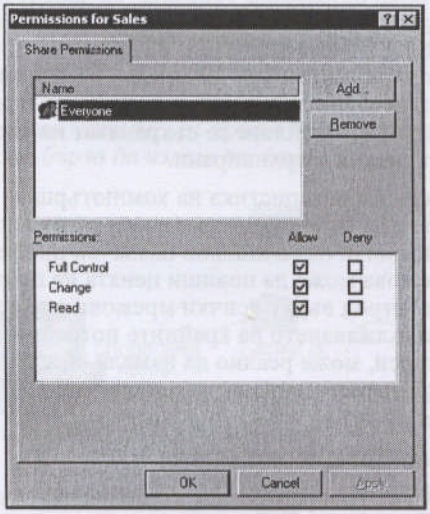
Сигурността, базирана на сървър, е значително по-добра от тази при равноправните мрежи. За да влезе в мрежата, всеки потребител трябва да има валиден потребителски акаунт и парола, създадени на сървъра. Това позволява достъп до ресурси по мрежата и не съществува необходимостта от множество потребителски акаунти на различни машини, както в случая с работната група с NT Workstation. Също така няма нужда от запомняне на пароли за различните споделени ресурси, както в случая с работните групи в Windows 9x, защото за осъществяване на контрол на достъпа сървърно-базираните мрежи разчитат на *автентикация* (*authentication*) и *позволения* (*permissions*) на потребителите.

Мрежовият администратор може да зададе позволения за всеки споделен ресурс на отделни потребители или групи. Тези позволения могат да дадат възможност за задаване на различни нива на достъп за различни потребители. Например да кажем, че имаме споделена папка на сървъра, наречена Sales (продажби). Искаме Мери, която е секретарка в отдел Продажби, да има възможност да чете документите в папката, но да не може да прави промени в тях. Искаме Джейн, която е заместник-началник на отдел Продажби, да може да чете, променя, изтрива и изобщо да има пълен контрол върху документите в папката Sales. За да постигнем това в мрежа с Windows 2000, можем да редактираме свойствата на споделянето и да зададем позволения за четене на потребителския акаунт на Мери и позволения за пълен контрол на потребителския акаунт на Джейн.

ЗАБЕЛЕЖКА По-добър начин за управление на позволенията, вместо задаването им за отделни потребителски акаунти, е организирането на потребителските акаунти в *групи на сигурност (security groups)* и задаване на позволения за групите. Използването на групи ще разгледаме по-детайлно в Глава 10, „Мрежови операционни системи“, в секцията „Общо администриране на мрежите“.

Когато задаваме позволения за папката Sales на Мери и Джейн (или на групите, към които те принадлежат), трябва да премахнем подразбиращото се позволение за споделения ресурс, както е показано на Фигура 2-8.

Фигура 2-8 *В Windows мрежите подразбиращото се позволение за споделен ресурс дава пълен контрол (Full Control) за всеки (Everyone).*



Както виждате на Фигура 2-8, когато създавате нов споделен ресурс, на групата Everyone автоматично се задава Full Control. Тази група включва всички потребители, които имат валиден акаунт за логване в мрежата. За щастие, можете лесно да изтриете това позволение, за да ограничите достъпа само до тези, които наистина трябва да го притежават.

ЗАБЕЛЕЖКА Това е опростено обяснение за илюстриране на разликата между позволения за споделяне, базирани на сървър, и такива, базирани на работна група. Windows 2000 може да реализира няколко различни слоя на сигурност в зависимост от използваните файлова система и протоколи. Позволенията, зададени за споделения ресурс, са само една от ключалките на вратата към него.

Категоризация на мрежите по мрежова операционна система

Понякога мрежите се категоризират на базата на мрежовата операционна система, инсталирана на сървърите и използвана за управление на мрежата. Ето няколко примера на типове мрежи, базирани на сървърна операционна система:

- Windows (Windows NT и Windows 2000)
- NetWare
- UNIX

Много мрежи комбинират два или повече типа сървъри в мрежата, затова често биват означавани като *хибридни мрежи*.

Windows мрежи

Windows мрежите, базирани на сървър, се наричат *домейни*. В домейните на Windows NT 4.0 един главен компютър, наречен *главен домейн контролер* (*primary domain controller*), съхранява единственото копие за четене/запис на базата данни за управление на акаунтите за сигурност (SAM). От издаването на Windows 2000, Microsoft означава NT 4.0 домейните като *домейни от ниско ниво* (*downlevel domains*).

Windows 2000 домейните са базирани на Active Directory, копие на която се съхранява на всеки домейн контролер и която съдържа информация за акаунтите за сигурност и обекти, представящи мрежови ресурси. Дадена мрежа може да има множество домейн контролери; всеки от тях чете и записва в базата данни на директорията.

Windows 2000 Professional, Windows NT Workstation, Windows 95 и 98, Window for Workgroups и MS-DOS могат да бъдат клиенти както на Windows NT сървъри, така и на Windows 2000 сървъри. Операционни системи, които не са произведени от Microsoft, като Macintosh и Linux, също могат да осъществяват достъп до ресурси на Windows сървъри при инсталиран подходящ допълнителен софтуер.

ЗАБЕЛЕЖКА Всички популярни мрежови операционни системи са разгледани детайлно в Глава 10.

NetWare мрежи

Novell NetWare е популярна мрежова операционна система, която осигурява сигурност при влизане и такива функции, като файлов сървър и принт сървър. Настолните (клиентските) операционни системи от фамилията Windows могат да осъществяват достъп до NetWare сървъри, ако имат инсталиран подходящ клиентски софтуер. Windows 9x, NT и 2000 включват клиентски услуги за NetWare. Също така Novell създава допълнителна клиентска програма – Client32, която може да бъде инсталирана на 32-битова операционна система Windows за осигуряване на по-голяма функционалност.

Версии 4.x и 5.x на NetWare осигуряват директорийни услуги с помощта на NetWare Directory Services (NDS) – йерархична база данни, подобна на (предхождаща и вероятно вдъхновила) Active Directory на Microsoft. По-старите версии на NetWare (3.x и по-късни) все още са в употреба; те използват база данни, наречена Bindery, която служи за организиране на мрежовите обекти.

UNIX мрежи

UNIX беше мрежовата операционна система, използвана от повечето хостове на ARPAnet – предшественикът на Интернет. UNIX е разработен от Bell Labs през 1969 г. и е разпространен в много разновидности поради неговата структура с отворен код. Той е мощна мрежова операционна система, но повечето UNIX реализации са текстово базирани и са относително трудни за изучаване.

Linux е вариант на UNIX, който отскоро стана популярен както като сървър, така и като настолна операционна система. Подобно на неговия по-стар брат UNIX, Linux представлява отворен стандарт и множество различни компании предлагат на пазара техни собствени версии. Популярни версии са RedHat, Caldera и Corel.

Хибридни мрежи

Повечето съвременни средни и големи мрежи могат да бъдат считани за хибридни. Те работят със софтуер, разработен от различни производители, използват множество протоколи и дори могат да комбинират концепциите на домейн и работна група.

Microsoft мрежа, в която клиентите влизат в Windows NT домейн контролер, може да има също NetWare файлов сървър, до който същите тези клиент имат достъп, както и UNIX машина, която се използва за осигуряване на услуги за Web хостинг. Персоналните компютри могат да се свързват дори към мейнфрейм компютър IBM AS/400, за да осъществяват достъп до определени приложения и записи.

Повечето производители предоставят инструменти за софтуерна интероперативност (взаимодействие между различни видове софтуер), които или се включват в операционната система, или са достъпни като допълнителни модули (add-ons); тези инструменти са предназначени за улесняване на интеграцията в подобна среда със софтуер от множество производители. Например продуктите Windows NT и 2000 Server на Microsoft включват услугите Gateway Services for NetWare и Services for Macintosh.

Ето някои популярни програми за интероперативност:

- **Client Services for NetWare (CSNW) и Gateway Services for NetWare (GSNW)** – CSNW позволява отделни клиентски компютри със софтуер на Microsoft да осъществяват директен достъп до NetWare сървъри. GSNW позволява на клиенти на Microsoft сървъри да осъществяват достъп до ресурси на NetWare сървъри чрез преминаване през шлюзов (gateway) софтуер, инсталиран на NT сървъра или на Windows 2000 сървър.
- **File and print services for NetWare** – Позволява на клиенти на NetWare сървър достъп до ресурси на Windows сървър.
- **Services for Macintosh** – Позволява на Macintosh компютри да осъществяват достъп до файлове и принтери в Microsoft мрежа.
- **Systems Network Architecture (SNA)** – SNA позволява PC мрежи да бъдат свързвани към IBM мейнфрейм компютри.
- **SAMBA** – SAMBA представлява набор от помощни програми, позволяващи на Microsoft компютри да осъществяват достъп до файлови и принтерни услуги на UNIX сървъри.

Тези решения за интероперативност се разгледани по-детайлно в Глава 13, „Хибридни мрежи".

Категоризиране на мрежите по протокол

Понякога мрежите биват категоризирани в зависимост от протоколите, които използват за комуникация. Мрежовите протоколи представляват правилата, следвани от свързаните компютри при установяване и поддържане на комуникация по мрежата. Трите най-популярни LAN протокола са NetBEUI, IPX/SPX и TCP/IP – те са описани в следващите секции. Други LAN протоколи са AppleTalk и комплекта от OSI протоколи.

NetBEUI мрежи

Малка проста локална мрежа, използваща операционни системи на Microsoft, която може да комуникира с помощта на протокола NetBEUI. NetBEUI (съкращение от NetBIOS Extended User Interface) е базиран на протоколите NetBIOS (Network Basic Input/Output System), разработени от IBM за работни групи. Обърнете внимание, че NetBEUI мрежата не може да бъде маршрутизирана, защото самият протокол не може да бъде маршрутизиран. Това означава, че ако вашата мрежа е разделена на подмрежи, трябва да използвате различен LAN протокол, за да могат компютрите от една подмрежа да комуникират с компютрите в друга подмрежа.

Защо мрежите се разделят на подмрежи ще научите в Глава 8, в секцията „IP подмрежи и надмрежи". Предимствата на NetBEUI са неговата простота и малкото използвани ресурси. Той е бърз и не изисква конфигуриране на сложна информация при инсталиране.

IPX/SPX мрежи

Novell използва стека от протоколи Internet Package Exchange/Sequenced Packet Exchange (IPX/SPX) като свой протокол за локални мрежи, и затова той е задължителен при NetWare мрежи преди версия 5.0.

ЗАБЕЛЕЖКА NetWare, версия 5.0, е първата версия на NetWare, която поддържа изпълнението на „чист IP" (протоколът Internet Protocol от стека от протоколи TCP/IP) и не изисква IPX/SPX.

IPX/SPX обикновено се асоциира с NetWare мрежите, но не е ограничен само за тази цел. Работна група или домейн от Microsoft компютри също могат да използват протокола IPX/SPX. Microsoft включва своя собствена реализация на IPX/SPX-съвместими протоколи, наречени NWLink, в операционните системи Windows 9.x, NT и 2000. Microsoft клиентът трябва да има инсталиран NWLink или IPX/SPX, за да може да се свързва към NetWare сървър, работещ с NetWare 4.x или по-стара версия.

IPX/SPX изисква минимално конфигуриране (повече от NetBEUI, но по-малко от TCP/IP) и предлага по-висока производителност от TCP/IP. IPX/SPX понякога се използва на вътрешни Microsoft мрежи, свързани към Интернет, от съображения за сигурност. Тази опция ще разгледаме подробно в Глава 13, в секцията „Аспекти на сигурността при използване на множество протоколи".

TCP/IP мрежи

Независимо от факта, че е най-бавният и най-труден за конфигуриране от популярните LAN протоколи, TCP/IP е най-широко използваният. За това има няколко основни причини:

- TCP/IP използва гъвкава схема на адресиране, която е изключително подходяща за маршрутизиране дори при най-големите мрежи.
- Почти всички операционни системи и платформи могат да използват TCP/IP.

- Достъпни са огромен брой помощни програми и инструменти, някои от които са включени в комплекта от протоколи, а други са допълнително добавяни програми за наблюдение и управление на TCP/IP.
- TCP/IP е протоколът на глобалния Интернет. За да се свърже към Интернет, дадена системата трябва да работи с TCP/IP.

Повечето корпоративни мрежи изпълняват TCP/IP и затова е много важно мрежовите администратори да бъдат запознати с неговите протоколи. Отделните компоненти на комплекта TCP/IP ще разгледаме в Глава 8.

Други LAN протоколи, използвани в мрежи

Повечето локални мрежи използват един от трите описани по-горе протокола, но при изучаването на компютърните мрежи можете да срещнете и няколко други протокола или комплекти от протоколи.

AppleTalk

AppleTalk представлява набор от протоколи, разработени от Apple за организиране на мрежи с техните машини Macintosh. Комплектът AppleTalk включва следните протоколи:

- **LocalTalk** – Използван за свързване на Macintosh компютри в малки работни групи. Той е относително бавен (230,4 kbps) и поддържа само 32 устройства.
- **EtherTalk** – Използва се за свързване на Macintosh работни групи към Ethernet мрежи.
- **TokenTalk** – Използва се за свързване на Macintosh работни групи към Token Ring мрежи.

AppleTalk мрежите използват протокола AppleTalk Address Resolution Protocol (AARP) за асоцииране на AppleTalk адреси с физически MAC (Media Access Control) адреси от Ethernet и Token Ring.

Комплектът от протоколи OSI

Комплектът от протоколи Open System Interconnection (OSI) беше предназначен да замени TCP/IP, който се очакваше да слезе от сцената. Комплектът OSI беше разработен от организацията International Organization for Standardization (ISO), за да осигури подобрен набор от протоколи с цел по-малко объркване и по-лесна стандартизация на мрежовите продукти между множеството производители.

ЗАБЕЛЕЖКА Организацията International Organization for Standardization се нарича също ISO. Не, това не е типографска грешка – „ISO“ не е акроним, а дума, произлизаща от гръцкото „isos“, което означава „равно“.

Прекратяването на използването на TCP/IP и използването на OSI на негово място звучи добре на теория, но TCP/IP се оказа малко по-труден за убиване, отколкото се предполагаше. Американското правителство застана зад комплекта OSI и в края на 80-те години Министерството на отбраната издаде декрет, според който от м. август 1990 г. всички негови компютърни комуникации

трябва да използват OSI протоколи. Но това не се случи. Мрежите не направиха промяната, а TCP/IP все още остава кралят на Интернет. Неговата позиция изглежда силна, особено с неговата способност да се развива (демонстрирана от планирания преход към IPv6), за да отговори на предизвикателствата на бъдещото развитие.

Категоризиране на мрежите по топология

В някои случаи мрежите биват категоризирани на базата на физическата или логическата *топология* на мрежата. *Физическата топология* означава формата на мрежата – начинът, по който се разполага кабелът. *Логическата топология* означава пътя, по който пътуват сигналите от една точка на мрежата до друга.

Физическата и логическата топология може да бъде една и съща; в мрежа, физически оформена като линейна шина (т.е. в права линия), данните пътуват в права линия от един компютър към следващия. Мрежата може да има също различна физическа и логическа топология. Кабелните сегменти могат да свързват всички компютри към централен хъб във формата на звезда, но вътре в хъба връзките да бъдат свързвани така, че сигналът да пътува в окръжност от един порт към следващия, създавайки логически кръг.

Ето най-популярните LAN топологии за мрежи:

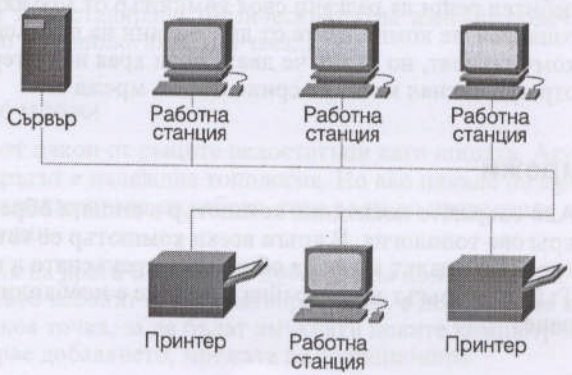
- Линейна шина
- Кръг
- Звезда
- Решетка
- Хибридна

Те са описани по-детайлно в следващите секции.

Мрежи с линейна шина

Както показва самото име, линейната шина (понякога наричана просто *шина*) представлява мрежа, която е разположена в права линия. Реално линията не е задължително да бъде права; просто кабелът преминава от един компютър към следващия, след това към следващия и т. н. Фигура 2-9 илюстрира линейна шина.

Фигура 2-9 *Компютрите в мрежа с линейна шинна топология се свързват в една линия един след друг.*



Тъй като има начало и край, мрежата с линейна шинна топология изисква *терминиране* на всеки край. Ако не бъдат терминирани и двата края на кабела, възниква *отразен сигнал*, който може да наруши или да прекъсне комуникациите по мрежата. Единият от краищата на линейната шина – но *не и двата* – трябва да бъде заземен.

ЗАБЕЛЕЖКА Към края на шината, на първия и последния компютър, свързани към линейния кабел, към „празната" страна на Т-конектора на мрежовата интерфейсна карта се свързва устройство, наречено терминатор.

Шинните мрежи обикновено използват дебел или тънък коаксиален кабел и архитектура Ethernet 10Base2 или 10Base5. Повече за характеристиките на различните типове кабели ще научите в Глава 7, „Физически компоненти на мрежата".

Комуникации по шинна мрежа

По шинна мрежа, когато един компютър изпрати съобщение, това съобщение отива до всеки компютър в мрежата. Всяка мрежова интерфейсна карта (NIC) проверява хедъра на съобщението, за да определи дали то е адресирано за този компютър. Ако не е, съобщението бива игнорирано.

Предимства на шинните мрежи

Шинната топология е много проста и лесна за инсталиране. Тя е относително евтина и използва по-малко кабел в сравнение с други топологии. Шината е особено подходяща за малки, временни мрежи, например такива в класни стаи, които може да бъдат използвани само няколко дни или седмици.

Недостатъци на шинните мрежи

Шината е известна като пасивна топология, защото компютрите не регенерират сигнала и не го предават нататък, както правят това в кръга. Това прави мрежата уязвима към *затихване* (*attenuation*), представляващо загуба на силата на сигнала с увеличаване на разстоянието. За решаване на този проблем могат да бъдат използвани повторители. Повторителите ще разгледаме по-детайлно в Глава 7.

Друг недостатък на шината е, че при прекъсване на кабела (или ако някой потребител реши да разкачи своя компютър от мрежата) линията се прекъсва. Това означава, че компютрите от двете стани на прекъсването не само не могат да комуникират, но също, че двата нови края не са терминирани и резултатният отразен сигнал може да срине цялата мрежа

Кръгови мрежи

Ако свържете последния компютър в шината обратно към първия, получавате кръгова топология. В кръга всеки компютър се свързва към два други компютъра, а сигналът може да обикаля непрекъснато в кръга (вижте Фигура 2-l0). Тъй като кръгът няма крайна точка, не е необходимо (или възможно) терминиране.

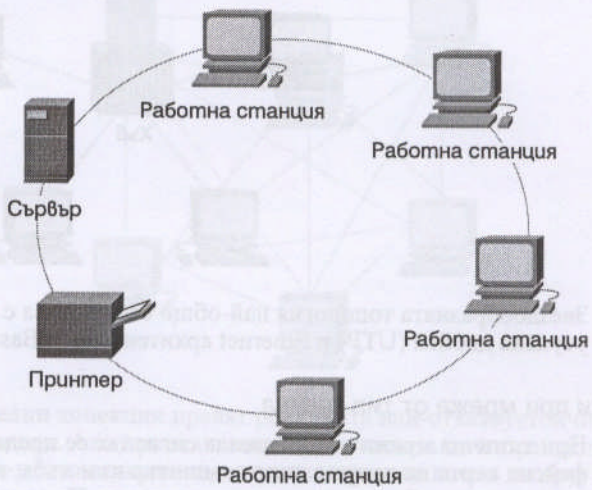
За изграждане на мрежа с физически кръг най-общо се използва коаксиален кабел, както при шината. Мрежата Token Ring, която представлява логически кръг, използва STP кабел (тип IBM) и отговаря на спецификациите IEEE 802.5.

Комуникации по кръгова мрежа

По кръгова мрежа сигналът пътува в една посока. Всеки компютър приема сигнала от своя *възходящ съсед* (*upstream neighbor*) и го изпраща на своя *низходящ съсед* (*downstream neighbor*). Кръгът се счита за *активна топология*, защото всеки компютър регенерира сигнала, преди да го предаде към следващия.

Кръговата топология най-често се асоциира с архитектурата Token Ring. В тази реализация кръгът най-общо е *логически* – като окръжността се свързва вътре в Token Ring хъб, който се нарича модул за достъп до множество станции (multistation access unit – MSAU).

Фигура 2-10 *В кръгова мрежа компютрите се свързват към кръг, като последният компютър се свързва обратно към първия.*



Предимства на кръговите мрежи

Кръгът е сравнително лесен за отстраняване на неизправности и подобно на шината е прост за инсталиране. Физическият кръг изисква повече кабел от шината и по-малко от топологията тип звезда.

Недостатъци на кръговите мрежи

Кръгът страда от някои от същите недостатъци като шината. Ако се запази непрекъснат, кръгът е надеждна топология. Но ако някъде по мрежата възникне прекъсване или изключване от кабела, това води до прекъсване на всички мрежови комуникации.

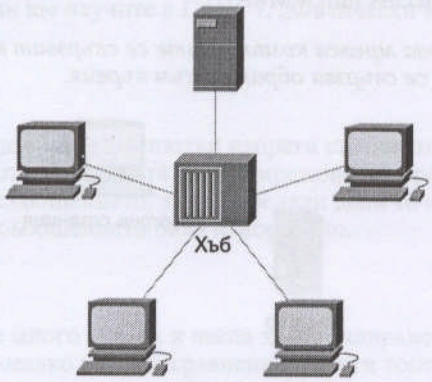
Друг недостатък на кръга е трудното добавяне на допълнителни компютри към мрежата. Тъй като кабелът описва затворен кръг, е необходимо кръгът да бъде прекъснат в някоя точка, за да бъдат вмъкнати новите компютри. Това означава, че докато трае добавянето, мрежата не функционира.

Мрежи от тип звезда

Звездата (*star*) е една от най-популярните LAN топологии. Тя се реализира чрез свързване на всеки компютър към централен хъб, както е показано на Фигура 2-11.

Хъбът може да бъде *активен*, *пасивен* или *интелигентен*. Пасивният хъб е просто точка на свързване. Той не изисква електрическо захранване. Активният хъб (най-разпространеният тип) реално представлява *повторител* с множество портове; той усилва сигнала, преди да го предаде към другите компютри. Интелигентният хъб представлява активен хъб с диагностични възможности. Той има вграден процесорен чип. Хъбовете ще разгледаме по-подробно в Глава 7.

Фигура 2-11 *Топологията тип звезда свързва всички компютри към един централен хъб.*



Звездообразната топология най-общо се използва с кабел тип неекранирана усукана двойка (UTP) и Ethernet архитектура 10BaseT или 100BaseT.

Комуникации при мрежа от тип звезда

При типична мрежа от тип звезда сигналът се предава от мрежовата интерфейсна карта на изпращащия компютър към хъба, повишава се (т.е. усилва се) и се изпраща обратно през всички портове. При звездата, подобно на шината, всички компютри приемат съобщението, но само компютърът, чийто адрес отговаря на адреса на местоназначението в хедъра на съобщението, му обръща внимание.

Предимства на мрежите от тип звезда

Топологията тип звезда има две големи предимства пред шината и кръга. Първо, тя е много *по-отказоустойчива* (*fault tolerant*); т.е. ако един компютър бъде изключен или неговият кабел бъде прекъснат, само *този* компютър бива засегнат, а останалата част от мрежата може да продължи да комуникира нормално. Второ, тя предлага възможност за лесно преконфигуриране. Добавянето на още компютри към мрежата или премахването на компютри е много просто, защото се състои само във включване или изключване на техния кабел в хъба. Отстраняването на проблеми на физическия слой в мрежата от тип звезда също е лесно, особено при наличие на интелигентен хъб, който осигурява диагностична информация. Повече за физическия слой и за другите слоеве, дефинирани от стандартните мрежови модели, ще научите в Глава 3, „Мрежови концепции, модели и стандарти“.

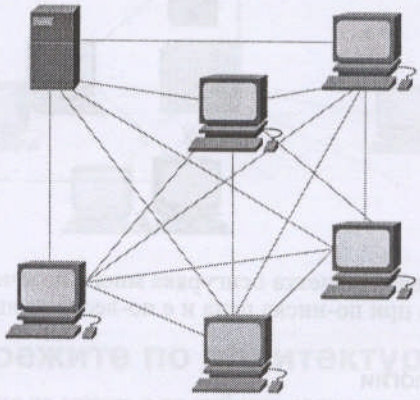
Недостатъци на мрежите от тип звезда

Независимо от предимствата на звездата, тя има и няколко недостатъка, свързани главно с нейната цена. Първо, тя използва повече кабел, отколкото линейната шина или кръга, защото трябва да има отделен кабел от хъба до всеки компютър. Друг източник на допълнително оскъпяване е самият хъб, който трябва да бъде закупен наред с кабела. Все пак малък плюс при мрежите от тип звезда е, че UTP кабелът е сравнително евтин и няма нужда от терминатори.

Решетъчни мрежи

Решетката (*mesh*) представлява топология, която не може да видите толкова често, колкото трите топологии, разгледани дотук. В решетъчната мрежа всеки компютър има директна връзка към всеки друг компютър в мрежата, както е показано на Фигура 2-12.

Фигура 2-12 *В решетъчната мрежа всеки компютър е свързан към всеки друг компютър.*



Тези допълнителни конекции правят решетката най-отказоустойчива от всички останали топологии. Ако пропадне един от пътищата от изпращащия компютър към компютъра-местоназначение, сигналът може да поеме по друг път.

За нещастие, това предимство става за сметка на високата цена и огромното количество кабел, необходим за реализиране на решетка и сложността на мрежата, ако в нея влизат повече от няколко компютъра. Броят на конекциите нараства експоненциално при добавяне на всеки нов компютър. Не е случайно, че „mesh“ (решетка) звучи подобно на „mess“ (бъркотия) – точно това получавате при нарастването на решетъчната мрежа.

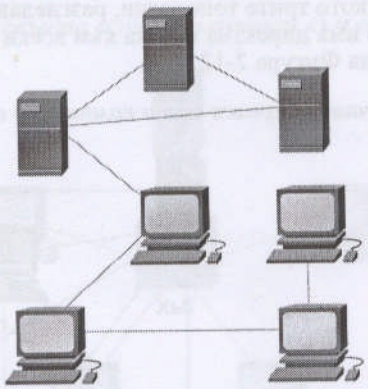
Хибридни топологии

Думата *хибрид* се използва в два различни смисъла за означаване на мрежова топология. В Глава 13 ще обясним използването на термина *хибрид* за описание на мрежи, които работят с множество протоколи, операционни системи или компютърни платформи. В тази глава думата се използва за означаване на топология, която комбинира елементи на две или повече стандартни топологии (например хибридна решетка, звезда или кръг).

Хибридни решетъчни мрежи

Тъй като решетъчната топология бързо става сложна и неуправляема при нарастване, много мрежи се базират на полурешетъчна топология, при която има допълнителни връзки между някои от компютрите, но не между всички; този тип мрежа често се означава като *хибридна решетка*. Допълнителните връзки трябва да бъдат създадени между компютрите, които имат най-голяма нужда от отказоустойчивост на връзката. Фигура 2-13 показва един пример на такава мрежа.

Фигура 2-13 *В хибридната решетка се осигуряват допълнителни връзки между някои компютри, но не между всички.*



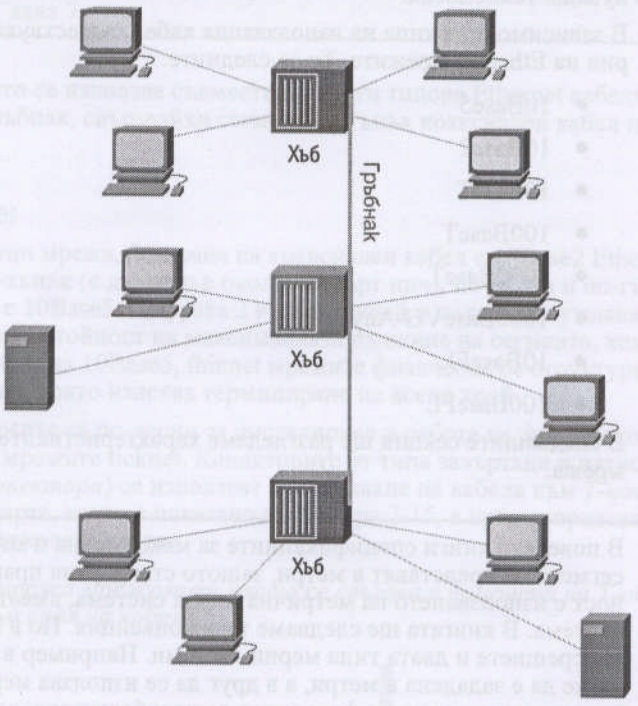
Хибридната решетка осигурява много повече предимства от обикновената решетката при по-ниска цена и е по-лесна за инсталиране и управление.

Комбинирани топологии

Терминът *хибриден* се използва и за означаване на мрежи, които използват множество топологии. Много мрежи комбинират една или няколко топологии. Например може да имате няколко хъба, към всеки от които има компютри, свързани в топология от тип звезда, а след това хъбовете да бъдат свързани в линейна шина. За тази цел много хъбове имат BNC конектор за тънък коаксиален кабел заедно с няколко RJ45 порта за UTP връзки.

В този тип свързване (вижте Фигура 2-14) коаксиалният кабел, свързващ хъбовете, се нарича *гръбнак* (*backbone*). Гръбнакът е част от мрежата, свързваща всички по-малки части, наричани още (*сегменти*). Няколко сегмента могат да бъдат свързани към един гръбнак за създаване на по-голяма мрежа.

Фигура 2-14 *Коаксиалният кабел, свързващ хъбовете, се нарича гръбнак на мрежата.*



Категоризация на мрежите по архитектура

Друг начин за описание на мрежа е по нейната архитектура. Най-общо казано, *мрежовата архитектура* включва набор от спецификации, които отчитат нейната физическа и логическа топологии, типа на използвания кабел, ограниченията в разстоянията, методите за достъп до преносната среда, размера на пакетите и хедърите, и други фактори. Може да видите тези спецификации под името *протоколи на каналния слой*.

В момента най-популярните LAN архитектури са Ethernet и Token Ring. Други общоприети LAN архитектури са AppleTalk и ARCnet. Всички те са описани в следващите секции.

Ethernet мрежи

Ethernet мрежата е разработена през 60-те години и е усъвършенствана от Xerox, Digital и Intel за формиране на базата на спецификациите IEEE 802.3; днес тя е най-популярната мрежова архитектура. Ролята на спецификациите на IEEE ще разгледаме в Глава 3.

Ethernet мрежите се конфигурират като физическа шина или звезда и използват метод на достъп до преносната среда, наречен множествен достъп с разпознаване на носещата и откриване на колизии (CSMA/CD). Стандартният Ethernet е ограничен по скорост до 10 Mbps, но сега масово е разпространен *Fast Ethernet*, който работи на 100 Mbps. Съществува и *Gigabit Ethernet*, който има възмож-

ност за работа при скорост, надхвърляща 1 Gbps, и се очертава като нова и вълнуваща технология.

В зависимост от типа на използвания кабел съществуват различни подкатегории на Ethernet мрежите. Те са следните:

- 10Base5
- 10Base2
- 10BaseT
- 100BaseT
- 1000BaseT
- 1000BaseVG-AnyLAN
- 10BaseFL
- 100BaseFL

В следващите секции ще разгледаме характеристиките на всеки тип Ethernet мрежа.

ЗАБЕЛЕЖКА В повечето книги спецификациите за максимална и минимална дължина на сегмент се представят в метри, защото стандартна практика в научната общност е използването на метрична мерна система, вместо американската мерна система. В книгата ще следваме тази конвенция. Но в изпитите за сертификати ще срещнете и двата типа мерни системи. Например в един въпрос дължината може да е зададена в метри, а в друг да се използва мерна единица футове; затова е важно да знаете формулата за преобразуване: един метър е равен на 3,28 фута.

Мрежи 10Base5 Ethernet

Означавани като стандартен Ethernet, макар и вече не така популярни като някои от другите типове, мрежите 10Base5 използват дебел коаксиален кабел (с диаметър около половин инч) и се наричат също *Thicknet мрежи*. Дебелият коаксиален кабел се означава като RG-8 или RG-11.

Числото десет в 10Base5 означава максималната скорост по този тип мрежа:10 Mbps. Цифрата 5 означава максималната дължина на сегмента, която е 500 метра. Thicknet мрежите използват шинна топология.

Окабеляването на Thicknet е по-трудно в сравнение с другите Ethernet мрежи по две причини. Първо, кабелът не е толкова гъвкав поради по-големия диаметър. Второ, връзките се правят с помощта на устройство, наречено *вампирски зъб (vampire tap)*, който изисква да пробиете малък отвор в кабела, за да свържете конектора. Мрежите 10Base5 използват външни приемопредаватели (трансивъри). Приемопредавателят е устройство, което генерира и приема сигнали с данни; в други Ethernet архитектури приемопредавателят е вграден в мрежовата карта. Технологията 10Base5 използва DIX конектори с AUI кабел за свързване на приемопредавателя към мрежовата интерфейсна карта (NIC).

ЗАБЕЛЕЖКА Мрежовите интерфейсни карти и различните типове конектори ще разгледаме детайлно в Глава 7.

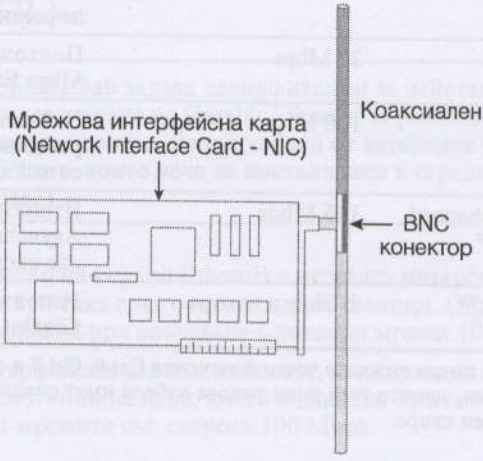
Thicknet често се използва съвместно с други типове Ethernet кабели за осигуряване на гръбнак, свързвайки сегменти с тънък коаксиален кабел или 10BaseT хъбове.

Мрежи 10Base2 Ethernet

Популярен тип мрежа, базирана на коаксиален кабел е 10Base2 Ethernet, която използва по-тънък (с диаметър около четвърт инч), по-евтин и по-гъвкав кабел, в сравнение с 10Base5. Цифрата 2 в този случай е малко заблуждаваща; реално тя е закръглена стойност на максималната дължина на сегмента, която е 185 метра. Подобно на 10Base5, thinnet мрежите физически се структурират като линейна шина, която изисква терминиране на всеки край.

10Base2 мрежите са по-лесни за инсталиране и работа на физическо ниво в сравнение с мрежите ticknet. Конекторите от типа завъртане и натискане (наречени *BNC конектори*) се използват за свързване на кабела към *Т-конектор* на мрежовата карта, както е показано на Фигура 2-15, а приемопредавателят е вграден в мрежовата карта.

Фигура 2-15 *При thinnet мрежа мрежовата карта се свързва с помощта на Т-образен BNC конектор към края на кабела.*



Тънкият коаксиален кабел за мрежа 10Bsse2 е 50-омов RG-58A/U или RG-58C/U. (Първият се използва най-често; вторият е военна спецификация.)

ПРЕДУПРЕЖДЕНИЕ Кабелът RG-58 е подобен по външен вид на RG-59, който се използва за инсталациите на кабелните телевизии, затова внимавайте да не объркате двата кабела. RG-59 е 75-омов кабел и не трябва да бъде използван за изграждане на компютърни мрежи. RG-58U е подобен тип кабел, който не отговаря на спецификациите на IEEE и трябва да бъде избягван.

Кабелът thinnet понякога се нарича Cheapernet, защото реализацията на окабеляването с този кабел струва по-малко, отколкото с дебел коаксиален кабел. Thinnet като цяло е по-скъп на линеен метър от UTP, но за коаксиална мрежа е необходим по-малко кабел поради шинната конфигурация.

Мрежи UTP Ethernet

Най-популярната преносна среда за новите LAN инсталации е кабелът UTP, който се използва в 10BaseT мрежи (T означава twisted – усукан). Повечето от нас вече познават кабелите с усукана двойка, които се използват за телефонната кабелна система.

UTP се произвежда в различни категории, идентифицирани с числа, които следват модела Cat 1, Cat2 и т. н. Таблица 2-3 показва UTP категориите, тяхното предназначение и характеристиките им.

Таблица 2-3 *Категории UTP кабел.*

UTP категория	Максимална скорост на предаване	Характеристики и предназначение
Cat 1	Само за глас	Използва се в стари телефонни инсталации
Cat 2	4 Mbps	Не се препоръчва за предаване на данни
Cat 3	16 Mbps	Най-ниската категория за предаване на данни; използва се най-вече за телефонно окабеляване
Cat 4	20 Mbps	Подходящ за изграждане на мрежи 10 Mbps Ethernet
Cat 5	100 Mbps – 1 Gbps	Най-популярната категория за изграждане на локални мрежи. Използва се за Fast Ethernet (100 Mbps)
Cat 5 Enhanced (Cat Se)*	155 Mbps	Използва се за Fast Ethernet и Asynchronous Transfer Mode (ATM) със скорост 155 Mbps
Cat 6 & 7*	1 Gbps и нагоре	Използва се за новите технологии Gigabit Ethernet

* Едва ли ще виждате често означения Cat 6, Cat 7 и enhanced Cat 5 в текстовете за мрежи, защото тези нови типове кабели имат спецификации, които бяха създадени съвсем скоро.

Както виждате, UTP поддържа по-високи скорости на предаване, отколкото коаксиалният кабел. Също така UTP е много гъвкав и лесен за инсталиране. Той използва RJ конектори, които са същите като модулния тип конектори, използвани за телефоните. Макар че телефонните кабели обикновено използват помалкия конектор RJ-11, повечето Ethernet кабели се свързват с малко по-големия конектор RJ-45.

В мрежа, базирана на UTP, всеки компютър има парче кабел, което го свързва към централен хъб в топология звезда. Различните типове хъбове ще разгледаме в Глава 7.

Мрежи 10BaseT

Спецификацията 10BaseT е популярна за локални мрежи от всички размери. Тя може да бъде изпълнена с кабел Cat 3, който е вече инсталиран в много сгради за целите на телефонните комуникации. Новите мрежи 10BaseT обикновено се изграждат с използване на кабел Cat 5 или 5e, така че по-късно лесно да могат да бъдат ъпгрейдвани до 100 Mbps.

Мрежи 100BaseT

Класификацията 100BaseT означава Ethernet мрежи, които работят на 100 Mbps по кабел Cat 5 или 5e. Тези мрежи използват същата топология и методи за достъп като 100BaseT. Всъщност единствените разлики са изискването за кабел от по-висока категория и фактът, че мрежовите карти и хъбове трябва да поддържат скорост на предаване 100 Mbps.

Много мрежови интерфейсни карти и хъбове се произвеждат за поддръжка на скорости на предаване както 10, така и 100 Mbps, което улеснява тяхното постепенно ъпгрейдване. Освен това при подходящи хардуер можете да работите по част от мрежата на 100 Mbps, а други части още да работят на 10 Mbps.

Мрежи 1000BaseT (Gigabit Ethernet)

Първоначалните стандарти за много високоскоростен Ethernet, наричан най-често Gigabit Ethernet, бяха създадени от IEEE през 1996 г. и публикувани като спецификации 802.3z. Тези стандарти осигуряват предаване със скорост 1000 Mbps (1 Gbps), с помощта на формата за фреймове 802.3 Ethernet и метода за достъп CSMA/CD.

ЗАБЕЛЕЖКА Стандартът IEEE 802.3ab задава спецификации за действието, тестването и изискванията за използване на Gigabit Ethernet за разстояния до 100 метра, с използване на четири двойки медни кабели от категория Cat 5. Това включва повечето от кабелите, които вече са инсталирани в сградите за мрежите 10BaseT и 100BaseT.

Голямо предимство на Gigabit Ethernet е неговата интероперативност и съвместимост в обратна посока с неговите предшественици. Gigabit Ethernet е отлична гръбначна технология при свързване с локални мрежи 10BaseT и 100BaseT.

Мрежовите интерфейсни карти и хъбовете, поддържащи стандартите 1000BaseT, са достъпни на цена, която е няколко пъти по-голяма от компонентите на Ethernet мрежите със скорост 100 Mbps.

Мрежи 100BaseVG-AnyLAN

Hewlett Packard разработиха технологията 100BaseVG-AnyL.AN като бърза, достъпна мрежова архитектура, използваща хъб, който функционира като интелигентен централен контролер. Този хъб управлява достъпа до мрежата, като непрекъснато извършва бързо кръгово сканиране на заявки за мрежови портове, за да проверява за заявки за услуги от свързаните към тях възли. Хъбът приема входящия пакет данни и го насочва само към порта със съответния адрес на местоназначение. Това съответствие осигурява голяма сигурност на данните в мрежата.

Хъбовете могат да бъдат свързани заедно и всеки хъб може да бъде конфигуриран да поддържа фреймовия формат 802.3 Ethernet или 802.5 Token Ring. Въпреки това всички хъбове в една и съща мрежа трябва да бъдат конфигурирани да използват един и същ фреймов формат.

Мрежите 100BaseVG-AnyLAN често биват поставяни в категорията Ethernet, но те използват различни типове метод за достъп до преносната среда, наречен *приоритет по поискване (demand priority)*, дефиниран в спецификацията 802.12 на IEEE.

Мрежи 10BaseFL и 100BaseFL

Буквите FL в 10BaseFL означават fiber link (оптична влакно); тези мрежи използват предаване на немодулирани сигнали по кабел с оптично влакно. Повече за методите за предаване на сигнали ще научите в Глава 4 – „Методи за комуникация по мрежи".

Кабелите с оптично влакно използват светлинни импулси вместо електрически сигнали за представяне на нулите и единиците на използваната от компютрите двоична комуникация. Голямо предимство на оптичните кабели пред медните е тяхната устойчивост на смущения и затихване (т.е. загубата на силата на сигнала при предаване на разстояние). Един кабелен сегмент от спецификациите FL може да бъде дълъг 2000 метра, което е 4 пъти повече от 10Base5, над 10 пъти повече от 10Base2 и 20 пъти повече от лимита за 10BaseT!

Мрежи Token Ring

Token Ring представлява архитектура за изграждане на мрежи, разработена от IBM през 80-те години. Тя е проектира с цел преодоляване на някои от проблемите, свойствени на конкурентната мрежа, каквато е Ethernet, където компютрите в мрежата се конкурират или състезават за правото да предават. Това ще разгледаме по-подробно в Глава 4, в секцията „Методи за достъп до преносната среда".

В Token Ring мрежа, използваща топология логически кръг, един сигнал, наречен *маркер (token)*, се предава в кръг и даден компютър не може да предава, докато не получи маркера. Това означава, че за разлика от Ethernet мрежите, в Token Ring не съществуват *колизии на данни*. Колизия на данни възниква, когато два компютъра изпращат данни едновременно.

Макар че представляват логически кръг, Token Ring мрежите физически се разполагат като топологии звезда. Компютрите се свързват към централен хъб (концентратор), наречен модул за достъп до множество станции (MSAU). Кръгът реално се реализира вътре в хъба, където се осъществява конекция между кабелите и портовете в непрекъсната окръжност и данните пътуват по кръгообразен път.

Стандартите за Token Ring мрежи са дефинирани в IEEE 802.5. Използват се типове кабели на IBM, основно екранирана усукана двойка (STP). Изобщо мрежовите карти за Token Ring и другите компоненти са по-скъпи от тези за Ethernet мрежи. Въпреки това Token Ring е високонадеждна архитектура, която все още се използва в много локални мрежи.

По-старите компоненти за Token Ring поддържат скорости на предаване само от 4 Mbps, но по-новите реализации могат да предават данни с 16 Mbps.

ЗАБЕЛЕЖКА В момента се полагат усилия за разработване на ефективна високоскоростна технология Token Ring, която реализира Token Ring мрежа по FDDI или ATM. За повече информация вижте документацията, предоставена от консорциума High-Speed Token Ring Alliance на адрес www.hstra.com/whitepapers.html.

Предимствата на Token Ring са следните:

- Когато Token Ring мрежата се претовари, нейната производителност спада леко. Т.е. мрежата постепенно става по-бавна, но не се срива внезапно, както става с Ethernet.
- Token Ring използва *активна топология (active topology)*, в която всеки компютър в кръга регенерира сигнала, докато сигналът пътува по кръга. Ethernet мрежите изискват поставяне на повторители за усилване на сигнала при по-големи разстояния.

Мрежи AppleTalk

Apple Computers разработиха комплекта протоколи AppleTalk, предназначен за изграждане на мрежи с техните машини Macintosh за споделяне на файлове и принтери в среда на работна група. AppleShare представлява комплект от протоколи на приложно ниво, които осигуряват тази функционалност. Компонентите на AppleShare, вградени в операционната система на Macintosh, са следните:

- **AppleShare File Server** – Позволява на потребителите достъп до ресурсите на компютъра
- **AppleShare Print Server** – Осигурява споделяне на принтери

AppleShare PC е услуга, която се изпълнява на DOS компютри, за да им позволи да осъществяват достъп до файлове на файлов сървър AppleShare или да печатат на споделен принт сървър AppleShare.

Мрежите AppleTalk често биват означавани като *LocalTalk* мрежи. Протоколът LocalTalk Link Access Protocol (LLAP) е основният използван протокол, който поддържа динамично адресиране.

Мрежите AppleTalk могат да бъдат разделени на групи, наречени *зони*, подобно на разделянето на голяма мрежа на работни групи. Потребителите виждат само тези споделени ресурси, намиращи се в зоната, към която принадлежат. За комуникация между зоните маршрутизаторите използват протокола Zone Information Protocol (ZIP).

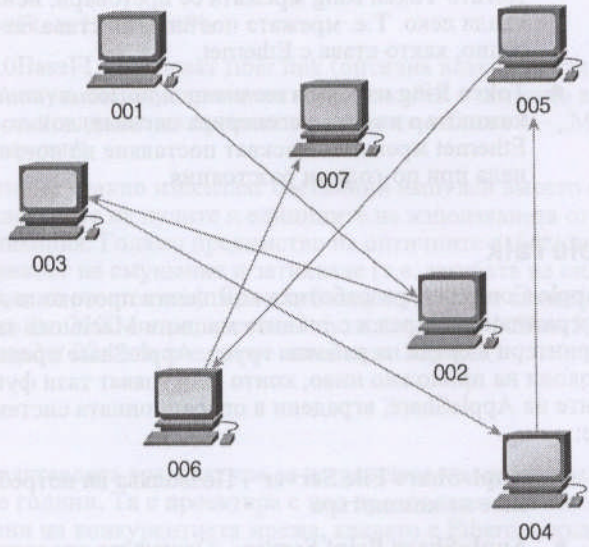
Мрежи ARCnet

Мрежата Attached Resource Computer Network (ARCnet) е по-стара архитектура за локални мрежи, която в по-голямата си част беше заменена от Ethernet и Token Ring. ARCnet използва метод за достъп с предаване на маркер, но реализира мрежова топология шина или звезда, вместо кръг.

В ARCnet мрежата маркерът се предава в числов ред в съответствие с *адреса на възела*, представляващ осемцифрено двоично число, което се задава на ARCnet мрежовата интерфейсна карта с помощта на DIP превключватели или джъмпери. Ако картите не са номерирани внимателно, така че сигналът да преминава в

логически ред, или ако компютрите по-късно се преместят на други места, без да бъде променено адресирането, може да се получи пътуване на сигнала на по-големи разстояния, отколкото е необходимо. Фигура 2-16 илюстрира този проблеми.

Фигура 2-16 *Ако адресите на мрежовите интерфейсни карти на ARCnet не са зададени правилно, пътят, по който преминава маркерът, може да бъде много неефикасен.*



ЗАБЕЛЕЖКА ARCnet мрежите са бавни в сравнение с повечето LAN технологии: 2,5 Mbps за стандартния ARCnet, макар че по-новият стандарт, наречен ARCnet Plus, подобрява значително тази характеристика със скорост на предаване 20 Mbps.

ARCnet може да използва коаксиален кабел, UTP или дори оптичен кабел, но най-често се асоциира с 90-омовия коаксиален кабел RG-62/U. Един от недостатъците на ARCnet, който е причина за липсата на популярност за изграждане на локални мрежи, е неговата нестандартна природа. Но все пак това е една стабилна и надеждна архитектура.

Обобщение

В тази глава разгледахме многото различни начини за категоризация на мрежи, а именно:

- Физическият обхват на мрежата
- Административният модел, използван за управление на мрежата
- Мрежовата операционна система (NOS), изпълнявана на сървърите, които контролират мрежата
- Протоколите, използвани от мрежата за комуникация

- Топологията или разположението на мрежата
- Архитектурата, включваща стандартите и спецификациите, по които функционира мрежата

Разбира се, има и други начини, по които мрежите могат да бъдат категоризирани. Темата на тази книга е изграждането на мрежи от персонални компютри, но при един по-общ поглед мрежите могат да бъдат класифицирани също на мрежи от персонални компютри и мрежи от мейнфрейм компютри.

Много от категориите, които разгледахме, могат да бъдат подразделени допълнително; например UNIX мрежите могат да бъдат разделени на HP-UX мрежи, SUN Solaris мрежи, AIX мрежи, SCO мрежи и т.н. Microsoft мрежите могат да бъдат разделени на Windows 2000 мрежи, Windows NT 4.0 мрежи и Windows NT 3.51 мрежи – без да споменаваме работните групи с Windows 9x.

Докато описвахме всеки от методите за категоризация, може би сте забелязали, че определени архитектури се асоциират с определени топологии; или че конкретни мрежови операционни системи използват конкретни модели на администриране; или че някои протоколи се използват по-често в мрежи от конкретен физически обхват. В следващите глави ще доизградим тези закономерности.

Ще научите за различните методи на предаване на сигнали, използвани от различните технологии, и различните типове кабели, асоциирани с различните методи за достъп до преносната среда. Глава 3 осигурява общ преглед на популярните модели, използвани за описание на комплексния процес, в който вземат участие всички тези компоненти. Ще разгледаме също спецификациите и стандартите, на които са базирани мрежите.

Допълнителни източници

Един добър информационен ресурс за Gigabit Ethernet е страницата на Gigabit Ethernet Consortium – www.iol.unh.edu/consortiums/ge/main.html.

GEC2000 е ежегодна конференция по въпросите на Gigabit Ethernet; последната бе проведена през март 2000 г. в Сан Хосе, Калифорния. Вижте Web сайта GEC2000 на адрес www.etherconference.com/English/Main_Splash.html.

Един чудесен ресурс за информация за 100BaseVG-AnyLAN на Hewlett Packard е достъпен на адрес www.100vg.com.

За обща информация относно начина на работа на локалните мрежи, вижте www.net-engineer.com/lanbasics1.html.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Кое от следните е категория, използвана при класифициране на мрежите според физическия обхват на мрежата?

a 10Base2

b WAN

c IPX/SPX

d Ring

2 Кое от следните е истина за типичната локална мрежа? (Изберете всички верни отговори.)

a LAN е голяма мрежа, съставена от множество малки мрежи.

b LAN обикновено обхваща разпръснатата географска област, с възли, разположени в различни щати или държави.

c LAN обикновено е затворена в рамките на ограничена област, при която компютрите се намират във физическа близост един до друг.

d LAN мрежите могат да бъдат разделяни на работни групи за по-лесно управление.

3 Как се нарича група от мрежи, свързани в мрежа една с друга?

a интернет

b интранет

c екстранет

d работна група

4 Кое от следните е истина за мрежата клиент/сървър (сървърно-базираната мрежа), но не е истина за равноправната мрежа? (Изберете всички верни отговори)

a Мрежите клиент/сървър по принцип са по-евтини за реализиране.

b Мрежите клиент/сървър осигуряват централизирано съхраняване на данните, което улеснява тяхното архивиране.

c Мрежите клиент/сървър най-общо изискват специално назначен мрежов администратор.

d Мрежите клиент/сървър предлагат по-добра сигурност.

5 Кой от следните термини се използва за идентифициране на сървър за автентикация при влизане в мрежа клиент/сървър на Microsoft?

a демон

b мениджър на сигурността на акаунтите

c домейн контролер

d клъстерен сървър

6 Кое от следните е истина за сигурността в равноправната среда (работната група)? (Изберете всички правилни отговори.)

a Сигурността е централизирана и се администрира от мрежов администратор.

b Сигурността е по-силна и по-трудна за пробив в среда клиент/сървър.

c Всяка машина в работната група поддържа своя собствена локална база данни на сигурността.

d Сигурността се реализира на ниво споделен ресурс, вместо на ниво потребител.

7 Коя от следните характеристики на Windows 2000 домейните представлява промяна от домейн модела на Windows NT? (Изберете всички верни отговори.)

- **a** Windows2000 домейните са базирани на директорийна услуга, наречена Active Directory.
- **b** Windows 2000 домейните са базирани на директорийна услуга, наречена Bindery.
- **c** Windows 2000 домейните се означават като домейни от ниско ниво.
- **d** Windows 2000 домейните могат да съдържат множество домейн контролери, които могат да четат и записват в базата данни на директорията.

8 Кое от следните е истина за TCP/IP мрежите?

- **a** TCP/IP мрежите обикновено са мрежи със среден и голям размер, които съдържат множество подмрежи.
- **b** Глобалният Интернет е TCP/IP мрежа.
- **c** За TCP/IP мрежи са достъпни няколко инструмента и помощни програми.
- **d** TCP/IP мрежите са по-лесни за администриране от NetBEUI мрежите.

9 Какво е името на мрежовата топология, която има начало и край, и изисква терминиране за предотвратяване на отразяване на сигнала?

- **a** Звезда
- **b** Хибридна решетка
- **c** Линейна шина
- **d** Token Ring

10 Кои от следните мрежови архитектури използват кабел с неекранирана усукана двойка.

- **a** 10Base2
- **b** 10BaseT
- **c** 100BaseFL
- **d** Token Ring

Глава 3

Мрежови концепции, модели и стандарти

Изучаването, особено на нова и сложна тема, каквато е изграждането на компютърни мрежи, е по-лесно, когато започнем с теорията и концепциите и след това преминем към по-конкретни аспекти на реализацията. Както бъдещите лекари първо изучават теориите на биологията, биохимията и човешката физика, преди да започнат да преглеждат пациенти, така и специалистите по мрежи първо изучават принципите на мрежовите комуникации, преди да се опитат да инсталират, управляват или отстраняват неизправности на свързаните в мрежа компютри.

Тази глава представя основните концепции на изграждането на компютърни мрежи и разглежда начините за тяхното представяне, разбиране и запомняне. По-конкретно ще разгледаме мрежовите модели, стандарти, спецификации (и организациите, които ги създават) и добре познатите правила за изграждане на мрежи, които трябва да имате предвид, когато четете следващите глави на книгата за дизайна на мрежовия хардуер и софтуер.

Концепции на компютърните комуникации

Независимо от размера и обхвата на мрежата, топологията, архитектурата, типа на преносната среда или използвания модел на администриране, ние свързваме компютрите поради една главна причина: за да им позволим да комуникират един с друг. Това звучи просто, но всъщност е сложен процес. За да разберете принципите на комуникацията по мрежата, първо трябва да разберете как компютрите обработват информация.

В следващите секции ще разгледаме концепциите, които стоят за мрежовата комуникация, а именно:

- Двоичният език, използван за комуникация с машини (наричан също *машинен език*)
- Моделите за изграждане на мрежи, създадени за графично представяне на процеса на комуникациите
- Стандартите и спецификациите, създадени за улесняване на комуникацията между мрежовите продукти на различни производители

Нашата първа стъпка ще бъде разглеждането на езика или *кода*, който говорят компютрите, и възможността да използваме този език, за да ги програмираме така, че да изпълняват желаните от нас задачи.

Езикът на машината

Модерните компютри са интелигентни машини, способни да изпълняват безброй сложни задачи. Когато въвеждате писмо или доклад в текстообработваща програма, компютърът не само записва вашата работа и ви позволява по-късно да правите промени в нея, а също може да провери правописа и граматиката, да форматира външния вид в съответствие с ваши предварително зададени предпочитания и дори да ви даде възможност да изпратите документа на някой, който работи на друг компютър в стаята или на другия край на света.

При използване на подходящ софтуер вашият персонален компютър може да визуализира поразителен графичен дизайн, да следи вашия дневен график и да ви уведомява кога имате делова среща. Можете да изпълнявате помощни програми, с помощта на които да поддържате неговата операционната система и таблиците на файловете в добър ред; компютърът да влиза в Интернет (с или без ваша намеса) и да сваля обновявания за инсталирания на него софтуер. Той може да мисли дори като световен шампион по шах.

Компютърът постига всички тези функции, а и още много други, като извършва математически изчисления с висока скорост, използвайки само единици и нули. „Зад кулисите" компютрите обработват команди и връщат резултати, използвайки *двоична* бройна система (бройна система с *основа* 2), която, както ще видите след малко, е абсолютно подходяща за електронна комуникация. Понякога двоичният код се нарича машинен език.

Разпространени бройни системи

Съществуват няколко числови бройни системи. Най-често използваме *десетичната* за всекидневни пресмятания, но има и други системи, които се използват изключително в научната сфера, като например *шестнадесетичната* и *двоичната*. В следващите секции ще разгледаме всяка от тях.

Десетичната система

Десетичната бройна система се нарича също система с *основа* 10, защото е базирана на 10 цифри (от 0 до 9), които могат да бъдат използвани за записване на числа – дори такива, които са прекалено големи дори за произнасяне.

ЗАБЕЛЕЖКА Не се объркайте от името. Не е задължително десетичното число да съдържа десетична запетая.

В едно десетично число, например 342, цифрата 3 представя три *стотици*, цифрата 4 представя четири *десетици*, а цифрата 2 представя две *единици* – според мястото, което заема всяка от цифрите спрямо другите в записа на числото.

Шестнадесетичната система

Друга бройна система, която също се използва в компютърната индустрия, е шестнадесетичната. Hex, както се нарича, не е лошо заклинание, извикано от вещица върху метла, макар че работата с тази система изглежда малко като черна магия за непосветените. Шестнадесетичната система има *основа* 16 и използва същите 10 цифри като десетичната система, плюс буквените знакове от A до F.

В шестнадесетичната бройна система числата от 0 до 9 имат същия запис, както в десетичната бройна система. Но тук числото, което обикновено представяме като 10 (9 плюс 1) се записва в шестнадесетичен запис като A. Десетичното число 11 е B в шестнадесетичен запис;12 е C; 13 е D; 14 е E; а 15 е F. Добре, това е сравнително просто, но когато буквите свършат, става малко по-объркано. Например числото 16 в десетичната бройна система е 10 в шестнадесетичната, а 17 е 11.

ЗАБЕЛЕЖКА Ако се опитате да намерите произхода на думата hexadecimal, ще откриете, че тя е хибрид от гръцкото *hexa*, което означава шест, и латинското *decem*, което означава десет.

Как можем да направим преобразуване между двете бройни системи? Да, най-лесният начин е да използваме калкулатора на Windows в режим Scientific или някакъв друг калкулатор за научни изследвания. Всъщност броенето се извършва по един и същ начин в шестнадесетичната и десетичната бройна система, с изключение на това, че има шест допълнителни цифри, с които трябва да се преборим. Таблица 3-1 показва съответствието между десетични и шестнадесетични числа. Десетичният еквивалент е даден в скоби.

Таблица 3-1 *Как шестнадесетичната система съответства на десетичната (десетичните числа са в скоби).*

0 (0)	1 (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (7)	8 (8)
9 (9)	A (10)	B (11)	C (12)	D (13)	E (14)	F(15)		
10 (16)	11 (17)	12 (18)	13 (19)	14 (20)	15(21)	16 (22)	17 (23)	18 (24)
19 (25)	1A (26)	1B (27)	1C (28)	1D (29)	1E(30)	1F (31)		
20 (32)	21 (33)	22 (34)	23 (35)	24 (36)	25 (37)	26 (38)	27 (39)	28 (40)
29 (41)	2A (42)	2B (43)	2C (44)	2D (45)	2E(46)	2F (47)		

Шестнадесетичният запис се използва в компютърната индустрия, защото е полесно преобразуването между шестнадесетична и двоична система, отколкото между десетична и двоична. Тъй като шестнадесетичната има основа 16, можете да използвате две шестнадесетични цифри за представяне на всеки *байт* (който се състои от 8 двоични *бита*). В следващата секция от тази глава ще се върнем отново към битовете и байтовете.

Обърнете внимание в таблица 3-1, че някои шестнадесетични числа изглеждат като десетични дори когато не представят същата стойност. Ако видим числото 12 без допълнителни обяснения, как можем да разберем дали то представлява десетичното число 12 или шестнадесетичния запис на десетичното число 18? Необходим ни е начин за идентифициране на основната система, която се из-

ползва. За щастие, шестнадесетичният запис се индицира по едни от следните два начина:

- Чрез добавяне на H в края на числото, например 12H
- Чрез поставяне пред числото на префикса 0x, например 0x12

Обърнете внимание, че вторият метод е стандартният начин за индициране на шестнадесетичен запис в езика C++ и в някои други езици за програмиране.

Двоична система

Несъмнено двоичната бройна система е най-простата; тя използва само две цифри: 0 и 1. Но тъй като всички числа трябва да бъдат представени с помощта само на две цифри, с нарастването си числата много бързо стават дълги. Например десетичното число 519 в двоичен запис става 10000000111.

Думата *двоично (binary)* идва от латинското *bi*, което означава две, а двоична система се нарича също бройна система с *основа* 2. Пример за двоично число е 01001100.

Нули и единици

Ако никога досега не сте срещали двоични числа, може би се учудвате как може всички възможни числа да бъдат представени само с две цифри. Разбира се, същият въпрос може да бъде зададен за използваните на практика само 10 числа, но ние ги използваме цял живот. Например изглежда нормално използването на позиции за индициране на стойността на всяка цифра в десетичната бройна система, според което третата позиция от дясно на ляво се представя като стотици. Двоичната бройна система работи по подобен начин.

ЗАБЕЛЕЖКА Помнете, че в двоичния език 0 и 1 са единствените съществуващи цифри.

Битове и байтове

Двоичната цифра (1 или 0) се нарича *бит*. В повечето компютърни системи един байт е равен на 8 бита. *Байтът* представлява низ от битове, групирани за удобство, и е единицата, която компютрите използват за представяне на един *знак* (буква от азбуката, цифра или друг символ).

ЗАБЕЛЕЖКА Терминът „байт“ идва от фразата „binary term“ и означава количеството компютърна памет, необходима за съхраняване на един знак със зададен размер. Този размер на знак е стандартизиран на 8 бита за микрокомпютрите, но байтът може да представя и 16 бита на някои по-големи компютри (миникомпютрите и мейнфрейм компютрите).

Преобразуване от двоична в десетична бройна система

Погледнете отново нашето примерно двоично число: 01001100. За да определите какво представлява десетичният запис на това число, трябва да знаете как

да интерпретирате стойността на всяка двоична цифра в зависимост от нейната позиция.

В двоичния запис всеки бит е „включен“ или „изключен“. Нулата индицира, че битът е изключен, а битът, който е изключен, няма стойност (т.е. тя е 0). Включеният бит има стойност, зависеща от позицията, която той заема в записа на числото. Както при добре познатата ни десетична система, определяме позицията (мястото), като броим от дясно на ляво.

В двоичната система, както и в десетичната, 1-ца в първата (най-дясната) позиция има стойност 1. Но тук завършва всяка прилика между десетичната и двоичната системи. В двоичната система, която има основа 2, стойността на включения бит (1) нараства по степен на основата 2 с преминаване към всяка следваща позиция наляво. По този начин десетичният еквивалент на всяка двоична стойност (когато битът е включен или означен с 1) е показан в таблица 3-2.

Таблица 3-2 *Определяне на стойността на двоичните битове*

Двоично	1	1	1	1	1	1	1	1
Десетично	128	64	32	16	8	4	2	1

Ако цифрата е 0, битът на това място е изключен и неговата стойност е 0. Затова, за да преобразуваме двоичното число 01001100 в десетично, просто ще съберем стойностите за всеки бит, който е включен (1). Таблица 3-3 илюстрира това.

Таблица 3-3 *Преобразуване на двоично число в неговия десетичен еквивалент*

Двоично	0	1	0	0	1	1	0	0
Десетично	0	64	0	0	8	4	0	0

За да получим десетичния еквивалент на 01001100, събираме 64 + 8 + 4, което дава стойност 76. Можете да проверите отговора, като въведете двоичното число в научен калкулатор и изберете опцията Dec, за да извършите преобразуването.

Защо използваме двоична система?

Всичко това е интересно (особено ако присъствате на парти, пълно с инженери по мрежи), но сигурно все още се чудите защо компютърните комуникации са базирани на двоичната система. Защо не на шестнадесетичната? Или още по-добре, защо да не се използва десетичната, за да не се налага да отделяте време за преобразуване в други бройни системи?

Има причина. Помислете за следното: Компютрите са електронни машини и в тях данните се представят като електрически импулси. Компютрите използват *цифрови* сигнали. В Глава 4, „Методи за комуникация по мрежи“, ще поговорим още за цифровите сигнали и за това по какво те се различават от *аналоговите* сигнали, предавани по радиото.

За целите на това изложение, обърнете внимание, че цифровите сигнали са форма на *дискретно състояние* на сигнала. Дискретното състояние действа подобно на проста осветителна лампа, която може да бъде включена или изключена. Тя не може да бъде и в двете състояния в един и същ момент, и също така между двете състояния няма състояния „полувключена“ или „полуизключена“.

Разбирате, че двоичният запис е много лесен за представяне с помощта на цифрови електронни сигнали. Както при осветителната лампа, или има, или няма електрически ток. Ако има ток (включено), компютърът разбира 1. Ако няма (изключено), компютърът разбира 0.

Двоичното смятане и начинът, по който то е свързано с използването на цифрови сигнали, е първата и най-разпространена концепция, която трябва да изучите, за да разберете как работят компютрите в мрежа. Вижте секцията „Допълнителни източници" в края на главата, за да получите по-задълбочена информация относно двоичните комуникации.

Използване на пакети

Преди данните да бъдат предадени по мрежата като електрически импулси, те първо трябва да бъдат разделени на отделни парчета, които лесно могат да бъдат управлявани. Целият документ от текстообработваща програма или съобщение от електронна поща не могат да бъдат изпратени в един дълъг, непрекъснат поток. Това ще ограничи мрежата, и другите компютри няма да могат да предават. За да могат много компютри да използват мрежата едновременно, големите файлове трябва да бъдат разделени на по-малки секции, преди да бъдат изпратени по кабела или друга преносна среда.

Представете си следната аналогия: Да предположим, че искате да изпратите по пощата документ от 100 страници до ваш колега, но разполагате само с пликове, които побират по два листа. Едно от решенията е да разделите големия документ на части по два листа, да поставите всяка от тях в отделен плик, да ги адресирате до вашия колега и да ги поставите в пощенската кутия. Когато пристигнат всички пликове, получателят може отново да подреди целия документ.

В един идеален свят всичките пликове ще пристигнат в правилен ред. Но пощенските услуги не работят така. Вашият колега дори може да не получи всичките пликове в един и същ ден поради сложния процес на доставяне от пощенската кутия до пощенската станция. Пликът, съдържащ първите страници на документа, не е задължително да пристигне първи. Как тогава вашият колега ще подреди документа отново в правилен ред? Можете да улесните работата на вашия колега, ако номерирате страниците, така че да може да определи тяхната последователност.

В секцията „Сглобяване на данните" ще разгледаме как протоколите за работа в мрежа осигуряват последователно предаване на информацията, така че пакетите да бъдат сглобявани правилно на мястото на тяхното приемане.

Малките парчета данни, на които се разделят компютърните данни за предаване по мрежата, се наричат *пакети*. В зависимост от мрежовата архитектура и от точката в процеса на комуникация, до която е достигнало дадено парче, когато говорим за пакети, можем да използваме и термина *фреймове*. Освен тях, думата *сегмент* означава единица с данни, предавана с помощта на протокола Transmission Control Protocol (TCP). За означаване на тези управляеми парчета най-общо използваме термина *пакет*.

Предимства от разделянето на данните на пакети

Предлагането на данните на малки пакети има няколко предимства:

- Компютрите в мрежата могат да използват обиколни пътища за предаване на пакетите и един компютър, който предава големи количества дан-

ни, не може да монополизира пропускателната способност (честотната лента, капацитета) на мрежата.

- Ако мрежовата комуникация бъде прекъсната или даден пакет бъде изгубен, трябва да бъде предадена отново само тази малка част от данните, а не целият файл.
- В зависимост от топологията на мрежата и типа на свързването, всеки пакет може да премине по различен път, за да достигне до местоназначението. По този начин, ако един път започне да се препълва или стане прекалено бавен, следващите пакети могат да поемат по по-ефикасен маршрут.

Сглобяване на данните

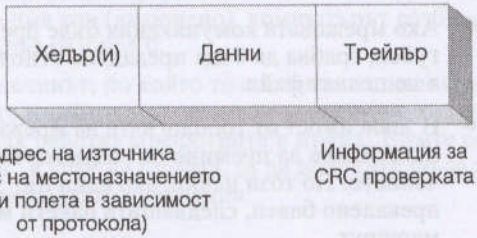
Ако обособим данните на отделни парчета и след това изпратим всяко парче поотделно, какво става, когато те пристигнат на тяхното местоназначение? Да се върнем отново на примера с пощата; мрежовите компоненти правят нещо подобно. Всеки пакет данни съдържа информация, добавена в него към обикновените данни, под формата на *хедъри*. Хедърите съдържат адресна информация, с помощта на която пакетите достигат своето местоназначение. Те съдържат също информация за последователността, така че данните да могат да бъдат подредени отново правилно, когато всички пакети достигнат до приемащия компютър.

ЗАБЕЛЕЖКА Може би сте забелязали, че използваме думата *данни* за описание на сигналите, изпращани по мрежата. *Информация* и *данни* са два термина, които понякога се използват взаимозаменяемо. *Информацията* представлява данни в използваема форма, например съобщение, създадено с помощта на програмата за електронна поща. Самите данни не са информация; те са кодирана форма на информацията, представляваща поредица от електрически импулси, в които информацията се преобразува, за да бъде изпратена.

Информацията в *хедъра* се поставя в началото на пакета, преди оригиналните данни. Пакетите могат да включват също *завършваща информация* или *трейлър (trailer information)*, която се добавя към края на пакета след оригиналните данни. Често тя включва информация за проверка за грешки. Фигура 3-1 показва структурата на типичен пакет с данни.

ЗАБЕЛЕЖКА Компонента за проверка за грешки в трейлъра се нарича *циклична проверка с излишък* (*cyclical redundancy check – CRC*). CRC извършва изчисления – в двоична бройна система, разбира се – върху пакета, преди той да напусне компютъра-източник, и втори път, когато пакетът достигне местоназначението. Ако резултатите от тези изчисления са различни, това означава, че данните са променени по време на пренасянето. Това може да стане вследствие прекъсване на електрическите сигнали, представляващи нулите и единиците, които образуват данните. Ако бъде открито различие, този пакет може да бъде изпратен отново.

Фигура 3-1 *Типичният пакет данни включва информация за хедъра и трейлъра.*



Точният брой на полетата в хедъра и трейлъра на пакета, както и размерът на всяка поле, зависят от мрежовата архитектура и протоколите. Например в една Ethernet мрежа единицата данни се нарича фрейм (или още кадър). Един Ethernet фрейм може да бъде с размер между 64 и 1518 байта, но 18 байта се използват за самия Ethernet фрейм. Това означава, че във всеки фрейм (пакет) може да има максимум 1500 байта данни. Фреймът или пакетът на Token Ring е доста по-голям и обикновено съдържа 4202 байта данни.

Многослоен процес на комуникация

Не стига сложният начин на вътрешно функциониране на един самостоятелен компютър – преобразуващ данните в 0-ли и 1-ци за обработка – след това очакваме от него да изпрати данните на друг компютър, дори ако другият компютър не използва същата операционна система или приложна програма. Например ако искате да използвате компютър с Windows NT за изпращане на съобщение от електронна поща, създадено в програмата за поща Outlook Express на Microsoft, до получател, който използва програмата Eudora Pro на компютър Apple Macintosh, вие очаквате съобщението да бъде прехвърлено бързо и точно!

Процесът на мрежова комуникация е сложен. Всички думи, които въвеждате, заедно с информацията за достигане на съобщението до неговото правилно местоназначение, заедно с прикачените графични или други файлове, трябва по някакъв начин да бъде сведена до поредица от електрически импулси, представляващи нули и единици.

ЗАБЕЛЕЖКА Електрическите импулси са типично средство за LAN комуникации, макар че бихме могли да ги заменим със светлинни импулси или радиопредавания, в зависимост от използваната мрежова преносна среда. Различните типове преносни среди ще разгледаме по-подробно в Глава 7, „Физически компоненти на мрежата".

Данните под формата на електронни сигнали трябва да пътуват по кабела до правилния компютър-местоназначение и след това да бъдат конвертирани в тяхната първоначална форма, която може да бъде прочетена от получателя. Както сигурно предполагате, този процес включва няколко стъпки. Поради тази причина разработчиците на хардуер, софтуер и протоколи са разбрали, че най-ефикасният начин за реализиране на мрежови комуникации е под формата на *многослоен* процес.

Работа в екип по мрежа

Произвеждането на една лека кола, подобно на трансфера на данни по мрежа, е *процес*, който включва много отделни функции. Едно лице може да вземе всичките части и с помощта на подходящи инструменти да ги сглоби във функциониращ автомобил, но колите не се правят по този начин. Защо?

Опитът показва, че е по-ефикасно да се използва конвейер за сглобяване на автомобили. На конвейера колата се произвежда на слоеве. Всеки работник на всяка станция по пътя отговаря за конкретно нещо. Стъпките, необходими за сглобяване на колата, се разделят на множество елементарни операции: един работник (или робот) може да постави колелата, следващият може да постави гайките, а трети да завие тези гайки. Тази методология дава следните предимства:

- Всеки работник може да се съсредоточи изключително върху своята собствена сфера на отговорност.
- Тъй като всеки работник повтаря една и съща задача отново и отново, всеки става много опитен в своята конкретна дейност.
- Чрез работа в екип работниците могат да произведат крайния продукт много по-бързо и по-ефикасно, отколкото може да направи това едно лице или група от хора без зададени конкретни отговорности.
- Лесно може да се води отчет на работата. Ако има проблем в даден слой (например ако конкретна гайка не е завита), лесно може да се определи кой е виновен.

По подобен начин работи и процесът на комуникация на слоеве. Всеки слой (т.е. всеки компонент от системата на мрежата) извършва конкретна задача. Както при автомобилния конвейер, това води до по-бързо и по-ефикасно изпълнение на процеса. Освен това, точно както контрольорът на качеството знае кого да обвини, когато е направена грешка, така и мрежовият администратор може да стесни обхвата на повредата, когато стане нещо лошо.

Процеси и протоколи

С помощта на многослойния модел процесът на мрежова комуникация се разделя на стъпки, подобно на автомобилния конвейер. В нашия пример за автомобилен завод, някой първо трябва да влезе във връзка с проектанта, да интерпретира спецификациите и да стартира процеса на сглобяване. По подобен начин един „работник“ се грижи за взаимодействието с потребителското приложение и стартира процеса на изпращане на данни по мрежата. Друг извършва такива задачи, като компресиране на данните, криптиране или пакетиране по някакъв друг начин за транспортиране. Друг се занимава с осигуряване на точността, следващият с проверката дали данните са адресирани правилно, така че да достигнат до желаното местоназначение, и т.н.

Работниците по линията за сглобяване в този процес представляват отделните *протоколи*, които работят на всеки слой от нашия модел. Когато разглеждаме моделите подробно в следващите секции, е важно да разберете кои мрежови протоколи на кои слоеве функционират. Това не само индицира функциите на протоколите, а също ви осигурява ценна информация за отстраняване на неизправности, когато процесът на комуникация не протича гладко.

Мрежови модели

Повечето хора зависят от визуалното стимулиране. Разбираме нещо по-добре, когато можем да го видим с очите си. Но абстрактните концепции, които нямат конкретна форма, могат да бъдат представени в модел, който да ни създаде визуална представа за дадена структура, процес или релационна връзка.

Моделите са навсякъде около нас. Генетиците използват двойна спирала за представяне на структурата на молекулата на ДНК. Физиците представят релационните връзки на протони и електрони на ниво атом. Атомите са много малки, за да могат да бъдат видени, но учените използват модели за подпомагане на изучаването на явления, които не могат да бъдат наблюдавани директно.

Целта на моделите

Ако потърсим думата модел в речника, ще открием много нейни значения, например „схематично описание на система, теория или явление, което представя нейни познати или предполагаеми свойства и може да бъде използвано за допълнително изучаване на нейните характеристики“ (*American Heritage Dictionary*). Тази дефиниция обхваща една от целите на мрежовите модели: да ни помогнат да опишем, разберем и изучим процеса на мрежова комуникация.

Моделът също „служи като пример, който може да бъде следван или сравняван“ (*American Heritage Dictionary*). Мрежовите модели са основата на стандартизацията; ако един и същ модел се използва от производителите на мрежови продукти, тези продукти могат да бъдат сравнени с едни с други. Моделите описват начина, по който се извършват комуникациите на данни. Ако даден производител, произвеждащ продукти за изграждане на мрежи, съблюдава стандартите на всеки слой, мрежовите компоненти трябва да работят с тези, произведени от други производители. Другите аспекти на стандартизацията и организациите, които установяват стандартите, ще разгледаме по-късно в тази глава.

Моделът OSI

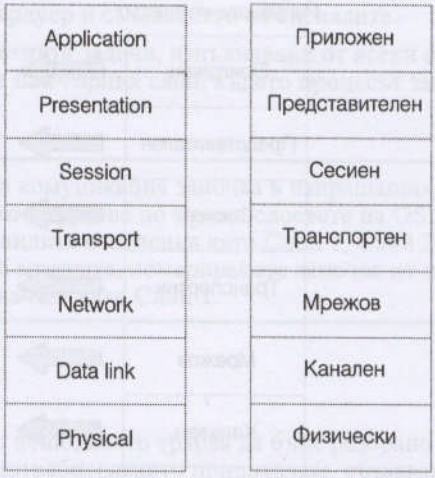
„Моделът на моделите“ в света на мрежите е моделът Open System Interconnection (OSI). На практика всяка книга за компютърни мрежи разглежда този модел, който е разработен от Международната организация за стандартизация (ISO).

ЗАБЕЛЕЖКА В някои книги моделът OSI се означава като Open System *Interconnect*, вместо *Interconnection*. Но по-късно се наложи използването на Web сайта на ISO и затова решихме, че те знаят най-добре.

Структурата на OSI модела

Моделът OSI е изграден от седем слоя, всеки от които представлява една стъпка в процеса на мрежовите комуникации. Седемте слоя на OSI модела са показани на Фигура 3-2.

Фигура 3-2 *Моделът OSI има седем слоя.*



Протоколите, които изграждат *комплекта от протоколи (protocol suit)*, работят на различни слоеве. Повече за мрежовите протоколи ще научите в Глава 8, „Мрежови протоколи и услуги".

Всеки слой на OSI модела изпълнява конкретна задача в процеса на мрежовата комуникация и след това предава данните нагоре или надолу към следващия слой (в зависимост от това дали слоят функционира в предаващия или приемащия компютър). Тъй като данните се предават през слоевете, всеки слой добавя своя собствена информация под формата на хедъри, които биват добавяни пред оригиналните данни. Разгледайте Фигура 3-1, на която е показана илюстрация на начина на прикрепване на хедърите.

Комуникация между равноправни хедъри

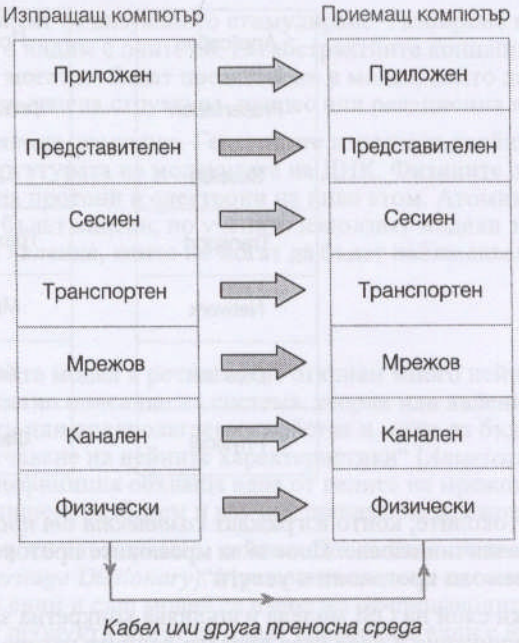
Процесът на мрежова комуникация работи по следния начин: от изпращащата страна дадено приложение създава данни, които трябва да бъдат предадени по мрежата. След това той ги предава на приложния слой от мрежовия компонент на операционната система.

Когато данните преминават през слоевете, те биват *капсулирани* или затваряни в рамките на по-голяма единица, тъй като всеки слой добавя хедърна информация. Когато данните достигнат приемащият компютър, процесът се извършва в обратния ред; информацията се предава нагоре през всеки слой и докато става това, капсулиращата информация постепенно бива премахвана, слой по слой, в ред, обратен на реда, в който е била добавяна.

Каналният слой (*data link layer*) в приемния край чете и снема хедъра, добавен от каналния слой на изпращащата страна. След това мрежовият слой на приемащата страна обработва информацията в хедъра, добавен от съответния слой на изпращащия компютър, и т.н. Всъщност всеки слой комуникира със слоя, който носи същото име от другата страна.

Фигура 3-3 илюстрира как работи този процес на комуникация.

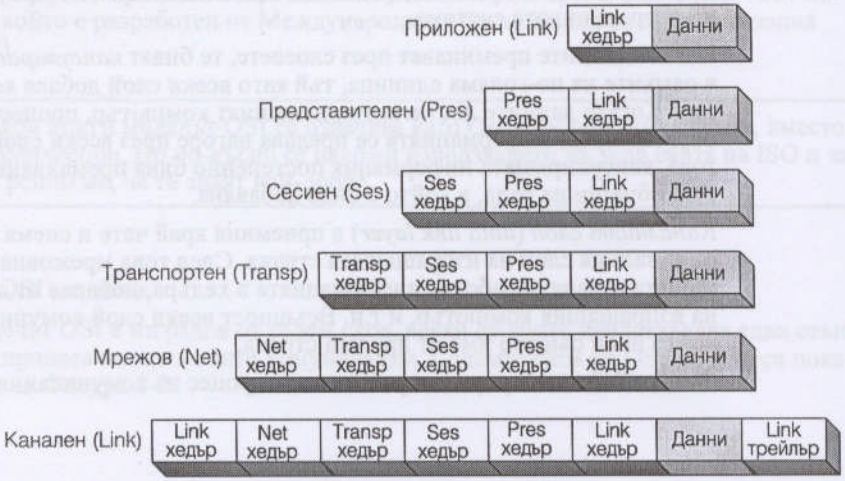
Фигура 3-3 *Всеки слой комуникира директно със своя равноправен слой от другата страна.*



Когато данните преминат целия си път през слоевете на приемащия компютър, цялата хедър информация бива премахната и данните се възстановяват в тяхната оригинална форма, т.е. както са създадени от приложната програма на изпращащия. В тази форма те се представят на приложението на приемника под формата на информация.

Фигура 3-4 показва как се добавя хедър информацията, когато данните напредват през слоевете.

Фигура 3-4 *Всеки слой добавя хедър информация към данните, докато пътува надолу през слоевете.*



Обърнете внимание, че физическият слой не добавя хедър информация. Неговата функция не изисква добавяне на тази информация, защото той се занимава главно с мрежовия хардуер и създаването на сигналите.

Да разгледаме конкретните задачи, изпълнявани от всеки от слоевете на OSI модела. Започваме от най-горния слой, където процесът започва в изпращащия компютър.

ЗАБЕЛЕЖКА Макар че процесът на комуникация започва в изпращащия компютър в горния край на модела, в много курсове по мрежи слоевете на OSI се преподават от горе на долу. Може да видите означения като Слой 1, Слой 2 и т.н. По стандартната терминология на мрежите, номерирането започва от най-долния, като физическият слой се означава като Слой 1.

Приложният слой

Първото и най-важно нещо, което трябва да бъде разбрано за приложният слой, е, че това не е потребителското приложение, създаващо съобщението. Този слой осигурява взаимодействие между приложната програма и мрежата. Протоколите, функциониращи в приложния слой, изпълняват функции като услуги за трансфер на файлове, достъп за печат и обмен на съобщения.

Протоколите, които функционират в приложния слой, са следните:

- **File Transfer Protocol (FTP)** – FTP се използва за трансфер на файлове между компютри, които не е задължително да работят под една и съща операционна система или платформа. Софтуерът на FTP сървъра се изпълнява на компютъра, който хоства файловете, а FTP *клиентската програма* се използва за свързване към, качване на или сваляне от сървъра. В повечето реализации на комплекта протоколи TCP/IP е включен FTP клиент, който работи от командния ред. Съществуват множество популярни графични FTP клиенти, като WSFTP, CuteFTP и FTP Voyager. Модерните версии на Web браузъри, като Microsoft Internet Explorer и Navigator/Communicator на Netscape, също включват вградени възможности за трансфер на файлове.
- **Telnet** – Telnet се използва за терминална емулация и за осъществяване на достъп до приложения и файлове на друг компютър. За разлика от FTP, той не може да бъде използван за копиране на файлове от един компютър на друг, а само за тяхното четене или изпълнение от отдалечения хост. Telnet софтуерът включва сървърния Telnet софтуер, изпълняващ се на отдалечения компютър, до който се осъществява достъп, и Telnet клиента, който се изпълнява на осъществяващия достъпа компютър.
- **Simple Mail Transfer Protocol (SMTP)** – SMTP е независим от производителя, прост ASCII протокол, използван за изпращане на електронна поща по Интернет. Много популярни програми за e-mail използват SMTP за изпращане на поща; за сваляне се използва и протоколът Post Office Protocol (текущата версия е POP3) или протоколът Internet Message Access Protocol (IMAP).
- **Simple Network Management Protocol (SNMP)** – SNMP събира информация за мрежата. SNMP може да бъде използван с различни платформи и операционни системи. Често той се приема за TCP/IP протокол, но мо-

же да бъде изпълняван и върху Internet Packet Exchange (IPX) и OSI. Протоколът SNMP използва база с управляваща информация (Management Information Base – MIB), представляваща база данни, която съдържа информация за работещ в мрежата компютър. SNMP има две части: *агентски* софтуер, който се изпълнява на наблюдавания компютър, и *управленски* софтуер, изпълняващ се на компютъра, който провежда наблюдението.

Това са само няколко от протоколите на приложния слой. В Глава 9, „Най-широкомащабната мрежа: глобалният Интернет" ще разгледаме и други, като Hypertext Transfer Protocol (HTTP) и Network News Transfer Protocol (NNTP).

Не бъркайте самите приложни програми с протоколите със същото име, на които са базирани програмите. Например съществуват разнообразни приложни програми, наречени FTP клиенти (например FTP Voyager, FTP Explorer, Fetch за Macintosh и GREED за Linux), предоставяни от различни производители. Тези програми използват протокола FTP за трансфер на файлове, но приложенията включват също и възможности като графични интерфейси (които се различават между различните реализации) или допълнителни функции, като например машини за търсене на файлове.

Представителният слой

Протоколът от приложния слой приема данните от потребителското приложение и ги предава надолу в стека към представителния слой. Както подсказва името, този слой изпълнява действията, свързани с пакетирането или представянето на данните. Тези действия са следните:

- **Компресиране на данни** – Представлява редуциране на размера на данните с цел способстване на по-бързото им предаване по мрежата. Различните типове данни могат да бъдат компресирани в различна степен.
- **Криптиране на данни** – Представлява преобразуване на данните в кодирана форма, която не може да бъде прочетена от неоторизирани лица.
- **Транслация на протоколи** – Конвертиране на данните от един протокол в друг с цел осъществяване на техния трансфер между разнородни платформи или операционни системи.

Представителният слой на приемащия компютър отговаря за декомпресирането, декриптирането и всички други транслации на данни в разбираем за приложението формат и тяхното представяне на приложния слой.

В представителния слой работят много шлюзове (gateways). *Шлюзът* представлява устройство или софтуер, което служи като точка на свързване между две различни мрежи. Популярните шлюзове са следните:

- **Gateway Services for Netware (GSNW)** – Този софтуер е включен в операционните системи Windows NT и Windows 2000 Server, за да даде възможност на клиентите на сървъра да осъществяват достъп до файлове на Novell Netware сървър. Софтуерът извършва транслиране между протокола Server Message Block (SMB), използван в софтуера на Microsoft, и протокола Netware Core Protocol (NCP), който е протоколът за поделяне на файлове, използван от Netware.
- **E-mail шлюз** – Това е тип софтуер, транслиращ съобщения от разнородни несъвместими e-mail системи в общоприет Интернет формат, какъвто е SMTP. Това ви позволява да изпращате електронни съобщения от ком-

пютър Macintosh, използващ клиента за електронна поща Eudora, до получател, използващ например Lotus Notes в NetWare мрежа. Независимо от разликата в системите за електронна поща, съобщението преминава успешно и може да бъде прочетено.

- **Systems Network Architecture (SNA) шлюз** – SNA представлява собствена архитектура на IBM, която се използва в мейнфрейм компютърни системи като AS/400. Софтуерът на SNA шлюза позволява на PC компютри от локална мрежа да осъществяват достъп до файлове и приложения на мейнфрейм компютър от своите десктопи.

Редиректорът (*redirector*) представлява софтуер, който определя дали дадена заявка трябва да бъде обработена от локалния компютър или от мрежово устройство, като пренасочват (преадресират) входно/изходните заявки по подходящ начин и по правило действат в представителния слой.

Сесиен слой

Следващият слой по пътя надолу в стека в OSI модела е сесийният слой. Протоколите, които работят в този слой, отговарят за изграждането на директна сесия между изпращащия и приемащия компютър. Сесийният слой установява и прекратява диалозите приложение–приложение. Той осигурява също така нареченото *поставяне на контролни точки (checkpointing)* за синхронизиране на потока от данни за приложенията. Това включва поставяне на маркери в потока от данни. При пропадане на комуникацията трябва да бъдат предадени отново само данните с най-скорошен маркер (контролна точка).

Друга функция на сесийния слой е да контролира дари предаването се изпраща като *полудуплекс* или като *пълен дуплекс*. Пълният дуплекс представлява двупосочна комуникация, при която и двете страни могат да изпращат и приемат едновременно. Полудуплексът също е двупосочен, но в даден момент сигналите могат да протичат само в една посока.

Сесията в пълен дуплекс работи до известна степен подобно на разговор по обикновен аналогов телефон. И двете страни могат да говорят едновременно, и докато говорите, можете да чувате гласа на другия човек. Полудуплексът прилича повече на разговор по двуканална радиостанция. Когато включите микрофона, за да предавате, няма да можете да чувате нищо, казано от другото лице, с което говорите. Предаването може да преминава във всяка от двете посоки, но не и в двете едновременно.

ЗАБЕЛЕЖКА *Еднопосочната* комуникация, в която сигналът може да върви само по един път и никога не може да се обърне в другата посока, се означава като *симплекс*. УКВ радиопредаванията и телевизионните предавания представляват симплексни предавания. Но въвеждането на технологии като „интерактивната телевизия“ изисква двупосочни комуникации, затова много кабелни компании (CATV оператори) модифицират своите инфраструктури, за да направят възможно двупосочното предаване на сигнали.

Сесийният слой отговаря за много неща, например за установяването на правила за обмен на данни между приложенията по време на сесията. Това донякъде наподобява работата на рефер или посредник, който гарантира, че и двете страни знаят правилата на играта и са съгласни да ги спазват – поне за времето на тази сесия.

Какво друго прави този работлив слой? Сесийният слой осигурява експедиране на данните, клас на услугата и докладване на проблемите в самия слой и в слоевете над него в мрежовия модел.

Протоколите от сесийния слой включват следното:

- **Network Basic Input/Output System (NetBIOS) интерфейс** – В сесиен режим NetBIOS позволява два компютъра да установяват връзка, позволява обработката на големи съобщения и осигурява откриване на грешки и тяхното коригиране. Също така този интерфейс освобождава приложението от необходимостта да е наясно с детайлите на мрежата.
- **Windows Sockets (Winsock) интерфейс** – Този интерфейс управлява входно/изходните заявки за Интернет приложения в среда на Windows. Winsock произлиза от интерфейса Berkeley UNIX sockets, който се използва за установяване на конекции със и обмен на данни между два програмни процеса в рамките на един и същ компютър или по мрежа. Сокетите ще разгледаме по-подробно в следващата секция.

Сесийният слой може също да изпълнява функции на сигурността и преобразуване на имена.

Транспортният слой

Транспортният слой изпълнява няколко важни функции и е важен елемент в мрежовите комуникации. Основното предназначение на този слой е да осигури надежден контрол на грешките и потока при пряката комуникация. Протоколите от транспортния слой осъществяват структурирането на съобщенията.

Транспортният слой следи за такива неща, като валидността на пакетите с данни, реда на следване и управлението, както и за обработката на дублирани пакети. Транспортният слой на приемащия край може да изпраща обратно потвърждение до изпращащия компютър, за да съобщи на изпращача, че пакетът е пристигнал. Това става само ако транспортният слой използва *връзково-ориентиран* протокол за изпращане на съобщението.

Съществуват два типа протоколи, използвани от транспортния слой – връзково-ориентиран (с установяване на връзка) и безвръзково-ориентиран (без установяване на връзка) – които са описани в следващите секции. Други важни концепции на транспортния слой са *преобразуването на имена* и *портовете и сокетите*.

Връзково-ориентирани транспортни протоколи TCP е връзково-ориентиран протокол, който работи в транспортния слой като част от протоколния стек TCP/IP. Връзково-ориентираните услуги изграждат връзка преди изпращането на данните и използват потвърждения за удостоверяване, че данните са пристигнали успешно до своето местоназначение.

Ето една аналогия: Ако искате да изпратите пакет по пощата до ваш приятел, можете да направите това по два начина. При първия начин, ако съдържанието е важно, може първо да се обадите на вашия приятел, за да му кажете, че пакетът е на път към него. Подобно нещо правят връзково-ориентираните протоколи; те установяват връзка, преди да започнат изпращането.

При втория начин можете да изпратите пакета по куриерска поща с изискване за връщане на обратна разписка. Това означава, че ще бъдете уведомени, че вашият приятел наистина е получил пакета. Обратната разписка, която идва при вас, е подобна на потвърждението, което връща връзково-ориентираният протоколът на изпращащия компютър.

Безвръзково-ориентирани протоколи Протоколът UDP (User Datagram Protocol), който също е член на комплекта TCP/IP, е безвръзково-ориентиран транспортен протокол. Безвръзково-ориентираните протоколи работят подобно на обикновената пощенска услуга. Когато поставите марка на писмото и го изпратите по пощата, вие вярвате, че то ще стигне до местоназначението си, до което е адресирано, но не разполагате с механизъм, който да ви гарантира, че това е станало.

Безвръзково-ориентираните транспортни услуги се използват за изпращане на съобщения, които не са критично важни или които са къси и прости, и лесно могат да бъдат изпратени отново, ако бъдат изгубени. Например бродкастните съобщения, които се изпращат до всички компютри в една подмрежа, използват UDP.

Какво е предимството на безвръзково-ориентираните протоколи, при положение че те са по-малко надеждни? Предимството е тяхната скорост; простотата и малкото натоварване, които водят до по-висока производителност.

Преобразуване на имена Друга задача на транспортния слой е преобразуването на имената на компютрите (хостовете) в логически мрежови адреси. Както TCP/IP, така и IPX/SPX (Internet Package Exchange/Sequenced Packet Exchange) задават логически имена на мрежовите компютри и използват зададените логически адреси за идентифициране на компютрите в мрежата.

В транспортния слой действа услугата Domain Name System (DNS). DNS и другите услуги за преобразуване на имена ще разгледаме в Глава 9.

Портове и сокети *Многозадачността* в мрежовите приложения е предимство, което модерните операционни системи имат пред по-старите такива (например MS-DOS); многозадачността позволява на потребителя в даден момент да изпълнява повече от една мрежова програма. Например можете да използвате Web браузър за достъп до Web сайт и в същото време софтуерът за електронна поща да сваля вашите e-mail съобщения.

Транспортният слой включва механизъм за разделяне на вашата входяща поща и отговора на заявката от страна на вашия браузър, когато и двете пристигат на един и същ мрежов адрес. За да осъществят това разделяне, протоколите от транспортния слой, като TCP и UDP, използват портове.

Номерата на портове разделят мрежовия адрес на части. В Глава 9 разглеждаме детайлно IP адресирането, използвано от TCP/IP за маршрутизиране на данни до компютъра-местоназначение. Засега можете да си представяте IP адресирането по следния начин: IP адресът, или логическият мрежов адрес, има отделни части, представляващи мрежовата идентификация (в коя мрежа се намира компютърът) и идентификацията на хоста (конкретният компютър).

IP адресите работят подобно на начина, по който името на улицата и конкретният номер на тази улица идентифицират местоположението на дадена сграда или офис. По тази аналогия номерът на порта може да бъде сравнен с номера на конкретния апартамент вътре в сградата. По тази причина протоколите от транспортния слой (TCP и UDP) задават номера на портове на всяко приложение. Това гарантира, че данните, предназначени за Web браузъра в апартамент B, няма да бъдат изпратени на програмата за електронна поща, която „живее" в апартамент D.

Мрежовият слой

Мрежовият слой е отговорен за доставяне на пакетите до техните местоназначения. Този слой управлява *маршрутизирането (routing)*. Можете да сравните

отговорностите на протоколите от мрежовия слой с тези на навигатор, който чертае курс от едно местоположение до друго, като избира най-ефикасния възможен път. Повечето протоколи за маршрутизация (разгледани в Глава 9) работят в мрежовия слой.

Този слой също така управлява приоритетите на типовете данни (основата на QoS [Quality of Service]), което осигурява някакво ниво на гаранция за достатъчно мрежови ресурси за приложения, изискващи висока пропускателна способност – например за видео на живо.

Устройства от мрежовия слой Устройствата, които работят в мрежовия слой, включват маршрутизатори и Layer 3 суичове. (Не забравяйте, че номерата на слоевете започват от най-долния, което прави мрежовия слой трети слой.) Тези устройства за свързване на мрежата са разгледани по-детайлно в Глава 7.

Каналният слой

Layer 2 бе дефиниран като канален слой (data link layer) в оригиналните спецификации на OSI; но този слой беше разделен допълнително на два подслоя:

- Контрол за достъп до преносната среда (Media Access Control – MAC)
- Контрол на логическите връзки (Logical Link Control – LLC)

MAC адресиране MAC подслоят обработва въпросите по *физическото адресиране*. Реално физическият адрес, който в една Ethernet или Token Ring мрежа представлява шестнадесетично число, постоянно записано в чипа на мрежовата интерфейсна карта (NIC), се нарича MAC адрес.

MAC адресът в Ethernet мрежа (понякога наричан с още едно име – Ethernet адрес) най-общо се записва като 12 шестнадесетични цифри, подредени по двойки, като всяка двойка е отделена с двоеточие (например 17:A4:2C:43:2F:09).

Тези 12 цифри в шестнадесетична бройна система представят 48-битови (т.е. 6-байтови) двоични числа. Първите 3 байта съдържат кода на производителя, който се задава от Института на инженерите по електроника и електротехника (IEEE). Последните 3 байта се задават от производителя и идентифицират конкретната карта.

ЗАБЕЛЕЖКА MAC адресът, или физическият адрес, се означава също като хардуерен адрес. Той се различава от логическите адреси (т.е. от IP адреса в TCP/IP мрежа) по това, че не може да бъде променян. Логическият адрес се задава с помощта на софтуер и лесно може да бъде модифициран. И двата идентифицират местоположението на компютъра в мрежата. Представете си логическия адрес като адрес на улица, който може да бъде променен с декрет на градския съвет. MAC адресът наподобява координата на географска ширина или дължина, която винаги остава постоянна.

На теория никога не трябва да има две карти с едни и същи MAC адреси. Но на практика производителите допускат грешки, като създават карти с дублиращи се адреси. Освен това някои производители започнаха да рециклират (използват отново) своите номера. Дублираните MAC адреси предизвикват проблеми, ако две карти с един и същ адрес се намират в една и съща мрежа, подобно на наличието на две къщи на една и съща улица с един и същ номер. Пощенската служба не знае къде да достави пощата, адресирана до „Васил Левски“ 150, ако там има два такива адреса.

Ако две мрежови интерфейсни карти в мрежата имат един и същ адрес, вие трябва да замените една от картите или да промените адреса на една от тях. Някои производители предоставят софтуер, който прави възможно това с помощта на препрограмиране на чипа на мрежовата карта.

Методът за контрол на достъпа до преносната среда разпределя достъпа на компютрите до мрежата. Контролът на достъпа до преносната среда се извършва в MAC подслоя. Разнообразните методи за контрол на достъпа и начина, по който работят, ще разгледаме в Глава 4.

LLC слоят и логическата топология В LLC подслоя се дефинира логическата топология на мрежата. Както бе споменато, логическата топология може да не е същата като физическата.

Този подслой отговаря също за осигуряване на връзка или интерфейс между MAC подслоя, който следва след него, и мрежовия слой над него.

Устройства от каналния слой В каналния слой действат както *мостовете*, така и *суичовете* от Слой 2 (наричани също *комутиращи хъбове*). И двата вида устройства са описани детайлно в Глава 7.

Физическият слой

Накрая стигаме до Слой 1 – физическия слой. Това е мястото, където данните и хедърите, добавени от другите по-горни слоеве, биват транслирани в сигнали, които могат да бъдат предавани и прехвърляни в кабела, за да започнат пътуването си по мрежата (или в случай на безжична преносна среда, изпращани като радиовълни или по други начини). Протоколите от физическия слой превръщат всички тези 0-ли и 1-ци в електрически импулси или светлинни импулси.

Физическият слой се занимава с проблемите, свързани с *предаването на сигнали*, а именно:

- Аналогово или цифрово предаване на сигнали
- Теснолентова или широколентова технология на предаване
- Асинхронно или синхронно предаване
- Мултиплексиране

В Глава 4 ще разгледаме детайлно методите за предаване на сигнали и техните характеристики.

Друг проблем, решаван от физическия слой, е мрежовата топология. Във физическия слой това се отнася за физическото разположение на мрежата, за разлика от логическата топология, която се определя в каналния слой. Може би си спомняте от Глава 2, че най-известните LAN топологии са линейната шина, шината звезда, кръгът и решетката.

Устройствата от физическия слой са тези, които осъществяват основното предаване на сигнали. Мрежовите интерфейсни карти работят във физическия слой както повторителите и хъбовете. Тези хъбове са хъб за мрежа Token Ring, който се означава като *устройство за множествен достъп* (MSAU), и пасивните, активните и интелигентните хъбове. Тук не влизат *комутиращите хъбове*, които действат в каналния слой. (Понякога „MSAU“ се записва като „MAU“).

Мрежови интерфейсни карти (NIC) Мрежовата интерфейсна карта (NIC) е основен компонент, който най-общо се използва за изграждане на комуникация между компютри. Казвам „най-общо“, защото има ситуации, при които даден компютър може да участва в мрежа и без NIC. Такива случаи са *отдалеченият*

достъп (remote access), в който се използват модем и телефонни линии за свързване към мрежата, и простата връзка между два компютъра с помощта на специален сериен кабел, наречен *нулев модем*. Мрежовите карти отговорят за подготвяне на данните, които трябва да бъдат предадени по мрежовата преносна среда.

Мрежовите интерфейсни карти се разпространяват в множество различни типове и избирането на правилната карта може да бъде предизвикателство. Когато избирате, трябва да се съобразите със следното:

- **Архитектура на мрежата** – Картата трябва да бъде предназначена за работа с архитектурата, която използвате във вашата мрежа. Например една Token Ring карта не може да работи в Ethernet мрежа.
- **Тип на преносната среда (медията)** – Ethernet мрежите могат да използват тънък коаксиален кабел, кабел с усукана двойка и дори кабел с оптично влакно. Вашата карта трябва да има правилен тип конектор, за да може да бъде свързана към преносната среда на вашата мрежа. (Ако имате безжична конекция, картата трябва да бъде предназначена за съответния тип безжична комуникация – инфрачервена, лазерна или радио.)
- **Архитектура на шината** – Картата трябва да бъде предназначена за работа с архитектурата, използвана на вашия компютър. Трябва да имате съответния тип шина и интерфейс от тип PCI, ISA или PC card, за да може картата да работи в компютъра.

ЗАБЕЛЕЖКА Също така е възможно, а често и желателно, да си купите комбинирана карта, която има конектори за два или дори три типа Ethernet кабели. Това е особено удобно, ако очаквате ъпгрейд на вашата thinnet мрежа например към UTP.

- **Скорост** – Ethernet мрежа, работеща по кабел Cat 5 с неекранирана усукана двойка, може да бъде пусната на скорости 10 Mbps или 100 Mbps. Token Ring мрежа, използваща IBM кабел, може да бъде пусната на 4 Mbps или на 16 Mbps. Трябва да поддържате съответствие между скоростта на картата и останалите мрежови компоненти.

ЗАБЕЛЕЖКА Ethernet картите с конектори за UTP се разпространяват във версии със скорости 10 Mbps, 100 Mbps и 10/100 Mbps. Макар и по-скъп, вариантът 10/100 Mbps има очевидни предимства. Обърнете внимание, че ако вашият хъб поддържа 100 Mbps, с него можете да използвате карти на 100 Mbps или на 10/100 Mbps, но картата с 10 Mbps няма да работи.

Мрежови приемопредаватели Приемопредавателят (трансивърът) се наричан така, защото е устройство, което предава и приема. Мрежата 10Base5 (thicknet) използва *външен приемопредавател*, представляващ устройство, свързано към мрежовата интерфейсна карта чрез AUI конектор (наричан също DIX конектор). AUI конекторът, който е от 15-изводен DIN тип, позволява конвертирането на различните типове преносни среди чрез свързване на външния приемопредавател за желания тип кабел.

Всички мрежови карти използват приемопредавател, който се вгражда в картите, предназначени за използване в мрежи 10Base2, 10BaseT или 100BaseT.

Повторители Повторителят свързва две дължини (два сегмента) на мрежовия кабел и усилва сигнала, предавайки го от първия към втория кабелен сегмент. Повторителят ви позволява да увеличите дължината на мрежовия кабел повече, отколкото е възможно по друг начин, като решите проблема със затихването (загубата на сигнала), което възниква при увеличаване на разстоянието.

Повторителите не филтрират сигналите. Те предават както данните, така и шума. Ето защо могат да бъдат използвани само ограничен брой повторители; в противен случай възникват проблеми в комуникацията. Използването на повторители в мрежа с коаксиален кабел се установява с помощта на правилото 5-4-3, което ще разгледаме в Глава 5, „LAN връзки“, в секцията „Правила за изграждане на Ethernet“.

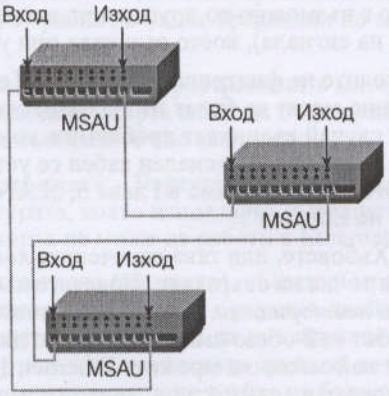
Хъбове Хъбовете, или така наречените *концентратори*, служат като точка на централна точка на свързване. Повечето хъбове реално представляват *множествени повторители*. Докато един повторител обикновено има само два порта, хъбът най-общо има от четири до двадесет и повече порта. Хъбовете се използват най-масово в мрежите Ethernet, 10BaseT или 100BaseT, макара че има и други мрежови архитектури, които ги използват.

Хъбовете се разпространяват в три основни типа:

- **Пасивни** – Пасивният хъб служи само като точка за физическо свързване. Той не се нуждае от електрическо захранване, защото той не усилва и не изчиства сигнала, а просто го препредава. Днес пасивните хъбове не са много разпространени.
- **Активни** – Активният хъб трябва да бъде включен към електрическо захранване, защото използва енергия за усилване на входния сигнал, преди да го предаде обратно до другите портове. Активният хъб е многопортов повторител и е най-често срещания тип хъб. Обърнете внимание, че всички Ethernet хъбове изискват електрическо захранване и поради това се класифицират като активни хъбове.
- **Интелигентни или „smart“** – Тези устройства функционират като активни хъбове, но включват също микропроцесорен чип и диагностични възможности. Те са по-скъпи от активните хъбове (без допълнителни възможности), но могат да бъдат полезни в ситуации на отстраняване на неизправности.

Друго специално устройство, което често се означава като Token Ring хъб, реално е устройството за множествен достъп – MSAU. Уникалната възможност на MSAU е логическата кръгова топология, която то създава благодарение на връзките вътре в самото устройство. Няколко MSAU устройства могат да бъдат свързани за осигуряване на непрекъснат кръгов път, по който да пътува сигналът, както е показано на Фигура 3-5.

Фигура 3-5 *MSAU устройствата, свързани в Token Ring мрежа, осигуряват непрекъснат кръгов път за данните.*



Моделът DoD

Макар че OSI моделът е най-популярен, той не е единственият, нито първият модел за изграждане на мрежи. Факт е, че моделът на Министерството на отбраната на САЩ (Department of Defense – DoD) – понякога означаван като TCP/IP модел – беше разработен около десет години по-рано от OSI модела, през 70-те години на миналия век.

Моделът на DoD беше разработен в сътрудничество със самия TCP/IP – част от проекта ARPAnet. Той е по-прост модел, състоящ се само от четири слоя, които могат да бъдат приблизително асоциирани със седемте слоя на OSI модела. Както виждате на Фигура 3-6, най-горният и най-долният слой на модела DoD комбинират функциите на повече от един OSI слой.

Функцията на всеки слой е следната:

- **Слой приложение/процес (application/process layer)** – Най-горният слой на модела DoD, който обхваща функциите на трите най-горни слоя на OSI модела: приложен, представителен и сесиен. В текстовете, отнасящи се за TCP/IP, може да прочетете, че криптирането на данните и контролът на диалога се осъществяват в приложния слой. Ако запомните, че това *не* означава приложния слой на OSI модела, ще избегнете объркването.
- **Слой хост до хост (транспортен слой) (host to host (transport) layer)** – В някои източници слоят хост до хост се означава като транспортен слой, дори в четирислойни диаграми на DoD, и съответства на транспортния слой от OSI модела. Тук функционират TCP, UDP и DNS.
- **Слой интермрежа (internetworking layer)** – Този слой съответства много близко на мрежовия слой на OSI. Той се занимава с маршрутизация, базирана на логически адреси. Протоколът Address Resolution Protocol (ARP) транслира логическите адреси в MAC адреси. Тази транслация е необходима, защото по-долните слоеве могат да обработват само MAC адресите.

- **Слой мрежов интерфейс (network interface layer)** – Слоят мрежов интерфейс съответства на двата слоя – канален и физически – от референтния модел OSI. В този слой работят стандартните Ethernet и Token Ring протоколи от каналния слой и физическия слой.

Фигура 3-6 *Четирите слоя на модела DoD са показани по начина, по който те съответстват на слоевете от референтния OSI модел.*

Една от целите на ISO при разработката на OSI модела беше по-конкретно да дефинира мрежовите функции, определени от DoD модела при създаване на TCP/IP. Но TCP/IP протоколите бяха проектирани по DoD модела, а не по OSI модела.

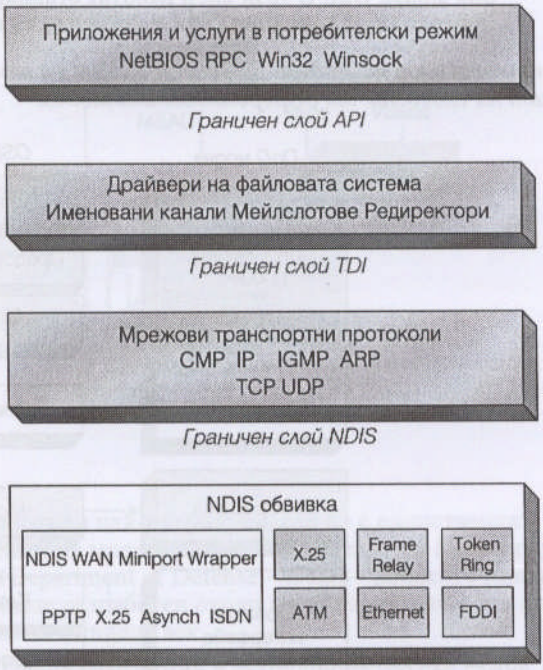
Специфични за производителите модели

Производители на софтуер за мрежови операционни системи могат да имат техни собствени мрежови модели, за да опишат начина, по който работят компонентите на мрежовата операционна система. Например мрежовият модел на Microsoft Windows за NT и Windows 2000 е показан на Фигура 3-7.

Както виждате, моделът на Microsoft трудно може да бъде асоцииран директно с другите модели. Той включва нов тип слой, наречен *граничен слой*, който представлява интерфейс между действителните слоеве от мрежови компоненти. Граничните слоеве представляват отворени спецификации, докато компонентните слоеве между тях са специфични за конкретната операционна система.

Други производители на мрежови операционни системи имат техни собствени модели, но OSI моделът е стандарт, с който всички те са съвместими.

Фигура 3-7 *Microsoft разработи свой собствен модел за мрежови комуникации, предназначен за изграждането на Windows мрежи.*



Мрежови стандарти и спецификации

Моделите не са единствените стандарти и спецификации, по които се разработват мрежови компоненти. Множество организации за стандартизация публикуват спецификации за свързан с мрежите хардуер и софтуер. Разбира се, тези спецификации не са *закон*. Организациите по стандартизация не са правителствени институции и не могат да налагат задължително съответствие към дадени стандарти. Производителят е свободен да се отклонява от стандартите толкова, колкото желае, но не е в негов интерес да прави това. Нестандартни продукти, които работят само с други продукти, произведени от същия производител, по принцип са непопулярни. В ранните дни на компютърните мрежи производителите безнаказано създаваха такива продукти, но днешната мрежова индустрия изисква съвместимост.

Защо трябва да се спазват стандарти?

ISO (www.iso.ch) дефинира стандартите като „документирани споразумения, съдържащи технически спецификации или други точни критерии, които трябва да бъдат използвани задължително като правила, указания или дефиниции на характеристики, за да гарантират, че дадени материали, продукти, процеси и услуги отговарят на целта, за която са предназначени".

Пазарът, както разбрахте, е една от причините производителите да спазват стандартите, но има и други предимства. Например стандартите осигуряват

указания, които улесняват проектирането и производството на продукти, а от гледна точка на потребителя стандартизацията осигурява надеждност на продуктите и услугите.

Организации за стандартизация

ISO съществува от дълго време и е добре позната организация за стандартизация, но тя не е единствената организация, която осигурява стандартизирани спецификации за компютърни и мрежови компоненти. Някои от главните международни организации за стандартизация са следните, разгледани в следващите секции по азбучен ред:

- ISO
- IEC
- ITU
- IETF
- IEEE

ISO

ISO е световна федерация на националните организации по стандартизация, с по един представител от всичките 100 различни страни. Тя е формирана през 1947 г. с цел разработване на международни стандарти в различни сфери. Един от стандартите на ISO, който много хора са виждали през годините, е ISO номерът на кутийката на фотографските филми, който показва скоростта на филма. Международните буквени кодове на страните са друг пример на работата на ISO.

ISO работи в партньорство с други организации, като International Electrotechnical Commission (IEC), World Trade Commission (WTO) и International Telecommunications Union (ITU).

Повече информация за ISO е достъпна на официалния сайт на ISO – www.iso.ch.

IEC

IEC съществува дълго преди ISO, още от 1906 г., но е по-специализирана. Докато ISO създава стандарти от всички видове, целта на IEC е създаването и установяването на стандарти в областта на електро- и електронния инженеринг.

IEC е изградена от 47 национални комитета и през 1967 г. влезе в споразумение за съвместна работа с ISO по разработката на стандарти и спецификации.

Web сайтът на IEC може да бъде посетен на адрес www.hike.te.chiba-u.ac.jp/ikeda/IEC/home.html.

ITU

ITU е друга международна организация, усилията на която са съсредоточени върху спонсорирането на събития, публикуването на документи и установяването на стандарти за продукти и услуги, свързани с телекомуникациите.

Web сайтът на ITU – www.itu.int – съдържа информация за структурата и дейностите на организацията.

IETF

Internet Engineering Task Force (IETF) е част от Internet Architecture Board (IAB), който от своя страна е техническа консултативна група, принадлежаща на Internet Society (ISOC).

IETF е разделена на две *работни групи*, всяка от които решава различен проблем, свързан с изграждането на Интернет стандарти. Членството в нея е отворено; всяка заинтересована страна може да се присъедини към тази организация.

Основната задача на групите на IETF включва разработката и издаването на Интернет проекти (Internet Drafts), прерастващи в официални документи (Request For Comments – IRFC), които от своя страна преминават през установен процес на одобрение, за да се превърнат в Интернет стандарти.

RFC и Интернет стандарти

В качеството си на професионалисти по мрежи може да срещнете препратки към „RFC [номер]" за повече информация по характеристиките на определени мрежови услуги и протоколи. Тези услуги и протоколи включват такива елементи, като:

- Реализация на услугата Domain Name System (DNS)
- Разширения на TCP/IP
- Спецификации за софтуер от типа Network Address Translation (NAT)

Макар че много RFC документи произлизат от IETF, всяка заинтересована страна може да подава предложения за RFC. Не всички RFC документи описват стандарти, но ако даден документ е предназначен за стандарт, той преминава през три фази:

- Proposed Standard – предложен стандарт
- Draft Standard – пробен (проектен) стандарт
- Internet Standard – Интернет стандарт

Има дори RFC номер 2226 – „Инструкции за автори", който съдържа информация за начина на написване и форматиране на проект. След като бъде изпратен, групата Internet Engineering Steering Group (IESG), която е част от IETF, разглежда документа. За повече информация за този процес вижте Web сайта на IETF на адрес www.ietf.org/home.html.

След обсъждането, ако проектът бъде одобрен, той се редактира и публикува. Редакторът на RFC, назначен от Internet Society, поддържа и публикува главен списък на RFC документите. Той отговаря също за окончателното редактиране на документите. Началната страница на RFC редакторите се намира на адрес www.rfe-editor.org.

Следва преглед от техническите експерти или така наречената група „task force", по време на който RFC се класифицира в една от следните категории:

- **Required Status (изискван статут)** – Задължителен
- **Recommended Status (препоръчителен статут)** – Препоръчителен
- **Elective Status (незадължителен статут)** – Може да бъде реализиран, но реализацията не е задължителна

- **Limited Use Status (статут на ограничено използване)** – Не е предназначен за масова реализация
- **Not Recommended Status (непрепоръчван статут)** – Не се препоръчва реализация

Ако искате още информация за изпращането на RFC и процеса на одобряване, можете да свалите RFC 2026 от ftp://ftp.isi.edu/in-notes/rfc2026.txt.

IEEE

IEEE (наричан на английски „Ай-трипъл И“ от членовете на индустрията) осигурява обмена на информация и разработва стандарти и спецификации за ниско ниво на мрежовите технологии (това на физическия и каналния слой).

От особен интерес за професионалистите по мрежи представляват спецификациите на проекта IEEE 802. Името е базирано на датата на заседанието на комитета. 80 означава годината (1980), а 2 означава месеца (февруари). Протоколите от физическия и каналния слой, за които комитетът установява стандартите 802, са следните:

- **802.1** – Въведение в стандартите: LAN и MAN мениджмънт, мостове, които действат в MAC подслоя и алгоритъмът STA (Spanning-Tree Algorithm), който предотвратява комуникационни проблеми, наречени *междумостово зацикляне* (*bridge looping*).
- **802.2** – Logical Link Control (LLC): Тези спецификации бяха предназначени за недопускане на затрупване на приемниците от изпращащите. Този стандарт се грижи за разделянето на каналния OSI слой на два подслоя, при което слоят LLC осигурява интерфейс между MAC подслоя и мрежовия слой.
- **802.3** – CSMA/CD: Тази спецификация установява правилата за работа на Ethernet мрежи, използващи метода на множествен достъп с разпознаване на носещата (честота) и откриване на колизии (CSMA/CD), и установяват стандарти за формата на Ethernet фреймовете (пакетите). Първоначално стандартът бе дефиниран като мрежа с линейно-шинна топология, използваща коаксиален кабел, но след това бе обновен за включване на 10BaseT мрежи (топология звезда).
- **802.4** – Token Bus: Задава стандарти за мрежи, реализиращи физическа и логическа шинна топология, която използва 75-омов CATV коаксиален или оптичен кабел и метод за достъп с предаване на маркер.
- **802.5** – Token Ring: Тази спецификация задава физическия стандарт и метод за достъп до преносната среда за мрежа с физическа топология звезда и логически кръг, която може да използва кабел с екранирана или неекранирана усукана двойка и метод на достъп с предаване на маркер. Този стандарт беше разработен на базата на технологията Token Ring на IBM.
- **802.6** – MAN: Задава стандарти за мрежи, които са по-големи от локалните мрежи и по-малки от глобалните мрежи.
- **802.7** – Broadband: Установява правилата за изграждане на мрежи с технологии за широколентово предаване, например CATV, използващи Frequency Division Multiplexing (FDM) за изпращане на различни сигнали на отделни честоти по един и същ кабел.

- **802.8** – Fiber Optics: Осигурява спецификации за мрежи, използващи оптични кабели – например Fiber Distributed Data Interface (FDDI).
- **802.9** – Integrated Voice and Data: Понякога наричан само „integrated services“ (вградени услуги), този стандарт установява правилата за предаване на глас и данни по ISDN.
- **802.10** – LAN Security: Тези спецификации имат отношение към изграждането на виртуални частни мрежи (VPN) – начин за изграждане на сигурна връзка към частна мрежа по обществения Интернет.
- **802.11** – Wireless: Дава указания за реализиране на безжични (безкабелни) LAN технологии.
- **802.12** – 100 VG AnyLAN: Този стандарт се отнася за метода на достъп с приоритет по заявка, разработен от Hewlett Packard с цел комбиниране на предимствата на Ethernet, Token Ring и ATM технологиите в едно високоскоростно решение за локални мрежи.

IEEE може да бъде намерен онлайн (включително каталог на неговите стандарти, достъпни за абониране) на адрес standards.ieee.org.

Обобщение

В тази глава обхванахме накратко повечето от концепциите, свързани с компютърните мрежи. Започнахме с основните принципи на компютърната комуникация, сравнявайки двоичната, шестнадесетичната и десетичната бройни системи, за да разберем защо двоичният машинен език е най-подходящ за начина, по който компютрите обработват данни. Научихте, че за да бъдат предадени по мрежата, данните се разделят на малки управляеми парчета; освен това разгледахме как слоестият подход за мрежови комуникации опростява процеса и поддържа целостта на предаваната информация.

Изучихме целите и приложенията на мрежовите модели и дадохме съответствието между четирите слоя на DoD модела към седемте слоя на OSI версията. След това представихме предимствата от стандартизацията в света на мрежите и разгледахме някои конкретни стандарти, например RFC документите и спецификациите на проекта 802, които вероятно ще срещате често при изучаване на технологиите на компютърните мрежи.

В следващата глава се връщаме обратно към източника; т.е. ще изследваме сигнала, който представя предаваните данни. Ще научим за типовете предавани сигнали и техните характеристики, а след това ще разгледаме методите за достъп до преносната среда и начините, по които всичките тези сигнали, предавани от множество компютри по мрежата, избягват превръщането на всичко това в едно огромно електронно задръстване на трафика.

Допълнителни източници

За по-задълбочено разглеждане на двоичните и шестнадесетичните изчисления вижте „A Practical Guide to Birtary, Decimal and Hexadecimal Numbers“ на адрес www.myhome.org/pg/numbers.html.

World Standards Services Network (WSSN) е мрежа от обществено достъпни сървъри в World Wide Web, принадлежащи на организации за стандартизация по целия свят. За повече информация посетете www.wssn.net/WSSN.

Хубаво кратко ръководство за OSI модела, заедно с тест, може да намерите на www.lex-con.com/osimodel.htm.

Диаграма на съответствието между протоколите и OSI модела може да бъде намерена на www.lex-con.com/osimodel.htm.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Какво е името на бройната система, която използва 16 цифри за представяне на числови стойности?

- **a** Десетична
- **b** Шестнадесетична
- **c** Двоична
- **d** Машинен код

2 Как се нарича двоичната цифра (самостоятелна 0 или 1)?

- **a** Бит
- **b** Байт
- **c** Кубит
- **d** Гиг

3 Кое от следните е десетичният еквивалент на двоично число 10010001?

- **a** 256
- **b** 128
- **c** 145
- **d** 64

4 Какво е името на малките, лесно предаваеми единици, на които се разделят компютърните данни за предаване по мрежата?

- **a** Хексадецимали
- **b** Пакети
- **c** Хедъри
- **d** Битове

5 Какво е името на компонента за проверка за грешки, който понякога бива включван в трейлъра на пакета с данни?

- **a** Бит за верификация
- **b** Фрейм
- **c** UDP
- **d** CRC

6 „Схематично описание на система, теория или явление, което представя нейни познати или предполагаеми свойства и може да бъде използвано за допълнително изучаване на нейните характеристики“ е дефиниция на кое от следните?

a Протокол
b Модел
c Процес
d Слой

7 Кой слой на OSI модела е разделен на два подслоя?

a Физическият
b Каналният
c Мрежовият
d Транспортният

8 Кой слой на OSI модела не добавя хедър информация към пакета данни, докато пакетът пътува надолу в стека от слоеве?

a Физическият слой
b Каналният слой
c Сесийният слой
d Приложният слой

9 Кой от следните е протокол от сесийния слой?

a TCP
b IPX
c NetBIOS
d Telnet

10 Какво е другото име на множествения повторител?

a Мост
b Маршрутизатор
c Суич
d Хъб

Глава 4

Методи за комуникация по мрежи

Дотук в книгата направихме обширен преглед на начините на свързване на компютрите за комуникация един с друг. Сега знаете как компютрите обработват информация в двоичен формат, а също и че двоичните цифри се трансформират в електронни сигнали, за да отпътуват по преносната среда на мрежата. В тази глава ще навлезем по-дълбоко в сърцевината на мрежовата комуникация — в самия сигнал. След това ще изучим методите, използвани в различните мрежови архитектури за управление на достъпа до преносната среда.

Методи на предаване на сигнали и характеристики

Както беше отбелязано преди, съществуват много начини, по които сигналът може да бъде създаден физически: като електрически импулси, пътуващи по меден проводник, като светлинни импулси, които пътуват по влакна от стъкло или пластмаса, като радиопредавания, които се пренасят по радиовълни, като лазерни или сателитни предавания и като инфрачервени импулси. Когато единиците и нулите, представляващи компютърните данни, се превръщат в електроимпулси, те биват кодирани или модулирани.

Подобно на категоризацията на мрежите по различни начини, можем да категоризираме кодираните сигнали в зависимост от различни характеристики, а именно:

- Аналогови или цифрови
- Теснолентови или широколентови
- Синхронни или асинхронни
- Симплекс, полудуплекс, пълен дуплекс или мултиплексни

В следващите секции ще разгледаме всеки от изброените типове сигнали.

Аналогови и цифрови

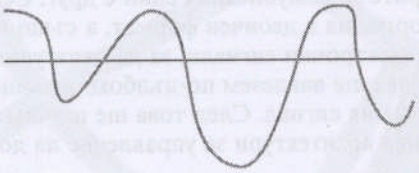
Методите за предаване на сигнали се класифицират на аналогови или цифрови, които представляват две много различни форми на кодиране. Вероятно сте запознати с тези термини от домашните електронни уреди, като магнетофони, стерео приемници и телевизионни тунери.

Условно може да приемете, че аналоговото оборудване е старият стил, а цифровото е новият стил в електронната индустрия. Помнете, че единият тип предаване на сигнали не е задължително по-добър от другия; всеки има своите предимства и недостатъци, и всеки е подходящ за определени типове предавания. Малко вероятно е цифровото предаване на сигнали някога напълно да замени аналоговото, макар че цифровите технологии определено добиват популярност.

Характеристики на аналоговото предаване на сигнали

Аналоговите сигнали могат да бъдат илюстрирани графично като вълнови форми, защото те се променят плавно и непрекъснато. Фигура 4-1 представя графика на аналогов сигнал.

Фигура 4-1 *Аналоговият сигнал представлява електромагнитна вълна, която се променя постоянно.*



Много процеси са аналогови по своята природа. Гласовите вълни например са аналогови, защото тонът и височината варират плавно по пътя на вълната. За допълнително разширяване на примера за аналогова информация, представете си традиционния уред за измерване на скоростта на автомобила. Когато повишавате скоростта на колата, стрелката се премества плавно от едно число към следващото. Друг пример са старите радиоприемници. Когато преместите стрелката на честотната скála от една станция към следващата, радиопредаването между станциите се нарушава от статични или слаби сигнали.

Аналоговите сигнали се измерват в *цикли*, при което един цикъл представлява промяната от висок към нисък и след това отново към висок сигнал (или обратно). Измерват се следните три характеристики:

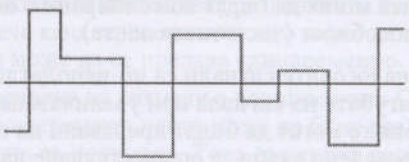
- **Амплитуда** – Силата на сигнала, представена от височината на вълната.
- **Честота** – Времето, необходимо на вълната да изпълни цикъла. Честотата се измерва в *херци* (цикли в секунда).
- **Фаза** – Относителното състояние на една вълна спрямо друга, измерено в *градуси*.

Както виждате, аналоговото предаване на сигнали е доста сложно.

Характеристики на цифровото предаване на сигнали

Цифровото предаване на сигнали се нарича също *дискретно* предаване на сигнали. Цифровите сигнали се променят от едно състояние в друго мигновено, без да спират на някакво междинно състояние. Фигура 4-2 илюстрира цифровото предаване на сигнали.

Фигура 4-2 *Цифровото предаване на сигнали представлява фиксирани, дискретни сигнали.*



Като пример на цифрова информация си представете новите радио тунери, в които въвеждате точното число на честотата за достъп до дадена станция. Друг пример на цифрова информация са LED или LCD дисплеите за скоростта, които се монтират в някои нови автомобили, в които милите или километрите в час се показват в цели числа.

Сравнение между аналогови и цифрови сигнали

Компютрите представляват цифрови машини. Информацията, която те обработват, се базира на единици и нули. Една двоична цифра (бит) е 1 или 0 и няма други междинни стойности. Ето защо цифровото предаване на сигнали често пъти е по-подходящ формат за предаване на компютърни данни, затова повечето мрежи използват методите на цифровото предаване на сигнали.

ЗАБЕЛЕЖКА Интересно е, че информацията, която по природа е аналогова, може да бъде представена цифрово, и обратно. За илюстрация нека да се върнем на примера за скоростомера. Обърнете внимание, че скоростта на колата не преминава директно от 51 km/h на 52 km/h; тя се увеличава плавно. Но скоростомерът от нов стил пропуска частичните междинни увеличения и показва информацията в цифров формат.

За разлика от това, електроенцефалографът (EEG) осигурява информация за мозъчните вълни в аналогов формат. Но този уред реално представя дискретни (отделни) състояния на невроните в мозъка, които в даден момент са или включени, или изключени.

Цифровото предаване на сигнали очевидно е по-просто от аналоговото. За да илюстрираме това твърдение, представете си, че се явявате на изпит. Въпросите от типа „истина или неистина“ и тези с множество отговори за избор представляват въпроси с дискретни състояния; отговорът е или истина, или неистина, или пък е A, B, C или D. Въпросът, свързан с написване на есе, прилича повече на аналогов въпрос. Вашият отговор може да бъде напълно неправилен, напълно правилен или нещо между двете.

Тъй като представлява по-проста технология, цифровото предаване на сигнали има някои предимства пред аналоговото:

- Най-общо създаването на цифрово оборудване е по-евтино и затова цифровите часовници струват по-малко от аналоговите.
- Цифровите сигнали като цяло са по-малко уязвими към грешки, предизвикани от смущения. Дискретното състояние включено или изключено не се влияе толкова лесно от малко изкривяване, както непрекъснатата вълнова форма.

Аналоговите сигнали имат следните предимства:

- Аналоговите сигнали могат лесно да бъдат *мултиплексирани*; т.е. сигналите могат да бъдат комбинирани с цел увеличаване на пропускателната способност (честотната лента).
- Аналоговите сигнали са по-неподатливи към проблема на *затихването* (загубата на сигнала при увеличаване на разстоянието на предаване), затова те могат да бъдат предавани на по-далечни разстояния, без да стават прекалено слаби за осъществяване на надеждно предаване.

И аналоговото и цифровото предаване на сигнали е полезно. Решенията с цифрова връзка като цяло предлагат по-добра сигурност, по-висока производителност и по-висока надеждност. Наред с това цифровите линии са по-малко предразположени към грешки в сравнение с аналоговите.

Локалните мрежи по принцип разчитат на кабели, по които се предават цифрови сигнали. Някои технологии използват методи за аналогово предаване на сигнали. Една трета технология на предаване, използвана за изграждане на глобални мрежи, която ще разгледаме в Глава 6, „WAN връзки“, е *комутирането на пакети*.

Теснолентови и широколентови

Друг въпрос на предаването на сигнали се отнася до начина на използване на честотната лента по мрежовата преносна среда. *Честотната лента* най-общо се отнася до скоростта или капацитета на мрежовата връзка. Например целият капацитет на Ethernet кабела се използва за предаване на данните по един канал. Поради това Ethernet е *теснолентова* технология.

ЗАБЕЛЕЖКА *Каналът* представлява запазена част от достъпната честотна лента на преносната среда, която може да бъде използвана за предаване.

Можете да разделяте честотната лента на множество канали и да изпращате различни потоци от данни по всеки канал. За пример можем да дадем кабелната телевизия (CATV), при която десетки отделни канали, всеки от тях с различна програма, се доставят до вашия телевизор по коаксиален кабел. CATV е широколентова технология.

Характеристики на теснолентовата технология

Теснолентовото предаване е просто – в даден момент по кабела се предава един сигнал. Този сигнал се възползва от предимството да притежава цялата честотна лента само за себе си. Теснолентовото предаване обикновено се асоциира с цифрово предаване на сигнали (макар че може да бъде използвано и при аналоговото).

Повечето компютърни комуникации са теснолентови; например фóрмата на сигнала, предаван от компютър към монитори, принтери и други периферни устройства, е теснолентова, защото това са аналогови комуникации. От друга страна ISDN е широколентов, защото множество сигнали могат да бъдат пренасяни по отделни канала в един и същ кабел. Теснолентовото предаване на сигнали е двупосочно; сигналът може да протича и в двете посоки, така че е възможно да предавате и приемате по един и същ кабел.

Характеристики на широколентовата технология

Широколентовите технологии позволяват разделянето на капацитета на дадена връзка на два или повече канала, всеки от които може да пренася различен сигнал. По всички канали може да се предава едновременно.

Широколентовото предаване на сигнали е еднопосочно. Сигналите протичат само в една посока, но честотната лента може да бъде разделена на два канала – един за предаване и един за приемане. Това се нарича разпределена по равно (midsplit) широколентова конфигурация. Друга опция е свързването на два отделни кабела към устройството и използване на единия за предаване на сигнали, а другия за приемане.

Освен в CATV, широколентовите технологии включват телефонната услуга Digital Subscriber Line (DSL), при която данни и глас могат да бъдат пренасяни едновременно по една и съща линия, сателит и други безжични технологии.

За разделяне на честотната лента се използва *мултиплексиране*, както е описано в следващата секция.

Мултиплексиране

Мултиплексирането е метод за едновременно изпращане на различни потоци от информация по дадена връзка под формата на един сложен сигнал. След това на приемния край отделните потоци се възстановяват в начално състояние. Връщайки се към нашия пример на предаванията по CATV, един CATV тунер, вграден в телевизора или в кабелна кутия, която декодира сигналите, ви позволява да избирате канала, който искате да гледате.

Макар че някои книги за мрежи асоциират мултиплексирането само с предаването на аналогови сигнали, и аналоговите, и цифровите сигнали могат да бъдат мултиплексирани. Мултиплексирането може да бъде постигнато с помощта на следните методи:

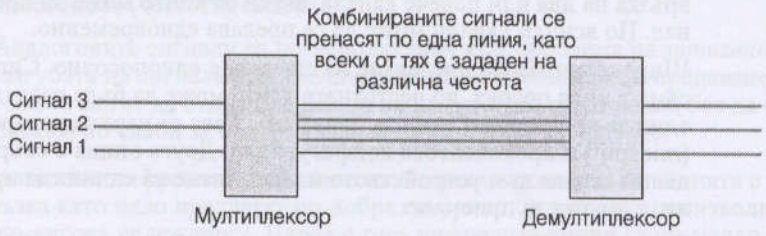
- Мултиплексиране чрез разделяне по честота (Frequency-division multiplexing – FDM)
- Мултиплексиране чрез времеделение (Time-division multiplexing – TDM)
- Мултиплексиране чрез разделяне по дължината на вълната с висока плътност (Dense wavelength division multiplexing – DWDM)

В следващите секции ще разгледаме всеки от тези методи.

FDM

Аналоговите сигнали обикновено се мултиплексират по метода FDM. По една линия за предаване се комбинират множество сигнали и за всеки канал се задава различна честота (лента). Една двупосочна комуникационна верига изисква наличието на мултиплексор/демултиплексор на всеки край, както е показано на Фигура 4-3.

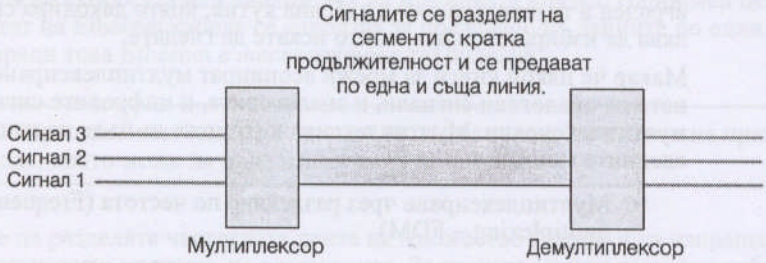
Фигура 4-3 *При FDM на всеки канал се задава отделна честота и всички честоти се комбинират за предаване по една линия.*



TDM

Цифровите сигнали обикновено използват мултиплексиране с времеделение (TDM). Този метод комбинира сигналите за предаване по една комуникационна линия и разделя всеки сигнал на сегменти с кратка продължителност. След това сигналите се пренасят по линията в редуващи се времеви слотове, един след друг. От другия край те се отделят в оригиналната си форма от демултиплексор, както е показано на Фигура 4-4.

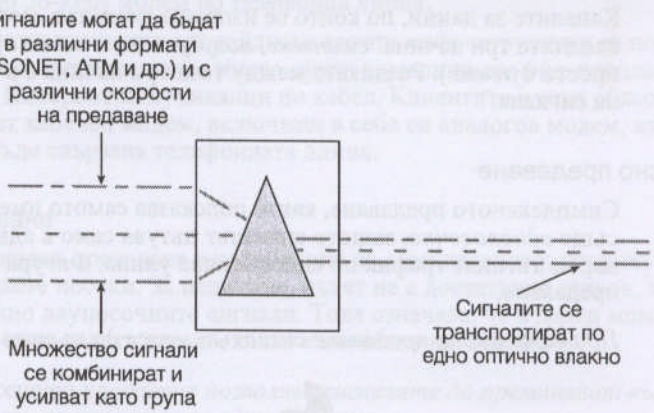
Фигура 4-4 *TDM разделя всеки сигнал на сегменти с кратка продължителност и предава всички сегменти по една линия.*



DWDM

Мрежи, които работят с кабели с оптични влакна, могат да използват още един тип мултиплексиране –DWDM. При DWDM всеки сигнал се пренася с отделна дължина на светлинната вълна. Различни формати данни (например SONET и ATM) могат да пътуват едновременно по един и същ оптичен кабел, както е показано на Фигура 4-5.

Фигура 4-5 *DWDM пренася всеки сигнал на отделна дължина на вълната на светлината.*



Асинхронно и синхронно предаване

Спомнете си, че данните, които се кодират като аналогови или цифрови, зависят от промените в състоянието (т.е. модулациите) за представяне на двоични данни. За да интерпретира правилно сигналите, приемащото мрежово устройство трябва точно да знае кога трябва да бъде измерен сигналът. Синхронизирането в мрежата, както и в много други аспекти на живота, е много важно.

При работа в компютърни мрежи този синхронизиращ фактор се нарича *побитова синхронизация*. Устройствата могат да синхронизират битовете с помощта на асинхронен метод или синхронен метод, както е описано в следващите секции.

Характеристики на асинхронното предаване

Асинхронните предавания използват *старт бит* в началото на всяко съобщение. Когато приемащото устройство приема старт бита, то може да синхронизира своя вътрешен тактов генератор с тактовия генератор на предаващото устройство.

Характеристики на синхронното предаване

При синхронните предавания един вграден механизъм за тактуване координира тактовете на предавателя и приемника. Например тактовата информация може да бъде вградена в сигнала с данните. Това се нарича синхронизация с *гарантирана промяна на състоянието* и е по-широко разпространен тип от синхронните методи.

Други два синхронни метода на предаване са *отделният тактов сигнал*, при който съществува отделен канал между предавателя и приемника за предаване на тактовата информация, и *овърсемплинг*, при който приемащото устройство семплира сигнала с много по-бърза скорост от тази, с която се изпращат данните. То прави това с помощта на допълнителни измервания, за да определи дали тактовете са синхронизирани.

Симплексно, полудуплексно и пълнодуплексно предаване

Каналите за данни, по които се изпраща сигналът, могат да работят по един от следните три начина: *симплекс, полудуплекс* и *пълен дуплекс* (често наричано просто *дуплекс*). Разликата между тези три начина е в посоката на преминаване на сигнала.

Симплексно предаване

Симплексното предаване, както подсказва самото име, е просто. То се нарича също *еднопосочно*, защото сигналът пътува само в една посока, точно както върви пътният трафик по еднопосочна улица. Фигура 4-6 илюстрира този тип предаване.

Фигура 4-6 *При симплексно предаване сигналът може да пътува само в една посока.*

Телевизионното предаване е пример за симплексна комуникация. Данните (т.е. телевизионните програми) се изпращат на вашия телевизор. Не се предават никакви сигнали обратно от телевизора към телевизионния предавател или кабелната компания. Ето защо телевизорът е *приемник,* но не и *предавател.*

Тъй като традиционните телевизионни предавания (преди разработването на технологиите за интерактивна телевизия) нямаха необходимост от двупосочна комуникация, оборудването на много кабелни компании поддържа само симплексни предавания. Когато беше разработен кабелният Интернет достъп, това се превърна в проблем. Вече съществуваше възможността за предаване на сигнали *надолу* към потребителя, но нямаше начин потребителят да *качва* (да предава *нагоре*) данни.

Този недостиг засегна например възможността на потребителя за достъп до Web сайтове, защото приложението-браузър на потребителя не можеше да изпраща малкото количество данни, за да заявява конкретна Web страница. Кабелните компании имаха два избора за решаване на този проблем:

- Да реализират технологии, които използват кабелната честотна лента за предавания надолу (низходящ поток – downstream) и телефонните линии на потребителите за предавания нагоре (възходящ поток – upstream)
- Да инсталират нова двупосочна инфраструктура

Повечето компании използваха първата опция, докато получат възможността за изпълнение на втората. При симплексен кабелен достъп потребителят използва предимствата на високоскоростната кабелна технология при *сваляне* (*down-*

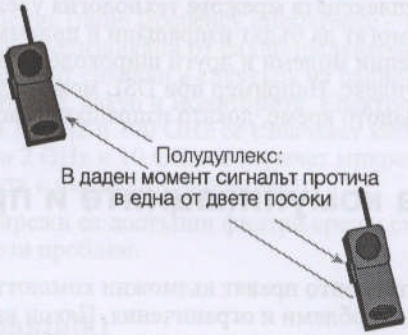
loading) на данни на неговата или нейната машина; изпращането на данните се извършва по 56-kbps модем по телефонна линия.

Много кабелни компании ъпгрейднаха своите инфраструктури за поддръжка на двупосочни комуникации, но много други компании все още предлагат само низходяща Интернет комуникации по кабел. Клиентите в тези области трябва да използват кабелен модем, включващ в себе си аналогов модем, към който трябва да бъде свързана телефонната линия.

Полудуплексно предаване

Полудуплекното предаване е подобрение на симплексното; трафикът може да върви и в двете посоки. За нещастие, пътят не е достатъчно широк, за да побере едновременно двупосочните сигнали. Това означава, че в даден момент може да предава само едната страна, както е показано на Фигура 4-7.

Фигура 4-7 *Полудуплексното предаване позволява сигналите да преминават във всяка от двете посоки, но не и в двете едновременно.*



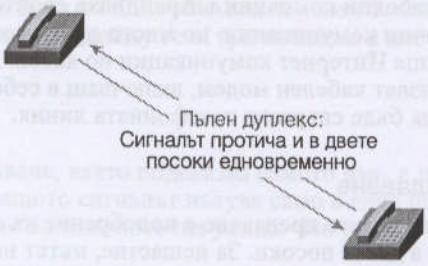
Радиостанциите на радиолюбителите и мобилните радиостанции на полицията и екипите на бърза помощ работят с полудуплексни предавания. Когато натиснете бутона на микрофона за предаване, не можете да чуете това, което се казва от другата страна. Ако хората и от двата края се опитат да говорят по едно и също време, не преминава никакво предаване.

ЗАБЕЛЕЖКА Модемите са полудуплексни устройства. Те могат да предават и приемат, но не по едно и също време. Въпреки това е възможно създаването на пълнодуплексна комуникация с модеми с помощта на две телефонни линии и два модема.

Пълнодуплексно предаване

Пълнодуплексното предаване работи подобно на двупосочна улица с две платна. Трафикът може да пътува и в двете посоки по едно и също време, както е показано на Фигура 4-8.

Фигура 4-8 *При пълнодуплексното предаване сигналите могат да пътуват и в двете посоки едновременно.*



Обикновеният телефонен разговор е пример на пълнодуплексна комуникация. И двете страни могат да говорят едновременно, и пак да чувате човека от другата страна, докато говорите (макар че има вероятност да не разберете какво точно ви казва).

Пълнодуплексната мрежова технология увеличава производителността, защото данните могат да бъдат изпращани и приемани едновременно. DSL, двупосочните кабелни модеми и други широколентови технологии работят в режим на пълен дуплекс. Например при DSL можете да сваляте данни на вашия компютър по същото време, докато изпращате гласови съобщения по линията.

Проблеми на комуникациите и предаването на сигнали

Сигналите, които правят възможни компютърните комуникации, са обект на различни проблеми и ограничения. Някои кабелни типове и методи за сигнализиране са по-предразположени към проблеми от други. Когато възникне проблем във връзката по мрежата, трябва да имате предвид следните неща.

Електромагнитни смущения

Електромагнитните смущения (electromagnetic interference – EMI) се изразяват в навлизане на външни електромагнитни сигнали, влияещи на сигнала, които се изпраща по мрежовата преносна среда. Когато външното смущение нахлуе в мрежовите сигнали, приемащите компютри трудно интерпретират сигналите. Електромагнитните смущения са подобни на проблема, който може да имате, ако слушате радиото в колата, докато преминавате през индустриална зона с голямо количество електронно оборудване. Преди това чистият канал внезапно бива заглушен от шум и припуквания, предизвикани от други сигнали, които се смесват с радиопредаването. Ето защо електромагнитните смущения понякога се означават като *шум*.

Не е задължително смущаващите сигнали да идват от източници, които бихте очаквали. Клетъчните телефони, радиостанциите и уоки-токитата работят с предаване на сигнали, но други типове електронно оборудване също излъчват безшумно, невидимо електромагнитно поле, което може да се простира на разстояние до над три километра.

Електромагнитните смущения не са проблем само за компютърните комуникации. Те са виновни и за лошо приемащите телевизори, неправилно функциони-

ращите безжични телефони, катастрофи със самолети, смъртни случаи, предизвикани от прекъсване на работата на сърдечни пулсатори и друго медицинско оборудване, и дори дълговременни ефекти, като рак или левкимия, предизвикани от електромагнитното поле, създавано от силовите кабели на електрическата компания.

Медните проводници са особени податливи към електромагнитни смущения. Дебелият външен екран на коаксиалния кабел предлага известна защита от тях, както и екраниращият материал на екранираната усукана двойка (STP). Неекранираната усукана двойка (UTP) е изключително предразположена към електромагнитни смущения, но усукването на двойката проводници във вътрешността на кабела помага за тяхното редуциране. Оптичният кабел, поради това, че използва светлинни импулси вместо електрически импулси за изпращане на сигнала, е най-добрият избор за среда с високо количество електромагнитни смущения.

Радиочестотни смущения

Радиочестотното смущение (radio frequency interference – RFI) се отнася до смущенията на сигнала, предизвикани от радиопредаватели и други типове оборудване, които генерират сигнали в спектъра на радиочестотите. Тук влизат процесорите на компютрите, както и мониторите. Електромагнитната радиация с честоти между около 10 kHz и 100 GHz се означават като радио честоти (RF). Честотите между около 2 GHz и 10 GHz се наричат микровълни (тъй като тяхната дължина на вълната е изключително малка).

За различните типове мрежи са достъпни филтри срещу смущения, предназначени за решаване на този проблем.

Смесване на сигнали (Crosstalk)

Смесването на разговори е конкретен тип смущение, при което сигналите от проводници, намиращи се на близко разстояние, се „преливат“ един в друг. Може би досега сте срещали нещо подобно, когато говорите по телефона и чувате по-тих, едва доловим разговор, който се провежда на фона на вашия разговор в момента.

Редуцирането на такова смесване на сигнали от съседни проводници е още една причина за усукването в кабелите с усукана двойка. Колкото повече усуквания има кабелът на линеен метър, толкова по-добра е защитата. Да повторим, че оптичният кабел е типът кабел, който трябва да бъде избран, ако искате да елиминирате този проблем напълно. Във вътрешността на една и съща обвивка могат да преминават множество оптични влакна, без сигналите да се смесват, защото по всяка стъклена или пластмасова нишка протичат светлинни вълни, а не електронни импулси, както при кабела с медни проводници.

Затихване

Електрическите сигнали стават все по-слаби при разпространението си по кабела; колкото по-голямо е разстоянието от източника, толкова по-слаб става сигналът. Това лесно може да бъде разбрано, ако си представите, че викате към друг човек. Ако този човек е на 1 метър, вашият глас (т.е. сигналът) е изключително силен и ясен. Но ако човекът е отдалечен на 100 метра, може би трудно

ще може да ви чуе. Терминът за изгубване на силата на сигнала се нарича *затихване (attenuation)*.

Затихването е причината в спецификациите на различните мрежови архитектури да се задават ограничения за дължината на кабела. Най-общо ограниченията гарантират, че ефектът от затихването няма да бъде толкова голям, че да предизвика значително понижаване на сигнала.

ЗАБЕЛЕЖКА Сигналът може да бъде усилен, или повишен, за да бъде увеличено максималното разрешено разстояние. За усилване на цифровите сигнали се използват *повторители*, а за същата цел при аналоговите сигнали служат усилвателите. Тези устройства ще разгледаме в Глава 7, „Физически компоненти на мрежата".

Затихването се увеличава при по-високи температури и по-високи честоти. Според законите на физиката, атомите се движат по-бързо при нарастване на температурата и използват повече енергия. Това е в сила и за високите честоти; за достигане на по-висока честота се изразходва повече енергия. Същото е истина за бягането, сравнено с ходенето; бягането изисква от вас да изразходвате повече енергия за изминаване на едно и също разстояние, затова се уморявате по-бързо; в същото време можете да извървите много по-голямо разстояние, без да се уморите изобщо. По подобен начин сигналът ще се „измори" (отслабне) на по-късо разстояние, ако за него е изразходвана по-голяма енергия.

Кабелът с оптично влакно не е напълно имунизиран срещу затихване; изгубването на сигнала в стъкленото влакно може да бъде причинено от замърсяване на стъклото, а *разсейването* (*scattering*) може да се появи в резултат от малки вариации в плътността, получени при производството на стъклото. Но кабелът с оптично е в състояние да работи на по-големи разстояния, отколкото медния кабел, и може да прави това без нежелателна загуба на сигнала поради затихване.

Проблеми, свързани с пропускателната способност (честотната лента)

Капацитета на пропускателната способност на мрежата обикновено се измерва в мегабитове в секунда (Mbps). Типът на предаването на сигналите и разстоянието, на което се предава сигналът, влияят на пропускателната способност на конкретния тип преносна среда.

Класификацията на висока и ниска пропускателна способност е относителна концепция. 10-Mbps Ethernet е изключително бърза преносна среда в сравнение със средната скорост на трансфер от 40-50 Kbps по аналогови телефонни линии, но изглежда печално бавен, сравнен със скорости от 1 Gbps или повече, които могат да бъдат постигнати при високоскоростни WAN връзки като SONET и ATM.

Един важен критерий при избиране на типа на кабела и архитектурата за мрежата е големината на необходимата пропускателна способност, както в момента, така и в бъдеще.

Планиране на мрежата, като се взема предвид бъдещото развитие

Добро практическо правило, което трябва да се има предвид по време на фазата на планирането, е, че пропускателната способност на мрежата е подобна на финансова поддръжка, при която почти винаги имате нужда от повече, отколкото сте предвиждали.

Компютърните и комуникационните технологии нарастват с бърз темп. През 80-те години, когато връзките към глобални мрежи обикновено се считаха за добри при пропускателна способност по-малка от 10 Kbps, а много локални мрежи работеха на 2,5 Mbps и по-малко, няколко души решиха, че някога може да се появи необходимост от скорости на трансфер 100 Mbps и повече. Това стана преди появата на такива гладни за пропускателна способност технологии като видеоконференциите, поточното аудио и големите файлови трансфери, които днес са масово разпространени.

Много по-лесно се правят ъпгрейди по времето, когато инсталирате кабела, отколкото в бъдеще. Например може да спестите няколко долара, като използвате Cat 3 кабел, вместо Cat 5, за мрежа 10BaseT (изискваща скорости на трансфер само 10 Mbps, поддържана от кабела Cat 3). Но ако пет години по-късно откриете, че се нуждаете от ъпгрейд на локалната мрежа на 100 Mbps, ще изгубите много повече време и пари от спестените преди това средства, за да изтръгнете Cat 3 окабеляването и да инсталирате кабели от по-висока категория.

Методи за достъп до преносната среда

Сега, когато познавате различните методи за предаване на сигнали и техните характеристики, да научим как мрежата управлява предаването на сигнали от множество компютри така, че пакетите данни да достигнат своите местоназначения.

Представете си натоварен пътен трафик. Ако няма устройства за управление на трафика или правила за движение по пътя, които да ги ръководят, шофьорите щяха да се влачат като мравки към техните местоназначения. Вероятно щяха да настъпят конфликти и пътищата щяха да станат толкова задръстени, че движението щеше да става по-бързо пеша.

Светофарите, знаците „спри, осигури предимство", регулировчиците и правилата за движение по пътищата, които всички трябва да знаем, за да получим шофьорска книжка, представляват *методи за достъп*, контролиращи това, коя кола може да премине при всяка една пътна ситуация. Методите за достъп са предназначени да гарантират, че трафикът върви по подреден начин и че всеки достига до своето местоназначение колкото е възможно по-бързо.

При мрежите по подобен начин се нуждаем от метод за контрол на достъпа до преносната среда. С различните мрежови архитектури и топологии се асоциират няколко различни метода за достъп. В следващите секции ще представим най-популярните от тях:

- Множествен достъп с разпознаване на носещата (честота) и откриване на колизии (CSMA/CD)
- Множествен достъп с разпознаване на носещата (честота) и избягване на колизии (CSMA/CA)
- Предаване на маркер
- Приоритет по заявка

CSMA/CD

Най-популярният метод за контрол на достъпа, използван днес в локалните мрежи, е множественият достъп с разпознаване на носещата (честота) и откриване на колизии (CSMA/CD). Това е доста обширно определение, затова за по-кратко се използва неговото съкращение. Популярността на метода се дължи на факта, че това е методът за достъп, използван от Ethernet – най-разпространената архитектура за локални мрежи.

CSMA/CD е относително бърз и ефикасен метод за разпределяне на достъпа до Ethernet кабела. За да разберете как работи, първо ще разделим името на неговите съставни части:

- **Разпознаване на носещата** – Когато даден компютър иска да предава по мрежа, използваща метода CSMA/CD, той първо „подслушва" кабела, за да определи дали в момента друг компютър не предава данни. Затова той разпознава състоянието на носещата честота – т.е. дали в момента се използва носещата.
- **Множествен достъп** – Това показва, че по едно и също време в мрежата могат да предават множество компютри.
- **Откриване на колизии** – Тук стигаме до същинския принцип на работата на CSMA/CD. Когато компютърът е готов за предаване, той разпознава състоянието на носещата, и ако кабелът е зает, той не изпраща своя сигнал. Ако компютърът не разпознае наличие на сигнал в проводника, той предава. Това действа добре, но когато два компютъра подслушват едновременно и заедно установят, че няма сигнал по линията, тогава те изпращат сигнал едновременно. Тогава обаче възниква *колизия*.

Когато настъпи колизия на сигнали в мрежа с коаксиален кабел, пакетите данни се нарушават. Но не всичко е загубено: при CSMA/CD всеки компютър изчаква *случайно количество време* и след това отново изпраща същия сигнал. Защо случайно количество? Очевидно, ако и на двата компютъра е зададено да изчакат X милисекунди, същият конфликт би настъпил отново след X милисекунди. Компютърът, който първи започне да предава отново (този, който е избрал по-краткото време) „спечелва" достъпа до кабела.

При CSMA/CD все пак настъпват колизии на данните, но тъй като сигналът пътува бързо (на 10 Mbps или на 100 Mbps по една типична Ethernet мрежа), производителността остава висока.

Спецификациите за реализацията на CSMA/CD се съдържат в IEEE 802.3.

CSMA/CA

Както можете да предположите, методът на множествен достъп с разпознаване на носещата (честота) и избягване на колизии (CSMA/CA) е свързан в определена степен с CSMA/CD. Да повторим, че първата стъпка за компютъра, който иска да предаде данни, е да наблюдава кабела и да определи дали е свободен.

Но CSMA/CA е по-малко надежден метод на достъп. Ако компютърът разпознае, че по кабела няма сигнал, той не приема, че това е безопасно, и след това изпраща своите ценни данни навън, рискувайки те да бъдат унищожени, ако друг компютър е решил да направи същото нещо по същото време. Вместо това компютърът първо изпраща сигнал, наречен заявка за изпращане (request to send - RTS). Сигналът обявява намерението на компютъра да предава. Ако друг компютър има същото намерение, тези сигнали ще влязат в конфликт (настъпи

колизия), но няма да има загуба на данни, защото самите пакети с данни никога не могат да влязат в конфликт. Това е познато като избягване на колизиите.

На пръв поглед може да изглежда, че CSMA/CA превъзхожда метода с откриване на колизии. Но той има отрицателно въздействие върху производителността поради наличието на голям брой RTS съобщения (много от тях излишни), които трябва да бъдат изпратени в допълнение към самите данни. Всъщност вие дублирате количеството на сигналите, който преминават по кабела.

Мрежите AppleTalk използват метода на достъп CSMA/CA.

ЗАБЕЛЕЖКА И CSMA/CD, и CSMA/CA са известни като конкурентни (състезателни) методи, защото сигналите трябва да се състезават или конкурират за използването на кабела.

Предаване на маркер

Какво ще кажете за метод на достъп, който ви позволява да се справите изобщо с колизиите? Да, има такъв – нарича се предаване на маркер.

Предаването на маркер е *несъстезателен* метод, при който два компютъра не могат да предават сигнал по едно и също време. Той действа донякъде подобно на съвещание на комитет, където на даден член е разрешено да говори, когато му бъде предоставена думата. По подобен начин един компютър в мрежа с предаване на маркер изчаква, докато получи маркера и тогава може да говори (предава).

Предаването на маркер е много учтив и цивилизован метод за контрол на достъпа. В мрежата циркулира в кръг сигнал, наречен *маркер* (най-често се използва топология кръг, но предаване на маркер може да бъде използвано също и в шинна мрежа), докато той достигне компютър, който има данни за изпращане.

Фигура 4-9 илюстрира процеса на предаване на маркера.

Най-разпространената мрежа с предаване на маркер е Token Ring. Ето как работи тя: когато маркерът пристигне по мрежата до компютъра, чакащ да предава, този компютър получава управлението върху маркера. По-конкретно той добавя своите данни към сигнала на маркера и го поставя обратно в мрежата. Пакетът с данни съдържа адресна информация, и когато сигналът продължи своето движение по кръга на мрежата, тези станции, чиито адреси не отговарят на тези в хедъра, го предават нататък.

Когато накрая маркерът достигне местоназначението, посочено в адреса в хедъра, мрежовата карта на този компютър копира данните. След това този компютър добавя информация към маркера, потвърждаваща, че данните са приети, и изпраща маркера отново по кръга. Първоначалният предаващ компютър получава маркера, след което или изпраща още данни, или освобождава маркера, обозначавайки го като свободен за циркулация. Следва поставяне на маркера отново в мрежата.

Фигура 4-9 *Компютърът в мрежа с предаване на маркер не може да предава, докато не получи маркера.*

В някои архитектури с предаване на маркер, като например Fiber Distributed Data Interface (FDDI), по мрежата могат да циркулират множество маркери едновременно. Token Ring и FDDI ще разгледаме по-детайлно в Глава 5, „LAN връзки". Token Ring стандартите са изброени в спецификацията IEEE 802.5.

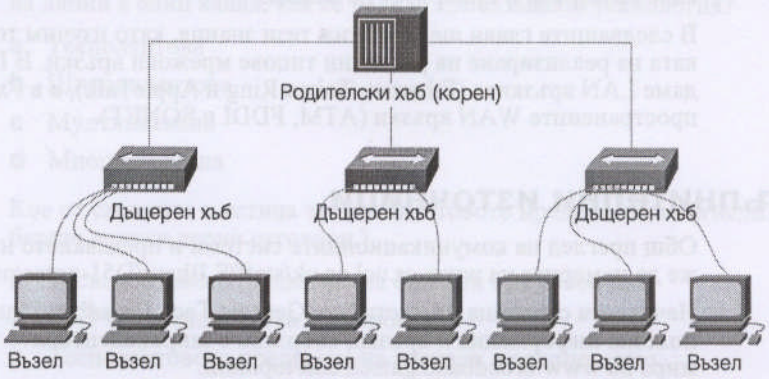
Приоритет по заявка

Методът на достъп с приоритет по заявка е разработен от Hewlett-Packard, за да бъде използван в LAN архитектурата, наречена 100VG-AnyLAN. Тази архитектура се означава също като VG-AnyLAN, или просто AnyLAN. VG-AnyLAN е проектирана като високоскоростна, гъвкава и ефикасна алтернатива на Ethernet.

Методът с приоритет по заявка за управление на достъпа до преносната среда използва многопортови повторители (хъбове), които извършват търсения с кръгово редуване (round-robin) на свързаните възли (компютри, маршрутизатори или други мрежови устройства), като наблюдават за наличие на заявки за предаване. Топологията на мрежата VG-AnyLAN има формата на звездообразно дърво. Хъбовете могат да бъдат свързани каскадно към хъб-корен (наричан също родителски хъб) за осъществяване на централизирано управление.

Фигура 4-10 илюстрира мрежа 100VG-AnyLAN.

Фигура 4-10 *Мрежата 100VG-AnyLAN използва поредица от хъбове за реализиране на метода на достъп с приоритет по заявка.*



Частта *приоритет* от термина приоритет по заявка се отнася до факта, че можете да зададете приоритет на определен тип данни, така че те да бъдат обработвани първи, ако хъбът едновременно приеме две заявки за изпращане. Това осигурява гарантирана пропускателна способност за високоскоростни приложения, например за видео на живо. Приоритетът по заявка е по-ефикасен метод от CSMA/CD, защото използваните кабели (четири двойки проводници, като всяка двойка има възможност да пренася сигнали) позволяват на компютъра да предава и приема едновременно. Освен това този метод избягва практиката на CSMA/CD на бродкастно предаване до цялата мрежа. Вместо това само компютрите, свързани към конкретен хъб, приемат бродкаст. Хъбовете комуникират един с друг; всеки от тях се занимава само с възлите, свързани към него, и не отговаря за възлите, свързани към други хъбове.

Тъй като не всички данни преминават през всички станции, което е нормален процес при Ethernet и Token Ring, мрежата VG-AnyLAN по своята същност е доста по-сигурна.

VG-AnyLAN мрежите могат да използват кабели с две или четири двойки UTP, две двойки STP или оптичен кабел. IEEE 802.12 съдържа спецификациите за приоритета по заявка.

За нещастие, продуктите за VG-AnyLAN мрежата са достъпни само от малък брой производители и архитектурата не е широко реализирана. Затова повечето мрежови администратори не срещат мрежа VG-AnyLAN в своята практика.

Обобщение

В тази глава разгледахме предаването на компютърни данни на ниво сигнали и представихме най-разпространените начини за класифициране на сигналите.

Научихте разликите между аналогово и цифрово предаване и по какво теснолентовите технологии се различават от широколентовите. Също така разгледахме характеристиките както на синхронните, така и на асинхронните комуникации, и се научихме да разпознаваме трите термина, свързани с протичането на сигнала: симплексно предаване, полудуплексно предаване и пълнодуплексно предаване. Разгледахме някои общи проблеми, свързани със сигналите, като EMI, RFI, смесване на сигнали и затихване.

След това разгледахме най-популярните методи, използвани от PC мрежите за управление на достъпа до преносната среда, като CSMA/CD, CSMA/CA, предаване на маркер и приоритет по заявка.

В следващите глави ще обогатим тези знания, като изучим теорията и практиката на реализиране на различни типове мрежови връзки. В Глава 5 ще разгледаме LAN връзките (Ethernet, Token Ring и AppleTalk), а в Глава 6 – най-разпространените WAN връзки (ATM, FDDI и SONET).

Допълнителни източници

Общ преглед на комуникационните системи и предаването на информация може да намерите на www.cs.ucl.ac.uk/staff/S.Bhatti/D51-notes/node1.html.

Началната страница на института Georgia Tech Broadband Institute, съдържаща полезна информация и връзки, свързани с широколентовите технологии, се намира на www.broadband.gatech.edu/top.html.

Едно чудесно ръководство по 100VG-AnyLAN може да бъде намерено на www.iol.unh.edu/training/vganylan.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Когато единиците и нулите, които представят компютърни данни, се превърнат в електрически или светлинни импулси, какви стават?

- **a** Криптирани
- **b** Модулирани
- **c** Защитени
- **d** Пулсирани

2 Кое от следните е истина за цифровото предаване на сигнали?

- **a** Цифровият сигнал е електромагнитна вълна, която постоянно се променя.
- **b** Цифровите сигнали се измерват по амплитуда, честота и фаза.
- **c** Цифровите сигнали се измерват в цикли.
- **d** Цифровото предаване на сигнали се нарича предаване на сигнали с дискретно състояние.

3 Кое от следните е предимство на аналоговото предаване на сигнали пре цифровото? (Изберете всички верни отговори.)

- **a** Аналоговите сигнали по принцип са по-неподатливи на грешки, предизвикани от смущения.
- **b** Аналоговите устройства са по-евтини за направа от цифровите устройства.
- **c** Аналоговите сигнали са по-лесни за мултиплексиране.

d Аналоговите сигнали са по-неподатливи на затихване.

4 Когато целият капацитет на преносната среда се използва за предаване на данни в един канал, как се нарича използваната технология?

a Теснолентова

b Широколентова

c Мултиплексна

d Многосвързана

5 Кое от следните е истина за теснолентовото предаване на сигнали? (Изберете всички верни отговори.)

a Теснолентовото предаване на сигнали е двупосочно.

b CATV е теснолентова технология.

c Теснолентовото предаване на сигнали е еднопосочно.

d Теснолентовото предаване обикновено се асоциира с предаването на цифрови сигнали.

6 Кой от следните типове мултиплексиране се използва с оптични мрежи, при който всеки сигнал се пренася на отделна дължина на светлинната вълна?

a FDM

b TDM

c DWDM

d MPPE

7 Кое от следните е истина за асинхронното предаване?

a Асинхронните предавания включват вграден механизъм за тактуване.

b Асинхронните предавания използват синхронизация с гарантирана промяна на състоянието.

c Асинхронните предавания използват метод на синхронизация с овърсемплинг (свръхсемплиране).

d Асинхронните предавания използват старт бит за синхронизация на тактовите генератори на предаващите и приемащите устройства.

8 Кое от следните е пример на полудуплексно предаване?

a Традиционните телевизионни програми

b Градските радиостанции

c Телефонните комуникации

d Цифровата абонаментна линия (Digital Subscriber Line – DSL)

9 Коя от следните медии е по-предразположена към електромагнитни смущения (EMI)?

a UTP

b Коаксиален кабел

c Оптичен кабел

d STP

10 Кой метод за достъп до преносната среда се използва в мрежите Ethernet?

a CSMA/CA

b CSMA/CD

c Предаване на маркер

d Приоритет по заявка

Глава 5

LAN връзки

В първите четири глави на тази книга изучихте целта и структурата на мрежите, мрежовите модели и стандарти, начините за предаване на сигналите по преносната среда и методите за управление на достъпа до тази среда.

В тази глава ще сглобим някои от тези концепции, за да разгледаме как всички те се вписват в спецификациите, изграждащи конкретен тип мрежова връзка (означавано още като мрежова *архитектура*).

Най-общо можем да разделим типовете връзки на следните две категории:

- Такива, използвани за локални мрежи (LAN) или големи градски мрежи (MAN); т.е. мрежи с ограничен географски обхват
- Такива, използвани за глобални мрежи (WAN), които обхващат градове, държава или дори континенти

В тази глава ще разгледаме характеристиките на първият тип връзки и как да направим избор на най-лесно осъществимото, най-ценово ефективното и изобщо оптималното решение за дадена ситуация. Вторият тип е описан в Глава 6, „WAN връзки".

Съществуват няколко типа връзки, използвани за свързване на компютри по LAN или MAN. Тъй като тези мрежи обхващат относително къси разстояния, могат да бъдат използвани такива типове кабели, които не могат да работят при WAN мрежите поради тяхното предразположение към затихване.

От предишните глави вече сте запознати с повечето LAN архитектури, но тази глава очертава характеристиките и стандартите на всяка от тях:

- Ethernet
- Token Ring
- Fiber Distributed Data Interface (FDDI)
- AppleTalk
- ARCnet

Ethernet

Ethernet архитектурата е най-популярният тип LAN връзка в наши дни. Тя е базирана на стандарта 802.3, който дефинира мрежа, реализираща метода на достъп CSMA/CD и използваща теснолентово предаване по коаксиален кабел или

кабел с усукана двойка, разположен в шинна топология (т.е. линейна шина или шина звезда). Стандартните скорости на трансфер са 10 Mbps или 100 Mbps, но новите стандарти дефинират *Gigabit Ethernet*, който има възможност за постигане на скорости до 1 Gbps по оптичен кабел или друга високоскоростна преносна среда.

Ethernet води началото си от мрежата ALOHA WAN в Хавайския университет, в която се използва метод за контрол на достъпа CSMA/CD. През 70-те години изследователският център на Xerox в Пало Алто (PARC) разработва проекта на 2,95 Mbps Ethernet. Скоро след това Xerox, Intel и Digital в сътрудничество разработват стандарт за Ethernet, който предава на 10 Mbps.

Днес се използват разнообразни Ethernet топологии, включващи следните широко реализирани форми:

- 10Base2 (thinnet)
- 10Base5 (thicknet)
- 10BaseT (UTP)
- 100BaseT (Fast Ethernet)
- 100BaseFX (Ethernet по оптичен кабел)
- 1000BaseT (Gigabit Ethernet)

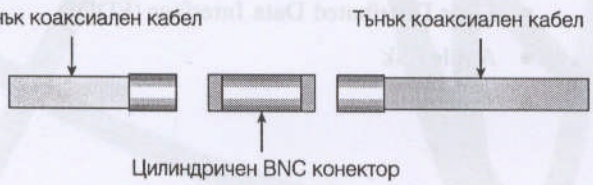
10Base2

Според стандарта IEEE 802.3, Ethernet топологията 10Base2 реализира метода на достъп CSMA/CD в разположение линейна шина и използва тънък коаксиален кабел. Тази топология е известна и под името *thinnet*.

Числото 10 в името означава скоростта на трансфер на thinnet, която е 10Mbps. Ethernet е мрежа с теснолентово предаване (пряко предаване без модулация). Числото 2 се определя малко по-трудно; то показва приблизителната стойност на максималната дължина на един кабелен сегмент за тази топология, която е 185 метра (закръглено 200 метра, или 2).

Мрежата 10Base2 е ограничена до 30 възела (компютри или други мрежови устройства) на един 185-метров кабелен сегмент. Thinnet използва цилиндрични метални конектори и Т-конектори (и двата вида се наричат BNC конектори) и BNC терминатори на всеки край на шината. Фигура 5-1 илюстрира начина на използване на цилиндричен конектор за увеличаване на дължината на кабела.

Фигура 5-1 *Цилиндричен BNC конектор може да бъде използван за удължаване на парче тънък коаксиален кабел.*



ЗАБЕЛЕЖКА В мрежовата индустрия има известно разногласие относно първоизточника на съкращението BNC. В някои текстове може да го срещнете дефинирано като *British Naval Connector*. Други източници го дефинират *като Bayonet Nut Connector*. Много източници отнасят съкращението към имената на тези, които са го създали Neil и Concelman. Сред тези, които защитават последната дефиниция, има допълнителни разногласия дали името се пише *Neil* или *Neill*. Проучването показва, че Пол Нейл, служител в Bell Labs, създава конектор, който нарича „N" конектор; този конектор се използва от Британската флота (Navy). По-късно Карл Концелман адаптира дизайна, за да създаде конектор с байонетно монтиране, който се нарича „C" конектор. Накрая Нийл и Концелман заедно създават по-малката версия – BNC конектора.

Предимства на 10Base2

Топологията 10Base2 е лесна за инсталиране и конфигуриране. По тази причина тя е подходяща за малки временни мрежи (например в класни стаи, които се налага често да бъдат инсталирани и деинсталирани). В 10Base2 се използва по-малко кабел, отколкото в 10BaseT, и използваният кабел е по-евтин на линеен метър от този при 10Base5. Мрежата не изисква допълнителни компоненти, като хъбове или външни приемопредаватели. Поради това 10Base2 е относително евтина за реализиране мрежа.

Недостатъци на 10Base2

За нещастие, 10Base2 не е подходяща за големи мрежи поради ограниченията в дължината на кабелния сегмент и броя на възлите в един сегмент. Освен това нейната скорост на трансфер от 10 Mbps е относително бавна за нуждите на днешния свят, характеризиращи се с натоварено използване на честотни ленти.

ЗАБЕЛЕЖКА В спецификациите на мрежата се налага ограничение на максималната дължина на един кабелен сегмент, защото сигналът губи свята сила при увеличаване на разстоянието (затихване). Също така са важни изискванията за минимална дължина, защото ако кабелният сегмент между два компютъра е прекалено къс, сигналите на двете устройства ще се насложат (припокрият), което в резултат ще доведе до необикновено напрежение по кабела, наречено *колизия*.

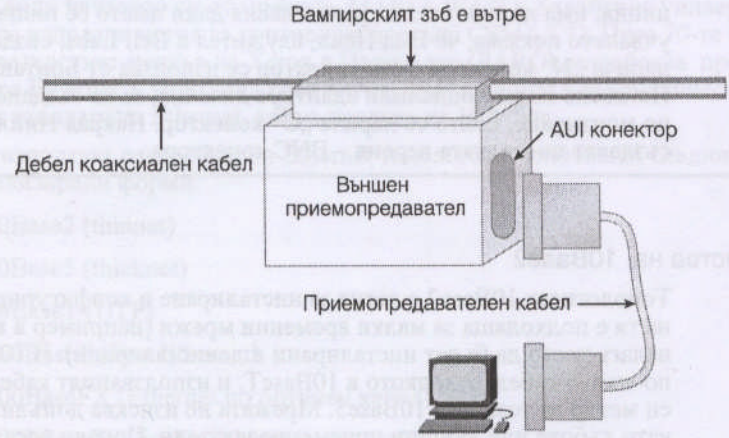
10Base5

Понякога 10Base5 бива означавана като *стандартен Ethernet*. Тя се нарича също *thicknet*. Кабелът на thicknet има диаметър около половин инч, т.е. той е два пъти по-дебел от този на thinnet. Thicknet използва топология линейна шина, но поради използвания по-дебел коаксиален кабел има възможност за предаване на по-голямо разстояние (500 метра) без загуба на сигнал. Спецификациите на Thicknet налагат ограничение за минимална дължина на сегмента от 2,5 метра.

Инсталирането на thicknet мрежа е по-сложно от това на thinnet. 10Base5 използва външни приемопредаватели, които осигуряват предаване и приемане. Те се свързват към мрежовата карта с помощта на приемопредавателен кабел, използващ 15-изводни AUI (DIX) конектори, а към коаксиалния кабел посредством

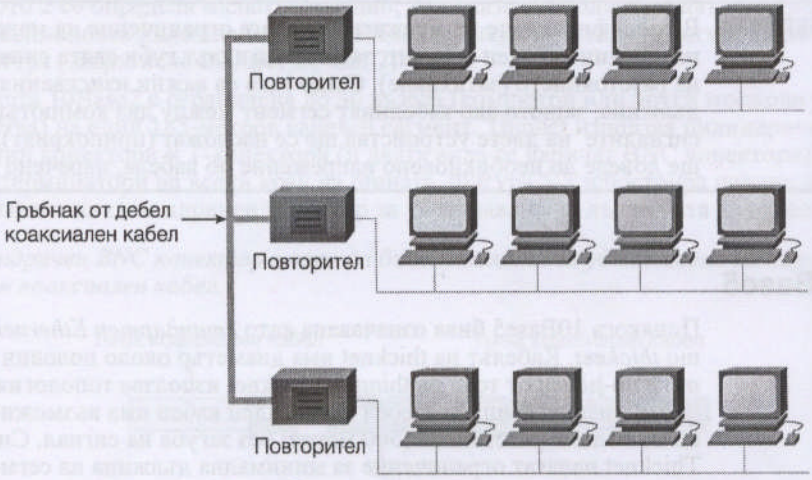
така наречения *„вампирски зъб"* (vampire tap). На Фигура 5-2 е показана илюстрация на този тип връзка.

Фигура 5-2 *Мрежовата карта се свързва към thicknet посредством външен приемопредавател и вампирски зъб.*



10Base5 често се използва като *гръбнак* (backbone), защото дебелият коаксиален кабел се използва за покриване на дълги разстояния, например свързване на повторители на различни етажи, към които след това се свързва тънък коаксиален кабел thinnet и компютрите на всеки етаж се свързват към тънкия коаксиален кабел. На Фигура 5-3 е показано как става това.

Фигура 5-3 *Дебелият коаксиален кабел може да бъде използван като гръбнак в комбинация със сегменти от тънък коаксиален кабел.*



Подобно на другите Ethernet мрежи, 10Base5 използва метод на достъп до преносната среда CSMA/CD и теснолентово предаване. Дължината на кабела може да бъде увеличена с помощта на N-цилиндричен конектор, а шината се терминира с помощта на N-терминатори.

Предимства на 10Base5

Thicknet притежава две големи предимства пред thinnet:

- Възможност да обхваща по-големи разстояния между повторителите
- Капацитет за повече възли (компютри) във всеки сегмент

Предимството на дебелия (и тънкия) коаксиален кабел пред UTP кабела се състои в частичната защита срещу EMI (електромагнитни смущения), която предлага дебелата външна обвивка.

Недостатъци на 10Base5

Дебелият коаксиален кабел има някои недостатъци. Липсата на гъвкавост затруднява работата с него, а добавянето на станции изисква пробиване на кабела за създаване на разклонения.

Thicknet мрежата е относително скъпа. Това се дължи не само на по-скъпия кабел, в сравнение с тънкия коаксиален кабел или UTP, но и на факта, че трябва да закупите и допълнително оборудване (например приемопредавател и приемопредавателен кабел) за всеки компютър в мрежата.

10BaseT

В момента 10BaseT е една от най-популярните Ethernet реализации. Може да се каже, че 10BaseT е звезда в света на компютърните мрежи – още повече, че използва шинна топология от тип звезда.

ЗАБЕЛЕЖКА Вътре в самия Ethernet хъб системата на предаване на сигналите е шина, както при коаксиалните Ethernet мрежи.

На практика сигурно ще чуете термина *Ethernet кабел*, използван за описание на кабел с неекранирана усукана двойка (UTP), използван най-често в тази архитектура (може да се използва и екранирана усукана двойка – STP). 10BaseT и нейният братовчед 100BaseX направиха възможно лесното инсталиране и разширяване на мрежите.

Предимства на 10BaseT

Мрежите, базирани на спецификациите 10BaseT, са относително евтини. Макар че се изисква включването на хъб, когато свързвате повече от два компютъра, на пазара се предлагат малки хъбове с ниска цена, а мрежовите карти за 10BaseT не са скъпи и са широко разпространени.

ЗАБЕЛЕЖКА Спецификациите на 10BaseT изискват задължително включване на хъб. Но ако искате да свържете само два компютъра (например за домашна мрежа) и искате да използвате UTP вместо thinnet, можете да направите това, като използвате *кръстосан (crossover) кабел*. Това е тип кабел, при който двойките проводници са кръстосано свързани и се използва за свързване на два хъба един към друг, ако хъбовете нямат uplink портове.

Използваните кабели с усукана двойка, най-вече UTP, са тънки, гъвкави и полесни за полагане в сравнение с коаксиалния кабел. Използват се модулни RJ-45 конектори, които правят изключително лесно свързването на кабела към мрежовата интерфейсна карта или хъба.

Друго голямо предимство на 10BaseT е възможността за ъпгрейд. Макар че по дефиниция мрежата 10BaseT работи на 10 Mbps, с помощта на кабел от категория Cat 5 или по-висока и мрежови интерфейсни карти с двойна скорост от 10/100 Mbps можете лесно да ъпгрейдвате до 100 Mbps просто като замените хъбовете.

Недостатъци на 10BaseT

Максималната дължина на един сегмент от 10BaseT (без повторители) е само 100 метра. Използваният в такава мрежа UTP кабел е по-податлив на електромагнитни смущения (EMI) и затихване, отколкото други типове кабели. Освен това допълнителната цена на хъба може да направи това решение малко по-скъпо от мрежата с тънък коаксиален кабел.

100BaseX

Изискванията за висока пропускателна способност, налагани от такива технологии като видеото на живо, конферирането и поточното аудио, създадоха необходимостта от нарастване на скоростта на много мрежи над 10 Mbps, възможни за Ethernet. Тогава на сцената излезе 100BaseX, наречена също *Fast Ethernet*.

100BaseX се разпространява в няколко различни модела. Тя може да бъде реализирана по UTP кабели Cat 3, 4 или 5 с 4 двойки (100BaseT), по UTP кабели Cat 5 или STP с 2 двойки (100BaseTX) или като Ethernet по оптичен кабел с две оптични влакна (100BaseFX).

Предимства на 100BaseX

Независимо от реализацията, голямото предимство на 100BaseX е високата скорост и производителност. При 100 Mbps скоростите на трансфер са 10 пъти по-големи от тези на 10Base2, 10Base5 и 10BaseT.

Тъй като използва кабел с усукана двойка, 100BaseX има същите предимства като 10BaseT: ниска цена, гъвкавост и лесна реализация и разширение.

Недостатъци на 100BaseX

100BaseX притежава недостатъците на 10BaseT, наследявани от кабела с усукана двойка, като предразположеност към EMI и затихване. Мрежовите карти и хъбовете със скорост 100 Mbps като цяло са по-скъпи от тези, предназначени за мрежи 10 Mbps, но с нарастване на популярността на 100BaseX цените спадат.

Оптичният кабел остава скъпа възможност, не толкова поради цената на самия кабел, а поради необходимостта от опит и уменията по неговото инсталиране. Инсталирането на кабели ще разгледаме по-подробно в Глава 6.

1000BaseT

100BaseX е позната като *Fast Ethernet*, а най-новото допълнение към фамилията Ethernet – 1000BaseT, трябва да бъде считано за скоростен демон. Неговото прозвище е *Gigibit Ethernet*. Макар още да не е широко разпространена реализация при производството на мрежи, тази архитектура поддържа скорости на трансфер на данни 1 Gbps, което е почти седем пъти по-бързо от T-1 линия. В преобладаващата си част Gigabit Ethernet е LAN архитектура, макар че нейната реализация по оптичен кабел я прави подходяща и за MAN архитектура.

Предимства на 1000BaseT

Най-голямото предимство на 1000BaseT е, разбира се, производителността. При скорост от 1 Gbps тя е 10 пъти по-бърза от Fast Ethernet и 100 пъти по-бърза от стандартния Ethernet. Това прави възможно реализирането на приложения, които използват интензивно пропускателната способност, като например видео на живо.

Предимства на 1000BaseT

Единствените недостатъци, асоциирани с 1000BaseT, са недостатъците на всички UTP мрежи, описани в секциите за 10BaseT и 100BaseT.

Структура на Ethernet фрейма

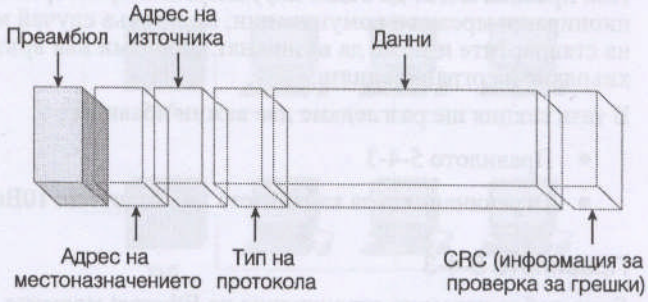
В терминологията на Ethernet, пакетите, на които се разделят данните за предаване по мрежата, се наричат *фреймове* (*frames*) (наричат се също кадри[1]). Фреймът съдържа хедър (заглавна информация), предаваните данни и трейлър (завършваща информация).

Типове Ethernet фреймове

В Ethernet комуникациите се използват четири различни типа фреймове (Ethernet_802.2, Ethernet_802.3, Ethernet_II и Ethernet_SNAP). Двата типа фреймове, използвани по правило в TCP/IP мрежа, са Ethernet_II и Ethernet_SNAP (Subnetwork Access Protocol). Типът на фрейма се дефинира от неговата структура (т.е. от броя на байтовете, заделени за всяко поле в хедъра, поле за данни и поле за трейлър). Например хедърът на Ethernet_II е по-прост и съдържа само четири полета. Хедърът на Ethernet_SNAP съдържа девет полета.

Фигура 5-4 илюстрира структурата на Ethernet фрейма (тип Ethernet II).

Фигура 5-4 *Фреймът Ethernet II съдържа четири полета в хедъра и един трейлър.*



[1] За да е напълно ясна терминологията, при мрежите е прието „фрейм" да се асоциира с пакет, освен това е по-употребяван в техническите среди. Терминът „кадър" не е грешен, а е синоним – б.р.

Първото поле на хедъра, което е просто индикатор за началото на фрейма, е *преамбюлът (preamble)*. Следващите две полета съдържат адресите на местоназначението и източника (т.е. приемащият и предаващият компютър), а четвъртото поле се използва за идентифициране на протокола, работещ в мрежовия слой (обикновено IP или IPX). Следват същинските данни, които могат да бъдат с дължина до 1500 байта. Ethernet използва допълнителни 18 байта за конструиране на самия фрейм. Накрая е трейлърът, който съдържа информация за циклична проверка с излишък (CRC), представляваща изчисление, което се използва за удостоверяване, че приетият кадър отговаря на предадения.

Проверка за грешки с използване на CRC

CRC е стандартен начин за проверка за грешки в данните след тяхното предаване по мрежата. Ето как става това: Компютърът, който предава данните, ги третира като едни дълъг полином. Полиномът (многочленът) представлява алгебричен израз, сума от един или повече членове, като всеки член съдържа постоянен коефициент и една или повече променливи, повдигнати на цели степени. Предаващият компютър разделя този полином на предварително дефиниран 16- или 32-битов полином. Частното от това деление е CRC, което се добавя към блока с данни преди предаването и се предава заедно с тях. След това компютърът на приемната страна използва същия предварително дефиниран 16- или 32-битов полином, който прилага към приеманите данни. Приемащата система сравнява своя резултат с резултата, записан от предаващата система. Ако двата са едни и същи, приемащият компютър прави заключението, че данните са приети успешно. Ако са различни, предаващият компютър бива уведомен отново да изпрати същия блок от данни.

Правила за инсталиране на Ethernet

За да се осигури правилна работа на мрежите, е важно спазването на правилата, установени в спецификациите на всяка отделна реализация. Това са ограничения, налагани от характеристиките на преносната среда. Обърнете внимание, че тези правила могат да бъдат нарушени или пренебрегнати и пак да имате функциониращи мрежови комуникации; но в такъв случай мрежата няма да отговаря на стандартите и може да възникнат проблеми във връзката вследствие надхвърляне на ограниченията.

В тази секция ще разгледаме две важни правила:

- Правилото 5-4-3
- Ограниченията за капацитета на възлите на 10BaseT

Правилото 5-4-3

Едно добре известно ограничение на Ethernet мрежите, базирани на коаксиален кабел, е правилото 5-4-3. Числата представят следните ограничения:

- **5** – Максималният разрешен брой кабелни сегменти в мрежа thinnet или thicknet е пет (всеки сегмент може да бъде дълъг до 185 метра за thinnet или 500 метра за thicknet).
- **4** – Максималният брой повторители, които могат да бъдат използвани за свързване на сегментите, е четири.

- **3** – Максималният брой сегменти, които могат да бъдат *запълнени* (т.е. да съдържат възли) е три. Другите два сегмента служат само за увеличаване на разстоянието.

ЗАБЕЛЕЖКА Когато правилото 5-4-3 се прилага към мрежа 10Base5 (thicknet), за измерване на разстоянието се използва дължината на дебелия коаксиален кабел. В това измерване не се отчита дължината на приемопредавателните кабели.

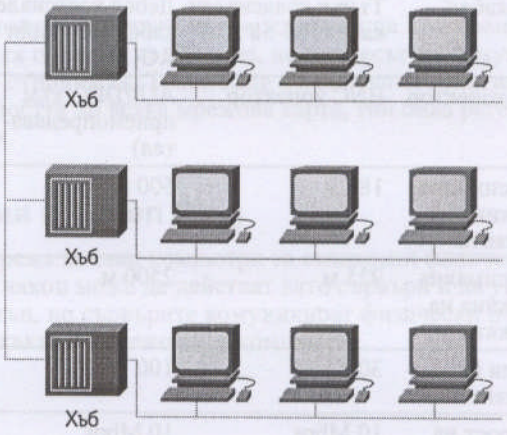
5-4-3 и 10BaseT

Прилага ли се правилото 5-4-3 за Ethernet мрежи с усукана двойка? Много книги ви навеждат на мисълта, че не се прилага. Но ограничението за броя на хъбовете, които могат да бъдат свързвани един с друг (uplink), всъщност е приложение точно на това правило.

Прилагането на правилото 5-4-3 за UTP мрежа тип звезда означава, че един запълнен хъб според правилото се брои за сегмент, при което максималният брой от каскадно свързани запълнени хъбове, позволен в мрежа с усукана двойка, е три.

Ако се замислите за факта, че свързването вътре във всеки хъб всъщност представлява шина, към която са свързани компютрите, точно както е в един кабелен сегмент между повторители в мрежа с линейна шина, горното придобива смисъл, както е показано на Фигура 5-5. Това е причината топологията да се нарича *шина от тип звезда (star bus)*.

Фигура 5-5 *Всеки хъб, към който са свързани компютри, представлява един запълнен сегмент.*



5-4-3 и разширяване на мрежата

В този момент сигурно се питате колко големи Ethernet мрежи могат изобщо да бъдат създадени при ограниченията, които налага това правило. Сигурно сте чували или виждали мрежи със стотици компютри, свързани посредством кабел с усукана двойка или коаксиален кабел, но по какъв начин в тези мрежи се заобикалят ограниченията на правилото 5-4-3?

За да разберете начина, по който могат да бъдат разширени мрежите Ethernet, първо трябва да разберете самото правило. Правилото 5-4-3 често започва като „не повече от пет сегмента, четири повторителя и три запълнени сегмента в *мрежа*". В този случай „мрежа" се дефинира като *домейн на колизии*, т.е. мрежа, в която ще настъпи колизия, ако два компютъра предават едновременно.

Същността на домейна на колизии е ключът към свързване на повече устройства, отколкото разрешава на пръв поглед правилото 5-4-3. Можем да създадем много отделни домейни на колизии в една мрежа, като разделим мрежата с помощта на такива комутационни устройства, каквито са суичовете и маршрутизаторите. В Глава 7 ще разгледаме детайлно начина на работа на тези устройства.

Капацитет от възли на 10BaseT

Броят на възлите на един сегмент в шина с топология звезда по кабел с усукана двойка винаги е точно 2: компютърът или устройството в единия край на кабела и хъбът в другия. Максималният брой възли в мрежата, базирана на хъбове, не трябва да надхвърля 100 поради експоненциалното нарастване на колизиите след 100 възела. Това ограничение може да бъде надхвърлено с помощта на свързващи устройства, като мостове и суичове. Теоретически общият брой на мрежовите устройства в мрежа 10BaseT е 1024.

Обобщение на характеристиките на Ethernet

Таблица 5-1 съдържа кратко обобщение на спецификациите на най-широко използваните реализации на Ethernet.

Таблица 5-1 *Обобщени Ethernet спецификации*

	10Base2	10Base5	10BaseT	100BaseX
Тип кабел	Тънък коаксиален кабел RG-58 A/U	Дебел коаксиален кабел RG-8 или RG-11	UTP Cat 3, 4, 5 и 5e	UTP Cat 3, 4, 5 и 5e
Тип конектор	BNC конектор	AUI/DIX (към приемопредавател)	RG-45 модулен	RG-11 модулен
Максимална дължина на сегмента	185 м	500 м	100 м	100 м
Максимална дължина на мрежата	925 м	2500 м	Шинна топология звезда	Шинна топология звезда
Възли на сегмент	30	100	2 (1024 на една мрежа)*	2 (1024 на една мрежа)*
Скорост на трансфер	10 Mbps	10 Mbps	10 Mbps	100 Mbps

* Тъй като при мрежи, базирани на UTP, като централна точка на свързване се използва хъб, всеки сегмент от кабела има само два възела – компютър или друго мрежово устройство на единия край, и хъб на другия край в този сегмент.

Ethernet е популярна LAN архитектура, която работи с почти всички популярни сървърни и клиентски операционни системи, включващи Windows for Workgroups, Windows 9x, Windows NT, Windows 2000, Novell NetWare, AppleTalk/AppleShare и UNIX/Linux.

Token Ring

Оригиналният Token Ring е разработен от IBM и е проектиран като надеждна мрежова архитектура, базирана на метода за управление на достъпа с предаване на маркер. Често се интегрира с мейнфрейм системите на IBM, като AS/400, и е предназначен за използване с персонални компютри (PC-та), миникомпютри и мейнфрейм компютри. Работи добре със Systems Network Architecture (SNA) – архитектурата на IBM, използвана за свързване към мейнфрейм мрежи.

Стандартите на Token Ring са зададени в IEEE 802.5.

Топологията на Token Ring

На пръв поглед топологията на Token Ring може да бъде доста объркваща. Тя е ярък пример на архитектура, физическата топология на която се различава от нейната логическа топология. Топологията Token Ring се означава като кръг със свързване звезда, защото външният вид на дизайна на мрежата е звезда, при която компютрите са свързани към централен хъб, наречен устройство за множествен достъп (multistation access unit – MSAU). Но вътре в устройството свързването формира път на данните във формата на окръжност, създавайки логически кръг.

Token Ring е наречена така поради нейната логическа топология и метода за управление на достъпа до преносната среда: предаване на маркер. Скоростта на трансфер за Token Ring може да бъде 4 Mbps или 16 Mbps.

Token Ring е теснолентова архитектура, използваща предаване на цифрови сигнали. По това тя прилича на Ethernet, но процесът на комуникация е доста различен в много отношения. Token Ring е *активна* топология: докато сигналът пътува по окръжността до всяка мрежова карта, той бива регенериран, преди да продължи пътя си.

Процес на комуникация в Token Ring

В една Ethernet мрежа всички компютри са създадени физически равноправни. На ниво софтуер някои може да действат като сървъри и да управляват мрежови акаунти и достъп, но сървърите комуникират физически по мрежата точно по същия начин, както и клиентските компютри.

Наблюдателят на кръга

В една Token Ring мрежа първият компютър, който влезе онлайн, става „главен наблюдател" (hall monitor) и трябва да отчита колко пъти всеки фрейм преминава циклично в кръга, а също поема отговорността да гарантира, че в даден момент в мрежата има само един маркер.

Компютърът-наблюдател периодично изпраща сигнал, наречен *маяк (beacon)*, който циркулира по кръга както всеки друг сигнал. Всеки компютър в мрежата следи за маяка. Ако даден компютър не го приеме от своя най-близък активен по-горен съсед в кръга (nearest active upstream neighbor – NAUN), когато очаква

такъв, той предава в мрежата съобщение, с което уведомява наблюдаващия компютър за неполучения маяк, изпращайки своя собствен адрес и този на NAUN съседа, който не е изпратил очаквания сигнал. В много случаи това предизвиква автоматично преконфигуриране, което възстановява комуникациите.

Трансфер на данни

Мрежата Token Ring използва маркер (т.е. специален сигнал) за управление на достъпа до кабела. Маркерът първоначално се генерира при влизане онлайн на първия компютър в мрежата. Както научихте в Глава 4, когато даден компютър иска да предава, той изчаква маркера и след това поема контрола над него.

По кръга маркерът може да пътува във всяка посока, но само в една посока в даден момент. Хардуерната конфигурация определя посоката на пътуване на маркера.

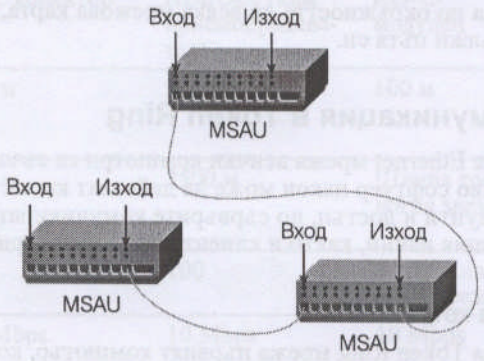
Хардуерни компоненти на Token Ring

Мрежите Token Ring използват специален хардуер. Една от причините за по-ограниченото реализиране на Token Ring в сравнение с Ethernet е по-високата цена на компонентите на Token Ring.

MSAU устройства

Хъбът на Token Ring се нарича MSAU или smart (умен) MSAU (SMSAU). Отличителната характеристика на MSAU е кръговата конфигурация на вътрешното свързване. Множество MSAU устройства могат да бъдат свързани заедно, при условие че „out" порта на едното се свързва към „in" порта на следващото, поддържайки по този начин целостта на кръговата топология. Данните трябва да пътуват в непрекъсната окръжност.

Фигура 5-6 *Множество MSAU устройства могат да бъдат свързани, при условие че кръгът се поддържа чрез правилно включване на входния и изходния кабел.*



Кабели и мрежови карти

Token Ring използва IBM кабели тип 1, 2 или 3. IBM означава своите кабели с усукана двойка „типове", вместо „категории". Вижте таблица 5-2 за пълни описания.

Таблица 5-2 *Типове IBM кабели*

Тип на кабела	Описание
Type 1	STP; две двойки проводници с външен екран
Type 2	STP; две двойки проводници за данни и четири двойки проводници за глас
Type 3	UTP; използва конектори RJ-45 или RJ-11; четири двойки проводници
Type 5	Оптичен кабел
Type 6	STP; използван като кабел за свързване на данни
Type 9	Огнеупорен STP кабел

ЗАБЕЛЕЖКА IBM кабелът използва специален IBM конектор, наречен конектор тип A, който не е съвместим със стандартните BNC конектори.

Token Ring мрежовите карти, например Ethernet UTP картите, притежават различни скорости, проектирани за работа на 4 Mbps или на 16 Mbps. Ако мрежата работи на 4 Mbps, можете да използвате карта 16-Mbps (макар че ще работи само на по-бавната скорост).

ПРЕДУПРЕЖДЕНИЕ *Не* можете да използвате карта, проектирана за работа на 4 Mbps, в мрежа Token Ring на 16-Mbps. Компютърът няма да може изобщо да комуникира.

Други компоненти

С Token Ring се използват и разнообразни други хардуерни компоненти. Например конекторите за интерфейс към преносната среда (media interface connectors – MIC конектори) се използват за свързване на IBM кабел тип 1 към IBM кабел тип 2. Филтрите за преносна среда (media filters) се използват за свързване на Token Ring мрежова карта към модулен конектор и за редуциране на шума по линията.

За регенериране на цифровия сигнал могат да бъдат използвани повторители както в Ethernet мрежите; с тях се увеличава дължината на мрежата.

Предимства на Token Ring

Token Ring е високо надеждна архитектура, а нейната схема с предаване на маркер елиминира колизиите на данни. Освен това MSAU устройствата могат да откриват мястото на прекъсване на мрежата и автоматично да го изключват от кръга, като по този начин гарантират непрекъснато движение на маркера по кръга. Следователно мрежата не се срива при прекъсване на едни компютър.

Друго предимство е възможността за лесно взаимодействие между PC и мейнфрейм компютри.

Недостатъци на Token Ring

Главните недостатъци на архитектурата Token Ring са нейната по-висока цена в сравнение с 10BaseT или 100BaseT и нейните сравнително по-бавни скорости.

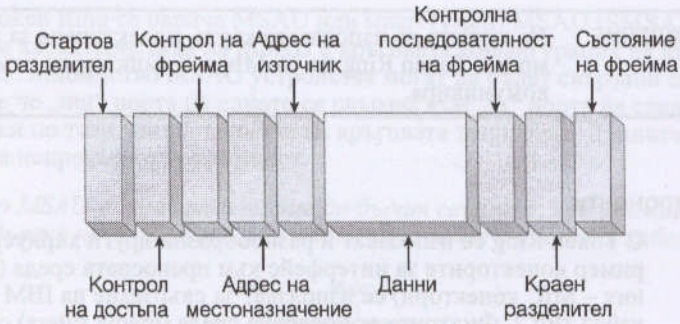
Структура на Token Ring фрейма

Token Ring мрежите използват три различни типа фреймове:

- **Фрейм за данни** – Пренася информацията, предавана от един компютър към друг
- **Фрейм за маркер** – Циркулира в мрежата, докато не бъде прихванат от компютър, който е готов да предава информация
- **Фрейм за управление** – Предава информация за грешка или друга управляваща информация

Структурата на Token Ring фрейма за данни на е малко по-сложна от тази на фрейма за данни в Ethernet II. Фигура 5-7 илюстрира фрейма за данни на Token Ring, който понякога се нарича също LLC фрейм (local link control).

Фигура 5-7 *Фреймът за данни на Token Ring е малко по-сложен от фрейма за данни на стандартния Ethernet.*



Стартовият разделител във фрейма на Token Ring служи за същата цел, както предисловието във фрейма на Ethernet. Другите полета функционират по следния начин:

- **Поле за контрол на достъпа** – Означава дали фреймът е маркер или фрейм с данни и неговия приоритет
- **Поле за контрол на фрейма** – Съдържа информация за контрол на достъпа
- **Адрес на местоназначение** – Адресът (адресите) на компютъра (компютрите), към които са предадени данните
- **Адрес на източник** – Адресът на предаващия компютър
- **Данни** – Реалната информация, която се предава (например съдържанието на съобщение за електронна поща)
- **Контролна последователност на фрейма (FCS)** – CRC битове за проверка за грешка

- **Краен разделител** – Означава края на фрейма
- **Поле за състояние на фрейма** – Индицира дали адресът е разпознат и фреймът копиран (маркирано от приемащия компютър, преди да бъде изпратен отново в движение по кръга)

ЗАБЕЛЕЖКА Фреймът с маркера (понякога наричан просто „маркер“) циркулира по мрежата, докато бъде уловен от компютър, който е готов да предава. Фреймът с маркера има само три полета: стартов разделител, поле за контрол на достъпа и краен разделител.

Правила на кръга

Спецификациите на Token Ring налагат някои ограничения върху нейната реализация:

- Разстоянието между MSAU устройствата е ограничено до 365 метра за кабели тип 3 и до 730 метра за кабели тип 1 или 2.
- Максималната дължина на кабелен сегмент зависи от типа кабел и варира от 45 до 200 метра.
- Максималната дължина за patch кабел тип 6 е 46 метра.
- Минималната дължина на сегмент е 2,5 метра.
- Максималният брой компютри в един сегмент, за IBM спецификации, е 72 при неекраниран кабел и 260 при екраниран.
- Максималният брой сегменти (т.е. MSAU устройства), които могат да бъдат свързани, е 33 (пак според спецификациите на IBM).

Обобщение на характеристиките на Token Ring

Token Ring е надеждна технология, но по-малко популярна от Ethernet поради относително по-високата цена и по-бавните скорости на предаване. Въпреки това се разработват спецификации за 100Mbps Token Ring и Gigabit Token Ring, затова тази архитектура още не е приключила своето развитие.

FDDI

FDDI представлява тип Token Ring мрежа. Нейната реализация и топология се различават от LAN архитектурата Token Ring на IBM, която е установена от IEE 802.5. FDDI се използва често за MAN мрежи или по-големи LAN, например при свързване на няколко сгради в офис или университетски комплекс.

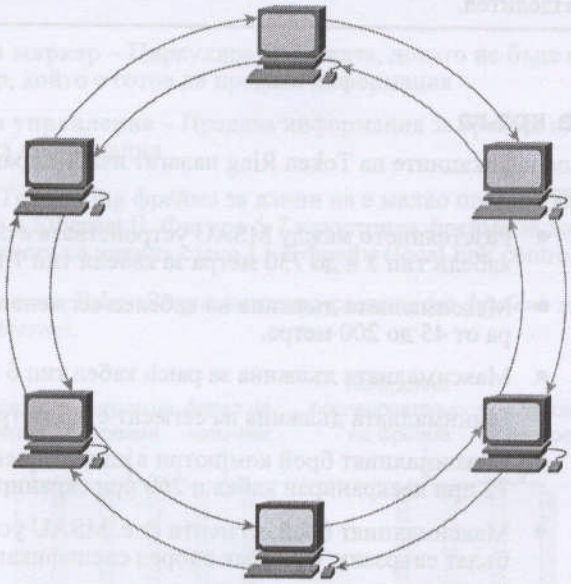
Как работи FDDI?

Както подсказва името, FDDI работи по оптичен кабел и следователно комбинира висока производителност с предимствата на кръговата технология с предаване на маркер. FDDI работи на 100 Mbps и нейната топология е *двоен кръг*.

Външният кръг се нарича *първостепенен* кръг, а вътрешният е *второстепенен* кръг.

Нормално трафикът тече само по първостепенния кръг, но ако той пропадне, потокът от данни автоматично преминава по второстепенния кръг, в противоположна посока. Когато стане това, се казва, че мрежата е в *превключено състояние (wrapped state)*. По този начин се осигурява отказоустойчивост за мрежовата връзка. Фигура 5-8 илюстрира начина на работа на FDDI.

Фигура 5-8 *FDDI използва двойно кръгова топология с отказоустойчивост.*



Компютрите в една FDDI мрежа се разделят на два класа:

- **Клас А** – Компютри, свързани към кабелите и на двата кръга
- **Клас В** – Компютри, свързани само към един кръг

Друга разлика между FDDI и 802.5 Token Ring е разрешеният брой фреймове по мрежата. Мрежата FDDI позволява едновременна циркулация на множество фреймове по кръга. По едно и също време може да предава повече от един компютър. Това се нарича *технология на споделена мрежа* (*shared network technology*).

Подобно на 802.5 Token Ring, FDDI използва предаване на маяци (beacons) за откриване и изолиране на проблеми в кръга.

FDDI спецификации

FDDI с двоен кръг поддържа максимум 500 възела на кръг. Общото разстояние на всяка дължина на кабелния кръг е 100 километра. Необходимо е поставяне на повторители на всеки 2 километра; ето защо FDDI не се счита за WAN връзка.

ЗАБЕЛЕЖКА Тези спецификации се отнасят за FDDI мрежа, реализирана по оптичен кабел. Технологията FDDI може да бъде използвана също по меден кабел. Това се нарича *Copper Distributed Data Interface (CDDI)*. Максималните разстояния за CDDI са значително по-малки от тези за FDDI.

Кръговата топология на FDDI може да бъде реализирана като физически кръг или като логически кръг със свързване в звезда и използване на хъб.

Предимства на FDDI

FDDI комбинира предимствата на предаването на маркера по кръговата топология с високата скорост на предаването на светлинни сигнали по оптични кабели. Нейната топология с двоен кръг осигурява редундантност и отказоустойчивост. Оптичният кабел не е предразположен към EMI и шум, и е по-сигурен от медния кабел. Данните могат да бъдат предавани на по-големи разстояния между повторители, отколкото при Ethernet и традиционния Token Ring.

Недостатъци на FDDI

Както винаги високата скорост и надеждност имат цена. FDDI е сравнително скъпа за реализиране и нейните ограничения в разстоянията, макар и по-малки от тези на други LAN връзки, я правят неизползваема за истински WAN комуникации.

Структура на FDDI фрейма

Структурата на FDDI фрейма е подобна на тази на Token Ring; разликата е, че FDDI използва протокол със синхронизиран маркер (timed token), докато Token Ring използва метод на достъп с приоритет/резервиране на маркера. Максималният размер на FDDI фрейма е 4500 байта.

Маркерът на FDDI е специален фрейм, състоящ се от три октета. Компютърът, който има данни за предаване, изчаква получаване на фрейма с маркера, придобива притежание над него, предава един или няколко фрейма с данни и след това освобождава маркера.

Обобщение на характеристиките на FDDI

FDDI представлява добра възможност за избор при мрежи със среден размер – MAN и големи LAN. Той е подходящ за мрежи, които изискват висока пропускателна способност, например за работа с приложения в инженерството, компютърната графика и видеото.

AppleTalk

Сигурно няма да се изненадате, че AppleTalk мрежата е проектирана за свързване на Apple компютри и нейните софтуерни компоненти са вградени в операционните системи за Macintosh. AppleTalk е името на архитектурата. Тя се разпространява в две разновидности: Phase 1 (включена в ранните версии на MAC OS) и Phase 2 (текущото издание).

LocalTalk е терминът, използван за означаване на кабелите, хардуера и протокола от каналния слой на AppleTalk мрежите.

Спецификации на AppleTalk

Мрежите AppleTalk/LocalTalk използват метода CSMA/CA за контрол на достъпа до преносната среда. Най-често се използват кабели STP, но е възможно също да се използва UTP кабел или оптичен кабел. Мрежовата топология представлява шина или дърво, а LocalTalk мрежата (използваща Apple компоненти) е ограничена до 32 възела.

AppleShare е протоколът, който осигурява споделяне на файлове и принтери по AppleTalk мрежа.

ЗАБЕЛЕЖКА Наред с Apple и други производители също предлагат кабели и компоненти за връзка, които позволяват свързване на повече компютри към AppleTalk мрежа.

Как работи AppleTalk

Мрежите AppleTalk използват схема на адресиране, в която всеки компютър, който влиза в мрежата, най-напред проверява за съхранен адрес (този, който е използвал в предишната сесия). Ако намери такъв, го използва; ако не намери, си задава сам адрес, избран по случаен начин от диапазона на запазените адреси. След това той предава бродкастно адреса, за да определи дали друг компютър в мрежата не го използва. Ако се окаже, че има такъв компютър, процесът се повтаря. Ако няма, той съхранява адреса, който ще използва и следващия път, когато влезе в мрежата.

AppleTalk е предназначена за малки мрежи. Въпреки това могат да бъдат свързани няколко отделни мрежи една към друга. Всяка подмрежа се нарича *зона* и има име, което я идентифицира. Донякъде зоните функционират подобно на работни групи. Можете да осъществявате достъп до ресурси в различна зона от вашата, като щракнете върху името на зоната.

Мрежите AppleTalk могат да бъдат свързвани също към мрежи, използващи други архитектури, например Ethernet или Token Ring. Apple предлага EtherTalk и TokenTalk, които представляват карти, позволяващи на Macintosh компютри да се свързват към мрежи, работещи съответно със спецификациите 802.3 и 802.5

Предимства на AppleTalk

Тъй като Apple включи AppleTalk в операционната система за Macintosh, тя се реализира и конфигурира лесно. Инсталирането на малка работна група за Macintosh компютри е просто и евтино.

Недостатъци на AppleTalk

AppleTalk архитектурата не е подходяща за изграждане на много големи мрежи. Тя е много бавна в сравнение с други LAN връзки (230,4 Kbps) и поради това не е подходяща за приложения, които интензивно използват честотната лента.

Предаване на данни с LocalTalk

LocalTalk е оригиналният протокол от каналния слой, използван от AppleTalk. С помощта на LocalTalk компютрите Macintosh се свързват един с друг посредством своите принтерски портове.

ЗАБЕЛЕЖКА Макар че мрежите AppleTalk първоначално използваха LocalTalk, AppleTalk работи също по Ethernet. Последната реализация придоби по-голяма популярност, защото LocalTalk е бавен (230.4 kbps) и е предназначен за малки работни групи с нисък трафик.

Обобщение на характеристиките на AppleTalk

Независимо от ограниченията към производителността, наборът от протоколи AppleTalk осигурява бърз и лесен начин за свързване на Macintosh компютри в малки работни групи за споделяне на файлове, принтери и други ресурси.

ARCnet

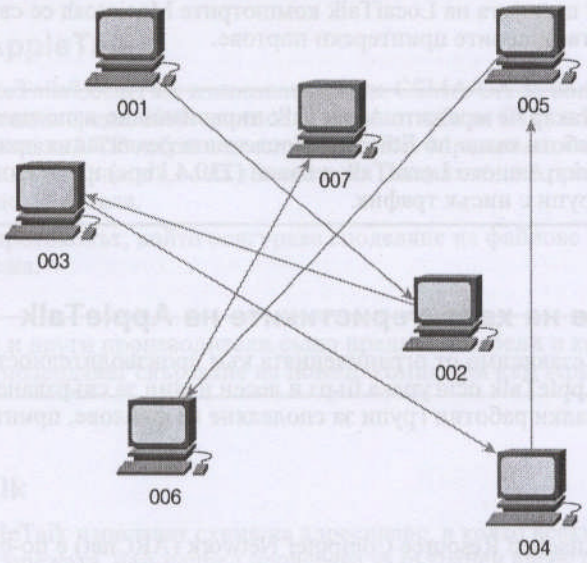
Attached Resource Computer Network (ARCnet) е по-стара LAN технология, която използва специален метод за контрол на достъпа с предаване на маркер по шинна топология тип звезда.

В някои книги ARCnet се асоциира със спецификациите 802.4 token bus, но реално тя беше разработена преди стандартите 802 и не отговаря напълно на тази спецификация. Тя е проектирана за малки работни групи и е много проста и евтина архитектура.

Как работи ARCnet

Методът с предаване на маркер, използван от ARCnet, се различава от този на Token Ring. В ARCnet мрежата маркерът не се движи по път, базиран на физическото местоположение. Вместо това той преминава от еди компютър към друг на базата на позицията на компютъра в зададения ред на номериране. Това прави ARCnet неефикасна преносна среда за предаване, в която данните пътуват до своето местоназначение по много по-дълъг път, отколкото е необходимо. Фигура 5-9 илюстрира начина на работа на ARCnet.

Фигура 5-9 *Методът на предаване на маркера на ARCnet може да доведе до преминаване по неефикасен маршрут до местоназначението.*



Спецификации на ARCnet

ARCnet използва хъб за свързване на компютри в шинна конфигурация от тип звезда и по принцип използва 93-омов коаксиален кабел, означаван като RG-62 A/U. Но ARCnet може да работи също по кабели с усукана двойка или оптични кабели.

При използване на по-често срещания коаксиален кабел, максималната дължина на сегмента (от компютър до хъба) е 610 метра. При използване на UTP кабели максималната дължина на сегмента спада до 244 метра.

ЗАБЕЛЕЖКА ARCnet може да използва топология линейна шина, вместо звезда, с коаксиален кабел; в този случай максималната дължина на сегмента достига 305 метра.

Стандартната ARCnet мрежа страда от ниска производителност; скоростта на трансфер е само 2,5 Mbps. По-късната реализация –ARCnet Plus, може да предава с 20 Mbps.

Предимства на ARCnet

ARCnet е евтина и работи адекватно при малки мрежи. ARCnet Plus предлага по-висока скорост на предаване на данни от стандартния Ethernet.

Недостатъци на ARCnet

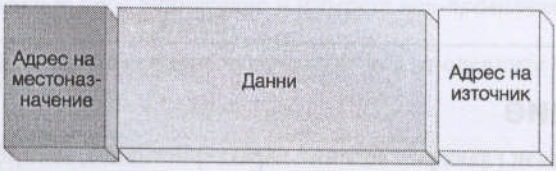
ARCnet е по-стара технология, която не е така популярна като Ethernet и Token Ring. Нейните мрежови компоненти не са така широко достъпни и е по-трудно

намирането на техници с опит за работа с технологията на ARCnet. Дори в нейния по-бърз вариант тя е далеч по-бавна от 100BaseT и не е подходяща за приложения, изискващи висока пропускателна способност.

Структура на пакетите на ARCnet

В мрежата ARCnet единицата данни, предавана по мрежата, се нарича *пакет*. Той е аналог на *фрейма* в Ethernet или Token Ring. Стандартният пакет на ARCnet е много прост по структура, както е показано на Фигура 5-10.

Фигура 5-10 *Пакетът ARCnet съдържа адресна информация и данни.*



Както виждате, полетата на хедъра и трейлъра съдържат адресите на компютрите – източник и местоназначение – а между тези адреси се намират данните. Пакетът на стандартния ARCnet е ограничен до 506 байта данни, а пакетите на ARCnet Plus могат да съдържат до 4096 байта.

Обобщение на характеристиките на ARCnet

ARCnet е проста технология, която в много среди се заменя от Ethernet или Token Ring. Въпреки че ARCnet е относително евтина и осигурява адекватна производителност за малки мрежи с ниска пропускателна способност, нейната ограничена скорост на предаване и неефикасен метод с предаване на маркера доведоха до спадане на популярността ѝ.

Сравнение на мрежовите архитектури

Таблица 5-3 обобщава характеристиките на мрежовите архитектури.

Таблица 5-3 *Сравнение на мрежовите архитектури*

Мрежова архитектура	Типове кабели	Скорост на трансфер	Метод на достъп	Топология
Ethernet 10Base2	Тънък коаксиален	10 Mbps	CSMA/CD	Линейна шина
Ethernet 10Base5	Дебел коаксиален	10 Mbps	CSMA/CD	Линейна шина
Ethernet 10BaseT	UTP Cat 3-5	10 Mbps	CSMA/CD	Звезда
Ethernet 100BaseT	UTP Cat 5	100 Mbps	CSMA/CD	Звезда
Ethernet 100BaseFX	Оптичен	100 Mbps	CSMA/CD	Звезда

Мрежова архитектура	Типове кабели	Скорост на трансфер	Метод на достъп	Топология
Ethernet 1000BaseT	UTP Cat 7	1 Gbps	CSMA/CD	Звезда
Token Ring	STP или UTP	4 Mbps или 16 Mbps	Предаване на маркер	Физическа звезда, логически кръг
FDDI	Оптичен	100 Mbps	Предаване на маркер	Двоен кръг
AppleTalk	STP или UTP	LocalTalk: 230,4 Mbps Ethernet: 10 Mbps	CDMA/CA	LocalTalk: Линейна шина Ethernet: Звезда

Обобщение

В тази глава разгледахме характеристиките, спецификациите и реализациите на няколко популярни LAN архитектури.

Научихте, че Ethernet е една от най-популярните LAN връзки, че е базирана на метода на достъп CSMA/CD и че се управлява от стандарта IEEE 802.3. Разгледахме различните разновидности на Ethernet, включващи:

- 10Base2 (thinnet)
- 10Base5 (thicknet)
- 10BaseT, 100BaseT и 1000BaseT

Също така разгледахме архитектурата Token Ring, установена от IEEE 802.5, и начина за изпълнение на комуникациите по Token Ring мрежа. След това разгледахме FDDI, архитектура с предаване на маркер, реализирана по оптичен кабел, която е подходяща за големи LAN и WAN. След това разгледахме AppleTalk и компонентите, изграждащи архитектурата: LocalTalk, AppleShare, EtherTalk и TokenTalk. Накрая разгледахме ARCnet – по-стара технология, използваща уникална схема на предаване на маркера, при която данните следват логически, а не физически път.

В следващата глава ще разширим още малко нашия хоризонт, като разгледаме концепциите и практическите изпълнения на глобалните мрежи. Ще разгледаме популярни WAN връзки и начина за тяхното реализиране, и ще обясним как можете да свържете вашата LAN мрежа към WAN (включително и към най-глобалната мрежа – Интернет).

Допълнителни източници

Още информация за LAN връзките можете да намерите на:

- Web сайта на Чарлз Спърджън за Ethernet (802.3) на адрес www.host.ots.utexas.edu/Ethernet/ethernet-home.html.
- Консорциумът Token Ring Consortium на www.iol.unh.edu/consortiums/tokenring/main.htm.

- Ръководството по FDDI на Interoperability Lab на адрес www.iol.unh.edu/training/fddi/htmls/index.html.
- Документът Core Competence за AppleTalk на адрес www.corecom.com/html/appletalk.html.
- Web сайтът на търговската асоциация на ARCNET на адрес www.arcnet.com/home.html.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 IEEE 802. дефинира спецификациите на коя от следните мрежови архитектури?

a Token Ring
b Ethernet
c ARCnet
d FDDI

2 Кой метод за достъп до преносната среда се използва от Ethernet мрежите?

a CSMA/CD
b CSMA/CA
c Предаване на маркер
d Приоритет по заявка

3 Спецификациите на 10Base2 Ethernet ограничават броя на възлите на един сегмент от кабела до какъв брой?

a 30
b 100
c 185
d 1024

4 Кой от следните типове кабели използва BNC конектор?

a UTP
b дебел коаксиален
c тънък коаксиален
d оптичен

5 Терминът „стандартен Ethernet“ се използва за означаване на коя от следните мрежи?

a мрежи 10BaseT
b мрежи 100BaseT
c мрежи 10Base2
d мрежи 10Base5

6 Какво е максималното зададено кабелно разстояние за мрежа 10Base5?

a 100 метра

b 500 метра

c 100 фута

d 500 фута

7 Кое от следното е истина за архитектурата Token Ring? (Изберете всички верни отговори)

a Token Ring е пасивна топология.

b Мрежите Token Ring работят на 4 или 16 Mbps

c Хъбовете в Token Ring се наричат устройства за множествен достъп.

d Token Ring е широколентова архитектура.

8 Какво е името на циркулиращия сигнал, изпратен от наблюдаващия компютър в мрежа Token Ring, чиято цел е да открие кога дадена станция е пропаднала, така че мрежата да може да се преконфигурира за възстановяване на комуникациите?

a маркер

b кадър с данни

c маяк

d NAUN

9 Кое от следните е протокол от каналния слой, първоначално използван за AppleTalk мрежите?

a Ethernet

b LocalTalk

c EtherTalk

d TokenTalk

10 Каква е скоростта на трансфера за стандартната ARCnet мрежа?

a 2,5 Mbps

b 25 Mbps

c 16 Mbps

d 10 Mbps

Глава 6

WAN връзки

Технологиите, преносните среди и оборудването, които работят добре на къси разстояния, обхващащи LAN или MAN, изобщо не са подходящи за дългите разстояния на глобалните мрежи (WAN). В днешния мобилен свят са необходими високопроизводителни, ценово-ефективни WAN технологии, и то по редица причини:

- Ръководителите и други служители се нуждаят от достъп до техните корпоративни мрежи, когато са на път или вкъщи.
- Компании с офиси на филиали, разпръснати в отдалечени географски местоположения, се нуждаят от мрежова връзка.
- Организацията иска да споделя информация с други организации, физически отдалечени на голямо разстояние.
- Търговските, правителствените и образователните организации и отделни лица се нуждаят от достъп до ресурси в глобалния Интернет.

Очевидно е невъзможно да се прокара Ethernet кабел от главния офис на една фирма в Денвър до офиса на филиала на фирмата в Хюстън. Дори кабелът да не налагаше ограничения в разстоянието, това пак нямаше да бъде осъществимо решение за свързване на международни сайтове.

Реализацията на WAN мрежите изисква напълно нов набор от технологии и правила. В тази глава ще разгледаме концепцията на изграждането на мрежи на големи разстояния и технологиите, използвани най-често за свързване на компютри, разположени в различни щати, страни или дори различни континенти. Те варират от Public Switched Telephone Network (PSTN — обществена комутируема телефона мрежа), която вече е реализирана в по-голямата част от света, до модерните високотехнологични решения, каквито са сателитните комуникации, позволяващи ни да „разговаряме“ с компютри в космоса.

Изграждането на глобални мрежи е свързано с много предизвикателства, които не се срещат при реализиране на мрежа, ограничена само до една географска област. WAN не е просто голяма LAN, а представлява сбор от много отделни LAN мрежи, свързани с връзки, които се различават по много неща от LAN връзките. Проектирането на WAN мрежи, които се простират по цялата планета, изисква съобразяване на множество фактори, между които часовите пояси и езиковите разлики.

Проектирането на WAN е сложна задача. Избирането на подходяща технология включва анализиране на процесите, които ще обслужва WAN, броя на потреби-

телите, изискванията за пропускателна способност и използваните модели устройства. Тези съображения можем да категоризираме по следния начин:

- WAN хардуер
- WAN топологии
- Типове мрежово комутиране
- Нови и перспективни WAN технологии
- LAN/WAN конективност

В следващите секции ще разгледаме всеки от тези въпроси.

WAN хардуер

Хардуерът, необходим за реализиране на WAN връзка, може да бъде прост и евтин, например по телефонна линия и модеми на всеки край. От друга страна, той може да бъде сложен и скъп. Най-общо цената и сложността на оборудването нарастват с увеличаване на скоростта и надеждността.

В следващите секции ще разгледаме най-широко използваните WAN устройства, включващи модеми, ISDN терминални адаптери за технологията цифрова абонатна линия (digital subscriber line – DSL) и оборудването на страната на клиента (customer premises equipment – CPE), използвани при специализирани връзки, каквито са T-връзките и X.25.

Модеми

За изграждане на мрежова връзка (към доставчик на интернет услуги (ISP) или към dial-up сървър в частна мрежа) по обществени телефонни линии, се използва устройство, наречено *модем*.

СЪВЕТ Думата „модем“ произлиза от действията, които изпълнява устройството; модемът ***модулира*** и ***демодулира*** сигнала. С други думи конвертира изпращания от компютъра цифров сигнал в аналогов с цел неговото предаване по аналоговата линия и след това го конвертира обратно в цифров вид за обработка от приемащия компютър.

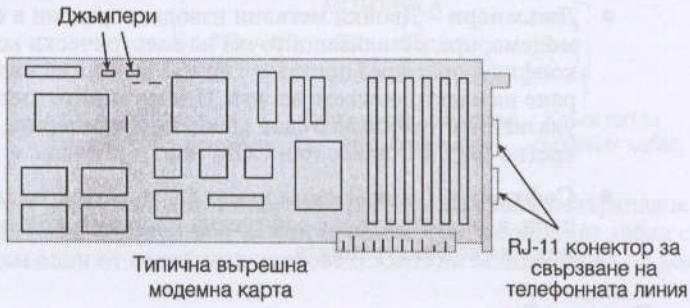
Модемите се произвеждат като два физически типа: *вътрешни* и *външни*. Всеки от двата типа има предимства и недостатъци; конфигурацията е леко различна в зависимост от типа. И в двата случая модемите са серийни устройства, което означава, че битовете се предават последователно един по един по линията. Това е обратно на паралелните устройства, каквито са принтерите, към които едновременно могат да бъдат изпращани множество битове. Серийното предаване може да бъде оприличено на група от хора, които маршируват в една колона един след друг, а паралелното предаване е подобно на същата група, маршируваща в успоредни редици.

Вътрешни модеми

Едно предимство на вътрешните модеми е тяхната компактност. Вътрешният модем представлява електронна платка (карта), която се включва в ISA

(Industry Standard Architecture) или PCI (Peripheral Component Interconnect) слот във вътрешността на компютъра, както е показано на Фигура 6-1. Това означава, че не се налага да търсите място за допълнително устройство на вашето бюро. Освен това не е нужно да купувате сериен кабел, който ще ви трябва, ако използвате външен модем; често пъти такъв кабел липсва в комплекта на модема.

Фигура 6-1 *Вътрешният модем представлява електронна платка, която се включва в слот в компютъра.*



Конфигурационни параметри на вътрешния модем

Традиционно вътрешните модеми са по-трудни за конфигуриране от външните. Трябва да зададете номер на заявка за прекъсване – IRQ, входно/изходен адрес и виртуален *com* порт, за да гарантирате, че тези настройки няма да влязат в конфликт с настройките на друго устройство в компютъра. Да разгледаме по-подробно всяка настройка и начина, по който се използва:

- **Заявка за прекъсване (IRQ)** – Това е запазено местоположение, което определя къде системата трябва да очаква сигнал за прекъсване от устройството, когато то изпрати такъв. Сигналите от различните устройства, които отиват към процесора по една и съща линия на прекъсване, могат да се смесят едни с други, затова за всяко устройство трябва да бъде зададена отделна IRQ линия.
- **Входно/изходен адрес** – Това е местоположението, където данните, изпращани от устройството, се съхраняват преди тяхната обработка от процесора (CPU). Както при IRQ, ако множество устройства се опитат да използват един и същ входно/изходен адрес, то едно или повече устройства може да не работят правилно.
- **Виртуален com порт** – Това е логически номер на порт, с помощта на който операционната система идентифицира даден сериен порт. Трябва задължително да настроите всяко серийно устройство да използва различен com порт.

Всички популярни операционни системи осигуряват средства, с помощта на които можете да разгледате използваните и свободните ресурси, така че да сте в състояние да изберете ресурси, които да зададете на вашето ново устройство.

Промяна на настройките на вътрешен модем

Вътрешните модеми най-общо осигуряват начин за промяна на конфигурационните настройки. В зависимост от производителя и модела, можете да промените настройките на IRQ, I/O адресите и COM портовете с помощта на:

- **DIP превключватели** – Това са малки едноредови или двуредови пакети от ключове, монтирани на електронната платка на модема, които могат да бъдат премествани в различни позиции. Позицията на превключвателя определя коя настройка трябва да бъде използвана.
- **Джъмпери** – Двойки метални изводи, вградени в електронната платка на модема, представляващи точка на електрически контакт. Джъмперите се конфигурират чрез поставяне на малко мостче върху изводите за затваряне на електрическата верига. Инструкциите към вътрешния модем указват как трябва да бъдат зададени джъмперите, за да използвате конкретно IRQ, I/O адрес или COM порт.
- **Софтуер** – Някои модеми нямат физически превключватели или джъмпери, а се доставят със софтуерна програма, която се изпълнява за промяна на конфигурацията.

Plug and Play

Много съвременни модеми поддържат технологията Plug and Play (PnP), която позволява на операционната система автоматично да открива устройството, да инсталира необходимите софтуерни драйвери, да открива какви ресурси са свободни на компютъра и да назначи тези ресурси на устройството. От страна на потребителя се изисква много малка намеса.

PnP е чудесна – когато работи и когато се съобразявате с няколко особености. Ако сте закупили модем или друго устройство, рекламирано като Plug and Play, то се конфигурира автоматично *само* ако е истина следното:

- BIOS-ът (Basic Input/Output System – базова система за вход/изход) на компютъра поддържа PnP.
- Работите с PnP операционна система.

Трябва да бъдат изпълнени *и двата* критерия. Дънните платки на компютрите, произведени след 1995 г., обикновено поддържат PnP. Операционни системи с поддръжка на PnP са Windows 95, 98, ME и 2000.

ЗАБЕЛЕЖКА Windows NT *не е* PnP операционна система. Но тя има ограничена PnP функционалност и открива някои типове модеми.

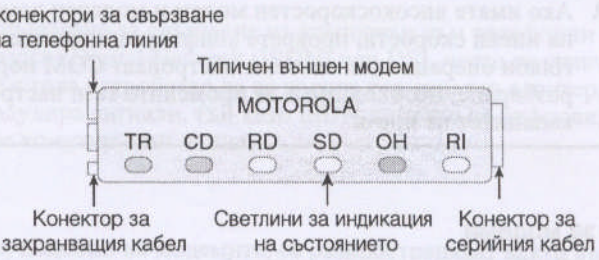
Външни модеми

Външните модеми имат две предимства пред вътрешните:

- Повечето външни модеми имат светлинна индикация на състоянието, която показват кога на модема е подадено захранване, кога е свързан или осъществява трансфер на данни. Вижте Фигура 6-2.

- Външните модеми като цяло са по-лесни за инсталиране и конфигуриране. Те нямат превключватели и джъмпери за настройка и не е нужно да отваряте кутията на компютъра.

Фигура 6-2 *Външните модеми осигуряват светлинна индикация за състоянието.*



Външните модеми използват отделен източник на електрозахранване, а вътрешните модеми се захранват от самия компютър. Серийният кабел свързва модема към един от серийните портове (COM) на задния панел на компютъра.

Съображения при избор на сериен порт

За да използвате външен модем, трябва да имате свободен сериен порт. Повечето компютри имат два вградени серийни порта, означени като COM 1 и COM 2, които имат конектори на задния панел на компютъра.

Много устройства, например скенери, цифрови фотоапарати и серийни посочващи устройства (например мишка), също използват серийни портове. Ако вашият компютър няма свободен сериен порт, разполагате с няколко опции:

- Използване на вътрешен модем.
- Инсталиране на разширителна карта на компютъра, която позволява да добавяте още серийни портове.
- Ако дънната платка на компютъра поддържа универсална серийна шина (universal serial bus – USB), можете да свържете множество серийни устройства, включително модеми, към един сериен порт. Може да се наложи да добавите карта за поддръжка на USB конектор, но в такъв случай ще ви бъде нужен USB модем.

UART чипове

Серийните портове използват чип, наречен универсален асинхронен приемник/предавател (Universal Asynchronous Receiver/Transmitter – UART) за осъществяване на серийни комуникации. Този чип се разпространява в различни типове, а използваният тип определя скоростта на предаване на данните по този сериен порт.

Първите персонални компютри имаха чипове 8250 UART. Най-високата скорост на този чип е 9600 bps, което означава, че ако свържете високоскоростен (56 kbps) модем към един от тези портове, реалната скорост ще бъде ограничена от скоростта на UART чипа.

Модерните компютри имат UART чипове от сериите 16450 или 16550. Тези серийни портове поддържат скорости на трансфер до 115 200 bps.

UART чиповете 16650 и 16750 са достъпни също като допълнителни карти от тип „разширен сериен порт“. Вътрешните модеми имат свои собствени UART чипове, вградени в платката, затова скоростта на com порта на компютъра няма значение.

ЗАБЕЛЕЖКА Ако имате високоскоростен модем и модерен компютър, но се свързвате само на ниски скорости, проверете конфигурационните настройки на COM порта. Някои операционни системи настройват COM портовете на 9600 bps по подразбиране; необходимо е да промените тази настройка, за да постигнете пълния капацитет на порта.

Драйвери за модема

Драйверите представляват софтуерни програми, които действат като връзка между хардуерното устройство и операционната система. Драйверният софтуер обикновено се доставя от производителя на модема със самото устройство, или може да бъде свален от Web сайта на производителя.

Трябва да инсталирате правилния драйверен софтуер за вашето устройство, защото ако кодът на операционната система включваше поддръжка за всички хардуерни устройства, които биха могли някога да бъдат използвани с него, операционната система щеше да изисква значително повече дисково пространство – повечето от което зает от софтуер, който никога няма да бъде използван.

Конфигуриране на модема

В допълнение към инсталирането на драйверния софтуер, който позволява операционната система да разпознава модема и настройките на IRQ, I/O адреса и COM порта, трябва да конфигурирате модема да набира телефонни номера и да поддържа връзката. Модерните операционни системи имат вградена поддръжка за dialup мрежа. Може да се наложи да инсталирате услугите за отдалечен достъп, ако модемът не е бил поставен при първоначалното инсталиране на операционната система.

Банки от модеми

Даден компютър може да бъде конфигуриран като *dialup сървър (dialup server)*, (наричан също *сървър за отдалечен достъп* (*remote access server*), за да позволява други компютри да го набират и да се свързват към него по телефонните линии. Компютрите, изпълняващи мощен сървърен софтуер, могат да поддържат едновременно голям брой входящи връзки за отдалечен достъп; например Windows NT Server поддържа до 256 връзки.

Как можете да свържете 256 модема към отдалечен сървър? Когато имате много едновременно изпълнявани dial-in връзки (например когато сървърът принадлежи на компания с много служители, работещи дистанционно, които трябва да се свързват към корпоративната мрежа на организацията от вкъщи), можете да използвате *банка от модеми*. Банките от модеми се наричат също гнезда от модеми или *модемни пулове (modem pools)*.

Банката от модеми ви позволява да използвате група от модеми (обикновено монтирани на общ стенд) с един сървър и да хоствате множество отдалечени

връзки. Стендът от модемни карти се управлява от интерфейс, който се свързва към сървъра, към маршрутизатора или директно към локалната мрежа. Разбира се, необходима е и телефонна линия за всяка отделна връзка.

ISDN и DSL адаптери

Устройството, използвано за свързване на компютър към телефонни линии от тип Integrated Services Digital Network (ISDN) или DSL често се означава като модем. По-точно е това устройство да се нарича терминален адаптер, защото не модулира и демодулира сигнали, тъй като ISDN линиите са цифрови, за разлика от аналоговите комутируеми линии.

ISDN адаптери

ISDN адаптерите, подобно на модемите, се разпространяват както във вътрешни, така и във външни модификации. Те се конфигурират подобно на модемите, но типичната ISDN услуга със скорост 128 kbps се състои от два канала за данни, всеки от които работи на 64 kbps. Двата канала се използват най-често в *multilink* конфигурация за осигуряване на пропускателна способност от 128 kbps. Технологията ISDN ще разгледаме по-късно в тази глава, в секцията „ISDN".

В повечето случаи двата канала за данни имат отделни телефонни номера. ISDN адаптерите са конфигурирани с информация за *идентификатора на услугата и линията (service profile identifier – SPID)* за всеки канал, който се състои от телефонния номер, двуцифрен терминален идентификатор за споделяне и двуцифрен терминален идентификатор (TID). Някои модерни ISDN адаптери поддържат автоматично селектиране на SPID и не изискват от вас въвеждане на тази информация.

DSL адаптери

И двата края на DSL връзката се изисква устройство, наречено *крайна точка* (*endpoint*) (често означавано като DSL модем), което се свързва към Ethernet мрежовата интерфейсна карта, инсталирана в компютъра. В някои случаи крайната точка е външна. В други крайната точка и мрежовата интерфейсна карта са разположени заедно на една и съща карта.

Оборудването от страната на клиента

Оборудването от страната на клиента (Customer premises equipment – CPE) е обобщен термин, който обхваща няколко различни устройства. При клиента се изисква задължително наличие на този хардуер, за да обработва входните предавания от WAN връзки, като линии от T тип, X.25 връзки и Frame Relay връзки.

Разпространените типове CPE са следните:

- Устройство за обслужване на канала/устройство за връзка с цифровата услуга (Channel Service Unit/Digital Service Unit – CSU/DSU), използвано с връзките с комутиране на вериги, например T-1 линия. Устройството за обслужване на канала (CSU) приема и предава сигнали към/от WAN линията. Устройството за връзка с цифровата услуга (DSU) поддържа контрола над линията, грешките в синхронизацията и регенерира сигнала.
- Асемблатор/деасемблатор на пакети (packet assembler/disassembler – PAD), използван при връзки с комутиране на пакети, като X.25. PAD е

асинхронно устройство, което позволява на множество терминали да споделят една мрежова линия. Потребителите набират PAD устройствата посредством модеми.

WAN топологии

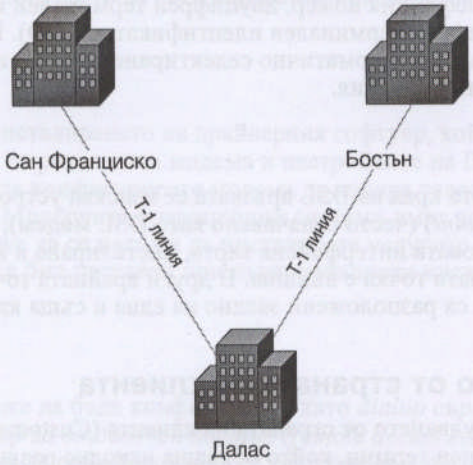
Някои от концепциите на LAN топологиите, които разгледахме в Глава 2, „Категоризация на мрежите“, се прилагат и към WAN мрежите. Но в контекста на WAN мрежите *топологията* описва подреждането на предавателните съоръжения.

Най-простата WAN топология е простата връзка от точка до точка. WAN мрежата, подобно на LAN, може да използва също традиционни мрежови топологии, например кръг или звезда.

WAN от точка до точка

WAN от точка до точка е подобна на LAN топологията, означавана като линейна шина. Връзката за отдалечен достъп, която може да бъде най-разнообразна – от dial-up връзка с модеми до специализирана T-1 линия, свързва всяка точка на WAN към следващата. За илюстрация на това вижте Фигура 6-3.

Фигура 6-3 *WAN от точка до точка свързва директно две крайни точки.*



Това е сравнително евтин начин за свързване на малък брой WAN сайтове. Но този метод не притежава отказоустойчивост. Например на Фигура 6-3, ако оборудването в офиса в Далас излезе от строя, Сан Франциско и Бостън не могат да комуникират един с друг. Друг недостатък е ограничената възможност за мащабиране (възможността за елегантно нарастване), т.е. мрежата да продължава да функционира ефикасно с нарастването на нейната големина). Ако добавите още една точка към WAN в Нешвил, между Далас и Бостън, увеличавате броя на необходимите скокове (hops) за комуникация с Бостън или Сан Франциско.

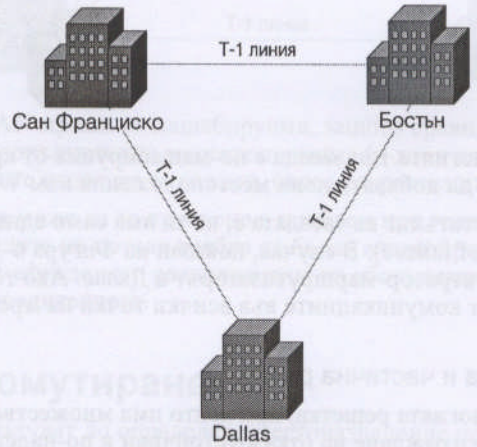
ЗАБЕЛЕЖКА В глобалните мрежи *скокът* (*hop*) се дефинира като пътуването от един маршрутизатор до следващия. *Броят на скоковете* (*hop count*) е броят на маршрутизаторите, през които преминава пакетът при своето предаване от източника до местоназначението.

Връзката от точка до точка работи най-добре при малки WAN мрежи, само с две или три местоположения.

WAN кръг

Както е показано на Фигура 6, кръгът се конструира с изграждане на връзка тип „от точка до точка" – това са връзките от точка A до точка B, от точка B до точка C и от точка C обратно до точка A.

Фигура 6-4 *WAN може да използва кръгова топология.*



Кръговата топология осигурява редундантност (излишък). В примерът, показан на Фигура 6-4, ако линията между Далас и Сан Франциско пропадне, данните между двата града могат да бъдат предавани през Бостън.

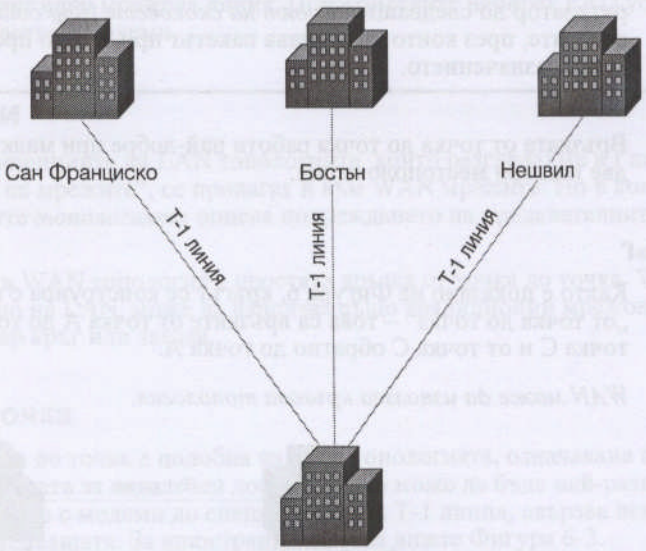
Кръговата топология е по-скъпа за реализиране от топологията от точка до точка и страда от същия проблем на мащабируемостта, характерен за топологията от точка до точка.

Кръговата топология е подходяща за WAN мрежи, които свързват само няколко местоположения и имат нужда от надеждността, предлагана от редундантните пътища.

WAN от тип звезда

Когато WAN се разполага в конфигурация звезда, се използва устройство, наречено *концентратор-маршрутизатор*; то служи за централна точка, към която се свързват всички мрежови маршрутизатори. Например на Фигура 6-5 концентратор-маршрутизаторът е разположен в главния офис в Далас.

Фигура 6-5 *WAN мрежата, подредена в топология тип звезда, е мащабируема.*



Топологията тип звезда е по-мащабируема от кръга; също така в звезда е полесно да добавяте нови местоположения към WAN мрежата.

Недостатъкът на звездата е, че тя има само една точка на прекъсване (single point of failure). В случая, показан на Фигура 6-5, тази точка на прекъсване е концентратор-маршрутизаторът в Далас. Ако това устройство пропадне, прекъсват комуникациите във всички точки на мрежата.

WAN от тип пълна и частична решетка

Топологията решетка, при която има множество връзки между точките, осигурява изграждане на отказоустойчиви и по-надеждни WAN мрежи. Но за нещастие тя е и най-скъпата топология за реализиране и става неудобна при голям брой сайтове.

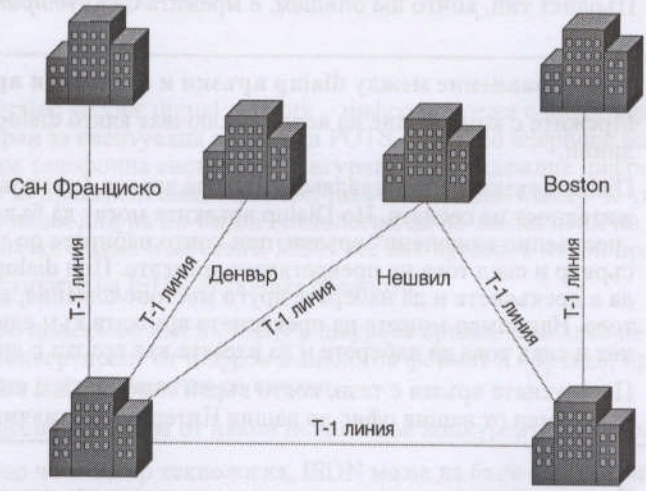
Пълната решетъчна топология изисква всеки сайт в мрежата да бъде свързан към всеки друг сайт. При частичната решетка има по-малък брой редундантни връзки. Това осигурява надеждност, близка до тази на пълната решетка, на значително по-ниска цена.

Разгледайте Фигури 2-10 и 2-11 в Глава 2 за илюстрация на топологиите решетка и частична (хибридна) решетка.

Многослойни WAN мрежи

Многослойната WAN мрежа прилича на звездата по това, че използва концентратор-маршрутизатори, но е по-надеждна, защото свързва два или повече от тези концентратори с други местоположения, разположени каскадно (в поднива) на главните маршрутизатори. За илюстрация вижте Фигура 6-6.

Фигура 6-6 *Многослойната WAN мрежа предлага повече надеждност от простата звезда.*



Многослойните WAN мрежи са мащабируеми, защото сравнително лесно могат да бъдат добавяни допълнителни местоположения (и дори допълнителни слоеве). Тази топология се използва за големи, бързо разрастващи се мрежи.

Потокът на трафика може да се превърне в проблем при големите многослойни WAN мрежи. Моделите на потока трябва да бъдат анализирани внимателно, за да се гарантира най-ефикасното разположение на оборудването с цел постигане на най-добра производителност.

Типове мрежово комутиране

Данните могат да пътуват до определено местоназначение по няколко различни типа линии, използвайки една от следните технологии на комутиране:

- Комутиране на вериги
- Комутиране на пакети

В следващите секции ще разгледаме как работи всяка от тези технологии.

Сравнение между комутирането на вериги и комутирането на пакети

Много хора бъркат комутирането на вериги и комутирането на пакети. Пример за мрежа с комутиране на вериги е телефонната мрежа. Когато изберете номера на филиален офис в Бостън, се установява верига за цялото времетраене на телефонния разговор. Сигналът продължава да използва тази верига (пътека), докато прекъснете връзката, поставяйки телефонната слушалка обратно в гнездото. Ако на другия ден се обадите отново, може да бъде използван различен път.

Пример на мрежа с комутиране на пакети е Интернет. Когато изпратите съобщение по електронната поща до офиса в Бостън, то бива разделено на парчета, наречени пакети. Всеки пакет може да премине по различен път, за да достигне до компютъра местоназначение; тези пакети се подреждат отново на другия (приемния) край.

Мрежи с комутиране на вериги

Първият тип, който ще опишем, е мрежата с *комутиране на вериги*.

Сравнение между dialup връзки и посветени връзки

Мрежите с комутиране на вериги включват както dialup, така и посветени наети линии.

Dialup връзката представлява временна връзка, установявана за цялата продължителност на сесията. Но Dialup връзките могат да бъдат реализирани като „постоянно включени" връзки, при които набирате по телефона отдалечения сървър и след това не прекратявате връзката. При dialup връзката е възможно да я прекъснете и да наберете друго местоположение, ако желаете да направите това. Например можете да прекъснете връзката към един доставчик на Интернет и след това да наберете и да влезете във връзка с друг.

Посветената връзка е тази, която върви само от една конкретна точка до друга (например от вашия офис до вашия Интернет доставчик).

Технологията на комутиране на вериги има дълга история и е по-стара от комутирането на пакети. Комутирането на вериги е по-подходящо, когато данните трябва да бъдат предавани в реално време (както при телефонен разговор). Мрежите с комутиране на вериги са връзково-ориентирани мрежи, защото преди да започне предаването, се изгражда връзка.

В тази глава ще опишем накратко следните технологии за комутиране на вериги:

- PSTN
- ISDN
- DSL
- Наети линии
- Digital data service (DDS)
- T-носещи
- Switched 56

PSTN

Най-разпространеният тип dialup WAN връзки се изграждат с помощта на PSTN – аналоговите телефонни линии, инсталирани в повечето обществени и бизнес организации.

PSTN имат две големи предимства:

- Достъпни са почти навсякъде по света.
- Не са скъпи

Дадена dialup връзка, използваща обикновени телефонни линии, е лесна за реализиране. Освен модема не се изисква специално оборудване, а аналоговите модеми са лесно достъпни, прости за конфигуриране и не особено скъпи.

Още по начало телефонната система не е създадена за трансфер на данни; тя е предназначена за предаване на глас. Високата скорост не е била на дневен ред, което е довело до вродено ограничение на скоростта на предаване на данни.

Качеството на линията също е определящ фактор. Дори при най-съвременни модеми със скорост 56 kbps, много телефонни линии са способни да осигуряват не-повече от 40-45 kbps.

ISDN

ISDN (integrated service digital network – цифрова мрежа с интегрирани услуги) бе проектиран за евентуална замяна на POTS (plain old telephone service – обикновена стара телефонна система) и осигуряване на надеждна цифрова връзка, подходяща за предаване както на глас, така и на данни. Макар че това не стана, а появата в наши дни на по-бързи технологии на по-ниски цени ни кара да мислим, че то никога няма и да стане, ISDN все пак предлага някои предимства.

Характеристиките на ISDN включват следното:

- Както подсказва името, ISDN е цифрова връзка. Тъй като не е необходимо конвертиране от цифров в аналогов формат и обратно, производителността и надеждността са високи.
- По-лесно достъпна от някои нейни нови конкуренти, например DSL.
- Макар че е dialup технология, ISDN може да бъде използвана като постоянно включена връзка, т.е. като посветен ISDN).
- Услугата ISDN е по-скъпа от аналоговата услуга (PSTN) и изисква специализирано оборудване както в централата на телефонната компания (т.е. цифрово комутиране), така и от страната на клиента (т.е. при ISDN терминалния адаптер).

ISDN веригата се изгражда от един или повече канали, които пренасят данни (наречени носещи (bearer) канали или B-канали) и канал за управление (наречен Delta-канал или D-канал).

Всеки B-канал осигурява пропускателна способност 64 kbps, а B-каналите могат да бъдат обединявани с помощта на *инверсно мултиплексиране*. Това позволява да комбинирате честотната лента на множество канали, за да създадете една високоскоростна връзка. D-каналът осигурява 16 или 64 kbps в зависимост от реализацията на интерфейса.

ISDN се предлага от повечето телефонни компании в два стандартни интерфейса за достъп:

- **Basic Rate ISDN (BRI)** – Този интерфейс се състои от два B-канала със скорост 64 kbps (за постигане на обединена използваема пропускателна способност от 128 kbps) и един D-канал със скорост 16 kbps.
- **Primary Rate ISDN (PRI)** – Състои се от 23 B-канала със скорост 64 kbps (формиращи обща пропускателна способност от 1,472 Mbps) и един D-канал със скорост 64 kbps.

BRI често се реализира за висикоскоростен трансфер в жилищни райони или между малки бизнес организации, а PRI се използва най-често за предаване на цифров глас заедно с телефонни системи от вида PBX (private branch exchange – частни телефонни централи).

ЗАБЕЛЕЖКА PBX представлява частна телефонна мрежа, която работи в една организация. Вътрешните потребители споделят общи външни линии и избирането на вътрешни номера в организацията изисква набиране само на разширение от три или четири цифри. Традиционната PBX изискваше оператор, който отговаряше на всички входящи обаждания и след това включваше всеки към съответното вътрешно направление. Модерното оборудване автоматизира този процес.

DSL

DSL е относително нова технология, предложена от телефонните компании като допълнителна услуга върху съществуващите медни кабели. DSL предлага няколко предимства върху други типове WAN връзки.

Следващият списък представя характеристиките на DSL:

- DSL предлага скорости до и надхвърлящи тези на T-1, при това само на част от цената на вторите. В много области DSL услугата струва по-малко от ISDN.
- DSL е технология, която винаги е включена. Няма нужда от избиране при всяко желание за установяване на връзка.
- По една и съща линия едновременно могат да бъдат предавани глас и данни.
- В момента достъпността е ограничена. В централата на телефонната компания, обслужваща местоположението, в което се намирате, трябва да има инсталирано DSL оборудване, а при повечето разновидности на DSL услугата трябва да отстоите на определено разстояние от централата, за да получите тази услуга.

DSL се среща в няколко варианта:

- **ADSL (Asymmetric DSL)** – Това е най-разпространената реализация. Скоростите варират от 384 kbps до 6 Mbps (или повече) по низходящия поток (downstream), обикновено комбиниран с по-ниска скорост на възходящия поток (upstream).
- **SDSL (Symmetric DSL)** – Осигурява същата скорост за сваляне и качване.
- **HDSL (High Data Rate DSL)** – Тази разновидност обикновено осигурява пропускателна способност от 768 kbps и в двете посоки.
- **VDSL (Very High Data Rate DSL)** – Има възможност за пропускателни способности между 13 Mbps и 52 Mbps.
- **IDSG** – Това е DSL по ISDN линии. Има максимална скорост от 144 kbps, но е достъпна в зони, които не са подходящи за други DSL реализации.

Универсалният термин за DSL, обхващащ всички реализации, е xDSL.

ADSL, която в момента е най-популярната реализация на DSL, по принцип осигурява бърза скорост на трансфер по низходящия поток (обикновено 1,5 Mbps) и по-бавен възходящ поток. Това почива на теорията, че повечето потребители на Интернет осъществяват достъп главно до електронна поща и сърфират в Web, т.е. изпълняват задачи с интензивно сваляне (download). Но

по-ниските скорости на качване (upload) не са толкова подходящи, ако се занимавате с хостване на Web или FTP сървър, или изпълнявате други задачи с интензивно качване.

ADSL обикновено използва мултиплексиране с разделяне на честотата (frequency division multiplex – FDM) за разделяне на честотната лента и създаване на множество канали. Някои реализации на ADSL използват различен метод, наречен *ехоподтискане (echo cancellation)*. Той е по-ефективен, но също така по-сложен и по-скъп.

Таблица 6-1 обобщава достъпните в момента реализации на DSL.

Таблица 6-1 *Сравнение на реализациите на DSL.*

Тип DSL	Средни скорости	Предимства	Недостатъци
ADSL	384 kbps до 6 Mbps	Сравнително не скъпи; по-широко реализирани от другите типове	Могат да бъдат инсталирани само на разстояние около 5 км от централата на телефонната компания; скоростта на възходящия трафик е малко по-ниска.
SDSL	До 3 Mbps	Предлага една и съща скорост за предаване на данни по възходящия и низходящия поток.	По принцип са по-скъпи и по-малко разпространени от ADSL; значително по-бавна скорост
IDSL	144 kbps	Могат да бъдат инсталирани в много местоположения, където не са достъпни други типове DSL поради разстоянието.	По-скъпи от ADSL; значително по-ниска скорост.
HDSL	768 kbps възходящ и низходящ поток	По-бързи от IDSL и някои реализации на ADSL.	Не са широко достъпни.
VDSL	13 Mbps до 52 Mbps	Изключително висока скорост, подходяща за аудио и видео на живо.	Не са широко достъпни; най-скъпият тип DSL.

Наети линии

За WAN връзки, които изискват гарантирана висока производителност и надеждност, съществува възможността за наемане на линии от телефонната компания за частно ползване. Наетата линия осигурява постоянна връзка от една точка до друга (например от един филиален офис до друг или от LAN мрежата на вашата компания към вашия Интернет доставчик).

DDS

DDS беше една от първите цифрови услуги, които станаха достъпни за обществото. DDS осигуряваше скорост на трансфер 56 kbps. Тя изгуби популярността си в състезанието с технологията T-носеща поради това, че линията T-1 обикновено осигурява по-висока пропускателна способност на долар.

Т-носещи

Т-носещите представляват специализирани вериги, които обикновено се наемат от големи компании за осигуряване на високоскоростни данни, глас, аудио и видео по високонадеждна връзка от точка до точка.

Т-носещите вериги обикновено се изграждат по медни проводници, но могат да се използват също оптични кабели, коаксиални кабели и дори безжични технологии.

Във всеки от краищата се използва CSU/DSU устройство за кодиране на данните, изпращани по Т-носещата. Макар че цените за Т-1 линии паднаха драстично през последното десетилетие, те си остават скъпа възможност. Една Т-1 линия обикновено струва от 10 до 20 пъти повече от услугата DSL при една и съща сравнявана скорост (1,5 Mbps).

Защо някой трябва да плаща за Т-1, когато са достъпни опции на по-ниска цена с високи скорости? Самата достъпност е една от причините; DSL се разпространи едва отскоро и дори в областите, където се предлага, много бизнес организации и държавни институции не се намират в границите, изисквани за доставяне на услугата.

Друга причина да платите допълнително за Т-1 е гарантираната пропускателна способност. Това се нарича *съгласувана скорост на предаване на информацията (committed information rate – CIR)*. При DSL услуга със скорост 1.5 Mbps телефонната компания ви продава услуга, която има максимална скорост на трансфер 1,5 Mbps. Реално вашата линия може да не работи на тази скорост през цялото време. Когато наемете Т-1 връзка, телефонната компания гарантира скоростта на данните от 1,544 Mbps. Това може да бъде важно съображение за корпоративни организации, които зависят от производителността на мрежата.

Буквата Т в Т-носещата се отнася до предавателния канал; самият сигнал поточно се означава като скорост на сигнала за данни (DS rate). Сигурно сте чували и двете наименования – DS-1 и Т-1, използвани за означаване на един и същ тип линия. Таблица 6-2 съдържа списък на най-разпространените реализации на Т-носещи.

Таблица 6-2 *Разпространени реализации на Т-носещи*

Означение на носещата	Скорост на сигнала за данни	Скорост на трансфер на данни
Т-1	DS-1	1,544 Mbps
Т-2	DS-2	6,312 Mbps
Т-3	DS-3	44,736 Mbps
Т-4	DS-4	274,760 Mbps

Т-носещите линии се състоят от множество канали с скорост 64 kbps. Възможно е да наемете само част от Т-1 линия (на инкременти от 64 kbps), ако не желаете цялата пропускателна способност от 1,544 Mbps; това се нарича *частична* Т-1.

Switched 56

Switched 56 е разширена версия на PSTN. Това е цифрова връзка с комутиране на вериги, която осъществява трансфер на данни по един канал с пропускателна способност 56 kbps. Switched 56 е по-евтина, но също е по-бавна от линията

T-1. Тя е dialup технология, затова може да бъде подходяща в случаи, в които не е нужна постоянна посветена връзка.

За разлика от PSTN мрежите, които теоретично имат възможност за скорости от 56 kbps, но на практика най-често постигат скорости не по-високи от 50 kbps (а понякога падат и много по-ниско от тази стойност), Switched 56 може да осигури надеждна връзка с пълни 56 kbps. Тъй като е цифрова връзка, коефициентът на грешките е по-нисък, отколкото при обикновената PSTN (аналогова) линия.

Връзката се нарича „switched" (комутирана), защото отделните канали на 56 kbps се комутират през T-1 верига и се предават към местоположението на конкретен потребител.

Популярността на Switched 56 намаля с разпространението на други опции с ниска цена и висока пропускателна способност (като ISDN и DSL).

Мрежи с комутиране на пакети

Мрежите с комутиране на пакети са мрежи, в които пакетите от данни могат да преминават по различни маршрути за достигане до едно и също местоназначение. В приемащия край пакетите се сглобяват отново в правилен ред. Мрежите с комутиране на пакети често се илюстрират като облак, защото точният маршрут на пътуване на данните е неизвестен.

Технологиите на комутиране на пакети са следните:

- X.25
- Frame Relay
- Asynchronous Transfer Mode (ATM)

ЗАБЕЛЕЖКА Макар че често чувате термина *мрежа X.25*, технически правилният термин е PSDN (*Packet Switched Data Network – мрежа с комутиране на пакети от данни*). X.25 всъщност е протоколът, който се използва за комуникация между терминалното оборудване за данни и мрежата.

В следващите секции ще разгледаме по-детайлно всяка от технологиите.

X.25

X.25 беше една от първите мрежи с комутиране на пакети и беше проектирана за работа с мейнфрейм компютри на IBM (като IBM 360) и използване на аналогово предаване.

X.25 първоначално се наричаше протокол ARPAnet I822; името X.25 дойде от спецификациите за протоколи, използвани от тази технология, които бяха установени от Международния комитет по телефония и телеграфия (CCITT) през 1976 г.

ЗАБЕЛЕЖКА През 1993 г. CCITT промени своето име на Международен съюз по телекомуникации (ITU).

Технологията PSDN работи в първите три слоя на OSI модела. Технологията, наречена X.25, всъщност се осъществява от няколко протокола:

- PSDN използва протокол, наречен X.21, във физическия слой (вариант на протокола X.21от физическия слой, наречен X.21bis, се използва в САЩ).
- Протокол с име Link Access Procedure Balanced (LAPB) се използва в каналния слой.
- В мрежовия слой се използва протокола Packet Layer Protocol (PLP) за асемблиране на фреймове от каналния слой в пакети.

Основната цел при разработката на протокола X.25 беше надеждността. По времето на неговото проектиране през 70-те години, тогавашните компютри и телефонни линии бяха предразположени към грешки. Затова PSDN, работещ по X.25, включваше проверка за грешки с излишък за компенсиране на тези проблеми. Резултатът беше високо надеждни средства за трансфер на данни, но производителността беше понижена от активната допълнителна проверка за грешки. Протоколът PSDN обикновено прави трансфер със скорост 64 kbps или по-малка.

Днес още има мрежи с комутиране на пакети от данни (PSDN), които се използват. За да реализирате WAN връзка по PSDN, може да направите едно от следните:

- Да наберете по телефонна линия асемблатор/деасемблатор (PAD) с асинхронен модем
- Да осъществите синхронна връзка с помощта на протокола X.32
- Да използвате X.25 смарт карта за директно свързване към PSDN

Frame Relay

Frame Relay е по-нова технология с комутиране на пакети, която беше проектирана за използване само по цифрови линии и която измести X.25. Frame Relay е вариант и подобрение на технологията X.25, разработена от CCITT. Тя използва само първите два слоя на OSI, вместо първите три (както X.25). Frame Relay беше разработена с цел използване на предимствата на модерните компютри и телефонни линии, които са много по-надеждни от използваните по време на създаването на X.25. Тя стана популярна опция за WAN връзки и най-общо предлага висока производителност и ценово по-ефективно решение в сравнение с X.25.

Frame Relay работи само в двата най-ниски слоя на OSI модела – физическият и каналният. Frame Relay използва по-малко допълнителна информация от X.25 и поради това е по-бърза. Тя може да работи на скорости T-1 и T-3 (от 1,5 Mbps до почти 45 Mbps).

Frame Relay се нарича технология с *бързи пакети (fast packet)*.

Типичната реализация на Frame Relay използва *постоянна виртуална верига (permanent virtual circuit – PVC)* за осигуряване на постоянно установена връзка. Тъй като доставчиците на услуги по правило променят цените според степента на използване (което се нарича *пропускателна способност по заявка [bandwidth on demand]*), можете да избегнете цената на специалната наетата линия.

Frame Relay има висока производителност, защото не включва интензивна проверка и корекция на грешки, характерна за X.25. Фреймовете с грешки се игнорират, а отговорността за откриване на липсващия пакет и заявка за повторното

му предаване се пада на крайните точки (комуникационните компютри). Тъй като предаването е цифрово, има относително малко грешки, затова Frame Relay работи добре в WAN среда по T-1 линии.

ATM

ATM е популярна технология с комутиране на пакети, която беше проектирана за поддръжка на високоскоростни приложения, като поточно аудио и видео. Важна концепция за ATM мрежата е качеството на услугата (quality of service – QoS), която представлява начин за контролиране на заделянето на пропускателна способност за конкретни приложения с цел осигуряване на гарантирана пропускателна способност там, където е най-важна.

ATM е базирана на хардуер, което означава, че цялото оборудване на мрежата трябва да бъде проектирано за работа с ATM. Предимството е, че в резултат получаваме високи скорости на обработка и комутиране. Стандартните скорости на ATM трансфера са 25 Mbps, 155,520 Mbps и 622.080 Mbps; ATM има възможност и за скорости от порядъка на 10 Gbps. За нещастие, тази производителност се предлага на висока цена. ATM е скъпа за реализиране технология, защото целият хардуер на мрежата трябва да поддържа ATM – мрежовите интерфейсни карти (NIC), хъбовете и другото ATM-съвместимо оборудване.

ATM е модерна цифрова технология, която разделя данните на парчета с фиксирана дължина 53 байта, наречени *клетки*. За ATM хедъра се използват пет байта, които съдържат адресна информация.

ATM може да бъде използвана както за LAN, така и за WAN мрежи и използва мултиплексиране за едновременен трансфер на глас и видео по мрежата. Комутирането на клетки е функция на ATM хардуера (за разлика от Frame Relay, при която това е софтуерна функция).

Можете да се свържете към ATM мрежа чрез директна връзка или връзка по заявка. Връзката между две крайни точки е *виртуална верига*; тя може да бъде PVC или комутируема виртуална верига (switched virtual circuit – SVC). И при PVC, и при SVC ATM използва предварително дефинирани вериги за изграждане на виртуални вериги по времето на връзката, както правят X.25 и Frame Relay. Това спестява голямо количество време и е още един фактор за високата скорост на ATM.

Много експерти по мрежи предричат, че в бъдеще ATM ще стане масова технология както за LAN, така и за WAN мрежи.

Перспективни WAN технологии

Постоянно се разработват нови, по-бързи и по-ефикасни WAN технологии. Много от тях взаимодействат една с друга за осигуряване на поддръжка на приложения, изискващи висока пропускателна способност, като тези, които се използват днес, и тези, които се очакват в бъдеще.

В следващите секции ще разгледаме нови високоскоростни технологии, включващи OC-SONET, широколентов ISDN, CATV и SMDS.

OC-SONET

OC означава *optical carrier (оптична носеща)*, а SONET означава Synchronous Optical Network (синхронна оптична мрежа). SONET е протокол от физическия

слой, който осигурява високоскоростно предаване с използване на оптичен кабел. SONET има възможност за скорости на предаване почти до 20 Gbps, а ATM може да се изпълнява по SONET за постигане на много високи скорости на трансфер на данни.

ЗАБЕЛЕЖКА За означаване на технологията SONET извън САЩ може да срещнете термина Synchronous Digital Hierarchy (SDH).

Скоростта на SONET се измерва по стандартите OC. Таблица 6-3 илюстрира достъпните скорости на предаване (наречени OC нива).

Таблица 6-3 *OC скорости на предаване на сигнала.*

OC ниво	Скорост на предаване на сигнала
OC-1 (базова скорост)	51,84 Mbps
OC –3	155,52 Mbps
OC –12	622,08 Mbps
OC –48	2,488 Gbps

SONET се използва като физическа основа за друга технология – широколентов ISDN – която е разгледана в следващата секция.

Широколентов ISDN

Широколентовият ISDN (BISDN) представлява перспективна технология, предназначена за използване на оптичен кабел и радиовълни за предаване на данни на високи скорости по SONET, FDDI (Fiber Distributed Data Interface) и Frame Relay.

Широколентовите технологии, които могат да изпращат множество канали с данни, видео и глас по един и същ кабел или друга преносна среда, нарастват по популярност с нарастването на връзките към Интернет и други мрежи с изисквания за висока пропускателна способност. Други широколентови технологии са DSL и кабелните модеми.

CATV

Компаниите за кабелна телевизия (CATV) усетиха страхотна възможност: Те вече притежаваха развита инфраструктура от коаксиален кабел в повечето големи градове и много селски райони. Този кабел можеше да бъде използван не само за предаване на телевизионни сигнали, а също за предаване на компютърни данни. Множество кабелни оператори днес предлагат акаунти за достъп до Интернет.

Кабелът не е основна WAN технология. Първоначално той бе предназначен да ви позволи да комуникирате само със сървъра на кабелната компания (под формата на приемане на входящи телевизионни канали). Макар че всички клиенти бяха свързани към една и съща мрежа с коаксиален кабел, преминаващ през техните съседи, мрежата не беше предназначена за комуникация между самите крайни абонати. Реално мрежата изобщо не беше проектирана да дава

на потребителите възможност да си предават данни, а само да ги приемат. Кабелният модем промени всичко това.

Достъпът до Интернет по кабел изисква кабелен модем, който се свързва както към входящия коаксиален кабел, така и към мрежовата интерфейсна карта на компютъра на потребителя (обикновено това е 10BaseT Ethernet карта).

В този сценарий кабелната компания играе ролята на ISP за потребителя. Няма възможност за отделяне на физическата линия от услугата за достъп, както при достъпа по телефонни линии. С други думи, не можете да наемете линията от кабелната компания и да я използвате за свързване към сървъра на някой друг ISP.

От друга страна, когато плащате телефонна такса за използване на телефонна линия (независимо дали линията е PSTN или специализирана T-1), можете да закупите Интернет акаунт от всеки ISP, който изберете (включително от телефонната компания, която предоставя линията). Макар че същият този метод е технически възможен при кабела, кабелните компании пакетираха двете услуги заедно и условията на техните договори за услугата изискват да използвате единствено кабелната компания като ваш ISP (доставчик на Интернет).

Кабелната инфраструктура може да поддържа или еднопосочни, или двупосочни предавания. *Еднопосочният кабел* осигурява предаване по коаксиалния кабел само на низходящия поток (downstream). Качването трябва да бъде извършено по обикновена аналогова телефонна линия, която също се включва в кабелния модем. При еднопосочния кабел скоростите на качване са ограничени до стандартните нива, които могат да бъдат постигнати по PSTN, т.е. по-малко от 56 kbps. Скоростите на сваляне варират от 364 kbps до 1,5 Mbps.

Двупосочният кабел осигурява както качване, така и сваляне по коаксиален кабел. Независимо от това много кабелни компании ограничават скоростта на възходящия поток до 128 kbps, за да откажат клиентите от пускане на сървъри (което често се забранява и от условията на договора с кабелната телевизия).

Кабелът е постоянно включена технология, но еднопосочният кабел пак изисква от вас да изберете изграждане на връзка. Голямо предимство на CATV е нейната ниска цена; но в много области потребителите се сблъскват с проблеми на надеждността. Тъй като кабелът е технология със „споделена честотна лента“ (т.е. цялата честотна лента или пропускателна способност се разделя между всички потребители, които в даден момент се намират в даден кабелен сегмент), производителността може да спадне, когато множество хора в съседство влязат в мрежата. Съществуват също проблеми със сигурността, които в момента правят CATV по-подходяща за жилищните райони, отколкото за бизнеса.

SMDS

Switched Multimegabit Data Service (SMDS) е нова технология с комутиране на пакети, която е предназначена специално за WAN връзки, подложени на голямо количество „пиков“ трафик. (*Пиков* означава предаване, което се извършва на пикове, а не в постоянен равномерен поток.)

SMDS е безвръзково-ориентиран; т.е. няма изискване преди да започне предаването на данните да бъде установена връзка или верига. Тя използва сравнително големи пакети, с дължина до 7168 байта. SMDS адресите, които представляват десетцифрени номера (като телефонни номера), се използват за идентифициране на SMDS подмрежата. SMDS връзките се свързват към SMDS суич по гръбнака на мрежата на телефонната компания, обикновено по множество връзки от типа OC-3 SONET.

SMDS беше разработена като обществена мрежа за осигуряване на услуги, подобни на тези на LAN, с изключение на това, че обхваща голяма градска област. Скоростите на трансфер на данни обикновено варират от 1,544 Mbps до 45 Mbps. Технологията е мащабируема и може да бъде използвана заедно с ATM. Но SDMS не е широко достъпна като Frame Relay и други услуги, а SMDS оборудването може да бъде намерено трудно.

Безжични WAN мрежи

В много случаи е невъзможно – или най-малкото неудобно или скъпо – да се прокара кабелна линия за свързване на WAN сайтове. Безжичните решения са особено подходящи, когато е важно данните да бъдат комуникирани в реално време, или когато потребителите са в движение. Безжичните WAN работят най-добре при комуникация на малки количества данни.

Безжичните технологии, използвани за WAN, са следните:

- **Радиочестотни (RF) технологии** – Specialized Mobile Radio (SMR) осигурява скорости за предаване на данни от 1200 bps до 19 200 bps. Разширеният SMR (ESMR) е цифровата реализация на SMR.
- **Сателитни технологии** – Тази технология използва както услуги с комутиране на вериги, така и услуги с комутиране на пакети на скорости от 4800 до 9600 bps.
- **Микровълнови технологии** – Тази технология използва клетъчни техники на микровълнови честоти за осигуряване на висока скорост и капацитет (безжична широка лента).
- **Клетъчни технологии** – Това осигурява връзка с комутиране на вериги по аналогови или цифрови клетъчни връзки.
- **Технологии за мрежи с пакети от данни** – Тази технология осигурява WAN с комутиране на пакети без настройка на обаждането.

Сравнени с кабелните връзки, безжичните комуникации често са по-скъпи и относително бавни. Например аналоговите клетъчни системи обикновено осигуряват скорости на трансфер не повече от 14 000 докато цифровите клетъчни системи осигуряват до 64 kbps.

Връзки между LAN и WAN

В днешния кабелизиран свят локалната връзка често пъти не е достатъчна. Нито една LAN не е остров, или най-малкото все по-малко остават локалните мрежи, които не са свързани към други мрежи, тъй като за бизнес организациите стана критично важно свързването на LAN към корпоративна WAN, към глобалния Интернет или и към двете.

Съществуват няколко начина да свържете вашата LAN мрежа към външния свят, в зависимост от вашия бюджет и нужди. Разбира се, най-очевидният начин да осигурите на потребителите на мрежата достъп до други мрежи е да оборудвате всеки компютър с модем и телефонна линия. По този начин всеки потребител може да установява dialup връзка към Интернет доставчик или друг отдалечен сървър. Но това решение има много недостатъци:

- То става ужасно скъпо с нарастване на броя на потребителите. Трябва не само да купите хардуер (модема) за всеки компютър, а също да платите

за всяка отделна телефонна линия, а ако потребителите се свързват към Интернет – отделен ISP акаунт за всеки от тях.

- Ако разрешите на потребителите да избират външни номера с помощта на модем, можете да създадете сериозни рискове за сигурността, в случай че данните във вашата мрежа са конфиденциални. Организацията има малък контрол върху мрежите, към които се свързват потребителите, и аудиторията, пред която могат да бъдат изложени данните на организацията.
- Изисква се висока степен на интелигентност на потребителите, което означава значителни разходи за обучението им по конфигуриране и управление на техните собствени dialup връзки.

Съществува по-добър начин. Реално няколко алтернативи предлагат предимства пред стария начин за свързване на LAN потребители към WAN. Всеки от тях има предимства и недостатъци, които зависят от конкретната ситуация.

В следващите секции накратко ще опишем следните опции за връзка LAN/WAN:

- Транслирани връзки
- Прокси сървъри
- Маршрутизирани връзки

Транслирани връзки

Един от най-ценово ефективните начини за свързване на всички компютри от малка LAN към Интернет или друга WAN връзка е чрез адресна транслация. *Адресната транслация (address translation)* позволява всички компютри да осъществяват достъп до WAN мрежата посредством един хост компютър, използващ само една телефонна линия и ISP акаунт (или друга WAN връзка) и само един регистриран публичен IP адрес.

Как се действа адресната транслация

Компютърът, на който се изпълнява софтуерът за транслация на адреси се поставя между обществената WAN и частната LAN. Той има интерфейси и към двете мрежи. Този компютър има частен IP адрес, използван за комуникации с другите компютри в LAN, и публичен IP адрес (който може да бъде задаван с помощта на услугата Dynamic Host Configuration Protocol (DHCP) от сървъра на Интернет доставчика при установяване на WAN връзката). Този компютър ще наричаме *хост за адресна транслация*.

ЗАБЕЛЕЖКА DHCP е услуга, задаваща автоматично IP адреси и други TCP/IP настройки на компютри, които са конфигурирани да използват DHCP. Повече за DHCP ще научите в Глава 8, „Мрежови протоколи и услуги“.

Адресната транслация работи, като асоциира частния IP адрес на всеки компютър в LAN, изпращащ данни „навън“, към номер на порт на хост компютъра. Тази информация се добавя към IP хедъра на пакета, който след това се изпраща навън по WAN с IP адреса на хост компютъра (този, който има физическа връзка към WAN).

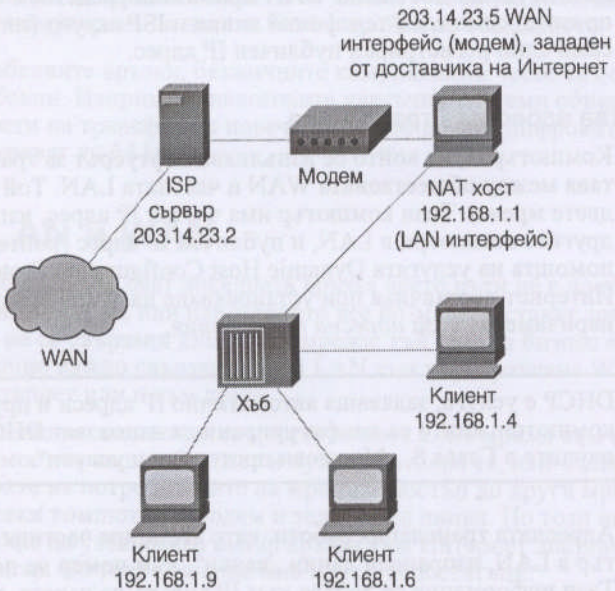
Когато компютър в локалната мрежа отвори Web браузър и например изпрати заявка за разглеждане на URL, хост компютърът задава на тази заявка номер на порт, идентифициращ компютъра от локалната мрежа, който е изпратил заявката. След това хостът изпраща заявката навън към Web сървъра на Интернет доставчика. Когато страницата се върне на хост компютъра (на който IP адресът е показан в хедъра като източник на заявката), хостът се консултира със своята таблица за преобразуване на адресите, намира съответствието между пакетите и компютъра, който първоначално е изпратил заявката, и след това препраща Web страницата към този компютър.

Информацията в таблицата за адресна транслация включва следното:

- Оригиналните IP адреси на източника и местоназначението (идентифициращи изпращащия компютър в мрежата и компютърът извън мрежата, към който са изпратени данните)
- Оригиналните номера на портове на източника и местоназначението (идентифициращи приложението, което изпраща или приема заявката; например HTTP изисква Web страниците обикновено да бъдат изпращани до TCP порт 80)
- Последователни номера (идентифициращи реда, в който се изпращат пакетите)
- Времеви маркер

Транслирането на мрежови адреси (network address translation – NAT) е обобщен термин, стандартите за който са разработени и публикувани в RFC 1631. Не всички технологии за адресна транслация спазват тези стандарти. Фигура 6-7 илюстрира стъпките на процеса на транслацията.

Фигура 6-7 *Процесът на NAT включва транслирането на частни адреси в публични адреси.*



1. Потребителят на клиентския компютър (IP адрес 192.168.1.9) отваря Web браузър и въвежда URL адреса www.tacteam.net в полето за адреси. Софтуерът на браузъра изпраща HTTP заявка до IP адреса, асоцииран с „дружелюбното име" www.tacteam.net.
2. NAT хостът в локалната мрежа на клиента асоциира заявката от 192.168.1.9 за www.tacteam.net към номер на порт в таблицата със съответствията. Таблицата съдържа IP адресите на оригиналния източник и местоназначението, а също и номерата на TCP/UDP портовете на оригиналния източник и местоназначението.
3. NAT хостът променя хедъра така, че за външната мрежа първоизточникът на пакета изглежда сякаш не идва от 192.168.1.9, а от публичния IP адрес, назначен от доставчика на Интернет на адаптера на хоста, свързван към външната мрежа.
4. NAT хостът изпраща заявка за www.tacteam.net до ISP сървъра. DNS (Domain Name System) услугата „преобразува" дружелюбното името в IP адреса на сървъра, на който се съхранява началната страница на www.tacteam.net.
5. Заявката се приема от сървъра www.tacteam.net и страницата се връща на публичния IP адрес, използван от NAT хоста.
6. NAT хостът се консултира със своята таблица адресна транслация, след което определя, че страницата трябва да бъде изпратена до клиента на адрес 192.168.1.9 (и на съответния номер на TCP/UDP порт).

NAT софтуер

Някои операционни системи, например Windows 98/2000 и текущите версии на Linux, имат вградена поддръжка на адресна транслация. В Linux това се означава като IP *маскиране*. Windows 98 и 2000 Professional наричат тази възможност Internet Connection Sharing (ICS), макар че тази услуга може да бъде използвана за споделяне на връзка към частна отдалечена мрежа или също към виртуална частна мрежа (VPN). Windows 2000 Server поддържа най-гъвкавата и устойчива версия на адресна транслация. Ако операционната система не включва адресна транслация, можете да използвате допълнителна NAT програма, за да осигурите същата функционалност. Такива програми са:

- **Sygate от Sybergen Software** – www.sygate.com
- **NAT32 от A.C.T. Software** – www.nat32.com

Друг по-интелигентен (и малко по-труден за конфигуриране) тип софтуер, който можете да използвате за споделяне на връзка, е *проксито*. Тази опция ще разгледаме в следващата секция.

Прокси сървъри

Прокси сървърът прави много повече от осигуряването на споделена връзка към WAN, макар че служи за тази цел. Прокси сървърът действа като посредник, разделяйки LAN мрежата от външната мрежа, и може да осигури защита чрез филтриране на входящите и изходящите пакети. Също така той увеличава Web производителността, като *кешира* Web места, за които често са правени заявки.

Прокситата използват метод за адресна транслация, но той не е задължително съвместим с NAT спецификациите в RFC 1631.

Как работи проксито

Прокси сървърът приема заявки за Интернет ресурси от прокси клиенти, подобно на начина, по който работи NAT. Прокси сървърът проверява своите настройки за филтриране (които се конфигурират от администратора). Ако заявката отговаря на изискванията на филтъра, сървърът първо проверява в своя кеш от съхранени страници. В случай че исканата страница е там, прокси сървърът връща страницата на клиента, отправил заявката. В този случай отпада необходимостта от изпращане на заявка до ISP сървъра. Ако страницата не е в кеша, прокси сървърът отправя заявка за страницата до ISP сървъра, приема я и я връща на клиента.

Както при NAT, вътрешните клиенти, които осъществяват достъп до Интернет посредством прокси сървър, са невидими за Интернет: цялата външна комуникация се извършва от прокси сървъра.

Прокси софтуер

Софтуерът на прокси сървъра осигурява повече защита и разширена производителност от NAT. Въпреки това той може да бъде доста скъп и обикновено е по-труден за инсталиране и настройка, защото Интернет приложенията на всички клиентски машини (например Web браузърите) трябва да бъдат индивидуално конфигурирани за използване на прокси сървъра.

За да използвате NAT, трябва да настроите само TCP/IP конфигурацията на клиента, за да придобиете IP адрес посредством DHCP, а другата необходима информация може да бъде разпространена автоматично до клиентите от DHCP сървъра.

За популярните операционни системи са достъпни множество приложения за прокси сървъри, сред които:

- **Rideway на DGL** – dgl.com/rideway
- **Winproxy на Ositis** – www.winproxy.com/toc
- **Microsoft Proxy Server на Microsoft** – www.microsoft.com
- **Squid за UNIX на SCO** – www.sco.com

Някои прокси програми, например Microsoft Proxy Server, се изпълняват само на мрежова операционна система (NOS), например Windows NT или Windows 2000 Server. Други, подобно на Rideway и Winproxy, могат да бъдат използвани в настолни операционни системи, като Windows 95/98, Windows NT Workstation и Windows 2000 Professional.

Софтуерът, който комбинира прокси и NAT технологии, понякога се означават като *прозрачни проксита*.

Маршрутизирани връзки

Маршрутизираната връзка представлява друг начин, осигуряващ на компютрите в LAN мрежата достъп до WAN. Маршрутизираната връзка позволява всеки компютър да участва директно в Интернет, за разлика от NAT и прокси връзките, където отделните компютри трябва да преминават през посредник.

Конфигурирането на маршрутизирана връзка изисква подробни познания върху TCP/IP адресирането и трябва да закупите и конфигурирате *маршрутизатор*.

Допълнително всеки компютър в LAN, който се свързва към външната мрежа, трябва да има „законен“ регистриран публичен IP адрес.

ЗАБЕЛЕЖКА Вижте Глава 8 за повече информация относно TCP/IP и IP адресирането, и Глава 9, „Най-широкомащабната мрежа: глобалният Интернет“, за да научите повече за маршрутизацията.

Защо да се използва маршрутизирана връзка?

Голямо предимство на NAT и прокси решенията е възможността за свързване на малки LAN към публични WAN с помощта само на един IP адрес. Но в някои ситуации това може да не е най-доброто решение.

Поради начина на работа на транслацията, протоколи, които не съхраняват информация за адресиране в IP хедъра, не работят с NAT. В някои случаи могат да бъдат добавени NAT редактори за модифициране на IP пакета, така че NAT да може да работи. В други случаи (например когато пакетите се автентицират и криптират с помощта на IP Security [IPSec]) адресната транслация е невъзможна.

Конфигуриране на маршрутизирана връзка

Маршрутизираната връзка изисква или специализирано маршрутизиращо устройство, каквото е маршрутизаторът, или използването на компютър, изпълняващ операционна система, която дава възможност за IP препращане (в последния случай компютърът действа като маршрутизатор).

Компютри, които използват TCP/IP за комуникация, трябва да имат конфигурирани следните свойства:

- IP адрес, който е валиден за мрежата, в която ще комуникират компютрите
- Подмрежова маска, определяща каква част от IP адреса идентифицира компютъра и каква част идентифицира мрежата.

Компютрите, участващи в *маршрутизирана* мрежа, трябва също да имат *конфигуриран подразбиращ се* шлюз (gateway). Това е адресът на маршрутизатора, който има две мрежови връзки: едната към LAN мрежата, а другата към външната мрежа.

ЗАБЕЛЕЖКА Трябва да въведете адреса за DNS сървър, ако искате да използвате „дружелюбни“ имена на хостове (например URL като www.tacteam.net) вместо IP адреси. Повече за DNS ще научите в Глава 8.

За да настроите маршрутизирана връзка към Интернет, TCP/IP протоколът на маршрутизатора се конфигурира с IP адрес, подмрежова маска и адрес на DNS сървър, осигурени от доставчика на Интернет, след което се конфигурира статичен подразбиращ се маршрут за използване на Интернет интерфейса.

Компютрите в LAN мрежата, които се свързват към Интернет по подобен начин, се конфигурират с IP адреси, подмрежова маска и адрес на DNS сървъра, получен от ISP доставчика. Също така те се конфигурират да използват IP адреса на маршрутизатора в техния LAN интерфейс като техен подразбиращ се адрес на шлюз.

Обобщение

В тази глава изучихте глобалните мрежи и утвърдени и перспективни технологии, които могат да бъдат използвани за свързване на компютри в отдалечени местоположения.

Разгледахме хардуера на WAN и след това преминахме към WAN топологиите. После разгледахме предимствата и недостатъците на WAN конфигурациите, като връзките от точка до точка, кръг, звезда, пълна или частична решетка и многослойни WAN мрежи.

След това се видяхме разликите между мрежите с комутиране на вериги и тези с комутиране на пакети, след което разгледахме характеристиките и технологиите, асоциирани с PSTN, ISDN, xDSL, DDS, T-носещи, X.25, Frame Relay, ATM, OC-SONET, BISDN, CATV, SMDS и безжичните WAN технологии.

После разгледахме как можете да свържете LAN към WAN. По-конкретно изучихме няколко начина за осигуряване на достъп до Интернет или друга външна мрежа за всички компютри от локална мрежа. Научихме за транслиращите връзки, използващи NAT, което понякога се нарича споделяне на връзка или IP маскиране. След това разгледахме начина на настройка на маршрутизирана връзка за тези обстоятелства, при които адресната транслация е нежелана или невъзможна.

С тази глава завършва Част I на книгата. Сега вече имате изградени познания за основните концепции на мрежите. В Част II ще разгледаме хардуера и софтуера, с помощта на които работят мрежите. Глава 7 ви запознава с физическите компоненти на мрежата.

Допълнителни източници

Един отличен ресурс за информация за различни WAN технологии в WANsites на адрес www.networkcomputing.com/wansites/default.html.

Подробни и ясни изложения на различните WAN технологии могат да бъдат намерени на Web сайта на High Performance Networking Unleashed, на адрес www.officewizard.com/books/network.

Чудесно подробно разглеждане на NAT е достъпно онлайн на адрес www.suse.de/~mha/linux-ip-nat/diplom.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Кои от следните хардуерни настройки се използват най-често за конфигуриране на вътрешния модем. (Изберете всички верни отговори.)

- **a** I/O адрес
- **b** IP адрес
- **c** IRQ
- **d** Виртуален COM порт

2 CSU/DSU и PAD са примери на кое от следните?

a ISDN терминални адаптери
b Оборудване от страната на клиента
c Терминални идентификатори
d Концентратор-маршрутизатори

3 На какъв тип мрежа са примери връзките от тип PSTN, ISDN, DSL, DDS и T-носеща?

a Мрежи с комутиране на вериги
b Мрежи с комутиране на пакети
c Switched 56 мрежи
d LAN мрежи

4 Кое от следните е истина за ISDN? (Изберете всички верни отговори.)

a Това е аналогова връзка.
b Най-общо е по-скъпа от PSTN.
c Изисква специално оборудване в телефонната централа и от страната на клиента.
d Използва верига, състояща се само от един канал.
e Може да извършва трансфер едновременно на глас и данни.

5 Коя WAN топология е най-мащабируема?

a От точка до точка.
b Кръг.
c Звезда.
d Всички изброени са еднакво мащабируеми.

6 Коя беше първата технология за комутиране на пакети, която беше базирана на протокола ARPAnet 1822?

a Frame Relay
b X.25
c ATM
d DSL

7 Коя от следните характеристики на технологията Frame Relay я различава от X.25? (Изберете всички верни отговори.)

a Frame Relay предлага висока производителност.
b Frame Relay използва комутиране на пакети.
c Frame Relay използва цифрово предаване на сигнали.
d Frame Relay не включва разширена проверка за грешки.

8 Кое от следните описва ATM? (Изберете всички верни отговори.)

a Използва пакети с променлива дължина.

b Използва 53 байтови единици от данни, наречени клетки.

c Може да извършва трансфер едновременно на видео, глас и данни.

d Използва предварително дефинирани вериги.

e По-евтина е от други WAN технологии.

9 Коя от следните технологии има възможност за скорости на предаване до 2,488 Gbps?

a ADSL

b TI

c T-1

d OC-SONET

10 Кое от следните е истина за NAT? (Изберете всички верни отговори.)

a NAT изисква всеки компютър във вътрешната мрежа да има регистриран публичен IP адрес.

b NAT транслацията е съвместима с всички приложения.

c NAT транслацията е несъвместима с технологии, които криптират IP данни.

d NAT използва таблица за асоцииране на частни вътрешни IP адреси с един или повече външни публични адреси.

Част II

Мрежов хардуер и софтуер

Глава 7 Физически компоненти на мрежата

Глава 8 Мрежови протоколи и услуги

Глава 9 Най-широкомащабната мрежа: глобалният Интернет

Глава 10 Мрежови операционни системи 7

Глава 11 Директорийни услуги

Глава 12 Настолни операционни системи

Глава 13 Хибридни мрежи

Глава 7

Физически компоненти на мрежата

След като вече научихте основните концепции, свързани с компютърните мрежи, ще обърнем вашето внимание към нещо по-конкретно: физическите компоненти, използвани за свързване на PC-тата така, че те да могат да споделят ресурси.

Компонентите, необходими за свързването на компютрите в мрежа, могат да са изключително евтини и прости — няколко мрежови интерфейсни карти (network interface cards — NICs) и Ethernet кабел. От друга страна, мрежата може да бъде и достатъчно сложна, че да изисква ползване на услугите на *мрежов архитект*, който да определи необходимите устройства, а бюджетът е възможно да достигне до шестцифрени суми и повече.

В тази глава дискутираме някои от най-често използваните мрежови хардуерни устройства и среди за пренос, включващи мрежови интерфейсни карти, кабелна и безжична среда за пренос, а също и устройства за свързване.

Мрежови интерфейсни карти

Най-основният хардуер, необходим за свързване на един компютър в режа, е мрежовата интерфейсна карта, наричана също мрежов адаптер или просто мрежова карта. Мрежовите карти съществуват под няколко форми, които са дискутирани в секцията „Избиране на мрежова карта".

Мрежовата карта обикновено е устройство от физическия слой, а драйверите за нея (софтуерът, осъществяващ връзката между картата и операционната система на компютъра) работят в каналния слой на OSI модела.

В следващите секции разглеждаме ролята на мрежовата карта в мрежовите комуникации. Ще научите как да избирате подходящия мрежов адаптер и как мрежовите карти се конфигурират и използват за изпращане и приемане на данни по мрежата.

Ролята на мрежовите карти в мрежовите комуникации

За комуникиране по мрежа винаги се изисква някакъв вид мрежов интерфейс. Когато се свързвате към мрежа отдалечено посредством аналогова телефонна линия, мрежовият интерфейс се явява вашият модем — той играе същата роля, каквато се пада на мрежовата карта в една локална мрежа.

Мрежовата интерфейсна карта е основният хардуерен компонент в мрежовите комуникации. Тя преобразува *паралелния* сигнал, произведен от компютъра, в

серийна (*последователна*) форма, която се изпраща по мрежовия кабел. Единиците и нулите на двоичната комуникация се преобразуват в електрически импулси, светлинни импулси, радиовълни или каквато и да е друга схема за предаване на сигнали, използвана от преносната среда.

Важна част от мрежовия интерфейс е така наречения *трансивър* (или *приемопредавател*). При някои мрежови карти, като например тези за 10Base2 и 10BaseT мрежи, трансивърът е вграден в самите тях. Други, например предназначените за 10Base5 мрежи, са снабдени с интерфейс за свързване на (мрежови) устройства (attachment unit interface – AUI), представляващ конектор, към който кабелът се свързва към външен трансивър. Трансивърът (приемопредавателят) служи именно за приемане и предаване на сигнали.

Освен че подготвя данните за изпращане към преносната среда, мрежовата карта отговаря и за управлението на потока от данни между компютрите и преносната среда, както и за приемане на входящите данни.

Избиране на мрежова карта

Когато избирате мрежова карта за даден компютър, трябва да вземете предвид следните неща:

- **Мрежова архитектура** – Мрежовата карта трябва да може да работи със съществуващата технология за предаване. Въпреки това е възможно да се използва *филтър на преносната среда* (*media filter*), който ви позволява например да използвате Token Ring карта в Ethernet мрежа. За повече информация относно популярните LAN архитектури вижте глава 6, „WAN връзки".
- **Тип на преносната среда** – Ethernet мрежите могат да използват дебел коаксиален кабел (10Base5), тънък коаксиален кабел (10Base2) или кабел с усукана двойка (10BaseT). Конекторът на картата трябва да съвпада с буксата на кабела. Съществуват и мрежови карти за безжични или оптични мрежи. Кабелната и безжичната преносна среда са дискутирани по-нататък в тази глава в секцията „Мрежова преносна среда".
- **Скорост на предаване на данните** – Ако имате 100Mbps хъбове, една 10Mbps мрежова карта няма да работи с тях. Можете обаче да поставите двускоростни компоненти (било то мрежови карти или хъбове), които работят със скорост или 10Mbps или 100Mbps. По същия начин една 4Mbps Token Ring карта не работи в 16Mbps мрежа. Една 16Mbps карта обаче *работи* в по-бавна мрежа, но скоростта ѝ пада до 4Mbps.
- **Тип на свободен разширителен слот** – Имате ли свободен ISA или PCI слот? Дали компютърът е лаптоп и трябва да използва PCMCIA (т.е. PC Card) интерфейс? Нуждаете ли се от специална карта, която се свързва към сериен или SCSI порт? Забележете, че ако имате свободни ISA и PCI слотове, PCI шината е по-бърза.

Типове разширителни шини

Шината за данни представлява канал за предаване, разположен на дънната платка на компютъра. Сигналите се приемат от или предават към всяко устройство, свързано към този канал. Съществуват няколко шинни архитектури, за които се произвеждат мрежови карти:

- **ISA (Industry Standard Architecture – стандартна за индустрията архитектура)** – 16-битов разширителен слот на дънната платка. Цветът му обикновено е черен, а дължината му е по-голяма от тази на PCI слота.
- **EISA (Extended ISA – разширена ISA)** – 32-битова архитектура, съвместима с ISA. Повечето съвременни „ISA" слотове всъщност са EISA.
- **PCI (Peripheral Component Interconnect – свързване на периферни компоненти)** – 32-битова шина, използвана в съвременните компютри (PC-та от клас Pentium и нагоре, както и Macintosh-и). PCI архитектурата поддържа Plug and Play (PnP) устройства. PCI слотовете на дънната платка са бели на цвят и са по-къси от ISA/EISA слотовете.
- **MCA (Micro Channel Architecture)** – Фирмена шина, използвана в някои от компютрите на IBM, която може да работи и като 16-битова, и като 32-битова. В днешно време се среща рядко.
- **PCMCIA (Personal Computer Memory Card International Association; нарича се още PC Card)** – Входно/изходна шина, използваща устройства с размер и форма на кредитна карта. Използвани обикновено в лаптоп и ноутбук компютри, PC Card адаптерите съществуват и за настолни машини.

Съществуват и мрежови карти, които се свързват към SCSI шина. Има също USB (universal serial bus – универсална серийна шина) модели, но те се срещат рядко. Също така забележете, че дънните платки на някои компютри притежават вградени мрежови адаптери, т.е. компонентите на мрежовата карта се намират на самата дънна платка.

- **Операционната система** – Трябва да се уверите, че производителят на мрежовата карта осигурява драйвери за използваната от вас операционна система. Ако използвате някоя от операционните системи Windows, погледнете списъка Microsoft Hardware Compatibility List (HCL) на адрес www.microsoft.com, където са изброени тестваните с операционната система мрежови карти. Популярните операционни системи за настолни компютри са дискутирани в Глава 12, „Настолни операционни системи".

Конфигуриране и използване на мрежова карта

Конфигурирането на мрежова карта е подобно на процеса на конфигуриране на модем, което беше дискутирано в Глава 6. Забележете, че мрежова карта и модемът по същество изпълняват една и съща основна функция.

Както при модемите, трябва да установите следното:

- Прекъсване (IRQ линия)
- Входно/изходен адрес

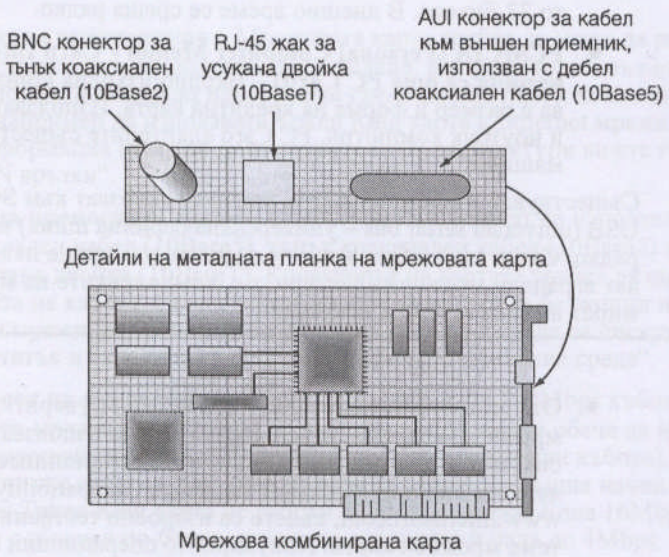
- Адрес от паметта

Това става чрез dip-превключватели, джъмпери или чрез програма за софтуерно конфигуриране, доставена с картата. PnP мрежовите карти могат да бъдат откривани и установявани автоматично от една PnP операционна система, стига и BIOS-ът на компютъра също да поддържа PnP.

Възможно е да се изискват допълнителни конфигурационни параметри, ако мрежовата карта е *комбинирана* (*combo*) т.е., ако може да използва различни типове преносна среда. Една комбинирана карта обикновено има BNC конектор за тънък коаксиален кабел, RJ-45 конектор (RJ е съкращение от registered jack) за усукана двойка, а понякога и AUI конектор за дебел коаксиален кабел. Това означава, че една такава карта работи в 10Base2, 10Base5 и 10BaseT мрежи. Въпреки това в даден момент може да се използва само една преносна среда. Възможно е картата да може сама да определя типа на преносната среда, към която е свързана – в противен случай трябва да избирате ръчно.

Фигура 7-1 показва комбинирана карта с три различни конектора.

Фигура 7-1 *Една комбинирана мрежова карта може да се използва 10Base2, 10Base5 и 10BaseT мрежи.*



Конфигуриране на прекъсването

Обикновено една мрежова карта използва IRQ 3 или IRQ 5. Много карти са установени по подразбиране да използват едно от тези прекъсвания. Ако имате друго устройство, което да използва предефинираното IRQ, ще трябва да промените настройките на едно от устройствата, за да не влизат в конфликт.

Добра идея е да запомните следващата таблица, показваща стандартните подразбиращи се настройки за прекъсванията в едно типично PC. Забележете, че в ранните PC-та бяха налични само първите осем прекъсвания. IRQ 2 се използва като контролер на прекъсванията, за да „пренасочи" заявката за прекъсване към IRQ 9, през което се осъществява връзката към прекъсванията с по-големите номера.

Таблица 7-1 *Стандартни подразбиращи се настройки на прекъсванията при PC-тата*

Устройство	Подразбиращо се прекъсване
VGA графичен адаптер	2 (9)
COM 2 и COM 4 (вторични серийни портове)	3*
COM 1 и COM 3 (главни серийни портове)	4
Вторичен паралелен порт (LPT2) или звукова карта	5
Флопидисков контролер	6
Главен паралелен порт (LPT1)	7
Часовник за реално време	8
Главен SCSI контролер	10*
Вторичен SCSI контролер	11*
PS/2 мишка	12
Математически копроцесор	13
Главен IDE контролер	14
Вторичен IDE контролер	15*

* Тези устройства са опционални и е възможно да не присъстват в много от компютрите. Когато тези устройства липсват, съответните прекъсвания са свободни. Например, при отсъствието на SCSI контролери, IRQ 10 и IRQ 11 са свободни и могат да се назначат на мрежовата карта.

Конфигуриране на входно/изходните портове и адресите от паметта

Освен уникално прекъсване, всяко устройство трябва да има различна настройка за диапазона от входно/изходни портове. *Входно/изходният порт* (I/O порт) е канал, през който данните се прехвърлят между хардуерното устройство и процесора. Номерата на портовете се задават чрез шестнадесетични числа. Следните портове обикновено са свободни за използване от мрежовите карти:

- 300 до 30F
- 310 до 31F

Възможно е да има и други. Обикновено подразбиращата се настройка за входно/изходните портове (тази, която е била зададена фабрично при производството) работи нормално.

Един *адрес от паметта* представлява местоположение в RAM, използвано за съхранение на приеманите и изпращаните данни. Някои мрежови карти не използват паметта на компютъра за тази цел, поради които нямат такава настройка. В противен случай фабрично зададената настройка обикновено работи.

Мрежова преносна среда

Мрежовата *преносна среда* служи за пренасяне на сигналите от едно мрежово устройство към друго. Най-често срещаната преносна среда е кабелът, но съществуват и модерни форми на безжични връзки (например радиовълни, лазерни и инфрачервени лъчи, сателитни връзки и микровълни).

В тази секция най-напред дискутираме типове кабели, използвани за свързване на мрежови компютри, а след това разглеждаме и безжичните опции.

Типове кабели

Повечето съвременни мрежи са кабелни, като най-често използваните кабели са коаксиален, усукана двойка или оптично влакно.

Коаксиален кабел

Коаксиалният кабел би трябвало да е познат на всички, притежаващи кабелна телевизия. Сърцевината му е изградена от мед, като може да бъде или многожичен, или солиден проводник. Сигналът се предава по медта, която е увита в изолатор. Около изолатора е увит друг проводник – метално фолио или оплетка. Този външен проводник е разположен по цялата дължина на кабела. От тук идва и името коаксиален (coaxial), защото по цялата дължина вървят съвместно (co) два физически канала – единият за пренос на сигналите, а другият за земя – при това по една и съща ос (axis). Външният проводник играе ролята на екран срещу различните електромагнитни смущения. Всички тези компоненти накрая са увити във външна защитна обвивка от пластмаса, гума или негорим материал – например тефлон.

ЗАБЕЛЕЖКА Кабелите с негорима опаковка са задължителни за повечето сгради, в които мрежата се прокарва през *пленума* – пространството между окачения таван и етажната плоча над него. Това се налага, защото опаковката на стандартния коаксиален кабел е направена от поливинилхлорид (PVC), който отделя токсични газове при изгаряне.

Поради дебелата изолация и доброто екраниране, коаксиалният кабел е по-неподатлив на външни електромагнитни смущения, отколкото усуканата двойка.

Съществуват хиляди различни типове и категории коаксиални кабели, както може да се види от каталозите на всеки производител. Много от тях се използват от мрежи със специално предназначение, като например за свързване на научни инструменти или друга специализирана апаратура. Дискутираните в следващите секции типове са обобщени в Таблица 7-2 и са единствените, които трябва да познавате, когато става въпрос за компютърни мрежи.

Таблица 7-2 *Типове коаксиални кабели и техните характеристики*

Обозначение	Общо наименование	Описание	Предназначение
RG-8, RG-11	Thicknet	Дебел коаксиален кабел с диаметър половин инч	10Base5
RG-58 A/U	Thinnet	Тънък коаксиален кабел с диаметър четвърт инч	10Base2
RG-58 C/U	Thinnet (военна спец.)	Тънък коаксиален кабел с диаметър четвърт инч	10Base2 (военни цели)
RG-62	ARCnet	Тънък коаксиален кабел	ARCnet мрежи

В ранните реализации на Ethernet, коаксиалният кабел беше най-популярният тип. Кабелът с усукана двойка обаче го измести. Коаксиалният кабел за Ethernet мрежите има две основни разновидности: тънък и дебел, които се наричат съответно *thinnet* и *thicknet*.

ЗАБЕЛЕЖКА Коаксиалният кабел, използван от кабелните телевизионни оператори, прилича много на thinnet кабела, но те не са взаимозаменяеми. Този за кабелната телевизия е RG-59 и има импеданс 75 ома.

Тънък коаксиален кабел

Тънкият коаксиален кабел е с диаметър приблизително една четвърт инч и е по-гъвкав, отколкото thicknet кабела. Използва се в Ethernet 10Base2 мрежи, а сигналът може да се пренася на разстояние до 185 метра, без да се влошава неговото качество.

Тънкият коаксиален кабел понякога се нарича RG-58. Неговият *импеданс* (т.е. неговото съпротивление спрямо течащия по проводника ток) е 50 ома.

Основна технология на електрониката

Електрическият ток е поток от електрони, или положително заредени атоми. *Ампер* е основната единица за измерване на електрическия ток.

Съпротивлението (наричано също импеданс) е начин за измерване на количеството съпротива срещу протичането на електрически ток. Различните материали притежават различно ниво на съпротивление. Съпротивлението се измерва в *омове* – на името на немския учен Георг Ом, който е постулирал математическата връзка между електрическия ток, съпротивлението и напрежението (законът на Ом). Символът за ом е гръцката буква омега (Ω).

Напрежението, или *електродвижещата сила*, се нарича също електрически потенциал. То се измерва със силата, която кара електроните в проводника (среда, провеждаща или предаваща електрически заряд) да се движат.

Честотата е мярката за това, колко често се извършва дадено периодично събитие (например сигнал, извършващ един пълен цикъл). Единицата мярка за честота е *херц*.

Коаксиалният кабел е стандартизиран за цялата индустрия чрез спецификациите RG (Registered Grade). В компютърните мрежи се използват само няколко от стотиците класификации.

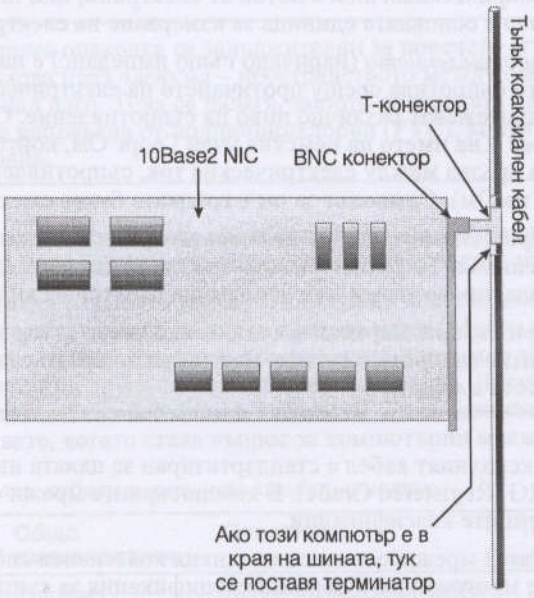
10Base2 мрежите използват тънкия коаксиален кабел RG-58 A/U. Сърцевината му е многожична. Военната спецификация за същия тип кабел е RG-58 C/U. При него външната обвивка е малко по-дебела, което го прави по-устойчив на топлина, студ, течности и други външни влияния.

RG-58 /U на външен вид е подобен на RG-58 A/U, само че медната сърцевина е плътна. Той не отговаря на 10Base2 спецификациите, затова *не* трябва да го използвате при изграждане на компютърни мрежи. Тъй като импедансът му е различен, той се използва като антенен кабел, а също и за други цели. За разликата между двата типа кабели вижте Фигура 7-2.

Фигура 7-2 *Разликата между кабелите с многожична и плътна сърцевина.*

Thinnet кабелът се свързва към мрежовата карта посредством BNC Т-конектор, който се закрепва към BNC конектора на самата мрежова карта, както е показано на Фигура 7-3.

Фигура 7-3 *Тънкият коаксиален кабел се свързва към мрежовата карта чрез BNC Т-конектор.*



Във всеки от краищата на thinnet мрежата се изисква наличието на терминатор. Терминаторът се свързва към неизползвания край на Т-конектора.

Дебел коаксиален кабел

Дебелият коаксиален кабел, наричан също thicknet, има приблизително два пъти по-голям диаметър от този на thinnet кабела – около половин инч. Thicknet беше оригиналният тип кабел, използван в ранните Ethernet мрежи, поради което често се нарича *стандартен Ethernet*.

Дебелият коаксиален кабел е тип RG-8 или RG-11. Поради по-дебелата сърцевина той може да предава сигнали на доста дълги разстояния – 500 метра – без затихване. Той обаче е по-скъп и с него се работи по-трудно, отколкото с тън-

ката версия, защото не е толкова гъвкав и се използва външен приемопредавател, който трябва да се свързва към кабела с помощта на така наречения „*вампирски зъб*“. Зъбът се впива в сърцевината на кабела. Изграждането на връзка е по-сложно, отколкото използването на BNC конектори при thinnet, както е показано на Фигура 7-4.

Фигура 7-4 *10Base5 мрежите използват външен приемопредавател, който се свързва към дебелия коаксиален кабел посредством вампирски зъб.*

ЗАБЕЛЕЖКА Един друг вид коаксиален кабел, използван често в миналото за изграждане на ARCnet мрежи, е 90-омовият RG-62. През последните години ARCnet архитектурата загуби своята популярност, както е дискутирано в Глава 5, „LAN връзки“.

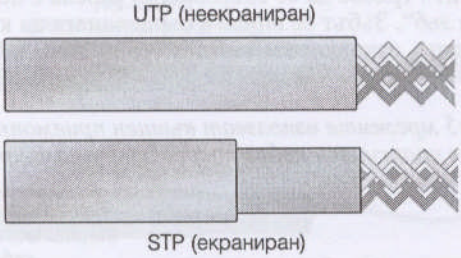
Кабел тип усукана двойка

В днешно време, когато повечето хора споменават термина *Ethernet кабел*, те имат предвид кабела тип усукана двойка, използван в повечето съвременни Ethernet мрежи. Той се нарича *усукана двойка*, защото под външната опаковка са скрити усукани по двойки изолирани медни проводници, като по този начин се предотвратяват паразитните кръстосани шумове (т.е. влиянието на сигнала от единия проводник върху сигнала, предаван по другия). Колкото по-голям е броят на усукванията за един фут, толкова по-добра е степента на защита срещу кръстосаните шумове.

Телефонните компании използват кабел усукана двойка за вътрешно опроводяване: това спомага за неговата популярност, защото повечето сгради вече са окабелени с такъв тип кабел за целите на телефонната система.

Кабелът тип усукана двойка е наличен в два основни типа: неекранирана усукана двойка (unshielded twisted-pair – UTP) и екранирана усукана двойка (shielded twisted-pair – STP), както е показано на Фигура 7-5. Телефонните комуникации и повечето Ethernet мрежи използват UTP. STP се използва в Token Ring и AppleTalk мрежи.

Фигура 7-5 *Разликата между STP и UTP.*



Когато към усуканата двойка се добави екраниране, то намалява влиянието на външните електромагнитни смущения. Това обаче увеличава затихването и може да повлияе върху съпротивлението на проводника, предизвиквайки загуба на данни.

UTP кабел

UTP е много популярен тип кабел за LAN мрежи поради няколко причини:

- Относително евтин
- Гъвкав е и с него се работи лесно
- Използва популярните RJ-45 конектори, които изглеждат и действат като по-малките RJ-11 конектори (популярни в България като евро-жакове), използвани от телефонните апарати.
- Използва се в звездна топология, предоставяща преимуществата, дискутирани в Глава 2, „Категоризиране на мрежите“.

UTP кабелите са разделени на категории в зависимост от тяхното приложение и скоростта на пренасяне на данните. За справка вижте Таблица 2-3 в Глава 2 – в нея са изброени UTP категориите, като е дадено тяхното приложение и скоростта на пренос.

ЗАБЕЛЕЖКА UTP стои в основата на телефонните връзки, които са положени в стените на сградите; кабелите завършват с розетки, в които се включват RJ-11 конектори (жакове). Най-често кабелът от розетката до телефонния апарат е *праволинейна* двойка медни проводници и се нарича „сребърен атлаз“ поради лъскавия му сив цвят.

Подобно на коаксиалния кабел, UTP има две разновидности – стандартна и огнеупорна (за пленум).

STP кабел

Екранирането се реализира чрез медна оплетка или фолио, обвити около изолираните медни двойки вътре в най-външната опаковка. Това намалява въздействието на електромагнитните смущения, но пък оскъпява кабела в сравнение с UTP версията и създава други проблеми, както беше дискутирано в предишните секции на тази глава.

STP най-често се използва в AppleTalk мрежите и Token Ring мрежите на IBM.

Влакнесто-оптичен кабел

Влакнесто-оптичният кабел (наричан също *оптично влакно*, *оптичен кабел*, или само *влакно*) е по-нова и по-бърза, но и сравнително скъпа преносна среда, набираща все по-голяма популярност с нарастването на популярността на високоскоростните приложения. Въпреки че често се използва за мрежи със скорост 100 Mbps, той може да работи и със скорост 1 Gbps и повече.

ЗАБЕЛЕЖКА Lucent Technologies са документирали скорост на предаване на данни от порядъка на над 3 *терабита* в секунда в лабораторни условия, използвайки множество лазери в комбинация с оптично влакно. Един терабит се равнява на един трилион бита (1000 Gbps).

Вместо мед, влакнесто-оптичният кабел използва тънки нишки стъкло или пластмаса, по които сигналът се предава под формата на светлинни импулси.

Освен скоростта, оптичният кабел има още няколко преимущества:

- Той е по-сигурен от коаксиалния кабел и усуканата двойка, тъй като няма електрически сигнал, който да може да бъде прихванат.
- По-устойчив е на затихване спрямо останалите видове кабели, поради което може да се разполага на големи разстояния – 2000 метра и повече.
- Неподатлив е на външни електрически смущения като електромагнитни и радиочестотни излъчвания.

В сравнение с останалите типове кабели оптичният е доста по-скъп. Освен самата му себестойност, най-големите разходи по използването му са свързани с човешкия труд; с оптичен кабел се работи много по-трудно, а за снаждането на мъничките нишки от стъкло или пластмаса се изискват специално обучени техници.

Режими на работа на оптичните кабели

Влакнесто-оптичният кабел работи в един от следните два режима:

- **Единичен режим (Single mode)** – Единичният режим се нарича също *аксиален*, защото светлината пътува по оста на кабела.
- **Множествен режим (Multimode)** – При множествения режим светлинните вълни навлизат в стъкления канал под различни ъгли и пътуват *неаксиално*, което ще рече, че те непрекъснато се отразяват и отскачат от стените на стъклената тръба.

Еднорежимният оптичен кабел е по-бърз от многорежимния (до 10 Gbps) поради *дисперсията* (разпръскването или разделянето на светлинните вълни) в множествения режим, дължаща се на това, че в края на кабела светлинните импулси пристигат в различно време. Единичният режим се използва най-вече във WAN мрежите (например връзките между централите на телефонните компании). Множественият режим се използва в LAN мрежите.

Светлинни източници за влакнесто-оптични кабели

Влакнесто-оптичният кабел може да се категоризира по типа на използвания светлинен източник:

- **Светодиод (light emitting diode – LED)** – Светодиодът се използва най-често при еднорежимното оптично влакно. Той е относително слаб.
- **Инжекционен лазерен диод (injection laser diode – ILD)** – Инжекционният лазерен диод излъчва силен, интензивен и точно фокусиран светлинен лъч. Използва се най-вече при многорежимното оптично влакно, което спомага за неутрализирането на по-ниската производителност на множествения режим.

Светодиодите се използват широко в електронните часовници, дистанционните управления и електронните инструменти. Светодиодът е полупроводников прибор. Когато през него премине електрически ток, той излъчва светлина. Тази светлина обикновено е червена, но може да се изменя в спектъра до синьо-виолетов цвят в зависимост от дължината на вълната. Светодиоди, излъчващи инфрачервена светлина, се наричат *инфрачервени светодиоди* (infrared emitting diodes – IREDs).

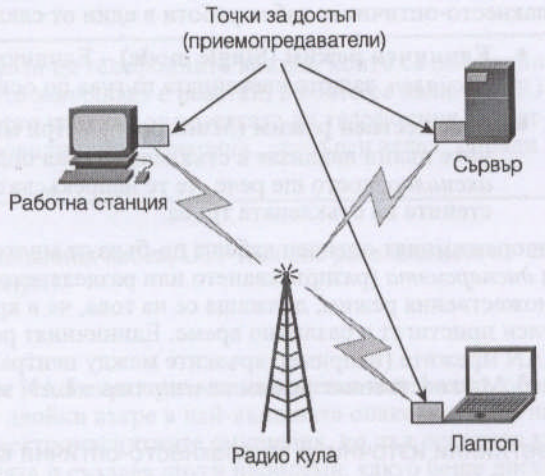
Инжекционните лазерни диоди понякога се използват в ръчните лазерни скенери.

Безжична преносна среда

Безжичните технологии стават все по-популярна алтернатива на мрежите. Въпреки че методите за безжично предаване често пъти са много по-бавни от кабелните връзки, те имат значителни преимущества при конкретни ситуации, както е дискутирано в Глава 6. Същите основни концепции, които засягат безжичните WAN мрежи, се отнасят и за безжичните LAN мрежи.

Обикновено една „безжична" мрежа не се изгражда съвсем без нито един кабел, но включва безжични устройства, които комуникират с традиционна кабелна мрежа. Приемопредавателите, наричани *точки за достъп (access points)*, се използват за предаване и приемане на данни между безжичното устройство или устройства и кабелната мрежа, както е показано на Фигура 7-6.

Фигура 7-6 *Безжичните мрежи използват приемопредаватели, за да приемат и предават данни без помощта на кабели.*



ЗАБЕЛЕЖКА Cisco Systems, съвместно с други компании като Motorola, EDS, Samsung и Texas Instruments, играе водеща роля в разработването на високоскоростни, надеждни и широко достъпни безжични технологии.

Безжичната LAN комуникация е категория, включваща най-различни методи за предаване:

- Чрез лазер
- С инфрачервени лъчи
- С помощта на радио честоти

Ще разгледаме някои от характеристиките на всички тях в следващите секции.

Лазер

Лазер (laser) е съкращение от „light amplification by stimulated emission of radiation" (усилване на светлината чрез стимулирана емисия на лъчение, или още оптичен квантов генератор). Лазерът излъчва поле от кохерентна електромагнитна енергия, в което всички вълни са с еднаква честота и са подредени във фаза. *Фазата* е част от пълен цикъл, която е изминала и се измерва от конкретна отправна точка. Различните типове лазери произвеждат лъчи с различна дължина на вълната.

ЗАБЕЛЕЖКА Повечето хора си мислят за лазерната светлина като за „червена точка", но аргоновите лазери (наречени така заради използването на аргонов газ като среда за лазера) произвеждат синя или зелена светлина. Криптоновите лазери (използващи едноименен газ) произвеждат червена светлина, а лазерите със „смесен газ" комбинират двата газа, произвеждайки едновременно червена, зелена и синя светлина. Резултатът от това е бял лъч.

Лазерите се използват за много цели – като се започне от евтини посочващи устройства и се стигне до високо прецизни мерници за оръжия, принтери, електронни игри, дистанционни управления, хирургически манипулации и мрежови комуникации.

Лазерните мрежи работят чрез използване на импулси лазерна светлина, с които се представя сигналът. Лазерът е технология, изискваща „*пряка видимост*", т.е. между предаващите и приемащите устройства не трябва да има никакви препятствия. Необходимостта от гарантирана пряка видимост е недостатък на базираните на лазер безжични комуникации.

Инфрачервени лъчи

Инфрачервената (Infrared – IR) технология е позната на много хора, тъй като тя се използва в дистанционните устройства за телевизори, видеокасетофони, аудио уредби и т.н. Тя може да се използва и за изграждане на безжични мрежи, като сигналът се пренася с помощта на лъчи в инфрачервения спектър. За целта се използват много високи честоти, намиращи се в диапазона точно под видимия спектър на светлината.

Стандартите за IR хардуера и софтуера се задават от организацията Infrared Data Association (IrDA). IrDA-съвместимите устройства са проектирани така, че

когато даден потребител прекрати инфрачервената връзка, тя да се възстановява при повторното навлизане на устройство в IR обхвата.

IR мрежите изискват наличие на приемопредавател и в двете комуникиращи устройства, като е възможно да изисква и софтуер за синхронизация. Някои операционни системи, като Windows 98 и 2000, притежават вградена IR поддръжка. Скоростта на предаване варира от 4 Mbps до 16 Mbps.

Инфрачервените вълни, подобно на лазера, са технология с пряка видимост. Само че в някои реализации сигналът може да се отразява или пренасочва. Но дори и в тези случи инфрачервените вълни не могат да преминават през непрозрачни обекти като стени.

Недостатъците при IR технологията за мрежи включват следното:

- **Ограничение на обхвата** – Въпреки че е възможно да се реализират IR връзки на разстояния по-големи от една миля (1609 километра), най-често срещаният обхват е по-малък от 100 фута (30,48 метра).
- **Уязвимост** – околната светлина може да причини смущения.

Широколентовият оптичен телепойнт е IR технология, предназначена да поддържа мултимедийни приложения, които изискват широка честотна лента.

Радиовълни

Знаем, че телефонните линии, които първоначално се използваха за предаване на глас, могат да предават и данни. По същия начин радиовълните – среда, която асоциираме предимно с радиопредавания – могат да се използват за предаване на сигнали, носещи данни.

Предаването на данни по радиовълни може да се реализира с най-различни технологии. В следващите секции разглеждаме две категории:

- Теснолентови радиовълни
- Радиовълни с разширен спектър

Теснолентови радиовълни

Теснолентовото радио е познато на повечето от нас. Предавателят изпраща сигнал на определена честота, а приемникът, настроен на същата честота, приема сигнала. Ето как работят комерсиалните радиостанции, двупосочните радиостанции и традиционните канали за извънредни съобщения.

Когато данните се прехвърлят по теснолентов радио канал, много е лесно неоторизирана личност да прихване сигнала. Една по-сигурна и по-надеждна радио технология, разработена най-напред от военните, се нарича *радиовълни с разширен спектър (spread spectrum)*.

Радиовълни с разширен спектър

Радиовълните с разширен спектър са *широколентова* технология. Въпреки че е по-неефективна спрямо теснолентовата (т.е. използва по-голяма честотна лента), тя е по-сигурна, защото използва множество честоти. Теснолентовите приемници не могат да прихващат предавания с разширен спектър. Съществуват два основни типа радиовълни с разширен спектър:

- **Разширен спектър със скокообразно изменение на честотата (frequency hopping spread spectrum – FHSS)** – При FHSS, предавателят прескача от една честота на друга. Приемникът трябва да знае честотите, реда на смяната, както и времената на смяната. Това затруднява прихващането на сигнала от неоторизирани личности.
- **Разширен спектър с пряка последователност (direct sequence spread spectrum – DSSS)** – Тази техника използва специално кодиране (наречено *раздробяване*), което създава излишен битов шаблон за всеки бит от предаваните данни. Това осигурява отказоустойчивост, защото ако някои битове се повредят при предаването, оригиналните данни пак могат да бъдат възстановени, без да се налага повторно предаване.

Устройства за свързване на мрежата

Терминът *устройство за свързване на мрежата* е общ и включва простите и сложните устройства, използвани за свързване на една част от мрежата с друга. В повечето случаи това означава, че към дадено устройство се свързват две или повече парчета кабел.

В следващите секции на тази глава ще разгледаме три типа устройства за свързване на мрежата:

- Прости конектори
- Сложни конектори
- Устройства за разделяне на сегменти и подмрежи

Прости конектори

Простите устройства за свързване на мрежата са тези, които осигуряват само точка на свързване и не усилват, нито пък модифицират по какъвто и да било начин сигнала. В тази група влизат:

- BNC конектори
- RJ конектори
- Конектори за оптични влакна
- Свързващи панели
- Пасивни хъбове

Следващите секции описват тези конектори по-подробно.

BNC конектори

10Base2 мрежите (т.е. тези с тънък коаксиален кабел) използват BNC конектори за да направят връзка между мрежовата карта и кабела. BNC конекторът представлява малко цилиндрично устройство с игла по средата, която се свързва с проводника в кабела. Той се захваща чрез завъртане на външен пръстен.

BNC устройствата включват:

- **BNC Т-конектор** – При този конектор стеблото на Т се свързва към мрежовата карта, а всеки от останалите два края се свързва към кабела.

Ако към Т-конектора се свързва само един кабел, от другата му страна се поставя терминатор.

- **BNC цилиндричен конектор** – Този конектор представлява прав цилиндър, към който се свързва краят на кабела, така че можете да съедините две парчета кабел, за да увеличите общата дължина.

ВНИМАНИЕ Използването на цилиндрични конектори трябва да е минимално, защото във всяка точка на свързване може да възниква загуба на сигнала.

BNC *терминаторът* представлява 50-омово устройство за терминиране, което се инсталира във всеки от краищата на коаксиалната шина. Терминаторът предотвратява отразяването на сигнала при достигането му до края на кабела, което иначе предизвиква смущение. И двата края на кабела трябва да са терминирани, а единият от тях е необходимо да е *заземен* с помощта на проводник към нулев електрически потенциал. Терминът „земя" се използва затова, защото в много случаи проводникът е физически свързан към земята.

RJ конектори

RJ (registered jack – регистриран жак) конекторите се наричат така, защото са регистрирани от Федералната комисия по комуникациите (Federal Communications Commission – FCC) на САЩ. RJ конекторите се състоят от мъжки и женски жак.

Обикновените аналогови телефонни линии в САЩ по принцип използват RJ-11 конектори. Това са модулни букси, свързани към познатия плосък телефонен кабел, който свързва розетката на стената с телефонния апарат. Вътре в стената розетката се свързва към UTP кабел (обикновено Cat 3 или 5 в модерните сгради). Модемите разполагат с RJ-11 конектори.

RJ-45 конекторите се използват при UTP кабела, предназначен за Ethernet мрежи. Мъжкият и женският RJ-45 конектор изглеждат като RJ-11, но са малко по-големи. Двойките кабели се закрепват към RJ буксата с помощта на специален инструмент, наречен кримпер.

Съществуват огромен брой RJ обозначения, но RJ-11 и RJ-45 са тези, които се срещат най-често при компютърните мрежи.

Конектори за оптични влакна

Конекторите за оптични кабели са най-трудни за инсталиране, защото всяка отделна нишка стъкло или пластмаса трябва да се подравни прецизно. След като се подравнят, кабелът се свързва към конектора с нагорещено лепило, епоксидна смола или анаеробно лепило.

Често използваните конектори за оптични влакна включват:

- **SC** – Действа чрез натискане и дърпане
- **ST** – байонетен тип
- **FC** – Със заключване на нишките
- **SMA** – Нишков тип
- **FSD** – Устройство с фиксирана опаковка, използвано при FDDI

Свързващи панели и пасивни хъбове

Свързващият панел представлява свързваща и разпределяща точка, използвана за организиране на кабелите, които идват заедно на едно централно място. Това е подобно на ранните телефонни комутатори, при които връзката се осъществяваше чрез жакове, пъхани в определени отвори.

При мрежите със звездна топология кабелите от компютрите, намиращи се на различни местоположения в сградата, се събират на едно централно място – комутационен шкаф, където са разположени свързващите панели. Кабелите се свързват към монтажен блок в задната част на панела. Отпред се намират RJ-45 жаковете, от които свързващите кабели достигат до хъба.

Свързващият панел играе същата роля като пасивен хъб. Пасивният хъб е централно свързващо устройство, в което се срещат кабелите от компютрите и останалите мрежови устройства. В него няма никакви електронни части и не изисква захранване. Сигналът в него не се регенерира, а по-скоро се изпраща по всички портове.

Сложни конектори

Простите устройства за свързване на мрежата просто съединяват кабелите; сложните вършат много повече неща. Например те могат да усилват сигнала, преди да го предадат нататък, и дори да го конвертират от един тип преносна среда за друг.

В следващите секции дискутираме следните типове сложни конектори:

- Конвертори на преносната среда
- Повторители
- Активни/интелигентни хъбове

Конвертори на преносната среда

Конверторите на преносната среда се наричат също *адаптери за преносна среда (media adapters)* или *транслатори на преносна среда (media translators)*. Те се използват, за да конвертират един сегментен тип в друг; например те могат да конвертират 10Base2 в 10BaseT, 100BaseT Ethernet в оптично влакно или Token Ring в оптично влакно.

Повторители

Повторителят свързва два мрежови сегмента или служи за наставяне на кабел. Само че за разлика от цилиндричния конектор, повторителят не прехвърля просто сигнала от единия кабел към другия – той го *регенерира*. Поради тази причина, ако сигналът е отслабнал поради ефекта на затихването, той се усилва, а ефективната дистанция на кабела се увеличава.

ЗАБЕЛЕЖКА Повторителите могат да се използват за свързване на различни типове преносна среда, като например 10Base2 сегмент в 10Base5 сегмент. И двете архитектури са Ethernet и използват един и същ метод за достъп до преносната среда. Повторителите не могат да се използват за свързване на сегменти, използващи различни архитектури или методи за достъп. Например не можете да свържете Ethernet сегмент (който използва CSMA/CD) и Token Ring сегмент (който използва предаване на маркер).

Повторителите не филтрират преминаващите през тях данни. Те регенерират *всички* сигнали, включително бродкастните съобщения, шума и смущенията, предавайки ги нататък. Повторителите работят във физическия слой на референтния OSI модел.

Активни и интелигентни хъбове

Активните хъбове се наричат също *многопортови повторители (multiport repeaters)*, защото разполагат с множество портове (подобно на пасивните хъбове) и регенерират сигнала, идващ от даден порт, преди да го предадат по друг порт (подобно на повторител). Активните хъбове изискват електрическо захранване.

Интелигентният хъб е специален тип активен хъб. Той не само регенерира сигнала, но също така разполага с процесор, позволявайки ви да извършвате диагностика и да разберете дали има проблем с даден порт. Хъбовете работят във физическия слой на референтния OSI модел.

Устройства за разделяне на сегменти и подмрежи

Устройствата за разделяне на сегменти и подмрежи са най-сложните от всички устройства за свързване на мрежата. Въпреки че термините понякога са взаимозаменяеми, *сегментирането* на мрежата се отнася до разделянето на сегменти, които пак си остават част от същата мрежа. *Разделянето на подмрежи* отива още по-нататък, разделяйки мрежата на отделни мрежи, наречени *подмрежи* (базирани на информация за мрежовите адреси). Разделянето на подмрежи е дискутирано по-подробно в Глава 8, „Мрежови протоколи и услуги“, и в Глава 9, „Най-широкомащабната мрежа: глобалният Интернет.“

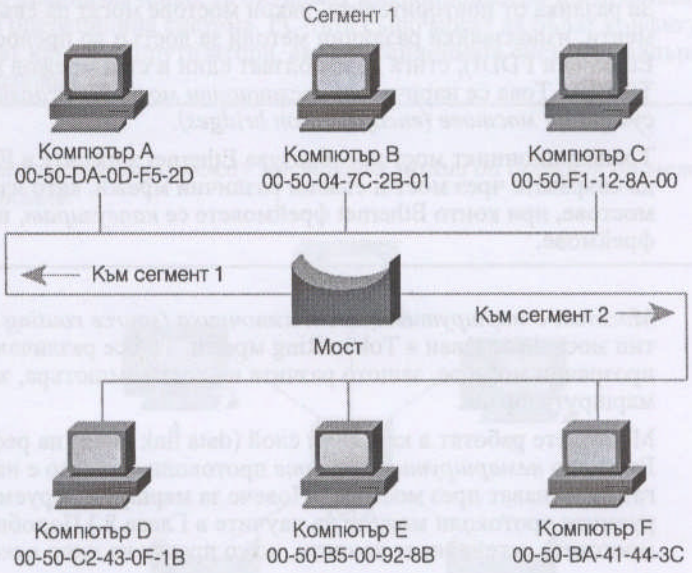
Мостове

Един традиционен мост (наричан също *прост прозрачен мост*) свързва два мрежови сегмента и извършва *филтриране* на трафика, като се базира на MAC (media access control) адресите в пакетите. Когато се използва правилно, това ви позволява да намалите претоварването. Мрежата е разделена на два сегмента с мост между тях, както е показано на Фигура 7-7. MAC адресите са посочени като шестнадесетични числа.

Мостът изгражда таблица от адреси, изпълнявайки следните стъпки:

1. Когато по мрежата се изпрати пакет, мостът проверява адреса източник и адреса местоназначение (т.е. MAC адреса). Таблицата казва на моста в кой сегмент (т.е. от коя страна на моста) е разположен всеки адрес.
2. Ако адресът местоназначение на даден пакет не се намира в таблицата на моста, мостът го препраща и в двата сегмента. В случай че адресът източник не е в таблицата, мостът го добавя в нея.
3. В случай че адресът местоназначение се намира в таблицата, мостът препраща пакета към подходящия сегмент освен ако компютърът подател и компютърът приемник се намират в един и същ сегмент.
4. Ако таблицата показва, че източникът и местоназначението са в един и същ сегмент, мостът не препраща пакета.

Фигура 7-7 *Мостът разделя мрежата на два сегмента.*



ЗАБЕЛЕЖКА Изградената от моста таблица с адреси се нарича *маршрутна таблица (routing table)*, защото се използва за определяне на това, към коя страна трябва да бъдат маршрутизирани пакетите. Не объркайте това с маршрутната таблица, използвана от маршрутизаторите. Маршрутната таблица на моста използва хардуерни адреси, докато тази на маршрутизатора се базира на IP адреси от високо ниво.

В примера, показан на Фигура 7-7, ако Компютър B изпрати съобщение на Компютър F, мостът препраща пакета към Сегмент 2. Той прави това независимо дали адресът на Computer F е в таблицата, тъй като пакетът се препраща към всички сегменти, ако в таблицата липсва запис за адреса на подателя.

Но ако Компютър B изпрати съобщение на Компютър A, мостът проверява своята таблица. Ако адресът на Компютър A не е там, пакетът преминава през моста към другия сегмент. Ако обаче адресът на Компютър A е въведен (защото Компютър A преди това е изпращал съобщение), съобщението *не* преминава през моста. Можете да видите как това намалява ненужния трафик по Сегмент 2.

Мостът се нарича *прозрачен*, защото компютрите в една Ethernet мрежа не знаят за неговото присъствие.

Мостовете препращат бродкастните съобщения – тези, които са адресирани до хардуерния *бродкастен адрес* (FF-FF-FF-FF-FF-FF).

Транслационни и капсулиращи мостове

За разлика от повторителите, някои мостове могат да свързват мрежови сегменти, използвайки различни методи за достъп до преносната среда (например Ethernet и FDDI), стига да използват един и същ мрежов протокол (например TCP/IP). Това се наричат *транслационни мостове (translation bridges)* или *капсулиращи мостове (encapsulation bridges)*.

Транслационният мост преобразува Ethernet адресите в FDDI адреси. Можете да свързвате чрез мост и съвсем различни мрежи, като използвате капсулиращи мостове, при които Ethernet фреймовете се *капсулират*, или обвиват, в FDDI фреймове.

Мостът с маршрутизация от източника (source routing bridge) е специален тип мост, използван в Token Ring мрежи. Той се различава от стандартните прозрачни мостове, защото разчита на хост компютъра, за да вземе решение за маршрутизиране.

Мостовете работят в каналния слой (data link layer) на референтния OSI модел. Ето защо *немаршрутизируемите* протоколи, какъвто е например NetBEUI, могат да минават през мостове. (Повече за маршрутизируемите и немаршрутизируемите протоколи можете да научите в Глава 8.) Подобно на повторителите, мостовете регенерират данните, но го правят на ниво *пакет*.

В една мрежа може да има повече от един мост. Това осигурява отказоустойчивост, но може да доведе до проблема *междумостово зацикляне (bridging loop)*, който възниква при наличие на няколко пътя между две точки и пакетите зациклят в кръг. Това създава ненужен трафик (вижте Фигура 7-8).

Алгоритъмът *STA (Spanning-Tree Algorithm – алгоритъм на свързващото дърво)* беше разработен да разреши проблема с междумостовото зацикляне. STA създава поднабор от междумостови връзки, който елиминира зациклянето. Техническите подробности относно междумостовото зацикляне и STA са извън обсега на тази книга, но в края на главата са изброени отлични източници на информация.

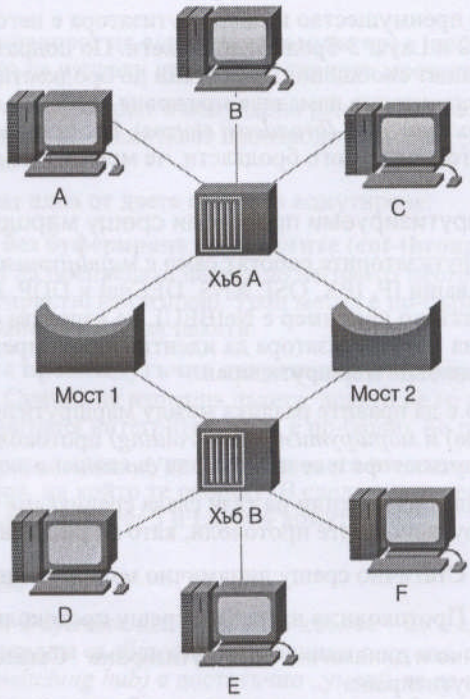
Маршрутизатори

Вървейки по пътя на референтния OSI модел, се натъкваме на устройството за свързване на мрежата, което работи в мрежовия слой: *маршрутизаторът*. Маршрутизаторите свързват отделни мрежи една с друга. Това може да се случи в една локална мрежа (в който случай отделните мрежи се наричат *подмрежи*) или между независими една от друга мрежи в WAN, както е например при глобалния Интернет.

Подобно на моста, маршрутизаторът филтрира трафик. За разлика от моста обаче, маршрутизаторът прави това, използвайки логически мрежови адреси (IP или IPX адреси) вместо физическите хардуерни адреси. Маршрутизаторите са по-интелигентни от мостовете; те вземат сложни решения, избирайки най-добрия маршрут до дадена дестинация измежду множество възможни пътища.

ЗАБЕЛЕЖКА Специализираните маршрутизиращи устройства всъщност са компютри със специално предназначение; те съдържат микропроцесори и изпълняват своя собствена операционна система. PC-тата също могат да бъдат конфигурирани да действат като маршрутизатори, ако операционната система поддържа IP или IPX препращане.

Фигура 7-8 *Множеството пътища между мостовете могат да доведат до междумостово зацикляне.*



Маршрутизаторите поддържат маршрутни таблици, съдържащи мрежовите адреси на други маршрутизатори. Един маршрутизатор трябва да притежава поне два мрежови интерфейса, защото той служи като *шлюз (gateway)* между мрежи. Адресът на интерфейса на маршрутизатора, който обслужва конкретна подмрежа, се нарича *подразбиращ се шлюз (default gateway)* за тази подмрежа. (Забележете, че терминът „шлюз" се използва и за описание на софтуер и устройства, работещи в по-високите слоеве на OSI, където се извършва транслиране между протоколи.)

Функционалност на маршрутизаторите

Маршрутизаторите могат да се използват за свързване на множество мрежи в една по-голяма, както и да разделят една голяма мрежа на няколко по-малки. В Глава 9 дискутираме защо мрежите трябва да се разделят на подмрежи.

Когато пакет с данни пътува от един маршрутизатор до друг, хедърите на каналния слой (т.е. парчетата адресна информация) се премахват и създават на-

ново. Това позволява на маршрутизаторите да обменят пакети между нееднакви мрежи, като например Ethernet и Token Ring. Този процес обаче изисква допълнително натоварване, което прави мрежовата производителност по-ниска, отколкото ако се използват устройства от по-ниско ниво.

Когато в дадена мрежа съществуват множество пътища, мостът избира един от тях и винаги използва него, за да достигне до специфична дестинация. Маршрутизаторите взимат под внимание всички налични пътища за всеки изпратен пакет и взимат решение за всеки отделен пакет. По този начин, ако даден маршрут е много натоварен в дадено време, маршрутизаторът избира друг по-ефективен маршрут.

Друго преимущество на маршрутизатора е неговата способност да филтрира Layer 2 и Layer 3 бродкастни пакети. По подразбиране маршрутизаторите *не* препращат съобщения, изпратени до бродкастния IP адрес (255.255.255.255). Това значително намалява мрежовия трафик и предотвратява разразяването на *бродкастни бури (broadcast storms)*. Бродкастна буря възниква, когато съществуват толкова много бродкасти, че мрежата не може да функционира нормално.

Маршрутизируеми протоколи срещу маршрутизиращи протоколи

Маршрутизаторите работят само с *маршрутизируеми (routable)* протоколи, включващи IP, IPX, OSI, XNS, DECnet и DDP. Един немаршрутизируем протокол, какъвто например е NetBEUI, не използва схема за адресиране, позволяваща на маршрутизатора да идентифицира мрежата; ето защо протоколът не може да бъде маршрутизиран.

Важно е да правите разлика между маршрутизируеми протоколи (дискутирани по-горе) и *маршрутизиращи (routing)* протоколи. Последните се използват от маршрутизатора и се изискват за *динамично маршрутизиране (dynamic routing)*.

В следващите секции на тази глава сравняваме типовете маршрутизиране и маршрутизиращите протоколи, като ги разглеждаме в следните двойки:

- Статично срещу динамично маршрутизиране
- Протоколи за вътрешна срещу протоколи за външна маршрутизация

Статично и динамично маршрутизиране Съществуват два основни начина на маршрутизиране:

- **Статично маршрутизиране** – Това изисква администраторът ръчно да въвежда адреси в маршрутната таблица и да я поддържа актуална.
- **Динамично маршрутизиране** – Използват се протоколи като Routing Information Protocol (RIP), Open Shortest Path First (OSPF) или NetWare Link Services Protocol (NLSP), за да могат маршрутизаторите автоматично и динамично да обменят информацията в маршрутните си таблици един с друг.

Повече за динамичното маршрутизиране и тези протоколи ще научите в Глава 9.

Протоколи за вътрешна и протоколи за външна маршрутизация Маршрутизиращите протоколи се класифицират като вътрешни шлюзови протоколи (interior gateway protocols – IGP) или външни шлюзови протоколи (exterior gateway protocols – EGP). Те са дискутирани по-подробно в Глава 9.

Маршрутизиращите протоколи, работещи в *автономна система (autonomous system)* – т.е. мрежа под управлението на конкретна компания или организация – са от клас IGP.

Мост-маршрутизатори

Един мост-маршрутизатор (brouter) може да действа или като мост, или като маршрутизатор, в зависимост от използвания мрежов транспортен протокол. Мост-маршрутизаторът действа като мост за съобщения, изпратени с NetBEUI или други немаршрутизируеми протоколи, но осигурява функционалността на маршрутизатор за маршрутизируемите протоколи като TCP/IP. Съвременните маршрутизатори са способни да работят както като мостове, така и като маршрутизатори.

Суичове

Основната функционалност на един суич (комутатор) е измамливо проста: да избере път, по който да изпрати данните до тяхното местоназначение.

Ethernet суичовете се превръщат в популярно решение за свързване, при това поради добра причина. Те увеличават производителността (скоростта) и са сравнително евтини.

Суичовете използват една от двете схеми за комутиране:

- **Комутация без буфериране на пакетите (cut-through switching)** – Суичът започва да препредава пакета до неговото местоназначение, преди пакетът да е пристигнал изцяло. Този метод е по-бърз, но може да доведе до преминаването на лоши пакети.
- **Комутация с промеждутъчно съхранение (store-and-forward switching)** – Суичът не изпраща пакета, докато не го получи напълно и не провери неговия интегритет. Това е по-бавно, но по-надеждно.

Съществуват различни типове суичове. Суичовете понякога се категоризират на базата на OSI слоя, на който те работят. В следващите секции дискутираме разликите между Layer 2, Layer 3 и Layer 4 комутирането.

Layer 2 комутиране

Стандартните Layer 2 суичове действат като хъбове – но с една важна разлика. Докато един хъб изпраща съобщенията до всички портове, суичът (наричан *комутиращ хъб – switching hub)* е достатъчно „умен", за да определи кой порт е свързан към компютъра, за който е предназначено съобщението, при което го изпраща само на този порт. Това има няколко положителни ефекта:

- Общото количество ненужен мрежов трафик се намалява, което пък намалява претоварването.
- Създават се отделни области на колизии, което предотвратява колизиите на данни, забавящи производителността и изискващи повторно изпращане на съобщенията.
- Сигурността е увеличена, защото съобщенията не се разпространяват по всички портове. Тези, които се предават по всички портове, са по-лесни за прихващане.

Тези комутиращи хъбове се наричат също *портови суичове (port switches)*, защото към всеки порт се свързва мрежово устройство или компютър. Всяко устройство си има свой собствен посветен път до суича.

Друг тип суич е *сегментният суич (segment switch),* който ви позволява към всеки от портовете да свържете цял мрежов сегмент.

Суичовете могат да се използват за създаване на *виртуални LAN мрежи (VLAN)*, които разделят физическата мрежа, свързана към един суич, в множество логически мрежи. Това може да повиши както производителността, така и сигурността.

Layer 3 комутиране

Layer 3 суичовете, както се подразбира от името, работят в мрежовия слой на референтния OSI модел. Това устройство първоначално беше разработено от 3Com през 1992 година, когато компанията започна да интегрира своите суичове и маршрутизатори, за да намали броя на устройствата, които трябваше да се управляват.

Най-важното нещо, което трябва да знаете за Layer 3 суичовете, е, че те са маршрутизатори, но от специален тип. Един Layer 3 суич (или *комутиращ маршрутизатор (switched router)*, както понякога се нарича) изпълнява същите функции като специализиран маршрутизатор и използва маршрутизиращи протоколи като RIP и OSPF.

Разликата е, че Layer 3 суичовете изпълняват функциите, изпълнявани и от един Layer 2 суич. Суичът използва хардуерно базирана архитектура, за да прилага политики, основаващи се на информацията от мрежовия слой в хедъра на пакета.

Layer 3 суичовете по принцип са по-лесни за установяване и конфигуриране от маршрутизаторите, и могат да се използват в повечето ситуации (в рамките на локална мрежа), където може да се използва маршрутизатор. Изненадващо е обаче, че въпреки добавената функционалност и леснота на използване, Layer 3 суичовете по принцип са по-евтини в сравнение с маршрутизаторите.

Layer 4 комутиране

Неотдавнашните подобрения на Layer 3 суичовете им позволяват да използват информация, например номера на портове, от TCP и UDP хедъри. Тези подобрения се наричат от някои *Layer 4 комутиране*, защото TCP и UDP работят в транспортния слой (Layer 4) на референтния OSI модел. Въпреки името си, тези суичове често са способни да използват информация и от по-горните слоеве.

Едно важно приложение на Layer 4 комутирането е осигуряване на ACL (access control list – списък за контрол на достъпа) филтриране за целите на сигурността. Въпреки че традиционните маршрутизатори могат да „виждат" Layer 4 информация – а някои (като Cisco 7500) дори могат да изпълняват Layer 4 функции – разрешаването на ACL филтрите води до значителен спад в производителността. Тъй като обработката на пакетите се извършва в хардуера с Layer 4 суичове, няма загуба в производителността.

Layer 4 суичовете са способни да управляват разпределението на честотната лента за реализиране на качество на услугата (quality of service – QoS) и балансиране на натоварването.

Много от съвременните суичове притежават функции за Layer 4 комутиране.

Обобщение

В тази глава дискутирахме широк набор от мрежови хардуерни устройства. Научихте как да избирате, инсталирате, конфигурирате и отстранявате проблеми при различни типове мрежови карти.

Също така обсъдихме множеството възможности за избор на мрежова транспортна среда – както кабелна, така и безжична. По специално разгледахме характеристиките на трите основни типа кабели: коаксиален кабел (тънък и дебел), кабел усукана двойка (екраниран и неекраниран) и влакнесто-оптичен кабел. Научихте за някои от преимуществата и недостатъците на всеки от тях, а също и как могат да се използват в различни LAN конфигурации.

След това изследвахме популярните устройство, които могат да се използват за свързване на сегменти или подмрежи. Най-напред разгледахме простите устройства без електроника, като кабелните конектори, свързващите панели и пасивните хъбове. След това погледнахме по-отблизо по-сложните устройства, като повторители, активни хъбове и интелигентни хъбове. Накрая научихме за решенията със сегментиране и разделяне на подмрежи, реализирани чрез мостове, маршрутизатори и суичове.

Сега, след като добре познавате хардуерните компоненти, участващи в изграждането на една типична мрежа, в следващата глава ще надникнем по-надълбоко в мрежовите протоколи и услуги, карящи мрежата да работи.

Допълнителни източници

Отлично ръководство по безжични мрежи се намира в Мрежата на адрес www.proxim.com/ wireless/whiteppr/whatwlan.shtml.

За по-подробна информация относно мостовете, междумостовите зацикляния и алгоритъма STA вижте www.officewizard.com/books/network/ch07.htm.

Отлично обяснение на Layer 3 комутирането може да се открие на www.3com.com/technology/tech_net/white_papers/500660.html.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Кой е най-основният хардуерен компонент, изискван за включване на един компютър в мрежа?

- **a** Маршрутизатор
- **b** Кабел
- **c** Мрежова карта
- **d** Хъб

2 Кой тип мрежа използва външен приемопредавател (трансивър)?

- **a** 10Base2
- **b** 10Base5
- **c** 10BaseT

d Всички от гореизброените

3 Ако искате да инсталирате мрежова карта в компютър с PS/2 мишка, клавиатура, принтер и два IDE контролера, всички използващи подразбиращи се IRQ линии, както и със звукова карта, установена на IRQ 10, коя от следните IRQ линии трябва да остане свободна за мрежовата карта?

a 5

b 7

c 12

d 14

4 Какъв тип кабел се изисква от повечето противопожарни наредби, когато инсталирате кабел в пространството между висящия таван и етажната плоча отгоре?

a Cat 5

b Дебел коаксиален кабел

c От военен клас

d Огнеупорен (Plenum grade)

5 Кой тип кабел е указан за използване при типична 10Base2 мрежа?

a RG-58 /U

b RG-58 A/U

c RG-58 C/U

d RG-59

6 Какъв тип кабел е асоцииран с използването на вампирския зъб?

a UTP

b STP

c Дебел коаксиален кабел

d Тънък коаксиален кабел

7 Как се нарича преминаването на сигнали от един проводник в друг, което може да бъде намалено при усукване на проводниците един около друг?

a Радиочестотни смущения (RFI)

b Затихване (Attenuation)

c Изкривяване (Distortion)

d Смесване (Crosstalk)

8 Какъв тип конектор се използва по принцип за UTP Cat 5 кабели в Ethernet мрежи?

a RJ-45

b RJ-11

c BNC конектор

d F конектор

9 Кое от следните твърдения е вярно за влакнесто-оптичния кабел? (Изберете всички верни отговори.)

a От всички типове кабели с влакнесто-оптичния е най-лесно да се работи и да се инсталира.

b Влакнесто-оптичният кабел осигурява по-добра сигурност от медния.

c Влакнесто-оптичният кабел е по-податлив на затихване от медния.

d Еднорежимният влакнесто-оптичен кабел е по-бърз от многорежимния.

10 Кое от следните устройства се използва за свързване на два сегмента от мрежов кабел, като сигналът се регенерира при преминаването си през него, елиминирайки по този начин ефекта от затихването?

a Цилиндричен конектор

b Свързващ панел

c Повторител

d Пасивен хъб

Глава 8

Мрежови протоколи и услуги

Ако приемем мрежата за тяло, тогава мрежовият хардуер представлява скелетът и органите, а аналоговите сигнали са циркулиращата кръв. Продължавайки аналогията, можем да кажем, че протоколите и услугите, с които една мрежа работи, са разумът на тялото. Протоколите казват на мрежата как да изпълнява своите функции. Те я контролират по същия начин, както умът управлява тялото.

Мрежовите протоколи са набор от правила — логиката, по която мрежата работи. Мрежовите услуги, като например тези за преобразуване на имена или назначаване на адреси, изпълняват специфични функции и управляват конкретни задачи. Това до известна степен наподобява начина, по който различните центрове на мозъка управляват слуха, зрението, дишането, речта и т.н.

Съществуват много видове компютърни протоколи. Всеки работи в различен слой на OSI модела. Когато става дума за компютърни мрежи, терминът „протокол" често се използва за означаване на *мрежовите/транспортните* протоколи — тези, които работят в слоевете 3 и 4 на OSI модела. За да могат свързаните в мрежа компютри да комуникират помежду си, те трябва да използват един и същ протокол.

В тази глава обсъждаме три мрежови/транспортни протокола:

- NetBEUI (NetBIOS Extended User Interface)
- IPX/SPX (Internet Packet Exchange/Sequenced Packet Exchange)
- TCP/IP (Transmission Control Protocol/Internet Protocol)

Това са трите стандартни стека, поддържани от множество популярни операционни системи за PC-та. Всеки от тях си има предимства и недостатъци, като това зависи от самата локална мрежа.

В тази глава разглеждаме също и някои мрежови услуги, като DNS (Domain Name System — система за имена на домейни), WINS (Windows Internet Name Service — система за Интернет имена в Windows) и DHCP (Dynamic Host Configuration Protocol — протокол за динамично конфигуриране на хостове), които работят с TCP/IP, за да разширят неговата функционалност.

NetBIOS/NetBEUI

Може да откриете използвания на NetBIOS и NetBEUI, при които се подразбира, че те са едно и също нещо. Всъщност по едно време това беше истина. NetBIOS (Network Basic Input/Output System — мрежова базова система за вход/

изход) беше разработен от IBM и приет от Microsoft за ранните LAN комуникации. По това време терминът се отнасяше както до приложния програмен интерфейс (application programming interface – API) така и за стека от мрежови/транспортни протоколи.

ЗАБЕЛЕЖКА *Протоколният стек (protocol stack)* е група от два или повече протокола, работещи заедно, като всеки от тях оперира в различен слой на референтния OSI модел.

В последствие тези компоненти бяха разделени на NetBIOS (отнася се за API интерфейса) и NetBEUI (което се отнася за протоколите от мрежовия/транспортния слой). NetBIOS не осигурява рамка за формáта на данните при предаването им по мрежата; NetBEUI го прави.

NetBIOS: API интерфейсът

NetBIOS може да работи по NetBEUI, IPX/SPX или TCP/IP. NetBIOS позволява на приложенията да си имат работа с общ програмен интерфейс, така че информацията да може да се споделя по различни протоколи от по-ниско ниво.

Работейки в по-горните слоеве (това са приложният слой на модела на Министерството на отбраната (Department of Defense – DoD) и сесийният слой на референтния OSI модел), NetBIOS осигурява два режима на комуникация: сесиен режим и датаграмен режим.

Когато работи в сесиен режим, NetBIOS позволява на комуникиращите компютри да установят връзка, или *сесия,* с откриване на грешки и възстановяване. Когато NetBIOS се използва в датаграмен режим, самостоятелните съобщения се изпращат отделно без установяване на връзка, което ще рече, че откриването на грешки и тяхното коригиране трябва да се поеме от самото приложение.

NetBIOS също така осигурява услуга за имена (т.е. NetBIOS имена) чрез която компютрите и приложенията могат да се идентифицират по мрежата.

NetBEUI е най-простият от трите протоколни стека. Неговата простота го прави най-високопроизводителният по отношение на същинската скорост, но също така ограничава неговата функционалност. Тъй като NetBEUI не включва средства за логическо адресиране на адреси в мрежовия слой, той не може да се маршрутизира от една мрежа или подмрежа към друга. Въпреки това той работи много добре за комуникации в единична LAN мрежа и е лесен за установяване. Може да се използва съвместно с друг маршрутизируем протокол като TCP/IP. Това комбинира предимствата на високата производителност на NetBEUI в локалната мрежа и способност за комуникация извън тази мрежа с помощта на TCP/IP.

IPX/SPX

IPX работи заедно с SPX, за да осигури маршрутизируеми мрежови комуникации. Novell разработи IPX/SPX за своите NetWare сървъри и клиенти, но тези протоколи могат да се използват и с друг операционни системи (като Microsoft Windows). Novell базираха IPX/SPX на протоколите XNS (Xerox Network System).

ЗАБЕЛЕЖКА IPX/SPX или NWLink се изисква за свързване на Microsoft клиенти към NetWare 4.x и по-стари сървъри. Някои NetWare 5.x сървъри могат да комуникират само чрез TCP/IP.

При IPX/SPX конфигурирането е по-лесно и производителността е по-висока в сравнение с TCP/IP. IPX/ SPX понякога се използва за вътрешни LAN комуникации като част от план за сигурност. „Външните" компютри, осъществяващи достъп до LAN мрежата от Интернет, които работят само с TCP/IP, не могат да достигнат LAN системите, работещи само с IPX/SPX.

Microsoft осигурява IPX/SPX-съвместим протоколен стек, наречен NWLink, който е включен във всички съвременни Windows операционни системи, въпреки че по подразбиране не се инсталира.

IPX работи в мрежовия слой на референтния OSI модел и е безвръзково-ориентиран (connectionless). SPX работи в транспортния слой на референтния OSI модел и осигурява потвърждения, сглобяване на пакетите и други връзково-ориентирани услуги.

ЗАБЕЛЕЖКА *Връзково-ориентираната (connection-oriented)* комуникация е подобна на телефонен разговор между двама души. Ако искате да разговаряте с г-н Иванов, набирате неговия номер и след това го търсите по име. Не започвате да предавате вашите съобщения, докато не сте сигурни, че г-н Иванов не е от другата страна на линията (с други думи, докато не установите вашата сесия).

Безвръзково-ориентираната (connectionless) комуникация действа по-скоро като да използвате система за местни радиопредавания, за да предадете своето съобщение до член на голяма тълпа. Говорите в микрофона и вашето съобщение се предава. Надявате се г-н Иванов да е в тълпата и да е чул съобщението ви, но няма начин да знаете дали съобщението наистина е стигнало до своето местоназначение, защото няма установена сесия.

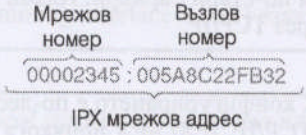
Протоколът от мрежовия слой: IPX

В Глава 3, „Мрежови концепции, модели и стандарти", научихте, че мрежовият слой на референтния OSI модел е отговорен за логическото адресиране и функциите по маршрутизиране, т.е. за доставяне на съобщенията до правилните местоназначения. Това е главната функция на IPX.

За да бъде един протокол маршрутизируем, трябва да има начин за идентификация на мрежата, в която се намира компютърът. IPX използва шестнадесетични *мрежови номера (network numbers)*, за да идентифицира мрежата (подмрежата). Един типичен IPX мрежов номер изглежда по следния начин: 805609a0. Мрежовият номер се назначава от мрежовия администратор.

Един IPX адрес се състои от две части: мрежовият номер и *възловия номер (node number)*, както е показано на Фигура 8-1. Възловият номер (или номерът на възел) идентифицира специфичното устройство и се базира на MAC (Media Access Control – контрол за достъп до преносната среда) адреса на интерфейса.

Фигура 8-1 *Един IPX адрес се състои от две части: мрежов номер и възлов номер.*



В мрежи, работещи както с TCP/IP, така и с IPX/SPX, мрежовите номера често се създават на базата на IP адреса, като IP адресът просто се преобразува от десетичен в шестнадесетичен (например 214.12.1.42 в шестнадесетичното D6C12A).

Ролята на протокола за рекламиране на услуги (SAP)

IPX използва протокола за рекламиране на услуги (Service Advertising Protocol – SAP), за да рекламира адреса на мрежови услуги, като например файлови сървъри. Към всяка услуга се назначава число, наречено SAP ID или SAP идентификатор, като SAP бродкастите се излъчват на всеки 60 секунди. Маршрутизаторите и сървърите пазят таблици със съответствия между SAP идентификаторите и услугите, като ги обновяват динамично при всеки бродкаст. По този начин таблиците се поддържат актуални, но се използва и значителен капацитет от мрежата. SAP бродкастите не се препращат през маршрутизаторите, макар че самите маршрутизатори могат да препращат своите SAP таблици на други маршрутизатори.

Протоколът от транспортния слой: SPX

SPX работи над IPX – в транспортния слой. Докато IPX е безвръзково-ориентиран протокол, SPX е връзково-ориентиран. Това прави SPX по-надежден, което има смисъл, когато се замислите за факта, че транспортният слой е отговорен за потвържденията, проверката за грешки и други подобни дейности.

IPX доставя пакета до неговото местоназначение. SPX се занимава с това да гарантира, че пакетът пристига изцяло и в добро състояние. SPX управлява установяването на последователността и следи броя на предадените пакети. Той гарантира доставката, като проверява дали данните са получени.

TCP/IP

TCP/IP стекът е крайъгълният камък на Интернет комуникациите. Той бързо се превръща в най-използваното мрежово/транспортно решение за мрежи с всякакъв размер и конфигурации. Ето защо се фокусираме именно на него в тази дискусия на мрежови/транспортни протоколи.

Следващите секции на тази глава са съсредоточени върху концепциите и теорията, стоящи зад различните членове на комплекта TCP/IP, какво прави всеки от тях, както и начинът им на работа. В Глава 12, „Настолни операционни системи“, ще научите как да конфигурирате TCP/IP за различни настолни операционни системи.

Комплектът TCP/IP

TCP/IP е не само протоколен стек, състоящ се от протокол от мрежовия слой и протокол от транспортния слой, но и пълен комплект от протоколи, работещи в много слоеве на мрежовия модел. По дефиниция комплект от протоколи (protocol suite) включва „екстри", които не се изискват за мрежовата комуникация. Тези екстри включват например помощни програми от приложния слой, които са част от комплекта TCP/IP.

Много от протоколите, включени в комплекта, функционират като инструменти за събиране на информация и отстраняване на проблеми. В следващите секции на тази глава разглеждаме всеки от тях, започвайки с основните играчи: протоколите от мрежовия и от транспортния слой.

Протоколът от мрежовия слой: IP

Знаете, че мрежовият слой се занимава със задачите по маршрутизирането. TCP/IP протоколите позволяват това маршрутизиране, като използват IP адреси, за да идентифицират мрежовите устройства. Всеки компютър, свързан към мрежата принтер, маршрутизатор и други мрежови устройства, притежават уникален IP адрес.

ЗАБЕЛЕЖКА В действителност едно устройство може да има няколко IP адреса – по един за всеки от неговите *мрежови интерфейси*. Маршрутизаторите имат минимум два интерфейса, които се свързват към различни подмрежи. Всеки от тези интерфейси притежава уникален IP адрес. *Груповите (multihomed)* компютри разполагат с повече от една мрежова интерфейсна карта (network interface card – NIC), като на всяка карта е назначен IP адрес.

Какво представлява IP адресирането

Всеки IP адрес се състои от две части. Заедно те идентифицират мрежата, в която се намира устройството, и конкретното устройство в тази мрежа. Една част от IP адреса представлява *мрежата*, а втората част представлява *хоста* (отделният компютър). Това наподобява начина, по който един пощенски адрес от две части идентифицира конкретна къща, до която се доставя пощата:

- Името на улицата казва на пощенската служба по-общата част, в която се намира къщата. Много отделни къщи споделят „Елм" за име на улица като част от техния адрес.
- Всеки номер на дадена улица е уникален за всяка отделна къща. Може да има много къщи в града с номер „101", но има само една къща на улица „Елм" (Elm Street) с този номер.

По подобен начин много компютри споделят един и същ мрежов адрес, но комбинацията от мрежов адрес и адрес на хоста е уникална за всеки компютър (или по-точно, за всеки мрежов интерфейс). Например в IP адреса 201.32.0.4 първите три секции (наречени *октети* и дискутирани в секцията „Класове IP адреси" по-нататък в тази глава) идентифицират мрежата. Последната секция идентифицира мрежовия интерфейс на индивидуалния компютър. Всички компютри в същата подмрежа имат един и същ мрежов идентификатор (201.32.0), но всеки има различен идентификатор на хост (т.е. в подмрежата може да има само един адрес .4).

Ако изпратите по обикновена поща писмо от Далас до Сан Франциско, пощенската станция в Далас въобще не се интересува от уличния номер в Сан Франциско. Първата задача е писмото да се изпрати до правилния град. По същия начин, когато изпратите съобщение по Интернет до различна LAN, маршрутизаторите не се интересуват от хост порцията на IP адреса; те се интересуват само от частта с мрежовия адрес. След като пакетът достигне вярната мрежа (подмрежа), хост адресът се използва за препращане до специфичен компютър – точно както местният пощенски клон в Сан Франциско използва уличния адрес, за да гарантира, че вашето писмо достига до своето местоназначение.

По подобен начин, ако даден компютър изпрати съобщение на IP адрес 201.32.0.4, в който 204.32.0 представлява мрежата, а 4 представлява хоста, първата стъпка е пакетът да се достави до правилната мрежа. След неговото пристигане той се маршрутизира вътрешно в самата мрежа до компютъра, представен от идентификатора на хоста (който е 4).

В нашия пример първите три октета идентифицират мрежата. Случаят обаче не винаги е такъв. В традиционната схема за IP адресиране, частта от адреса, която представлява мрежата, и частта, която представлява хоста, се определя от *класа (class)* на адреса, както е дискутирано в следващата секция.

Класове IP адреси

IP адресите, подобно на останалата информация, обработвана от компютрите, са изградени от двоични цифри, или *битове*. Тъй като работата с дълги низове от единици и нули е трудна за повечето хора, ние обикновено обозначаваме IP адресите в *точково-десетичен (dotted-decimal)* формат. (Вижте Глава 3, ако искате да си припомните бройните системи и начина на преобразуване на двоични числа в десетични.) Точково-десетичният формат понякога се нарича *точкова четворка (dotted quad)*, защото има четири набора от числа, разделени с точки, като всеки набор представлява октет.

Дължината на един *октет* е осем бита; има осем цифри, всяка от които е единица или нула. Четирите октета понякога се обозначават като w.x.y.z. При това обозначение най-десният октет се нарича „z“ октет, следващият е „y“ и т.н.

Тъй като има по осем бита във всеки от четирите октета, всеки IP адрес е 32-битово число. Това означава, че съществуват над четири милиарда възможни IP адреси (за да бъдем точни, 4 294 967 296, което е 2^{32}). Един IP адрес обикновено изглежда по следния начин: 192.168.1.12.

ЗАБЕЛЕЖКА Тази дискусия се базира на версия 4 на Интернет протокола (IPv4), която масово се използва днес. В момента се тества нов стандарт, IPv6, или IPng (което е съкращение от IP, Next Generation [Интернет протокол от следващо поколение]), който използва 128-битов адрес и осигурява 2^{128} използваеми адреси.

Знаем, че част от IP адреса идентифицира мрежата, а останалата част идентифицира отделното устройство (хоста), но коя част коя е и кое от двете представлява? За нещастие, отговорът е, че зависи. По традиция това зависеше от класа, към който принадлежеше мрежата (един нов метод за адресиране, наречен *безкласово адресиране (classless addressing)*, ще бъде дискутиран в секцията „Какво представлява безкласовото адресиране“).

Организацията IANA (Internet Assigned Numbers Authority) раздава IP адреси. В ранните дни на Интернет комуникациите изглеждаше логично да се назначават

IP адреси на компании и организации на блокове, защото всеки компютър в локалната мрежа се нуждаеше от уникален адрес, чрез който да комуникира в Интернет.

ЗАБЕЛЕЖКА С изобретяването на технологии като транслирането на мрежови адреси (Network Address Translation – NAT), което беше дискутирано в Глава 6, „WAN връзки", вече не е важи изискването всеки компютър в локалната мрежа да притежава публичен IP адрес.

Блокове от адреси бяха назначавани на база размера на локалната мрежа. Мрежите на големите предприятия се нуждаеха от по-големи блокове от адреси, а малките само с по няколко устройства изискваха по-малки блокове. *Класовете на адресите* се определяха на база размера на мрежата (броят на хост адресите). Таблица 8-1 показва традиционните класове IP адреси.

Таблица 8-1 *Класове IP адреси*

Адресен клас	Брой мрежи	Брой хостове за мрежа
A	126*	16 777 216
B	16,384	65 535
C	2 097 152	254
D (мултикаст)	N/A	N/A

* Диапазонът от адреси 127.*x.x.x* е запазен за адрес за обратна връзка (loopback address), използван за тестови и диагностични цели.

ЗАБЕЛЕЖКА Поради използване на целия 127.x.x.x мрежов адрес за обратна връзка (loopback), над 24 милиона IP адреси бяха загубени. В ранните дни на Интернет това не беше проблем, защото имаше много повече свободни IP адреси, отколкото бяха Интернет компютрите, а комерсиализацията и неимоверното разрастване на Интернет въобще не се очакваха.

Както можете да видите в Таблица 8-1, в наличност има само 126 адреси от Клас A. Тези адреси бяха изчерпани още преди години; те бяха назначени на много големи корпорации и образователни институции, включващи IBM, Hewlett Packard, Xerox, Масачузетския технологичен институт (Massachusetts Institute of Technology – MIT), Университетът на Колумбия, Digital Equipment Corporation, General Electric и Apple. Всяка мрежа има над 16 милиона хост адреса, които могат да бъдат назначавани на компютрите в тези мрежи.

Схемата за класове от IP адреси създава над 2 милиона Клас C мрежи, но всяка от тези мрежи не може да има повече от 254 хост адреса. Мрежовите адреси от Клас C често пъти се назначават на Интернет доставчици, които разпределят дадения им диапазон на по-малки блокове за компании, разполагащи само с 10 до 20 хост машини в техните мрежи.

Клас B адресите попадат между адресите от Клас A и тези от Клас C. Те се назначават главно на големи компании, които в ранните дни на Интернет са били твърде малки (или не са съществували), за да получат Клас A адрес. Microsoft Corporation е пример за компания с Клас B мрежа.

Клас D адресите не се използват за мрежи, а за *мултикаст съобщения*, представляващи средство за изпращане на едно съобщение до множество получатели едновременно. Клас D адрес се назначава на указана група от компютри, а мултикастните протоколи се занимават с дистрибуцията на пакетите.

Методът на разделяне на IP адреси на класове според размера на мрежата се нарича *класово адресиране (classful addressing)*. (Методът за *безкласово адресиране* е дискутиран в секцията „Какво представлява безкласовото адресиране" в тази глава.)

Мултикаст и мрежата MBONE

Мултикаст съобщенията изпълняват функция в Интернет, подобна на тази на бродкастните съобщения в една локална мрежа. Само че вместо да се изпращат на *всички* компютри в мрежата, мултикаст съобщенията се изпращат само до компютри, принадлежащи към предварително дефинирани мултикаст групи.

Мултикаст съобщенията имат няколко преимущества:

- Те спестяват пропускателна способност, защото изпращате един и същ пакет до множество адреси, вместо да предавате пакета по веднъж за всеки отделен адрес.
- Не е необходимо да знаете адреса на всеки компютър, към който изпращате пакети; трябва да знаете само мултикаст адреса.

Традиционните предавания с единично местоназначение се наричат *уникаст съобщения (unicast messages)*. Традиционните Интернет маршрутизатори са конфигурирани за уникаст предавания, поради което много от тях не могат да боравят с мултикаст пакети. За да разреши този проблем, IETF (Internet Engineering Task Force) разработи виртуална мрежа, наречена MBONE (multicast backbone – мултикаст гръбнак), която работи на върха на Интернет. Използвайки същия хардуер като Интернет, MBONE софтуерът предава мултикаст пакети вътре в уникаст пакети. *Капсулацията* (наричана също *тунелиране*) крие мултикаст пакета от маршрутизатори, които не могат да го обработват, и му позволява да пътува през традиционните не-мултикаст маршрутизатори.

Какво представлява класовото адресиране

Запомнете, че въпреки че ние използваме най-вече десетичната нотация, IP адресите всъщност са изградени от двоични числа. Таблица 8-2 показва как адресните класове могат да се идентифицират на базата на диапазона от адреси на първия октет. За да разберете Таблица 8-2, необходимо е отново да се върнем за момент към двоичната бройна система.

Запомнете, че адресният клас се идентифицира от *старшите битове*, т.е. първите няколко бита в най-левия октет (понякога наричан октет „w").

Таблица 8-2 *Идентифициране на адресните класове*

Клас IP адреси	Старши битове	Диапазон от адреси на първия октет	Брой битове в мрежовия адрес
Клас A	0	0–127*	7
Клас B	10	128–191	14
Клас C	110	192–223	21
Клас D	1110	224–239	28

* Диапазонът от адреси 127.x.x.x е резервиран като адрес за обратна връзка, използван с цел тестване и диагностика.

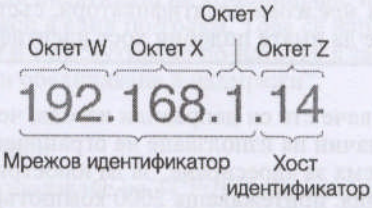
Както можете да видите в Таблица 8-2, Клас A адресите се идентифицират от първия бит (със стойност 0), Клас B адресите се определят от първите два бита –10, първите три бита на Клас C адресите са 110, а мултикаст адресите (Клас D) използват 1110 за първите четири бита.

Разгледайте следния IP адрес: 11001111.00101100.01010001.11100111. Тъй като първите три бита най-вляво (най-старшите) са 110, знаем, че това е Клас C адрес. Ако конвертираме двоичния адрес в точково-десетична нотификация (с помощта на научен калкулатор или метода, описан в Глава 3), получаваме следното: 207.44.81.231.

Забележете, че първият октет, 207, попада в диапазона 192–223, показан в Таблица 8-2. Тъй като първите три бита на всички Клас C адреси са със стойност 110, те всички са с „w" октет, попадащ в този диапазон. Това означава, че можем да определим към кой клас спада даден IP адрес просто като погледнем първия му октет.

В предния пример 207.44.81 идентифицира мрежата (подмрежата) в която се намира компютърът. IP адресите на всички компютри в тази подмрежа започват със същите три октета. Числото 231 определя специфичния хост компютър. Нито едно друго устройство в тази подмрежа не може да има същото число за най-десния октет в своя IP адрес. Фигура 8-2 дава пример за това, как един IP адрес се разделя на мрежов и хост идентификатор.

Фигура 8-2 *В един Клас C адрес първите три октета представляват мрежовия идентификатор.*



Дотук добре, но как определяме броя на мрежите и хостовете, налични за всеки клас? По традиция един Клас A адрес използва първия октет като мрежов адрес, а останалите три като хост адрес. Тъй като най-първият бит (най-старшият бит) в един Клас A адрес се използва за идентификация на адресния клас, в първия октет остават седем бита, които могат да се използват за идентификация на мрежата.

Един Клас B адрес използва първите два октета за мрежата, а останалите два за хоста. В първите два октета има 16 бита, но първите два бита се използват за идентифициране на класа. Ето защо ни остават само 14 бита за мрежовия идентификатор.

Следвайки същата логика, Клас C използва първите три октета (8 бита по три октета, което прави 24 бита), за да идентифицира мрежата, като само последният октет остава за идентификация на хостове. Трите най-старши бита идентифицират класа, така че вадим 3 от 24 и получаваме 21 бита за мрежовия идентификатор.

Нека се върнем към нашата Клас A мрежа. Знаем, че мрежовия идентификатор имаме в наличност 7 бита. Ако всички те са „включени" (имат стойност 1), най-голямото число, което можем да получим за мрежовия идентификатор, е 1111111. След като конвертираме това число в десетично, получаваме 127 – броят на възможните Клас A мрежи (диапазонът 127 е запазен за тестване с обратна връзка). Адресът 0.0.0.0 е запазен за представяне на всички IP адреси.

Един по-лесен метод за достигане до това число е да повдигнете 2 на степен x, където x е броят на битовете, налични за мрежовия идентификатор. Ако използваме този метод, получаваме 2^7, което дава 128. Когато изключим мрежовия адрес 0.0.0.0 и мрежовия адрес за обратна връзка, получаваме 126 – броят на възможните Клас A адреси.

Същият процес може да се използва за Клас B и Клас C мрежи:

- **Клас B** – 14 бита = 2^{14} = 16 384
- **Клас C** – 21 бита = 2^{21} = 2 097 252

ЗАБЕЛЕЖКА Някои книги ви казват да използвате формулата $2^x - 2$. Причината за изваждането на 2 е поради едно старо правило, гласящо, че мрежовият идентификатор не може да е изцяло нули или изцяло единици. Причината за това правило се крие в по-старите маршрутизатори, защото те не можеха да обработват мрежови идентификатори от такъв тип. Само че много от модерните маршрутизатори позволяват мрежови идентификатори, състоящи се изцяло от нули или от единици; ето защо не е нужно да изваждате 2.

Числата в предходния списък с точки представляват максималния теоретичен брой мрежи, налични във всеки адресен клас. Въпреки че съвременният метод позволява *мрежови* идентификатори, състоящи се изцяло от нули или единици, не можете да имате подобни хост идентификатори.

Може би вече сте си направили извода, че класовото адресиране не е най-ефективният начин на използване на ограничения брой IP адреси, налични в 32-битовата схема за адресиране. За да илюстрираме това, нека използваме примера за компания, притежаваща 2000 компютъра, които иска да свърже към Интернет. Един Клас C адрес няма да свърши работа, защото това би ограничило мрежата до 254 хоста. Следващият по-горен клас са Клас B адресите, но ако компанията получи такъв адрес, той би заел диапазон от 65 000 адреса. Тъй като компанията се нуждае само от 2000 от тези адреси, над 63 000 IP адреси ще бъдат загубени. *Безкласовото адресиране,* дискутирано в следващата секция, се справя с този проблем.

Какво представлява безкласовото адресиране

Загубата на адреси, свързана с класовото адресиране, съдейства за бързото изчерпване на свободни IP адреси. Едно от предложените решения е реализацията на IPv6, който използва по-голямо адресно пространство (128 битово). Само че преминаването към нова версия на IP не е просто и ще отнеме известно време, докато това се случи. Междувременно съществува друго решение: безкласово адресиране, базирано на безкласовата междудомейнова маршрутизация (classless interdomain routing – CIDR).

Вместо да използва адресни класове, CIDR използва обозначение, прикрепено към всеки IP адрес, което указва броя битове, използвани за мрежовата част от адреса. CIDR мрежите понякога се наричат „slash x" (слаш екс) мрежи, защото IP адресът се разделя от суфикса посредством наклонена черта (слаш). При това положение един CIDR адрес изглежда по следния начин: 192.168.1.0/24. Числото 24 след наклонената черта означава, че 24-те най-леви бита се използват за идентификация на мрежата, а останалите осем бита се използват за идентификация на хоста. С други думи, първите три октета посочват мрежата, а последният посочва хост компютъра. Ако адресирането беше класово това щеше да е Клас С мрежа.

Таблица 8-3 показва как CIDR адресите съответстват на традиционните класови адреси.

Таблица 8-3 *CIDR (безкласови) адреси и традиционни класови адреси*

CIDR адрес	Класов адрес
/8	Клас А
/16	Клас В
/24	Клас С

CIDR позволява много по-ефективно разпределение на IP адреси. Освен slash-х означенията в Таблица 8-3, CIDR мрежите могат да бъдат означавани като /12, /20, /21, /28 и т.н.; това означава, че след наклонената черта може да следва какъвто и да е брой битове, които искате да използвате за мрежов идентификатор. Това позволява създаване на мрежи с размери, които попадат между традиционните мрежови класове.

CIDR също така поддържа практиката на комбиниране на малки непрекъснати блокове от мрежови адреси в един по-голям. Това се нарича *обединяване в надмрежи (supernetting)* и е дискутирано по-нататък в тази глава, в секцията „Разделяне в подмрежи и обединяване в надмрежи".

Автоматично разпределяне на адреси

За да комуникира чрез използване на TCP/IP, един компютър или мрежово устройство трябва да притежава уникален IP адрес. Това е *логически* адрес и се обработва в мрежовия слой.

Частта от адреса, предназначена за мрежата, трябва да бъде същата като тази на останалите компютри в дадената подмрежа. Например, ако използвате подразбиращата се подмрежова маска за Клас С мрежи, тогава 192.168.1.12 и 192.168.1.34 ще бъдат два компютъра в една и съща подмрежа, защото мрежовият идентификатор, представян от първите три октета, е един и същ.

Точно обратното е при хост частта – тя *не* трябва да бъде същата за нито един друг компютър в дадената подмрежа. Например, не може да има два компютъра с хост адрес .6 в същата подмрежа.

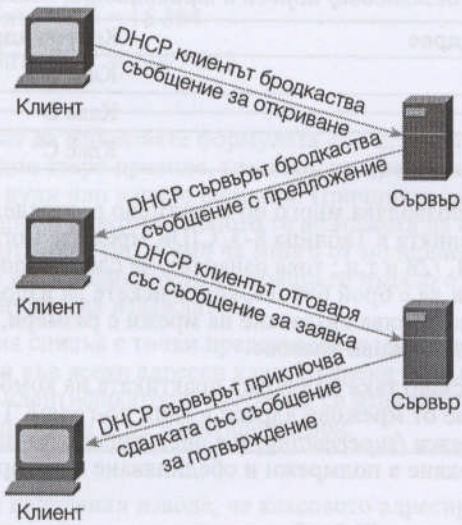
Съществуват два начина за получаване на IP адрес:

- Адресът може да се въведе ръчно в TCP/IP свойствата на операционната система. Това изисква мрежовият администратор да разбира TCP/IP адресирането и да знае как да избере валиден адрес за конкретната мрежа.
- Адресът може да се назначи автоматично. По принцип това означава, че даден компютър в мрежата се конфигурира като DHCP сървър, за да задава IP адреси. В други случаи една възможност на операционната система, наречена Automatic Private IP Addressing (APIPA), позволява на компютъра да си самоназначи адрес, ако не успее да се свърже с DHCP сървър.

DHCP

DHCP е протокол, работещ на машина, конфигурирана като DHCP сървър, която назначава IP адреси на машини, конфигурирани като DHCP клиенти. Фигура 8-3 илюстрира процеса.

Фигура 8-3 *DHCP сървърът отдава под наем адрес на DHCP клиент.*



Стъпките, изпълнявани, когато DHCP клиент получава наем за IP адрес от DHCP сървър, са следните:

1. Компютър, чиито TCP/IP свойства са установени за получаване на IP адрес чрез DHCP, се появява в мрежата. Този компютър бродкаства съобщение, наречено съобщение за откриване на DHCP. (Бродкастните съобщения се изпращат до всеки компютър чрез използване на специален бродкастен адрес.)
2. Ако в мрежата има DHCP сървър, той приема бродкастното съобщение и отговаря със съобщение, наречено DHCP предложение. Съобщението предлага на клиента IP адрес от диапазона от адреси на сървъра, които са

налични за разпределение. Предложеният адрес временно се резервира, докато сървърът не получи отговор от клиента. Съобщението с предложението също се изпраща като бродкаст, защото клиентът все още няма IP адрес, до който съобщението да бъде изпратено директно.

3 Клиентът може да получи множество предложения, ако в мрежата има множество DHCP сървъри. Когато пристигне първото предложение, клиентът отговаря със съобщение, наречено DHCP заявка (DHCP request). Това е приемане на първото получено предложение. То отново е бродкастно съобщение; по този начин всички DHCP сървъри го получават и онези, отправили предложенията си по-късно, ще знаят, че техните предложения не са приети. След това те могат да поставят предложените адреси, които са резервирали за клиента, обратно в своите пулове от свободни адреси.

4 Последната стъпка в тези преговори е DHCP потвърждението (DHCP acknowledgment) (наречено също ACK). DHCP сървърът, чието предложение е прието, получава съобщението за заявка от клиента. Сървърът потвърждава приемането и назначава IP адреса на този клиент за предварително дефиниран „наемен" период. Сървърът може да изпрати на клиента допълнителна информация за конфигуриране на TCP/IP, като например IP адресите на DNS и WINS сървъри. (Ролята на тези сървъри е дискутирана по-нататък в тази глава.)

Когато тези стъпки приключат, клиентът може да използва назначения му IP адрес, за да комуникира с останалите компютри, работещи с протокола TCP/IP. Това става, докато не изтече предоставеният наем. Забележете, че наемният период може да се зададе от администратор на DHCP сървъра.

Преди изтичането на наема клиентът започва да преговаря, за да го поднови, така че да продължи да използва адреса. Обикновено DHCP сървърът отговаря положително на заявката. Ако обаче DHCP сървърът е изключен, или ако изпрати отговор за отрицателно потвърждение (Negative Acknowledgment – NACK), клиентът трябва да започне DHCP процеса от самото начало.

ЗАБЕЛЕЖКА DHCP сървърът може да изпрати NACK, ако например клиентската машина се е преместила в различна подмрежа, при което адресът, който се опитва да поднови, вече не е валиден за новото местоположение.

DHCP има множество предимства пред ръчното задаване на IP адреси:

- Спестява време, защото администраторът не трябва да въвежда адрес в настройките на всеки компютър.
- Гарантира по-голяма точност, защото администраторът не е необходимо да следи кои адреси вече са били назначени и кои все още са свободни.

Ако компютри в една мрежа трябва постоянно да имат един и същ IP адрес (това често е в сила за сървърите), те пак могат да използва DHCP. В този случай трябва да конфигурирате тези компютри да използват *резервиран адрес (reserved address)*. DHCP сървърът винаги назначава същия адрес на даден клиент, притежаващ такава резервация. Резервацията се извършва на базата на MAC адреса на DHCP клиента (т.е. на база физическия му адрес).

Произходът на DHCP

DHCP се разви от един по-ранен протокол, наречен Bootstrap Protocol (BOOTP). BOOTP беше разработен, за да позволи на бездисковите работни станции да извършват първоначално зареждане, да им се назначава IP адрес, след което да зареждат операционната система по мрежата.

DHCP е много по-усъвършенстван от BOOTP и позволява на администратора да конфигурира множество опции, както и да задава времетраене на наема. DHCP добавя динамично разпределение на адреси. Някои DHCP сървъри са конфигурирани да поддържат BOOTP клиенти.

DHCP не е специфичен за дадена операционна система. Той може да се използва с Microsoft, UNIX, NetWare и други популярни типове мрежи. Въпреки това реализациите на DHCP услугите от страна на отделните производители могат да се различават. Например Windows 2000 DHCP сървърите са интегрирани в Active Directory. Това позволява на администраторите да предотвратяват неавторизирани DHCP сървъри да раздават IP адреси в мрежата.

APIPA

Друг начин за автоматично получаване на IP адрес е APIPA. TCP/IP реализацията на неотдавнашните операционни системи на Microsoft, като например Windows 98 и Windows 2000, включват тази възможност.

По традиция, ако даден компютър е бил конфигуриран като DHCP клиент и не е в състояние да се свърже с DHCP сървър, когато се включи в мрежата, този компютър няма да има IP адрес и няма да е в състояние да комуникира по TCP/IP. APIPA адресирането беше разработено да разреши този проблем.

Когато един компютър с разрешено APIPA адресиране не може да открие DHCP сървър, той си самоназначава адрес от предварително заделен за целта диапазон от адреси (Клас B мрежата 169.254.0.0). Самоназначеният адрес може да се използва, докато DHCP сървърът отново започне да функционира.

Разделяне в подмрежи и обединяване в надмрежи

Да разделите дадена мрежа на подмрежи означава да я разделите на части. Разделянето на подмрежи (subnetting) превръща двустепенната йерархия на адресиране в тристепенна. За да разделите дадена мрежа на подмрежи, вие „заемате“ някои от битовете, които нормално се използват за хост частта от адреса, и ги използвате като второ ниво на мрежов адрес (подмрежов адрес).

Подмрежовата маска

Разделянето на подмрежи е свързано с процеса на заемане на една част от адреса и прехвърлянето ѝ към друга част. Когато извършваме разделяне на подмрежи, IP трябва да има някакъв механизъм да определя кои битове идентифицират мрежата и кои все още се използват за идентифициране на хоста. IP определя това, като използва *подмрежова маска (subnet mask),* 32-битово число, въвеждано от администратора при конфигурирането на TCP/IP настройките. Подмрежовата маска установява битовете, представляващи мрежовия идентификатор, в единици, а битовете, представляващи хост идентификатора, се установяват в нули. За частта за мрежовия идентификатор се казва, че е „маскирана“ от вдигнатите битове.

По подразбиране, за мрежов идентификатор Клас А мрежите използват битовете в първия октет, Клас В мрежите използват битовете в първите два октета, а Клас С мрежите използват първите три октета. *Подразбиращите се подмрежови маски (default subnet masks),* явяващи се резултат от това правило, са показани в Таблица 8-4.

Таблица 8-4 *Подразбиращите се подмрежови маски*

Класове адреси	Двоична подмрежова маска	Десетична подмрежова маска
Клас А	11111111.00000000.00000000.00000000	255.0.0.0
Клас В	11111111.11111111.00000000.00000000	255.255.0.0
Клас С	11111111.11111111.11111111.00000000	255.255.255.0

Подмрежовите маски в Таблица 8-4 се прилагат към мрежите, които не са разделени на подмрежи, и стига да се придържаме към тях, нещата са достатъчно прости.

Какво става обаче, ако решим да разделим дадена подмрежа? Нека приемем, че ни е назначен мрежов адрес от Клас В, като например 181.25.0.0. Знаем, че една Клас В мрежа може да съдържа 65 535 хост компютъра. Но ако имаме толкова много компютри в една мрежа, тогава бродкастният трафик ще бъде неуправляем.

Като решение на проблема нека приемем, че сме решили да разделим мрежата на шест подмрежи. За да направим това, трябва да заемем битове от хост частта на адреса, които да използваме за посочване на подмрежите, и освен това трябва да изчислим правилната подмрежова маска, която да казва на IP, че нашата мрежа има шест подмрежи (или осем възможни подмрежи).

Изчисляване на подмрежовата маска

Една подмрежова маска, различна от подразбиращите се маски, се нарича подмрежова маска с *вариращa дължина (variable-length)* или *потребителска (custom)* подмрежова маска. За да изчислим правилната подмрежова маска за нашия сценарий, при който искаме да имаме шест отделни подмрежи, трябва най-напред да определим колко бита трябва да заемем от хост частта на адреса.

Тъй като двоичните числа са в бройна система с основа 2, подмрежите трябва да се създават в блокове, които са степени на двойката. За да изчислим подмрежовата маска, трябва да открием каква степен на 2 ни дава 6 (или повече) подмрежи.

Ако повдигнем 2 на втора степен (2×2), получаваме 4. Трябват ни повече подмрежи, така че нека пробваме да повдигнем 2 на трета степен ($2 \times 2 \times 2 = 8$). Ако извадим 2, за да изпълним старото правило, което гласи, че не можем да използваме мрежови идентификатори, които се състоят само от 0-ли или само от 1-ци, ни остават 6 използваеми подмрежи. Ето защо трябва да заемем три бита от хост частта на адреса. Това означава, че трябва да обърнем първите три нули, индициращи хост идентификатора, в единици, които да индицират мрежовия идентификатор. Нашата оригинална подмрежова маска с взетите на заем битове сега изглежда така: 11111111.11111111.11100000.00000000. Ако преобразуваме в десетични стойности, получаваме 255.255.224.0.

По колко хост компютъра можем да имаме във всяка подмрежа? Погледнете оставащите нули, индициращи хост частта от адреса. Ще откриете, че те са са-

мо 13, което ни дава $2^{13} = 8192$. Това означава, че можем да имаме по 8190 хоста във всяка подмрежа, след като извадим 2, така че да няма хост адрес, съдържащ само нули или единици. (Запомнете, че забраната за това всички битове да са нули или единици беше премахната само по отношение на мрежовите идентификатори. Хост идентификаторите все още се подчиняват на това правило.)

Таблица 8-5 ни дава бърза справка за броя на подмрежите и хостовете, които можем да имаме за всяка подмрежова маска.

Таблица 8-5 *Схема за бърза справка след разделянето на подмрежи*

Десетичен запис за първия октет	Брой подмрежи	Брой Клас А хостове	Брой Клас В хостове	Брой Клас С хостове
.192	2	4 194 302	16 382	62
.224	6	2 097 150	8190	30
.240	14	1 048 574	4094	14
.248	30	524 286	2046	6
.252	62	262 142	1022	2
.254	126	131 070	510	—
.255	254	65 534	254	—

Операцията логическо И

Когато се извършва предаване по мрежата чрез използване на TCP/IP, IP трябва да определи дали компютърът местоназначение се намира в същата подмрежа като изпращащия компютър. Ако и двата компютъра са в една и съща подмрежа, съобщението е бродкаства. Ако компютърът местоназначение е в различна подмрежа, съобщението се изпраща към адреса на *подразбиращия се шлюз (default gateway)*, който е адресът на интерфейса на маршрутизатора (маршрутизаторът служи като шлюз към останалите подмрежи).

IP използва процес, наречен операция логическо И (ANDing), за да установи дали изпращащият и приемащия компютър са в една и съща подмрежа. Операцията логическо И се извършва чрез комбиниране на двоичните версии на IP адреса на всеки компютър с подмрежовата маска. При комбинирането на двоичните числа се използват следните правила:

- 1 И 1 = 1
- 1 И 0 = 0
- 0 И 0 = 0

Ето и пример за прилагане на логическо И: IP адресът на изпращащия компютър е 192.168.1.1, а подмрежовата маска е 255.255.255.0. IP адресът на компютъра местоназначение е 192.168.3.1, а подмрежовата маска за него е 255.255.255.0.

Най напред изпълняваме логическо И между IP адреса и подмрежовата маска на изпращащия компютър:

```
192.168.1.1 = 11000000.10101000.00000001.00000001  255.255.255.0 =
11111111.11111111.11111111.00000000

След операцията И = 11000000.10101000.00000001.00000000
```

След това извършваме същите изчисления за компютъра местоназначение и неговата подмрежова маска:

```
192.168.3.1 =          11000000.10101000.00000011.00000001
255.255.255.0 =      11111111.11111111.11111111.00000000

След операцията И =          11000000.10101000.00000011.00000000
```

Резултатите са различни, така че знаем (и по-важното, IP знае), че тези два компютъра се намират в различни подмрежи. След това съобщението се изпраща до маршрутизатора (подразбиращият се шлюз), за да бъде препратено към правилната подмрежа.

Ако резултатът беше еднакъв, IP щеше да знае, че компютърът местоназначение се намира в същата подмрежа и съобщението щеше да се изпрати чрез използване на Address Resolution Protocol (ARP) бродкаст. ARP се разглежда по-подробно по-нататък в тази глава.

Ползи от разделянето на подмрежи

Ползите от разделянето на една голяма мрежа на две или повече подмрежи включват следното:

- Намалява се бродкастният трафик. Подмрежите се свързват една с друга посредством маршрутизатори, а повечето маршрутизатори по подразбиране са конфигурирани да не предават бродкастни съобщения от една подмрежа в друга.
- Компютрите в различни местоположения могат да се организират в отделни подмрежи за по-лесно управление.
- Част от мрежата се изолира с цел сигурност или филтриране.
- Осигурява се по-ефективно използване на наличните адреси и има по-малки „похабени“ адреси.

Темата за разделянето на подмрежи може да заеме цяла книга. Това е сложна тема и всички подробности около нея са отвъд обхвата на тази книга, която по-скоро има въвеждащ характер (списъкът в края на тази глава съдържа адреси към добри ръководства по разделяне на една мрежа на подмрежи). Тук разгледахме само основните концепции на разделянето на подмрежи.

Протоколите от транспортния слой: TCP и UDP

Спомнете си от Глава 3, че транспортният слой (наречен *host-to-host* слой в DoD модела) е отговорен за осигуряването на надеждна директна връзка от точка до точка. Това се постига чрез механизми като потвърждения, които удостоверяват, че данните са пристигнали до своето местоназначение без повреда или загуба.

Протоколите от транспортния слой също така различават съобщенията, пристигащи до един и същ компютър. Тъй като различните приложения могат да изпращат или да получават съобщения едновременно, протоколите от транспортния слой използват *портове*, за да отделят съобщенията едно от друго. По-нататък в тази глава дискутираме концепцията за портовете и *сокетите*.

TCP/IP комплектът включва не един, а два протокола от транспортния слой:

- **Transmission Control Protocol (TCP)** – Връзково-ориентиран протокол

- **User Datagram Protocol (UDP)** – Безвръзков протокол

Кой от двата протокола се използва за изпращане на дадено съобщение? Зависи от нуждите за това предаване. TCP е подходящ, когато най-важна е надеждността, а UDP се използва, ако с най-висок приоритет е производителността (скоростта). В следващите секции изследваме характеристиките и функциите на всеки от тях.

Протоколът от транспортния слой: TCP

TCP, поради това, че е връзково-ориентиран протокол, установява сесия между двата комуникиращи си компютъра, преди да започне да изпраща данни. За установяването на сесията се използват съобщения за потвърждаване и отговор. След това се извършва проверка за грешки и тяхното коригиране, като данните се разделят на пакети.

Към всеки пакет се добавя информация за последователност, така че отделните части от съобщението да могат да се сглобят обратно в правилния ред. Тази информация също така позволява на приемащия компютър да открие дали няма липсващи пакети. Това прави TCP по-надежден от UDP, но на определена цена: всички тези допълнителни дейности намаляват производителността.

Протоколът от транспортния слой: UDP

UDP е безвръзков. Той не поставя ред на пакетите с данни; това означава, че той е по-подходящ за малки съобщения, които могат да се предадат в един пакет. UDP също така не следи какво е изпратил. Той обаче осигурява контролна сума, за да гарантира, че данните са непокътнати при пристигането им. Подобно на TCP, UDP осигурява номера на портове, за да разграничава заявките, подавани или доставяни на различни приложения.

Тъй като не трябва да се занимава с установяване на последователността или проверка за грешки, UDP е бърз. Неговите хедъри са по-прости от тези, добавяни от TCP. Routing Information Protocol (RIP), Trivial File Transfer Protocol (TFTP) и съобщенията за търсене на имена използват UDP.

ЗАБЕЛЕЖКА Какво е датаграма (*datagram*)? Терминът е дефиниран в RFC 1594 като „самостоятелна, независима единица данни, носеща достатъчно информация, за да бъде маршрутизирана от компютъра източник до компютъра местоназначение, без да разчита на по-раншни обмени между тези компютри и транспортиращата мрежа."

Термините датаграма и *пакет* понякога се използват взаимозаменяемо. Терминът „пакет" описва единица данни, която е част от група последователни единици или „парчета", на които е разбито дадено съобщение. Пакетите могат да поемат по различни маршрути в мрежата, за да достигнат своето местоназначение. След това те се сглобяват обратно. Датаграмата се използва за описание на по-простите и неподредени единици данни, предавани по UDP.

Портове и сокети

TCP/IP използва двукомпонентен логически адрес – IP адресът – за да идентифицира компютрите източници и компютрите местоназначения в мрежовите комуникации. Какво става обаче, ако две мрежови приложения, работещи на

един и същ компютър, изпращат заявки и получават отговори едновременно? Например какво става, ако дадено входящо съобщение е предназначено за вашата e-mail програма, докато друго е Web страница, която се връща към вашия Web браузър? Протоколът се нуждае от начин, по който да прави разлика между тях. Ето къде се намесват TCP и UDP портовете.

Ролята на номерата на портовете

Запомнете, че IP адресът на даден компютър местоназначение се състои от две части: мрежов адрес, който функционира подобно на име на улица, и хост адрес, функциониращ подобно на номер на къща. За номерата на портове можете да си мислите като специфична маршрутизираща информация вътре в даден адрес. Номерът на порт е допълнение към IP адреса, точно както името на адресата на пощенския плик е допълнение към адреса на улицата. По същия начин можете да си мислите за отделните приложения като за отделни обитатели.

Портът е *логическа точка на свързване*. Портовете се използват от транспортните протоколи, TCP и UDP, за да идентифицират специфичното приложение, което изпраща или получава съобщението.

Широко използваните Интернет приложения имат предефинирани номера на портове. Тази стандартизация улеснява комуникациите. Предварително назначените номера на портове се наричат *добре познати портове*. Таблица 8-6 изброява примери на тези широко използвани номера.

Таблица 8-6 *Добре познати номера на TCP/UDP портове*

Предварително назначен порт	Протокол	Приложение
80	TCP	HTTP
21	TCP/UDP	FTP
23	TCP/UDP	Telnet
25	TCP/UDP	SMTP
110	TCP/UDP	POP3
119	TCP/UDP	NNTP
137	TCP/UDP	NetBIOS name service
161	TCP/UDP	SNMP
194	TCP/UDP	IRC
389	TCP/UDP	LDAP
396	TCP/UDP	NetWare over IP
458	TCP/UDP	Apple QuickTime
500	TCP/UDP	ISAKMP

Съществуват 65 536 използваеми порта. Портове от 0 до 1024 („добре познатите портове“) са запазени за предефинирани услуги, като например показаните в Таблица 8-6.

Какво представляват сокетите?

След като вече разбирате функцията на портовете, ще дискутираме концепцията за сокетите. Общата дефиниция за сокет е „крайната точка на една връзка“; за да може да се осъществи комуникация, трябва да се създаде сокет.

Различните типове сокети използват различни методи за адресиране. Най-популярният метод използва IP адрес, комбиниран с номер на порт, за да идентифицира сокета. В UNIX терминологията това се нарича AF_INET адресиране. Втори метод за адресиране, AF_UNIX, за идентификация на сокетите използва имена на пътища.

Berkeley (BSD) Sockets се превърна в стандартния API интерфейс за TCP/IP комуникации. Популярна адаптация на интерфейса е *Windows Sockets*, или *Winsock*. Тази реализация предоставя API интерфейс за Интернет приложения, работещи под Windows операционни системи. Winsock се зарежда под формата на DLL.

Адресиране на плика: хедъри на пакети

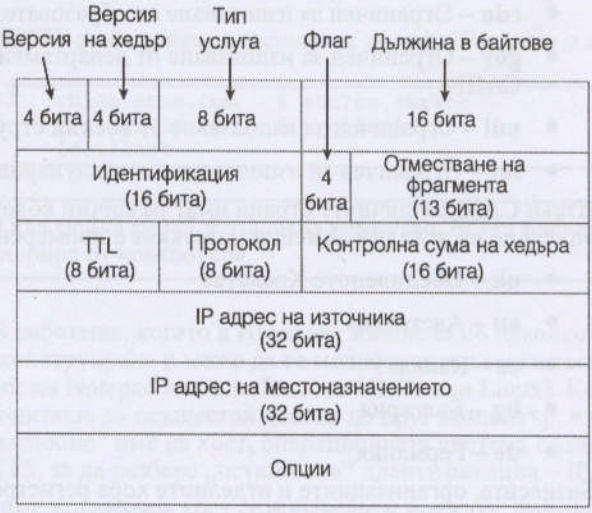
Вече знаете, че TCP/IP протоколите използват адресна информация, за да доставят дадено съобщение до неговото местоназначение. Вероятно обаче се чудите откъде протоколите намират цялата тази адресна информация. Точно както писмата, които изпращате по обикновена поща, трябва да са поставени в плик с обозначени на него адрес на подателя и адрес на получателя, така едно съобщение, изпращано по TCP/IP, трябва да бъде поставено „в плик".

Когато съобщението се поставя в „плика", данните се капсулират в протоколни *хедъри*, които съдържат адресите. Хедърите могат да включват и друга информация и специални инструкции, точно както на пощенския плик можете да напишете „Специална доставка", за да спомогнете за правилната доставка.

По подразбиране IP хедърът е дълъг 20 байта, като включва в себе си полета, посочващи следното (за повече подробности вижте Фигура 8-4):

- Тип на услугата
- Обща дължина на датаграмата
- Уникална идентификация на датаграмата
- Флагове и отместване при фрагментацията, които да помогнат при обратното сглобяване
- Време на живот (Time To Live – TTL), за да се ограничи броят на маршрутизаторите, през които датаграмата може да премине
- Протокол от по-горен слой, който трябва да получи данните (ICMP, TCP, UDP, IGRP или OSPF)
- Контролна сума за откриване на повреда
- IP адрес на източника (изпращащият компютър)
- IP адрес на местоназначението (приемащият компютър)

Фигура 8-4 *IP хедърът е съставен от 12 полета плюс опции.*



Хедърът може да включва опции, като ограничения по отношение на сигурността, времеви маркери и ограничения на маршрутизирането. Хедърът *без* опции е дълъг 20 байта.

Преобразуване на имена

Дискутирахме как TCP/IP използва IP адреси и номера на портове, за да идентифицира мрежи, компютри и специфични мрежови приложения, до които се изпращат съобщенията. Повечето хора обаче предпочитат да използват имена, вместо числа. Именно това предпочитание обяснява защо дори не искаме да си представим, че трябва да помним единните граждански номера, за да знаем с кого говорим!

Въпреки че обичаме да използваме имена, когато осъществяваме достъп до компютър в мрежата или въвеждаме местоположение на Web сървър в Web браузъра, компютрите работят само с числа. Поради тази несъвместимост се нуждаем от услуги, които превръщат „приятелските" имена в IP адреси. Използвайки тези услуги, когато искаме да посетим сайта на Xerox, можем да въведем www.xerox.com в адресната лента на нашия Web браузър, вместо 208.134.240.50. Името определено е по-лесно за запомняне. Но независимо от нашите действия, нашият браузър конвертира хост името в IP адрес, за да открие Web сървъра в Интернет и да извлече заявената страница.

Какво представлява едно име?

В компютърните мрежови комуникации се използват различни типове имена. В Интернет, имената на хостовете (компютрите) се подреждат в йерархична структура в *домейни*. Най-известните домейни от най-високо ниво в САЩ са следните:

- **com** – По начало предназначен за комерсиални организации
- **net** – По начало предназначен за мрежи на Интернет доставчици

- **org** – По начало предназначен за организации с идеална цел
- **edu** – Ограничен за използване от образователни институции
- **gov** – Ограничен за използване от департаменти на правителството на САЩ
- **mil** – Ограничен за използване от военни структури на САЩ
- **int** – Ограничен за използване от международни организации

Извън САЩ различните страни имат различни кодове, които се използват за описание на локални домейни (списъкът е примерен):

- **uk** – Обединеното Кралство
- **au** – Австралия
- **ca** – Канада
- **bg** – България
- **de** – Германия

Бизнесите, организациите и отделните хора регистрират *имена на домейни от второ ниво*, като например ibm.com, whitehouse.gov или dallas.net, вътре в домейните от най-високо ниво. По едно време имената на домейни от второ ниво се назначаваха от InterNIC, но сега тази задача е разпределена между няколко упълномощени регистратори.

Във вашия домейн от второ ниво отделните компютри се идентифицират от хост името, името на домейна от второ ниво и името на домейна от най-високо ниво, като всяка секция се разделя с точка. По този начин един Web сървър с име „www" в домейна dallas.net се идентифицира с името www.dallas.net. Това „разделено с точки" йерархично име се нарича *напълно квалифицирано име на домейн (fully qualified domain name – FQDN)*.

В мрежите на Microsoft на всеки компютър също така се назначава NetBIOS име. Това е име от максимум 16 знака, назначавано от администратора, което се използва за идентифициране на ресурси в локалната мрежа.

И двата типа имена трябва да се преобразуват в IP адреси, преди да може да се осъществи TCP/IP комуникация.

Транслиране на имена в числа

Можете да използвате следното, за да транслирате имена в IP адреси:

- HOSTS и LMHOSTS файлове, които са чисто текстови и се съхраняват на твърдия диск на компютъра
- DNS или Dynamic DNS (DDNS)
- WINS

Следващите секции описват тези средства за транслиране.

HOSTS и LMHOSTS файлове

В ранните дни на Интернет, методът за съпоставяне на имена на хостове (компютри) с IP адреси за TCP/IP комуникация беше файлът HOSTS. Това е текстов файл, съхраняван на локалния твърд диск; в него са изброени имената на хос-

товете и техните съответстващи IP адреси. Пример 8-1 показва пример за HOSTS файл.

Пример 8-1 *Един локален HOSTS файл прави съпоставяне между IP адреси и имена на хостове*

```
102.54.94.97    rhino.acme.com    # source server
38.25.63.10     x.acme.com        # x client host
127.0.0.1       localhost
```

ЗАБЕЛЕЖКА Знакът диез (#) във файла HOSTS означава коментар. Всяка информация след този знак се игнорира от компютъра.

Файлът HOSTS работеше, когато в Интернет имаше само няколко компютъра. Той е лесен за конструиране и може да се модифицира с всеки текстов редактор (например Windows Notepad и vi или Emacs в UNIX или Linux). Когато даден потребител се опиташе да осъществи достъп до друг компютър, използвайки неговото „дружелюбно" име на хост, операционната система правеше справка във файла HOSTS, за да разбере „истинската" идентификация – IP адресът.

Само че всеки път, когато нов хост се добавеше в мрежата, файлът HOSTS трябваше да се обновява ръчно, при това на всички компютри в мрежата. С нарастването на Интернет това се превърна в непосилна задача.

LMHOSTS изпълнява подобна функция в мрежите на Microsoft, като извършва съпоставяне между IP адреси и NetBIOS имена, вместо имена на компютри. Той обаче страда от същия недостатък като HOSTS; тъй като е статичен файл, той трябва да се обновява ръчно. Вижте Пример 8-2 за илюстрация на типичен LMHOSTS файл.

Пример 8-2 *Файлът LMHOSTS прави съпоставяне между IP адреси и NetBIOS имена*

```
102.54.94.97    rhino    #PRE #DOM:networking  #net group's DC
102.54.94.102 "appname  \0x14"   #special app server
102.54.94.123   popular #PRE      #source server
102.54.94.117   localsrv  #PRE    #needed for the include
```

Очевидно е, че има нужда от по-добро средство за съпоставяне на имена и IP адреси.

DNS и DDNS

Системата DNS беше разработена, за да разреши проблемите, свързани с използването на HOSTS файлове. DNS сървърите съхраняват бази данни с двойки IP адрес – име на хост, а TCP/IP свойствата на клиентите се конфигурират с адреса на DNS сървъра. Когато дружелюбно име на хост трябва да се транслира в съответстващия му IP адрес, клиентът се свързва с DNS сървъра.

В Интернет съществува йерархия от DNS сървъри, като отделните сървъри поддържат DNS информация за техните собствени „зони". Ако DNS сървърът, с който вашият компютър се е консултирал, не притежава IP съответствие за въведеното от вас име на хост, той предава заявката към друг DNS сървър, докато информацията не бъде получена.

DNS не е абсолютно задължителен, за да се извършва комуникация по Интернет, но без него всички комуникации трябва да използват IP адреси, вместо имена на хостове. Например, ако в TCP/IP свойствата нямате конфигуриран ад-

рес на DNS сървър, пак можете да осъществявате достъп до Web сайтове, като въвеждате техните IP адреси. Но ако вместо това въведете името на хоста, браузърът няма да може да върне страницата. Адресът на DNS сървъра може да се въведе ръчно или да се получи от DHCP сървър, ако компютърът ви е конфигуриран като DHCP клиент.

DNS е голямо подобрение на локалните HOSTS файлове, тъй като базата данни се съхранява на централен сървър и трябва да я обновявате само там, вместо на всички клиентски машини. Въпреки това базата данни на сървъра пак трябва да се обновява ръчно. *Dynamic DNS* се справя с този проблем чрез разрешаване на автоматични обновявания на DNS базата данни. Използвайки подобрената версия на DNS, клиентските компютри могат да регистрират и обновяват записите за своите ресурси на DNS сървъра при възникване на промени.

Windows 2000 DNS сървърите и BIND, версия 8, поддържат протоколното разширение DDNS. RFC 2136 съдържа спецификациите за DDNS стандарта.

Таблицата с базата данни на DNS

DNS използва различни типове записи в таблицата с базата данни. Тук са изброени някои от най-популярните типове записи:

- **Address (A) запис** – Съпоставя име на хост с IP адрес
- **Mail Exchange (MX) запис** – Сочи към сървър за обмяна на поща за специфичен хост
- **Canonical Name (CNAME) запис** – Съпоставя *псевдоними,* или допълнителни имена, с хост

Всички тези типове записи (и други за специализирани цели) са комбинирани в DNS таблицата.

WINS

WINS е друг метод за преобразуване на имена в IP адреси. В този случай NetBIOS имена (използвани за идентифициране на компютри и услуги в мрежи на Microsoft) се съпоставят в база данни на WINS сървър. Windows NT и Windows 2000 сървърите могат да функционират като WINS сървъри.

NetBIOS имената са плоски, а не йерархични както са FQDN имената (DNS хост имената). Докато FQDN за даден сървър може да е exeter.tacteam.net, едно NetBIOS име би било просто Exeter. TCP/IP не разбира от NetBIOS имена; за да се осъществи комуникация със сървъра, отново е необходим IP адрес. WINS, подобно на статичния LMHOST файл, може да транслира името в изисквания IP адрес.

WINS, за разлика от оригиналния DNS, използва динамично обновявана база данни. Когато в мрежата се появят WINS клиенти, те обявяват своето присъствие на WINS сървъра, давайки своето име и IP адрес. WINS сървърът изгражда своята база данни от тази информация.

DHCP, DNS и WINS могат да работят заедно в една мрежа. В новите операционни системи като Microsoft Windows 2000, трите услуги са интегрирани, за да работят съвместно и ефективно.

Обобщение на методите за преобразуване на имена

Лесно е да се объркате от различните методи за преобразуване на имена. Таблица 8-7 обобщава възможностите и употребата на всеки от тях.

Таблица 8-7 *Методи за преобразуване на имена*

Метод за преобразуване на имена	Тип на преобразуването	Характеристики
HOSTS файл	Имена на хостове в IP адреси	Текстов файл; трябва да се обновява ръчно на всеки компютър
LMHOSTS файл	NetBIOS имена в IP адреси	Текстов файл; трябва да се обновява ръчно на всеки компютър
DNS	Имена на хостове в IP адреси	Централизирана база данни, управлявана от DNS сървър; трябва да се обновява ръчно
DDNS	Имена на хостове в IP адреси	Централизирана база данни, управлявана от DNS сървър; може да се обновява динамично
WINS	NetBIOS имена в IP адреси	Централизирана база данни, управлявана от WINS сървър; може да се обновява динамично

TCP/IP помощни програми

TCP/IP е сложен сбор от протоколи. Повечето реализации на отделните производители включват най-различни помощни програми за разглеждане на конфигурационната информация и отстраняване на проблеми. В следващата секция разглеждаме следните общи TCP/IP помощни програми:

- Packet Internet groper (ping)
- Address Resolution Protocol (ARP) и Reverse ARP (RARP)
- Netstat и tpcon
- Nbtstat
- Помощни програми за конфигуриране на IP: ipconfig, winipcfg, config и ifconfig
- Помощни програми за проследяване на маршрута: traceroute, tracert и iptrace

ЗАБЕЛЕЖКА Помощните програми, които изпълняват една и съща функция, могат да имат различни имена, дадени им от различните производители.

Ping

Това е проста, но много полезна помощна програма за работа от командния ред, включвана в повечето реализации на TCP/ IP. Ping може да се използва както с името на хоста, така и с IP адреса, за да се тества IP свързването.

Ping работи, като изпраща ICMP ехо заявка към компютъра местоназначение. Приемащият компютър след това изпраща обратно съобщение за ICMP ехо отговор.

Също така е възможно да използвате ping, за да разберете IP адреса на даден хост, когато знаете името. Ако въведете командата **ping apple.com**, както е показано в Пример 8-3, ще видите IP адреса, от който е върнат отговорът.

Пример 8-3 *Върнатата информация в отговор на командата ping за apple.com*

```
c:\>ping apple.com
Pinging apple.com [17.254.3.183] with 32 bytes of data:
Reply from 17.254.3.183: bytes=32 time=430ms TTL=90
Reply from 17.254.3.183: bytes=32 time=371ms TTL=90
Reply from 17.254.3.183: bytes=32 time=370ms TTL=90
Reply from 17.254.3.183: bytes=32 time=371ms TTL=90

Ping statistics for 17.254.3.183:
    Packets: Sent = 4, Received = 4, Lost = 0 <0% loss.,
Approximate round trip times in milli-seconds:
    Minimum = 370ms, Maximum = 430ms, Average = 385ms
```

Една друга помощна програма, nslookup, връща IP адреса да дадено име на хост и хост името за даден IP адрес.

Novell реализира ping като NetWare Loadable Module (NLM). Windows и UNIX/Linux операционните системи използват командата **ping** от командния ред. Съществуват и ping реализации от независими производители, някои от които предоставят графичен интерфейс.

ARP и RARP

ARP се отнася до самия протокол и до помощната програма от командния ред, използвана за разглеждане и манипулиране на ARP кеша. Трябва да сте наясно с функцията на протокола, за да можете да използвате тази програма правилно.

ARP: Протоколът

ARP е средството, чрез което компютрите в мрежата съпоставят логически IP адреси с физически хардуерни (MAC) адреси. ARP изгражда и поддържа таблица, наречена *ARP кеш,* в която се съдържат тези съпоставяния. RARP се използва от машина, която не знае собствения си IP адрес, за да получи информацията на база своя MAC адрес.

ARP: Помощната програма

ARP също така е помощна програма, работеща от командния ред, която се разпространява с TCP/IP стека на Windows и UNIX/Linux; тя може да се използва за разглеждане и промяна на съпоставяният между IP и MAC адреси. (Novell реализира това като NLM модул, наречен tpcon.) С помощта на помощната програма ARP можете да покажете съдържанието на кеша и да добавяте или изтривате специфични записи, както е показано в Пример 8-4.

Пример 8-4 *Командата arp се използва за разглеждане на ARP кеша*

```
c:>arp -a
Interface: 192.168.1.201 on Interface 0x2
    Internet Address      Physical Address      Type
    192.168.1.16          00-40-f6-54-d7-43     dynamic
    192.168.1.185         00-50-da-0d-f5-2d     dynamic
```

С командата **arp** могат да се използват следните ключове:

- **arp –a** – Показва кеша
- **arp –s** – Добавя перманентно съпоставяне между IP и MAC адрес
- **arp –d** – Изтрива запис

В отделните реализации на производителите са включени и други ключове.

Netstat/Tpcon

Често пъти е полезно да разгледате мрежовите статистики. Командата **netstat** се използва в Windows и UNIX/Linux, за да покаже информация за TCP/IP връзките и протокола. За тази цел Novell използва NLM модула tpcon.

Командата **netstat** предоставя списък с връзки, които са текущо активни, както е показано в Пример 8-5.

Пример 8-5 *Командата netstat се използва за разглеждане на информация за връзките*

```
c:>netstat
Active Connections
  Proto   Local Address   Foreign Address                State
  TCP     DS2000:3301     msgr-ns18.hotmail.com:1863     ESTABLISHED
  TCP     DS2000:3450     constellation.tacteam.net:3389 ESTABLISHED
  TCP     DS2000:3860     ultra1.dallas.net:pop3         TIME_WAIT
  TCP     DS2000:3861     aux153.plano.net:pop3          TIME_WAIT
```

В Пример 8-5, можете да видите протоколите, използвани за всяка връзка, името на локалния компютър и номера на порта, използвани за връзката, „чуждестранният“ (foreign) адрес (името на отдалечения компютър) и състоянието на връзката.

Командата **netstat** може да се използва с няколко ключа, както е показано в Таблица 8-8.

Таблица 8-8 *Ключове на netstat и техните функции*

Ключ	Функция
-a	Показва всички връзки и слушащи портове
-e	Показва Ethernet статистики
-n	Показва адреси и портове
-p[1]	Позволява ви да показвате информация само за избран протокол
-t, -u, -w, -x[2]	Позволява ви да показвате информация за TCP, UDP, RAW или сокети
-r	Показва маршрутната таблица
-s	Предоставя обобщение на статистиките за всеки протокол

[1] Използва се с реализацията на Microsoft TCP/IP

[2] Използва се с реализацията на Linux TCP/IP

Netstat статистиките могат да бъдат полезни при отстраняване на проблеми с TCP/IP връзките. Пример 8-6 показва изобилието от информация, предоставяна в режим на обобщение (ключът -s). Тези доклади за грешки са особено полезни при диагностициране на проблеми с хардуера и маршрутизирането.

Пример 8-6 *Командата netstat -s извежда TCP/IP статистики*

```
C:>netstat -s
IP Statistics
  Packets Received                   = 1091043
  Received Header Errors             = 0
  Received Address Errors            = 7
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 0
  Received Packets Delivered         = 1091034
  Output Requests                    = 420049
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packets No Route            = 0
  Reassembly Required                = 6
  Reassembly Successful              = 3
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 12
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 24
ICMP Statistics

                        Received    Sent
Messages                     994    1129
Errors                         0       0
Destination Unreachable       12      82
Time Exceeded                  0       0
Parameter Problems             0       0
Source Quenches                0       0
Redirects                      0       0
Echoes                        37    1010
Echo Replies                 945      37
Timestamps                     0       0
Timestamp Replies              0       0
Address Masks                  0       0
Address Mask Replies           0       0

TCP Statistics
Active Opens                       = 3940
Passive Opens                      = 42
Failed Connection Attempts         = 77
Reset Connections                  = 930
Current Connections                = 2
Segments Received                  = 577343
Segments Sent                      = 388999
Segments Retransmitted             = 361

UDP Statistics
Datagrams Received                 = 38481
No Ports                           = 475173
Receive Errors                     = 0
Datagrams Sent                     = 29404
```

Nbtstat

Microsoft TCP/IP стековете, включени в Windows операционните системи, предоставят помощната програма nbtstat, която се използва за извеждане на NetBIOS информация. Пример 8-7 показва синтаксиса и ключовете, налични за командата **nbtstat**.

Пример 8-7 *Въведете nbtstat на командния ред, за да се покаже синтаксисът и списъкът с наличните ключове*

```
c:\>nbtstat

Displays protocol statistics and current TCP/IP connections using
NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given
                        its name
  -A   (Adapter status) Lists the remote machine's name table given
                        its IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names
                        and their IP addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via
                        WINS
  -R   (Reload)         Purges and reloads the remote cache name
                        table
  -S   (Sessions)       Lists sessions table with the destination IP
                        addresses
  -s   (sessions)       Lists sessions table converting destination
                        IP addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINs and then,
                        starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval
               seconds between each display. Press Ctrl+C to stop
               redisplaying statistics.
```

Ipconfig, Winipcfg, Config и Ifconfig

Информацията за TCP/IP конфигурацията може да се изведе чрез използване на следните помощни програми, които зависят от операционната система:

- **Ipconfig** – Windows NT и Windows 2000 (от командния ред)
- **Winipcfg** – Windows 95 и 98 (графичен интерфейс)
- **Ifconfig** – UNIX и Linux (от командния ред)
- **Config** – NetWare (сървърна конзола)

Конфигурационните помощни програми могат да предоставят богата информация, включваща текущо използвания IP адрес, MAC адреса, подмрежовата маска и подразбиращия се шлюз; адреси на DNS и WINS сървъри; DHCP информация; разрешени услуги. Съществуват множество ключове, зависещи от про-

изводителя и специфичната помощна програма. Вижте Пример 8-8 за резултатите от използването на командата **ipconfig** с ключа **/all** в Windows 2000.

Пример 8-8 *Конфигурационна информация, изведена от командата ipconfig /all в Windows 2000*

```
c:\>ipconfig/all
Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : DS2000
        Primary DNS Suffix  . . . . . . . : tacteam.net
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : Yes
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : tacteam.net

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 3Com EtherLink XL 10/100
PCI TX NIC(3C905B-TX)
Physical Address. . . . . . . . . : 00-50-04-7C-C0-D2
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.201
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.16
        DNS Servers . . . . . . . . . . . : 192.150.87.2
                                            216.87.128.131
        Primary WINS Server . . . . . . . : 192.168.1.185
```

Tracert, Iptrace и Traceroute

Често пъти е полезно да проследите маршрута, по който даден пакет поема пътя от компютъра източник до хоста местоназначение. TCP/IP стековете включват помощна програма за проследяване на маршрута, която ви позволява да идентифицирате маршрутизаторите, през които преминава съобщението. В зависимост от вашата операционна система можете да използвате една от следните:

- **Tracert** – Windows
- **Iptrace** – NetWare NLM
- **Traceroute** – UNIX/Linux

Пример 8-9 показва резултатите от проследяване чрез използване на командата **tracert**, която има следния синтаксис:

tracert *име на хоста местоназначение*

Пример 8-9 *Можете да използвате tracert, за да проследите маршрута на пакет от източника до местоназначението*

```
c:\>tracert dallas.net

Tracing route to dallas.net [204.215.60.1]
over a maximum of 30 hops:

  1  <10 ms   <10 ms   <10 ms  STARBLAZER [192.168.1.16]
  2   60 ms    90 ms    60 ms  dal-isdn0.august.net [216.87.128.117]
```

```
  3   80 ms    60 ms   100 ms  dal-gw-eth0.august.net
[216.87.128.126]
  4   60 ms    70 ms    61 ms  dal-gw2-fe2-0.august.net
[216.87.128.86]
  5   60 ms    70 ms   100 ms  500.Serial2-7.GW6.DFW9.ALTER.NET
[157.130.216.157]
  6   80 ms    70 ms    60 ms  158.at-5-0-0.XR1.DFW9.ALTER.NET
[152.63.100.186]
  7   60 ms   110 ms    70 ms  185.ATM6-0.XR1.DFW4.ALTER.NET
[152.63.96.137]
  8   80 ms    70 ms    80 ms  195.ATM11-0-0.GW1.DFW1.ALTER.NET
[146.188.240.41]
  9   90 ms   320 ms   171 ms  savvis-dfw-gw.customer.ALTER.NET
[157.130.128.54]
 10   90 ms    90 ms   100 ms  ETHOS-1.usdlls.savvis.net
[209.44.32.10]
 11  150 ms   130 ms   131 ms  cisco-plano-e0.dallas.net
[204.215.60.1]

Trace complete.
```

Както можете да видите, проследяването показва IP адрес и името на препращащия компютър или маршрутизатор. На пакета са му били необходими единадесет скока, за да достигне до своето местоназначение, което е хостът с име www.dallas.net. Времената за отиване и връщане (в милисекунди) са показани за всеки скок.

Обобщение на TCP/IP помощните програми

TCP/IP е голям и сложен комплект от протоколи. Повечето реализации включват най-различни помощни програми, които могат да бъдат използвани за събиране на информация и отстраняване на проблеми. Таблица 8-9 предлага обобщение на често използваните помощни програми.

Таблица 8-9 *TCP/IP помощни програми*

Помощна програма	Употреба
ARP/RARP	За разглеждане на записите със съпоставянията между IP адреси и MAC адреси, използвани от ARP протокола, за изтриване на записи от ARP кеша и за добавяне на нови IP-към-MAC съпоставяния
Netstat (Windows/UNIX), tpcon (NetWare)	За разглеждане на статистики относно мрежовите връзки и протоколи
Netbtstat (Windows)	За разглеждане на връзки и статистики за NetBIOS по TCP/IP (NetBT)
Ipconfig (Windows NT/2000), Winipcfg (Windows 95/98), Config (NetWare), Ifconfig (UNIX)	За разглеждане на информация относно TCP/IP конфигурацията, като например IP адрес, подмрежова маска, подразбиращ се шлюз, MAC адрес, разрешени услуги и други
Tracert (Windows), Iptrace (NetWare), Traceroute (UNIX)	За откриване на маршрута, поет от даден пакет по пътя от източника до местоназначението, както и за идентификация на маршрутизаторите, през които той преминава
Ping	За определяне на IP свързването между две системи

Протоколи от приложния слой

Комплектът TCP/IP включва най-различни протоколи от приложния слой, предоставящи услуги като терминална емулация, качване и сваляне на файлове, както и достъп до страници, публикувани в World Wide Web. Повечето реализации включват приложения, които използват следните протоколи:

- HTTP (Hypertext Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- NNTP (Network News Transfer Protocol)
- FTP (File Transfer Protocol)
- Telnet

Интернет протоколите и програмите, които ги използват, са дискутирани в Глава 9, „Най-широкомащабната мрежа: глобалният Интернет".

Обобщение

Много протоколи работят съвместно с мрежовите/транспортните протоколи и тези от по-висок слой, за да осигурят LAN и WAN комуникации. Необходимо е множество протоколи да работят заедно, за да се установят и поддържат мрежови комуникации между компютри в една LAN или WAN мрежа. В тази глава дискутирахме трите най-популярни мрежови/транспортни протоколни стека: NetBEUI, IPX/SPX и TCP/IP.

Научихте, че компютърните комуникации са базирани на двоични числа, но въпреки това хората продължават да предпочитат да използват имена, за да идентифицират системите и ресурсите. Дискутирахме съществуващите методи за преобразуване на тези „дружелюбни" имена в IP адреси, които могат да се използват от компютрите.

Тази глава беше посветена главно на TCP/IP, тъй като това е протоколът на глобалния Интернет и на повечето средни или големи съвременни LAN мрежи. Научихте за комплекта от протоколи, изграждащи TCP/IP.

Тази глава дискутира основните концепции на IP адресирането и научихте за традиционните адресни класове и CIDR, което е нов метод за маршрутизиране, използващ безкласово адресиране. Научихте за двете части на всеки IP адрес, ролята на TCP и UDP портовете при доставяне на дадено съобщение до неговото местоназначение, а също как и защо се налага да разделяме една IP мрежа на подмрежи. Научихте също така за DHCP, който автоматично назначава IP адреси на компютри, конфигурирани като DHCP клиенти.

Протоколите, използвани за мрежови комуникации, са сложни. Тази глава осигурява само ограничен преглед. Множество отлични книги, Web сайтове и учебници, както и онлайн курсове, дискутират тези теми много по-задълбочено.

След като вече имате основните познания относно начина на работа на мрежовите протоколи, в следващата глава ще разгледаме най-голямата и най-сложна мрежа в света: глобалният Интернет.

Допълнителни източници

За преглед на IPv6, следващото поколение на Интернет протокола, вижте playground.sun.com/pub/ipng/html/ipng-main.html.

Отличен източник, описващ мултикастването и MBONE, можете да намерите на www.savetz.com/mbone/ch3.html.

3Com предоставя добър основен преглед на IP адресирането, включвайки темата за разделянето на подмрежи, на адрес www.3com.com/nsc/501302.html.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Кой от следните мрежови/транспортни протоколи е най-бърз и най-лесен за конфигуриране, но е немаршрутизируем?

- **a** NWLink
- **b** NetBIOS
- **c** NetBEUI
- **d** IPX/SPX

2 Коя от следните части на едни IPX адрес е базирана на MAC адреса на устройството?

- **a** Възлов номер
- **b** Мрежов номер
- **c** Номер на подмрежа
- **d** Номер на хост

3 Кои от следните протоколи са връзково-ориентирани? (Изберете всички верни отговори.)

- **a** TCP
- **b** UDP
- **c** IP
- **d** SPX
- **e** IPX

4 Кое от следните е вярно за IP адресите? (Изберете всички верни отговори.)

- **a** IP адресите са съставени от два октета.
- **b** Октетът е IP адрес, състоящ се от осем бита.
- **c** IP адресите са 32-битови двоични числа.
- **d** IP адресите обикновено се записват в шестнадесетичен формат.

5 Колко хост компютъра теоретично може да има в една Клас B мрежа?

- **a** 16 384

b 254
c 65 535
d 2 097 152
e Над 16 милиона

6 Каква е подразбиращата се подмрежова маска на една Клас С мрежа?

a 255.255.255.255
b 255.255.255.0
c 255.255.0.0
d 255.0.0.0

7 Като имаме предвид класовото адресиране, към кой адресен клас принадлежи IP адресът 190.23.201.6?

a Клас A
b Клас B
c Клас C
d Клас D

8 Кой е маршрутизиращият метод, използващ безкласово адресиране, при който мрежовият идентификатор, следващ след IP адреса, се посочва от „слаш екс"?

a CIR
b CD-R
c CIDR
d RIP

9 Каква е функцията на DHCP?

a Той преобразува NetBIOS имена в IP адреси.
b Транслира частните IP адреси в публични адреси.
c Преобразува IP адреси в MAC адреси.
d Автоматично назначава IP адреси на клиентските компютри.

10 Кои от следните TCP/IP помощни програми могат да бъдат използвани за разглеждане на кеша от IP адреси, които са преобразувани в MAC адреси?

a Ipconfig
b Iptrace
c ARP
d Nbtstat

Глава 9

Най-широкомащабната мрежа: глобалният Интернет

В Глава 8, „Мрежови протоколи и услуги“, научихте за мрежовите протоколи. Научихте, че някои от тях са по-подходящи за малки мрежи, а други могат да се мащабират невероятно много. Протоколният стек TCP/IP (Transmission Control Protocol/Internet Protocol) служи като основа за комуникиране по най-голямата и най-сложната мрежа в света: глобалният Интернет.

В тази глава изследваме еволюцията на Интернет, като междувременно ще научите повече за популярните Интернет приложения, като Мрежата (World Wide Web), електронната поща (e-mail), нюзгрупите и трансфера на файлове. Освен това дискутираме и модерни технологии, като поточната медия, аудиото в реално време и видео конференциите.

След това ще разгледаме как се маршрутизират пакетите, а също и популярните протоколи за откриване на маршрутите. Към края на главата ще научите за множеството организации, които наблюдават работата на Интернет и го поддържат в добра работна форма.

Еволюцията на Интернет

По дефиниция интернет е мрежа от мрежи, а Интернет е изграден от хиляди големи и малки мрежи, които сами по себе си са разпръснати из целия свят. Както научихте в Глава 1, „Въведение в мрежите“, Интернет води началото си от мрежата ARPAnet през 60-те години на миналия век, която представлява съвместен проект между големите образователни институции и Министерството на отбраната на САЩ.

В ранните дни на ARPAnet, т.е. по време на апогея на студената война, само малка елитна част от персонала на правителството и университетите имаха достъп до „супер мрежата“. Основна цел на военната част от така наречения „междумрежов проект“ беше да се разработи мрежа, която да оцелее и след ядрено поражение, оставайки работоспособна. Университетите, от друга страна, бяха заинтересовани в бързата обмяна на данни между различните изследователи.

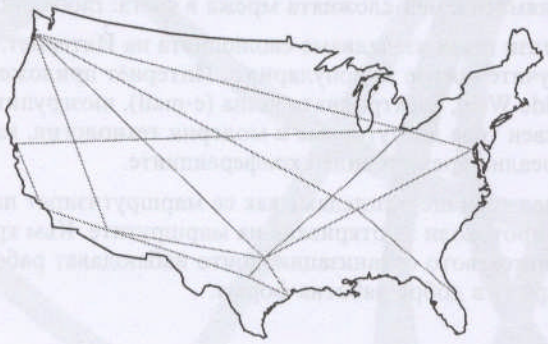
Разработката на опорния гръбнак

В среда на 1980-те Националната научна фондация (National Science Foundation – NSF) започна да разработва гръбнака на Интернет, като и до ден днешен тя осигурява някои Интернет услуги в САЩ. С разрастването и истинското глобализиране на Интернет се появиха и други обекти, служещи като гръбнак за комуникациите, като през 1995 година проектът за гръбнака беше приватизиран, а финансирането беше разпределено към регионалните мрежи. През периода 1986–1995 година NSF похарчи близо $200 милиона за разработката на гръбнака.

ЗАБЕЛЕЖКА Един *гръбнак* на Интернет представлява група от комуникационни канали, използвани от локалните мрежи за свързването им на големи разстояния. Гръбнаците на Интернет са изградени от точки на свързване, наречени *възли*.

Както можете да видите на Фигура 9-1, инфраструктурата на Интернет използва хибридна решетъчна топология. Тази топология осигурява редундантност, така че ако някоя от връзките бъде прекъсната, пакетите могат да поемат по алтернативен маршрут, за да достигнат до тяхното местоназначение.

Фигура 9-1 *Гръбнакът на Интернет е организиран в хибридна решетъчна топология.*



Инфраструктурата в САЩ на съвременния Интернет се състои от комерсиален гръбнак и високоскоростна услуга, наречена vBNS, което е съкращение от Very High-speed Backbone Network Service – опорна мрежова услуга с много висока скорост.

Комерсиалният гръбнак

Комерсиалният гръбнак е мрежа от комерсиално управлявани мрежи, осигурявани от компании като AT&T, Sprint, UUNET (подразделение на WorldCom), BBN Planet и Cable & Wireless USA. Доставчиците на Интернет услуги (ISPs – Internet Service Providers) се свързват към тези комерсиални мрежи.

Доставчиците на гръбнака и доставчиците на Интернет услуги установяват помежду си споразумения за *пиъринг* (*peering*), за да може всеки да пренася мрежовия трафик на останалите. Тези споразумения управляват взаимната свързаност и обмяната на данни. В САЩ (а и в много други страни) физическите кабели се притежават от регионалните телефонни компании, а те ги отдават под наем на доставчиците. Мрежите на доставчика се свързват чрез T-1, T-3 или OC-3 линии.

vBNS и центровете със суперкомпютри

vBNS услугата се използва за научни цели. Тя свързва пет центъра със „суперкомпютри", намиращи се на следните места:

- Националният център по използване на суперкомпютри (National Center for Supercomputing Applications – NCSA), Урбана, Илинойс
- Центърът по национално партньорство за усъвършенствана изчислителна инфраструктура (National Partnership for an Advanced Computational Infrastructure – NPACI), Сан Диего, Калифорния
- Корнелски теоретичен център, Итака, Ню Йорк
- Национален център за изследване на атмосферата, Болдър, Колорадо
- Центърът за суперкомпютри в Питсбърг, Питсбърг, Пенсилвания

vBNS се финансира от NSF чрез договор с MCI. Тя е изградена от OC-3 връзки, работещи със скорост 155 Mbps и повече. vBNS мрежата е свързана към национални точки за мрежов достъп (network access points – NAPs), които са дискутирани по-нататък в тази глава. Комерсиалният гръбнак също използва NAP точките.

Проектът Интернет2

vBNS е част от проекта Internet2 Project – съвместна разработка на американските университети и правителството на САЩ. Целта му е създаване на високоскоростен гръбнак, който да се използва за тестване на нови технологии. Например чрез Интернет2 е тестван протоколът IPv6, а също така е спонсорирана Qbone – инициатива за тестване на качеството на услугата (quality of service – QoS).

Интернет2 не е самостоятелна физическа мрежа и не е предназначен да замени „стария" Интернет. По-скоро той е консорциум от отделни единици, които са се обединили, за да развиват и тестват нови технологии, преди те да бъдат внедрени в комерсиалния Интернет.

Компонентите на Интернет

За съвременните потребители Интернет изглежда много прост. Свързвате модема на компютъра към телефонната линия, конфигурирате софтуера да набира Интернет доставчик или онлайн услуга, въвеждате име за акаунта и парола, и сте готови. Ако компютърът ви е свързан в локална мрежа с достъп до Интернет, нещата са още по-прости.

Повечето хора не оценяват, нито пък разбират сложността на технологията, позволяваща това, повече, отколкото разбират какво *наистина* става, когато си включат телевизора и превключат на любимия си канал. Те просто го приемат като едно от чудесата на съвременната наука.

Но понеже вие се интересувате от изучаване на технологиите, предполагаме, че искате да научите за компонентите, които се използват при осъществяване на достъп до един Web сайт или за изпращане на e-mail съобщение до някой, живеещ на отсрещната страна на улицата или на другия край на света. И така, в следващите секции дискутираме взаимодействието на следните елементи, изграждащи Интернет:

- Локален компютър или LAN мрежа, свързани към Интернет
- Доставчик на Интернет (ISP)
- Регионална мрежа
- NAP точки
- Градски централи (Metropolitan area exchanges – MAEs)

Локален компютър или LAN

Първият елемент, изискван за иницииране на връзка към Интернет и за комуникация, е локален компютър, на който са инсталирани подходящи протоколи и софтуер, или пък такъв, свързан към локална мрежа с прокси/NAT връзка.

TCP/IP е протоколният стек на Интернет, така че той трябва да е инсталиран и конфигуриран на локалния компютър или на прокси/NAT машината. За dial-up връзка е необходим софтуер за набиране. Модерните операционни системи обикновено имат вграден софтуер за набиране – например компонентът Dialup Networking на Microsoft.

Доставчик на Интернет

Когато се осъществи връзка към доставчик на Интернет, компютърът става отдалечен клиент на локалната мрежа на доставчика.

В началото на Интернет ерата вашият локален компютър или LAN мрежа трябваше да бъдат свързани директно към гръбнака на Интернет. Това беше скъпо и непостижимо за отделните хора или малките компании.

Доставчиците притежават или наемат скъпото и сложно оборудване, използвано за изграждане на *точка на присъствие* (*point of presence*), или точка за достъп, в Интернет. Те наемат специализирани високоскоростни линии от телефонната компания, или, както е в случаите с големите доставчици, притежават свои собствени. Малките местни доставчици на Интернет може и да не са свързани директно с гръбнака, като вместо това осъществяват връзка през по-голям регионален доставчик.

Регионална мрежа

Доставчиците на Интернет, които не са свързани директно към националния гръбнак, плащат на *регионален доставчик*, за да се свържат към регионалната му мрежа, която от своя страна е свързана към гръбнака. Основните регионални мрежи в САЩ включват:

- **BARRNet** – намира се в северна и централна Калифорния
- **Westnet** – покрива западната част на САЩ
- **NEARNET и NYSERNet** – покриват североизточната част на САЩ
- **MIDnet** – покрива централната част на САЩ
- **SURAnet** – покрива югоизточната част на САЩ
- **CICnet** – покрива централните западни части на САЩ

NAP точки

NAP точките (точките за достъп до мрежата) са такива местоположения, в които отделните доставчици се свързват помежду си. Националната научна фондация разработи и финансира първите четири NAP точки в САЩ. Те са разположени във или в близост до следните градове, като се управляват от изброените компании:

- **Ню Йорк** – Sprint
- **Вашингтон, окръг Колумбия** – WorldCom
- **Чикаго** – Ameritech
- **Сан Франциско** – Pacific Bell

NAP точките осигуряват комутиращи центрове, но не целият Интернет трафик трябва да преминава през тях. Доставчиците на Интернет в отделни географски региони могат да се свържат взаимно помежду си в пиъринг.

Градски централи

Градската централа (metropolitan area exchange – MAE) е точка, където Интернет доставчиците се свързват един с друг и трафикът се комутира между тях. NAP точката във Вашингтон, окръг Колумбия, е позната и като MAE EAST. WorldCom обслужва точката за достъп MAE WEST, намираща се в Силициевата долина, Калифорния. MAE EAST и MAE WEST са MAE централите от първо ниво.

Съществуват пет MAE централи от второ ниво: MAE CHICAGO, MAE DALLAS, MAE HOUSTON, MAE LOS ANGELES и MAE NEW YORK. Самата MAE централа не маршрутизира данни; това се извършва от Интернет доставчиците, свързани към MAE централата. Все пак MAE централите осигуряват *колокация (collocation)*, или терен, за маршрутизаторите, принадлежащи на ISP-тата (доставчиците на Интернет).

Свързаните към MAE маршрутизатори изискват много големи маршрутизиращи таблици; за целта се използват най-мощните маршрутизатори, като например тези от серията Cisco 7000. WorldCom притежава комутационните платформи, които са свързани в FDDI (Fiber Distributed Data Interface) мрежа. MAE устройствата се администрират през работни станции на Sun, като се използва протоколът SNMP (Simple Network Management Protocol – прост протокол за управление на мрежата) и специализирани приложения за наблюдение.

Основните национални Интернет доставчици, като например Sprint и Netcom, се свързват към двете MAE централи от първо ниво. Регионалните и по-малките ISP-та се свързват към MAE централите от второ ниво, където се използват по-малки маршрутизатори (например Cisco 4500-M).

Как Интернет компонентите работят заедно

Как компонентите на Интернет се отнасят към типичния Интернет потребител? Когато щракнете с мишката, за да изпратите e-mail съобщение, e-mail клиентското приложение форматира данните и след това преминава през процеса, за който научихте в Глава 3, „Мрежови концепции, модели и стандарти“. Фигура 9-2 показва опростена версия на тази последователност от събития.

Фигура 9-2 *Едно съобщение се изпраща през Интернет.*

1. Данните се раздробяват на управляеми парчета, наречени пакети.
2. Мрежовите протоколи добавят хедър и трейлър.
3. Двоичните единици и нули се преобразуват в електрически сигнали или светлинни импулси, за да могат да преминат през физическата транспортна среда.
4. Ако компютърът ви е свързан в локална мрежа, данните пътуват през локалната мрежа до сървър или маршрутизатор, свързан към телефонна линия или посветена наета линия.
5. Ако се използва модемна връзка, пакетите се капсулират в протокола, работещ в каналния слой, като например Point-to-Point Protocol (PPP) или Serial Line Internet Protocol (SLIP), след което цифровите сигнали се модулират, за да пътуват по аналоговата телефонна линия.
6. Сигналите достигат до сървъра за отдалечен достъп (remote access server – RAS) на Интернет доставчика, който сървър е конфигуриран да приема dial-in връзки, или пък е възможно да имате директна посветена връзка към ISP. С помощта на dial-in акаунт се логвате в сървъра, въвеждайки потребителско име и парола.
7. Компютърът се превръща в отдалечен възел на локалната мрежа на Интернет доставчика.
8. Данните пътуват от сървъра на Интернет доставчика към регионалната мрежа, към която той е свързан (ако използвате някой от най-големите национални доставчици, тази стъпка може и да се пропусне).
9. Ако е необходимо, данните ви пътуват през една от основните NAP точки, а от там през комерсиалния Интернет гръбнак.
10. От другата страна данните преминават през друга NAP точка, друга регионална мрежа, след което минават през Интернет доставчика на приемащата страна, който доставя данните до компютъра местоназначение (например пощенският сървър на Интернет доставчика).

11 Най-накрая данните се доставят на потребителя, когато неговият e-mail клиент се свърже с пощенския сървър на компанията или Интернет доставчика, и свали съдържанието на пощенската кутия, конфигурирана за този потребителски акаунт.

Както можете да видите, процесът е сложен и пакетите с вашите данни трябва да пътуват през множество сървъри и маршрутизатори, както и през най-различни физически преносни среди, за да достигнат до своето местоназначение. Въпреки това едно типично e-mail съобщение може да пропътува страната са минутка. Няма съмнение, че изглежда малко свръхестествено.

Сега, след като знаете *как* пакетите пътуват през тази огромна глобална мрежа от един град или една държава до друга, в следващите секции ще разгледаме някои от приложенията на тази технология. Какво *прави* Интернет и какво вие можете да направите с него? Вероятно по-важното е, след като решите *какво* искате да направите, как точно да го направите?

Какво прави Интернет

Ако трябва да обобщите целта на Интернет с една дума, тя вероятно ще бъде *комуникация*. Комуникацията може да е еднопосочна или двупосочна, за бизнес или за удоволствия, да се провежда в реално време или не. Освен това комуникацията може да приема много различни форми.

Една малка част от нещата, които даден потребител може да прави по Интернет, са:

- Да сърфира из Мрежата (World Wide Web), търсейки информация или забавление, както и да създава Web страници, които да могат да се посещават от други потребители.
- Да изпраща и да получава e-mail съобщения за частица от времето, което е необходимо на едно хартиено писмо да се достави от пощенската служба.
- Да се присъедини към пощенски списък и да обменя съобщения с хора, споделящи общи интереси, занимания, или притежаващи общи характери.
- Да участва или да стартира нюзгрупа, служеща като виртуална система за обмяна на съобщения, където заинтересованите страни могат да четат и да пускат съобщения.
- Да прехвърля файлове, като документи, графика и аудио, от някой друг компютър към своя, или от своя компютър към друг, използвайки протокола за трансфер на файлове (File Transfer Protocol – FTP).
- Да използва програма за емулация на терминал, като например Telnet, за да се свързва към отдалечен компютър с цел да стартира приложения или да прочете някакви данни на неговия харддиск.
- Да слуша радиопредавания или да гледа поточно видео.
- Да чатва в реално време с един или повече потребители на далечно разстояние.
- Да участва във виртуални съвещания, споделяйки документи и чертежи, като наред с това си комуникира посредством текст, аудио и видео.

- Да провежда телефонни разговори на далечно разстояние, без да плаща скъпи междуградски разговори на телефонната компания, като използва технология за телефония, комбинираща телекомуникациите и компютърните технологии.
- Да установява сигурна виртуална частна мрежа чрез изграждане на тунел през Интернет до частен сървър или локална мрежа (local-area network – LAN).

В следващите секции изследваме всяка от тези възможности и дискутираме приложенията и протоколите, които ги правят възможни.

Мрежата

За много хора Интернет е синоним на Мрежата (World Wide Web). Терминът *Интернет адрес* понякога се използва за описване на URL адресите на Web страниците, като например www.yahoo.com. Въпреки многото други приложения, които работят по Интернет, Мрежата *е* Интернет за голям брой мрежови потребители.

В следващите секции на тази глава дискутираме компонентите на Мрежата:

- Протокол за трансфер на хипертекст (Hypertext Transfer Protocol – HTTP)
- Език за форматиране на хипертекст (Hypertext Markup Language – HTML)
- Web услуги
- Система за имена на домейни (Domain Name System – DNS)
- Web браузъри

Също така разглеждаме какво има в Мрежата, кой я използва и как можете да навигирате из милионите страници, изграждащи Мрежата, без да се изгубите безнадеждно.

HTTP

Протоколът на Мрежата (Web) е HTTP. Както знаете, протоколът представлява набор от правила, а HTTP управлява начина, по който файловете (например текст, графика, звуци и видео) се обменят в Мрежата. HTTP е протокол от приложния слой. Стандартите за HTTP бяха разработени от групата за разработка на Интернет (Internet Engineering Task Force – IETF), а текущата версия е HTTP 1.1.

Както се подразбира от името, HTTP (протокол за трансфер на хипертекст) се използва за обмяна на *хипертекстови* файлове. Тези файлове могат да включват връзки към други файлове. Един Web сървър изпълнява HTTP услуга или *демон (daemon)*, представляващ програма, която обслужва HTTP заявките. Тези заявки се подават от HTTP клиентски софтуер – друго име за Web браузър.

Когато даден потребител въведе Web адрес или URL в адресната лента (или поле) на браузъра, или пък щракне върху хипервръзка, браузърът изпраща заявката към Web сървъра на този адрес. Web сървърът обработва заявката и връща заявения ресурс. Ресурсът може да е HTML страница, графика, звуков файл или някакъв друг тип файл.

Ако заявеният ресурс липсва на Web сървъра, или пък ако потребителят не притежава подходящите позволения за достъп до този ресурс, Web сървърът

връща съобщение за грешка. Често срещаните HTTP съобщения за грешки включват следното:

- **401/Unauthorized** – Достъпът е отказан поради хедър с неправилна авторизация.
- **403/Forbidden** – Достъпът е отказан поради неизвестни причини.
- **404/File not found** – Ресурсът липсва на този сървър.
- **500/Internal error** – Сървърът е имал проблем, който му е попречил да обработи заявката.

HTML

Web страниците се създават от *Web дизайнери*, които използват HTML, за да укажат на Web браузъра как трябва да изглежда страницата. HTML включва тагове, за да обозначава удебелени шрифтове, курсив, край на ред, край на параграф, хипервръзки, вмъкване на таблици и т.н. Пример 9-1 показва сорс код на Web страница, а Фигура 9-3 показва как тази страница се изобразява от Web браузъра Microsoft Internet Explorer.

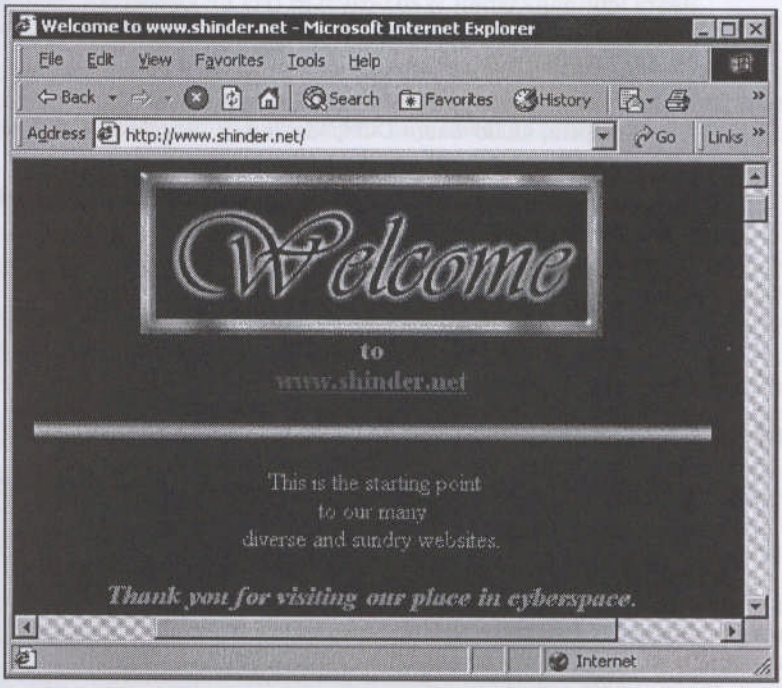
Пример 9-1 *HTML сорс кодът дефинира как трябва да се изведе на екрана дадена Web страница*

```
<html>

<head>
<meta name="GENERATOR" content="Microsoft FrontPage 4.0">
<bgsound src="picflute.mid" loop="-1">
<title>Welcome to www.shinder.net</title>
</head>

<body bgcolor="#000000" link="#C0C0C0">
<div align="center"><center>

<table border="0" width="644" height="605">
  <tr>
    <td width="13" height="601" rowspan="2"></td>
    <td width="682" valign="top" style="margin-left: 4px;
        margin-right: 4px; margin-top: 4px; padding-left: 2px;
        padding-right: 2px" colspan="3"
  height="330"><p align="center"> </p>
    <p align="center"> </p>
    <p align="center"><img src="welcomegold.jpg"
        alt="welcomegold.jpg (12428 bytes) " WIDTH="307"
        HEIGHT="108"><br>
    <big><font color="#808000"><strong>to<br>
    <a href="http://www.shinder.net">www.shinder.net</a></strong>
  </font></big></p>
    <p align="center"><img src="goldtube1.jpg" alt="goldtube1.jpg
        (2642 bytes) "
  WIDTH="450" HEIGHT="10"></p>
    <p align="center"><font color="#808000"> This is the
        starting point<br>
    to our many<br>
    diverse and sundry websites.<br>
    <br>
```

```
    <big><strong><em>Thank you for visiting our place in
        cyberspace</em>
  </strong>. </big></font></p>
    <p align="center"><strong><font face="Arial"
        color="#FFFFFF"><small>NOTE:
  These pages are designed for 800x600 resolution or
        better</small><br>
    <small>and are best viewed using Microsoft Internet Explorer 4.0
      or above.</small><br>
    <small>Click the icon to download the latest
        version.</small></font></strong>
  </p>
    <p align="center"><a href="http://www.microsoft.com/windows/
        ie/default.htm">
  <img src="Eastfield/ieget_animated1.gif" alt="ieget_animated[1].gif
  (7090 bytes) " WIDTH="88" HEIGHT="31"></a></p>
    <p align="center"> </td>
  </tr>
  <tr>
    <td width="200" valign="middle" style="margin-left: 4px;
      margin-right: 4px; margin-top: 4px; padding-left: 15px;
      padding-right: 15px" height="267">
  <p align="center"><img border="0" src="tom0400.jpg" width="206"
      height="212">
  </td>
    <td width="207" valign="middle" style="margin-left: 4px;
      margin-right: 4px; margin-top: 4px; padding-left: 2px;
      padding-right: 2px" height="267"><em>
  <font color="#408080"><strong><p align="center">
      <img src="swirl_mask.gif" alt="swirl_mask.gif (34856 bytes) "
      WIDTH="201" HEIGHT="187"></strong></font>
  </em></p>
    <p align="center"><a href="http://www.dallas.net/~shinder">
  <img src="goldframebutton.jpg" alt="goldframebutton.jpg
      (4461 bytes) " WIDTH="184" HEIGHT="65"></a></td>
    <td width="247" valign="middle" style="margin-left: 4px;
      margin-right: 4px; margin-top: 4px; padding-left: 15px;
      padding-right: 15px" height="267">
  <p align="center"><img src="family/me0399.jpg" width="209"
      height="221" alt="me0399.jpg (5916 bytes) "></td>
```

HTML сорс кодът може да бъде създаден чрез *софтуер за Web разработка* (наричан също *HTML редактор*), като например Adobe Pagemill, Macromedia Dreamweaver, Microsoft FrontPage, SoftQuad HoTMetaL Pro и Sausage Software HotDog. Много Web дизайнери предпочитат да пишат кода ръчно в прост текстов редактор (например Notepad в Windows или vi в UNIX и Linux).

Фигура 9-3 *Страницата, показана в Пример 9-1.*



Web сървъри

Веднъж създаден, сорс кодът на HTML страниците се качва на *Web сървър* – компютър, който е свързан към Интернет или интранет и на който се изпълнява софтуер за Web сървър, като например Apache (за Linux/UNIX), Internet Information Server (IIS) (за Microsoft), Domino (за Lotus) или Suitespot (за Netscape). Web сървърът *хоства* Web документите. Всички графики, звукови файлове и други вградени файлове, които се появяват в документа, също се качват на Web сървъра.

Web сървърът трябва да има връзка към Интернет и да притежава публичен IP адрес, по който да бъде идентифициран. Запомнете, че всеки сървър в Интернет има хост име, като например *www*, име на домейн от второ ниво, като например *tacteam*, и домейн от най-високо ниво, като *net*. Заедно те изграждат напълно квалифицираното име на домейн (в този пример www.tacteam.net), което служи като URL адрес на Web сайта.

Системата за имена на домейни (DNS)

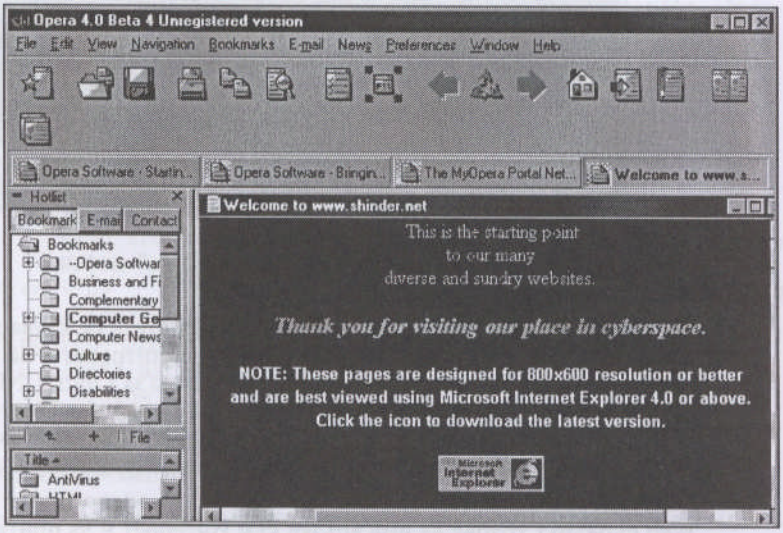
Когато един Web сърфист въведе URL адреса „www.tacteam.net“ в даден Web браузър и постави пред него „http://“ (което посочва HTTP – протоколът, използван за Web документи), заявката отива към DNS сървър, който транслира името в IP адрес. Браузърът използва IP адреса, за да открие Web сървъра в Интернет, след което изпраща съобщение, заявяващо страницата. Web сървърът връща файловете, от които е изградена заявената страница. След това страницата се извежда в браузъра на потребителя.

Web Браузъри

Двата най-популярни Web браузъра (HTTP клиентски софтуер) са Microsoft Internet Explorer и Netscape Communicator. Съществуват и много други браузъри, като например:

- **Lynx** – Текстов браузър, който може да се използва на различни платформи, включващи DOS, Macintosh, Windows, OS/2, AIX, SCO, Linux и други
- **Amaya** – Браузър, разпространяван от World Wide Web Consortium (наричан също W3C)
- **Emacs/W3** – Web браузър за UNIX, Windows, AmigaDOS, OS/2 и VMS
- **QNX Voyager** – Web браузър за операционната система QNX
- **Opera** – Малък и бърз Web браузър, работещ под Windows, Linux и BeOS (вижте Фигура 9-4)

Фигура 9-4 *Opera е малък и бърз Web браузър, наличен за няколко платформи.*



Някои Web браузъри са *freeware* (т.е. не струват пари) или *shareware* (т.е. можете да ги пробвате, преди да ги купите) и са налични за сваляне от Мрежата. Онлайн услугите могат да ползват собствени браузъри, а Интернет доставчиците често настройват версиите на Internet Explorer или Netscape, които те дистрибутират на своите клиенти.

Какво има в Мрежата?

От прости текстови документи до анимирани мултимедийни представления на базата на Java или ActiveX – в Мрежата има всичко. Да се каже просто, че Мрежата е увеличила нашите възможности да събираме информация бързо и лесно, би било доста сдържано. Да имате достъп до Мрежата е като да прелиствате цялата Библиотека на Конгреса, че дори и повече.

Мрежата измина доста път от нейното скромно начало. Терминът хипертекст за пръв път беше лансиран от Тед Нелсън, който го включи като част от неговия софтуерен проект, наречен Xanadu. Тим Бърнърс-Лий (често наричан бащата на Интернет) се счита за визионера, използвал тази интерактивна технология, за да създаде глобалната Мрежа (World Wide Web). Бърнърс-Лий все още е активен член на World Wide Web Consortium – международна организация, която подпомага разработването на стандарти за Web технологии.

Кой използва Мрежата?

С тези темпове на разрастване изглежда сякаш почти всеки се е включил в Мрежата. Притежаването на Web присъствие се превръща почти в задължително за много типове бизнеси. Личните и семейните домашни страници са масово разпространени. Дори тези, които не притежават собствени страници, са заети да сърфират и да проучват предложенията на другите.

Мрежата на националната научна фондация (National Science Foundation Network – NSFNET) пазеше статистическа информация за типовете трафик, преминаващи през гръбнака, но това беше до 1995 година – времето, когато NSF спря да управлява гръбнака и той бе поет от комерсиални интереси. Според техните данни, през юни 1993 година Мрежата е заемала само 0,5 процента от Интернет трафика. До март 1995 година тази цифра вече е скочила на 23,9 процента. Според проучване на NUA – международно призната компания за консултации в областта на Интернет – през април 2000 година приблизително 52 процента от домовете в САЩ са имали достъп до Мрежата. Според моите източници, броят на публикуваните в Мрежата страници грубо казано се удвоява всяка година. Освен това през януари 2000 година се смяташе, че в Мрежата са се съдържали приблизително 2 милиарда страници и над 450 милиона изображения. Тези цифри, разбира се, са динамични – стотици хиляди Web страници се добавят всеки ден, а други се премахват или променят.

Цента на персоналните компютри падна значително и Интернет услугата стана достъпна от финансова гледна точка. Някои компании дори предоставят такава услуга безплатно; тя се издържа от реклами. Това ще рече, че непрекъснато все повече хора се включват в „голямото семейство“. Училищата изграждат компютърни зали с постоянна връзка към Интернет, а компютърната грамотност става задължителен предмет. Кибер-кафетата, където потребителите могат да сърфират срещу заплащане също са в разцвета си.

Тези които имат Интернет достъп, използват Мрежата за най-различни цели, а много от тях я използват ежедневно. Потребителите използват Мрежата, за да научат повече за дадени продукти и евентуално да си ги купят. Учениците и студентите я използват за откриване на документи. Педагозите я използват за разпространяване на учебни материали. Пътешествениците я използват за резервиране на полети и хотелски стаи, както и за помагало при избор на ваканционни дестинации. Пациентите я използват, за да научат повече относно техните здравословни състояния и лечения. Бизнесмените я използват, за да се информират относно развитието в бранша и конкуренцията, както и за да рекламират свои собствени стоки и услуги.

Мрежата се превръща в технология, която променя нашето общество и нашия начин на живот по същия начин, както това са направили електричеството, телевизията и телефонът. Всъщност въпросът не е „Кой използва Мрежата?“, а „Кой *не* я използва?“.

Намиране на това, което ви интересува

Невероятното количество информация, достъпно за обществото в Мрежата, е както най-голямата ѝ сила, така и най-голямата ѝ слабост. Откриването на всички уместни данни относно дадена тема – и *само* данните, които в действителност са уместни – може да бъде обезкуражаваща задача.

В следващите секции разглеждаме как машините за търсене, машините за метатърсене и порталите могат да ви помогнат да навигирате из огромното количество данни в Мрежата.

Машини за търсене

Бяха разработени стотици *машини за търсене (search engines)* в опит навигацията в Мрежата да стане по-лесна. Машините за търсене са сайтове, съдържащи интерактивни бази данни, които категоризират Web сайтове обикновено с помощта на *метатагове (metatags)*. Метатагът е ключова дума, създадена от дизайнерите в HTML кода. Според www.wwwmetrics.com – един сайт, посветен на Web статистика – 85 процента от потребителите използват машини за търсене, но по-малко от 20 процента от обществената Мрежа е индексирана от тези машини.

Yahoo (www.yahoo.com) беше първата основна машина за търсене и днес все още се използва от много хора. Други популярни машини за търсене са следните:

- **Lycos** – www.lycos.com
- **DirectHit** – www.directhit.com
- **Excite** – www.excite.com
- **AltaVista** – www.altavista.com
- **Northern Light** – www.northernlight.com
- **Google** – www.google.com

Повечето машини за търсене работят, като индексират ключовите думи или метатаговете, разположени в HTML сорс кода от дизайнера на Web страницата. Тези термини представляват термини, които даден човек е най-вероятно да използва, търсейки документи, които са свързани с темата на Web страниците. Например, ако сте проектирали Web страница, в която се говори за вашия бизнес с отглеждане на сиамски котки, бихте могли да сложите следните ключови думи в HTML кода под формата на метатагове: котка, сиамска и отглеждане.

Машините за търсене имат три основни компонента:

- ***Паякът (spider)*** – Програма, която преминава от една връзка към друга в Мрежата, събирайки индексираща информация
- ***Индексът (index)*** – База данни, която съхранява копие на всяка Web страница, събрана от паяка
- **Механизмът за *търсене/извличане* (*search/retrieval* mechanism)** – Интерфейс, който позволява на потребителите да въвеждат своите заявки и да получават резултатите

Някои машини за търсене могат в действителност да претърсят целия текст на всеки документ, вместо само ключовите думи. Резултатът от това е много повече *попадения (hits)* (страница, която съответства на критерия за търсене), но

пък може да доведе и до много съответствия, които не са свързани с темата. Например, ако се нуждаете от информация относно рецепти за десерти и въведете думата „десерт“, ще получите списък от страници, съдържащи думата „десерт“ където и да е в текста. По този начин в списъка с намерените страници ще се появи и такава, в която се споменава за „десерта на екскурзията“ например.

Важно е да четете инструкциите за използване на дадена машина за търсене. Някои позволяват булево (Boolean) търсене, работещо с аргументи, които използват AND, OR или NOT. В предходния пример търсенето може да се стесни чрез въвеждане на „десерт AND рецепта“ в полето за търсене.

ЗАБЕЛЕЖКА Повечето машини за търсене не могат да индексират съдържанието на Web сайтовете, защитени с парола. Също така имайте предвид, че отнема известно време документите да се индексират, след като се качат на даден Web сървър, така че машините за търсене често не съдържат документи, публикувани наскоро.

Машини за метатърсене

Машините за *метатърсене (metasearch)*, като изброените по-долу, компилират резултатите от няколко машини:

- **MetaCrawler** – www.metacrawler.com
- **SavvySearch** – www.savvysearch.com
- **Ask Jeeves** – www.askjeeves.com

Една машина за метатърсене (понякога наричана и *мета машина)* не поддържат свой собствен индекс. Тя използва индексите на други машини, като претърсва множество бази данни едновременно, след което събира резултатите в един изчерпателен списък. По-съвършените мета машини могат да откриват и да премахват дублиращи се резултати.

Web портали

Много машини за търсене служат и като Web *портали*. Порталът е Web сайт, успял да се превърне в „стартова страница“ за потребителите – точка, в която те често се връщат за връзки, новини, Web поща, карти, телефонни указатели и обществени форуми. Потребителите могат да настройват свои персонализирани стартови страници, които да отразяват техните интереси. Например можете да изберете порталната страница да показва местните новини и времето във вашия район. Освен това можете да изберете специални теми, като спорт, бизнес, технологии и забавление, за които се извеждат текущи новини, когато осъществите достъп до страницата.

Онлайн услугите (като AOL и MSN) и доставчиците на Интернет, често осигуряват портали са своите потребители.

Други Web услуги

Освен текстово-графичните страници с връзки към други страници, Мрежата предлага и далеч по-развити услуги като следните:

- Анимации
- Чат в реално време
- Записано видео и видео на живо (използващо Web камери и RealVideo)
- Записани радиопредавания и такива на живо (използващи RealAudio)
- Игри с виртуална реалност (VRML)
- 3-D „разходки“ и панорами
- Сайтове за електронна търговия (т.е. интерактивно пазаруване)
- Web-базирани e-mail услуги

Много услуги (например тези, позволяващи ви да изпращате e-mail съобщения, да четете статии в нюзгрупи, да чатвате и да прехвърляте файлове), които по едно време изискваха отделни приложения, сега са вградени като функции в Web браузърите.

Електронна поща и пощенски списъци

Електронната поща (e-mail) е една от най-използваните услуги в Интернет. Според някои източници, на година през Интернет и онлайн услугите преминават над 6 милиарда e-mail съобщения.

В следващите секции разглеждаме преимуществата и недостатъците на електронната поща, сравнени с други форми на комуникация, изследваме как работи сървърният и клиентският e-mail софтуер, и дискутираме употребата на пощенските списъци, представляващи списъци за масово разпространение на e-mail съобщения.

Преимуществата на електронната поща

Електронната поща има много преимущества пред другите форми на комуникация. Тя комбинира много от предимствата на традиционната „хартиена поща“ (т.е. обикновените пощенски писма в пликове) с предимствата на телекомуникациите, успявайки да избегне някои от недостатъците и на двете.

Подобно на телефонните разговори, e-mail комуникациите могат да са бързи и неформални. Подобно на пощенските писма, e-mail съобщенията могат да се четат през свободното време на получателя, а могат и да се разпечатват на принтер, така че текстът да изглежда като от истинско писмо. При всички положения електронната поща е взела най-доброто и от двата типа комуникации.

E-mail съобщенията не е необходимо да са в чист текст. Модерните e-mail клиентски програми ви позволяват да прикрепяте файлове (като например текстови документи, картинки, аудио и видео файлове) и да форматирате текста със специални шрифтове, цветове и фонове.

Електронната поща също така е значително по-евтина от стандартната поща, особено що се отнася до много големи документи. По-евтина е и от междуградските и международните телефонни разговори. Електронната поща дава начин на приятелите и познатите да държат връзка, компаниите могат да водят бизнес кореспонденция по удобен и евтин начин, а рекламодателите имат възможност да разпространяват рекламни съобщения с минимални разходи. (Всъщност последната изгода от електронната поща се явява един от нейните крайно нежелани *недостатъци*, както е дискутирано по-долу.)

Недостатъци на електронната поща

Спамът, или нежеланата комерсиална електронна поща, е непрекъснато растящ проблем за потребителите и доставчиците на Интернет. В момента много организации правят опити да обуздаят потока от масово разпращани съобщения. Много съвременни e-mail програми притежават вградени филтри за „боклучава поща", които маркират подозрителните съобщения, местят ги в отделна папка, а понякога дори ги изтриват автоматично още при самото им пристигане.

Електронната поща споделя един недостатък с всички писмени комуникации: възможността за погрешна интерпретация. Проучванията показват, че човешките същества са много зависими от визуалните жестове и интонацията, когато интерпретират значенията на изговорените от някого думи. Езикът на тялото, изражението на лицето и измененията в интонацията показват дали говорещият Body language, facial expression, and changes in vocal pitch tell us whether the speaker е искрен, саркастичен, шеговит, ядосан и т.н. Електронната поща и другите писмени комуникации често пъти ни карат да бъдем несигурни относно намерението на подателя. За облекчаването на този проблем потребителите масово започнаха да използват така наречените *емоционални икони (emoticons)* (наречени също *смайлита*[1] *[smileys]*, въпреки че се обхваща широк набор от емоции), представляващи усмивки, цветя и други мимики и жестове.

Тъй като са неформални, e-mail съобщенията понякога се изпращат импулсивно, защото малко хора обмислят написаното, преди да го изпратят. Това доведе до репутация на електронната поща като неучтив начин на комуникация в някои кръгове. *Войните с обиди (flame wars)* (т.е. взаимните персонални атаки, често ескалиращи до вулгаризми) са често срещани в Интернет.

Накрая, въпросът с неприкосновеността е проблем при електронната поща, а законите в много юрисдикции относно e-mail съобщенията все още са колеблив. По принцип e-mail съобщенията могат да бъдат прихващани във всяка точка по пътя им между изпращача и получателя. (Съществуват и методи за криптиране, които ще бъдат дискутирани в Глава 14, „Защита на мрежата".) Въпреки това на e-mail потребителите се препоръчва да третират всичко, изпратено по Интернет, като пощенска картичка (която може да бъде прочетена от всеки), а не като запечатан плик с лично писмо.

E-mail софтуер

Фразата „e-mail софтуер" може да значи едно от следните две неща: e-mail сървърен софтуер или e-mail клиентски софтуер. И двата вида са дискутирани в следващите секции.

E-mail сървъри и протоколи за Интернет поща

E-mail сървърите използват базирани на стандарти протоколи, като простия протокол за трансфер на поща (Simple Mail Transfer Protocol – SMTP), пощенския протокол (Post Office Protocol – POP), чиято последна трета версия [POP3] е текущата му реализация, и протокола за достъп до Интернет съобщения (Internet Message Access Protocol – IMAP), чиято последна версия е 4 (IMAP4).

---

[1] Усмивки (от англ. smile – усмивка) – б.р.

ЗАБЕЛЕЖКА SMTP се използва за прехвърляне на поща от една точка до друга през Интернет. POP и IMAP се използват за четене и обработка на пристигащи e-mail съобщения, след като те са били доставени на вашия пощенски сървър.

SMTP сървърът обикновено се използва за изпращане на e-mail. Когато създавате и изпращате съобщение във вашия e-mail клиентски софтуер, то отива на SMTP сървъра на вашия Интернет доставчик, който сървър след това го изпраща по Интернет, използвайки TCP/IP стандарта – SMTP.

Sendmail е популярна UNIX SMTP сървърна програма. Ако сте свързани към локалната мрежа на даден компания, тя може да поддържа свои собствени вътрешни e-mail сървъри (например Exchange Server). В такъв случай съобщенията минават през локалния пощенски сървър, който препраща вътрешната поща до коректния получател и препраща пощата към Интернет доставчика, ако адресът е извън компанията.

POP сървърите получават e-mail съобщения, адресирани до специфично име на акаунт (като например deb@shinder.net), и ги съхраняват в папка, наречена *mailbox*. Когато POP3 пощенският клиент на локалния компютър се свърже със сървъра, пощата се сваля на локалния харддиск. Обикновено тя се изтрива от сървъра по същото време (въпреки че можете да конфигурирате вашия пощенски клиент да оставя копие на всяко съобщение на сървъра).

IMAP сървърите също получават поща, но те са по-сложни от POP сървърите. При тях един пощенски клиент може да разгледа хедърите на съобщенията и да избере кои от тях да свали. Имате възможност да изтриете съобщенията на сървъра даже без въобще да ги сваляте на вашата локална машина.

Примери за популярни пощенски сървъри са Microsoft Exchange, Netscape Messaging Server, Post Office, Sendmail, SLmail, IMail и MDaemon.

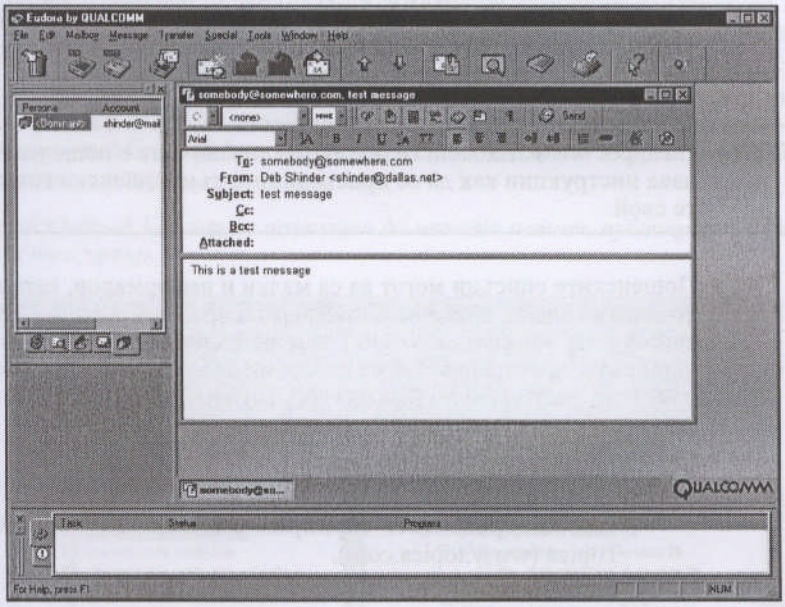
E-mail клиенти

E-mail клиентският софтуер е приложение, което ви позволява да пишете и да четете e-mail съобщения. То трябва да бъде конфигурирано да се свързва към пощенски сървър. Някои измежду многото приложения за e-mail клиенти включват следните:

- Eudora
- Pegasus
- Microsoft Outlook Express
- Netscape Mail

Съществуват и програми за персонално планиране и съвместна дейност, като Microsoft Outlook 2000 и Lotus Notes, които комбинират e-mail с други функции – планове и графици, списъци със задачи и бази данни с договори. Фигура 9-5 показва пример на един от популярните e-mail клиенти – Eudora.

Фигура 9-5 *Eudora е популярна програма за e-mail клиент и може да се свали от www.qualcomm.com.*



ЗАБЕЛЕЖКА Не е задължително винаги да имате инсталиран e-mail клиентски софтуер, за да изпращате и да четете e-mail съобщения. Съществуват множество Web-базирани e-mail сайтове. Те ви позволяват да пишете, изпращате и получавате електронна поща, като използвате вашия Web браузър. В много случаи Web-базираните e-mail акаунти са безплатни, въпреки че трябва да има начин да се свържете с Мрежата, за да ги използвате.

Повечето съвременни e-mail клиенти ви позволяват да организирате получената поща в папки. Някои ви дават възможност да установите правила или филтри, които автоматично да сортират пощата при пристигането ѝ. Много от тях позволяват да изпращате и получавате e-mail съобщения, които са форматирани в HTML, така че едно e-mail съобщение може да използва някои или всички елементи на една Web страница (вградени графики, звук, фонове и дори скриптове).

Пощенски списъци

Списъците за електронна дискусия са популярно приложение на електронната поща по Интернет. Не ги бъркайте с масовото изпращане на нежелани съобщения; пощенските списъци се доставят на множество адреси, но за да получите съобщение от списък, трябва да се абонирате за него. В някои случаи притежателят на списъка или модераторът трябва да одобри вашата заявка за членство, защото за много от списъците има дефинирани критерии за членство.

Съществуват пощенски списъци, посветени на почти всякаква тема, за която можете да се сетите. Има многобройни професионални списъци. Чрез тези спи-

съци, големи групи от доктори, адвокати, писатели, компютърни инженери и т.н. могат да дискутират въпроси от тяхната област. Съществуват също списъци за колекционери, играчи на шах, играчи на видеоигри, фотографи аматьори и собственици на домашни любимци. Дори съществуват списъци, посветени на книги, спортове, развлечения, телевизионни шоута и софтуерни програми – темите могат да се изброяват почти до безкрай.

ЗАБЕЛЕЖКА На адрес www.liszt.com се поддържа справочник с пощенските списъци. Той дава инструкции как да се присъедините към пощенски списък или да започнете свой.

Пощенските списъци могат да са малки и неформални, като пощата се разпространява ръчно до група от e-mail адреси чрез използване на функцията cc (т.е. carbon copy – нормално копие) на e-mail клиентския софтуер. По-големите списъци се разпространяват чрез програми за автоматизирани пощенски списъци, наречени лист-сървъри (list servers), като например следните:

- **Majordomo** – Често работи под UNIX сървъри.
- **ListServ** – Създадена от L-Soft и работи под Windows NT.
- **Web-базирани лист-сървъри** – Включват Egroups (www.egroups.com) и Topica (www.topica.com).

Нюзгрупи

Нюзгрупите наподобяват пощенските списъци по това, че обикновено са организирани около специфични интереси или теми. Най-голямата разлика е, че след като веднъж се присъедините към пощенски списък (обикновено чрез изпращане на e-mail на специфичен „абонаментен" адрес), всички публикувани съобщения се изпращат до посочения от вас e-mail адрес. За да спрете пристигането на съобщения, трябва да се отпишете (отабонирате) от списъка.

В повечето случаи не се изисква да се присъединявате към нюзгрупа (въпреки че съществуват ограничени нюзгрупи, до които достъпът се осигурява срещу потребителско име и парола); необходимо е само да конфигурирате вашия софтуер за четене на нюзгрупи (като Outlook Express, Netscape News или Free Agent), за да се свържете с конкретен нюзсървър. След това можете да разглеждате всички публикувани съобщения, да ги четете и самите вие да пускате съобщения.

Ако решите, че не искате повече да четете нюзгрупата, просто не се свързвате с нея. Вашата e-mail кутия не се наводнява от допълнителни съобщения, което е възможно при обемните пощенски списъци.

Мрежов протокол за предаване на новини

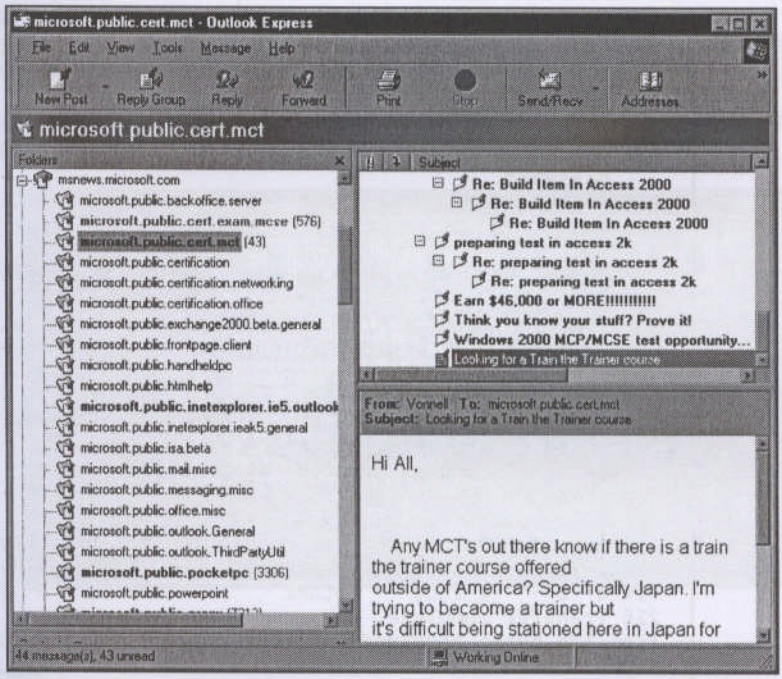
Протоколът, използван от повечето нюзсървъри и програми за четене на новини, както и за управляване на нюзгрупи, се нарича мрежов протокол за предаване на новини (Network News Transfer Protocol – NNTP). NNTP първоначално се наричаше *Usenet* и използваше протокола UNIX-to-UNIX Copy Protocol (UUCP). NNTP беше заменен от UUCP като стандарт за разпространение на новини. NNTP е протокол от приложния слой.

Софтуер за нюзгрупи

Както при електронната поща, нюзгрупите изискват два типа софтуер: софтуер за *нюзсървър*, работещ на машината, която хоства нюзгрупата, и софтуер за *нюзклиент*, наречен също *нюзридър* (четец на новини). (Фигура 9-6 показва нюзридър.)

Софтуерът за нюзсървър често пъти се включва с програмите за Web сървъри като Microsoft IIS. Някои e-mail програми и Web браузъри, като Netscape Communicator, Microsoft Internet Explorer/Outlook Express и Opera, притежават вградени нюзридъри.

Фигура 9-6 *Microsoft Outlook Express ви позволява да четете новини, публикувани в нюзгрупа на нюзсървър.*



Нюзсървърът, показан на Фигура 9-6, се нарича msnews.microsoft.com. (Можете да видите името в левия панел.) Списъкът с нюзгрупите на сървъра, към който се е абонирал потребителят, се показва под името на сървъра. В горния десен панел се намира списък със съобщения, публикувани в избраната нюзгрупа, в случая microsoft.public.cert.mct. Избраното съобщение е показано в долния десен панел.

Трансфер на файлове

FTP ви позволява да качвате файлове от вашия компютър на отдалечена машина и да сваляте файлове от отдалечена система на вашия харддиск.

FTP се използва за много цели, като качване на Web страници от локален компютър на отдалечен Web сървър, и сваляне на драйвери от FTP сървъра на производителя на даден хардуер.

В повечето операционни системи наред в TCP/IP стека е включен и FTP клиентски софтуер, работещ от командния ред. Множество FTP клиентски програми на трети страни предлагат лесен за използване графичен потребителски интерфейс. Последните версии на популярните Web браузъри, като Internet Explorer, Netscape и Opera, включват FTP функционалност.

Пример 9-2 показва FTP интерфейс от командния ред, в който е установена връзка с FTP сървъра на Xerox чрез използване на програмата FTP. Командата има следния синтаксис:

```
ftp
open име_на_ftp_сървър
```

Пример 9-2 *Използвате FTP клиент от командния ред, за да се свържете с FTP сървър*

```
G:\>ftp
ftp> open ftp.xerox.com
Connected to ftp.xerox.com.
220 FTP.XEROX.COM
User (ftp.xerox.com:(none)): anonymous
331 Anonymous login ok, send your complete e-mail address as
    password.
Password:
230-

 WELCOME TO THE DOCUMENT COMPANY - XEROX FTP SERVER.

 Information about your login and any transfers you do are logged on
 this server.  If you do not wish to be logged, please disconnect
 now.

 Any comments, questions, etc. regarding this archive should be
 directed to webmaster@xerox.com.
230 Anonymous access granted, restrictions apply.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
drwxr-xr-x 138 xerox    grpXerox     3072 Aug  3 04:55 pub
-rw-r--r--   1 root     other         293 Dec  3  1999 welcome.msg
226 Transfer complete.
ftp: 128 bytes received in 1.48Seconds 0.09Kbytes/sec.
ftp>
```

Първият ред в Пример 9-2 стартира FTP клиентския софтуер. Вторият ред отваря връзката с посочения FTP сървър (в този случай, ftp.xerox.com).

Много FTP сървъри позволяват анонимни логвания, но изискват от вас като парола да използвате вашия e-mail адрес. Когато логването приключи, командата **dir** дава списък с наличните директории, до които можете да осъществите достъп. Командата **get** сваля файл, а командата **put** качва файл на сървъра.

Популярните графични самостоятелни FTP клиенти включват WSFTP, CuteFTP и FTP Voyager. Можете да свалите тях, както и други FTP приложения, от Мрежата. някои са безплатни (като „леките" версии на WSFTP), но повечето са shareware.

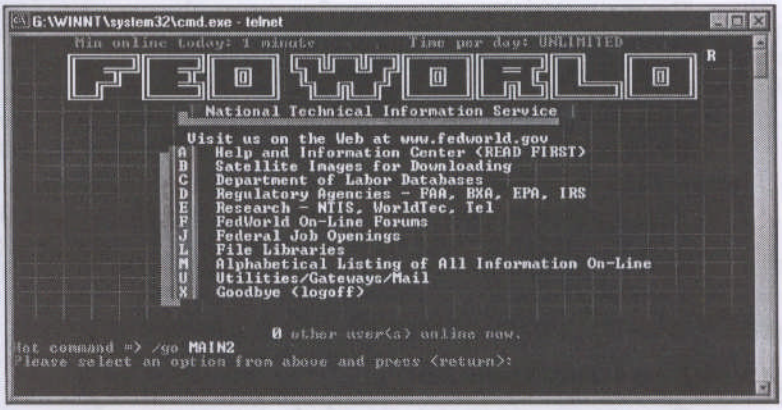
Telnet

Софтуерът за терминална емулация позволява на едно PC да изглежда и да функционира като „прост терминал" за друг компютър (обикновено мейнфрейм). След това потребителите могат да осъществяват достъп до програми на хост компютъра. Telnet е клиент за терминална емулация, използващ протокола Telnet, и се включва към повечето реализации на TCP/IP.

Протоколът Telnet позволява на един компютър, на който се изпълнява Telnet клиентски софтуер, да се свързва с Telnet сървър и да си взаимодейства с него от разстояние през терминален прозорец. Telnet не позволява прехвърляне на файлове от една машина на друга; той обаче позволява на потребителя да стартира програми или да преглежда файлове на сървъра.

Фигура 9-7 показва Telnet сесия, използваща Telnet клиента, който е включен в Windows 2000. В този пример е установена отдалечена сесия с Fedworld, Националната услуга за техническа информация (National Technical Information Service) на правителството на САЩ.

Фигура 9-7 *Telnet е протокол от приложния слой на TCP/IP и се използва за връзка с отдалечени сървъри.*



Поточна медия

С популяризирането и поевтиняването на висикоскоростните Интернет връзки и използването на съвременни технологии като ISDN, T-1, кабелен модем и DSL, стана възможно да се предават аудио и видео сигнали в непрекъснат поток. Това означава, че вместо да се налага да свалите цял файл, за го чуете или видите, може те да използвате постоянна връзка и да получите данните бит по бит.

За да гледате поточна медия без дразнещи паузи в аудиото и насечени движения във видеото, ви трябва не само бърза връзка, но и компютър с достатъчно памет и процесорна мощ, който да се справи с потока от данни. Падането на цените на PC-тата и Macintosh системите от висок клас съдействат за нарастващата популярност на поточната медия.

За достъп до поточна музика и видео клипове, както и за тяхното възпроизвеждане, се използват приложения като QuickTime на Apple, Real Audio/Real Video и Windows Media Player.

Чат на живо

Комуникирането в реално време е възможно през Интернет – за целта обикновено се използва системата IRC (Internet Relay Chat), Web чат или някоя от програмите за „моментални съобщения“, както е описано в следващите секции.

IRC и Web-базирани чат стаи

IRC осигурява среда, в която IRC клиентите се свързват към IRC сървър и участват в текстово-базирани „разговори“ в реално време. IRC сървърите хостват „канали“, или отделни форуми, обикновено посветени на специфични теми или общи интереси. Популярните IRC клиентски приложения включват mIRC (една от най-известните shareware IRC програми), Visual IRC и PIRCH (включва видео в реално време).

Web-базираните чат стаи са Web сайтове, използващи Java или други скриптови езици, за да осигурят форум, в който Web сърфистите могат да влизат в „чат общества“ и да изпращат текстови съобщения в реално време един на друг.

Моментални съобщения

Програмите за моментални съобщения ви позволяват да изпращате директни съобщения до други хора, които са онлайн и които имат инсталиран подходящ софтуер. В повечето случи на екрана на приемника изскача диалогов прозорец и в него се появява написаното от вас съобщение. Някои услуги за съобщения включват „гласов чат“ или възможности за двупосочно видео. (Тези възможности са подобни на инструментите за аудио конференции, дискутирани в следващата секция на тази глава.)

Популярните приложения за моментални съобщения включват Mirabilis ICQ („I seek you“ – „аз търся теб“), AOL/ Netscape Instant Messenger, Microsoft MSN Messenger, Yahoo Messenger, Tribal Voice PowWow и Elf Communications WinTalk.

Аудио/видео конференции

Технологиите за аудио/видео конференции ви позволяват да проведете среща с хора, намиращи се на далечни разстояния. Популярността на тези технологии нараства сред бизнес средите; те се използват и в образователните кръгове за създаване на „виртуални класни стаи“ за онлайн обучение.

В зависимост от използвания софтуер може да сте в състояние да показвате документи по време на конференцията, които да се виждат от всички участници на техните екрани. Също така е възможно да чертаете по виртуална бяла дъска и всички участници да виждат на мониторите си начертаното от вас.

Всеки участник в конференция трябва да стартира софтуера за конференции, както и да притежава звукова карта, микрофон и цифрова камера, които да са свързани към PC-то. Популярните програми за видео конференции включват CUseeMe (преди това White Pine Software) и Microsoft NetMeeting.

За видео конфериране бяха разработени специални стандарти – H.323 представлява стандарта ITU (International Telecommunications Union – Международен съюз за телекомуникации), управляващ различни мултимедийни комуникации по IP и IPX, които не осигуряват QoS. Приложенията за конференции, които са съвместими с H.323, би трябвало да се сработват едно с друго.

Софтуерът за видео конференции може да се раздели на две категории:

- **От точка до точка (point-to-point)** – Директна връзка между две машини, работеща подобно на видео телефон
- **Многоточков (multipoint)** – Софтуер, чрез който едновременно могат да комуникират повече от двама участника

Международният консорциум за мултимедийни телеконференции (International Multimedia Teleconferencing Consortium – IMTC) разработва стандарти, спонсорира събития и осигурява информация. Той е отворена за членство организация с идеална цел. Web сайтът на IMTC се намира на адрес www.imtc.org.

Интернет телефония

Приложенията за Интернет телефония ви позволяват да провеждате междуградски и международни телефонни разговори чрез използване на технологията *Voice over IP (глас по IP)*, без да плащате такси на телефонната компания за проведените разговори. Ранните приложения за телефония бяха с лошо качество, като и инициаторът, и приемникът на разговора трябваше да използват един и същ софтуер за телефония.

По-новите технологии ви позволяват да използвате шлюзови Интернет сървъри, за да се обадите на нормален телефонен номер. Човекът от приемащата страна дори не е задължително да притежава компютър или връзка към Интернет.

Извършването на телефонен разговор става по следния начин:

1. Обаждащият се набира IP адреса на шлюзовия Интернет сървър.
2. Разговорът се маршрутизира през Интернет до шлюзовия сървър.
3. Шлюзовият сървър маршрутизира разговора към PBX централа в града, в който се намира набраният номер.
4. Разговорът се прехвърля към изходяща линия, за да се осъществи връзка с телефонния номер на приемника.
5. Разговорът се счита от телефонната компания като местен, защото се инициира в PBX централата на същия град.

ЗАБЕЛЕЖКА Можете да използвате Интернет телефонията за изпращане и на факсове.

Някои популярни приложения за телефония включват Internet Phone (за Windows), Webphone (за Windows), NetPhone (за Macintosh), Cyberphone (за UNIX и Windows), PGPhone (за Windows и Macintosh) и Speak Freely (за UNIX и Windows).

Повечето приложения за телефония използват частна технология, а потребителите могат да комуникират само с други потребители, които са си инсталирали софтуер от същия производител. Приложенията, налични за повече платформи, по принцип се водят за междуплатформени. Например един потребител на PGPhone с Macintosh компютър може да комуникира с потребител на PGPhone с Windows компютър.

Виртуални частни мрежи

Един вълнуващ начин за използване на Интернет са *виртуалните частни мрежи (virtual private networks – VPN)*, чиято популярност непрекъснато се увеличава, защото те спестяват пари на компаниите. VPN технологията използва Интернет като канал, през който може да се установи сигурна връзка между отдалечен клиент и частна локална мрежа (LAN), без да се плаща за междуградски или международни разговори, в случай че се наложи сървърът на локалната мрежа да се набира директно.

Дискутираме VPN мрежите подробно в Глава 16, „Виртуални частни мрежи".

TCP/IP маршрутизиране и Интернет

Интернет приложенията, които дискутирахме в тази глава, се осланят на TCP/IP протоколите, свързващи различните операционни системи и платформи в Интернет. В Глава 8 научихте за компонентите на TCP/IP протоколния пакет и как те работят в една LAN среда. В тази секция се фокусираме на това, как TCP/IP работи в глобалната WAN мрежа.

Способността за маршрутизиране (routability) е аспект на TCP/IP, който е съществено важен за междумрежовите комуникации и комуникациите в Интернет. *Маршрутизиране (routing)* означава препращане на пакети от една мрежа (или подмрежа) към друга. Колкото и просто да е като концепция, IP маршрутизирането е всичко друго, но не и просто, когато нещата опрат до реализацията. Някои маршрутизиращи протоколи или специфични области, като конфигурирането на един маршрутизатор, изискват обяснения, които могат да запълнят страниците на цяла книга. Тази глава обяснява само най-основните концепции на маршрутизирането; за по-изчерпателни източници на информация вижте списъка с ресурси в края на тази глава.

Как работи IP маршрутизирането

В Глава 8 научихте, че съществуват няколко причини за разделянето на една голяма TCP/IP мрежа на подмрежи. Една от причините е, че подмрежите драстично намаляват бродкастния трафик, позволявайки бродкастните съобщения да достигат само до онези компютри, намиращи се в същата подмрежа, в която се намира и подателят. Това повишава ефективността на мрежата.

Как съобщенията, адресирани до компютър в различна подмрежа, достигат своето местоназначение? Това става чрез процес, наречен *IP препращане (IP forwarding)*.

ЗАБЕЛЕЖКА Както знаете IPX/SPX е маршрутизируем протоколен стек точно както TCP/IP. Повечето маршрутизатори поддържат както IP, така и IPX препращане.

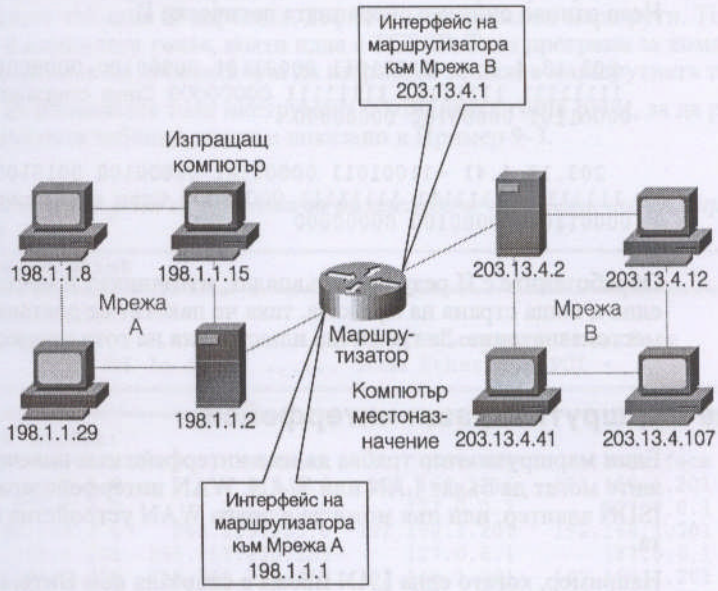
IP се занимава с логическото адресиране и маршрутизиране на пакети. Когато се изпрати пакет, IP гледа IP адреса на източника и този местоназначението, както и подмрежовата маска, след което извършва изчисление с оператора AND (И) (дискутирано в Глава 8). Това определя дали компютърът местоназначение се намира в същата подмрежа или в друга. В случай че той се намира в същата подмрежа, пакетът се доставя до него. Ако този компютър е в различна подмрежа, IP изпраща пакета до *подразбиращия се шлюз (default gateway)*.

Подразбиращият се шлюз е IP адресът на маршрутизатор, свързан към локалната мрежа и поне към още една мрежа. Маршрутизаторът се консултира със своята маршрутна таблица, за да определи най-добрият път, по който да достигне отправната мрежа. Пакетът може да пътува през много маршрутизатори, за да достигне до мрежата, в която се намира компютърът местоназначение. Когато пакетът достигне до мрежата, IP използва хост частта на IP адреса, за да достави пакета на правилния компютър в мрежата.

Пример за проста маршрутизирана мрежа

Нека погледнем една проста маршрутизирана мрежа. Идентификаторът на Мрежа А е 198.1.1.0. Идентификаторът на Мрежа В е 203.13.4.0. И двете са от Клас С без подмрежи, а връзката между тях се осъществява през *групов (multi-homed)* компютър (т.е. компютър с два мрежови интерфейса), работещ под Windows NT. IP препращането на NT компютъра е разрешено (в свойствата на TCP/IP), което му позволява да функционира като маршрутизатор, както е показано на Фигура 9-8.

Фигура 9-8 *Един пакет се маршрутизира от компютър в Мрежа А до компютър в Мрежа В.*



Един маршрутизатор (независимо дали е специализирано устройство или компютър, действащ като маршрутизатор) трябва да принадлежи поне на две мрежи. Това означава, че IP адресите, назначени на неговите две мрежови карти, са в различни мрежи или подмрежи. В нашия пример едната мрежова карта е конфигурирана като 198.1.1.1, а втората е конфигурирана като 203.13.4.1.

ЗАБЕЛЕЖКА Обичайна практика е първият IP адрес на мрежата да се назначава на маршрутизатора. Това не се изисква; по-скоро това е начин за лесно идентифициране на адреса на маршрутизатора в мрежата.

Ако компютър от първата мрежа, с IP адрес 198.1.1.15, изпрати пакет, адресиран до 203.13.4.41, IP изследва хедъра, за да определи IP адресите и подмрежовите маски. Подмрежовата маска за всеки от тях е 255.255.255.0, защото те са в мрежи от Клас С без подмрежи.

Следва операцията логическо И:

```
 198.1.1.15 =   1000110 00000001 00000001 00001111255.255.255.0 =
11111111 11111111 11111111 00000000        След операцията И
11000110 00000001 00000001 00000000

 203.13.4.41 =11001011 00001101 00000100 00101001255.255.255.0 =
11111111 11111111 11111111 00000000 След операцията И  11001011
00001101 00000100 00000000
```

Както можете да видите, обработените с И резултати са различни; ето защо IP заключава, че хостът източник и хостът местоназначение се намират в различни мрежи. Пакетът се изпраща на 198.1.1.1, подразбиращият се шлюз за първата мрежа.

След това пакетът се предава през шлюза към втората мрежа. Сега адресът източник става IP адресът от тази страна на маршрутизатора, т.е. 203.13.4.1.

Нека отново опитаме операцията логическо И:

```
 203.13.4.1 =  11001011 00001101 00000100 00000001255.255.255.0 =
11111111 11111111 11111111 00000000 След операцията И    11001011
00001101 00000100 00000000

 203.13.4.41 =11001011 00001101 00000100 00101001255.255.255.0 =
1111111 11111111 11111111 00000000 След операцията И  11001011
00001101 00000100 00000000
```

Обработените с И резултати съвпадат; източникът и местоназначението са от една и съща страна на мрежата, така че пакетът се доставя директно до хоста местоназначение. За графична илюстрация на този процес вижте Фигура 9-8.

Типове маршрутизиращи интерфейси

Един маршрутизатор трябва да има интерфейс към повече от една мрежа; мрежите могат да бъдат LAN или WAN. WAN интерфейс може да бъде модем или ISDN адаптер, или пък може да е друго WAN устройства вместо мрежова карта.

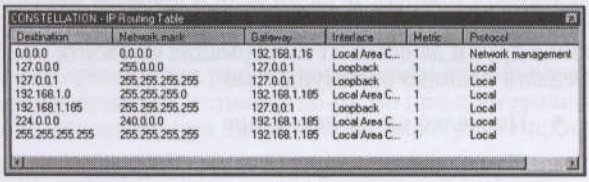
Например, когато една LAN мрежа е свързана към Интернет през dialup връзка, маршрутизаторът (или компютърът, действащ като маршрутизатор) има мрежова карта, свързана към LAN мрежата, и модем (WAN интерфейсът), който се свързва с „външната“ мрежа. Всеки интерфейс е конфигуриран отделно и всеки си има собствен IP адрес.

Статично срещу динамично маршрутизиране

Маршрутизаторите използва *маршрутни таблици (routing tables)*, представляващи бази данни, които съдържат маршрутите до различни мрежи. Фигура 9-9 показва маршрутна таблица в един компютър с Windows 2000 Server. Забележете записа от колоната Destination (местоназначение) с етикет „0.0.0.0.“ Това е

подразбиращият се маршрут (default route), който е IP адресът на подразбиращия се шлюз. Пакетите, адресирани до хостове извън мрежата 192.168.1.0 се изпращат до адреса на подразбиращия се шлюз (192.168.1.16) за препращане.

Фигура 9-9 *Маршрутната таблица за един компютър с Windows 2000 Server съдържа маршрути до други мрежи.*



CONSTELLATION - IP Routing Table

Destination	Network mask	Gateway	Interface	Metric	Protocol
0.0.0.0	0.0.0.0	192.168.1.16	Local Area C...	1	Network management
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.1.0	255.255.255.0	192.168.1.185	Local Area C...	1	Local
192.168.1.185	255.255.255.255	127.0.0.1	Loopback	1	Local
224.0.0.0	240.0.0.0	192.168.1.185	Local Area C...	1	Local
255.255.255.255	255.255.255.255	192.168.1.185	Local Area C...	1	Local

Откъде маршрутизаторът взима маршрутите, за да ги постави в своята маршрутна таблица? Отговорът зависи от това, дали той използва статично или динамично маршрутизиране, като и двата типа са описани в следващите секции.

Статично маршрутизиране

Статичното маршрутизиране изисква администраторът ръчно да въвежда в маршрутната таблица IP адресите, дефиниращи мрежови маршрути. Това може да стане с командата **route**, която идва с TCP/IP. Тази програма за командния ред ви позволява да добавяте или да изтривате записи в маршрутната таблица.

Можете да използвате този инструмент с командата **route print**, за да разгледате маршрутната таблица, както е показано в Пример 9-3.

Пример 9-3 *Командата route print се използва за разглеждане на статичната маршрутна таблица*

```
c:\>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 04 7c c0 d2 ...... 3Com EtherLink PCI
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.16   192.168.1.201       1
        127.0.0.0        255.0.0.0      127.0.0.1     127.0.0.1       1
      192.168.1.0    255.255.255.0  192.168.1.201   192.168.1.201       1
    192.168.1.201  255.255.255.255    127.0.0.1     127.0.0.1       1
    192.168.1.255  255.255.255.255  192.168.1.201   192.168.1.201       1
        224.0.0.0        224.0.0.0  192.168.1.201   192.168.1.201       1
  255.255.255.255  255.255.255.255  192.168.1.201   192.168.1.201       1
Default Gateway:       192.168.1.16
===========================================================================
Persistent Routes:
  None
```

Статичното маршрутизиране дава на администратора повече контрол над използваните маршрути. То обаче изисква продължителни и старателни усилия за поддръжка на таблицата, защото трябва да я обновявате всеки път, когато се

добавят нови маршрути или се променят вече съществуващи. За една голяма мрежа това може да се окаже непосилна задача.

Динамично маршрутизиране

Динамичното маршрутизиране използва протоколи (които дискутираме в следващата секция), за да изгради и променя маршрутните таблици автоматично. Тези протоколи позволява на маршрутизаторите в мрежата да комуникират един с друг и да обменят информация от своите маршрутни таблици. Това предлага няколко преимущества:

- По-малко администриране
- По-голяма отказоустойчивост (ако даден маршрутизатор откаже, останалите биват информирани и могат да избират други пътища до местоназначението)
- По-малък шанс за грешки в записите на маршрутните таблици

Динамичното маршрутизиране е подходящият избор за всякакви маршрутизирани мрежи, освен за малките.

Дистанционно-векторни протоколи срещу протоколи за състояние на връзките

Маршрутизиращите протоколи се разделят на две категории: *дистанционно векторни (distance-vector)* протоколи и протоколи за *състояние на връзките (link-state)*. Дистанционно-векторните протоколи са установен стандарт за динамично маршрутизиране. Те са базирани на алгоритми, разработени през 1960-те години за маршрутизирането в ARPAnet. Базата за тези протоколи е „уравнението на Белман", а алгоритмите често се наричат Белман-Форд алгоритми.

Дистанционно-векторните протоколи приемат, че всеки маршрутизатор или хост в мрежата има достъп до информация относно всички местоназначения в мрежата. Маршрутните таблици включват адреси на шлюзове и *показател (metric)* за всеки от тях. Показателят представлява общото разстояние (в брой „скокове") до мрежата местоназначение. Алгоритъмът изчислява най-добрият маршрут до определено местоназначение, базирайки се на тези дистанции.

„Динамичният" аспект влиза в играта, когато протоколът изпрати обновена маршрутна таблица на своите съседи. Когато се получи обновяване, маршрутната информация се сравнява с тази, която вече се намира в таблицата на маршрутизатора. Ако обновеният маршрут на съседния маршрутизатор има по-нисък показател от маршрута до тази мрежа в текущата таблица на маршрутизатора, той възприема този по-кратък маршрут.

Недостатъците на дистанционно-векторните протоколи включват следното:

- Податливи са на зацикляния между маршрутизатори.
- Максималното разстояние за един маршрут е 15 скока.
- Не се мащабират добре при големи мрежи.

Протоколът за състояние на връзките е по-нов тип протокол за динамично маршрутизиране. Използваните от тези протоколи алгоритми създават „карта" на топологията а мрежата и поддържат *база данни за състоянието на връзките*

(link-state database), която се базира на тази карта. Когато възникнат промени, базата данни се обновява.

При протоколите за състоянието на връзките маршрутизаторите бродкастват маршрутни данни и разпространяват информацията до останалата част от мрежата. Това е по-ефективно от дистанционно-векторния метод, елиминирайки някои от неговите проблеми. Методът обаче създава други проблеми. Например базата данни за състоянието на връзките може да нарасне значително, водейки до допълнително натоварване на процесорите и паметта.

Конвергенция (convergence), или разпространяването на обновената информация до други маршрутизатори, възниква по-бързо при протоколите за състоянието на връзките, отколкото при дистанционно-векторните протоколи.

Общоизползвани протоколи за маршрутизиране

Специализираните маршрутизиращи устройства, каквито са маршрутизаторите на Cisco, поддържат протоколи за динамично маршрутизиране. Някои операционни системи, като например Windows 2000, позволяват да се използват динамични протоколи, когато компютърът действа като маршрутизатор. Протоколите за динамично маршрутизиране за IP включват RIP (Routing Information Protocol –протокол за маршрутна информация) версии 1 и 2, и OSPF (Open Shortest Path First – първостепенно отваряне на най-краткия път). Следващите секции описват тези протоколи по-подробно.

ЗАБЕЛЕЖКА Протоколът NLSP (NetWare Link Services Protocol – протокол за комуникационни услуги в среда на NetWare) е протокол за динамично маршрутизиране за IPX. Начинът му на работа наподобява този на OSPF. Акронимът „NLSP“ се използва и за Network Layer Security Protocol.

RIP

RIP е дистанционно-векторен протокол и беше един от най-ранните протоколи за динамично маршрутизиране. (RFC 1058 дава подробни спецификации.) Произходът на RIP може да бъде проследен до програма, наречена Routed, която беше част от BSD UNIX 4.3. Едно преимущество на RIP е неговият статут на припознат стандарт.

RIP маршрутизаторите „обявяват“ информацията от своята маршрутна таблица на останалите маршрутизатори, като това става на периодични интервали. RIPv1 използва бродкастни пакети, за да изпрати известяващи съобщения, а RIPv2 добавя използването на мултикаст пакети.

За да се справи с някои от проблемите, вродени в дистанционно-векторните алгоритми на RIP, протоколът поддържа следните възможности:

- Split horizon (разделяне на хоризонта)
- Poison reverse (неутрализиране на отровата)
- Triggered updates (задействани обновявания)

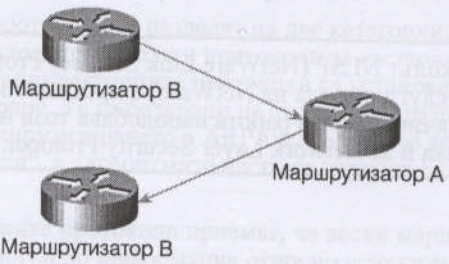
Всяка от възможностите е дискутирана в следващите секции.

Разделяне на хоризонта

Разделянето на хоризонта е средство за избягване на проблемите, възникващи когато даден маршрутизатор, след като получи обновяване от съседен маршрутизатор, в което има неточна информация, разпространява тази информация *обратно* към същия съседен маршрутизатор. Това може да доведе до ситуация, в която лош маршрут се разпространява безкрайно. Фигура 9-10 илюстрира този проблем, в който възниква следният процес:

1. Маршрутизатор B получава информация, че Маршрутизатор C не работи и изпраща тази информация на Маршрутизатор A.
2. Маршрутизатор A обновява своята маршрутна таблица, за да покаже, че Маршрутизатор C не е достъпен.
3. Маршрутизатор B получава информация, че Маршрутизатор C отново е на линия, но преди Маршрутизатор B да може да изпрати своето обновяване до Маршрутизатор A, Маршрутизатор A изпраща на Маршрутизатор B свое собствено обновяване, показващо, че Маршрутизатор C не работи.
4. Маршрутизатор B обновява своята маршрутна таблица с информацията от Маршрутизатор A, която вече не е валидна.

Фигура 9-10 *Разделянето на хоризонта се отнася до проблема с разпространяване на лоша информация напред-назад между маршрутизатори.*



При разрешаване на възможността „разделяне на хоризонта“, когато Маршрутизатор A изпраща своите обновявания към Маршрутизатор B, той *не* включва онези маршрути, които е получил *от* Маршрутизатор B.

Неутрализиране на отровата

Неутрализирането на отровата работи подобно на разделянето на хоризонта. Само че вместо да пропусне маршрутите, получени от Маршрутизатор B, Маршрутизатор A задава на тези маршрути показател 16. RIP има ограничение в разстоянието от 15 скока, така че маршрутите се считат за недостижими.

Задействани обновявания

При *задействаните обновявания* конвергенцията на промените в маршрутната таблица става по-често. Например можете да зададете правило, че ако Маршрутизатор A промени показателя за конкретен маршрут, той трябва да изпрати обновяването незабавно, вместо да чака да изтече интервалът между обновяванията. Това означава, че останалите маршрутизатори получават новата и вярна информация по-скоро, както и че се предотвратяват проблемите, причинени от някои маршрутизатори поради факта, че съдържат остаряла маршрутна информация.

OSPF

RIP работи добре за мрежи със среден размер, но за големите мрежи е необходим по-сложен протокол. За целта Cisco и останалите маршрутизатори, както и някои операционни системи, поддържащи IP препращане, използват OSPF.

OSPF е протокол за състояние на връзките, който борави с големи и сложни мрежи по-ефективно, отколкото RIP. Стандартите за OSPF могат да се намерят в RFC 1247 и RFC 1583. Алгоритъмът за състояние на връзките, използван от OSPF, не е предразположен към зацикляне между маршрутизатори и по принцип е по-ефикасен от RIP.

Причина за тази повишена ефективност (въпреки проблемите, причинени от големите бази данни) е методът на OSPF за разделяне на мрежата в *области*. Това осигурява йерархична структура за маршрутните таблици на OSPF – обратно на плоските бази данни, използвани от RIP.

Всеки OSPF маршрутизатор принадлежи на дадена област и поддържа база данни само за шлюзовете в нея. Един специален маршрутизатор, наречен *междуобластен граничен маршрутизатор (area border router – ABR)*, свързва всяка област към специална *гръбначна област (backbone area)*. Когато даден пакет трябва да премине от една област в друга, той преминава през тази гръбначна област. Този метод свива размера на маршрутните таблици и намалява времето, необходимо за преизчисляване на маршрутите, когато се извършат промени.

Кой притежава Интернет?

Въпреки че глобалният Интернет беше изграден от Министерството на отбраната на САЩ (Department of Defense – DoD) и по-късно се управляваше от NSF, преди години много организации дадоха своя принос за неговото развитие. Днес Интернет е комерсиална инициатива, но нетипична. Въпреки че отговорът на въпроса „Кой притежава Интернет?“ е „Никой“, стотици хиляди правителства, компании, организации и отделни личности притежават части от мрежата. Например инфраструктурата се основава на окабеляване и оборудване, притежавано от телефонните компании, частни предприятия и обществени агенции.

Въпреки че никой „не притежава“ Интернет, много организации, включващи следните, надзирават аспектите на неговата работа и въвеждат стандарти:

- Internet Society (ISOC)
- Internet Architecture Board (IAB)
- Internet Engineering Task Force (IETF)
- Internet Engineering Steering Group (IESG)
- Internet Assigned Numbers Authority (IANA) и Internet Corporation for Assigned Names and Numbers (ICANN)
- World Wide Web Consortium (W3C)

Следващите секции описват тези организации с подробности.

ISOC

ISOC (Интернет общество) е изградено от организации и отделни личности, посветени на мисията да осигурят ръководене и разработване на стандарти, за

да гарантират, че Интернет продължава да се развива и да носи ползи на обществата по цял свят.

ISOC координира свързаните с Интернет дейности, финансира поста RFC редактор и осигурява база за организации като IAB и IETF.

IAB

IAB (първоначално се наричаше Internet Activities Board) се състои от 13 члена с право на глас, единият от които е председателят на IETF. Останалите членове се номинират от IETF. IAB публикува така наречените Internet Drafts (Интернет проекти) и RFC документи, сформира изследователски групи и дискутира въпроси, засягащи инфраструктурата, обществото и работата на Интернет.

IETF

Организацията IETF е изградена от „работни групи", посветени на специфични въпроси, свързани с интермрежите. Например в момента една от активните групи се занимава със стандартите и реализирането на IPv6. IETF е отворена за всеки, който иска да вземе участие; повечето от дискусиите се извършват в самия Интернет. Всяка работна група има един или повече пощенски списъци, чрез които нейните членове комуникират.

IESG

IESG е част от ISOC и работи в сътрудничество с IAB. Тя администрира процеса, чрез който предложенията се превръщат в Интернет стандарти, както е дефинирано в RFC 2026.

IANA/ICANN

IANA е отговорна за назначаването на IP адреси и други уникални идентификатори в Интернет.

ICANN е организация с идеална цел, съставена от правителствени, търговски и технически членове. ICANN координира управлението на системата за имена на домейни в Интернет и отпускането на IP адреси.

W3C

W3C разработва общи протоколи и стандарти, приложими за Web (Мрежата). Тя е международна организация, посветена на осигуряването на ръководство и създаване на технически спецификации за работата и инфраструктурата на Web.

Обобщение

В тази глава дискутирахме еволюцията на Интернет – от ARPAnet до наши дни. Научихте за гръбнака на Интернет, осигуряващ информационна магистрала, която се използва от местни и регионални мрежи за свързване на големи разстояния. Дискутирахме както комерсиалния гръбнак, така и vBNS, който е запазен за научни цели. Научихте за проекта Internet2 – консорциум от университе-

ти, подкрепяни от правителството, които се занимават с разработването и тестването на нови технологии.

Дискутирахме начините, по които може да се установи една Интернет връзка, а също и ролята на Интернет доставчиците, регионалните мрежи, NAP точките и MAE централите. След като обсъдихме как пакетите пътуват през физическата инфраструктура, насочихме нашето внимание към многото приложения, използвани в Интернет, както и протоколите, с които те работят. Хвърлихме поглед на World Wide Web, машините за търсене, електронната поща, нюзгрупите, файловия трансфер и Telnet. Дискутирахме и модерни технологии, като поточна медия, чат на живо, аудио/видео конфериране и Интернет телефония.

Обърнахме внимание и на ролята на TCP/IP маршрутизирането по Интернет; научихте някои от най-основните концепции на маршрутизацията, като например разликата между статично и динамично маршрутизиране. Дискутирахме накратко дистанционно-векторните протоколи и протоколите за състояние на връзките, в частност RIP и OSPF.

Накрая говорихме за организациите, надзиращи различни аспекти от Интернет – това са ISOC, IAB, IETF, IESG, IANA, ICANN и W3C.

Сега, след като имате повече познания върху мрежовия хардуер и протоколите, както и върху най-голямата от всички мрежи, в следващата глава ще се запознаете с мрежовите операционни системи (Network Operating Systems – NOSs), които се изпълняват на сървъри, предоставяйки техните ресурси на LAN мрежите, както и на Интернет.

Допълнителни източници

За повече информация относно MAE системата на WorldCom вижте http://208.234.102.97/MAE/doc/maedesc/maedesc1.html.

За колекция от карти, показващи гръбнаците на Интернет в САЩ и Европа, както и за други полезни карти и графични представяния, свързани с Интернет, вижте статията „An Atlas of Cyberspace“ на адрес www.cybergeography.org/atlas/atlas.html.

За повече информация относно World Wide Web и Web стандартите вижте Web сайта на W3C на адрес www.w3.org.

За повече информация относно стандартите за изпращане на поща в Интернет вижте Web сайта на Internet Mail Consortium на адрес www.imc.org.

За връзки към ръководства и ресурси, свързани с видео конферирането, вижте http://netconference.about.com/internet/netconference/msub1.htm.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Гръбнаците на Интернет са групи от информационни магистрали, използвани от локални мрежи за осъществяване на връзки на далечни разстояния. Как се наричат съответните точки на свързване?

   a Хостове

   b Възли

c Подмрежи
d Сървъри

2 Как се наричат местата, в които основните Интернет доставчици се свързват един с друг?

a ISP
b vBNS
c Суперкомпютри
d NAP точки

3 Кое от следните е дефиниращата характеристика за хипертекстовите файлове?

a Разположени са на Web сървър.
b Достъпът до тях се осъществява чрез URL адрес.
c Съдържат връзки (линкове) към други файлове.
d Не могат да съдържат вградена графика.

4 Кой от следните е правилният синтаксис за въвеждане на URL адрес на отдалечен Web сайт в един Web браузър?

a http:\www.acme\
b html://www.acme.com
c http://bigserver.acme.com/
d html:\acme.com

5 Кое от следните е Web сайт, служещ като „стартова точка" за потребителите и често се осигурява от доставчиците на Интернет или от онлайн услугите на техните клиенти, както и от повечето сайтове с машини за търсене?

a Машина за метатърсене
b Портал
c Подразбиращ се шлюз
d Хипервръзка

6 Кой пощенски протокол се изпълнява на сървъри, получаващи поща, и ви позволява да преглеждате хедърите на сървъра, след което да изберете кои съобщения да свалите?

a SMTP
b SNMP
c POP
d IMAP

7 За коя от следните дейности се използва NNTP?

a За управление на пощенски списъци в Интернет
b За работа на Novell NetWare по TCP/IP

c За достъп до публикации в нюзгрупи

d За свързване към отдалечени компютри с цел разглеждане на файлове и стартиране на приложения

8 Кое от следните се използва за провеждане на текстово-базиран „чат на живо“ по Интернет?

a IRC

b Telnet

c IGMP

d FTP

9 Към какво се прилага стандартът H.323 ITU?

a Програмиране на Web страници

b Видеоконферииране

c Трансфер на файлове по Интернет

d Машини за търсене

10 Кое от следните твърдения е вярно за RIP? (Изберете всички верни отговори.)

a RIP е протокол за динамично маршрутизиране.

b RIP разделя мрежата на области, включвайки гръбначна област, към която се са свързани всички останали области.

c RIP е по-ефективен и мащабируем от OSPF.

d RIP е дистанционно-векторен протокол.

Глава 10

Мрежови операционни системи

Компютърната операционна система е софтуерът, осигуряващ основата, върху която работят приложенията и услугите. По подобен начин една *мрежова операционна система* (*network operating system – NOS*) позволява на устройствата да комуникират помежду си, както и да споделят ресурси по мрежата.

Мрежовата операционна система понякога се използва за описание на която и да е операционна система с вградени мрежови компоненти. Това е противоположно на *самостоятелната* операционна система, проектирана да се използва в изолация. Все пак мрежовата операционна система си е операционна система, като например NetWare или NT Server, работеща на мрежов сървър. Ще използваме тази дефиниция по-нататък в главата, когато разглеждаме следните популярни сървърни операционни системи:

- Microsoft Windows NT 4.0
- Microsoft Windows 2000
- Novell NetWare
- UNIX
- Linux
- Banyan Vines
- OS/2 Warp Server
- Apple NOS
- LANtastic

Преди да започнем да разглеждаме характеристиките на всяка мрежова операционна система и мрежата, в която тя работи, ще дискутираме някои общи принципи на мрежовата администрация в среда клиент/сървър.

Общи принципи на мрежовата администрация

Една сървърно-базирана мрежа притежава един или няколко посветени сървъра. Сървърът обикновено е (но не задължително) машина с по-бърз процесор, голямо количество RAM и по-голям твърд диск или дискове, отколкото работните станции, които се свързват с него.

Въпреки че една сървърна операционна система може да осигури централизирано администриране и централизирано местоположение за съхранение на данни, сървърно-базираната обработка е различна от *централизираната* обработка – термин, използван предимно по отношение на мейнфрейм компютрите. При един мейнфрейм компютър, терминалите се свързват към голяма и мощна машина, като всички изчисления се извършват от нея. В противовес на това клиентските работни станции в една сървърно-базирана мрежа са мощни компютри. В зависимост от приложението, всички обработки могат да се извършват на клиентската машина, или пък това може да става споделено между клиента и сървъра.

ЗАБЕЛЕЖКА В Глава 2, „Категоризиране на мрежите", научихте, че има нещо средно между самостоятелен компютър и сървърно-базирана мрежа, което използва Мрежова операционна система: равноправната (peer-to-peer) мрежа. Windows 9x, Windows NT и Windows 2000 машините имат вградена способност да се присъединяват към „работна група", вместо към сървърно-базиран домейн.

ЗАБЕЛЕЖКА NetWare също имат продукт за равноправна мрежа, наречен NetWare Lite. Освен това, въпреки че UNIX беше проектиран като ориентирана към сървър мрежова операционна система, Linux машините могат много лесно да се свързват към равноправна конфигурация (въпреки че Linux също се използва главно за сървърно-ориентирана мрежова операционна система). Apple Macintosh компютрите имат вградена поддръжка за равноправна мрежа, като самият AppleTalk първоначално е създаден за малки работни групи.

Клиент/сървър средата се различава от *равноправната (peer-to-peer)* среда, която дискутирахме в Глава 2 (вижте Фигура 10-1).

В следващите секции дискутираме характеристиките на обкръжението клиент/сървър и как се споделят и управляват мрежовите ресурси.

Средата клиент/сървър

Базираната на сървъри мрежа предлага среда, която е лесна за администриране, архивиране и обезопасяване. В тази среда клиентските машини заявяват данни и ресурси от сървъра. Сървърът може да споделя само файлове, но е възможно да споделя и принтери, приложения, модеми, Интернет връзки и други ресурси.

В следващите секции дискутираме клиент/сървър приложенията и как се конфигурира една клиент/сървър мрежа.

Клиент/сървър приложения

Клиент/сървър приложенията оползотворяват процесорната мощ на даден сървър, за да оптимизират задачи, като например заявки към бази данни (едно такова приложение е сървърът за бази данни SQL Server на Microsoft. Повечето големи приложения за бази данни използват SQL; ето как работи той:

Фигура 10-1 *Средите работна група, клиент/сървър и мейнфрейм.*

1. Един клиент, на който се изпълнява клиент за бази данни (наречен „front end"), какъвто е Microsoft Access, заявява данни от SQL сървъра (наречен „back end"). След това заявката се транслира в SQL.
2. SQL заявките се предават до сървъра, който провежда търсене за заявената информация на компютъра, на който се намира и самата база данни.
3. Сървърът връща резултатите от търсенето към клиента, след което то се представят на потребителя от клиентското приложение.

ЗАБЕЛЕЖКА На някои мрежови сървъри може да се изпълнява *софтуер за терминални услуги*, позволяващ на мрежов клиентски компютър, на който се изпълнява софтуерът за терминални услуги, да се свърже със сървъра и да стартира програми, при които сървърът се занимава с този процес. Това в някои отношения е подобно на централизираните изчислителни среди.

Сравнете метода с клиент/сървър приложение и този, в който потребителите създават бази данни в Access (работещ на техните локални машини), след което съхраняват базите данни на файлов сървър. Когато се направи заявка, цялата база данни се сваля на клиентската машина и процесът на търсене се провежда там. Виждате, че пропускателната способност на мрежата се пести при метода с клиент/сървър приложение.

Недостатъкът на клиент/сървър приложенията е първоначалната цена. Програмите за клиент/сървър бази данни, като SQL Server или Oracle, са относително скъпи и могат да не са ценово-ефективни за малки мрежи, където заявките към базите данни са прости и не много чести.

Конфигурация на мрежа клиент/сървър

Клиент/сървър мрежата може да бъде конфигурирана по един от следните два начина:

- Данните могат да бъдат разположени на един сървър за бази данни.
- Данните могат да бъдат разпределени (distributed), или разпръснати, на множество сървъри за бази данни.

Фигура 10-2 илюстрира разликата между тези две конфигурации.

Фигура 10-2 *Данните могат да са разположение на един сървър или да бъдат разпределени на множество сървъри.*

Едно *хранилище за данни (data warehouse)* представлява централно място, където се съхраняват огромни количества данни. По традиция хранилищата за данни бяха базирани на мейнфреймове, но някои мрежови операционни системи за PC-та, като например Microsoft Windows 2000 Datacenter Server, са проектирани специално за тази цел. В хранилището данните могат да бъдат съхранявани на масив от дискове, инсталирани на един сървър, или да бъдат разпръснати на дисковете на множество сървъри във *ферма от сървъри (server farm)*.

Споделяне на мрежови ресурси

Процесът на споделяне по мрежата зависи от мрежовата операционна система. Някои мрежови операционни системи, като тези от фамилията Windows, по подразбиране не споделят абсолютно нищо. Ако искате до дадени ресурси да има достъп по мрежата, те трябва изрично да се споделят в процес, наречен *създаване на споделен ресурс (creating a share)*. Други мрежови операционни системи, като NetWare, се държат точно по обратния начин – ресурсите са споделени по подразбиране.

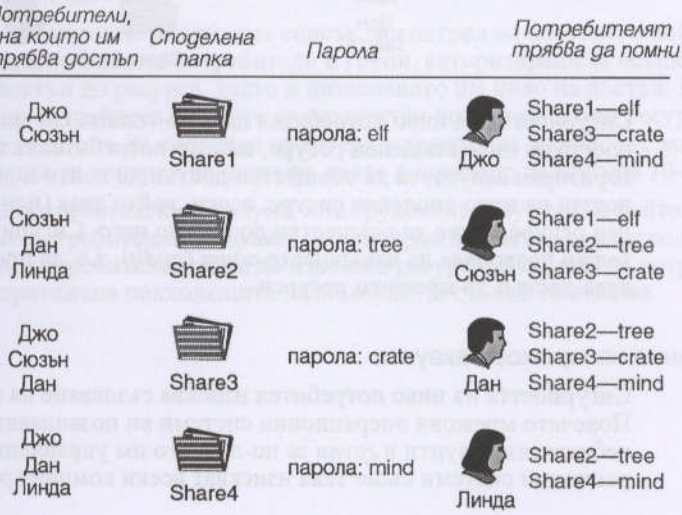
За да може един Windows 9*x* компютър да споделя своите ресурси, услугата *File and Print Sharing* трябва да е разрешена. Ако компютърът използва Windows NT или Windows 2000, там трябва да е инсталирана и да работи *услугата server*.

Целта компютрите да се свързват в мрежа е да споделят ресурси, но това не означава, че всеки ресурс трябва да бъде споделен с всички потребители. Ето защо една NOS (мрежова операционна система) трябва да осигури средства за контролиране на достъпа до файлове, папки, принтери и други ресурси. Има два начина за постигане на това: сигурност на ниво споделен ресурс и сигурност на ниво потребител.

Сигурността на ниво споделен ресурс (share-level security) по принцип се използва в равноправните (peer-to-peer) мрежи, където машините обикновено работят под операционни системи като Windows 95 и 98. При този тип сигурност, когато изберете да споделите някой ресурс по мрежата, например папка, задавате парола за този ресурс. За да може някой да осъществи достъп до споделената папка, той трябва да знае и да въведе вярната парола, когато бъде подканен да направи това.

Въпреки своята простота, сигурността на ниво споделен ресурс се превръща в кошмар, когато в мрежата има много потребители и много споделени ресурси. Всеки споделен ресурс има различна парола, като тези пароли трябва да бъдат дадени на всички хора, които са авторизирани да осъществяват достъп до съответните споделени ресурси (вижте Фигура 10-3).

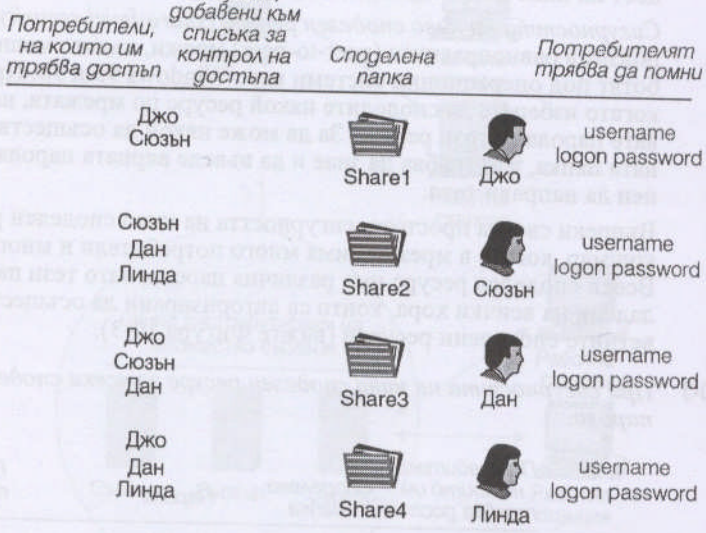
Фигура 10-3 *При сигурността на ниво споделен ресурс за всеки споделен ресурс се задава парола.*



Сигурността на ниво потребител (user-level security) е много по-лесна за управление в средна или голяма мрежа, отколкото сигурността на ниво споделен ресурс. При сигурността на ниво потребител всеки потребител има *потребителски акаунт (user account)*, който е защитен с парола. Потребителят се логва (влиза в) компютъра с този акаунт. Всеки споделен ресурс се конфигурира така че да достъпът до него да е разрешен само за авторизираните потребители. Когато даден потребител се опита да осъществи достъп до ресурс, се проверява *списъкът за контрол на достъпа (access control list)*, асоцииран с ресурса. Този списък съдържа авторизираните акаунти, които имат позволения за съответния ресурс. Ако акаунтът, с който е влязъл потребителят, е в списъка, тогава потребителят може да осъществи достъп.

При сигурността на ниво потребител, всеки потребител трябва да помни само една парола (вместо цял куп), за да осъществява достъп до множество различни мрежови ресурси (вижте Фигура 10-4).

Фигура 10-4 *Сигурността на ниво потребител работи чрез създаване на списък за контрол на достъпа за всеки споделен ресурс.*



Сигурността на ниво потребител дава по-голяма сигурност, отколкото сигурността на ниво споделен ресурс, защото потребителят трябва да се логнал с авторизиран акаунт, за да осъществи достъп до който и да е ресурс. При сигурността на ниво споделен ресурс, всеки, който знае (или отгатне) паролата за даден ресурс, може да осъществи достъп до него. Сигурността на ниво потребител ви позволява да извършвате *одит (audit)*, т.е. да проследявате кой осъществява достъп до мрежови ресурси.

Управление на мрежови акаунти

Сигурността на ниво потребител изисква създаване на потребителски акаунти. Повечето мрежови операционни системи ви позволяват да подредите тези потребителски акаунти в *групи* за по-лесното им управление. Някои мрежови операционни системи също така изискват всеки компютър, който се логва в мре-

жата, да има *компютърен акаунт* (наричан също *машинен акаунт*). Това осигурява допълнително ниво на защита и подобрява сигурността на мрежата. В следващите секции, разглеждаме тези три типа акаунти: потребителски, групови и компютърни.

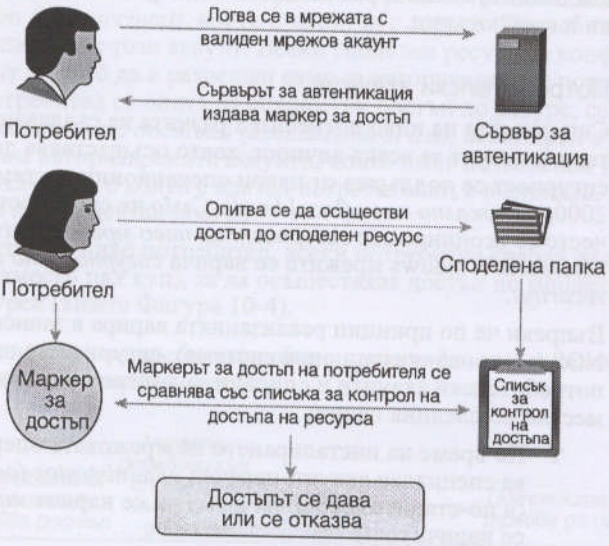
Потребителски акаунти

Сигурността на ниво потребител разчита на създаването на отделен потребителски акаунт за всяка личност, която осъществява достъп до ресурси. Този тип сигурност се поддържа от някои операционни системи, като Windows NT и 2000, на *локално ниво (local level)*. Само че сигурността на ниво потребител почесто се асоциира със *сигурност на ниво мрежа (network-level security)*, която в Microsoft Windows мрежите се нарича *сигурност на ниво домейн (domain-level security)*.

Въпреки че по принцип реализацията варира в зависимост от използваната NOS (мрежова операционна система), сигурността на ниво мрежа използва потребителски акаунти и списъци за контрол на достъпа, които работят съвместно по следния начин:

1. По време на инсталирането на мрежовата операционна система се създава специален акаунт, наречен *administrator (администраторски акаунт)* (в по-старите версии на NetWare се нарича *supervisor*, а в UNIX и Linux се нарича root).
2. Чрез използване на администраторския акаунт, мрежовият администратор може да създава потребителски акаунти за други хора, които ще използват мрежовите ресурси.
3. Когато потребителят се логва в мрежата, той въвежда име на потребителски акаунт и парола, след което те се проверяват в базата данни с акаунти за сигурност *(security accounts database)*. Тази база данни е разположена на сървър за автентикация при логване *(logon authentication server)*. (В Microsoft Windows мрежите този сървър се нарича домейн контролер [*domain controller*].)
4. Ако акредитивите се окажат валидни, на потребителя се издава маркер за достъп (*access token*), идентифициращ потребителя и групите, към които той принадлежи.
5. Всеки споделен ресурс има списък за контрол на достъпа, в който се съдържат отделните потребители и групи, авторизирани за осъществяване на достъп до ресурса, както и позволеното им ниво на достъп. Когато даден потребител се опита да осъществи достъп до даден ресурс (например да печата на споделен принтер), маркерът за достъп се сравнява със списъка за контрол на достъпа, както е показано на Фигура 10-5.
6. Ако потребителският акаунт, или груповият акаунт, към който принадлежи потребителят, се окаже авторизиран в списъка за контрол на достъпа, потребителят може да използва ресурса. В случай че потребителят не притежава подходящите позволения, достъпът се отказва.

Фигура 10-5 *Маркерът за достъп на потребителя се сравнява със списъка за контрол на достъпа на ресурса.*



Това е опростена версия на начина, по който работи сигурността на ниво мрежа. В Глава 14, „Защита на мрежата", дискутираме сигурността по-задълбочено. Там ще научите някои от методите, използвани за автентициране на потребителите в мрежата.

Създаване на потребителски акаунти Един потребителски акаунт се състои от следното:

- Потребителско име
- Парола (в някои случаи паролата може да е празна)
- Условия и ограничения на потребителя (компютрите, от които потребителят може да се логва, ограничения за час/дата, дали е позволено отдалечено логване и т.н.)
- Информация за сигурност относно потребителя (групи, към които принадлежи потребителят, и потребителски права)
- Незадължителна информация (пълното име на потребителя, звание или описание на позицията, справочна информация, като телефонни номера и e-mail адрес, и т.н.)

Точният метод за създаване на потребителски акаунти зависи от използваната NOS, но всички мрежови операционни системи притежават помощни програми, или *административни инструменти (administrative tools)*, които могат да се използват за добавяне на нов потребител към базата данни за сигурност. Независимо от използваната NOS, принципите са едни и същи:

- Потребителските имена трябва да са уникални.
- По принцип могат да се използват главни и малки букви, както и цифри.

- В повечето случаи трябва да избягвате използването на следните символи в потребителските имена: „ \ / : | = , + * ? < >.
- Операционната система може да ограничава броя на знаковете, използвани в едно име.
- Трябва да избягвате използването на интервали в потребителските имена.

Групови акаунти

Можете да управлявате позволенията за достъп и потребителските права чрез задаването им на отделни потребителски акаунти, но повечето мрежови операционни системи ви позволяват да използвате групи, за да опростите управлението на акаунтите.

Повечето мрежи на компании съдържат стотици, а понякога и хиляди потребители. Да предположим, че имаме десет споделени папки, в които се съхраняват всички документи на отдел продажби, както и 200 потребителя, работещи в този отдел, които се нуждаят от достъп до тези документи.

В нашия сценарий *бихме могли* да конфигурираме всяка от десетте папки така, че всеки от 200-те потребителски акаунта да има достъп, но си представете колко времеемка и отегчителна задача ще бъде това. Освен това всеки път, когато създаваме нова папка, до която персоналът от отдела трябва да има достъп, ще се налага да добавяме 200 потребителски акаунта към списъка за контрол на достъпа на тази папка. Трябва да има по-добър начин.

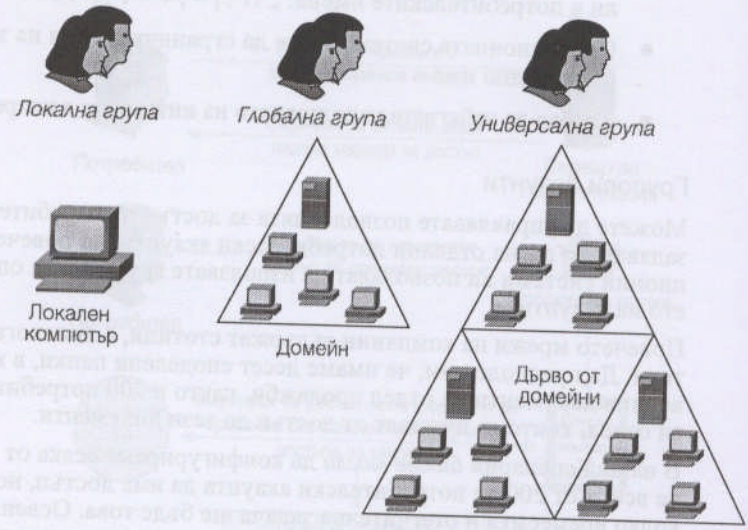
За щастие, *има* по-добър начин. Ако поставим всички потребителски акаунти за работниците от отдел продажби в група с име Sales, можем след това да зададем позволения за достъп за всяка от десетте папки на *един* групов акаунт, вместо на *200* потребителски акаунта. Ако създадем нова папка, отнема само минута да добавим групата Sales към списъка за достъп – вместо часове, за да добавим всички 200 потребителски акаунта.

Групите могат да се използва и за по-лесно изпращане на множество копия на дадено съобщение до голям брой потребители.

Групи на които се задават позволения за достъп, се наричат *групи за сигурност (security groups)*. Групите, създадени за използване само от приложения като e-mail програми, на които групи не се задават никакви позволения, се наричат *групи за разпределение (distribution groups)*.

Някои операционни системи разделят групите на категории, базирани на област на действие, като например локални и глобални, в зависимост от това дали са приложими за индивидуалния потребител или за целия домейн. Windows 2000 също включва групова област, наречена *universal*, която може да се използва във всички домейни в едно дърво или гора от домейни, както е показано на Фигура 10-6. NetWare и UNIX не правят разлика между локални и глобални групи.

Фигура 10-6 *Windows 2000 мрежите включват три групови области.*



Повечето мрежови операционни системи създават една или повече *подразбиращи се групи* по време на инсталиране. Една от тези групи обикновено е всеобхватна – в нея автоматично се поставят всички потребителски акаунти. В Windows NT, Windows 2000 и NetWare 3*x* тази група се нарича *Everyone* (в новите версии на NetWare такава група липсва). В UNIX тя се нарича *World*. Други подразбиращи се групи включват *Users* (потребители), *Administrators* (администратори), *Backup Operators* (архивиращи оператори) и т.н.

Всички потребители, принадлежащи към дадена група, притежават правата и позволенията, назначени на тази група. Тъй като в повечето мрежови операционни системи потребителите могат едновременно да принадлежат към повече от една група (а някои операционни системи позволяват *влагането (nesting)* на групи вътре в други групи), може да стане интересно, ако правата и позволенията на една група влязат в конфликт с тези на друга група, към която принадлежи потребителят. Изучаването на това, как се разрешават тези конфликти е важна част от обучението за работа с конкретна NOS.

Компютърни акаунти

Мрежовите операционни системи, проектирани за среди с висока сигурност, могат да изискват не само потребителите да имат акаунти за логване в мрежата, но и свързаните към мрежата компютри да притежават машинни акаунти. Например в един Windows домейн администраторът трябва да е създал компютърен акаунт за всяка система, работеща под Windows NT или Windows 2000, преди тя да може да се присъедини към домейна. Windows 9*x* компютрите обаче бяха предназначени за домашно използване и малък бизнес, т.е. за среди с по-ниско ниво на сигурност; тези машини не могат да се присъединяват към домейн, въпреки че потребител с валидно потребителски акаунт *може* да се логне в Windows домейн от Windows 9*x* система.

Операционната система използва компютърния акаунт, за да валидира идентичността на компютъра и да извършва одит на действията, извършвани по време на използване на компютърния акаунт.

Управление на споделени ресурси

В някои мрежови операционни системи, като например тези от фамилията Windows, когато създавате споделен ресурс, той автоматично се споделя по подразбиране с групата Everyone, която съдържа *всички* потребители. Ако това не е каквото желаете, не забравяйте да модифицирате позволенията, когато създавате споделения ресурс.

На споделените ресурси обикновено се задават *имена на споделени ресурси (share names)*, които могат да бъдат – но не задължително – същите като действителните имена на самите ресурси. Например, ако споделите папка, наречена salesdocs, за име на споделения ресурс можете да зададете Sales Documents, ако искате; това *не* променя името на самата папка.

След като ресурсите бъдат споделени, те трябва да се управляват. Управлението на ресурсите включва следното:

- Улесняване достъпа до споделените ресурси за онези, които са авторизирани да осъществяват достъп до тях
- Обезопасяване на споделените ресурси спрямо неавторизиран достъп

В известен смисъл тези цели са противоположни, но можете да постигнете и двете, като използвате *директорийни услуги (directory services)*, като NDS (Novell Directory Services) на Novell или Active Directory на Microsoft. Ще научите повече за директорийните услуги в Глава 11, „Директорийни услуги".

Могат да бъдат споделяни всякакви видове устройства, включително скенери, факс-устройства и външни запаметяващи устройства. Ако нещо се свърже към компютър, а компютърът е свързан към мрежа, някой вероятно е открил начин да го сподели – или поне ще го направи в скоро време. Но независимо от ресурса, целите на споделянето са едни и същи: достъпност и контрол на достъпа.

В следващите секции разглеждаме типовете споделени ресурси, които могат да се управлява от мрежовия администратор:

- Файлове и папки
- Принтери
- Приложения
- Връзки

Споделени файлове и папки

Съществуват няколко причини файловете и папките да се споделят по мрежата. Документите, които трябва да бъдат разглеждани или редактирани от множество потребители, е необходимо да бъдат споделени така, че всички да имат достъп до едно и също копие на документа. Това предотвратява объркването, възникващо от ситуацията, в която всеки си пази уникално копие на своя твърд диск.

Възможно е потребителят, създал документа, да го съхранява на своя собствен твърд диск и да създаде споделен ресурс. Само че по-добрият начин е документът да се съхранява на централизирано място – на *файлов сървър*. Това е по-ефективно, отколкото споделените документи да се съхраняват на различни компютри из цялата мрежа. Причините за това са няколко:

- Администраторът може да гарантира, че всички документи се архивират редовно.

- Ако работната станция на някой откаже, това няма да засегне достъпа до документите.
- За всички е по-лесно да открият споделените документи, ако те са разположени на един сървър.

Друга причина за използването на споделени мрежови папки е на всеки потребител да се предостави сигурно, но централизирано място за съхранение на документите. Понякога това място се нарича *домашна директория (home directory) (на жаргон – хоум директория)*. Всички данни, създадени от потребителя, отиват в неговата домашна директория, разположена на мрежовия сървър. Никой друг няма достъп до тази директория, но домашните директории на всички потребители се архивират всеки път, когато започне планираното архивиране на сървъра.

Една споделена папка може да бъде мапната като буква на мрежово устройство с цел по-лесен достъп. Това означава, че за крайният потребител отдалечената папка се появява като буква на устройство в инструмента за управление на локалните файлове (какъвто е Windows Explorer). Например, ако Джо често се нуждае от достъп до файлове в папка, наречена Marketing, която се съхранява на файловия сървър, той може да мапне тази папка, така че тя да се появява като устройство K в Windows Explorer. Ако потребителят щракне двукратно върху K, се изобразява съдържанието на отдалечената папка. Това е много по-лесно, отколкото всеки път при необходимост от достъп да се навигира из мрежата, докато не се открие желаният ресурс.

ЗАБЕЛЕЖКА По-нататък в тази глава ще научите как да мапвате мрежови устройства във всяка операционна система.

Споделени принтери

Движеща сила за мрежовите бизнес компютри е способността за споделяне на принтери и други скъпи периферни устройства. Чрез възможността за споделяне на принтери всеки в мрежата може да печата на принтер, свързан към който и да е друг компютър в мрежата (или директно свързан към мрежата принтер).

В зависимост от операционната система, има няколко начина за свързване с отдалечен споделен принтер. Единият начин, *прихващане на принтерския порт (capturing the printer port)*, пренасочва заданията за печат от локалния принтерски порт към мрежовия принтер. По-нататък в тази глава ще научите как да правите в различни операционни системи.

Споделени приложения

Един *приложен сървър* може да позволи на мрежовите потребители да използват неговите приложни програми. Това означава, че приложенията са инсталирани само на сървърната машина и не заемат дисково пространство на локалните работни станции. Производителността при използване на приложен сървър обикновено е по-ниска, отколкото ако приложението се стартира на локалния компютър, но няколко преимущества компенсират това:

- За работните станции се изискват по-малки твърди дискове.
- Администраторите имат контрол над конфигурирането на приложните програми.

- Администраторите могат да гарантират, че всички в организацията използват една и съща версия на приложението.
- Приложението може да се ъпгрейдне само веднъж, на сървъра, вместо на всяка работна станция.

Споделянето на приложения може да се осъществи и чрез използване на *терминални услуги (terminal services)*, които ще бъдат дискутирани в Глава 17, „Мрежи за тънки клиенти".

Споделени връзки

Друга причина за свързването на компютрите в мрежа, било то в офиса или вкъщи, е споделянето на Интернет връзка. Вместо за всеки отделен компютър да ви трябва модем, телефонна линия и акаунт към Интернет доставчик (Internet service provider – ISP), всички свързани в мрежа компютри могат да се свържат към Интернет през една линия и един акаунт. Има няколко начина да се направи това:

- Чрез използване на маршрутизатор, свързващ всички компютри към Интернет връзката, като всеки от компютрите разполага с отделен публичен IP адрес
- Чрез софтуер за транслиране на мрежови адреси (Network Address Translation – NAT), който позволява на компютрите в локалната мрежа да се свържат към Интернет през NAT хост, използвайки само един публичен IP адрес
- Чрез прокси сървър, използващ форма на адресно транслиране и осигуряващ сигурност за входящите и изходящите пакети

LAN/WAN връзките, използващи маршрутизиране или NAT, бяха дискутирани подробно в Глава 6, „WAN връзки".

Преглед на мрежовите операционни системи

Изборът на мрежова операционна система (NOS) може да бъде сложно решение. Всяка популярна NOS си има силни и слаби страни, и понеже мрежовите операционни системи по принцип са много по-скъпи от настолните (често с цена няколко стотин долара, в зависимост от броя на клиентите, които се свързват към сървъра), решението не се взима с лека ръка.

Мрежовите администратори трябва да знаят поне някои основни концепции по отношение на трите най популярни NOS семейства: Windows, NetWare и UNIX/Linux. Много от днешните мрежи включват повече от един тип сървър, така че познанието как да се накарат тези системи да работят в хармония е важно умение за мрежовия персонал. Поради тази причина посветихме глава 13, „Хибридни мрежи" на хибридните мрежи и въпросите, свързани със съвместната работа.

Важно е за един мрежов администратор да научи да „говори езика" на операционните системи в мрежата. Различните производители на мрежови операционни системи използват едни и същи термини по различни начини. Например „root" означава главният административен акаунт в една UNIX среда, но в NetWare мрежите се използва за идентифициране на NDS обект. В света на Windows, „root" може да се отнася за домейна, стоящ на върха на едно дърво от

Windows 2000 домейни, или да означава основния компонент на дистрибутирана файлова система (Distributed File System – Dfs).

В следващите секции дискутираме популярните мрежи, базирани на мрежови операционни системи, а именно:

- Windows NT и Windows 2000 мрежи
- NetWare мрежи
- UNIX/Linux мрежи

Windows NT и Windows 2000 мрежи

Мрежите, базирани на Windows сървър (Windows NT Server или Windows 2000 Server), се базират на концепцията за домейна. Един *домейн (domain)* представлява групиране на компютри и потребители, което служи като граница за дадена административна власт. Windows NT домейните и Windows 2000 домейните, макар че са подобни по функционалност, взаимодействат помежду си по различен начин.

Windows терминология

Microsoft използва термина „домейн", за да опише групи от компютри, потребители и ресурси, формиращи административна граница, и използва термина „домейн контролер", за да опише сървърите за автентикация при логване, съдържащи копие от базата данни с акаунтите за сигурност. Характерна за Microsoft мрежите е и разликата между термините *принтер*, използван за описание на логическа софтуерна конструкция, и терминът *печатащо устройство (print device)*, използван за означаване на действителния хардуер, отпечатващ документа.

Терминологията на Windows 2000 мрежите е позната за онези, които са работили с Windows NT 4.0, но за по-старите NT администратори някои от новите термини и концепции, като *дърво от домейни (domain tree)* и *гора (forest)*, може да не са познати. Освен това за администраторите, които преминават от NetWare среда към Windows мрежи, могат да открият, че някои познати термини, като например *„дърво"*, имат различни значения.

В следващите секции разглеждаме специфични характеристики на Windows NT 4.0 и Windows 2000, и дискутираме как се изпълняват обичайни административни задачи, включващи мапване на мрежови устройства и споделяне на принтери.

Windows NT 4.0

Графичният интерфейс на Windows NT 4. 0 е подобен на този на Windows 95, поради което е познат на потребителите, използвали тази популярна настолна операционна система. Всеки NT домейн изисква един (и само един) *главен контролер на домейн (primary domain controller – PDC)*. Това е главният сървър, съдържащ базата данни за управление на акаунтите за сигурност, често наричана SAM (от security accounts management). Един домейн също така може да притежава един или повече *резервни контролери на домейни (backup domain controllers – BDCs)*, всеки от които съдържа копие само за четене на SAM.

Потребителите могат да се логват във и след това да бъдат автентицирани или от PDC контролера, или от някой BDC, но промени в базата данни SAM могат

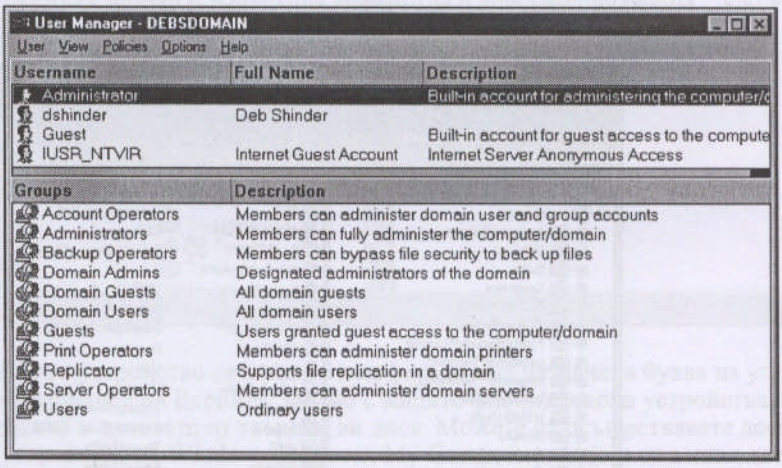
да се правят само в PDC. След това тези промени се репликират на BDC контролерите на регулярна база. BDC контролерите балансират натоварването на трафика, породен от процеса на автентициране, и служи като резерва, в случай че PDC контролерът отпадне. Ако PDC загуби трайно своята работоспособност, някой от BDC контролерите може да стане PDC.

Създаване и управление на потребителски акаунти в Windows NT 4.0

Microsoft осигурява административен инструмент, наречен User Manager for Domains, до който осъществявате достъп от домейн контролера и използвате за създаване, управление и премахване на потребителски акаунти от домейна. За да го стартирате, изберете Start, Programs, Administrative Tools, User Manager for Domains.

Инструментът User Manager for Domains позволява на администратора да създава нови потребителски и групови акаунти; да преименува, модифицира и изтрива акаунти; да назначава пароли; да установява политики за акаунтите; да задава рестрикции за потребителите. Рестрикциите включват указване на това, кога и от коя работна станция те могат да се логват. Вижте Фигура 10-7.

Фигура 10-7 *User Manager for Domains ви позволява да създавате и управлявате акаунти.*



Забележете групите, показани на Фигура 10-7. Всички те са вградени подразбиращи се групи за Windows NT 4.0 домейни. Двата вградени подразбиращи се потребителски акаунта са Administrator (администратор) и Guest (гост).

Windows 2000

Windows 2000 мрежите използват *Active Directory*, директорийна услуга, подобна на NDS на Novell, предназначена за съхраняване на информация за сигурност. (Ще научите повече за многото функции на Active Directory в Глава 11.) Докато базата данни за сигурността в NT е плоска, Active Directory по природа е йерархична.

Windows 2000 домейните могат да се обединяват в дървета, представляващи групи от домейни, споделящи непрекъснато пространство от имена (contiguous namespace). Множество дървета могат да се обединяват в гори, което прави мрежовата структура мащабируема до какъвто и да било размер.

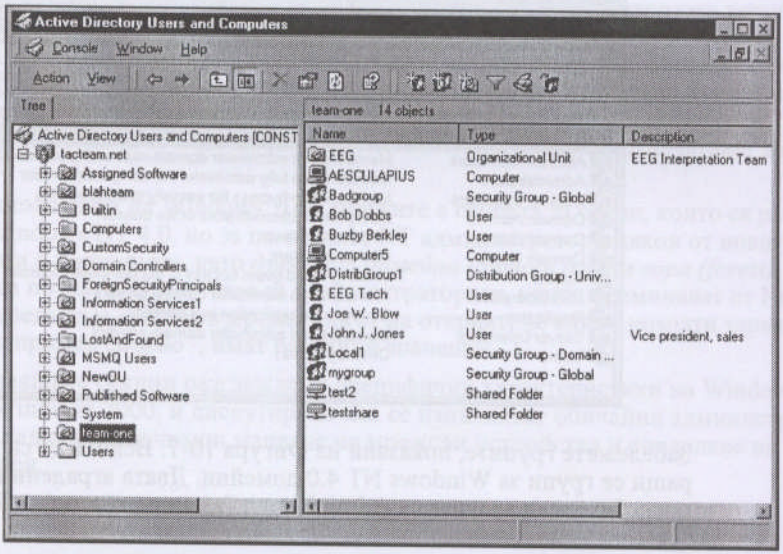
Windows 2000 домейните не притежават PDC или BDC контролери. Всички контролери на домейни притежават копие на дяла Active Directory, а промени могат да се правят в който и да е домейн контролер. След това промените се репликират на останалите домейн контролери.

Администриране на акаунти в Windows 2000

Административните задачи в Windows 2000 използват обща основа – *Microsoft Management Console (MMC)*. Този инструмент използва *snap-in модули* – такива модули, които съдържат инструментите за специфични административни функции. Потребителите и групите се създават и управляват чрез snap-in модула за MMC, наречен Active Directory Users and Computers. Можете да го стартирате, като изберете Start, Programs, Administrative Tools, Active Directory Users and Computers. Вижте Фигура 10-8.

Windows 2000, за разлика от Windows NT 4.0, ви позволява да поставяте обекти, като потребители и ресурси, в контейнерен обект, наречен *организационни единици (organizational units – OUs)*. Можете да делегирате на потребител или на група административна власт над всяка OU. Това позволява много по-голяма грануларност на контрола, отколкото беше възможно в Windows NT 4.0.

Фигура 10-8 *Потребителските и груповите акаунти в Windows 2000 се администрират чрез MMC snap-in модула Active Directory Users and Computers.*



Мапване на устройства в Windows мрежи

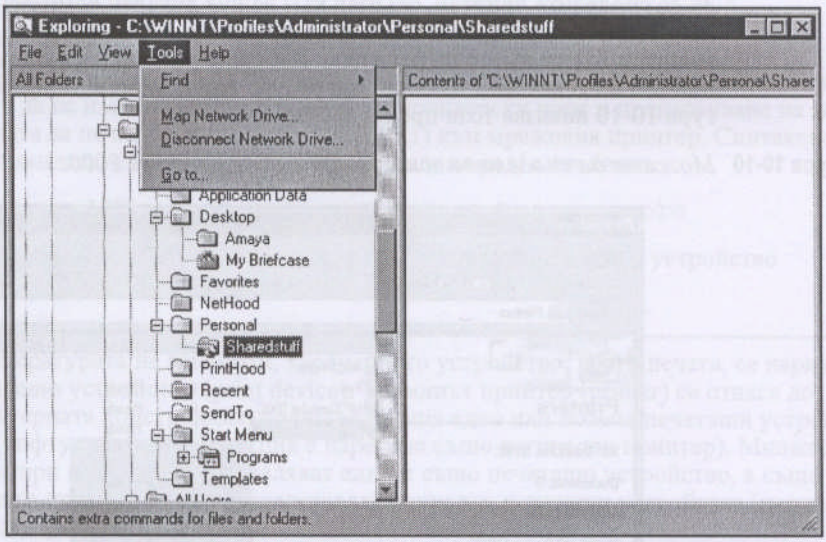
Мапването на мрежово устройство в Windows е лесно. Можете да го направите по два начина:

- Чрез използване на Windows Explorer
- Чрез използване на командата **net use**

Мапване на устройство в Windows Explorer

За да мапнете устройство с Windows Explorer, е необходимо само да достигнете до папката на отдалечената машина с помощта на Windows Explorer (изберете Network Neighborhood, *име на сървър*, *име на споделена папка*), отворете менюто Tools, след което изберете Map Network Drive, както е показано на Фигура 10-9. Забележете, че ако сте инсталирали Internet Explorer 4.0 или по-нова версия, друга опция е да щракнете с десния клавиш на мишката върху името на споделената папка и след това да изберете командата Map Network Drive от появилото се контекстно меню.

Фигура 10-9 *Можете да мапнете мрежово устройство в Windows NT 4.0, като използвате Windows Explorer.*



Мапнатото устройство се появява под формата на назначена буква на устройство в левия панел на Explorer, заедно с вашите флопидискови устройства, CD устройства и дяловете от твърдия ви диск. Можете да осъществявате достъп до това устройство от Windows Explorer, My Computer, както и от вашия десктоп, ако там създавате shortcut.

Мапване на устройство с командата net use

Друг начин за мапване на устройство в операционните системи Windows е чрез *път, използващ конвенцията за универсални имена (Universal Naming Convention – UNC)*. Можете да идентифицирате споделения ресурс чрез следния синтаксис:

```
\\име_на_компютър\име_на_споделен_ресурс
```

За да мапнете мрежово устройство към споделения ресурс, въведете следното на командния ред:

```
net use буква_на_устройство:
\\име_на_компютър\име_на_споделен_ресурс
```

Ако ви е удобно да извършвате администрирането от командния ред, може би ще предпочетете да използвате командата **net use**, вместо да мапвате устройства чрез Windows Explorer.

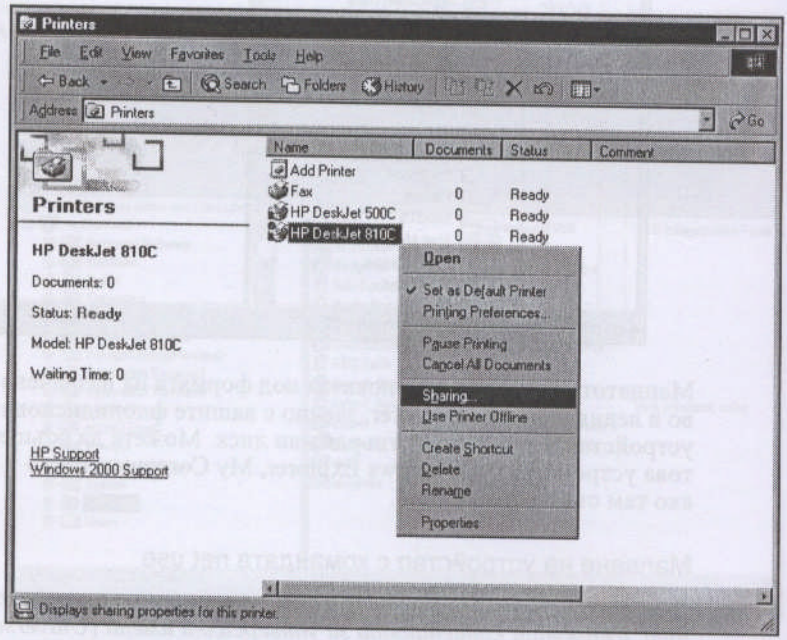
Споделяне на принтери в Windows мрежи

Споделянето на принтери и свързването към тях в Windows мрежа е просто. В следващите секции разглеждаме как се споделя локален принтер (такъв, който е свързан физически към вашата машина) и как да се свързвате към споделен принтер в мрежата.

Споделяне на локален принтер

За да споделите принтер, свързан към вашия локален компютър, отидете в папката Printers, достъпна от Control Panel, след което щракнете с десния бутон на мишката върху името на принтера. Изберете Sharing, щракнете върху Shared as и после въведете име на споделен ресурс или приемете подразбиращото се. Фигура 10-10 показва този процес в Windows 2000.

Фигура 10-10 *Можете да споделите локален принтер в Windows 2000.*



Свързване към поделен принтер

Както при мапването на мрежови устройства, има два начина да се свържете към споделен мрежов принтер: като използвате съветника Add Printer Wizard, или като използвате командата **net use** от командния ред.В следващите секции разглеждаме подробно всеки от методите.

Използване на съветника Add Printer Wizard Най-лесният начин да използвате отдалечен принтер в Windows е да го добавите със съветника Add Printer

Wizard. За да направите това, щракнете двукратно иконата Add Printer в папката Printers и следвайте инструкциите.

ЗАБЕЛЕЖКА Microsoft използва *съветници (wizards)*, представляващи систематична поредица от диалогови прозорци, предназначени да ви водят през множество административни задачи.

Когато съветникът приключи, мрежовият принтер се появява във вашата папка Printers, след което трябва да можете да печатате на него от вашите приложения така, все едно че това е локален принтер.

Заданията за печат се *спулират* (съхраняват се в паметта или на твърдия диск) „изчаквайки на линия" да бъдат отпечатани. Списъкът от чакащи задания за печат се нарича *принт спул (print spool)*.

Използване на net use за прихващане на принтерски порт Командата **net use** може да се използва за прихващане на принтерски порт и пренасочване на заданията за печат от локалния порт (LPT1) към мрежовия принтер. Синтаксисът за командата, която се въвежда на командния ред, е следният:

```
net use LPT1: \\име_на_компютър\име_на_споделен_ресурс
```

име_на_компютър е принт сървърът, към който печатащото устройство (*име_на_принтер*) е свързано физически.

СЪВЕТ В литературата на Microsoft, хардуерното устройство, което печата, се нарича печатащо устройство (print device). Терминът принтер (printer) се отнася до софтуерната конструкция, представляваща едно или повече печатащи устройства (софтуерната конструкция е наречена също логически принтер). Множество принтери могат да представляват едно и също печатащо устройство, а също така един принтер може да представлява няколко печатащи устройства (нарича се *пул от принтери*).

NetWare мрежи

Както при Windows NT и Windows 2000, има съществени разлики в администрирането на различните версии на NetWare. Въпреки че множество мрежи все още използват NetWare 3.*x* сървъри, най-новата версия е NetWare 5.1.

ЗАБЕЛЕЖКА Преди версия 5, NetWare сървърите изискваха протоколния стек IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange). NetWare 5 е първата версия, способна да работи с „чист IP", т.е. протоколния стек TCP/IP (Transmission Control Protocol/Internet Protocol).

NetWare терминология

Novell използва множество термини, които може и да не са познати на хората, нямали „контакт" с продукти на NetWare. Например терминът *bindery* може и да ви звучи мистериозно, но всъщност това е само една база данни, подобна на SAM в Windows NT домейн контролерите.

NetWare 3.x и базата данни Bindery

NetWare 3.x използва база данни, наречена bindery, на всеки сървър. Всяка bindery база съхранява информацията за акаунтите за сигурност само за тази машина. Ако в мрежата има два (или повече) NetWare сървъри, потребителят трябва да има акаунт на всички сървъри, за да има достъп до техните споделени ресурси. Няма репликиране на информацията за акаунтите. Това прави администрирането да бъде с нарастваща трудност, когато се добавят още сървъри към мрежата.

NetWare версия 3.11 въведе поддръжка за допълнително инсталиращи се софтуерни компоненти, наречени зареждаеми модули за NetWare (NetWare loadable modules – NLMs). Тези инструменти и драйвери се инсталират на сървъра за подобряване на неговата функционалност.

NetWare 4.x и NDS

NetWare 4 въведе сложна директорийна услуга, наречена NDS (съкращение от Novell Directory Services),която разреши административните проблеми, причинени от наличието на индивидуални бази данни за сигурност на всеки сървър. NDS е разпределена база данни, позволяваща на потребителите да се логват на който е да е сървър с един потребителски акаунт и да осъществяват достъп до всички мрежови ресурси. Базата данни bindery е плоска; NDS е йерархична и организирана като дърво. Всъщност Novell нарича мрежовите ресурси, като потребители, групи, принтери и томове, *листни обекти (leaf objects)*.

NDS беше пусната преди Active Directory на Microsoft. Двете имат много общи неща, включително концепцията за организационни единици (OU единици) и способността за откриване на обекти в дървовидната директорийна структура, без да се налага да се знае къде ресурсите са разположени физически в мрежата. И NDS, и Active Directory са директорийни услуги, съвместими с протокола LDAP (Lightweight Directory Access Protocol). (Ще научите за LDAP в Глава 11.)

ЗАБЕЛЕЖКА Значенията на термините „дърво“ (tree) и „корен“ (root) са различни в NetWare спрямо Windows 2000 или UNIX.

Администриране на акаунти в NetWare 4.x

Когато инсталирате NetWare 3.x, се създават два различни акаунта: Guest и Supervisor. Акаунтът Guest има ограничен достъп, а акаунтът Supervisor е административен акаунт. NetWare 4 и 5 имат само един подразбиращ се акаунт, наречен Admin.

Акаунтите в NetWare 4.x се създават и управляват с един от двата инструмента:

- **NetWare Administrator** – Работи от Windows клиент, на който се изпълнява Novell NDS клиентски софтуер
- **NETADMIN** – Текстово-базиран инструмент, който може да се стартира от DOS

NetWare 5.x

NetWare 5.x осигурява графична, базирана на Java административна конзола, наречена ConsoleOne, която позволява отдалечено администриране. Тя наподо-

бява интерфейса X Window в UNIX и е проектирана да осигури рамката за административните инструменти на NetWare по същия начин, по който MMC осигурява рамка в Windows 2000. NetWare 5 може да се администрира през стандартната конзола от командния ред или от базирана на менюта програма, наречена Monitor.

NetWare 5.1 въвежда NetWare Management Portal – Web-базиран инструмент, позволяващ ви да управлявате NetWare 5.1 сървъри от клиентска машина през Web браузър.

NetWare клиенти

NetWare е сървърна операционна система. Клиентските работни станции трябва да изпълняват настолна операционна система, за която е наличен NetWare клиентски софтуер. Novell прави клиентски софтуер за DOS и всички версии на Windows, а Microsoft притежава NetWare клиент в своите Windows операционни системи. За Macintosh и Linux съществуват NetWare клиенти от независими производители.

Що се отнася до операционни системи като BeOS, които не притежават NetWare клиентски софтуер, пак можете да осъществявате достъп до NetWare сървъри, като използвате SMB (Server Message Block) клиентска поддръжка. SMB клиентската поддръжка ви позволява да преминавате през Linux компютър, изпълняващ едновременно Samba софтуер и Linux NetWare клиент. Дискутиране Samba в Глава 13.

ЗАБЕЛЕЖКА Можете да използвате или Microsoft Client for Netware (наречен Client Services for NetWare [CSNW] в Windows NT и Windows 2000) или клиентският софтуер на Novell, но не *можете* да изпълнявате и двата клиента на една машина. Novell клиентът осигурява по-голяма функционалност от вградения Microsoft клиент.

Когато инсталирате и конфигурирате NetWare клиентски софтуер, трябва да осигурите следната информация:

- **За NetWare 3.x** – Предпочитаният сървър, който се избира от падащ списък с налични сървъри
- **За NetWare 4/5.x** – Предпочитаното дърво и контекст

Мапване на устройства в NetWare мрежи

Мапването на устройство на NetWare сървър може да се направи чрез Windows Explorer. Трябва да следвате същия процес, описан за мапването на устройства в мрежа на Microsoft, като вашите NetWare клиентски машини работят под Windows 95, 98, NT или 2000.

Можете да мапнете устройство и от командния ред, като използвате командата **map**. Синтаксисът е следният:

```
map име_на_устройство:=сървър\том:директория\поддиректория
```

Клиентският софтуер на Novell също така има функционалност за мапване на устройства, която ви позволява да мапвате устройство като главно (root) или като устройство за търсене (search drive).

Споделени принтери в NetWare мрежи

За да печатате на мрежов принтер, можете да използвате командата **capture**, за да пренасочите заданията за печат от локалния принтерски порт. Синтаксисът е следният:

```
capture L=<номер_а_порт> Q=<име_на_опашка> P=<име_на_принтер>
```

В NetWare, *опашката на принтера (printer queue)* представлява съхранените задания за печат, чакащи своя ред за отпечатване. Това е същото като принт спула в Windows мрежите.

UNIX и Linux мрежи

UNIX мрежовата операционна система съществува от доста години. Тя беше разработена през 1969 година, като се разви в множество варианти. Тъй като сорс кодът е отворен (т.е., достъпен е безплатно за всеки, който иска да го модифицира) и понеже е написан на популярния език за програмиране C, то бизнес организациите, академичните институции и дори отделните личности могат и разработват свои собствени версии.

UNIX операционните системи се използват в работни станции от висок клас, като например машините на Silicon Graphics и Sun. UNIX може да работи като операционна система с команден ред или с графичен потребителски интерфейс (graphical user interface – GUI), като X Window.

Инициативата на отворения код

Инициативата на отворения код (Open Source Initiative) осигурява търговска марка за софтуерните разработчици, желаещи да споделят своя код с други, които след това са свободни да модифицират и да редистрибутират кода. За да използва търговската марка, софтуерът трябва да отговаря на определени критерии: той трябва да се дистрибутира безплатно без ограничения, а сорс кодът трябва да е достъпен. Примери за подобен софтуер включват Linux, BSD версията на UNIX, системата X Window и приложенията, разработени под „шапката“ на проекта GNU. Web сайтът на инициативата на отворения код се намира на адрес www.opensource.org.

Linux е UNIX-базирана операционна система, предназначена да работи на Intel и съвместими с Intel PC-та. Линус Торвалдс разработи тази система в началото на 1990-те. Подобно на UNIX, Linux е операционна система с отворен код, като съществуват множество различни вариации. Освен това, подобно на UNIX, Linux може да изпълнява графичния интерфейс X Window, както и други графични интерфейси, като Gnome и KDE.

В следващите секции дискутираме UNIX терминологията, някои от наличните дистрибуции на UNIX и Linux, а също и как да администрирате акаунти и да извършвате общи задачи в UNIX и Linux.

UNIX терминология

В UNIX и Linux дистрибуциите, административният акаунт, който се използва за задачи за поддръжка на системата, се нарича *root*. *Bin* и *sys* са акаунти, които притежават и стартират програми.

Сървърните услуги се наричат *демони (daemons)*. Примери за демони включват демона за печат и FTP демона. Съществуват и други термини, характерни за UNIX средата, като много от тях дефинираме в следващите секции на тази глава.

UNIX операционни системи

Съществуват стотици различни версии на UNIX. Някои от най-популярните са следните:

- Berkeley Software Design, Inc. (BSD UNIX, от който са се породили разклонения като FreeBSD)
- Santa Cruz Operation (SCO) UNIX
- Sun Solaris
- AIX (UNIX на IBM)
- HP-UX (UNIX на Hewlett Packard)

Отвореният сорс код е и сила и слабост на UNIX операционните системи. Разработчиците са свободни да подобряват и настройват операционната система, но това води до липсата на стандартизация, което може да разочарова потребителите, администраторите и разработчиците на приложения. Само че това не е толкова зловещо, колкото звучи – доста софтуерни приложения могат да се използват на множество UNIX и Linux платформи.

Въпреки популярността на Windows и NetWare в корпоративните LAN мрежи, по-голямата част от Интернет все още работи на мощни UNIX системи. Въпреки че UNIX обикновено се асоциира със скъп хардуер и се счита за „недружелюбен към потребителя", скорошните разработки промениха този имидж. Поконкретно, появата на Linux в началото на 1990-те отвори вратите на UNIX към света на PC компютрите.

Linux операционни системи

Понякога Linux се нарича „UNIX Lite". Той е предназначен да работи на Intel-съвместими PC-та. (Работи и на RISC машини.) Linux води със себе си предимствата на UNIX, които стават достъпни за домашните компютри и компютрите в малкия бизнес.

Както и при UNIX, съществуват куп версии на Linux. някои можете да си свалите безплатно от Мрежата, а други се разпространяват комерсиално. Следва списък на най-популярните:

- RedHat Linux, разпространяван от RedHat Software
- OpenLinux, разпространяван от Caldera
- Corel Linux
- Slackware
- Debian GNU/Linux
- SuSE Linux

Една неотдавнашна тенденция беше да се създават версии на Linux, побиращи се на една или две дискети. Една такава орязана версия е LOAF (Linux On A Floppy), която се побира на една дискета. DOS Linux още една малка Linux мрежова операционна система, която може да се инсталира на съществуваща

DOS система. Трета дистрибуция, наречена Coyote Linux, е малка, специализирана, и е предназначена за споделяне на Интернет връзки.

Списък на текущите Linux дистрибуции можете да намерите на Web сайта на адрес www.linux.org.

Администриране на акаунти в UNIX и Linux

Мрежовата информационна система (Network Information System – NIS), разработена от Sun Microsystems, може да бъде използвана за управление на UNIX сървъри. NIS позволява достъп до мрежовите ресурси с едно логване, което ще рече, че потребителят може да се логне веднъж (с едно име на акаунт и една парола), след което да осъществява достъп до ресурсите на компютрите из цялата мрежа.

ЗАБЕЛЕЖКА Важно е да се отбележи, че в UNIX, за разлика от Windows, командите и имената са *чувствителни към регистъра на буквите (case-sensitive)*; това ще рече, че за операционната система файловото име „MyDocs“ не е същото като „mydocs.“ Всъщност тези два файла могат да съществуват в една и съща директория.

Може да сте се натъквали на това, докато сте въвеждали URL адреси във вашия Web браузър. Ако Web сървърът, към който се свързва вашият Web браузър, е UNIX-базиран, трябва да въведете адреса *точно както е показан*. Ако една Web страница е с име „WebSite.html“, а вие въведете „Website.html“, ще получите съобщение за грешка „file not found“ (файлът не е намерен).

Създаване и управление на потребителски акаунти

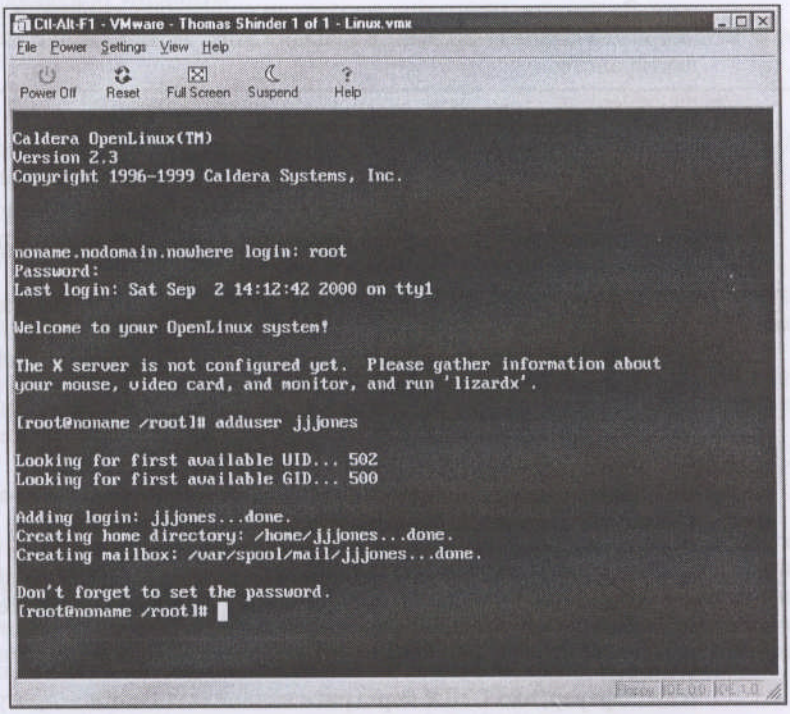
За да добавите нов потребителски акаунт в UNIX и Linux, трябва да използвате командата **adduser**, както е показано на Фигура 10-11. Трябва да сте се логнали като root или като supervisor, за да създадете нов акаунт. Синтаксисът е следният:

```
име_на_потребител:/# adduser
```

Потребителските акаунти се управляват чрез редактиране на файла /etc/passwd. Някои UNIX/Linux версии осигуряват *скриптове*, които ви водят в процеса, а файла можете да редактирате и ръчно, като използвате текстов редактор. (vi, Pico и Emacs са популярни текстови редактори за UNIX/Linux.)

ЗАБЕЛЕЖКА *Скриптовете* са малки програми; когато използвате скрипт, за да управлявате потребителски акаунти, скриптът задава поредица от въпроси, а вашите отговори определят промените, извършвани във файла passwd. Скриптовете в UNIX/Linux са еквиваленти на съветниците в Windows.

Фигура 10-11 *Командата **adduser** се използва за създаване на нови потребителски акаунти на UNIX и Linux сървъри.*



Ръчното редактиране на файла passwd може да е сложно; то включва въвеждане на информация за потребителя с този синтаксис:

```
deb://BimowSOF9Ev:503:100:Deb Shinder:/home/deb:/bin/bash
```

Таблица 10-1 показва полетата, включени при редактиране на файла passwd.

Таблица 10-1 *Частите на един запис от файла passwd*

Поле	Обяснение
deb	Име на потребител
BimowSOF9Ev	Парола (показва се във файла в криптирана форма, така че ако някой отвори файла, да не получи достъп до паролите на потребителите)
503	Потребителски идентификатор
100	Групов идентификатор
Deb Shinder	Пълното име на потребителя
/home/deb	Домашна директория на потребителя
/bin/bash	Подразбиращ се shell на потребителя

ВНИМАНИЕ Освен информация за потребителите, файлът passwd съдържа информация за конфигурирането на системата, така че трябва да внимавате, когато го редактирате. За щастие, много производители осигуряват графични програми, като например User Configurator в RedHat Linux, за изпълнение на задачите по редактирането.

UNIX групи

Както Windows и NetWare, така и UNIX поддържа групи за управление на потребителските акаунти спрямо ресурсите. UNIX групите работят много подобно на локалните групи в Windows NT и Windows 2000.

В UNIX групи се добавят чрез командата **addgroup**, а управлението на групите става чрез модифициране на файла /etc/groups. Ако вашата UNIX дистрибуция включва графични инструменти за тези задачи, много по-лесно и по-безопасно е да използвате тях, отколкото командния ред.

UNIX клиенти

Файловата система клиент/сървър, използвана от повечето варианти на UNIX файловите сървъри, е Network File System (NFS), която беше разработена от Sun Microsystems. Тя може да бъде инсталирана на Windows клиенти с помощта на софтуер като Solstice Network Client от Sun. NFS изисква TCP/IP, или друг NFS клиентски софтуер, за файлов трансфер. Операционните системи Windows не включват NFS клиент.

Windows клиентите могат да осъществяват достъп до UNIX сървъри без клиентски софтуер, ако UNIX сървърите изпълняват Samba – програма, която използва протокола SMB, работещ в приложния слой. Windows компютрите използват SMB за файлов достъп по мрежата. Samba им позволява да виждат файловата система на UNIX.

Мапване на устройства в UNIX мрежи

Мапването на устройство към UNIX дял се прави чрез използване на командата **mount**. Синтаксисът е следният:

```
mount име_на_сървър:/директория/поддиректория/локална_директория
```

Обозначението на локалната директория, която сочи към отдалечения споделен ресурс, посочен от първата чат на командата, се нарича *точка за монтиране на директория (directory mount point)*. Местоположението на точката за монтиране трябва вече да съществува, преди да мапнете споделения ресурс към нея.

Споделени принтери в UNIX мрежи

Можете да печатате на принтер, свързан към UNIX принт сървър, като използвате командата **lpr**. За да изпълни заявката за печатане, принт сървърът трябва да изпълнява lpd софтуер (*line printer daemon – демон за линеен принтер)*. Синтаксисът за печатане на UNIX принтер е следният:

```
lpr -P име_на_принтер име_на_файл
```

Ако въведете командата без име на принтер (т.е., **lpr** *име_на_файл*), заданието за печат се изпраща на подразбиращия се принтер. Други команди за печат под UNIX включват следните:

- **lpq** – Позволява ви да видите опашката за печат или да изведете заданията
- **lprm** – Премахва файл от опашката за печат

За взаимодействие при печат, Windows NT и Windows 2000 включват TCP/IP Printing Services и Print Services for UNIX.

Други мрежови операционни системи

По-голямата част от PC мрежите работят с една или повече от трите мрежови операционни системи, дискутирани в тази глава. Въпреки това съществуват и се използват и друго мрежови операционни системи. Такива например са Banyan VINES, OS/2 Warp Server, Apple NOS и LANtastic – всички те са алтернативни операционни системи, осигуряващи централизирано администриране на мрежата. Дискутираме всяка от тях в следващите секции на тази глава.

Banyan VINES

Banyan правят продукт, наречен Virtual Networking System (VINES). Това е вариация на UNIX, използваща собствена файлова система –VINES – вместо NFS. Въпреки че нейната популярност се стопи и сега тя се използва предимно в академични среди, VINES все още е от значение, защото тя въведе първата истинска директорийна услуга – StreetTalk. Дискутираме StreetTalk в Глава 11.

OS/2 Warp Server

За много хора OS/2 е позната като „настолната операционна система на IBM, която загуби състезанието с Windows". OS/2 почти изчезна, след като IBM спря да издава нови версии през 1996 година. Въпреки че IBM престана да поддържа настолната операционна система, компанията продължи да развива своя OS/2 сървърен продукт. Тъй като в момента фокусът е съсредоточен върху електронната търговия (e-commerce), IBM нарича операционната система OS/2 Warp Server for E-business. OS/2 се използва предимно в банкирането и финансовите индустрии.

Warp Server осигурява функционалност на файлов и приложен сървър, като използва файлова система, наречена JFS (Journaled File System). Тя е проектирана за широкомащабни приложения и повишена сигурност. NFS позволява връзка с AIX или други базирани на UNIX сървъри.

AppleShareIP

Apple Macintosh компютрите притежават вградена поддръжка на равноправна мрежа. Въпреки че от Apple направиха сървърен продукт, наречен AppleShareIP, той никога не придоби популярност извън една малка пазарна ниша. AppleShareIP предлага FTP, POP3/SMTP пощенски сървър, Web сървър и функционалност на файлов и принт сървър.

LANtastic

Въпреки че не е сървърно-базирана мрежова операционна система, LANtastic се използва от множество малки бизнес организации за свързване на DOS и Windows PC-та, така че да могат да споделят файлове, модеми и Интернет връзки. LANtastic осигурява възможности за управление на равноправна мрежа, позволяващи ви да свържете до 500 машини – далеч повече, отколкото е възможно в традиционната среда на една работна група.

Обобщение

В тази глава дискутирахме концепциите, свързани с мрежовата администрация, както и характеристиките на популярни мрежови операционни системи. Започнахме с разглеждане на разликите между мейнфрейм-базираните среди и клиент/сървър средите, базирани на PC-та. След това описахме характеристиките на типичната клиент/сървър среда и научихме как клиент/сървър приложенията, като например SQL Server и други продукти за бази данни, осигуряват оптимизирано споделяне на процесорното натоварване по мрежата.

Открихте колко е важно правилното управление на споделените ресурси, гарантиращо, че авторизираните потребители могат да откриват и да осъществяват достъп до споделени ресурси, а неавторизираните не могат. Дискутирахме спецификите на споделянето на файлове, папки, принтери, приложения и Интернет връзки.

След това разгледахме всяка от големите три мрежови операционни системи с някои подробности и обсъдихме техните инструменти за управление, както и специфичната за тях терминология. Освен това дискутирахме как се създават потребителски акаунти, как се мапват мрежови устройства и как се прихващат принтерски портове в Windows NT, Windows 2000, NetWare и UNIX/Linux.

Завършихме с поглед към някои от по-малко използваните мрежови операционни системи. В обзора бяха включени Banyan VINES, OS/2 Warp Server, AppleShareIP и LANtastic.

Сега, след като сте запознати с популярните сървърни операционни системи, в следващата глава ще изследваме един важен компонент на съвременните сървърни продукти – директорийните услуги.

Допълнителни източници

Можете да откриете информация за поддръжка и описания на продуктите Microsoft Windows NT и Windows 2000 Server на адрес www.microsoft.com.

Информация и ресурси за NetWare могат да се открият на Web сайта на Novell – www.novell.com.

Повече информация за дистрибуциите на Linux можете да намерите в Linux Online! на адрес www.linux.org.

Можете да свалите FreeBSD и да откриете ръководства, наръчници и списък с често задавани въпроси на адрес www.freebsd.org.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Кои мрежови приложения оползотворяват процесорната мощ на сървъра, за да оптимизират задачи като заявки към бази данни?

a Централизирани приложения
b Front-end приложения
c Клиент/сървър приложения
d Споделени приложения

2 Кой ресурс се прави достъпен, така че останалите потребители да могат да осъществяват достъп до него по мрежата?

a Сървър
b Споделен ресурс
c Клиент
d Дистрибутиран ресурс

3 Какво е името на типа сигурност, при която всеки потребител има потребителско име и парола, маркер за достъп и списък за контрол на достъпа, за да се определи дали даден потребител може да осъществи достъп до специфичен мрежов ресурс?

a Сигурност на ниво потребител
b Сигурност на ниво парола
c Сигурност на ниво споделен ресурс
d Сигурност на ниво работна група

4 Кои от следните характеристики притежава главният административен акаунт (който може да се нарича Administrator, Admin, Supervisor или Root в зависимост от операционната система)? (Изберете всички верни отговори.)

a Създава се по време на инсталиране на операционната система.
b Има само ограничен достъп до мрежови ресурси.
c За него трябва да се зададе силна парола.
d Може да се използва за създаване на други потребителски акаунти.

5 Кое от следните може да се използва безопасно като потребителско име в която и да е от трите основни мрежови операционни системи? (Изберете всички верни отговори.)

a joesmith
b Joe Smith
c J+Smith
d SMITH007

6 В една мрежа, базирана на Windows сървър, как се нарича групата от компютри, потребители и ресурси, формиращи основна административна граница?

a Корен (Root)
b Дърво (Tree)
c Домейн (Domain)
d Гора (Forest)

7 Как се казва инструментът, с който в един Windows NT 4.0 домейн контролер се управляват акаунтите на потребителите и се задават политики за пароли?

a User Administrator
b User Manager for Domains
c User Manager
d Account Administration Tool for Domains

8 Как се казва директорийната услуга, в която информацията за акаунтите за сигурност се съхранява в Windows 2000 мрежа?

a NDS
b LDAP Directory Service
c Active Directory
d Directory Access Service

9 Каква база данни съхранява информация за сигурност в един NetWare 3.x сървър?

a Root
b NDS
c Организационна единица (OU)
d Базата bindery

10 Кое от следните изказвания е вярно за операционните системи от семейството на UNIX? (Изберете всички верни отговори.)

a Файловите операции са чувствителни към регистъра на буквите.
b Главният административен акаунт се нарича Supervisor.
c Сървърните услуги се наричат демони.
d Групите в една UNIX система работят много подобно на глобалните групи в Windows NT 4.0.

Глава 11

Директорийни услуги

Една важна част от модерни мрежови операционни системи (network operating systems — NOSs) е директорийната услуга. *Директорийната услуга* (*directory service*) позволява съхраняването и осъществяването на достъп до информация относно мрежови ресурси, мрежови акаунти и мрежови услуги.

В тази глава ще научите за директории[1] и директорийни услуги, както и за тяхната нарастваща роля в съвременните мрежи. Дискутираме стандартите и спецификациите, управляващи реализацията на директорийните услуги. По-специално изследваме OSI (Open Systems Interconnection) спецификациите X.500, както и стандартите DAP (Directory Access Protocol) и LDAP (Lightweight Directory Access Protocol).

След това разглеждаме Directory-Enabled Networking (DEN) — инициатива, подкрепяна от Microsoft Corporation и Cisco Systems. DEN се фокусира върху използването на директорийни услуги, за да подобри мениджмънта на мрежовите устройства, ресурси и услуги.

Ще научите за най-популярните директорийни услуги, работещи в мрежови операционни системи за PC: Novell Directory Service (NDS) на Novell и Active Directory на Microsoft. Също така разглеждаме директорийни услуги, работещи на други платформи, като например Sun Microsystems' Directory Services (SDS) на Sun и AS/400 Directory Services на IBM. Освен това дискутираме интероперативността на различните директорийни услуги и изследваме идеята за директорийна услуга за глобалния Интернет.

Какво представляват директориите и директорийните услуги?

Използващите директории услуги изискват два компонента: самата директория и услуга, която я управлява. Нека ги разгледаме по-подробно.

---

[1] Термините *директория* и *директорийна услуга*, наложили се в българския език, не са съвсем ясни; точните им наименования са съответно *справочник* и *справочна услуга* (както ще разберете от обясненията по-нататък). Бедата е, че на английски терминът е directory (справочник) и в българската терминология е влязъл като чуждица, водейки до появата на думата *директория* — б.р.

Какво е директория?

Една *директория (справочник* – вижте бележката под линия на предходната страница*)* организира информация. Ежедневно използваме директории (справочници). Например използваме телефонния указател (telephone directory), който организира имената на абонатите на телефонната услуга в азбучен ред със съответните им адреси и телефонни номера.

В света на компютрите, една директория (справочник) може да е много различни неща. Вероятно сте запознати с използването ѝ във файловите системи, където директорията представлява сбор от файлове, групирани под едно идентифициращо ги име. Когато обаче говорим за директорийните услуги, използвани от мрежовите операционни системи, става въпрос за различна концепция. В този контекст директорията (справочникът) е специален тип база данни. Тя може да съдържа различни типове информация. (От тук насетне, навсякъде, където се споменава за директория, имайте предвид справочник – б.р.)

В една обектно-ориентирана операционна система директорията съдържа *обекти,* които имат *атрибути.* Например един потребителски акаунт, представлява обект, който може да се съдържа в директория. Неговите атрибути ще включват потребителското име, истинското име на потребителя, паролата за акаунта и друга информация за акаунта, както е показано на Фигура 11-1.

Фигура 11-1 *Директориите съхраняват обекти, които имат атрибути.*

За да разберете по-добре концепцията за директориите и атрибутите, нека се върнем към нашия пример с телефонния указател. В този случай името на абоната на телефонната услуга се явява обектът, а атрибутите му са адресът и телефонният номер. Виждате, че атрибутите до известна степен описват самия обект.

СЪВЕТ Директорийните обекти могат да притежават множество атрибути. Някои е възможно да са задължителни (например всеки потребителски акаунт трябва да има потребителско име), а други – опционални (например може да има поле за въвеждане на заеманата от потребителя длъжност, но то би могло да бъде оставено празно).

Обектните класове дефинират атрибутите, налични за един клас, както и неговото място в директорийната структура или йерархия. Дефиницията на обектните класове, заедно с изискваните и позволените ресурси на всеки от тях, се нарича *схема (schema)*. Мрежовата операционна система може да позволи на авторизираните администратори да модифицират или да разширяват схемата, за да добавят нови обектни класове и атрибути.

Какво представляват директорийните услуги?

Директорийните услуги предоставят начин за съхранение, обновяване, откриване и защита на информацията в директорията. Директорийните услуги могат да бъдат *локални* (т.е., ограничени до една машина) или *глобални* (т.е. да осигуряват услуги на множество машини). Ако самата информация е разпръсната на множество машини, тя се нарича *дистрибутирана.*

Използване на директорийни услуги

Ползите от използването на директорийни услуги в една мрежа включват следното:

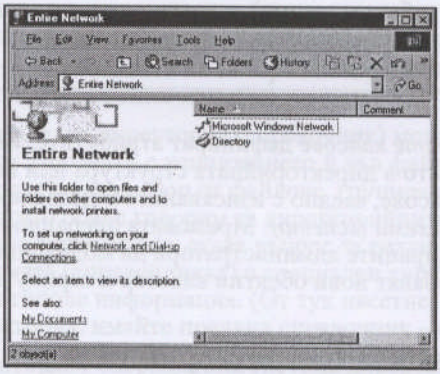
- Данните могат лесно да бъдат организирани.
- Данните могат лесно да бъдат обезопасени.
- Данните могат лесно да бъдат откривани и да се осъществява достъп до тях.

За да разберете ползите от използването на директорийни услуги, нека първо погледнем към традиционния начин за осъществяване на достъп до мрежови ресурси. При традиционния начин, споделените файлове и папки се съхраняват на твърдите дискове на отделните работни станции или файлови сървъри. За да се свърже със споделения ресурс, потребителят трябва да знае неговото местоположение.

Една директорийна услуга елиминира това изискване. Споделените ресурси се публикуват в директорията, а потребителите могат да ги откриват и да осъществяват достъп до тях, без изобщо да знаят на коя машина ресурсът е разположен физически. Фигура 11-2 показва прозореца за браузване на мрежата в Windows 2000. Както можете да видите, той ви дава две възможности:

- **Да браузвате Microsoft Windows мрежата по традиционния начин** – Тази опция ви позволява да браузвате споделените ресурси на всяка отделна машина.
- **Да браузвате директорията** – Тази опция показва всички ресурси, публикувани в Active Directory.

Фигура 11-2 *Браузърът на мрежата в Windows 2000 ви позволява да браузвате мрежата по традиционния начин, или да браузвате директорията.*



Пространството от имена на директорията

Пространството от имена (namespace) на директорията се отнася до начина, по който се идентифицират директорийните обекти. Директорийните услуги могат да използват два различни типа пространства от имена:

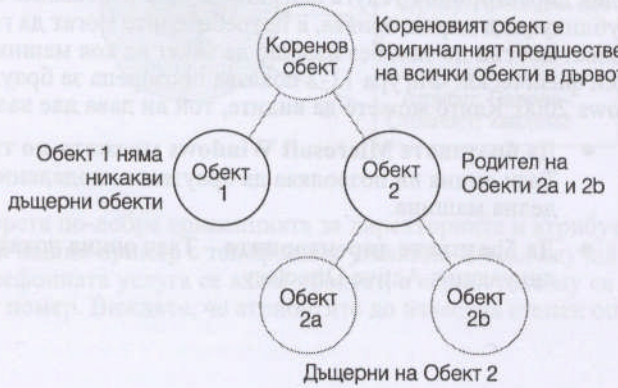
- Плоско пространство
- Йерархично пространство

Директорийната услуга на Windows NT (NTDS) и базата данни *bindery* на NetWare 3.*x* използват плоско пространство от имена. По-новите и по-усъвършенствани директорийни услуги използват йерархична структура. Често пъти тази структура се нарича *дърво*. Понякога се нарича и *инверсно дърво* (тъй като коренът се намира най-отгоре). Повечето компютърни файлови системи използват този тип структура.

Структура на дървото от директории

В директорийното дърво обектите могат да имат родителски и дъщерни обекти. *Родителският обект* се намира точно над даден обект в дървото, а *дъщерният обект* е точно под него, както е показано на Фигура 11-3.

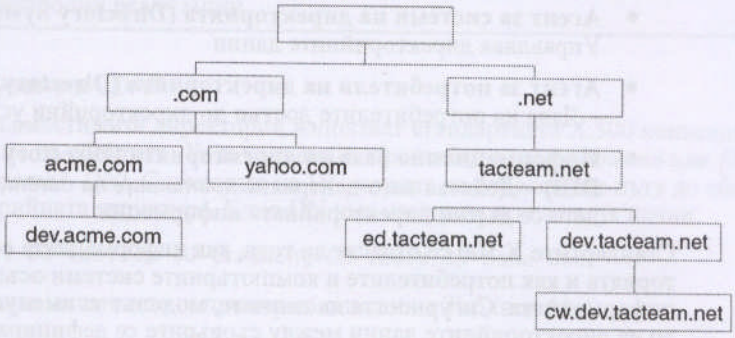
Фигура 11-3 *В едно йерархично дърво, обектите имат родители и деца.*



Конвенции за именуване на директории

Може би сте забелязали на Фигура 11-3, че дъщерните обекти на Обект 2 имат имена, включващи името на родителя. Това се нарича *родствено пространство от имена (contiguous namespace)*. Както научихте в Глава 8, „Мрежови протоколи и услуги", DNS (Domain Name System) имената са структурирани по същия начин. Структурата им е същата, защото DNS е директорийна услуга, използваща йерархично пространство от имена. Фигура 11-4 показва DNS пространство от имена.

Фигура 11-4 *DNS е директорийна услуга с йерархично пространство от имена.*



На фигурата, DNS коренът се представлява от точка. Под корена са двете деца – домейните .com и .net. Всеки има дъщерни домейни, които пък от своя страна също могат да имат деца и внуци. Забележете, че всяко поколение включва пълното име на своя родител като част от своето.

ЗАБЕЛЕЖКА Структурата на DNS домейните, използвана в Интернет, е същата, каквато се използва в Windows 2000 Active Directory – само без точката за кореновия домейн. Ще научите повече за Active Directory по-нататък в тази глава.

Дървовидната аналогия може да се продължи. Например NDS терминологията на Novell нарича обектите в края на всеки клон обекти листа (leaf objects). (Ще научите повече за NDS по-нататък в тази глава.)

Стандарти за директорийни услуги

С цел интероперативност, различните директорийни услуги се нуждаят от общ метод за именуване и сочене към обектите. Без стандарти, всяко приложение използва своя собствена директория, което увеличава използването на дисковото пространство и продуктите на даден производител не могат да използват базата данни, създадена от продуктите на друг производител.

Съвместимостта със стандартите позволява на производителите на директорийни услуги да гарантират, че техните услуги са съвместими както с множество платформи, така и с други директорийни услуги.

В тази секция дискутираме следните стандарти за директорийни услуги:

- OSI спецификациите X.500

- DAP
- LDAP

X.500

X.500 дефинира стандарти за електронна директорийна услуга (Electronic Directory Service – EDS) в ISO 9594. Директорийните услуги, описани в X.500, за проектирани да работят съвместно с X.400 услугите за съобщения.

Една X.500-съвместима директория има три основни компонента:

- **Агент за системи на директорията (Directory System Agent – DSA)** – Управлява директорийните данни
- **Агент за потребители на директорията (Directory User Agent – DUA)** – Дава на потребителите достъп до директорийни услуги
- **Информационна база на директорията (Directory Information Base – DIB)** – Действа като централно *хранилище на данни*, или база данни, където се държи директорийната информация

Стандартите X.500 се отнасят до това, как информацията се съхранява в директорията и как потребителите и компютърните системи осъществяват достъп до информацията. Сигурността на данните, моделът за именуване и репликирането на директорийните данни между сървърите се дефинират от X.500.

X.500 спецификациите дефинират директорийната структура като инверсно дърво, а базата данни е йерархична. Една X.500-съвместима директорийна услуга използва протокола DAP, който дискутираме в следващата секция.

DAP и LDAP

DAP позволява на DUA да комуникира с DSA. DAP дефинира средствата, с които потребителят може да претърсва директорията и да чете, добавя, изтрива и модифицира директорийните записи.

DAP е мощен протокол, но свързаната с него служебна информация, е доста. LDAP беше разработен като поднабор на DAP, който опростява достъпа до директории от тип X.500. LDAP се превърна в популярен стандарт, който интегрира директории от различни производители. LDAP е проектиран да използва по-малко системни ресурси от DAP, и е по-лесен за реализиране. Текущата версия на LDAP е LDAPv3.

LDAPv3 спецификации

RFC 2251 описва спецификациите за LDAPv3, включващи следното:

- Протоколният модел на LDAP
- Моделът за данни на LDAP
- Общи елементи на протокола, като конвенции за именуване, атрибутни типове, както и описания; също така са описани операциите свързване (bind), търсене, добавяне, модифициране и изтриване

Какво е новото в LDAPv3?

LDAPv3 предлага няколко основни подобрения спрямо по-ранните версии на LDAP. Подобрената сигурност е основният фокус на новата версия; LDAPv3 поддържа Secure Sockets Layer (SSL) криптиране между клиента и сървъра, като позволява автентициране на X.509 сертификати.

LDAPv3 също така позволява на сървъра да насочи LDAP клиента към друг сървър, ако самият той не може да отговори на заявката на клиента.

Друга нова възможност е поддръжката на Unicode. Това позволява кодирането на повече многоезични знакови таблици в директорийните атрибути; полезно е за международни реализации.

Конвенции за именуване в LDAP

LDAP-съвместимите директории използват стандартната X.500 конвенция за именуване на обектите. Тази конвенция произвежда *отличително име (distinguished name – DN)*. С помощта на DN можете да отбележите пътя до обект в директорийната структура. Едно DN име изглежда по следния начин:

```
DC=net DC=tacteam OU=training CN=Users CN=John Doe
```

Атрибутите за име в този пример са описани в Таблица 11-1.

Таблица 11-1 *DN атрибути и описания*

DN атрибут	Описание
DC	Име на компонент на домейн (domain component)
OU	Организационна единица (organizational unit)
CN	Общо име (common name)

Директорийните услуги като Active Directory могат да използват също *относителни отличителни имена (relative distinguished names – RDNs)*, които са по-къси версии на DN имената. RDN името е атрибут на обекта. В примера в Таблица 11-1, общото име „John Doe“, което е атрибут на обекта, представлява RDN името.

Два обекта в директорията могат да имат едно и също RDN име. Например можете да имате двама потребителя с RDN „John Doe“, но само ако се намират в различни OU единици или домейни. Едно пълно DN име обаче не може да се споделя от два обекта при каквито и да било обстоятелства.

LDAP-съответстващи и LDAP-съвместими директорийни услуги

Първата LDAP реализация се появи в Мичиганския университет, след което популярността ѝ се разпространи по цял свят. LDAP се превърна в стандарт за Интернет директорийни услуги, защото, за разлика от DAP, той беше разработен да работи по TCP.

Популярните LDAP реализации включват Banyan StreetTalk, Netscape Directory Server, AltaVista Directory и Lucent Internet Directory Server. LDAP-съответстващите (compliant) директории могат да бъдат синхронизирани една с друга дори ако са от различни производители.

И Novell NDS, и Microsoft Active Directory поддържат LDAP клиенти, и използват конвенциите за именуване X.500, въпреки че нито една от двете директорийни услуги не съответства напълно на X.500. Директорийните услуги, които поддържат LDAP клиенти, се наричат *LDAP-съвместими* (*compatible*).

LDAP интероперативност

Популярността на LDAP позволява не само интероперативност (съвместна работа) с всички LDAP-съвместими директории, но и функционалност като front-end за директории, базирани на пълни X.500 стандарти.

Съществуват LDAP клиенти за DOS, Windows, Macintosh, UNIX и системата X Window. Това прави LDAP и X.500 директориите подходящи за корпоративни мрежи, изградени от машини, които работят с различни платформи и операционни системи.

Мрежи с използване на директории

Мрежите с използване на услуги (directory-enabled networks – DENs) се превърнаха в интегрална част от управлението на ресурси на ниво корпоративни мрежи. Възможности като качество на услугата (quality of service – QoS), групуер (groupware) и съвместни изчисления, както и автоматизирането на обработката, повишиха важността от централизирано хранилище, което позволява на потребителите и приложенията да споделят данни.

В миналото, една корпоративна мрежа би имала множество отделни директории; различните приложения използваха свои собствени бази данни, а една и съща информация се случваше да се въвежда много пъти на различни места. Колкото повече се разрастваха мрежите и колкото повече мрежови приложения се реализираха, толкова по-неефективен ставаше методът.

Директорийните услуги, до които може да се осъществява достъп както от приложения, така и от потребители, спестяват време и дисково пространство. Друга движеща сила, стояща зад преминаването към стандартизирани директорийни услуги, е електронната търговия (e-commerce). Директориите се използват в методите за сигурност, които криптират и подписват цифровите транзакции. Тези методи за сигурност се наричат *инфраструктура от публични ключове (public key infrastructure – PKI)*.

Популярни директорийни услуги

Сега, след като знаете някои от концепциите, свързани с директориите и директорийните услуги, ще разгледаме някои специфични реализации. Двете най-популярни директорийни услуги за PC мрежи са Novell NDS и Microsoft Active Directory.

Novell NDS

Версиите на NetWare до 3.*x* включително използват директорийна база данни, наречена bindery. Най-големият недостатък на тази директорийна услуга е нейната локална природа. Всеки NetWare сървър в мрежата трябва да поддържа индивидуална база данни, а всеки потребител е необходимо да притежава акаунт на всеки от сървърите, за да може да използва неговите ресурси.

В следващите секции изследваме структурата на NDS базата данни и дискутираме NDS сигурността, както и NDS съвместимостта в различни операционни системи и хардуерни платформи.

Структура на базата данни NDS

Започвайки с версия 4, NetWare въведе NDS – глобална база данни, която се репликира между сървърите в мрежата. Чрез нея потребителите могат да се логнат в който и да е сървър, след което да осъществяват достъп до ресурсите на всички сървъри.

Базата данни NDS е йерархична и използва схемата с инверсно дърво. Тя може да съдържа два основни типа обекти: *контейнерни обекти (container objects)* и *листови обекти (leaf objects)*. Както се подразбира от имената, един контейнерен обект може да съдържа други обекти в себе си; листовият обект е „крайната точка" на даден клон – самият ресурс. Споделените файлове и принтери са примери за листови обекти. OU единиците са примери за контейнерни обекти.

Сигурност в NDS

NDS позволенията за достъп до обекти се назначават на OU единиците, а потребителите и групите се поставят в тези единици. Можете да промените позволенията на даден потребител, като преместите акаунта му от една OU в друга. Например, ако преместите потребителския акаунт johndoe от OU единицата Training в OU единицата Sales, този потребител вече няма да притежава позволенията за достъп, назначени на Training, но пък се сдобива с всички позволения, дадени на Sales. Това е различно от начина, по който работят позволенията в Microsoft Windows NT и Windows 2000 мрежите. (Ще научите за Windows позволенията по-нататък в тази глава.)

Платформена съвместимост на NDS

Въпреки че по принцип се асоциира с мрежовата операционна система NetWare, NDS може да работи на множество платформи. Novell осигурява NDS за следните платформи:

- NetWare 4 и 5
- Microsoft Windows NT и Windows 2000
- IBM AIX и OS/390
- Caldera OpenLinux
- SCO UNIX
- Sun Solaris

NDS eDirectory е междуплатформеното решение на Novell за интегрирани корпоративни изчисления с приложения, проектирани за работа с директории.

NDS позволява използването на различни протоколи за достъп до директорийната информация, включващи следните:

- Novell Directory Access Protocol (NDAP)
- LDAP
- HTTP (когато се използва Web сървър)

- Open Database Connectivity (ODBC) API
- Active Directory Services Interface (ADSI)

Microsoft Active Directory

С пускането на пазара на Windows 2000 Server, Microsoft направи фундаментални промени в своите мрежови компоненти, които са дори по-драстични от промените, извършени от Novell при преминаването от NetWare 3 към 4. Active Directory заема централно място в тези промени. Докато NDS базата данни на Novell действа като услуга, работеща с мрежовата операционна система, Active Directory на Microsoft действа като приложение, което е дълбоко интегрирано в операционната система.

В следващите секции изследваме структурата на базата данни Active Directory, как Active Directory се интегрира с DNS и Active Directory сървърите, и как информацията от Active Directory се репликира от един домейн контролер на друг.

Структура на базата данни на Active Directory

Информацията в Active Directory се съхранява в три файла:

- Active Directory база данни
- Active Directory отчетни файлове
- Shared System Volume

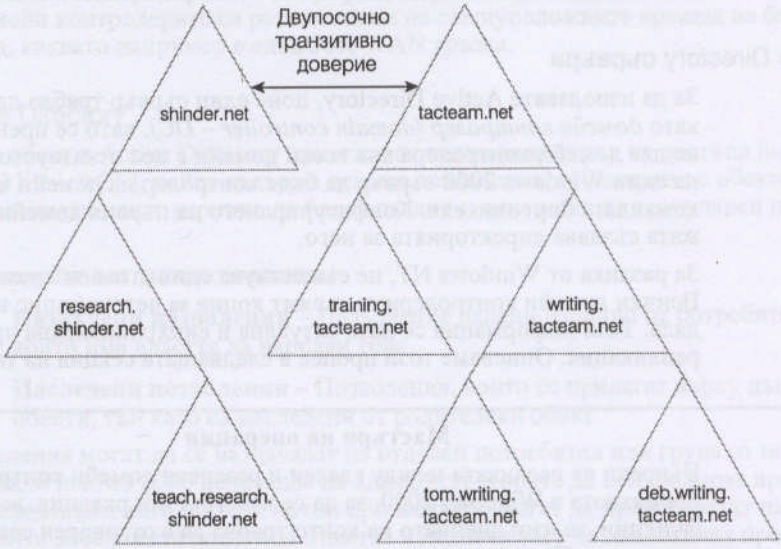
Самата база данни представлява директорията. Отчетните файлове записват промените, извършени в базата данни. Shared System Volume (наричан още Sysvol) съдържа скриптове и *обекти на групови политики* (*group policy objects*) на Windows 2000 домейн контролери. *Груповата политика* е средството, чрез което Windows 2000 администраторите контролират десктопите на потребителите, автоматично инсталират приложения и установяват правата на потребителите.

Windows 2000 домейни

Логическата структура на Active Directory се базира на единици, наречени *домейни*. Въпреки че се използва същата технология, Windows 2000 домейните действат по различен начин спрямо тези в Windows NT. Както в Windows NT, така и в Windows 2000 един домейн представлява административна граница и граница на сигурност, както и репликационна единица. Само че Windows NT използва плоска домейнова структура, а Windows 2000 подрежда домейните в йерархични *дървета от домейни (domain trees)*.

Концепцията за йерархично дърво работи по-различно в Active Directory, отколкото в NDS. NDS не разделя мрежата на домейни. Windows 2000 мрежите могат да имат множество домейни, организирани гори от домейни. Това ще рече, че тези дървета могат да се съединяват с други дървета, за да образуват *гори (forests)*. Фигура 11-5 показва структурата от домейни в Windows 2000, като са дадени две дървета от домейни (кореновите домейни са shinder.net и tacteam.net), свързани в гора.

Фигура 11-5 *Структурата от домейни в Windows 2000 е йерархично дърво.*



Ползата от свързването на дървета от домейни, които имат отделни, неродствени пространства от имена, е резултантното *доверително отношение (trust relationship)*. В следващите секции дискутираме доверените отношения в Windows 2000 и как OU единиците функционират в структурата на домейна.

Доверителни отношения в Windows 2000

Всички домейни в едно и също дърво и всички дървета в една и съща гора автоматично притежават подразбиращо се *транзитивно доверие (transitive trust)*. С такова доверие, потребителите, принадлежащи на един домейн, могат да осъществяват достъп до ресурси в друг домейн, стига техните потребителски акаунти да притежават подходящите позволения за тези ресурси. Транзитивните доверия за голямо подобрение спрямо Windows NT мрежите, при които администраторът трябваше ръчно да установява еднопосочни доверия между всяка двойка домейни в мрежата, за да постигне същия ефект.

Windows 2000 OU единици

Active Directory, подобно на NDS, използва OU единици, за да организира ресурсите в домейните. Административна власт може да се делегира на индивидуални OU единици; обратното на това, NT мрежите позволяват административни привилегии да се назначават само на домейн нивото.

Active Directory и DNS

Active Directory използва DNS конвенциите за именуване и зависи от DNS, за да работи. Трябва да има DNS сървър във всяка Windows 2000 мрежа. Освен това обновяванията на информацията за DNS зоните може да се интегрира с репликирането на Active Directory, което е по-ефективно от традиционните методи за обновяване на DNS.

Windows 2000 поддържа Dynamic DNS (DDNS), което позволява автоматично обновяване на DNS базата данни.

Active Directory сървъри

За да използвате Active Directory, поне един сървър трябва да е конфигуриран като *домейн контролер (domain controller – DC)*, като се препоръчва да има поне два домейн контролера във всеки домейн с цел отказоустойчивост. Задавате на един Windows 2000 сървър да бъде контролер на домейн чрез изпълнение на командата **dcpromo.exe**. Конфигурирането на първия домейн контролер в мрежата създава директорията за него.

За разлика от Windows NT, не съществува един „главен" домейн контролер. Всички домейн контролери съдържат копие за четене/запис на Active Directory дяла. Тази информация се пази актуална и синхронизирана чрез процеса на репликация. Описваме този процес в следващата секция на тази глава.

Мастъри на операции

Въпреки че разликата между главен и резервен домейн контролер в NT беше премахната в Windows 2000, за да се избегнат объркванията, все още има някои функции, за изпълнението на които трябва да е отговорен само един домейн контролер. Тези функции се наричат *едномастърни операции (single-master operations)*.

Например може да съществува само един домейн контролер, притежаващ окончателната власт върху информацията за паролите в случай на конфликт. Това може да се случи, когато се извърши смяна на паролата в един домейн контролер, но тя все още не се е репликирала на всички останали домейн контролери. Ако съществува Windows NT домейн контролер в Windows 2000 мрежа, трябва да има един-единствен домейн контролер, от който може да се получи репликационна информация. Домейн контролерът, изпълняващ тази функция в Windows 2000 мрежа, се нарича PDC емулатор.

PDC емулаторът е един от петте *мастъри на операции (operations masters)* в една Windows 2000 мрежа. Всеки мастър на операции представлява специална роля, изпълнявана само от един домейн контролер в даден домейн (или гора). Ролите в обхвата на домейните включват PDC емулатор, мастър за относителни идентификатори (Relative ID master – RID master) и инфраструктурен мастър. Ролите в обхвата на горите включват мастър на схеми и мастър за именуване на домейни.

Active Directory репликация

Репликацията (replication) е процесът на копиране на данни от един компютър на един или повече други компютри и синхронизиране на тези данни така, че да са идентични на всички останали системи.

Active Directory използва *многомастърна репликация (multimaster replication)*, за да копира директорийна информация между домейн контролерите в даден домейн. Промени могат да се правят във всеки домейн контролер, след което тези промени се репликират към останалите, освен ако не се изпълнява едномастърна операция.

Администраторите на Windows 2000 могат да установяват политики за репликиране, определящи кога и колко често да се извършва репликация на директо-

риите. Това позволява оптимално използване на пропускателната способност на мрежата. Контролирането на графика за репликиране е особено важно, когато домейн контролерите са разположени на срещуположните краища на бавна връзка, каквато например е една 56K WAN връзка.

Сигурност в Active Directory

Всеки обект в Active Directory притежава списък за контрол на достъпа (access control list – ACL), който съдържа всички позволения, асоциирани с обекта. Позволенията могат изрично да бъдат давани и отказвани на грануларен принцип.

Съществуват два типа позволения:

- **Назначени позволения** – Позволения дадени изрично от потребител, който има властта да направи това
- **Наследени позволения** – Позволения, които се прилагат върху дъщерни обекти, тъй като са наследени от родителски обект

Позволения могат да се назначават на отделен потребител или група от потребители. Windows 2000 позволява на администраторите да контролират процеса на наследяване, като по този начин при желание могат да предотвратят наследяването. Забележете полето за отметка в долната част на диалоговия прозорец (Фигура 11-6) със свойствата за сигурност на обекта.

Съвместимост с Active Directory

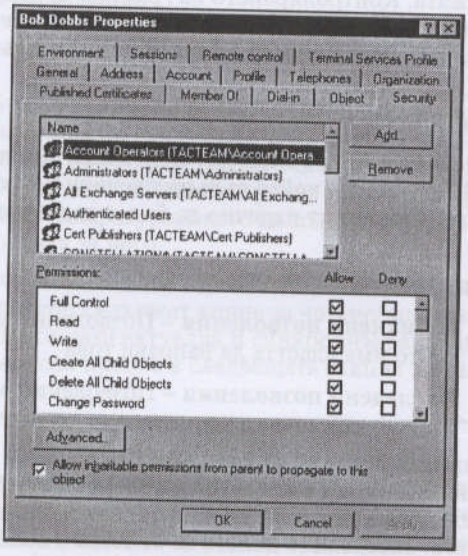
Тъй като зависи от операционната система и неизменно е интегрирана в нея, Active Directory работи само в Windows 2000 сървъри. Въпреки това LDAP клиентите могат да осъществява достъп до директорийните услуги Active Directory, а информацията може да се обменя с други LDAP директорийни услуги, тъй като Active Directory е LDAP-съвместима. Microsoft също така осигурява инструменти за мигриране на информацията от други директории, като например NDS, вActive Directory.

Други директорийни услуги

NDS и Active Directory са добре известни в света на PC-тата. Но съществуват и други директории, използвани от различни платформи, които също заслужават да бъдат споменати. В следващите секции ще направим кратък преглед на следните:

- Директорийни услуги за AS/400 на IBM
- Директорийни услуги на Sun
- StreetTalk на Banyan VINES

Фигура 11-6 *Администраторите контролират позволенията за обекти в Active Directory.*



Директорийни услуги за OS/400 на IBM

Като част от SecureWay Directory (наречена също директорийни услуги за OS/400), IBM осигурява LDAP директорийна услуга за своите AS/400 мейнфрейм компютри. Това позволява използването на приложения с LDAP-възможности, като програми за електронна поща, които използват LDAP услуги, за да намират адреси.

OS/400 LDAP клиентът за Windows позволява съвместна работа с операционни системи на Microsoft, а SecureWay Directory работи под OS/300, OS/400, AIX, Solaris, и Windows NT.

Директорийни услуги на Sun

Sun предлага SDS (Sun Directory Services) за Solaris като част от своя Solaris Easy Access Server. SDS е глобална директория, която поддържа глобални съобщения и отдалечена автентикация, и осигурява дистрибутирана корпоративна директория, организираща мрежовите ресурси.

SDS поддържа множество протоколи и псевдоними, като може да се мащабира до милиони записи. Тя е LDAPv3-съвместима и е предназначена за достъп през Web браузъри и Windows PC-та. Управлението се осъществява през интерфейс на Java.

Banyan StreetTalk

Banyan VINES StreetTalk беше една от първите усъвършенствани директории. По-късните реализации добавиха LDAP поддръжка, за да позволят интегриране с приложения, използващи директории. Banyan пренесе StreetTalk в NetWare, UNIX, и Windows NT. Пренасянето позволи на тези мрежи да споделят обща директория с VINES мрежи.

На 1 май 2000 година Banyan спряха своите програми за поддръжка на продуктите си. В момента компанията се занимава с консултации и решения в областта на електронната търговия.

Директорийни услуги в Интернет

Сайтовете за е-търговия разчитат на директориите, за да каталогизират техните стоки и да проследяват продажбите. Съществуват множество директорийни услуги, работещи на отделни Интернет сайтове. Например www.switchboard.com осигурява директория за лица, бизнеси, ресурси за пазаруване, карти и друга информация. Потребителите дори могат да добавят собствени списъци към директорията.

НА този етап обаче не съществува глобална директорийна услуга, която да покрива целия Интернет. Организацията IETF (Internet Engineering Task Force) е поела задачата да дефинира такава глобална услуга, базирана на LDAP стандарти.

Обобщение

В тази глава направихме обзор на ролята, която играят директорийните услуги в света на мрежите. Научихте, че директорията (справочникът) е база от данни, която организира информацията в логическа структура. Също така научихте, че директорийните услуги предоставят начин да съхранявате, откривате и обезопасявате информацията в една директория.

Дискутирахме пространството от имена на директорията, дефиниращо начина, по който се идентифицират директорийните обекти. Научихте, че пространството от имена на една директория може да бъде или плоско (като директорийната услуга на Windows NT и базата bindery на NetWare), или йерархично (като Active Directory и NDS).

Изследвахме популярната структура на инверсното дърво, използвана от йерархичните директории. В тези директории обектите могат да имат родителски, както и дъщерни обекти. Наименованието „дете“ или „обект“ е свързано с позицията в дървото на оригиналния обект. Когато дъщерните обекти на даден обект включват името на своя родителски обект като част от собствените си имена, пространството от имена е родствено.

След това разгледахме популярните стандарти за директорийни услуги: OSI X.500, DAP и LDAP. Научихте за някои популярни директорийни услуги – по-специално за NDS на Novell и Active Directory на Microsoft.

Дискутирахме и други директорийни услуги, като OS/400 Directory Services на IBM, SDS и вече излязлата от употреба Banyan StreetTalk. Обсъдихме и взаимната работа между директорийните услуги, базираща се на LDAP протоколи. Споменахме също нуждата от глобална директорийна услуга, която да обхваща целия Интернет.

Вече трябва по-добре да разбирате как мрежовите операционни системи могат да използват директорийни услуги, за да направят мрежовите ресурси полеснодостъпни за мрежовите клиенти. В следващата глава дискутирахме клиентската страна на една клиент/сървър мрежа, като ще научите някои основни конфигурации и имения, които да прилагате при използването на популярни клиентски операционни системи.

Допълнителни източници

За повече информация относно стандартите OSI X.500 вижте ръководството X.500 на адрес www.opendirectory.com/Whitepapers/x500tut.html.

За повече информация относно LDAP вижте Web сайта www.innosoft.com/ldapworld.

За повече информация относно NDSv8 на Novell вижте www.nwconnection.com/may.99/ nds859/index.html.

За повече информация относно Active Directory на Microsoft вижте ръководството по Active Directory на адрес www.worldowindows.com/w2000/active_directory.htm.

За повече информация относно глобална директорийна услуга в Интернет вижте www.isoc.org/HMP/PAPER/173/html/paper.html.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Директорията е специален тип какво?

- **a** Файл
- **b** Папка
- **c** База данни
- **d** Запаметяващ носител

2 Какъв тип база данни се създава, когато една директорийна услуга разпростре съхраняваната в нея информация на множество компютри?

- **a** Организирана база данни
- **b** Дистрибутирана база данни
- **c** Сигурна база данни
- **d** Публикувана база данни

3 Кое от следните използва плоско пространство от имена? (Изберете всички верни отговори.)

- **a** NDS
- **b** NTDS
- **c** Novell bindery
- **d** Active Directory

4 Какъв тип пространство от имена се създава, когато един дъщерен обект включва името на своя родителски обект като част от собственото си име?

- **a** Плосък (Flat)
- **b** Генерационен (Generational)
- **c** Транзитивен (Transitive)

d Родствен (Contiguous)

5 DSA (Directory System Agent), DUA (Directory User Agent) и DIB (Directory Information Base) са основни компоненти на кое от следните?

a Windows 2000 Active Directory

b DAP

c OSI X.500 спецификациите

d LDAP клиентски софтуер

6 Как се нарича X.500/LDAP конвенцията за именуване, която обозначава път – като например DC=net DC=tacteam OU=training CN=Users CN=John Doe – до обект в директорията?

a Атрибут

b Относителен DN

c DN

d Общо име

7 Как се нарича обект в NDSдървото, който представлява ресурс, или крайна точка в клон, вместо обект, съдържащ други обекти?

a Листов обект (leaf object)

b Коренов обект (root object)

c Стволов обект (stem object)

d Родителски обект (parent object)

8 Кой Active Directory файл съдържа скриптове и обекти за групови политики?

a Отчетен файл на Active Directory

b Скриптов файл

c Административен файл за групови политики

d Файл за споделен системен том

9 Кое от следните е вярно за Windows 2000 домейни, намиращи се в едно и също дърво от домейни?

a Не могат да споделят доверителни отношения.

b Споделят двупосочно транзитивно доверително отношение.

c Споделят еднопосочно не-транзитивно доверително отношение.

d Могат да споделят доверително отношение само ако отношението е създадено изрично от администратор.

10 Къде се съдържат всички позволения за достъп, асоциирани с Active Directory обект?

a В дъщерен обект

b В политика за репликация

c В ACL списък

d В организационна единица (OU)

Глава 12

Настолни операционни системи

В една базирана на сървър мрежа, *клиентските* машини се свързват към сървъра и осъществяват достъп до неговите ресурси. Тези клиентски машини работят под различни операционни системи (наричани обикновено *настолни операционни системи* или *клиентски операционни системи*), което ги различава от сървърните операционни системи.

Таи глава обсъжда най-популярните настолни операционни системи:

- MS-DOS
- Windows 3.x
- Windows 95 and Windows 98
- Windows NT Workstation
- Windows 2000 Professional
- Linux and UNIX
- Macintosh
- IBM OS/2

Най-важно е да разберете, че не е необходимо клиентските компютри да работят под настолна операционна система, разработена от същия производител, който е разработил и мрежовата операционна система, работеща на сървъра, към който се свързват клиентските компютри. Например Windows 98 клиентите могат да се свързват с UNIX или Linux сървър. Някои производители на мрежови операционни системи, като NetWare, дори не правят настолни операционни системи.

Основи на операционната система

Операционната система е основната програма, която се зарежда първоначално в компютъра. Операционната система управлява всички останали програми (*приложения*), работещи на компютъра, които включват следното:

- Програми за продуктивност, като текстообработка или електронни таблици
- Мрежови приложения, като e-mail или Web браузъри

- Мултимедийни програми, които възпроизвеждат филми и музикални файлове, или пък аудио CD-та
- Помощни програми за управление на операционната система, на други файлове и на други приложения
- Справочни програми, като речници и енциклопедии
- Игри

Операционната система изпълнява *услуги* за приложенията, които заявяват тези услуги посредством приложен програмен интерфейс (application programming interface – API). В една многозадачна среда операционната система разпределя процесорното време и паметта, за да изпълнява приложения едновременно; операционната система действа като свръзка между приложенията и хардуерните устройства.

Приложенията често пъти са допълнителни програми, които се закупуват отделно и се инсталират върху операционната система. Тези приложения включват програми за текстообработка, електронни таблици и бази данни, както и софтуер за обработка на илюстрации и графика. Операционните системи включват множество вградени приложения, като системни инструменти (например за създаване на резервни копия и за управление на дисковете), конфигурационни аплети и основни програми за продуктивност, като текстови редактори, калкулатори и прости програми за редактиране на изображения.

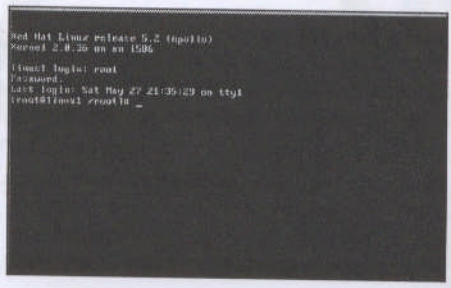
Интерфейси на операционните системи

Всеки потребител взаимодейства с операционната система и програмите чрез използване на *потребителския интерфейс*. Потребителските интерфейси могат да бъдат разделени на две категории: текстово базирани и графични. Графичният потребителски интерфейс често пъти се нарича за кратко GUI (произнася се „гуи“). В следващите секции ще дискутираме характеристиките на всеки от тях.

Текстово-базирани интерфейси

Първите операционни системи за PC използваха текстово-базирани (наричани също *знаково-базирани*) интерфейси. Потребителите въвеждаха команди след промпта (наречен *команден промпт)*. MS-DOS и UNIX/Linux са пример за операционни системи, използващи текстово-базирани интерфейси. Фигура 12-1 показва пример за текстово-базиран потребителски интерфейс.

Фигура 12-1 *Можете да се логнете в Linux, като използвате текстово-базиран интерфейс.*



Повечето текстово-базирани операционни системи могат да изпълняват графични *шелове*, осигуряващи GUI интерфейси. За Linux съществуват няколко графични интерфейса, като например X Window и KDE. DOSSHELL е ранен графичен шел, използван под MS-DOS.

Шеловете се различават от операционните системи с истински GUI интерфейс, тъй като шеловете са отделни програми, работещи върху операционната система. Операционната система може да работи и без шела, но шелът не може да функционира без операционната система.

ЗАБЕЛЕЖКА Windows 3.x, въпреки че се нарича операционна система, всъщност представлява един шел, работещ на върха на MS-DOS.

Знаково-базираните операционни системи са по-бързи и изискват по-малко системни ресурси от GUI интерфейсите.

Графични потребителски интерфейси

Операционни системи като Windows 9*x* и по-нови, операционната система Macintosh OS, както и OS/2, са базирани на GUI интерфейс. Един GUI интерфейс показва както картинки, така и текст. В графичния потребителски интерфейс повечето от командите и функциите се изпълняват чрез боравене с *икони*, представляващи картинни репрезентации на програми, файлове и други компоненти. Фигура 12-2 показва GUI интерфейс.

Фигура 12-2 *Логвате се в Windows 2000, като използвате GUI интерфейс.*

GUI интерфейсите по принцип са по-дружелюбни към потребителя (user friendly), отколкото текстово-базираните интерфейси, особено за хората, които се ориентират визуално. С помощта на GUI, потребителите например могат да *дърпат и да пускат (drag and drop)* графични елементи, за да местят файлове от едно място на друго.

GUI интерфейсите имат и недостатъци. Например те забавят реакциите на системата и изискват повече системни ресурси, за да изобразят сложните графики. Понякога взаимодействието с графичните елементи може да се окаже по-неудобно, отколкото да се въведе команда. Освен това е много трудно да боравите с машината, ако не разполагате с посочващо устройство (мишка или тракбол).

Поради недостатъците си, GUI-базираните операционни системи обикновено осигуряват програми за изпълнение от командния ред. Тези програми могат да се използват за изпълнение на общи административни задачи. Например в Windows NT можете да стартирате вградената backup програма или чрез графична икона от меню, или чрез въвеждане на **ntbackup.exe** на командния ред.

Използване на команди

Командите се използват, за да кажете на операционната система каква задача да изпълни. В текстово-базираните интерфейси тези команди се въвеждат като низ от знакове, а в GUI интерфейсите щраквате върху икона или елемент от меню. И в двата случая входът се интерпретира според *езика за програмиране* (например C или Java), на който е написана операционната система, след което се конвертира в *машинен език*, т.е. в 1-ци и 0-ли, които процесорът на компютъра разбира.

Команди и чувствителност към регистъра на буквите

Файловата система използвана от някои операционни системи (като UNIX) са *чувствителни към регистъра на буквите (case sensitive)*. Дори в онези операционни системи (като Windows), които използват файлови системи, нечувствителни към регистъра на буквите, някои команди и аргументи на команди се влияят от това дали въвеждате малки или главни букви. Например, когато въвеждате командата **nbtstat** в Windows, ключът **-r** (долен регистър) изброява имената, преобразувани от бродкаст и WINS, а ключът **-R** (горен регистър) изчиства и презарежда таблицата за кеширане на отдалечените имена.

Значението на синтаксиса

За да може една команда да бъде обработена правилно, тя трябва да използва правилния *синтаксис*, който представлява структурата на командата. Структурата включва реда на думите, интервали, а в някои случаи и въвеждане на главни букви и пунктуация.

Синтаксисът е елемент на говоримия и писмен език – част от това, което наричаме *граматика*. Например в английския език типичната конструкция на едно изречение поставя подлога на изречението (обикновено съществително или местоимение) най-отпред, а след тях и идват сказуемо (или глагол, който е дума за действие) и допълнение (ако има такова). Прилагателните и наречията обикновено се поставят точно преди съществителните или глаголите, които те модифицират. Разгледайте следното изречение: „Мери [подлог/съществително] си купи [сказуемо/глагол] нов [прилагателно, модифициращо *компютър*] компютър [допълнение/съществително].“

Но ако някой, който не е англичанин, иска да изрази същото, той може да потърси думите в речник и да използва синтаксиса на собствения си език, за да създаде изречение. В такъв случай изречението може да стане „Мери нов компютър си купи“. Повечето от нас пак биха разбрали какво се казва, въпреки че синтаксисът е неправилен.

Животът в света на компютрите обаче не е толкова лесен. Ако командата за копиране на файл от дискета на твърдия диск е

```
copy име_на_файл a: c:
```

но ние по погрешка напишем

име_на_файл **copy a: c:**

компютърът не разбира какво му казваме и няма да изпълни задачата.

Разликата идва от това, че хората могат да мислят, а машините само да изчисляват. Ето защо синтаксисът на командите трябва да е абсолютно точен, като се спазват и интервалите. Например въвеждането на командата **netview** в командния ред на Windows 2000 не прави нищо, но въвеждането на командата **net view** (с интервал между думите) извежда списък на сървърите в мрежата.

Използване на аргументи

Командите на операционната система често пъти позволяват дефиниране на допълнителни параметри чрез добавяне на *аргументи* или *ключове*. Например командата **net** view, написана по този начин, извежда списък на Microsoft компютрите в мрежата, изпълняващи услугата server, както е показано в Пример 12-1.

Пример 12-1 *Командата net view без ключове извежда Microsoft сървърите*

```
c:\>net view
Server Name            Remark
------------------------------------------------------------------
\\CONSTELLATION
\\CONSTITUTION
\\DELTA-FLYER
\\DS2000
\\EXETER
The command completed successfully.
```

Добавянето на ключ към командата – например **net view /network:nw**, извежда NetWare сървърите в мрежата, както е показно в Пример 12-2.

Пример 12-2 *Добавянето на подходящия ключ към командата net view води до извеждане само на NetWare сървърите*

```
c:\>net view /network:nw
Resources on NetWare or Compatible Network
------------------------------------------------------
\\DALTAC
\\NETGUY
The command completed successfully.
```

Лесен начин за показване на приемливия синтаксис и параметри за дадена команда е въведете **[команда] ?**, както е показано в Пример 12-3. За да изведете списъка на самите команди, въведете **help**. UNIX системите често пъти предоставят online ръководство, което можете да отворите с командата **man**.

Пример 12-3 *Въвеждането на команда, последвана от въпросителна, извежда приемливия синтаксис и параметрите за тази команда*

```
c:\>net view ?
The syntax of this command is:
NET VIEW [\\computername [/CACHE] : /DOMAIN[:domainname]]
NET VIEW /NETWORK:NW [\\computername]
```

Команди в различни езици

В някои случаи дадена команда е една и съща в различните операционни системи. Например командата **arp** извежда кешираната информация за ARP (Address Resolution Protocol) на компютри, изпълняващи TCP/IP, независимо дали операционната система е Windows NT, Windows 2000, Windows 95, Windows 98, UNIX или Linux.

От друга страна, някои команди се различават от една операционна система до друга. За да видите конфигурационната информация за TCP/IP, трябва да използвате специфична за операционната система команда, както е изброено в Таблица 12-1.

Таблица 12-1 *Команди за разглеждане на конфигурационната информация за TCP/IP*

Операционна система	Команда
Windows NT and Windows 2000	**ipconfig**
Windows 95 and Windows 98	**winipcfg**
Linux and UNIX	**ifconfig**
NetWare	**config**

Често използвани DOS команди

Всички Windows операционни системи включват команден ред, който ви позволява да въвеждате MS-DOS-базирани команди. За да достигнете до командния ред на Windows 9*x* машина например, можете да въведете **command** в диалоговия прозорец Run. (Този диалогов прозорец се отваря чрез избор на Run от менюто Start.)

В Windows NT/2000 машини трябва да въведете **cmd.** Това отваря „DOS прозорец" с промпт, след който можете да въвеждате командите. („DOS прозорецът" понякога се нарича „c: промпт", макар че началната директория на DOS промпта зависи от конфигурацията на вашия компютър.)

Простите DOS команди включват тези, изброени в Таблица 12-2.

Таблица 12-2 *Често използвани DOS команди*

Команда	Резултат
dir	Извежда файловете в текущата директория
cd *име на директория*	Преминава към указаната директория
time	Извежда или установява системното време
date	Извежда или установява датата
copy	Копира файлове на друго място
diskcopy	Копира съдържанието от една дискета на друга
attrib	Показва или променя файлови атрибути
find *текстов низ*	Търси текстов низ във файл
help	Извежда списък на други налични команди, както и техните функции

Команди за помощ и файлове за помощ

GUI-базираните операционни системи обикновено включват Help-файлове (файлове за помощ). Те могат да са под формата на .pdf за лесно разпечатване, или е възможно да са написани на HTML, включвайки активни връзки с цел препратки към свързан с темата материал. Често пъти се включва и машина за търсене. Например операционната система Windows 2000 включва обширна система за помощ с хипервръзки, както е показано на Фигура 12-3, която може да се претърсва по ключови думи, индексиран списък или детайлно описание на съдържанието. Можете също да разпечатвате отделни теми.

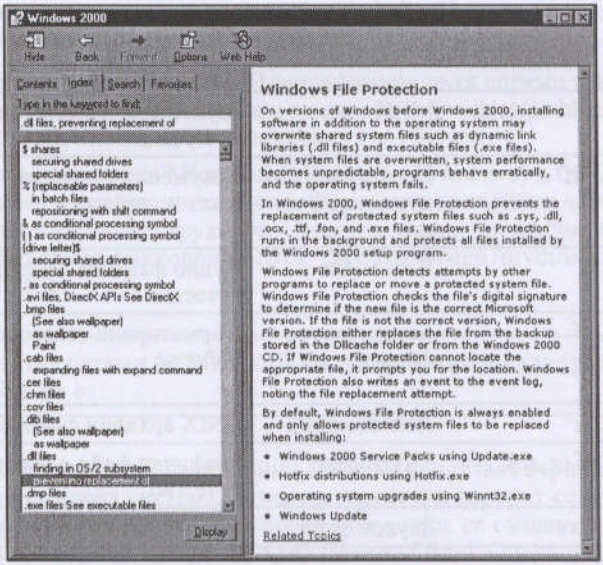
Файлове и файлови системи

Компютърната информация се съхранява под формата на единици, наречени *файлове*. Един файл се състои от група данни, които могат да бъдат манипулирани (например отваряни, разглеждани, копирани, изтривани и местени) като едно неделимо цяло. Всеки файл притежава уникално име в мястото, където се намира.

Съществуват много типове файлове. Всеки тип се асоциира с някакво приложение. Например счетоводната информация се съхранява във файл с електронна таблица. Писмата и друга кореспонденция се съхраняват във файл за текстообработка. Графиката често се съхранява в битмап (BMP), JPEG (Joint Photographic Experts Group) или друг тип графичен файл.

Различните типове файлове се създават, отварят и модифицират чрез използване на различни типове приложения. Например електронните таблици се обработват от приложения като Excel или Lotus 1-2-3. Писмата се обработват с приложения като WordPad, Notepad, Word или WordPerfect. Някои графики се обработват с програмата Paint, която е част от операционните системи на Microsoft. За един файлов тип се казва, че е *асоциран* с програма или програми, които могат да се използват за неговата обработка.

Фигура 12-3 *Съвременните операционни системи включват подробни файлове за помощ.*



Файлови разширения и файлови типове

Някои операционни системи използват *файлови разширения*, представляващи суфикси от по два или три знака, които идентифицират типа на файла и асоциираните с него приложения. Например, разширението .exe ф края на едно файлово име често се използва за означаване на изпълним (програмен) файл, .gif идентифицира графичен файл, а .htm (или .html) е файл, написан в HTML (HyperText Markup Language). Някои често срещани файлови разширения са изброени в Таблица 12-3.

Таблица 12-3 *Често срещани файлови разширения*

Файлово разширение	Файлов тип	Описание	Асоциирани програми
.avi	Аудио и видео	Файлове с филми	Медия плеъри
.bmp	Битмап	Графични файлове	Програми за разглеждане на изображения
.doc	Документ	Документ за текстообработка	Програми за текстообработка
.jpg or .jpeg	JPEG картинка	Компресирани (с малък размер) графични файлове	Програми за разглеждане на изображения и Web браузъри
.gif	GIF картинка	Графични файлове; могат да се комбинират за направа на анимации	Програми за разглеждане на изображения и Web браузъри
.hlp	Помощ	Файлове с помощни данни	Текстови редактори
.htm or .html	HTML	Документи, съдържащи хипертекстови връзки	Web браузъри
.ini	Инициализация	Конфигурационни файлове	Използват се от операционните системи за установяване на конфигурация; могат да се разглеждат в текстов редактор
.mid or .midi	MIDI звук	Звуков файл; синтезирана музика	Медия плеъри
.pdf	Портативен документен формат	Документи с печатим текст и графика	Adobe Acrobat
.ra	RealAudio	Аудио файлове с високо качество	RealPlayer
.rtf	Богат текстов формат	Форматирани текстови файлове	Програми за текстообработка или текстови редактори
.tar	Лентов архив	UNIX архивни файлове	UNIX команди
.tif or .tiff	Tiff формат	Графичен файл с високо качество	Програми за разглеждане на изображения
.wav	Звуков файл	Звук (глас или музика)	Медия плеъри

Файлови системи

Съхранените на твърдия диск файлове трябва да се организират така, че да могат да бъдат намерени при необходимост. Методът за поставяне и извличане на файлове се нарича *файлова система.*

Различните операционни системи използват различни файлови системи, а някои дори могат да използват повече от една файлова система. Например, въпреки че Windows 3.*x* може да използва само файловата система FAT16, Windows 2000 може да използва FAT16, FAT32 и NTFS. Всички тези файлови системи са дискутирани по-нататък в тази глава.

Файловата система определя конвенцията за именуване на файловете и форма́та за указване на *път* до местоположението на файла.

Конвенции за именуване на файлове

Конвенциите, или правилата, за именуване на файлове варират в зависимост от файловата система и включват няколко характеристики като следните:

- Максимален брой знакове, позволени в името на един файл
- Максимална дължина на файловите разширения
- Дали между думите са позволени интервали
- Дали файловите имена се влияят от регистъра на буквите
- Кои знакове за „позволени" за използване във файловите имена
- Формат за указване на пътя

Имена на пътища

Едно *име на път (pathname)* може да функционира по един от следните два начина:

- **Напълно определено (или абсолютно) име на път** – Идентифицира пълния път от кореновия дял до самия файл. Пример за токова име е c:\mydirectory\subdirectory1\myfile.ext.
- **Относително име на път** – Идентифицира пътя спрямо текущата директория или папка. Например ако текущата работна директория е mydirectory, относителният път е subdirectory1\myfile.ext.

Операционните системи на Microsoft (MS-DOS и Windows) и OS/2 използват формата, показан в предходния списък. Обратните наклонени черти разделят нивата на директорийната структура. От друга страна операционните системи UNIX използват право наклонени черти, като например /mydirectory/subdirectory/myfile.

ЗАБЕЛЕЖКА В операционните системи на Microsoft името на буквата на устройството е част от пътя; в UNIX не е.

Повечето от популярните операционни системи използват *дървовидна структура* за своята файлова система. В такава структура коренът се намира на върха, а контейнерите, наречени *директории* или *папки,* се създават под корена. Понякога това се нарича *инверсно дърво (inverted tree)*. Операционните систе-

ми, използващи дървовидна структура, включват MS-DOS, Windows (всички версии), Macintosh, OS/2, UNIX и Linux.

Контейнерните единици в DOS, Windows 3.*x*, UNIX и Linux се наричат директории. В Windows 9*x*, Windows NT 4.0, Windows 2000 и Macintosh OS те се казват папки. Терминът „папки" позволява на потребителите по-лесно да разбират структурата на файловата система, като я свързват с офис среда, в която хартиените досиета (файлове) се съхраняват в картонени папки. Файловете се поставят в контейнери с организационна цел.

Директориите (наричани също папки) могат да съдържат поддиректории (или подпапки), които могат от своя страна да съдържат свои поддиректории (подпапки), и т.н. Директориите и папките, подобно на файловете, трябва да имат уникални имена в своите контейнери; това ще рече, че ако имате директории с имена Dir1 и Dir2, всека от тях може да има поддиректория с едно и също име (Sub1). Не можете обаче да имате две поддиректории в Dir1, които да се казват Sub1, защото пълните имена на пътищата ще бъдат еднакви. В първия случай пълните имена на пътищата ще бъда различни (c:\Dir1\Sub1 и c:\Dir2\Sub1).

Популярни файлови системи

В следващите секции ще разгледаме някои от популярните файлови системи, използвани от съвременните операционни системи:

- File Allocation Table (FAT)
- NT File System (NTFS)
- High Performance File System (HPFS)
- Macintosh Hierarchical File System (HFS)
- Network File System (NFS)

FAT Има няколко варианта на файловата система FAT, включващи FAT12, FAT16, FAT32 и VFAT. Тези файлови системи са с такива имена, защото използват таблица за разположение на файловете (още и таблица за разпределение на дисковото пространство), поддържана на твърдия диск; таблицата осигурява „карта" на разположението на файловете. Файловете се съхраняват в *клъстери* – логическа единица за съхранение на диска. Един клъстер може да съдържа данни само на един файл; само че един файл може да заема множество клъстери.

Днес FAT12 се среща изключително рядко, защото тя се използва само за изключително малки дискови дялове. (Дяловете са дискутирани по-нататък в тази глава.) FAT16 е по-нова версия на файловата система и е създадена за използване с по-големи дялове (до 4 GB).

Въпреки че по-големите дискове могат да се форматират с FAT16, това води до неефективно използване на дисковото пространство, защото във FAT големите дялове водят до по-големи размери на клъстера. Например при един дял от 512 MB, размерът на клъстерите е 8 KB. Това означава, че дори ако даден файл е само 1 KB, той заема 8 KB, защото клъстерът е неделима част и не може да се използва от повече от един файл; останалите 7 KB се губят. За решаването на този проблем беше създадена FAT32. Тази 32-битова файлова система използва клъстери с по-малки размери. Тя поддържа дялове с размери до 2 *терабайта* (TB).

Преимущество на FAT16 е богатата гама от операционни системи, които я поддържат. MS-DOS, OS/2, всички версии на Windows и други операционни системи могат да четат и записват FAT16 файлове. Windows 95b (за който ще нау-

чите по-нататък в тази глава), Windows 98, Windows ME и Windows 2000 поддържат FAT32. MS-DOS/Windows 3.*x* и Windows NT не могат да използват FAT32. Това ограничава използването и в машини, на които са инсталирани две или повече операционни системи.

Компютри с две и повече операционни системи

При компютрите, на който са инсталирани две или повече операционни системи, обикновено се използва програма за управление на първоначалното зареждане, която ви позволява да изберете коя операционна система искате да заредите, когато стартирате машината. Инсталационните програми на някои операционни системи включват boot мениджър. Например Windows NT и Windows 2000 Включват NT boot manager (като опциите са дефинирани във файл с име boot.ini), а Linux включва boot мениджъра LILO. Съществуват и програми на независими компании, като например System Commander, позволяващи ви да зареждате до 100 операционни системи на една машина.

Оригиналната файлова система FAT беше разработена за MS-DOS и ограничава файловите имена до осем знака с разширение до три знака. *Virtual FAT (VFAT)* е вариант на FAT, разработен за Windows 95 с цел поддръжка на дълги файлови имена. VFAT е реализирана като *драйвер на файловата система*, който разширява възможностите на файловата система FAT за използване на файлови имена с дължина до 256 знака. По този начин могат да се задават много по-значими имена на файловете. VFAT поддържа и кеширане на диска, което повишава производителността и намалява времето за запис или четене от диска.

NTFS Microsoft разработи NTFS за Windows NT; тази файлова система може да се използва само от Windows NT и Windows 2000. NTFS беше проектирана да разреши някои от проблемите, като например липсата на сигурност на ниво файл.

NTFS включва следните възможности, които преодоляват различни ограничения на FAT:

- **Сигурност на ниво файл чрез NTFS позволения** – NTFS използва списък за контрол на достъпа (access control list – ACL), позволяващ ви да указвате специфични позволения за файловете, независимо дали потребителят осъществява достъп до тях от отдалечена машина или локално. FAT файловете могат да бъдат обезопасени чрез *позволения за споделяне*, които защитават файла от неоторизиран достъп по мрежата, но не го защитават от локален достъп. (NTFS файловете могат да се защитават едновременно както от позволения за споделяне, така и от NTFS позволения на ниво файл)
- **Компресия на файлово ниво** – За да се компресират данни във FAT, целят дял трябва да се компресира чрез използване на метод, преобразуващ цялото налично пространство в един голям файл. Ако този файл се повреди, всички данни на това локално устройство могат да се загубят. NTFS файловете могат да се компресират файл по файл. Ако един от файловете на този дял се повреди, останалите остават незасегнати.
- **Замяна на сектори (нарича се също *гореща поправка*)** – При наличието на тази възможност файловата система идентифицира лошите дискови сектори, мести данните в добър сектор и маркира лошия като неизползваем. Това се прави „в движение“ и процесът е невидим за потребителя.

- **Поддръжка на Unicode** – NTFS поддържа използването на файлови имена, съдържащи Unicode знакове, което ви позволява да показвате имена на други езици.
- **Поддръжка на изключително големи дялове (до 16 *ексабайта*)** – Един ексабайт данни се равнява приблизително на един милиард байта.
- **Поддръжка на дълги файлови имена** – NTFS поддържа дълги файлови имена и техни еквивалентни псевдоними във формат „осем точка три". (В имената „осем точка три" може да има до осем знака плюс тризнаково разширение, което дава имена подобни на „file.doc".) Това се прави с цел обратна съвместимост с MS-DOS и Windows 3.*x*.

ЗАБЕЛЕЖКА *Обратна съвместимост* се нарича способността на една файлова система, операционна система или приложение да работят с файлове, създадени от по-ранни версии на софтуера. За производителите на софтуер е важно да правят своите продукти обратно съвместими, така че потребителите, които правят ъпгрейд към новата версия на даден продукт, да не загубят създадените с по-ранната версия данни.

NTFS пази информация за файловите клъстери keeps чрез *директорийна схема тип b-дърво (двоично дърво [b идва от binary])*. Индексирането чрез b-дърво позволява разглеждането на данните в сортиран ред. Това се различава от файлова структура тип *свързан списък* при FAT. Структурата с b-дърво позволява по-бърз достъп до файловете в една голяма директория.

Докато FAT съхранява информацията за клъстерите на файловете само в таблицата за разположение на файловете, NTFS съхранява тази информация във всеки отделен клъстер. NTFS е по-неподатлива на *файлова фрагментация*, която може да забави производителността при осъществяване на достъп до записаните на твърдия диск данни.

Фрагментация на файловете

На един празен, или чист, диск данните се съхраняват в последователни клъстери. Ако даден файл е твърде голям, за да се поберат всичките му данни в един-единствен клъстер, остатъкът се съхранява в следващия свободен клъстер. Когато всички данни на всеки файл се съхраняват в последователни клъстери, за диска се казва, че е нефрагментиран.

Фрагментация обаче възниква, ако данните се местят или изтриват, защото подобно действие оставя свободни клъстери. Когато се съхраняват нови данни, процесът започва от първите свободни клъстери, така че ако новият файл е по-голям от премахнатия преди това, първата част от данните се съхраняват в освободените клъстери. След това останалата част се съхранява в следващите свободни клъстери, които може да са отделени от първите (т.е. да не се намират непосредствено след тях).

Когато операционната система или някое приложение трябва да осъществи достъп до файла, времето за това е по-дълго, отколкото ако данните са разположени само в последователни клъстери. Ето защо фрагментацията намалява производителността. Съществуват инструменти, наречени дефрагментатори (като Diskeeper на компанията Executive Software), могат да преподреждат данните, за да намалят фрагментацията и да повишат производителността. Windows 9x и Windows 2000 включват вградени инструменти за дефрагментиране.

Windows 2000 включва нова версия на NTFS, наречена NTFS 5. Windows NT може да чете NTFS 5 файлове, *ако* е инсталиран Service Pack 4 или по-нов. Windows NT обаче не може да използва разширените възможности на NTFS 5, като например криптиране на файлове, които се поддържат от Windows 2000. NTFS 5 осигурява множество допълнителни възможности и подобрения спрямо NTFS 4, включващи следното:

- Способността за криптиране на файлове на твърдия диск чрез използване на EFS (Encrypting File System).
- Поддръжка на разпръснати файлове, което позволява на програмите да създават много големи файлове, като същевременно консумират дисково пространство само колкото трябва.
- Поддръжка на дискови квоти, което позволява на администраторите да ограничават количеството дисково пространство, използвано от отделните потребители.
- Разпределено следене на връзки, което позволява на програмите да запазват връзките при преместване на сорс файловете.
- Точки за монтиране на томове, които ви позволяват да монтирате дисков дял в NTFS папка. Чрез това се преодолява ограничението, постановяващо, че можете да създавате само толкова томове, колкото букви има в латинската азбука.
- Поддръжка на отдалечено съхранение, което прави по-достъпни файловете, съхранени на сменяеми носители (като ленти).

Файловата система на UNIX Файловата система на UNIX е организирана като йерархия от директории и поддиректории, в които могат да се съхраняват файлове.

В UNIX, главната (root) директория се представя като наклонена черта (/), наричана още слаш. Ето защо един път до директория изглежда примерно така: „/dir2/subdir1"; поддиректория с име subdir1 се намира в директория dir2, която пък се намира в главната директория.

Системните директории на UNIX се намират непосредствено под главната директория. Те съдържат файловете, използвани от операционната система. Стандартните системни директории включват следното:

- **/bin** – Съдържа *изпълними двоични* файлове – командите и инструментите за ежедневна работа
- **/dev** – Съдържа специални файлове, представляващи физически *устройства*, като например принтери
- **/etc** – Съдържа команди и файлове, използвани за системно администриране
- **/lib** – Съдържа *библиотеки*, използвани от програмите
- **/tmp** – Съдържа *временни* файлове, които се изтриват при рестартиране на системата
- **/usr** – Съдържа *домашните директории* на потребителите заедно с други файлове като онлайн ръководства

Ядрото е сърцето на операционната система; то се зарежда, когато стартирате машината. Главната директория на UNIX съдържа файла с ядрото, както и за-

реждащия модул, представляващ малка програма, която започва зареждането на операционната система.

Файловата система на UNIX не позволява интервали в имената на файловете. Въпреки че в Windows 2000можете да кръстите един файл „Joe Brown Memos", в UNIX трябва да го наречете JoeBrownMemos, Joe_Brown_Memos или Joe-Brown-Memos.

UNIX позволява поставянето на точки в имената на файловете. Например името Joe.Brown.Memos е валидно. Това можете да правите и в 32-битовите Windows операционни системи, но в DOS/Windows 3.x е разрешена само една точка. Всичко, което идва след точката, се третира като файлово разширение.

Файловите имена в UNIX могат да са с дължина до 255 знака. Някои знакове (включително # / ? „ ' [ ]) не са позволени , защото имат специално значение за операционната система.

ЗАБЕЛЕЖКА Въпреки че знакът подчертавка (_) не е забранен в имената на файловете, добра идея е да го избягвате, защото едно такова име (било то на компютър или ресурс) в Интернет може да създаде проблеми с някои DNS сървъри, които не могат да преобразуват такива имена в IP адреси.

За потребителя една от най-забележимите разлики между файловите системи на UNIX и Microsoft е *чувствителността към регистъра (case sensitivity)*. В DOS или Windows, файловото име „mydocuments" е същото като „MyDocuments" или „MYDOCUMENTS." За файловата система на UNIX обаче това са различни имена и могат да съществуват заедно в една директория.

Докато сърфирате из Мрежата може би сте забелязали, че ако въведете URL адрес с използване на главни букви, вашият Web браузър понякога отива на Web сайта, без да се „оплаква"; други пъти обаче това не става. Това различие възниква, защото някои Web сървъри работят под Windows NT, който не използва чувствителна към регистъра файлова система, докато при UNIX сървърите не е така.

Други възможности на UNIX файловата система са:

- **Асоцииране на I-възли (i-node mapping)** – UNIX използва вътрешно число, наречено *i-възел (i-node)*, за да идентифицира всеки файл или директория. Операционната система асоциира този номер с местоположението на данните на физическия диск. Поддържа се таблица, в която пълното име на пътя отговаря на съответния i-възел.
- **Твърди връзки (hard links)** – Една твърда връзка ви позволява да асоциирате повече от едно файлово име с даден файл. Чрез използване на командата **ln**, за да ги свържете, можете да имате два различни файла – например единият с име Myfile, а другият с име Yourfile – които ще сочат един и същ i-възел. Когато направите това, промените във файла Myfile веднага се показват и в Yourfile.
- **Плоски файлове (flat files)** – Файловата система на UNIX не притежава сложни правила, дефиниращи хедъри за различните файлови типове. Вместо това файловете се изграждат като потоци от данни без предварително определена структура. От приложението зависи да дефинира структурата за форматиране на файловете.

HPFS IBM разработиха HPFS за операционната система OS/2. Въпреки че версия 1.0 на OS/2 притежаваше само FAT поддръжка, HPFS беше включена във версия 1.2. Някои от характеристиките на HPFS включват следното:

- Поддръжка на дълги файлови имена (до 254 знака)
- По-висока производителност от FAT
- Висока надеждност и способност за възстановяване
- По-малка фрагментация на файловете, отколкото при FAT

ЗАБЕЛЕЖКА Когато за описание на една файлова система се спомене терминът *надеждност*, това означава слаб наклон към грешки и повреждане на файлове. *Способността за възстановяване* е способността на файловата система да поддържа интегритета на данните например чрез създаване на редундантни копия на данните, които копия могат да се използват, ако оригиналните данни се повредят.

HPFS поддържа разширени знакови таблици, и въпреки че запазва регистъра на буквите, тя *не* е чувствителна към него. Ето защо, ако забравите къде в едно файлово име, например „mydocuments", сте задавали главни букви, тогава въвеждането на myDocuments или MYDOCUMENTS пак ви дава достъп до файла.

HPFS използва директорийна структура, разделяща диска на *ленти (bands)*, всяка от по 16 MB. Директорийната структура и информацията за разпределението се разполагат по средата на всяка лента. В резултат на това съдържанието на файловете не може да е по-далеч от 8 MB спрямо управляващата информация. Това е основата на високата производителност в HPFS.

HPFS поддържа дялове с размер до 64 GB и разпределя дисковото пространство, използвайки сектори, вместо клъстери; Това създава по-малко загубено дисково пространство и по-слаба необходимост от дефрагментиране. HPFS използва *секторни сигнатури (sector signatures)*, за да идентифицира всеки дисков сектор; поради тази причина данните могат да бъдат възстановявани дори от зле повредени дискове.

Macintosh HFS Операционната система на Mac използва HFS; в HFS, дисковете се разделят на *томове*, които могат да съдържат всеки от следните компоненти:

- Файлове
- Директории
- Директорийни нишки
- Файлови нишки

ЗАБЕЛЕЖКА Една *директорийна нишка* съдържа името на директорията и идентификация на родителя на директорията. Една файлова нишка съдържа името на файла и директорията, в която той се намира.

Файловата система използва индексиращ алгоритъм тип b-дърво, за да организира и открива съдържанието на директориите. Освен това HFS поддържа *разклоняване на файлове (file forking)*, при което файловете се съставят от следните части, или *клони (forks)*:

- **Ресурсен клон (resource fork)** – Този файл включва меню елементи, диалогови прозорци и т.н.
- **Даннов клон (data fork)** – Този файл съдържа потока от данни.

HFS използва *каталози*, като всеки файл или директория има *каталожни записи* с идентификационни номера, функциониращи донякъде като i-възлите в UNIX. Директорийните нишки и файловите нишки са каталожни записи, включващи името на директорията или файла заедно с идентификацията на тяхната родителска директория. Нишките осигуряват редундантност и възможност за възстановяване от дискови кешове.

Помощни програми като plug-in модула Global File System от Charismac и MacOpener от DataViz позволяват на Macintosh файловете да бъдат достъпни от операционните системи Linux, OS/2, Windows и DOS.

NFS NFS беше разработена от Sun Microsystems и се превърна в стандарт за файлови сървъри; за да комуникира, тя използва RPC (remote-procedure call) протоколи. За да може NFS да работи, на изпращащия заявката компютър трябва да е инсталиран NFS клиент, като и клиентът, и сървърът трябва да използват TCP/IP. WebNFS е разширение на NFS за използване по Интернет; то замества протоколи като HTTP и FTP.

Избор на правилна файлова система Изборът на файлова система зависи от инсталираната на компютъра операционна система, потребностите за сигурност и потребностите за достъп. Файловите системи обикновено се разработват за дадена операционна система, но някои операционни системи поддържат повече от една файлова система. Дори е възможно да използвате едновременно повече от една файлова система – стига да са на различни *дискови дялове*.

Дискове и дискови дялове

Основното запаметяващо устройство в PC-тата е *твърдият диск*. Размерите на тези устройства варират; ранните дискове съхраняваха само 5 MB данни. Модерните твърди дискове са способни да запаметят 120 GB и повече.

Един твърд диск се състои от пакет от дискове, работещ като грамофон. Само че докато каналът в грамофонната плоча представлява спирала от външния край до центъра, данните се записват на диска в концентрични окръжности, наречени *пътечки*.

Дисковото устройство има няколко *глави* (поне две), които четат и записват данни. Главите стоят неподвижно над пътечките, докато дискът между тях се върти. Скоростта на въртене се измерва в обороти в минута (rotates per minute – rpm), например 5400 rpm. Времето за достъп до диска, наречено *време за търсене*, се измерва в милисекунди – например 9 ms.

Времето за обръщение към данните на диска е много по-голямо от времето за обръщение към данните в RAM паметта, защото достъпът до диска изисква механични движения на физически обекти (главите за четене/запис). Механичното движение отнема време. Обръщението към RAM паметта отнема само толкова, колкото електричеството да протече през веригата. Това е по-бавно от скоростта на светлината, но по-бързо от придвижването на механиката на диска.

Съхранените на диска данни се разполагат според техния *сектор*, пътечка и *цилиндър*. Както беше дефинирано по-рано, пътечката е концентрична окръжност на диска. Един цилиндър представлява всички пътечки на едно и също място, но на различните дискови плочи. Секторът е част от една пътечка. Файловата система трябва да запомни точното физическо местоположение на диска, така че данните да могат да бъдат открити отново при необходимост.

Много от съвременните дискове са с голям капацитет. За по-доброто организиране на файловете можете да разделите един диск на няколко *дяла*, които за операционната система изглеждат като отделни *дискови устройства*. След това на всеки дял се назначава буква на устройство. Например можете да разделите един диск на дялове, така че да съхраните файловете на операционната система в един дял, приложният софтуер в друг, а потребителските данни в трети. Например, ако вашият диск е 15 GB, можете да създадете три дяла от по 5 GB.

ЗАБЕЛЕЖКА Дяловете *не е* задължително да са с един и същ размер. Един 15 GB твърд диск може да бъде разделен на дялове от по 2 GB, 5 GB, 7 GB и 1 GB.

Дисковете се *разделят на дялове* чрез използване на помощен софтуер. Такива програми, каквато например е командата FDISK в DOS, Windows 9*x* и Linux, или Disk Management инструментите в Windows NT и Windows 2000, могат да са вградени в операционната система. Съществуват и програми на независими компании – например Partition Magic.

В операционната система DOS, един диск може да има до четири *главни (primary)* дяла. На мястото на един от главните дялове можете да създадете *разширен (extended)* дял, в който пък можете да създадете множество *логически устройства (logical drives)*. Един главен дял трябва да бъде маркиран като *активен*. Това е дялът, от който компютърът извършва първоначално зареждане.

Ако притежавате множество хартиени документи (например финансови записки от няколко години насам), които искате да съхраните в шкаф, бихте могли да ги пъхнете всички в едно голямо чекмедже. Другият вариант е да ги сортирате, като поставите архивите от 1996 година в едно чекмедже, тези от 1997 година в друго, и т.н. По подобен начин разделянето на дялове на вашия диск ви помага да сортирате и организирате електронните си данни.

Съществуват две допълнителни причини за разделяне на един диск на дялове:

- Различните дялове могат да се форматират за различни файлови системи. Това означава, че устройство C може да е форматирано за FAT16, устройство D за FAT32, а устройство E за NTFS.
- В отделните дялове могат да бъдат инсталирани различни операционни системи, които могат да се зареждат по желание на потребителя. Въпреки че е възможно да се инсталират множество операционни системи на един и същ дял (ако могат да използват една файлова система), това не се препоръчва, защото е възможно да повредят файловете си взаимно.

Windows 2000 представи нова концепция за операционните системи на Microsoft – *динамични дискове*. Когато конвертирате даден диск в динамично състояние, вие създавате томове на диска, вместо дялове. Размерите на тези томове могат да се променят динамично, без да се изтриват данни. Можете да комбинирате парчета пространство от множество физически дискове в един том, за да осигурите по-голяма област за съхранение или *отказоустойчивост*. Повече за отказоустойчивостта при дисковете има в Глава 14, „Защита на мрежата“.

Един том функционира като единичен запис, въпреки че е възможно да е изграден от два или повече диска; за достъп до обединеното пространство се използва само една буква на устройство.

Общоизползвани настолни операционни системи

В тази секция разглеждаме следните общоизползвани настолни операционни системи, функциониращи като клиенти в мрежова среда от тип клиент/сървър:

- MS-DOS and Windows 3.x
- Windows 9x
- Windows NT Workstation
- Windows 2000 Professional
- Linux/UNIX
- Macintosh
- OS/2

Оставащите секции от тази глава включват постъпкови процедури и изображения на екрани, показващи как да конфигурирате мрежовите компоненти на някои настолни операционни системи. Забележете, че текстът не е поднесен като ръководство от типа „how-to" (вижте секцията „Допълнителни източници" в края на главата за препратки към подробни ръководства с инструкции). По-скоро тези секции са предназначени да ви покажат как се прави настройка на мрежата във всяка от операционните системи, като по този начин се запознавате с интерфейса, използван за конфигуриране.

MS-DOS и Windows 3.*x*

Въпреки че професионалистите в областта на информационните технологии може да ги смятат за архаични, много от все още действащите компютри в света на бизнеса използват „стари" операционни системи на Microsoft, като например MS-DOS.

Съществуват няколко добри причини за използване на MS-DOS:

- **MS-DOS е проста операционна система с минимални изисквания по отношение на системата** – Изискванията за памет и процесор са много ниски. DOS работи перфектно на вече остарял хардуер.
- **MS-DOS е евтин** – Не само операционната система е евтина, но и цената на съвместимия хардуер е ниска.
- **MS-DOS е стабилен и надежден** – Тъй като той не е многозадачна операционна система (в дадено време работи само една програма), няма нужда да се тревожите за конфликти и сривове, причинени от споделени адреси от паметта.
- **MS-DOS е лесен за научаване и използване** – Въпреки че не е толкова интуитивен, колкото една GUI-базирана операционна система, веднъж, след като научите синтаксиса на командите, DOS става относително прост за използване.

- **Съществуват много програми за MS-DOS** – Тъй като беше стандарт в продължение на много години, за тази операционна система бяха написани множество програми. Някои компании продължават да използват MS-DOS, защото специално написаният за техните нужди софтуер не работи добре под по-новите операционни системи.

Разбира се, съществуват много недостатъци при използването на тази остаряла операционна система. MS-DOS е 16-битова система и не може да изпълнява сложните графични програми, написани за 32-битовите Windows операционни системи. Липсата на многозадачност в най-добрия случай е едно голямо неудобство в съвременния корпоративен свят. Файловата система FAT – единствената, която DOS използва – предлага много малко в областта на сигурността. Освен това при работа в мрежа, MS-DOS клиентите може да не успеят да се свържат със споделени ресурси, използващи дълги файлови имена. Накрая, много потребители се плашат от командния интерфейс.

Изпълняването на Windows 3.*x* върху MS-DOS може да намали някои от тези недостатъци. Графичната среда на Windows 3.*x* поддържа *съвместна многозадачност (cooperative multitasking)*, което позволява на потребителите да стартират повече от една програма едновременно.

Съвместна и изместваща многозадачност

Съвместната многозадачност (cooperative multitasking) е среда, в която програмите споделят адреси от паметта и обменят информация. В среда със съвместна многозадачност приложенията споделят използването на процесора чрез метод, познат като *квантуване на време (time slicing)*. Приложните програми са написани така, че да връщат процесора след зададено количество време, за да може той да се използва от други програми, работещи едновременно. Ако програмата е написана зле, тя може да монополизира процесора, а ако някое от приложенията се срине, може да повлече и останалите със себе си.

Една по-ефективна форма на многозадачност се нарича *изместваща многозадачност (preemptive multitasking)* (наричана също и изпреварваща многозадачност или приоритетна многозадачност – б.р.), и се използва от Windows 9*x*, Windows NT и Windows 2000. Операционната система в този случай контролира разпределението на процесорното време, а 32-битовите програми работят в техни собствени адресни пространства. При изместващата многозадачност една непокорна програма не може да „превземе" системата, а ако някоя програма се срине, тя не засяга останалите.

MS-DOS и Windows 3.1 изискват от вас да инсталирате допълнителен софтуер за *мрежов клиент*, за да можете да се свържете в мрежа. Windows for Workgroups 3.11 е първата операционна система на Microsoft с вградени мрежови компоненти. Въпреки че са разработени за равноправни мрежи, Windows 3.*x* и MS-DOS могат да се използват за връзка с Windows NT или Windows 2000 домейн, стига да са конфигурирани правилно. Забележете, че тези машини не притежават компютърни акаунти в домейна; можете да ги използвате за логване в домейна (с подходящото потребителско име и парола) и използване на ресурси, но не можете да се присъедините към домейна.

Windows 9*x*

Microsoft Windows 95 беше проектиран за лесна работа в режа, като традицията беше пренесена и доразвита в Windows 98. Тези операционни системи се наричат с общото наименование Windows 9*x* и включват следните продукти:

- **Windows 95a** – Оригиналната версия на 32-битовата потребителска операционна система на Microsoft.
- **Windows 95b** – Нарича се още OSR2 и включва подобрения като FAT32 поддръжка. Тази версия се доставяше само на OEM производителите за инсталиране на продаваните от тях компютри.
- **Windows 98** – Ъпгрейд на Windows 95, който добави технологията Active Desktop, интерфейса ACPI (Advanced Configuration and Power Interface), поддръжка на универсалната серийна шина (universal serial bus – USB) и TV-тунер карти, както и подобрения по отношение на инсталирането и поддръжката.
- **Windows 98 Second Edition (SE)** – Въведен е Web браузърът Internet Explorer 5.0, по-силно криптиране при dialup networking, и е добавена поддръжка за споделяне на Интернет връзка (Internet Connection Sharing – ICS).
- **Windows Millennium Edition (Windows ME)** – Това е следващата операционна система за крайни клиенти от Microsoft и по принцип се води част от фамилията 9*x*. Възможностите на Windows ME включват следното:
  - Разширена мултимедийна поддръжка, която улеснява работата с филми и цифрови фотографии
  - Вградени възможности за възстановяване от бедствия, които ви позволяват да възстановите системата до предварително определено състояние
  - Опростяване на конфигурирането, изисквано за установяване на проста равноправна мрежа
  - По-бързо стартиране и изключване (при използване на хардуер с поддръжка на технологията FastBoot)

Операционната система Windows 9*x* включва клиент за Microsoft мрежи и клиент за NetWare. NetBEUI, TCP/IP и NWLink мрежовите и транспортните протоколи също са включени в операционната система. Вградена е и функцията Dialup networking за свързване към Интернет или отдалечена LAN мрежа.

Поради възможностите си за свързване, Windows 9*x* е една от най-популярните клиентски операционни системи в бизнес света. От няколко години насам това е предпочитаната настолна операционна система както в малките, така и в големите компании, а също и при създаването на равноправни мрежи.

Windows 9*x* поддържа 32-битови приложения, но включва и 16-битов кода за обратна съвместимост с програми за DOS и Windows 3.*x*. Използва се VFAT за дълги файлови имена, а Windows 95b, 98 и ME могат да използват FAT32 за по-ефективно управление на дисковото пространство.

Някои от преимуществата на Windows 9x като настолна операционна система и мрежов клиент включват следното:

- По-евтин е от Windows NT и Windows 2000.

- Изпълнява широка гама от DOS, 16-битови и 32-битови Windows приложения.
- Интерфейсът е познат на повечето PC потребители.
- Съществува клиентски софтуер за Windows 9x, предназначен за свързване с повечето типове мрежови операционни системи, като Windows, NetWare, UNIX и Linux.

ЗАБЕЛЕЖКА Novell не разработва настолни операционни системи. повечето клиентски машини в мрежите на NetWare използват Windows настолни операционни системи, които притежават клиентски софтуер на Novell или вградени компоненти за NetWare клиент. Novell също така осигурява и DOS клиент. Prosoft Engineering предлагат Macintosh Connectivity Solutions for NetWare.

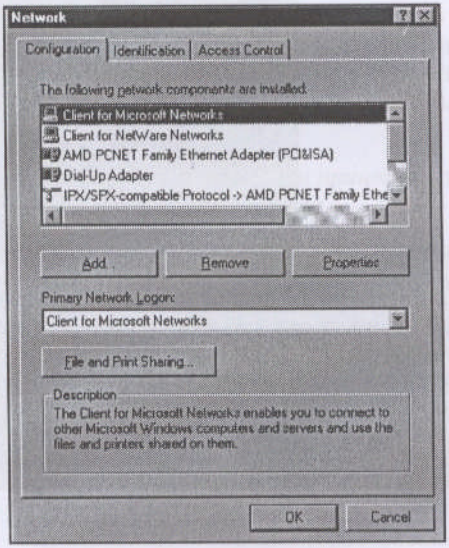
В следващите секции ще научите основите на свързването на Windows 9*x* клиент към Microsoft мрежа, NetWare мрежа или сървър за отдалечен достъп.

Свързване на Windows 9*x* клиент към мрежа на Microsoft

При Windows 9*x*, мрежовите компоненти са вградени в самата операционна система. Можете да конфигурирате компютъра като част от равноправна мрежа (работна група), или можете да се логвате в Windows NT или Windows 2000 домейн, за който имате валиден акаунт.

Мрежовите настройки се конфигурират в диалоговия прозорец със свойствата на мрежата (Network Properties), показан на Фигура 12-4, който се отваря чрез избор на Start, Settings, Control Panel, Network, или чрез щракване с десния бутон на мишката върху иконата Network Neighborhood на десктопа и избор на Properties от контекстно меню.

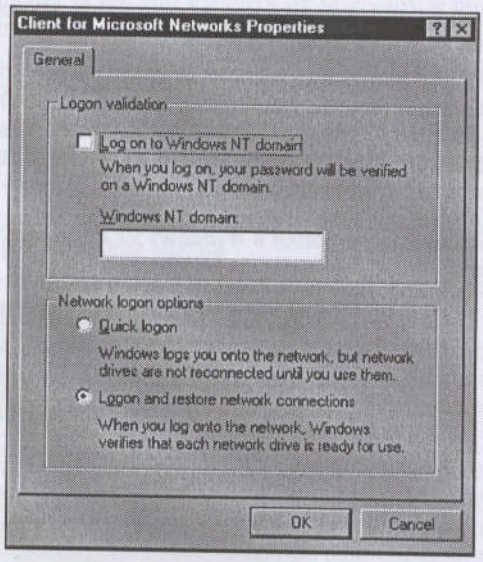
Фигура 12-4 *Мрежовите настройки в Windows 9x се конфигурират от диалоговия прозорец Network.*



За да установите един Windows 95 или Windows 98 компютър като равноправен в една Microsoft работна група, изпълнете следните стъпки:

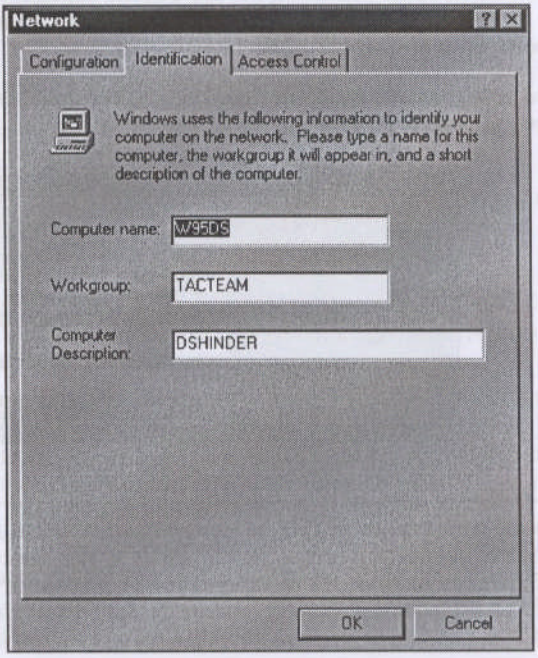
1. Уверете се, че е инсталирана мрежова карта (NIC), която е свързана чрез кабел или друга преносна среда към мрежата.
2. Инсталирайте софтуерните драйвери за мрежовата карта според инструкциите на производителя.
3. В страницата Configuration на диалоговия прозорец Network Properties се уверете, че е инсталиран клиентът Client for Microsoft Networks. Ако не е, можете да го инсталирате, като щракнете върху бутона Add и го изберете от списъка. Възможно е да бъдете подканени да пъхнете инсталационния диск на Windows 9x.
4. Ако използвате компютъра, за да се логвате в Windows NT или Windows 2000 домейн, конфигурирайте логването, като изберете Client for Microsoft Networks и щракнете върху бутона Properties. След това се появява диалоговият прозорец, показан на Фигура 12-5. Отбележете полето за отметка и въведете името на домейна. Можете да изберете или Quick logon, което не възстановява мапнатите мрежови устройства, докато не ги използвате, или Logon and restore network connections.

Фигура 12-5 *Трябва да конфигурирате свойствата на клиента, ако ще използвате компютъра да се логвате в Windows домейн.*



5. В страницата Identification, както е показано на Фигура 12-6, се уверете, че компютърът има уникално за мрежата име. Това име може да е с дължина до 15 буквено-цифрови знака. Ако компютърът ще бъде член на работна група, въведете и името на групата. Имам място и за опционално описание на компютъра.

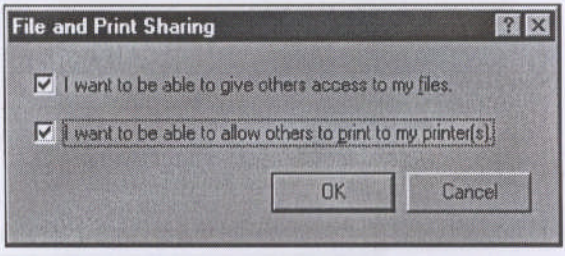
Фигура 12-6 *Името на компютъра и това на работната група се конфигурират в страницата Identification.*



6 Трябва да имате инсталиран поне един мрежов или транспортен протокол, който да е свързан с мрежовата карта. Този протокол трябва да е инсталиран и на другите компютри в мрежата – тези, с които искате да комуникирате. Протоколите се добавят, премахват и конфигурират от страницата Configuration. За да видите всички инсталирани компоненти, трябва да скролирате надолу.

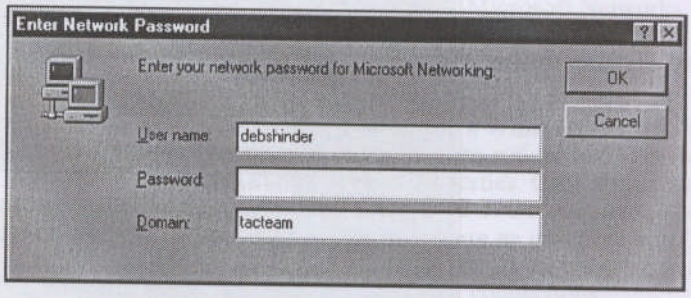
7 Ако искате да споделяте ресурсите на този компютър в мрежата, трябва да разрешите споделянето на файлове и принтери. Това се прави, като щракнете върху бутона File and Print Sharing в страницата Configuration и след това отбележите подходящите полета за отметка, както е показано на Фигура 12-7.

Фигура 12-7 *Трябва да разрешите споделянето на файлове и принтери, за да направите ресурсите на компютъра достъпни по мрежата.*



След като конфигурирате свойствата на мрежата, трябва да рестартирате компютъра, за да могат промените да влязат в действие. Ако конфигурационните промени са били успешни, когато отново заредите Windows, ще видите диалогов прозорец за логване, който ви подканва да въведете потребителско име и парола. Вижте Фигура 12-8.

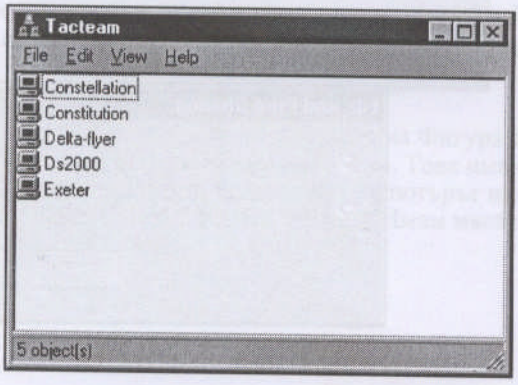
Фигура 12-8 *След като конфигурирате свойствата на мрежата и рестартирате компютъра, ще видите прозорец за логване в мрежата.*



ЗАБЕЛЕЖКА Ако ще използвате TCP/IP за мрежова комуникация, трябва да конфигурирате неговите свойства с подходящ IP адрес и подмрежова маска (и евентуално подразбиращ се шлюз) или да конфигурирате компютър да бъде DHCP (Dynamic Host Configuration Protocol) клиент. Един DHCP клиент заявява IP адрес от DHCP сървъра при първоначалното си свързване към мрежата.

Сега можете да щракнете двукратно върху Network Neighborhood и ще видите списък на компютрите в мрежата, които се намират във вашата работна група или домейн. (В този списък се показват компютри, на които е разрешено споделянето на файлове и принтери, както Windows NT и Windows 2000 машини, на които е стартирана услугата server.) Този списък се нарича *списък за браузване (browse list)*. Ако компютърът е логнат в домейн, ще трябва да щракнете върху името на домейна, за да видите списъка на компютрите, както е показано на Фигура 12-9.

Фигура 12-9 *Когато мрежовите компоненти са конфигурирани правилно, виждате списък на компютрите в Network Neighborhood.*



Осъществяването на достъп до ресурсите на компютрите в мрежата е става просто чрез двукратно щракване върху името на компютъра, стига потребителският ви акаунт да има подходящите позволения. Позволенията за достъп за дискутирани по-задълбочено в Глава 14.

Свързване на Windows 9*x* клиент към NetWare мрежа

Един Windows 9*x* компютър може да функционира като клиент на NetWare сървър по един от следните два начина:

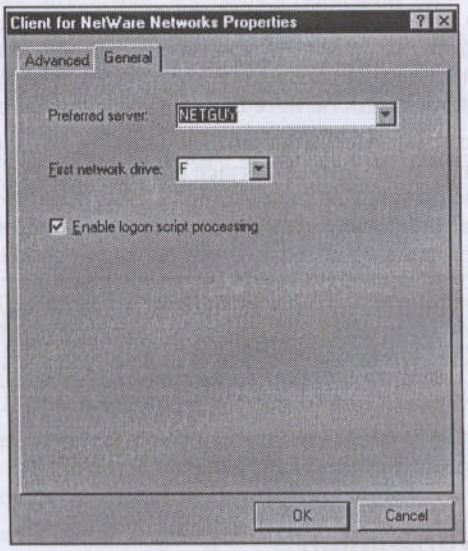
- Чрез използване на клиента Client for NetWare Networks на Microsoft, който е включен на инсталационното CD на Windows 9x (но не се използва по подразбиране)
- Чрез използване на Novell клиент за Windows 95/98

На една машина не могат да се инсталират и двата клиентски софтуерни пакета на NetWare.

Протоколният стек IPX/SPX се изисква за свързване към всички NetWare сървъри преди версия 5.0. NWLink – реализацията на Microsoft на IPX/SPX, се инсталира автоматично, когато инсталирате Client for NetWare Networks на Microsoft. Microsoft клиентът се инсталира като мрежов компонент в страницата Configuration на диалоговия прозорец Network Properties.

Избирането на Client for NetWare Networks и щракването върху бутона Properties ви позволява да настроите предпочитания NetWare сървър, както е показано на Фигура 12-10. Ако оставите това поле празно, компютърът се опитва да се логне в най-близкия NetWare сървър.

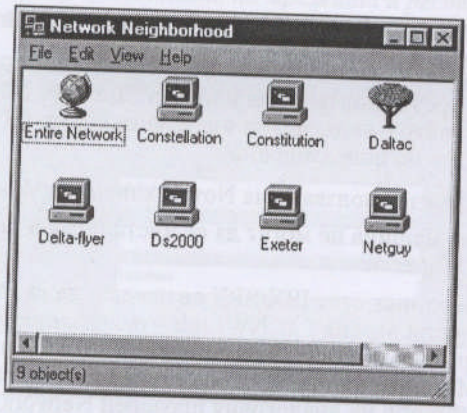
Фигура 12-10 *Можете да изберете предпочитан NetWare сървър, в който да се логва вашата Windows 9x машина.*



След инсталирането и конфигурирането на NetWare клиента трябва да рестартирате компютъра.

След като инсталирате и конфигурирате NetWare клиента (NWLink), в Network Neighborhood ще видите NetWare дървото. На Фигура 12-11 то се вижда под името Daltac.

Фигура 12-11 *NetWare дървото се появява в Network Neighborhood, след като инсталирате NetWare клиентски софтуер.*



В Windows 9*x* можете лесно да осъществите достъп до NetWare ресурсите, като навигирате из дървото и щракате двукратно върху избраните ресурси, стига да имате необходимите позволения на NetWare сървъра. За потребителя, NetWare ресурсите се изглеждат като тези на Microsoft сървър.

Свързване на Windows 9*x* клиент към отдалечен сървър

Лесно е да свържете Windows 9*x* компютър към отдалечен компютър по телефонна линия. За целта Microsoft включва компонента Dialup Networking. За да създадете dialup връзка, трябва най-напред да инсталирате и конфигурирате модем. Dialup връзките се конфигурират през аплета Dialup Networking, до който можете да достигнете през иконата My Computer на десктопа.

Можете да използвате dialup networking, за да се свържете с доставчик на Интернет услуги (Internet service provider – ISP) или RAS сървър. Windows 9*x* сам по себе си може да бъде dialup сървър; тази възможност се инсталира и конфигурира чрез аплета Add/Remove Programs в Control Panel.

ЗАБЕЛЕЖКА За да използвате dialup networking в Windows 95, е необходимо да е инсталиран пакетът Microsoft Plus! (група от допълнителни компоненти за операционната система). Windows 98 обаче включва тези компоненти в себе си.

Услугата за отдалечен достъп (remote access service – RAS) е дискутирана по-подробно в Глава 15, „Отдалечен достъп“.

Windows NT Workstation

Windows NT Workstation беше първата настолна операционна система на Microsoft, насочена към корпоративния пазар. Последната версия е NT 4.0 и притежава потребителски интерфейс, подобен на този в Windows 95. Някои компа-

нии все още използват NT 3.*x*, който е с Windows 3.*x* интерфейс. Windows NT беше проектиран да осигури по-стабилна среда за критични бизнес приложения.

ЗАБЕЛЕЖКА Когато беше пусната първата версия на Windows NT, Microsoft казаха, че акронимът означава „New Technology" (нова технология). Наскоро обаче от компанията заявиха, че „NT" е съвсем самостоятелна приставка и не е акроним.

Някои преимущества на Windows NT Workstation като настолна операционна система и мрежов клиент включват следното:

- Това е истинска 32-битова операционна система, поддържаща изместваща многозадачност и по-голяма стабилност на системата.
- Включва сигурност на пет нива, както и компресиране на данни на ниво файл.
- Притежава обратна съвместимост с много 16-битови програми, без да се жертва надеждността. NT изпълнява DOS и по-стари Windows програми във виртуални машини (VMs). При използване на този метод, ако едно приложение се срине, то не засяга останалите, нито пък изисква рестартиране на операционната система.

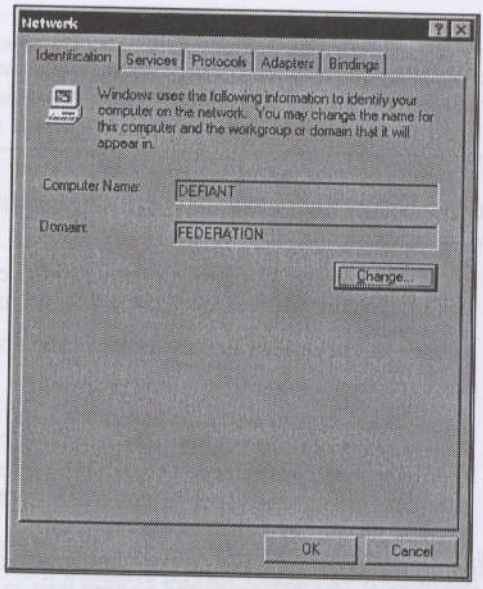
Мрежовата интеграция е основният фокус в дизайна на Microsoft относно Windows NT; освен това NT включва поддръжка за масово разпространените мрежови карти, както и софтуер, необходим за свързване с Microsoft и NetWare мрежи. Способността за функциониране като клиент за отдалечен достъп или сървър също е вградена.

Свързване на Windows NT Workstation към мрежа на Microsoft

Windows NT Workstation може да работи като равноправна машина в една Microsoft мрежа, или като клиент в домейни, базирани на NT Server. Свързването на една NT Workstation машина към Windows мрежа включва следните стъпки:

1. Уверете се, че мрежовата карта е инсталирана и свързана правилно чрез кабел или друга преносна среда към мрежата.
2. Инсталирайте софтуерните драйвери за мрежовата карта според инструкциите на производителя. Уверете се, че драйверите са написани за Windows NT.
3. Конфигурирайте свойствата на мрежата чрез аплета Network. Можете да го отворите, като изберете Start, Settings, Control Panel, Network, или като щракнете с десния бутон на мишката върху иконата Network Neighborhood на десктопа и изберете Properties от контекстното меню.
4. В страницата Identification, която е показана на Фигура 12-12, дайте на компютъра уникално име в мрежата. Това име може да има не повече от 15 буквено-цифрови знакове.
5. Въведете име на домейна (или работната група), към който компютърът ще принадлежи, както е показано на Фигура 12-12.

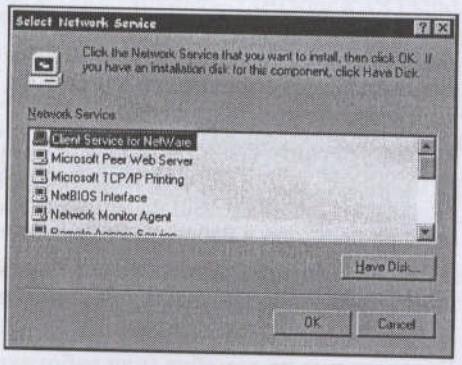
Фигура 12-12 *В страницата Identification на диалоговия прозорец Network се въвеждат уникално име на компютъра и името на домейна.*



Свързване на Windows NT Workstation към NetWare мрежа

Както при Windows 9*x*, лесно е да свържете един NT Workstation 4.0 компютър към NetWare мрежа. Microsoft осигурява Client Services for NetWare (CSNW) на инсталационното CD за NT Workstation; алтернативата е да си свалите клиента на Novell за NT от www.novell.com. NWLink се инсталира автоматично, когато инсталирате CSNW. Фигура 12-13 показва конфигурационния екран на CSNW.

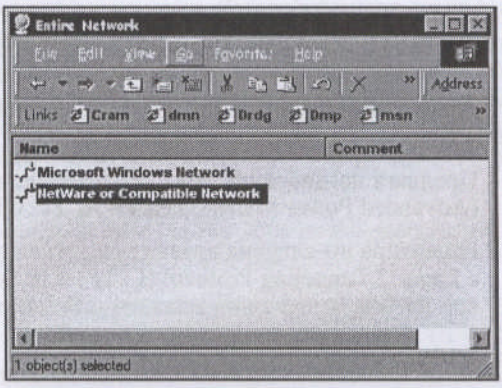
Фигура 12-13 *Услугата CSNW може да се използва за свързване на една Windows NT 4.0 машина с NetWare сървър.*



След като CSNW се инсталира на работната станция, в Control Panel се появява аплет. CSNW се конфигурира чрез него.

След като CSNW се инсталира и конфигурира, NetWare мрежата се появява в Network Neighborhood, както е показано на Фигура 12-14. Браузването и свързването към ресурси на NetWare, за които имате позволения, става по същия начин като при ресурсите на Microsoft сървърите.

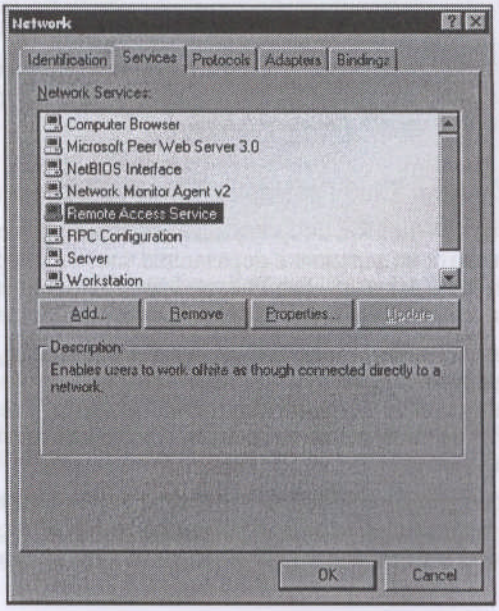
Фигура 12-14 *След като CSNW се инсталира, можете да достигнете до NetWare мрежата през Network Neighborhood.*



Свързване на Windows NT Workstation към отдалечен сървър

Конфигурирането на NT Workstation за свързване към отдалечен сървър е малко по-сложно, отколкото изпълнението на същата задача в Windows 9*x*. RAS най-напред трябва да се инсталира като услуга в конфигурационния диалогов прозорец Network, който е показан на Фигура 12-15.

Фигура 12-15 *RAS се инсталира като услуга в диалоговия прозорец Network.*



Windows 2000 Professional

Windows 2000 е една от съвременните настолни операционни системи на Microsoft за корпоративния сектор. Подобно на Windows 2000 Server продуктите, Professional версията е базирана на ядрото на NT, но включва множество подобрени и разширени възможности. За разлика от NT Workstation, Windows 2000 Professional поддържа Plug and Play технологията, може да се инсталира на твърди дискове, форматирани с FAT32, и включва криптиране на файлове с цел обезопасяване на данните на диска. За разлика от Windows 9*x*, Windows 2000 Professional осигурява високо ниво на сигурност и стабилност за критичните задачи.

Други преимущества на Windows 2000 Professional като настолна операционна система и мрежов клиент включват следното:

- Предлага по-добра поддръжка за мобилните потребители чрез APM (Advanced Power Management) и ACPI. Windows NT не поддържа ACPI.
- Гарантира по-сигурна връзка при изграждане на виртуална частна мрежа с Layer 2 Tunneling Protocol (L2TP) и IP Security (IPSec). По-ранните версии на Windows поддържаха само Point-to-Point Tunneling Protocol (PPTP) за VPN мрежи.
- Възможността за офлайн папки ви позволява да копирате и синхронизирате документи от мрежата в своята локална система, така че да осъществявате достъп до тях, когато компютърът ви не е свързан към мрежата.
- Протоколът IPP (Internet Printing Protocol) ви позволява да печатате към URL адрес и да управлявате принтери през интерфейса на Web браузъра.
- Вграденият дисков дефрагментатор и останалите инструменти и помощни програми ви помагат да поддържате и да управлявате операционната система. Последните трябва да се закупят отделно от независими производители.
- Поддържа Kerberos сигурност; можете да използвате възможностите на един Windows 2000 домейн като Active Directory клиент.

В следващите секции ще научите как да свързвате един Windows 2000 Professional компютър към мрежа на Microsoft, към мрежа на NetWare, или към сървър за отдалечен достъп (RAS).

Свързване на Windows 2000 Professional към мрежа на Microsoft

Тъй като Windows 2000 Professional беше проектиран за бизнес потребители, мрежовата поддръжка е неразделна част от операционната система. Мрежовият адаптер се открива чрез Plug and Play още при стартирането на компютъра. За всяка открита мрежова карта автоматично се създава мрежова връзка.

За лаптопите и останалите компютри, които ще работят с мрежова връзка само в определени моменти, а през останалото време ще бъдат изключени от мрежата, могат да се създадат *хардуерни профили*. Това елиминира проблема с показването на съобщения за грешка, когато компютърът не успява да открие мрежата.

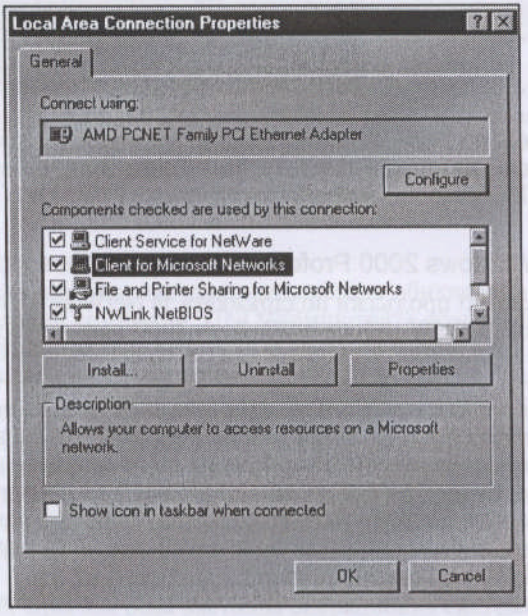
Конфигурирането на LAN връзка включва същите основни задачи, дискутирани в секцията „Свързване на Windows NT Workstation към мрежа на Microsoft“ по-рано в тази глава. TCP/IP се инсталира като подразбиращ се мрежов транс-

портен протокол, а информацията за IP адресите може да се установи или ръчно, или компютърът да се конфигурира като DHCP клиент.

За разлика от NT, Windows 2000 поддържа автоматично частно IP адресиране (Automatic Private IP Addressing – APIPA). APIPA позволява на един DHCP клиент, който не може да открие DHCP сървър, да си самоназначи IP адрес. След това компютърът ще може да комуникира с останалите компютри в същия сегмент, които също са си самоназначили APIPA адреси. При NT клиентите, ако DHCP сървърът е изключен, когато клиентът стане онлайн, TCP/IP на клиента се забранява.

Свойствата за конфигуриране на мрежата са достъпни през аплета Network and Dial-up Connections в Control Panel, или чрез избор на Start, Settings, Network and Dialup Connections. Фигура 12-16 показва диалоговия прозорец Local Area Connection Properties, където добавяте, премахвате и конфигурирате мрежовите клиенти услуги и протоколи.

Фигура 12-16 *Мрежовите компоненти на Windows 2000 се конфигурират от диалоговия прозорец Local Area Connection Properties.*

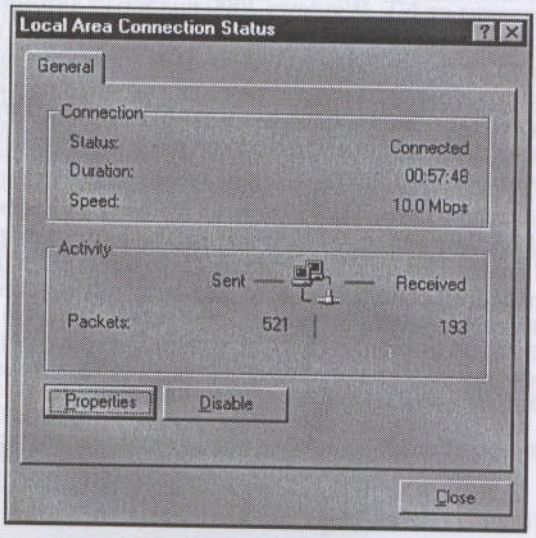


Диалоговият прозорец за състоянието на връзката, показан на Фигура 12-17, осигурява полезна информация, включваща следното:

- Дали мрежовата връзка е активна (етикетът Status) и колко време компютърът е свързан към мрежата (етикетът Duration)
- Скоростта на връзката в мегабитове в секунда (обикновено 10 или 100 за Ethernet връзка)
- Броят на изпратените и получените пакети

Можете да забраните връзката в този диалогов прозорец, или да щракнете върху бутона Properties, за да промените конфигурацията.

Фигура 12-17 *Диалоговият прозорец Local Area Connection Status осигурява информация относно указаната мрежова връзка.*



Windows 2000 поддържа широка гама от LAN и WAN връзки. Освен Ethernet, поддържаните връзки включват Token Ring, кабелен модем, DSL, FDDI, IP по ATM, безжична инфрачервена връзка (IrDA) и ATM LAN емулация (LANE).

Свързване на Windows 2000 Professional към NetWare мрежа

Microsoft продължи поддръжката за NetWare клиенти в Windows 2000 Professional. CSNW работи в Windows 2000 така както и в Windows NT.

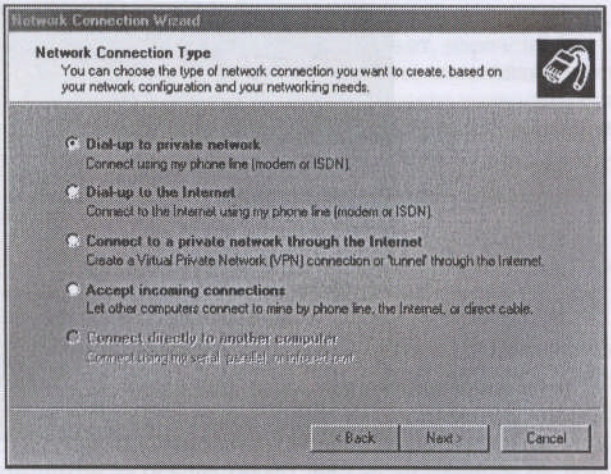
ЗАБЕЛЕЖКА Забележете, че CSNW се използва за свързване на Windows 2000 компютър към NetWare 4.x и по-ниска версия. Ако NetWare сървърът е версия 5.x, която работи изключително с IP, не можете да се свържете към него посредством CSNW. Вместо това трябва да използвате NetWare клиент (редиректор), който е съвместим с NetWare Core Protocol (NCP) и който поддържа IP. Подходящ клиент може да бъде свален от www.novell.com. Алтернативно можете да стартирате IP/IPX шлюза в NetWare 5.x.

В Windows 2000, CSNW се инсталира като услуга за мрежов клиент в диалоговия прозорец Network, както е показано на Фигура 12-15.

Свързване на Windows 2000 Professional към отдалечена мрежа

Windows 2000 включва съветника New Connection Wizard, който ви превежда през процеса на установяване на връзка към сървър за отдалечен достъп. Използвайки съветника, можете бързо да установите dialup връзка към отдалечена частна мрежа или към Интернет, да създадете VPN мрежа чрез тунел през Интернет, или да установите Windows 2000 Professional да действа като dialup сървър и да приема входящи връзки, както е показано на Фигура 12-18.

Фигура 12-18 *Съветникът Network Connection Wizard ви помага да конфигурирате dialup и VPN връзки, както и да установявате сървъри за отдалечен достъп.*



Windows 2000 може да бъде конфигуриран да се свързва директно с друг компютър през сериен, паралелен или инфрачервен порт. Тази възможност може да се използва за свързване на палм компютри към Windows 2000 компютър, което ви позволява да качвате и сваляте файлове от единия компютър на другия.

Linux/UNIX

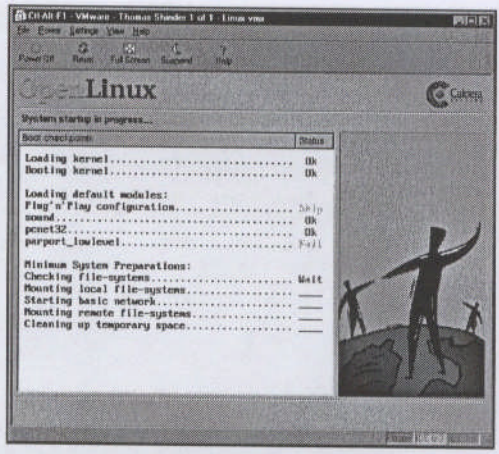
UNIX е мощна операционна система, изпълнявана обикновено на мрежови сървъри, а не на настолни компютри. UNIX компютрите обаче могат да осъществяват достъп до файловете на Microsoft и NetWare мрежи чрез използване на масово достъпни софтуерни допълнения.

Linux направи значителен пробив в света на бизнеса като мрежова операционна система (NOS). Използването му като корпоративна настолна операционна система обаче е рядко. Въпреки че съществуват GUI интерфейси, които правят Linux по-дружелюбен към потребителя, както е показано на Фигура 12-19, се изисква едно по-високо ниво на експертност от страна на потребителя, отколкото е при повечето останали настолни операционни системи. Въпреки това много компании (като RedHat, SuSE, Corel, Caldera и TurboLinux) се борят да направят от Linux една значима настолна операционна система.

В последните дистрибуции на Linux мрежовите компоненти са вградени в операционната система с цел свързване към LAN мрежа или установяване на dialup връзка за връзка с Интернет или друга отдалечена мрежа. Всъщност TCP/IP е интегриран в ядрото на Linux, вместо да се реализира като отделна подсистема.

Когато реализирате Linux като настолна система, трябва да вземете предвид поддръжката на наличните приложения. Броят на бизнес приложенията е ограничен, когато се сравнява с приложенията, написани за Windows. Само че някои производители осигуряват софтуер за емулиране на Windows (като WABI и WINE), който ви позволява да стартирате множество Windows приложения под Linux. Освен това компании като Corel правят Linux версии на своите офис пакети и друг популярен софтуер.

Фигура 12-19 *Модерните дистрибуции на Linux осигуряват графични потребителски интерфейси за една по-дружелюбна към потребителя среда.*



Някои от преимуществата на Linux като настолна операционна система и мрежов клиент включват следното:

- Това е истинска 32-битова операционна система.
- Поддържа изместваща многозадачност и виртуална памет.
- Кодът е отворен, което позволява на всеки да го разширява и подобрява.
- Може да споделя файлове с UNIX, NetWare, Windows и Macintosh системи.

В следващите секции дискутираме, как се свързва Linux/UNIX клиент към Microsoft мрежа, към NetWare мрежа, или към Интернет през dialup сървър за отдалечен достъп.

ЗАБЕЛЕЖКА Въпреки че UNIX по-често се реализира като сървърна операционна система, UNIX машините могат да функционират и като мрежови клиенти. В много случаи конфигурирането и командите за UNIX са същите като тези в Linux системите. Само че, понеже както UNIX, така и Linux съществуват в множество различни версии, инструкциите в следващите секции може и да не са приложими за всяка дистрибуция на UNIX или Linux. По принцип можете да използвате командата **man**, за да отворите ръководството за вашата специфична версия.

Свързване на Linux/UNIX клиент към мрежа на Microsoft

Linux работните станции могат да осъществяват достъп до файлове на Microsoft сървър, като използват SMB файлова система (SMBFS), базирана на кода на Samba. (Дискутираме Samba по-подробно в Глава 13, „Хибридни мрежи“.) UNIX системите могат да използват SMB клиентския софтуер, който е част от пакета Samba, за да се свързват към отдалечени SMB дялове (например такива на Microsoft сървър), да прехвърлят файлове и да печатат на отдалечени принтери.

ЗАБЕЛЕЖКА SMB е протоколът Server Message Block, който се използва от сървърите на Microsoft за споделяне на файлове.

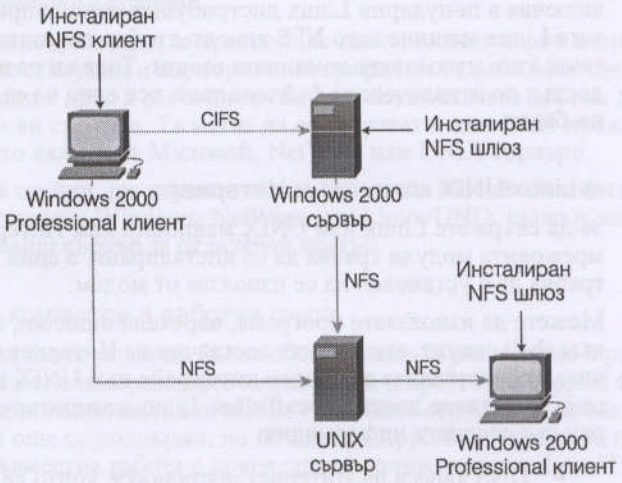
Microsoft осигурява допълнителен софтуерен пакет, наречен Microsoft Services for UNIX, който се състои от няколко компонента, използвани за интегриране на UNIX и Windows мрежи. Той използва NFS, което позволява споделяне на ресурсите между мрежови операционни системи чрез използване на RPC.

Компонентът на Microsoft, наречен Services for UNIX, включва NFS клиент, NFS сървър и NFS шлюз. Тези компоненти осигуряват следните функционалности:

- Споделяне на файлове и принтери между UNIX и Windows машини
- Отдалечен достъп от команден ред между Windows и UNIX машини
- Синхронизиране на пароли между Windows и UNIX машини

На Windows 2000 Professional машините се инсталира клиент за NFS, за да позволи достъп до файлове на UNIX компютри. На компютри, работещи под Windows 2000 Professional или Server, се инсталира сървър за NFS, за да позволи на UNIX компютри да осъществяват достъп до файлове на Windows машини. NFS шлюзът се инсталира на Windows 2000 сървъри, за да им позволи да действат като шлюз между CIFS протокола, използван от Windows 2000, и NFS протокола, използван от UNIX мрежите, както е показано на Фигура 12-20. Services for UNIX работи с няколко версии на UNIX и RedHat Linux.

Фигура 12-20 *Services for UNIX на Microsoft позволяват съвместна работа между Windows и UNIX мрежи.*



Свързване на Linux/UNIX клиент към NetWare сървър

Linux или UNIX могат да бъдат конфигурирани като NCP клиенти за достъп до файлове и принтери в NetWare мрежи. Съществува модул за ядрото на Linux, който може да монтира NetWare томове във файловата система на Linux чрез използване на софтуер за NCP файлова система (NCPFS). При наличието му

Linux работната станция емулира NetWare клиент и може да осъществява достъп до файлове на NetWare файлов сървър или да печата в NetWare опашка за печат. NCPFS файловете са налични за сваляне от ftp.gwdg.de или sunsite.unc.edu. По-ранните версии работеха само с NetWare 3.*x* или NetWare 4.*x* в режим на емулиране на bindery; по-късните версии поддържат NDS.

Можете да позволите на Linux машини да осъществят достъп до ресурси на NetWare, като инсталирате NFS сървърен софтуер на Novell върху NetWare сървъра.

Свързване на Linux клиент към Linux/UNIX сървър

Повечето популярни дистрибуции на Linux притежават необходимите инструменти за конфигуриране на мрежови устройства. Тези инструменти могат да се свалят и от ftp.uk.linux.org. Мрежови приложения като Telnet и FTP за Linux могат да се свалят от същия сайт.

Командата **ifconfig** може да се използва за конфигуриране на мрежовия интерфейс, както е показано в Пример 12-4. Тази команда конфигурира един Ethernet адаптер, идентифициран като eth0, да използва IP адреса 192.168.1.16 с подмрежова маска 255.255.255.0 (подразбиращата се Клас С маска). Думичката „up" в края активира интерфейса.

Пример 12-4 *Можете да използвате командата ifconfig, за да конфигурирате мрежовия интерфейс*

```
# ifconfig eth0 192.168.1.16 netmask 255.255.255.0 up
```

NFS е протоколът за споделяне на файлове, който по принцип се използва в сървърна UNIX среда. NFS може да се компилира в ядрото на Linux. Той се включва в популярни Linux дистрибуции, като например RedHat. За да използвате Linux машина като NFS клиент, трябва да монтирате NFS файловата система, като използвате командата **mount**. Това ви позволява да осъществявате достъп до отдалечените файлове така, все едно че са локални; достъпът обаче е по-бавен.

Свързване на Linux/UNIX клиент към Интернет

За да свържете Linux или UNIX машината към Интернет през dialup ISP акаунт, мрежовите модули трябва да са инсталирани, а един от серийните портове трябва да е установен да се използва от модем.

Можете да използвате програма, наречена minicom, за да се свържете директно към shell акаунт, ако вашият доставчик на Интернет осигурява такъв. Shell акаунтът представлява команден интерфейс към UNIX сървър, до който може да се осъществява достъп през Telnet. Linux компютърът трябва да е конфигуриран със следната информация:

- DNS адреса на Интернет доставчика, който се задава във файла /etc/revolv.conf
- Фиксирания IP адрес (ако такъв е назначен от доставчика), който се задава в etc/hosts
- Външния пощенски домейн, който се установява в /etc/mailname
- Името и паролата на потребителския акаунт, назначени от Интернет доставчика, които се установяват в etc/ppp/pap-secrets (ако се използва про-

токолът PAP [Password Authentication Protocol]) или в /etc/ppp/chap-secrets (ако се използва протоколът CHAP [Challenge Handshake Authentication Protocol])

В /etc/ppp/chatscript се установява скрипт за свързване, който указва процедурата по свързването; в него се включва низът за инициализиране на модема, телефонният номер на dialup сървъра на доставчика и друга информация в зависимост от процедурите за логване в сървъра.

За установяване на връзка по телефонна линия обикновено се използва протоколът PPP (Point-to-Point Protocol). В някои случаи вместо него може да се използва SLIP (Serial Line Internet Protocol) или UUCP (UNIX-to-UNIX Copy Protocol).

След като бъде установена връзката, можете да браузвате Мрежата чрез текстово-базирания браузър Lynx. Ако е инсталиран X Window или друг графичен shell, браузването може да се извършва през Netscape или друг графичен браузър (например Opera). Sendmail е програма, използвана за изпращане на e-mail, а за извличането на e-mail може да се използва POP (Post Office Protocol) версия 3.

Други UNIX/Linux e-mail програми включват Pine, Elm, Fetchmail и Smail. Procmail сортира входящата поща и управлява автоматичните отговори, както и други подобни задачи.

Macintosh

Apple Macintosh компютрите бяха проектирани за лесна работа в мрежа в равноправна среда (работна група). Всъщност мрежовите интерфейси често се включват като чат от хардуера и от мрежовите компоненти, вградени в операционната система на Macintosh. Macintosh може да използва също Ethernet и Token Ring мрежови адаптери.

Macintosh компютрите, или за кратко Mac-овете, са популярни в множество образователни институции и корпоративни графични отдели. Mac-овете могат да се свързват един с друг в работни групи и да осъществяват достъп до Appleshare файлови сървъри. Те могат да се свързват и към LAN мрежи, изградени от PC-та, които включват Microsoft, NetWare или UNIX сървъри.

В следващите секции, ще научите как да свързвате Macintosh компютри заедно в работна група; към Windows, NetWare или Linux/UNIX сървър; или към Интернет през dialup сървър за отдалечен достъп.

Свързване на Macintosh компютри в работна група

Macintosh машините могат да бъдат обединявани бързо и лесно в работни групи чрез използване на мрежовите компоненти и протоколи AppleTalk. По-ранните реализации използваха LocalTalk – по-бавна серийна мрежова връзка. LocalTalk все още се поддържа, но по-новите AppleTalk версии са по-бързи и позволяват съвместна работа с други операционни системи. LocalTalk използва кутия за свързване, която се свързва към серийния порт и телефонен кабел.

AppleTalk използва концепцията за *зони*, което в този контекст означава логически групирани ресурси. зоните функционират като работни групи в PC мрежите. Когато се свържете с AppleTalk мрежа, можете да достигнете до списъка със зоните, като отворите прозореца Chooser от Apple менюто. AppleTalk трябва да е установен на „active“ (активен) в Chooser, за да видите списъка на зоните. Може да се наложи да изберете типа на мрежата (като LocalTalk или

EtherTalk) в Network Control Panel, който се намира в папката Control Panel вътре в папката System.

Свързване на Macintosh компютри към Microsoft, NetWare и UNIX мрежи

Преди няколко години беше трудно или невъзможно да интегрирате Apple компютри в PC мрежи. Днес съществуват всякакви софтуерни пакети, които позволяват на Macintosh потребителите да участват в Microsoft, NetWare и UNIX мрежи.

Microsoft осигурява Services for Macintosh със своите NT и Windows 2000 сървърни продукти. Пакетът включва следните компоненти:

- Файлов сървър за Macintosh
- Принт сървър за Macintosh
- AppleTalk протокол

Когато тези услуги са инсталирани на Windows сървъра, Macintosh клиентите могат да използват файлове и принтери в Microsoft мрежата. Windows сървърът може да работи и като AppleTalk маршрутизатор, без да е необходимо инсталиране на допълнителен софтуер на Macintosh компютрите.

За NetWare сървъри е наличен add-on модул, който прави NetWare сървърите да се показват на Macintosh клиентите като Appleshare сървъри. Add-on модулът се нарича NetWare for Macintosh NLM (NetWare Loadable Module). Macintosh компютърът изпраща AppleTalk пакети с данни, които се приемат и обработват от модула. Mac-овете могат да комуникират и по IPX в NetWare 4.0 мрежите.

Софтуер като Syntax позволява на Macintosh клиенти (както и на DOS, Windows и OS/2 клиенти) да осъществяват достъп до файлове, принтери и приложения на UNIX сървър.

За свързването на съществуваща AppleTalk мрежа към корпоративна LAN мрежа могат да се използват шлюзове или маршрутизатори. Устройства, разработени специално за тази цел, са налични от компании като Shiva.

Свързване на Macintosh компютри към Интернет

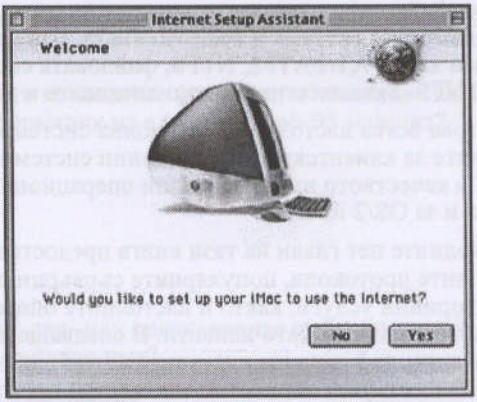
Свързването на Macintosh компютър към Интернет, както при всички останали операционни системи, изисква на Mac компютъра да е инсталиран протоколът TCP/IP. Apple предлага реализация, наречена AppleIP, като същевременно са налични и комерсиални продукти като MacTCP. Инсталирането на тези протоколи позволява на Mac-а да комуникира по TCP/IP-базирана LAN или WAN.

Както при останалите операционни системи, TCP/IP трябва да е конфигуриран с IP адрес, подмрежова маска и подразбиращ се шлюз (ако е необходимо). Необходим е и адрес на DNS сървър, който да преобразува хост имената в IP адреси. Изгледът на конфигурационните диалогови прозорци се различава в зависимост от използваната софтуерна реализация.

Ако Macintosh компютърът използва модем и dialup акаунт за Интернет връзката, PPP протоколът трябва да е конфигуриран. Macintosh PPP софтуер може да бъде свален от Web; ConfigPPP е една такава програма. В тези програми заедно с телефонния номер на отдалечения сървър се задават и модемен порт, скорост на порта, timeout времена и опции на връзката.

iMac машините осигуряват Internet Setup Assistant, както е показано на Фигура 12-21, който ви превежда през конфигурационния процес по същия начин, както го правят помощниците в Windows.

Фигура 12-21 *Macintosh iMac машините осигуряват подобен на помощник конфигурационен интерфейс за установяване на Интернет връзка.*



OS/2

Въпреки че IBM се отказаха от поддръжката и разработката на своята настолна операционна система OS/2 в средата на 1990-те години, все още съществуват множество верни потребители. OS/2 все още може да се срещне в някои бизнес LAN мрежи, особено в банките.

OS/2 започна като съвместен проект между IBM и Microsoft. Когато двете компании разделиха пътищата си, Microsoft разработиха Windows NT (базиран отчасти на OS/2 технологията), а IBM пуснаха на пазара OS/2, като по-късно смениха името на OS/2 Warp.

ЗАБЕЛЕЖКА IBM все още продават и поддържат OS/2 Warp Server. Текущата версия на продукта Warp Server е проектирана като сървър за електронна търговия и се купува от големи организации, правещи бизнес по Интернет.

OS/2 може да се свързва с NetWare сървъри чрез използване на Novell NetWare Client Kit for OS/ 2. IBM TCP/IP софтуер може да се използва за комуникиране по TCP/IP-базирана мрежа, като същевременно бяха разработени допълнителни комплекти, които да добавят поддръжка за NFS, NetBIOS и IPX/SPX.

OS/2 Warp, версия 4, включваше поддръжка за dialup networking и връзка с Интернет.

Обобщение

В тази глава дискутирахме най-широко използваните настолни операционни системи и как те могат да участват като клиенти в различни типове мрежи.

Започнахме с разглеждане на основите на операционните системи, включително на двата типа потребителски интерфейси: текстово-базираният и графичният (GUI). Дискутирахме синтаксиса на командите и научихте как към командите могат да се добавят ключове или аргументи, за да дефинират техните параметри.

Обсъдихме ролята на файловете и файловите системи, конвенциите за именуване на файлове, а също и как разширенията за файлови типове се използват от операционната система и приложенията. Бяха дискутирани популярни файлови системи като FAT/FAT32, NTFS, файловата система на UNIX, HPFS, Macintosh HFS и NFS. Бяха засегнати също дисковете и дисковите дялове.

След това всяка настолна операционна система беше разгледана индивидуално. Научихте за клиентските операционни системи MS-DOS и Windows, за Linux/UNIX в качеството им на настолни операционни системи, за Apple Macintosh, а накрая и за OS/2 на IBM.

Предходните пет глави на тази книга предоставиха основни знания относно мрежовите протоколи, популярните сървърни продукти, използваните от тях директорийни услуги, както и настолните операционни системи, които могат да се свързват към тях като клиенти. В следващата глава обединяваме всички тези теми в едно, тъй като ще дискутираме хибридните мрежи – мрежи, в които могат да съществуват съвместно множество протоколи, платформи и операционни системи.

Допълнителни източници

Обзор на файловите системи FAT, VFAT, FAT32 и NTFS ще откриете на Web сайта на Microsoft на адрес www.microsoft.com/technet/winnt/filesyst.asp.

Дискусия на възможностите на NTFS можете да намерите на Web сайта www.via.ecp.fr/~regis/ntfs/new.

Добро ръководство за файловата система на UNIX се намира на www.anet-stl.com/tech/unix/Pages/concepts_fsystem.html.

Софтуерът за работа с дискови дялове Partition Magic може да се поръча от www.powerquest.com.

Най-добрата отправна точка за информация относно операционните системи и мрежовите компоненти на Microsoft е Web сайтът TechNet на адрес www.microsoft.com/technet/default.asp.

Връзки и ръководства за Linux и работа в мрежа с Linux могат да се открият на www.linuxhq.com.

Добър източник за междуплатформени решения, занимаващи се със свързването на Macintosh компютри към PC мрежи е www.macwindows.com/Network.html.

За повече информация относно OS/2 Warp вижте индекса на Интернет сайта за OS/2 на адрес www.nfwa.com/os2/news/e-zines.html.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Кои от следните са преимущества на текстово-базираните операционни системи? (Изберете всички верни отговори.)

- **a** По принцип те са по-бързи от графичните интерфейси.
- **b** Те използват по-малко ресурси от графичните интерфейси.
- **c** Те са по-лесни за използване от графичните интерфейси.
- **d** По принцип те поддържат многозадачност, докато графичните операционни системи не го правят.

2 Коя от следните команди се използва за показване на TCP/IP конфигурационната информация на една Windows 95 машина?

- **a** ifconfig
- **b** ipconfig
- **c** winipcfg
- **d** config

3 Как се наричат дву- или тризнаковите суфикси, предхождани от точка, в края на едно файлово име?

- **a** Файлови разклонения
- **b** Файлови таблици
- **c** Файлови типове
- **d** Файлови разширения

4 Кое от следните е преимущество при използване на FAT16 файлова система в една операционна система на Microsoft?

- **a** Тя е съвместима с повече операционни системи, отколкото която и да било друга файлова система.
- **b** Предоставя по-добра сигурност от останалите популярни файлови системи.
- **c** По-надеждна е (по-малко податлива на загуба на данни) спрямо която и да е друга популярна файлова система.
- **d** Предлага по-висока производителност от която и да е друга файлова система.

5 Какъв е максималният размер на един дисков дял, поддържан от NTFS?

- **a** 2 GB
- **b** 4 GB
- **c** 4 TB
- **d** 16 EB

6 Кое от следните представлява път на директория във файловата система на UNIX?

- **a** c:/dir01/subdir02/myfile.ext
- **b** \dir01\subdir02\myfile.ext
- **c** /dir01/subdir02/myfile.ext

d /dir01/subdir02\myfile.ext

7 Коя от следните файлови системи използва асоцииране на i-възли?

a FAT32

b Файловата система на UNIX

c Macintosh HFS

d NTFS

8 Кое от следните трябва да инсталирате, за да позволите на един потребител на Windows NT Workstation да се логва директно в NetWare сървър?

a File and Print Services for NetWare

b Gateway Services for NetWare

c Client Services for NetWare

d IPX/SPX

9 Кое от следните може да се използва, за да се позволи на една Linux работна станция да осъществява достъп до файлове на Microsoft сървър?

a SMBFS

b NCP

c TCP/IP

d PPP

10 Коя от следните операционни системи използва файловата система HPFS?

a MS-DS

b Windows 2000

c OS/2

d Windows NT 4.0

Глава 13

Хибридни мрежи

В Част II на тази книга, „Мрежов хардуер и софтуер“, дискутирахме различните мрежови протоколи, които могат да се използват от компютрите за комуникация един с друг. Научихте за популярните мрежови операционни системи (network operating systems — NOSs), които работят на мрежови сървъри, и за настолните операционни системи, използвани от мрежовите клиенти. Също така научихте за директорийните услуги, използвани за организиране и откриване на ресурси в съвременните мрежи и интермрежи, свързващи множество LAN и WAN.

Хибридната мрежа е такава, в която могат съвместно да съществуват множество операционни системи, хардуерни платформи, протоколи и услуги. Интернет е най-голямата хибридна мрежа изобщо, а в днешния корпоративен свят не е изключено дори малка локална мрежа да работят като хибридна.

Тази глава ви дава някои насоки за работа с мрежи, състоящи се от различни софтуерни или хардуерни продукти. По-специално разглеждаме три типа хибридни мрежи:

- Мрежи, работещи с множество протоколи
- Мрежи, работещи с множество операционни системи (мрежови и настолни)
- Мрежи, работещи с множество хардуерни платформи

Разбира се, вашата хибридна мрежа може да влиза в две или повече от тези категории.

Преди да изследваме всяка от категориите в подробности, дискутираме общите характеристики на хибридните мрежи и причините за реализирането на една такава мрежа.

Характеристики на хибридната мрежа

Въпреки че съществуват преимущества при реализирането на „чиста“ мрежа — т.е. мрежа, базирана на една платформа, операционна система и протоколен стек — съществуват множество причини една мрежа да комбинира продуктите на различни потребители:

- Невъзможността един производител да осигури всички желани възможности

- Персонални предпочитания на потребителите
- Бюджетни фактори
- Случайно разрастване

В следващите секции разглеждаме всяка от причините за изграждане на хибридна мрежа.

Невъзможността един производител да осигури всички желани възможности

Една от най-честите причини за комбиниране на различни платформи или операционни системи в една мрежа е невъзможността за получаване на всички желани възможности от продуктите на един-единствен производител.

Например може да имате мрежа, която работи главно на UNIX сървъри, но се нуждаете от конкретно приложение или възможност, които се срещат само в Microsoft Windows NT или Windows 2000 Server. Ако имате клиентски машини, работещи под Windows 9*x*, и те трябва да комуникират една с друга, като използват NetBIOS имена, бихте могли да настроите един Windows NT или Windows 2000 Server като WINS сървър, за да осигурите NetBIOS имена за преобразуването на IP адресите.

В друг сценарий може да имате Windows NT мрежа с Windows 9*x* клиенти. Вашият графичен отдел обаче, може да се нуждае от приложение, работещо само на Macintosh платформа. В този случай бихте могли да използвате Macintosh системи само в този отдел и да реализирате Services for Macintosh на NT сървъра, така че Macintosh клиентите да могат да осъществяват достъп до файловете в мрежата.

Персонални предпочитания на потребителите

В някои компании на отделните работници им се позволява да избират компютърните системи, на които да работят. Това е особено вярно за потребители от ръководното тяло на компанията. Ако имате Windows 2000 мрежа с клиентски машини, работещи под Windows 2000 Professional, но вицепрезидентът на компанията предпочита Linux, ще трябва да интегрирате Linux машината във вашата Microsoft мрежа.

Бюджетни фактори

Понякога бюджетът не позволява да реализирате чиста мрежа. Например, ако компанията иска да премине от Novell NetWare към Windows 2000 мрежа, може да не разполагате с достатъчно пари за лицензиране на всички сървъри едновременно. При това положение като компромисна мярка ще трябва да организирате мрежата като хибридна, т.е. в нея да работят едновременно Windows и NetWare сървъри.

Подобна ситуация съществува, ако вашата организация реши да използва Windows 2000 Professional като клиентска операционна система, но не е в състояние да замени или ъпгрейдне хардуера на всички работни станции. За онези машини, които не могат да покрият системните изисквания на Windows 2000, ще трябва да продължите да използвате по-стара версия на Windows, или пък настолна операционна система като Linux, която изисква по-малко хардуерни ресурси.

Случайно разрастване

В много случаи не съществува действителен план за реализиране на хибридна мрежа. Просто системите са купувани с течение на времето, а операционните им системи са избирани според предпочитанията на този, който е купувал техниката, или според решението, което е било най-добро по това време.

Вероятно са използвани NetWare сървъри, защото мрежовият администратор е притежавал Novell сертификат. На по-късен етап са добавени NT сървъри, защото продуктите на Microsoft са станали популярни. Накрая, компанията е решила да хоства Web сайт и е наела уебмастър, който е обичал Apache софтуера, работещ на UNIX машини, така че в крайна сметка е поставен Web сървър, работещ под Linux. За да усложни нещата още повече, ръководството на вашата компания е решило, че PC мрежата трябва да комуникира с мрежа от мейнфрейм машини на IBM, използвани в счетоводния отдел. Сега вие, мрежовият администратор, трябва да накарате всички тези системи да работят заедно в една истинска хибридна мрежа.

Мрежи с множество протоколи

В мрежите се използват множество типове компютърни протоколи, които работят в различни слоеве на мрежовия модел.

В крайна сметка, *всички* мрежи използват множество протоколи. Когато обаче говорим за множество протоколи в контекста на хибридните мрежи, разглеждаме основно две ситуации:

- Мрежи, използващи повече от един мрежов/транспортен протокол
- Мрежи, използващи повече от един протокол за споделяне на файлове (понякога наричан същински протокол [*core protocol*])

Мрежови/транспортни протоколи

За да комуникират помежду си в една мрежа, компютрите трябва да споделят общ мрежов/транспортен протоколен стек като TCP/IP, IPX/SPX или NetBEUI. В много ситуации мрежата изисква повече от един мрежов/транспортен протоколен стек. Причините за използването на множество протоколи в една мрежа включват следното:

- Множество мрежови операционни системи
- Връзка с Интернет
- Сигурност

Нека видим защо в такива ситуации са необходими множество протоколи.

Множество мрежови операционни системи

Най-често срещаният сценарий, при който множество мрежови операционни системи създават необходимостта от множество протоколи, е хибридната мрежа Microsoft/NetWare.

Въпреки че NetWare 5.*x* е способна да работи с чист IP, все още в много корпоративни мрежи съществуват NetWare 3.*x* и 4.*x* сървъри. За да могат да комуникират с мрежата, тези сървъри изискват протоколния стек IPX/SPX.

Обикновено в една средна или голяма мрежа клиентите комуникират със сървърите на Microsoft посредством TCP/IP. Ако на същите тези клиенти им се наложи да осъществяват достъп до файлове на NetWare 3.*x* или 4.*x* сървър, на тях не само трябва да е инсталиран NetWare клиентски софтуер на Novell или Microsoft, но също така трябва да се изпълнява протоколен стек IPX/SPX, като например NWLink.

Връзка с Интернет

Ако имате малка Microsoft мрежа, която се състои само от една подмрежа (немаршрутизирана), за LAN комуникациите може да изберете да използвате протокола NetBEUI, защото той е по-бърз, по-лесен за конфигуриране и по-лесен за отстраняване на проблеми, отколкото са NWLink и TCP/IP.

Ако обаче искате да свържете някои или всичките си компютри в LAN мрежата към Интернет, те трябва да изпълняват протоколния стек, използван за комуникация в глобалната мрежа – TCP/IP. Компютрите могат да използват NetBEUI за комуникиране помежду си (с цел по-висока производителност), докато използват TCP/IP за връзка с Интернет.

ЗАБЕЛЕЖКА Когато свързвате малка мрежа към Интернет, използвайки транслиране на мрежови адреси (Network Address Translation – NAT), всеки компютър, осъществяващ достъп до Интернет, пак изисква TCP/IP, въпреки че само NAT хостът в действителност е свързан директно към Интернет. Това е така, защото NAT изисква на вътрешните компютри да са назначени IP адреси – по принцип от частния диапазон – с цел идентифициране.

Сценарият може да включва и клиенти, които се нуждаят от достъп до NetWare сървъри, комуникират с други Microsoft системи и се свързват към Интернет през NAT хост. В такъв случай ще трябва на една машина да инсталирате всички три протоколни стека – IPX/SPX, NetBEUI и TCP/IP – които да са обвързани с мрежовия адаптер.

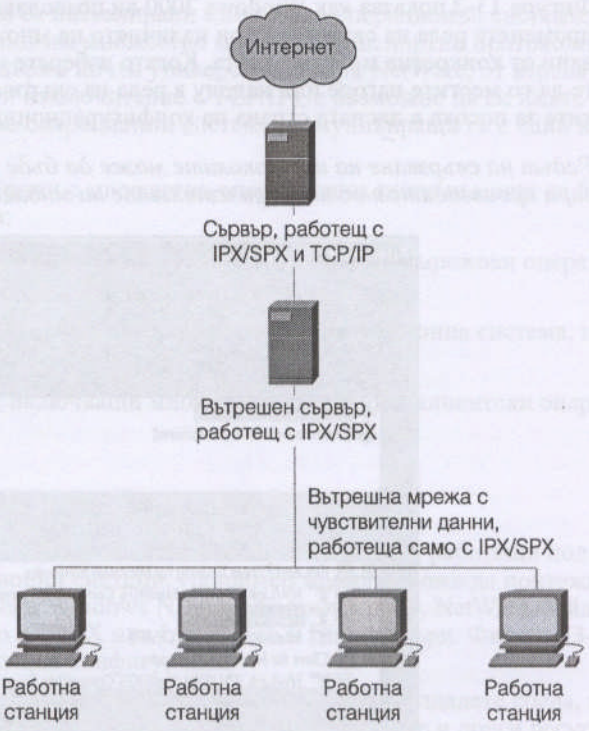
Използване на множество протоколи от гледна точка на сигурността

Някои мрежови администратори реализират различен мрежов/транспортен протоколен стек от TCP/IP във вътрешната мрежа (или поне в част от нея), за да изградят допълнително ниво на сигурност, когато мрежата се свързва към Интернет.

Например, ако имате група компютри в мрежата, съдържащи чувствителни данни, може да изберете те да комуникират през IPX/SPX, вместо през TCP/IP, защото компютрите с чувствителните данни не би трябвало да изискват достъп до Интернет. Другите компютри във вътрешната мрежа могат да комуникират с тях, като използват IPX/SPX, а с връзка с външния свят се прави чрез TCP/IP. При това положение компютър извън LAN мрежата, който не използва IPX/SPX (това е профилът на типичния, конфигуриран за Интернет компютър), няма да може да се свърже към машините, използващи само IPX/SPX, защото няма да има общ протокол. Фигура 13-1 илюстрира тази ситуация.

ЗАБЕЛЕЖКА Въпреки че по принцип IPX/SPX се асоциира с NetWare мрежи, той може да се използва и за LAN комуникации в среда, използваща само операционни системи на Microsoft. Това може да е ценна опция, адаптерна карта не се нуждаете от връзка с Интернет, но ви трябва маршрутизируем протоколен стек, който е полезен за конфигуриране и е по-бърз от TCP/IP.

Фигура 13-1 *Могат да се използват множество протоколи за защита на част от мрежата от външно натрапване.*



Значението на реда на свързване на протоколите

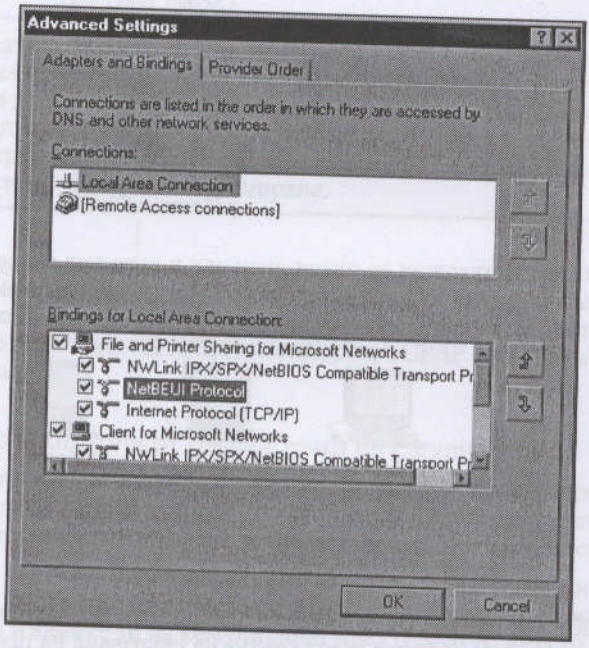
Когато множество мрежови/транспортни протоколни стекове са свързани с една и съща мрежова карта, редът на свързване на протоколите е от значение. *Редът на свързване (binding order)* на протоколите на клиентската машина определя кой протокол се използва за комуникиране със сървъра, когато двете машини използват повече от един общ протокол.

ЗАБЕЛЕЖКА Като спецификациите NDIS (Network Driver Interface Specification) на Microsoft, така и спецификациите ODI (Open Datalink Interface) на Novell за интерфейси за мрежови устройства позволяват към един мрежов адаптер да бъдат свързани няколко протокола, а също и няколко мрежови адаптера да бъдат свързани с един протокол.

Например, ако на една клиентска машина протоколите TCP/IP, NetBEUI и IPX/SPX са свързани към мрежовата ѝ карта в изброения ред, а на сървъра са инсталирани протоколите NetBEUI, IPX/SPX и TCP/IP, които са свързани към неговата мрежова карта в изброения ред, тогава клиентската машина се опитва да осъществи връзка най-напред чрез използване на TCP/IP (който е пръв в реда на свързване). Ако тя открие TCP/IP на сървъра, тогава за сесията се използва този протокол, въпреки че той е последен в реда на свързване на сървъра. Както можете да видите, за та оптимизирате производителността на мрежата, трябва да се уверите, че най-използваните протоколи се намират най-отгоре в реда на свързване на клиентските машини.

Фигура 13-2 показва как Windows 2000 ви позволява да конфигурирате или да промените реда на свързване при наличието на множество протоколи, използвани от конкретна мрежова карта. Когато изберете инсталиран протокол, можете да го местите нагоре или надолу в реда на свързване, като използвате стрелките за посока в дясната страна на конфигурационния диалогов прозорец.

Фигура 13-2 *Редът на свързване на протоколите може да бъде променян, за да се оптимизира производителността при използване на множество протоколи.*



Другите операционни системи притежават подобни механизми за конфигуриране на реда на свързване.

Протоколи за споделяне на файлове

Вторият тип протокол, който е важен за комуникациите в хибридните мрежи, е *протоколът за споделяне на файлове (file-sharing protocol)*, който понякога се нарича и същински протокол (core protocol). За споделяне на файлове мрежите на Microsoft използват Server Message Block (SMB); NetWare мрежите използват NetWare Core Protocol (NCP), а UNIX системите – Network File System (NFS).

Осъществяването на достъп до файлове на сървъра изисква даденият компютър да използва подходящ клиентски софтуер. Например, когато инсталирате Client Services for NetWare (или Novell клиента) на една Microsoft Windows машина, това осигурява и инсталирането на NCP клиентския софтуер. Samba включва SMB клиент за UNIX машини, така че тези машини да могат да осъществяват достъп до ресурсите на Microsoft сървъри, като използват SMB протокола за споделяне на файлове.

Мрежи с множество операционни системи

Мрежа, в която са инсталирани множество операционни системи, не е задължително да използва множество мрежови/транспортни протоколи. Тъй като TCP/IP се поддържа почти универсално (дори NetWare, от версия 5.0 нагоре, може да работи изключително с TCP/IP), е възможно да си имате работа с мрежа с множество операционни системи, комуникиращи се с един и същ протоколен стек.

Хибридните мрежи с множество операционни системи могат да бъдат разделени на три типа:

- Мрежи, в които са инсталирани множество мрежови операционни системи
- Мрежи, използващи една сървърна операционна система, но множество клиентски операционни системи
- Мрежи, включващи множество сървърни и клиентски операционни системи

Множество сървърни операционни системи

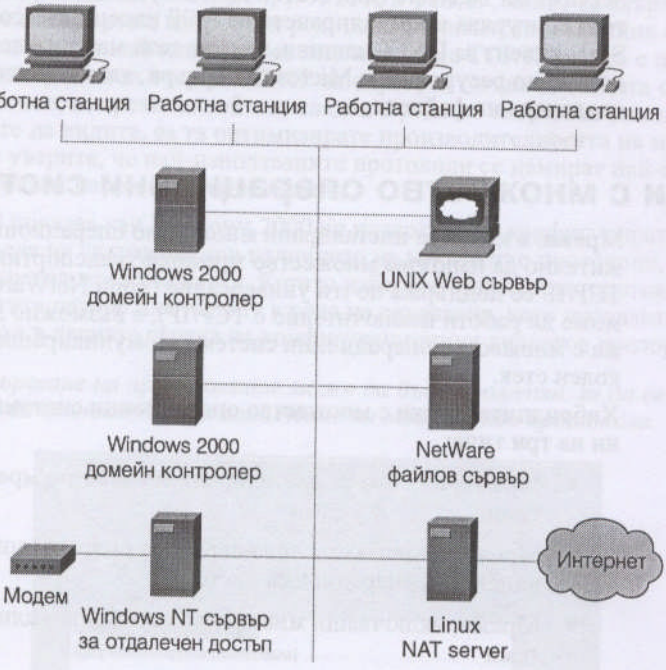
В една мрежа е възможно да съществуват сървъри, работещи под няколко различни операционни системи. Например мрежата може да притежава както Windows 2000, така и Windows NT домейн контролери, NetWare файлови и принт сървъри, както и UNIX или Linux Web и FTP сървъри. Фигура 13-3 показва една такава хибридна конфигурация.

Вашата работа като мрежов администратор е да създадете среда, в която потребителите могат да осъществяват достъп до файлове и други ресурси независимо от операционната система.

За щастие, съществуват софтуерни пакети, които ви позволяват да осигурите на клиентите достъп до различни сървъри. Някои от тези софтуерни пакети са включени в самата клиентска операционна система, докато други са продукти на независими компании. Следват някои от най-често използваните продукти за интеграция:

- **Client Services for NetWare (CSNW)** – Включва се в Windows NT Workstation и Windows 2000 Professional; позволява на Windows NT или Windows 2000 клиенти да осъществяват достъп до NetWare сървъри.
- **Microsoft Client for NetWare Networks** – Включва се в операционните системи Windows 9*x* и изпълнява същата функция като CSNW в Windows 95 и Windows 98 машините.

Фигура 13-3 *В една хибридна мрежа сървърите могат да работят под различни мрежови операционни системи.*



- **Gateway Service for NetWare (GSNW)** – Включва се в операционните системи Windows NT Server и Windows 2000 Server. Позволява на клиентите, логнали се в Windows сървър, да използват ресурси на NetWare сървър чрез преминаване през шлюза на един Windows NT или Windows 2000 сървър.
- **Novell Client for Windows 9*x*/NT/2000** – Може да се свали безплатно от Novell и позволява на Windows компютри да осъществяват достъп до файлове на NetWare сървър.
- **Samba** – Този продукт е независима безплатна разработка и позволява на SMB клиенти, като например Windows операционни системи, да осъществяват достъп до файлове на UNIX сървър, изпълняващ софтуера Samba.
- **SMB File System (SMBFS)** – Разпространява се със Samba и позволява на Linux компютри да мапват мрежово устройство към SMB споделен ресурс.
- **Microsoft Services for Macintosh** – Включва се в Windows NT/2000 Server; позволява на Macintosh клиенти да осъществяват достъп до ресурси в мрежи на Microsoft.
- **Linux Services for Macintosh** – Реализацията е независим продукт като Columbia AppleTalk Package (CAP) и Netatalk; позволява на Macintosh компютри да осъществяват достъп до ресурси на Linux компютри чрез добавяне на протокола DDP (AppleTalk Datagram Delivery Protocol) към ядрото на Linux.

Множество клиентски операционни системи

Конфигурирането на мрежови клиенти, които работят под различни операционни системи, не е толкова сложно, колкото да се работи с различни сървърни операционни системи. Как се конфигурират популярните настолни (клиентски) машини за връзка с различни мрежови операционни системи е дискутирано подробно в Глава 12, „Настолни операционни системи".

Множество сървърни и множество клиентски операционни системи

В много случаи ще се сблъсквате с хибридна мрежа, включваща множество сървърни операционни системи *и* множество клиентски операционни системи. Това повишава сложността на вашата администраторска работа, защото трябва да знаете как да поддържате различните операционни системи. В такъв тип сложна среда е особено важно да получавате най-актуалната информация относно сервизни пакети, горещи поправки и кръпки на сигурността за *всички* операционни системи, свързани в мрежата. В противен случай е възможно по невнимание да изложите сигурността на цялата мрежа на опасност от пробив.

Многоплатформени мрежи

Терминът *платформа* понякога се използва за означаване на операционни системи (например Windows платформа или UNIX платформа). В тази книга ние използваме термина за означаване на различни компютърни архитектури или хардуерни платформи. Въпреки това е важно да отбележим, че различните платформи обикновено (макар че не винаги) работят под различни операционни системи.

Например *PC платформата* използва хардуерна архитектура, различна от тази на *Macintosh платформата* или от тази на *IBM мейнфрейм платформата*. Една нова и набираща популярност компютърна платформа се използва от персоналните цифрови помощници (personal digital assistants – PDA) и хендхелд устройствата; тази платформа използва различна хардуерна конфигурация.

В следващите секции дискутираме как се постига комуникирането между следните платформи:

- PC и Macintosh
- PC и мейнфрейм
- PC и PDA (или хендхелд компютър)

PC-към-Macintosh комуникации

Комуникацията между IBM-съвместими PC-та (наречени така, защото IBM построиха първия масово достъпен персонален компютър на тази хардуерна платформа) и Macintosh компютри е относително проста форма на междуплатформена мрежа, защото двете платформи са подобни като мащаб и използване. Ето защо това обикновено се разглежда като свързване на различни операционни системи. Това обаче вече беше разгледано в секцията „Мрежи с множество операционни системи" по-рано в тази глава.

PC-към-мейнфрейм комуникации

Мейнфрейм и „мини мейнфрейм системите“, като например популярният IBM AS/400, се различават съществено по концепция и реализация от персоналния модел, за който са създадени PC-тата и Macintosh-ите. В много бизнес ситуации обаче мейнфрейм компютрите се използват за обработка на огромни количества данни, като често работят в мрежа с PC-та.

Например в една община мейнфрейм компютърът може да се използва за обработка на данъците и таксите. Работниците в данъчния отдел на общината вероятно взаимодействат с мейнфрейма чрез терминали за въвеждане на данни. Останалият общински персонал може да използва PC-та за текстообработка, e-mail съобщения, електронни таблици, приложения за бази данни и т.н. Само че на някой от тези работници може да му се наложи да осъществи достъп до данни, разположени на мейнфрейма. Един от начините да им осигурите достъп е да поставите мейнфрейм терминал на всяко работно място (в добавка към PC-то). Това решение обаче има няколко недостатъка:

- Харчат се пари за допълнителен излишен хардуер. (PC-то вече разполага с монитор и клавиатура – защо да се харчат пари за още един монитор и клавиатура?)
- В един офис свободното място на бюрото не е особено голямо, така че тези компоненти по-скоро ще пречат на служителя да работи ефективно.
- Трудно е да се интегрира информацията от терминала с документите, създадени на PC-то.

По-добро решение е да позволите на самите PC-та да работят като терминали за мейнфрейма, като същевременно запазват своята функционалност като настолен компютър. Тъй като мейнфрейм компютрите и PC-тата използват различни протоколи за мрежова комуникация, ви трябва софтуер за *протоколен шлюз (protocol gateway)*, който да извършва транслациите.

Един масово използван софтуерен пакет за свързване на PC мрежи към IBM мейнфрейм машини е Systems Network Architecture (SNA), който ще дискутираме по-нататък в тази глава в секцията „Шлюзове: решението за хибридно свързване“.

PDA-към-PC и хендхелд-към-PC комуникации

В нашето все по-мобилно общество хендхелд устройствата стават по-масово срещани. PDA устройствата са прости хендхелд компютри, ограничени до адресни указатели и списъци с контакти, календар и разписание, както и извличане на електронна поща. По-мощните PDA устройства включват, или ви позволяват да добавяте, още възможности чрез допълнителни програми, които могат да бъдат заредени в програмен модул – обикновено под формата на карта с памет (memory card). При добавянето на още функционалност границата между PDA и истинските хендхелд компютри започва да се размива. Примери за последното са Palm устройствата и Windows-базираните Pocket PC (джобни PC-та).

Хендхелд устройствата е необходимо да комуникират с настолните компютри, за да може един потребител да въвежда нови данни само на едно устройство и след това да го синхронизира с другото. Например, ако носите в себе си хендхелд устройство и създадете нов бизнес контакт, трябва да сте в състояние да въведете адреса на бизнес партньора ви, неговия телефонен номер и друга информация в списъка с контактите на вашето хендхелд устройство, след което да

прехвърлите данните автоматично и в списъка с контактите, намиращ се във вашата настолна машина.

Повечето хендхелд устройства включват средства за свързване към настолната машина през сериен или USB порт. Синхронизиращият софтуер (като ActiveSynch на Microsoft, използван за комуникиране между настолни Windows компютри и мобилни Windows CE устройства) позволява на системите да откриват промените и да актуализират информацията. Можете да прехвърляте файлове между устройствата, а софтуер за хендхелд устройства може да се сваля от Интернет на настолния компютър и след това да се инсталира на хендхелд устройството по серийна или друга връзка.

Шлюзове: решението за хибридно свързване

Терминът *шлюз* (или *шлюзова услуга*) има няколко значения в света на компютърните мрежи в зависимост от контекста. По принцип шлюзът е мрежова точка, служеща като вход към друга мрежа. Въпреки че и маршрутизаторът се вписва в тази дефиниция с функцията си за изход от подмрежа, или като входна точка към друга подмрежа или мрежа, в тази глава използваме по-широкото понятие.

Шлюзовият софтуер (като Gateway Service for NetWare) позволява на два различни типа мрежи да разговарят една с друга. С други думи, този софтуер служи като мост между компютри, използващи различни протоколи, операционни системи или платформи.

В следващите секции дискутираме различни типове шлюзов софтуер, включващ следното:

- Windows-към-NetWare редиректори
- Крос-платформени решения за конективност тип Macintosh-към-PC операционната система
- SNA за комуникации тип PC-към-мейнфрейм

Windows-към-NetWare редиректори

File and Print Service for NetWare (FPNW) позволява на NetWare клиенти да осъществяват достъп до ресурси на Windows сървъри. Тези софтуерни пакети се наричат *редиректори*, защото те прихващат заявка за дадения ресурс, транслират я в подходящия протокол за споделяне на файлове и я препращат по мрежата към сървъра, в който се намира ресурсът. Тъй като този софтуер извършва транслиране между различни протоколи, той попада в категорията шлюзов софтуер.

NetWare редиректорите, включени в операционната система Windows, включват и NWLink, който е NDIS съвместима 32-битовата реализация на протоколния стек Novell IPX/SPX. NWLink позволява комуникации, използващи един или повече приложни програмни интерфейси (APIs): Winsock (Windows Sockets) и NetBIOS.

ЗАБЕЛЕЖКА Свързването към клиент/сървър приложение (като SQL база данни) не изисква клиентски софтуер за споделяне на файлове и принтери. Например един NetWare клиент може да осъществява достъп до клиент/сървър приложение на NT Server, без да е инсталирана услугата FPNW, а един Windows клиент може да осъществява достъп до клиент/сървър приложение на NetWare сървър, без да са инсталирани CSNW, GSNW или какъвто и да е друг клиентски софтуер на Novell. Изисква се обаче общ протокол, като например IPX/SPX за NetWare машини преди 5.x.

GSNW осигурява достъп до NetWare ресурси от Windows клиенти, без да инсталира какъвто и да е софтуер на клиентските машини. GSNW постига това, функционирайки като шлюз (протоколен транслатор) между SMB, използван от мрежите на Windows, и NCP, който се използва в NetWare мрежата.

Когато се инсталира клиентът или шлюзовата услуга, потребителят на Windows компютъра може да стартира поддържаните NetWare помощни програми от командния ред.

Междуплатформени решения

Междуплатформените (крос-платформените) шлюзове са тези, които ви позволяват да свързвате различни платформи – например Macintosh машини към Windows мрежи. Интеграцията на Macintosh и Windows компютри изисква общ протокол (обикновено AppleTalk) и услуги за споделяне на файлове и принтери. За комуникация не се изисква допълнителен клиентски софтуер на Macintosh системите, но такъв съществува и се използва за автентициране на Macintosh клиентите с цел подобряване на сигурността.

На Macintosh клиентите може да им се даде и отдалечен (dial-in) достъп до един Windows Server чрез използване на протокола AppleTalk over Point-to-Point Protocol (PPP).

SNA

IBM разработиха SNA през 1970-те години, за да свързва несъвместими системи със слоеста архитектура. Идеята им беше да позволят на различни IBM системи (като IBM PC-тата и мейнфрейм машините) да споделят данни едни с други.

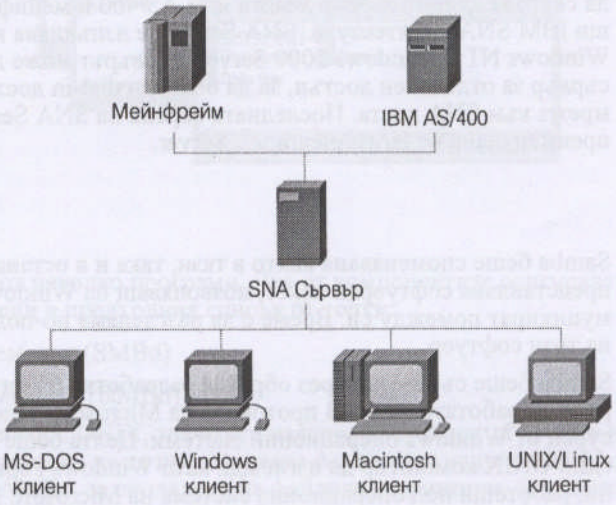
Компонентите на SNA включват следното:

- **Възел (node)** – Това е сбор от компютри в една SNA мрежа.
- **Мрежово адресируемо устройство (network addressable unit – NAU)** Това представлява отправната или крайната точка за предаваните данни. Едно NAU устройство може да бъде логическо устройство, физическо устройство или контролна точка за системни услуги (system services control point – SSCP).
- **Зареждащо устройство (logical unit – LU)** – Това е портът, използван от мрежовите потребители за достъп до SNA мрежата.
- **Физическо устройство (physical unit – PU)** – PU устройството управлява ресурсите на даден възел.

- **Контролна точка за системни услуги (system services control point – SSCP)** Това е точка в мрежата, използвана за управление на предоставяните на потребителите услуги.

Фигура 13-4 илюстрира как SNA служи като шлюз между PC мрежата и мейнфрейм машината.

Фигура 13-4 *Един Microsoft SNA сървър работи като шлюз между PC мрежата и мейнфрейм системата.*



Първоначално SNA мрежите се базираха на централен мейнфрейм компютър, който управляваше специализирани миникомпютри, изпълняващи софтуера за управление NCP. Миникомпютрите от своя страна управляваха група от терминали, работни станции и телефонни линии.

SNA комуникации

Текущата реализация на SNA се нарича Advanced Peer-to-Peer Networking (APPN). APPN поддържа два типа възли:

- **Мрежови възли (network** nodes) – Включват маршрутизатори и системи за управление на мрежата, както и клиентски и сървърни програми.
- **Крайни възли (end nodes)** – Съдържат само клиентски и сървърни програми.

SNA архитектурата изисква между клиента и сървъра да има установена сесия, преди да бъдат предадени каквито и да било данни. Това е обратното на IP, който не изисква установени сесии.

SNA е по-сложен протоколен набор от TCP/IP. SNA е част от AS/400 системите, но е реализиран и като Communications Manager for OS/2 (от IBM) и SNA Server for Windows NT (от Microsoft).

ЗАБЕЛЕЖКА В момента на писане на книгата, Linux-SNA беше в стадий на разработка. Текуща информация, засягаща бета тестване и окончателно пускане се намира на www.linux-sna.org.

Microsoft SNA Server

Продуктът SNA Server на Microsoft беше проектиран да осигури шлюз, който да свързва клиент/сървър мрежи към AS/400 и мейнфрейм системи, използващи IBM SNA архитектура. SNA Server се изпълнява на машини, работещи под Windows NT и Windows 2000 Server; сървърът може да бъде конфигуриран като сървър за отдалечен достъп, за да осигури dial-in достъп или достъп чрез VPN мрежа към SNA хоста. Последната версия на SNA Server на Microsoft беше преименувана на Host Integration Server.

Samba

Samba беше споменавана както в тази, така и в останалите глави на книгата. Тя представлява софтуерен пакет, позволяващ на Windows и UNIX машини да комуникират помежду си. Време е да разгледаме по-подробно начина на работа на този софтуер.

Samba беше създадена чрез обратна разработка (reverse-engineering) и анализиране на работата на SMB протокола на Microsoft, използван за споделяне на ресурси от Windows операционни системи. Целта беше да се направи така, че един UNIX компютър да изглежда като Windows сървър за клиентските машини, работещи под операционна система на Microsoft. Последната версия на Samba постига тази цел и дори повече.

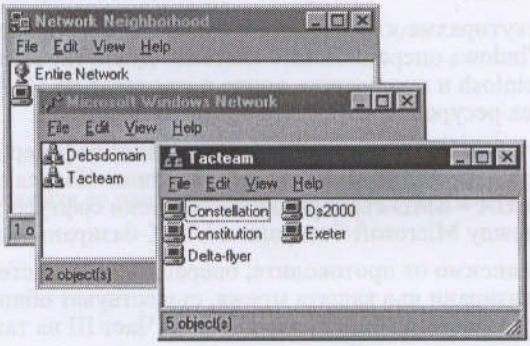
Samba позволява на Microsoft и UNIX операционните системи да си комуникират, използвайки файловата система CIFS (Common Internet File System), която се базира на SMB протокола за споделяне на файлове. CIFS осигурява четири услуги:

- Автентикация и авторизация
- Преобразуване на имена
- Услуги за споделяне на файлове и принтери
- Услуги за браузване на мрежата

Споделените ресурси могат да са защитени с парола, а преобразуването на NetBIOS имена може да се изпълнява чрез бродкастни съобщения, или чрез използване на сървър за NetBIOS имена, като например WINS, ако имате такъв в мрежата. Услугата за браузване предоставя списък на споделени мрежови ресурси в Network Neighborhood на Windows 9*x* и Windows NT машините, както е показано на Фигура 13-5.

В Windows 2000, иконата Network Neighborhood беше преименувана на My Network Places.

Фигура 13-5 *Network Neighborhood (или My Network Places в Windows 2000) показва списък на споделени мрежови ресурси.*



Как работи Samba

Samba е сбор от няколко програми. Два от компонентите осигуряват основните услуги, изброени в предходния списък от точки:

- SMB демонът (SMBd)
- NMB демонът (NMBd)

Ако сте запознати с UNIX, значи сте наясно, че буквата „d" в края на името на програмата означава, че тя представлява *демон*, или услуга. SMBd осигурява услугите на SAMBA за споделяне на файлове и принтери, за автентикация и за авторизация. NMBd осигурява преобразуването на имена и услугите за браузване.

ЗАБЕЛЕЖКА Linux компютрите могат да използват SMB File System (SMBFS), за да осъществяват достъп до отдалечени SMB дялове, например такива на Windows машини. SMBFS позволява на Linux потребителя да мапва споделения ресурс като мрежово устройство. SMBFS всъщност не е част от SAMBA, а само се разпространява се разпространява със SAMBA. Работи само с Linux операционни системи. Сам по себе си SAMBA софтуерът е пренесен да работи с NetWare, Virtual Memory System (VMS) и други операционни системи.

Обобщение

В тази глава дискутирахме различните типове хибридни мрежи, комбиниращи елементи от различни производители. Това включва мрежи, работещи с множество протоколи, мрежи, в които участващите компютри изпълняват множество операционни системи, и мрежи, работещи на множество хардуерни платформи.

Научихте за някои от предизвикателствата, стоящи пред мрежовия администратор, който трябва да интегрира различаващи се една от друга технологии и да създаде среда, в която PC-тата да могат да осъществяват достъп до данни на мейнфрейм компютри, или Apple Macintosh компютрите да могат да комуникират с UNIX сървъри.

Изследвахме някои от причините за реализиране на хибридни мрежови среди и решенията – като редиректори и шлюзов софтуер – които правят интеграцията по-лесна.

Дискутирахме клиентските и шлюзовите услуги за NetWare, които са включени в Windows операционните системи. Дискутирахме също Microsoft Services for Macintosh и продуктите, които позволяват на Macintosh клиенти да използват Linux ресурси.

Научихте за SNA и как SNA сървърният софтуер може да позволи на PC-та да комуникират с IBM мейнфрейм машини. Накрая дискутирахме как работи SAMBA – SMB сървърният и клиентски софтуер за UNIX – за да осигури връзка между Microsoft-базирани и UNIX-базирани мрежи.

Независимо от протоколите, операционните системи и хардуерните платформи, реализирани във вашата мрежа, съществуват общи административни въпроси, които трябва да бъдат разрешени. В Част III на тази книга, „Особености в областта на мрежите“, разглеждаме някои от специалните области, като започнем с нарастващите по популярност теми за мрежовата сигурност и защитата от бедствия.

Допълнителни източници

Полезно ръководство за интегриране на NetWare и Windows NT се намира на www.microsoft.com/TechNet/network/int-netw.asp.

За информация относно NFS клиентския софтуер на Intergraph за Windows, вижте www.intergraph.com/nfs/da-br.asp.

Добро резюме за начина на работа на SNA ще намерите на www.protocols.com/pbook/sna.htm.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Какво е другото име за протокола, използван за споделяне на файлове и ресурси в една мрежа?

- **a** Мрежов/транспортен протокол
- **b** Канален протокол (link protocol)
- **c** Същински протокол (core protocol)
- **d** Layer 2 протокол

2 Кое от следните е вярно за IPX/SPX?

- **a** IPX/SPX може да се използва само в NetWare мрежи.
- **b** IPX/SPX е маршрутизируем.
- **c** IPX/SPX не се поддържа от NetWare 5.x.
- **d** IPX/SPX е по-бавен и по-труден за конфигуриране от TCP/IP.

3 Кое от следните позволява множество протоколи да бъдат свързани с една мрежова карта, или един протокол да е свързан с множество мрежови карти? (Изберете всички верни отговори.)

a NDIS
b Winsock
c TDI
d ODI

4 Кое от следните се използва за споделяне на файлове в Microsoft мрежите?

a NCP
b SMB
c NFS
d DLC

5 Кое от следните е вярно за Gateway Service for NetWare (GSNW)? (Изберете всички верни отговори.)

a GSNW се инсталира на NetWare сървър, за да позволи на Windows клиенти да осъществяват достъп до неговите ресурси.
b GSNW се включва в операционните системи Microsoft Windows NT и Windows 2000 Server.
c GSNW позволява на клиенти на Windows сървър да се свързват с NetWare сървър, без да се инсталира каквото и да било, или да се конфигурира нещо на NetWare сървъра.
d GSNW се инсталира на Windows сървър, за да позволи на неговите клиенти да осъществяват достъп до ресурсите на един NetWare сървър.

6 Кое от следните е независим безплатен продукт, позволяващ на Windows и UNIX системи да обменят данни по мрежата?

a CDFS
b Samba
c Client Services for UNIX
d SNA

7 Какъв тип софтуер извършва транслиране между различни протоколи и позволява на компютри от различни типове мрежи да комуникират помежду си?

a Мостов софтуер
b Сървърен софтуер
c Шлюзов софтуер
d Маршрутизиращ софтуер

8 Как се нарича софтуерният компонент, който прихваща обръщения към ресурси и ги изпраща по мрежата, вместо към локалната шина?

a Платформа

b Клиент

c Директор

d Редиректор

9 Кои от следните са услуги, предоставяни от CIFS (Common Internet File System)? (Изберете всички верни отговори.)

a Преобразуване на имена

b Dialup достъп

c Услуги за споделяне на файлове и принтери

d Сигурност на ниво файлове

10 Кой от следните компоненти на SAMBA е отговорен за осигуряване на услуги за автентикация и авторизация?

a SMBd

b MBXd

c NMBd

d smbfs

Част III

Особености в областта на мрежите

Глава 14 Защита на мрежата

Глава 15 Отдалечен достъп

Глава 16 Виртуални частни мрежи

Глава 17 Мрежи за тънки клиенти

Глава 18 Инструменти за наблюдение, управление и отстраняване на неизправности

Глава 14

Защита на мрежата

В Част I, „Въведение в мрежите“, научихте техническите концепции, свързани със споделянето на данни в компютърни мрежи. В Част II, „Мрежов хардуер и софтуер“, разгледахме подробно начините за съвместна работа на хардуерните компоненти, операционните системи на клиента и сървъра, и мрежовите протоколи, правещи възможно споделянето на данни.

Още не сме разгледали един важен аспект на споделянето на компютърните ресурси по мрежата: поддържането на целостта на споделените данни. При защитата на данните от загуба или злоупотреба съществуват два проблема за решаване:

- Мрежова сигурност
- Предпазване от бедствия и възстановяване

Колкото повече бизнесът става зависим от компютърните мрежи и информацията, която те съдържат, толкова по-уязвим става той, когато нещо върви зле. Скандалният закон на Мърфи твърди, че рано или късно нещо *задължително* се скапва. „Нещото“ може да включва преднамерени или случайни пробиви на сигурността на мрежата, включващи дори промишлен шпионаж. От друга страна „нещото“ може да приеме формата на отказ на твърдия диск, наводнение или пожар, които да унищожат сървъра.

В тази глава ще обясним въпросите, свързани със защитата на данните, и ще разгледаме пътищата за редуциране на риска от загуба на данни, без да се отказваме от множеството предимства при свързването на компютрите в мрежа и свързването им към външния свят. Ще научите, че в някои случаи свързването в мрежа работи дори във ваша полза, правейки защитата и възстановяването на данните по-лесно, отколкото би било на една самостоятелна система.

Мрежова сигурност

Мрежовата сигурност е горещ проблем в света на информационните технологии. Често оповестявани в медиите са проникванията в мрежи на правителствени и големи бизнес организации, широко разпространените атаки на компютърни вируси и квалифицираните криминални случаи с компютърни хакери. От администраторите на многонационални корпоративни мрежи до потребителите на домашни компютри с dialup акаунти за Интернет, почти всеки, който е „онлайн“, е заинтересован до някаква степен от проследяването на възможността за неоторизиран достъп.

За различните хора *сигурността* означава различни неща. Макар че думата (според тълковния речник) е синоним на „гаранция“, в контекста на мрежите сигурността никога не е абсолютна. Единствената напълно сигурна система е тази, до която *никой* няма достъп. Очевидно тя е неработеща. *Компютърната сигурност* е дефинирана от Microsoft Press Computer and Internet Dictionary като „необходимите действия за защита на един компютър и информацията, която той съдържа“. В тази дефиниция не се споменава за никакви гаранции.

Проблемите на сигурността могат да създадат неприятелски отношения между мрежовия администратор и потребителите в мрежата. По принцип потребителите предпочитат да имат по-свободен достъп, а администраторите – да го ограничават с цел постигане на по-голяма сигурност.

В следващите секции ще разгледаме начините, по които можете да удовлетворите нуждите от сигурност на конкретна мрежа, да определите съществуващи и потенциални заплахи за сигурността и да реализирате подходящи мерки за сигурност. Също така ще разгледаме начините на работа на компонентите на сигурността и някои усъвършенствани технологии за идентификация и автентикация.

Определяне на нуждите за сигурност

Когато изграждаме компютърна мрежа, колко сигурност ще ѝ бъде достатъчна? Отговорът зависи от организацията. Първата стъпка в разработването на осъществим план за защита на вашите компютърни данни е определянето на нуждите от сигурност. Факторите, които трябва да бъдат оценени, са следните:

- Типът на бизнеса, в който участва компанията
- Типът на данните, съхранявани в мрежата
- Философията за управлението на организацията

Да разгледаме всяко поотделно и да обсъдим защо то е важно.

Тип на бизнеса

Някои типове бизнес, например юридическата сфера или медицината, поради самата си природа генерират поверителни данни. Частният характер на медицинските данни на пациента или комуникацията адвокат-клиент са защитени от закона. Ако във вашата мрежа се съхраняват конфиденциални документи, безапелационно трябва да бъде поддържано високо ниво на сигурност. Ако това не бъде направено, организацията се подлага на риска от гражданска отговорност и дори обвинения в криминално деяние.

И други типове организации често произвеждат поверителни данни:

- Агенциите на изпълнителната власт, съдилищата и други правителствени институции
- Образователни институции, които съхраняват данни за студенти в мрежа
- Болници, психиатрични заведения и заведения за временно лишаване от свобода
- Компании, които сътрудничат на Министерството на отбраната или извършват друга работа, свързана с националната сигурност.

- Всяка организация, която събира данни срещу гаранция за конфиденциалност
- Всяка организация, която произвежда продукт или предоставя услуга в областта на индустрията с висока конкурентност, или прави научни изследвания в такава област
- Всяка организация, мрежата на която е свързана към Интернет

Тип на данните

Независимо от типа на бизнеса, определени типове данни се считат за частни и трябва да бъдат защитени. Тези типове са следните:

- Заплатите и персоналната информация на служителите
- Счетоводната и данъчната информация
- Търговски тайни, като оригинален код, планове и диаграми, рецепти и бизнес стратегии

Ако във вашата мрежа се съхраняват такива типове информация, трябва да реализирате план за сигурност, за да защитите данните.

Философия на управление

Ако данните в мрежата не са от частен характер, нивото на сигурност може да зависи от персоналната философия на собствениците или мениджърите на бизнес организацията, като се вземе предвид колко отворена (или затворена) искат да бъде мрежата.

В някои организации всеки се счита за част от едно голямо щастливо семейство. Достъпността и лекотата на използване се радват на по-голяма популярност, отколкото конфиденциалността и сигурността. Други организации действат на принципа „необходимо му е да знае"; управлението предпочита информацията да бъде достъпна само за този, чиято работа я изисква. Нито една от двете политики не е нито напълно правилна, нито напълно погрешна; мрежовите администратори просто трябва да познават и реализират сигурността на мрежата съобразно стила на управление на организацията.

ЗАБЕЛЕЖКА Distributed Denial of Service (DDoS) (разпределен отказ на услуга) атакува работата на мрежата, като излага компютрите посредници и подмолно инсталира софтуер на тях, който ще бъде използван като част от атакуващата платформа. По този начин компютрите на компанията може неволно да участват в атаката и в резултат от това да си навлекат наказателна отговорност. По тази причина е важно всички мрежи, свързани към Интернет, да реализират политики на сигурност независимо от степента на конфиденциалност на техните собствени данни.

Определяне на заплахите за сигурността

След като вземете решението, че типът, данните и философията на управление на вашия бизнес изискват реализиране на мерки за сигурност, трябва да определите вероятните източници на заплаха за целостта на вашите данни.

Организациите могат лесно да подценят, надценят или напълно да пренебрегнат рисковете, на които са изложени техните мрежи. Въпреки това има много различни типове заплахи за сигурността на мрежата и те всички трябва да бъдат класифицирани в една от следните две най-общи категории:

- Външни заплахи
- Вътрешни заплахи

В следващите секции са описани тези типове заплахи.

Външни заплахи

Преди време външните заплахи не бяха сериозен проблем за локалните мрежи на повечето организации. Най-общо мрежата беше самостоятелна, и за да може даден нарушител да проникне отвън, той или тя трябваше да набере модем някъде в мрежата или до се закачи към кабела. Сега, когато повечето LAN мрежи са свързани към Интернет, всичко това е променено. Когато вашата мрежа може да осъществява достъп до външния свят, външните хора също имат достъп до вашата мрежа.

Мотивите на външните нарушители са различни. Най-често срещаните мотиви са отмъщение (недоволни клиенти, вечно обидени бивши служители и сърдити конкуренти), развлечение (такива, които се „хакват" в мрежите „просто за забавление", или за да докажат своите технически умения) и срещу заплащане. В последния случай на нарушителя е заплатено да нахлуе в мрежата, или той прави това за лична изгода; например хакерът може да се опита да прехвърли парични суми на своя собствена банкова сметка или да изтрие записите за своите дългове.

Външните пробиви в сигурността могат да приемат множество форми, в това число:

- Неоторизирано използване на пароли и ключове
- Атаки от типа Denial of Service (DOS)
- IP спуфинг
- Компютърни вируси и червеи
- Програми тип троянски коне

В следващите секции ще разгледаме всеки от тези методи на проникване.

Неоторизирано използване на пароли и ключове

Паролата представлява последователност от буквени, цифрови или символни знакове, използвани за удостоверяване, че даден потребител наистина е лицето, оторизирано да използва конкретен акаунт за достъп до система или мрежа. *Ключът* представлява число или шифър, използван от системата за проверка за валидност на целостта на комуникацията.

Паролите и ключовете са мерки за сигурност, предназначени за отблъскване на неоторизирани лица, но те са ефективни само ако се запазят в тайна. Ако някой знае името и паролата на вашия потребителски акаунт и има физически достъп до компютъра или мрежата, това лице може да осъществи достъп до всяко нещо, до което вие имате позволения за достъп. Придобиването на парола често е първата стъпка от хакването на системата.

Терминът *хакер* има различни значения в зависимост от това, кой го използва. В ранните дни на компютъризацията хакер означаваше добър програмист, но в съвременните медии бе популяризирано по-отрицателно значение. Днес това обикновено означава някой, който се вмъква в компютърни системи, често с намерение да открадне или унищожи данни.

Хакерите често биват представяни като зли гении, които използват интелигентни тайни техники, за да получат достъп до компютри и мрежи. Истината не е чак толкова вълнуваща – в голям процент от инцидентите вмъкването изобщо не е базирано на високи умения в програмирането. Често хакерите осъществяват достъп до мрежата по същия начин, както оторизираните потребители – чрез въвеждане на име и парола на потребителски акаунт. В този смисъл те често биват наричани „кракери", защото „кракват" (разбиват) или придобиват паролата и влизат в мрежата така, както касоразбивачът отваря банков сейф.

ЗАБЕЛЕЖКА Придобиването на неоторизиран достъп с използване на акредитивите на някое друго лице е форма на *имперсонация*. Този тип пробив на сигурността включва IP спуфинг и други методи на представяне като някой друг (или нещо друго, например системно устройство), какъвто всъщност не е.

Хакерите придобиват необходимите пароли по много начини. Често не се използва никакво техническо умение – хакерът просто използва способностите си да наблюдава или да убеждава, за да придобие пълномощията на потребителя, на когото те принадлежат.

Много потребители създават пароли, които лесно могат да бъдат отгатнати (например своите рождени дати или първите имена на съпрузите). Други създават – или им биват задавани от администраторите – пароли, които са по-трудни за отгатване. Тъй като това прави паролите по-трудни за запомняне, потребителите ги записват на хартия, често ги оставят в леснодостъпно чекмедже на бюрото или дори на залепваща се бележка на компютърния монитор.

Хакерите могат също да придобият пароли просто като се представят за мрежови техници, администратори на компании или други, на които наивният потребител счита за сигурно да разкрие своята парола. Понякога това се нарича *атака от тип социален инженеринг*.

Атаката на грубата сила е друг начин за придобиване на пароли. Това означава изпробване на всяка възможна парола, докато бъде открита такава, която става. Хакерите пишат скриптове и програми, наречени кракери на пароли, които автоматично изпробват списъци от често използвани думи и буквеноцифрови комбинации, така че нарушителят не е нужно да стои и ръчно да въвежда парола след парола.

Ако тези методи пропаднат, технически по-грамотните хакери могат да придобият пароли чрез прихващане на пакетите с данни, съдържащи паролите, с помощта на така наречения „снифър на пакети". Тази техника е причина за криптирането на паролите, вместо изпращането им по мрежата като чист текст. Подетайлно ще разгледаме снифър софтуера в Глава 18, „Инструменти за наблюдение, управление и отстраняване на проблеми".

Сигурността на паролите е важна част от изграждането на добра обща политика на сигурност за мрежата. Ще я разгледаме по-детайлно по-късно в тази глава в секцията „Сигурност на паролите".

DoS атаки

DoS атаките (т.е. атаки от тип отказ на услуга) могат да бъдат извършени по няколко начина. Независимо от метода, те са предназначени да прекъснат нормалните операции на машината, която е прицелна точка на атаката. Тези типове атаки понякога се наричат също *нюк (nuke) атаки*. През февруари 2000 г. няколко големи Web сайта (включително Amazon.com и Yahoo!) бяха временно изключени по този начин.

Някои DoS атаки използват бъгове в конкретни операционни системи или приложения, а други са насочени към самата мрежа. Често това са така наречените „кръпки", или пачове (софтуер, предоставян от производителите на операционни системи или приложения за отстраняване на проблем в програмата), предоставяни от производителя на софтуера за запушване на „дупките", които са обект на атаките.

DoS атаките не предизвикват срив на компютъра, а са проектирани така, че да прекъснат или да попречат на установяване на връзка към мрежата. Те работят, като наводняват мрежата с непотребни пакети, или като емулират мрежов проблем, който кара компютъра да прекрати установената връзка.

Някои най-често използвани форми на DoS атаки са:

- Наводнението на протокола Pimg/Internet Control Message Protocol (ICMP)
- Смърф атаката
- Ping на смъртта
- SYN атаките

В следващите секции всяка от тези форми е разгледана по-подробно.

Ping/ICMP наводнение ICMP наводнението е точно това, което подсказва неговото име – „наводнение" с пакети на протокола ICMP, водещо до задавяне на системата. ICMP е протокол за съобщения и проверка за грешки, използван за предаване на информация по Интернет. Командата **ping** е най-често използвана за изпращане на ICMP пакети с цел проверка дали конкретен компютър (който се идентифицира с помощта на IP адрес или име на хост, като второто в края на краищата също се преобразува в IP адрес) наистина съществува в мрежата. Ping работи, като изпраща съобщение, наречено ICMP Echo Request, и след това изчаква за отговор съобщение ICMP Echo Reply от „ping-вания" компютър.

Когато наводнението от пакети се изпраща непрекъснато до даден IP адрес, то може да дойде прекалено много на сървъра и той да забави своята работа, след което да се изключи поради таймаут на ping-а.

Смърф атака Смърф атаката е вид ICMP наводнение, което влияе на целия доставчик на услуга или мрежов адаптер целия мрежов сегмент. ICMP съобщенията се изпращат до бродкастен адрес, което принуждава всички компютри от тази подмрежа да отговорят. Когато даден ISP е „смърфиран", всички конекции биват забавени и всички потребители в крайна сметка губят връзката.

Смърф атаките са тип DoS атака. След като получи достъп до мрежата, атакуващият изпраща бродкаст в мрежата, използвайки като източник адрес в мрежата-цел. След това всички устройства в увредената мрежа изпращат ICMP отговори до адреса-цел. Може да имате стотици хостове, всеки от които изпраща хиляди битове ICMP ехо заявки в мрежата-цел. Трафикът, генериран от този процес, може лесно да задръсти връзките с ниска пропускателна способност, използвани във WAN връзките между някои ISP и мрежи. Мрежата-цел се сри-

IP спуфинг

IP спувингът (подправянето) включва промяна на хедърите на пакети на изпращаните съобщения. Това ги кара да изглеждат така, сякаш идват от IP адрес, различен от реалния адрес на първоизточника. Макар че спуфингът само по себе си не е форма на атака, той представлява метод за придобиване на неоторизиран достъп до компютър или мрежа за започване на атака, за кражба на данни или за унищожаване на данни.

Компютърни вируси и червеи

Компютърният вирус е програма, която може да се репликира и да се разпространява от един компютър на друг чрез копиране на нейния код в други файлове, съхранявани на системата, без съгласието или знанието на потребителя. Точно както при биологичните вируси, някои компютърни вируси са смъртоносни, а други са просто леко досадни. Например леките форми могат да визуализират съобщение на екрана на потребителя. По-злобните повреждат или унищожават данни, или изтриват файловете на операционната система, така че компютърът да не може да бъде стартиран.

Вирусите получаваха голямо внимание от медиите в миналото, когато вируси като Melissa, CIH (Чернобил), Michelangelo и Iloveyou проникваха в хиляди компютърни системи по целия свят.

Червеят (worm) е форма на злонамерен вирус, който се саморепликира и унищожава файлове на компютъра. Червеите често се разпространяват като атачмънти на електронна поща, като изпълними файлове, като документи, съдържащи макроси, или като HTML страници, съдържащи скриптове.

Програми тип троянски коне

Троянският кон представлява програма, която представя себе си като друга програма, за да придобие информация. Например има Троянски кон, който емулира екран за логване (login) в системата. Когато потребителят въведе на този фалшив екран своето име и парола, информацията се съхранява или предава до първоизточника на троянския кон. След това името и паролата могат да бъдат използвани за придобиване на достъп до системата.

Вътрешни заплахи

Много политики на сигурност в мрежата се фокусират само върху Интернет и външните заплахи. Това обикновено е грешка. По същия начин, по който компаниите за продажба на дребно откриват, че техните собствени служители крадат толкова (че дори и повече) от печалбите, колкото „външни“ клиенти, така и мрежовите администратори не трябва да пренебрегват риска от вътрешни пробиви на сигурността. Много случаи на кражба, злоупотреба или унищожаване на данни са „вътрешна работа“.

Съществуват няколко мотива за вътрешни пробиви на сигурността, а именно:

- Корпоративен шпионаж
- Вътрешни политики
- Недоволни служители (включително бивши служители)
- Случайни пробиви

Сега ще разгледаме накратко всички характеристики на всеки от тях и начините за предпазване.

Корпоративен шпионаж

Корпоративният шпионаж е най-интелигентният тип вътрешна заплаха за сигурността. Кражбата на търговски тайни е голям бизнес и благодарение на нея компаниите могат за една нощ да пропаднат или да успеят.

Служителите могат да бъдат сондирани от конкурентни компании и да им бъдат предложени изгодни възнаграждения за доставяне на секретна информация за организацията, в която работят. В други случаи служители на други компании могат да постъпят на работа във вашата компания, за да проникнат в нея и да събират данни за конкурента, като получават заплата едновременно и от двете компании.

Накрая, има корпоративни шпиони на свободна практика, които приемат поръчки под формата на договор. В индустриите с висока степен на конкуренция такива шпиони могат да откраднат данни по собствен план и след това да ги обявят за продажба на търг, за да извлекат максимална печалба. „Похитителите на данни" могат дори да държат като залог вашите конфиденциални данни, обещавайки да не ги разпространят на други организации, като в замяна поискат плащане на „откуп".

Корпоративните шпиони често са интелигентни хора с високи професионални умения и технически познания. Обикновено те са добре финансирани и могат да избегнат разкриване, докато не стане прекалено късно. Ако вашият бизнес е част от сфера, в която корпоративният шпионаж е разпространено явление (сфери като технологичната индустрия, горивата и енергията, изследователската медицина, инженеринга и други, в които успехът зависи от това да бъдеш първи на пазара с иновационни продукти или услуги), вашата мрежа може да стане цел на подобни атаки.

Мерките за сигурност, предназначени за осуетяване на тези професионални шпиони, трябва да бъдат от най-високо ниво. Може да се наложи да повикате консултанти, които са специалисти в защитата на корпоративни мрежи от такива намеси.

Вътрешни политики

Друг вътрешен риск представлява конкурентен служител, който ще направи всичко, за да върви напред и да надвие своите колеги за следващото повишение. Това лице може да се опита да осъществява достъп и да саботира работата на тези, в които вижда персонални конкуренти. Други може да се опитат да навредят на репутацията на други хора от екипа, в който работят, като претърсят тяхната електронна поща или файлове за уличаващи ги съобщения или друга персонална информация. Особено безскрупулна форма на такава амбициозна личност може дори да подстави инкриминиращи елементи в компютъра на жертвата или да изпрати уличаваща електронна поща, която изглежда като оригиналната на жертвата.

Макар че този тип злонамерено използване на мрежата представлява по-малка заплаха за важните данни на компанията, отколкото шпионажът, тя може да предизвика множество проблеми в организацията. Тъй като много от тези извършители на престъпления не са висококвалифицирани техници, добрите основни политики на сигурност (например силни пароли и одитинг на сигурността) могат да предотвратят или да изобличат техните действия.

Недоволни служители

Особено деструктивен тип заплаха за сигурността представлява служителят или бившият служител, който има зъб на организацията и иска да ѝ навреди. Тези хора могат да унищожат критично важни данни или да разрушат жизненоважни мрежови комуникации „просто за забавление“ или поради криворазбрано усещане за „справедливост“.

Компанията може да се окаже изложена на тази заплаха, когато е уволнен технически грамотен служител. Не са редки случаите, когато разгневеното лице отмъщава за своето уволнение, като изтрива твърди дискове, повреждa компютърен хардуер или разпространява вируси в мрежата на компанията.

Вашата политика на сигурност трябва да решава този проблем. Масовата практика показва, че потребителските акаунти на уволнените служители трябва незабавно да бъдат изтривани, а в някои случаи да бъде прекратен и техния физически достъп до компютрите на компанията. Последното може да бъде постигнато, като някой друг бъде натоварен да ескортира уволнения, докато пакетира личните си вещи, или когато влиза повторно в офиса на организацията.

Случайни пробиви

В много случаи вътрешните пробиви на сигурността не са преднамерени действия, а са причинени от техническото невежество или липса на подготовка на част от служителите. Мрежовите администратори познават добре потребители, които унищожават файлове на операционната система, докато се опитват да „оправят“ дребен проблем, или решават да „освободят малко дисково пространство“, като изтрият всички файлове на дадена приложна програма.

Случайните пробиви са основателна причина в света на бизнеса да са предпочитани за използване операционни системи със силни възможности за сигурност. Чрез реализиране на позволения на ниво файл с помощта на възможността System Policies на Windows NT или възможността Group Policies на Windows 2000, потребителите могат да бъдат възпрепятствани да изтриват или да преместват критично важни системни файлове.

Непокорни потребители

Вътрешните пробиви на сигурността могат да бъдат резултат също от потребители, които не са съгласни с политиките на сигурност, намирайки ги за прекалено ограничаващи. Макар че не са „случайни“, тези пробиви не са предназначени да предизвикват вреда; вместо това те имат за цел да разрешат на потребителя да прави нещо, което в противен случай не може да прави. Например ако настройките на сигурността не забраняват инсталирането на приложен софтуер или хардуерни драйвери, непокорният потребител, който не харесва вашите политики за достъп до Интернет, може да свърже външен модем, да включи телефонна линия, да инсталира драйверите и да набере свой собствен Интернет доставчик. Друг потребител може да инсталира приложение за отдалечен достъп, като PCAnywhere, което може да отвори този компютър – и вътрешната мрежа – за външните потребители, които също са си инсталирали софтуера PCAnywhere на техните компютри.

Вашите ответни действия срещу непокорните потребители ще зависят от политиките на организацията и от степента на сигурност, наложена в мрежата. Може да бъде уместно да се реализират по-строги правила за контрол; в други случаи може да бъде по-подходящо да се прецени дали вашите политики за сигурност реално не са излишно строги и дали не трябва да разрешите на потребителите да имат повече обществен достъп.

Реализиране на мерки за сигурност

Защитата на данните в мрежата често изисква прилагане на комбинирани методи за сигурност. В тази секция ще научите как потребителските акаунти, групи и позволения могат да послужат като първа линия на отбраната. След това ще разгледаме начините за криптиране на конфиденциални данни – във файлове на диска или в пакети, които пътуват по мрежата.

Тъй като електронната поща е едно от най-широко използваните мрежови приложения и тъй като това е формата на комуникация по мрежи, която най-вероятно съдържа конфиденциална информация, ще се фокусираме върху технологиите за управление на сигурността на e-mail съобщения. След като научите как се реализират мерките за сигурност, ще разгледаме реалния начин на действие на тези мерки.

Нива на сигурност на операционната система

Някои операционни системи сами по себе си са по-сигурни от други. По-старите операционни системи, например MS-DOS, не позволяват на потребителските акаунти да осъществяват достъп до операционната система (макар че за достъп до мрежата се изисква акаунт). Всеки може да седне на една DOS машина, да зареди операционната система и след това да стартира програми или да осъществява достъп до своите файлове на диска.

По-модерните операционни системи, като Windows 98, ви позволяват да създавате потребителски акаунти на компютъра. Въпреки това паролите могат да бъдат записани в незащитен текстов файл или до тях да бъде осъществен достъп чрез зареждане на компютъра от дискета с MS-DOS. По подразбиране, ако изберете Cancel, когато бъдете подканени да въведете потребителското име и парола, операционната система пак ще се зареди с пълни възможности за използване.

Операционните системи с висока сигурност, като Windows NT, Windows 2000 и Linux, изискват от вас да въведете валидно потребителско име и парола, за да заредите операционната система и да я използвате. Също така тези операционни системи съхраняват паролите в криптирана форма, до която не може да бъде осъществен лесен достъп.

Американското правителство осигурява спецификации за рейтинга на нивата на сигурност на компютрите. Те са разгледани в секцията „Разработка на политики на сигурност“ в тази глава.

Потребители, групи и позволения

Модерните операционни системи позволяват на множество потребители да осъществяват достъп до компютъра и мрежата чрез създаване на отделни потребителски акаунти, и дават възможност за задаване на различна парола за всеки от тях. Въвеждането на комбинацията от потребителско име и парола от промпта за логване води до следния резултат:

- На потребителя се дава достъп до операционната система и мрежата.
- Потребителят може да чете и записва в тези споделени ресурси, за които на неговия акаунт са дадени позволения.
- Потребителят може да упражнява такива права (например правото да изключва операционната система или да инсталира програми), каквито са зададени на неговия акаунт.

- Зареждат се общите настройки за потребителя, като например икони на десктопа и тапет (wallpaper).

В някои компютърни среди, в които на компютрите не се съхраняват конфиденциални данни и няма изисквания за сигурност, може да не се създават отделни потребителски акаунти. Всички потребители могат да използват един и същ акаунт за логване. Това означава, че всеки потребител има едни и същи позволения за достъп. Това не само създава отворена, необезопасена среда, а също означава, че потребителите не могат да приспособяват по свой вкус десктопа и други настройки.

В повечето бизнес организации е по-добре да се създадат отделни акаунти за различните потребители. Ако неоторизираният достъп не е проблем, паролите могат да бъдат оставени празни.

Сигурност на паролите

Важна част от всеки план за сигурност на мрежата трябва да включва осигуряване на колкото е възможно по-неразгадаеми пароли. Ако на потребителите се разреши сами да избират своите собствени пароли, трябва да бъдат зададени правила в съответствие с нуждите на сигурността на мрежата.

Ето някои примери за политики на сигурност:

- Паролите не трябва никога да бъдат думи или числа, които лесно могат да бъдат отгатнати поради тяхната връзка с потребителя (например номера на социалната осигуровка, името на потребителя или името на неговото куче).
- Тъй като много програми за атаки по метода на „грубата сила“ използват списъци от често използвани думи, паролите не трябва да бъдат думи, записани в речника. Добра политика е комбинирането на букви и цифри (например „heavy238“).
- В повечето операционни системи при въвеждане на паролата се отчита разликата между главни и малки букви, затова паролата, която съдържа главни букви на случайно подбрани позиции, е трудна за разгадаване (например „mYdoGspOt“).
- Паролата *трябва* да бъде лесна за запомняне от потребителя. Ако не е, рано или късно тя ще бъде записана на хартия.
- Колкото повече знакове има паролата, толкова по-трудно е някой да я разгадае; затова „visualize“ е по-добра парола от „see“. Този фактор трябва да бъде балансиран със способността на потребителя да запомни дългата парола.
- В среда с висока степен на сигурност, потребителите трябва да се задължават периодично да променят своите пароли. Новите пароли не трябва да приличат на старите. Например потребителят не трябва да може да промени паролата си от „panda3“ на „panda6“. Ще повторим, че е важно да се поддържа баланс, защото потребители, от които се изисква да променят своите пароли прекалено често, няма да могат да ги запомнят и ще започнат да ги записват на хартия.
- Повечето мрежови операционни системи позволяват на администратора да задава такива критерии, като минимална дължина на парола, история на паролите (в която се съхранява списък на предишните пароли на потребителите и не се допуска повторното им използване) и сроковете на

годност на паролите (което задължава потребителя да променя паролата на зададени интервали от време). Също така има програми за сигурност на паролите, които дават възможност на администраторите да задават параметри за пароли. Например даден параметър може да забрани пароли, които не присъстват в речника.

ЗАБЕЛЕЖКА Някои операционни системи със засилена система за сигурност (например Windows NT и Windows 2000) няма да ви позволят да оставите паролите празни по подразбиране; за да разреши това, администраторът трябва да промени настройките на политиката за пароли.

Политики за контрол на достъпа

Модерните мрежови операционни системи (NOS) позволяват на администраторите да управляват достъпа до ресурсите на грануларна основа. На потребителския акаунт marysmith например може да бъде дадено позволение да разглежда съдържанието на file1.doc, но да не е разрешено да прави промени. В същото време потребителят може да има позволение да разглежда, променя, изтрива или дори да задава позволения за достъп за file2.doc, но да няма позволения за достъп до file3.doc.

На всеки отделен потребител може да бъдат дадени точно позволенията, от които се нуждае. С помощта на файлови системи с висока сигурност позволенията могат да бъдат задавани не само за ресурси, до които се осъществява достъп по мрежата, а също и за ресурсите, до които се извършва достъп от самата локална машина. Локалните и мрежовите позволения не е задължително да бъдат едни и същи. На Мери може да бъде даден пълен контрол върху file4.doc, когато тя осъществява достъп до този файл след логване на машината, на която е съхранен файлът, но да бъде ограничена да го чете, ако осъществява достъп до него от отдалечена машина по мрежата.

Важно е да знаете и да се съобразявате с подразбиращите се позволения, използвани от мрежовата операционна система. Например при Windows NT или Windows 2000 Server, когато споделите ресурс, той е напълно достъпен за всеки в мрежата, докато не отмените изрично тези позволения. На сървър с NetWare е в сила обратното – споделеният ресурс не е достъпен за никого чак докато изрично не промените позволенията на даден потребител.

Нито един от методите не е изцяло правилен или погрешен, но ако не знаете как работят позволенията на вашата мрежова операционна система, може да се окаже, че сте разрешили достъп до ресурси, които не искате да откривате, или пък сте забранили достъпа на потребители, които трябва да имат такъв.

В организация, заинтересувана от прилагане на система за сигурност, трябва да бъдат създадени политики, в които да бъде указано кой трябва да има достъп и до кои ресурси. Най-общо достъпът трябва да бъде предоставян на принципа „трябва да знае“. Ако потребителят трябва да има достъп до ресурса, за да изпълнява своите служебни задачи, трябва да бъдат дадени позволения. В противен случай достъпът трябва да бъде отказан.

Използване на групи на сигурност

Групите на сигурност са създадени в помощ на администраторите и се поддържат от много мрежови операционни системи с цел улесняване на задаването на

позволения в голяма мрежа. Създават се групи, и на тези групи се дават позволения за достъп до ресурси. След това в групата се поставят съответните потребителски акаунти, като по този начин на всеки потребител веднага се дават всички позволения, зададени за групата като цяло. Това е по-лесно, отколкото задаването на позволения на всеки потребител поотделно.

Например ако някой от отдела по продажби трябва да има достъп до няколко папки (да ги наречем salestats, salesbudget, salestatsmemos), можете да зададете позволения за достъп за всяка папка на до 20 потребителя в отдела. Но по-лесният метод е да създадете група на сигурност, наречена sales, да ѝ дадете позволение за достъп до всичките три папки и да поставите 20 потребителски акаунта в нея. След това, ако създадете нова папка – например salescalendars, до която трябва да има достъп целият отдел – то всичко, което трябва да направите, е да зададете позволения за групата sales. В противен случай ще трябва да зададете позволения за новата папка на 20 различни акаунта.

Ако не искате даден потребител да има достъп до определен ресурс, не приемайте, че е достатъчно само да премахнете това позволение от неговия потребителски акаунт. Трябва също да се уверите, че потребителят не е член на никоя група, която има позволения за достъп до ресурса. Освен това, ако операционната система (например Windows NT или Windows 2000) ви позволява конкретно да забраните достъпа, трябва изрично да направите това.

Криптиране на файлове

Криптирането включва конвертиране на данните във форма, която не може лесно да бъде разбрана от другите. Техническите аспекти на криптирането са разгледани по-детайлно в секцията „Как работят компонентите на сигурността“ по-нататък в тази глава.

Криптирането на файлове е способ за криптиране на данни, съхранявани на диска на компютъра, така че те да не могат да бъдат прочетени от никого, а само от създателя на данните. Някои операционни системи, като Windows 2000, включват функция за криптиране на файлове. За тези, които не поддържат такава функция (например Windows 9x и Windows NT), са достъпни програми за криптиране от външни производители.

Когато документите са криптирани на диска, може да ги разглежда само потребител, който има правилен ключ. Ако други опитат да осъществят достъп, тогава или файлът няма да се отвори изобщо, или ще се появи като объркани безсмислени знакове. Обърнете внимание, че конфиденциалните данни трябва да бъдат защитени както с позволения за достъп, така и с криптиране.

Протоколът IP Security

Криптирането на файловете защитава данните, съхранявани на диска, но то не предлага сигурност за данните по време на тяхното пътуване по мрежата. Протоколът IP Security (IPSec) беше разработен като средство за решаване на този проблем. IPSec реализира сигурност на данните на нивото на отделния пакет. Тъй като работи в мрежовия слой на референтния OSI модел, приложенията не го забелязват. Cisco Systems включва поддръжка на IPSec в своите маршрутизатори, а Windows 2000 включва IPSec в своя TCP/IP стек.

IPSec използва два протокола:

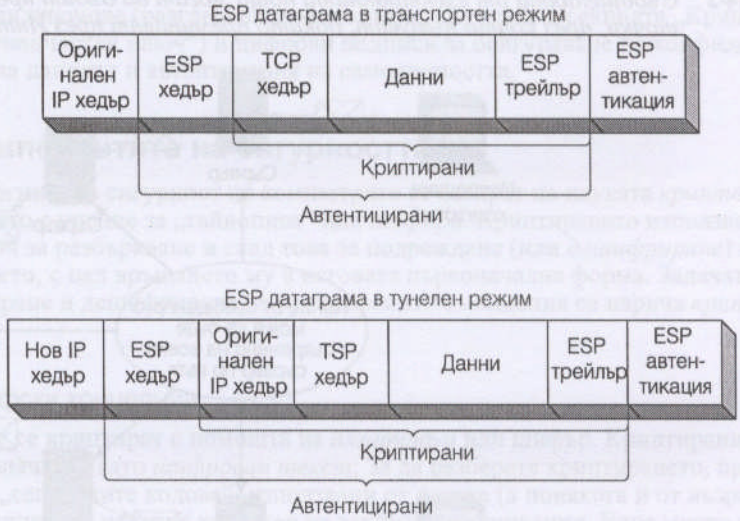
- **Authentication Header (AH)** – Позволява проверка на самоличността на изпращащия IPSec

- **Encapsulating Security payload (ESP)** – гарантира конфиденциалността на самите данни

Тези два протокола могат да бъдат използвани поотделно или заедно.

IPSec може да работи в два режима: транспортен и тунелен. Вижте Фигура 14-2. Транспортният режим осигурява *сигурност от край до край*; т.е. криптирането се извършва от компютъра източник до компютъра местоназначение. Тунелният режим защитава данните от изходната точка на една мрежа до входната точка на друга.

Фигура 14-2 *Хедърите на пакетите се различават в зависимост от това, дали IPSec се използва в транспортен или тунелен режим.*



Secure Sockets Layer (SSL)

SSL е друго средство за управление на сигурността на мрежовите комуникации. Недостатъкът на SSL е, че работи в приложния слой; затова трябва да бъде поддържан от потребителското приложение.

SSL беше разработен от Netscape за управление на сигурността на техния Web браузър. Той използва *криптиране с публичен и частен ключ*. Тези средства са описани в секцията „Как работят компонентите на сигурността“ по-нататък в тази глава.

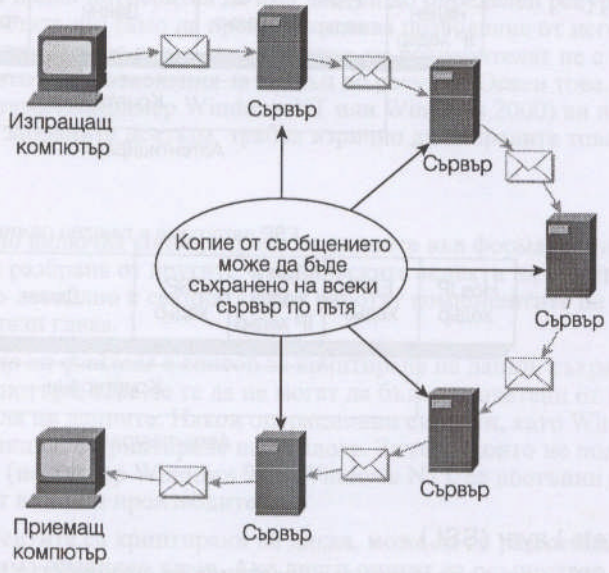
Сигурност на електронната поща

Много компютърни потребители се радват на измамно чувство за сигурност на мрежовите комуникации като цяло и в частност на съобщенията по електронната поща. Потребителите приемат, че съобщенията, които съставят и изпращат по локалната мрежа или по Интернет, се четат само от получателите, до които са адресирани съобщенията. Потребителите на електронна поща се държат така, сякаш при изпращане на електронна поща очакват същата конфиденциалност, както при изпращане на писмо по обикновена поща. По-вярното сравнение е, че електронната поща прилича на открита пощенска картичка, ко-

ято може да бъде прочетена от всеки, който я пренася по време на нейното пътуване от подателя до получателя.

Съобщенията от електронната поща са много лесни за прихващане (Фигура 14-3). Те често пътуват през десетки възли (сървъри) по своя път от предаващата до приемащата страна. Дори ако съобщението е изпратено до някой в локалната мрежа, негово копие се съхранява поне на три машини: на компютъра на изпращащия, на компютъра на приемащия и на вътрешния сървър за електронна поща. Електронна поща, изпратена по Интернет, може да премине също през няколко сървъра. Ако не е криптирано или подписано с цифров подпис, съобщението може лесно да бъде прочетено, копирано или променено във всяка една точка по неговия път.

Фигура 14-3 *Съобщенията от електронната поща могат да бъдат прехващани в много точки, през които пътуват, докато преминават през Интернет.*



ПРЕДУПРЕЖДЕНИЕ Изтриването на съобщението на машината на потребителя *не* гарантира, че негово копие не се намира на един или повече сървъри.

За решаване на този проблем са разработени много софтуерни продукти. Тези продукти са предназначени за постигане на следните цели:

- Съобщението не може да бъде четено от неоторизирани страни.
- Съобщението не може да бъде променяно от момента на напускане на изпращащата страна до момента на отварянето му от приемащата страна.
- Лицето, идентифицирано като изпращаща страна на съобщението, реално е това, което претендира, че е.

Важен фактор в софтуера за защита на електронната поща е лекотата на използване. Ако потребителите трябва да изпълняват сложни или бавни действия, наред с изпращане и четене на защитената електронна поща, те вероятно изобщо ще се откажат от софтуера за сигурност.

Популярни програми за защита на електронната поща са:

- Pretty Good Privacy (PGP)
- Kerberos
- Baltimore Mail Secure
- MailMarshal на Softec

Повечето от софтуера за защита на електронната поща използва криптиране с публични ключове (разгледано по-нататък в тази глава в секцията „Криптиране с публичен/частен ключ“) и цифрови подписи за осигуряване на конфиденциалност на данните и автентикация на самоличността.

Как работят компонентите на сигурността

Технологиите за сигурност на компютрите се базират на науката *криптография*, която е учение за „тайнописа“ или *шифъра*. Криптирането използва код или ключ за разбъркване и след това за подреждане (или *дешифриране*) на съобщението, с цел връщането му в неговата първоначална форма. Задачата по анализиране и дешифриране на криптираните съобщения се нарича *криптоанализ*.

Основни криптографски концепции

Данните се криптират с помощта на *алгоритъм* или шифър. Криптираните данни се означават като *шифрован текст*. За да разберете криптирането, представете си „секретните кодове“, използвани от децата (а понякога и от възрастните) за защита на частния характер на техните комуникации. Една много проста схема на криптиране задава число на всяка буква от азбуката. Ако започнем с A като 1, B като 2 и т.н., можем да изпратим „кодирано“ съобщение като следното:

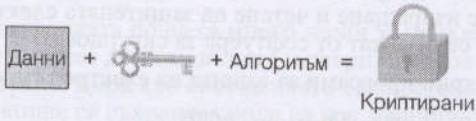
```
4-9-14-14-5-18   9-19  18-5-1-4-25
```

Съобщението лесно може да бъде „декодирано“ или *декриптирано* до оригинала:

```
Dinner is ready (вечерята е готова)
```

За нещастие, този шифър лесно може да бъде разбит (кракнат) и затова не е сигурен. Криптирането при компютрите е по-сложно. Най-общо се използва *ключ (key)*, който е някакъв вид променлива, комбинираща се с данните, които се криптират. Методът на комбиниране на ключа с данните се нарича *алгоритъм*. Тъй като компютрите обработват двоична информация, тези изчисления се прилагат към всеки бит или група от битове (вижте Фигура 14-4).

Фигура 14-4 *Техниките на компютъризирано криптиране използват ключове и алгоритми.*



Колкото по-дълъг е ключът за криптиране, толкова по-трудно е да се разбие кодът. В областта на криптирането 40- и 56-битовото криптиране се нарича *стандартно криптиране*, а 128-битовото криптиране се нарича *силно криптиране*.

Закони, управляващи технологиите за криптиране

Много държави имат законови ограничения върху експорта или импорта на технологии за криптиране. САЩ класифицират криптирането като „бойно средство“ и забраняват експортирането на софтуер за силно криптиране. Може да бъде експортирана криптология до 40 бита, а криптология над 56 бита може да бъде експортирана при определени условия. Технологии за криптиране над 128 бита не могат да бъдат експортирани. В импорта на елементите за криптиране няма ограничения.

Законите в другите страни варират от Аржентина, която няма контрол над експорта и импорта и ограничения на използването на криптография, до Русия, където се регулира както импорта, така и експорта, а използването на неоторизирано криптиране в страната е забранено.

Два популярни типа криптиране са криптирането със секретен ключ и криптирането с публичен/частен ключ. Да разгледаме как работи всяко от тях.

Криптиране със секретен ключ

Криптирането със секретен ключ често се означава като *симетрично криптиране*, защото един ключ се използва както за криптиране, така и за декриптиране на данните. Предаващата и приемащата страни се договарят за използване на общ ключ или криптиращ алгоритъм, който представлява *споделена тайна*. Например, ако Тед и Керъл искат да обменят поверителни съобщения, те се решават, че всяка буква от азбуката ще се представя от следния код:

1. Конвертиране на буквата в цифра с помощта на схема, при която A=6, B=7, C=8 и т.н.
2. Умножаване на резултатното число по 4.

Този ключ, макар че не е невъзможно да бъде разгадан, е доста по-сигурен от първия пример. Сега, за да изпрати съобщението „Dinner is ready“, Керъл преминава през следния процес, за да постигне крайното криптирано съобщение:

```
D = 9
9 · 4 = 36
I = 14
14 · 4 = 56
```

Накрая тя достига до крайното криптирано съобщение:

```
36-56-76-76-40-92 56-96 92-40-24-36-120
```

Тед има същия ключ и знае, че за да декриптира съобщението, трябва само да раздели всяко число на 4 и след това да приложи същата таблица A=6, B=7, C=8 и т.н., за да възстанови оригиналното съобщение.

Популярни алгоритми за криптиране със секретен ключ са Data Encryption Standard (DES) и 3DES (произнасян „трипъл DES“). Друг алгоритъм е RC (Rivest Cipher)-4, създаден от Рон Ривест. Този човек, заедно с Ади Шамир и Леонард Адлеман, разработват популярната схема за криптиране с публичен ключ RSA, разгледана в следващата секция на тази глава.

При криптирането със секретен ключ има три същностни проблема:

- Генериране на секретни ключове
- Обмен на ключовете между оторизираните страни, без да попадат в ръцете на неоторизирани страни
- Справяне със сложността, характерна за реализиране на сигурност на комуникациите до много различни страни

Благоразумно е да променяме ключовете през определени интервали от време, за да избегнем компрометиране на сигурността. Това означава, че трябва да бъдат генерирани допълнителни ключове. Също така трябва да има начин за получаване на ключа от страната, оторизирана да дешифрира съобщението. В предишния ни пример, ако Керъл изпрати по електронната поща ключа на Тед без криптиране, тя осуетява целта на криптирането на комуникацията. От друга страна, ако тя му изпрати съобщението криптирано, той няма да може да го прочете, защото не знае ключа.

Разработени са механизми за сигурно генериране и обмен на ключове. Един пример е алгоритъмът на Дифи-Хелман, който позволява на две страни да създават тайна, известна само на тях, независимо от факта, че комуникират по мрежа без реализирана сигурност.

Третият проблем от горния списък е малко по-проблематичен. Керъл и Тед могат щастливо да обменят (до известна степен) сигурни съобщения с години, използвайки техния секретен ключ, но какво ще стане, ако Керъл поиска да изпрати сигурно съобщение до Боб? Ако тя използва същия ключ, Тед ще може да дешифрира съобщението. Освен това, след като Боб има ключа, той също може да дешифрира съобщенията на Керъл до Тед.

За да разрешим ситуацията, Керъл и Боб могат да използват напълно различен ключ. Например съобщенията до Боб могат да бъдат криптирани чрез преобразуване на буквата в число с помощта на цифровата схема A=12, B=13 и т.н., и след това прибавяне на 15 към резултата. Но сега Керъл трябва да помни два ключа, и ако иска да изпрати сигурни съобщения до голям брой хора, тази техника бързо става неуправляема. По-просто решение е да се използва различен тип криптиране: криптиране с публичен/частен ключ.

Криптиране с публичен/частен ключ

Макар че за краткост често пъти се означава като криптиране с публичен ключ, по-точният термин е *криптиране с публичен/частен ключ (public/private key encryption)*, тъй като този тип криптиране използва два ключа – единият от тях се публикува и е широко достъпен, а другият е частен и се знае само от потребителя. За извършване на сигурната комуникация са необходими и двата ключа. Този тип криптиране се нарича също *асиметрично криптиране*. При него всеки

потребител има и публичен, и частен ключ, наречени *двойка ключове*. Ето как работи това:

1. Керъл и Тед обменят своите публични ключове. Няма значение, че това се прави по несигурен начин, защото съобщенията не могат да бъдат дешифрирани само с публичния ключ.
2. Керъл иска да изпрати съобщение на Тед, затова тя криптира съобщението, използвайки публичния ключ на Тед. Публичният ключ се асоциира (съответства) само на един частен ключ. За да се декриптира съобщение, което е криптирано с помощта на публичен ключ, е необходим съответстващият му частен ключ. (В сила е и обратното – за да се декриптира съобщение, криптирано с помощта на частен ключ, е необходим съответстващият му публичен ключ).
3. Тед, използвайки своя частен ключ, може да дешифрира съобщението, защото то е криптирано с неговия публичен ключ. Обърнете внимание, че в този процес на криптиране бяха използвани само ключовете на Тед – публичен и частен.

Ако Керъл криптира съобщението с помощта на нейния частен ключ, всеки може да декриптира съобщението, използвайки нейния публичен ключ, който е достъпен за всички.

За да работи този вид криптиране, трябва да бъдат използвани и двата ключа на една двойка ключове; не е нужно никой да знае частния ключ на някой друг. Един добър начин да разберете този тип криптиране е да си представите двете части информация, необходими за влизане в къща, защитена от ключалка с цифрова комбинация. Ако някой иска да влезе в къщата, той или тя трябва да знае както адреса на улицата, така и цифровата комбинация за отваряне на заключващото устройство. Адресът е публична информация, която се публикува в телефонния указател. Тя е достъпна за всеки, точно както публичният ключ е достъпен на всеки. Комбинацията на ключалката е аналогична на частния ключ на потребителя; тя е позната само на собственика на къщата. За тази конкретна къща и двата ключа са уникални, но единият е направен публичен, докато другият е запазен в тайна.

Автентикация

Примерите, които разгледахме дотук, се занимават с *конфиденциалността* на данните. Отделен проблем е *автентикацията* на изпращащия данните.

С помощта на метода на публичния/частния ключ можете лесно да реализирате сигурността за самите данни. Но тъй като публичният ключ е достъпен за всеки, Тед не може да знае със сигурност, че съобщението, което е приел и което е криптирано с неговия публичен ключ, наистина е от Керъл. За да провери истинността на самоличността на изпращащия (да го автентицира), Керъл трябва да криптира съобщението с нейния *частен* ключ. След това Тед може да го декриптира с нейния публичен ключ, като е сигурен, че тя е истинският подател, защото само тя знае собственият си частен ключ.

Друг начин за осигуряване на автентикация на изпращащия е да се използват цифрови подписи, които ще разгледаме в следващата секция.

Цифрови подписи

Цифровите подписи се състоят от криптирана подписваща информация, добавена към документа. Тази информация верифицира както идентичността на из-

пращащия, така и целостта на самия документ. Цифровите подписи не криптират данните. Те само гарантират, че данните не са променени и че изпращачът е автентичен.

Алгоритмите с публичен ключ се използват за създаване и верифициране на цифрови подписи и *хеш алгоритми*. Хеш алгоритмите ще разгледаме по-долу.

Хеш алгоритми

Хешът представлява резултатът от еднопосочно математическо изчисление (хеширащ алгоритъм), което създава *дайджест на съобщение (message digest)*. Алгоритъмът се нарича „еднопосочен", защото не можете да обръщате (реверсирате) резултата, за да откриете оригиналното съобщение.

Хешът верифицира автентичността на съобщението по следния начин:

1. Изпращачът хешира съобщението с ключ, който е споделена тайна; т.е. ключът е известен както на изпращача, така и на получателя. Хешът изработва числов резултат (например 0010110010100001).
2. Съобщението и резултатът, или *дайджест на съобщението*, се изпращат на приемника.
3. За да потвърди, че съобщението не е променено, получателят прилага същия ключ и трябва да получи същия числов резултат (0010110010100001). Ако съдържанието на съобщението е променено, резултатът на хеша няма да съвпада.

Ето някои популярни алгоритми за хеширане:

- **Secure Hash Algorithm (SHA)** – Разработен от Националния институт по стандарти и технологии (NIST) и Националната агенция по сигурността (NSA)
- **Message Digest 5 (MD5)** – Разработен от Рон Ривест в Масачузетския технологичен институт (MIT)

Най-общо хеширащите алгоритми изработват стойност от поне 128 бита, което прави особено трудно или невъзможно изработването на същия резултат с различен набор входни данни.

Цифрови сертификати

Цифровите сертификати представляват съобщения, които съдържат цифровия подпис на доверена трета страна, наречена *сертификационна власт* (*certificate authority*). Третата страна гарантира, че конкретен публичен ключ реално принадлежи на конкретно лице. Сертификатите се използват за гарантиране на автентичността на съобщенията, които пътуват по несигурни публични мрежи, например Интернет.

Потребител, който притежава частния ключ, асоцииран с конкретен публичен ключ, изпраща заявка за сертификат от сертификационната власт. Сертификационната власт отговаря за верифицирането, че този конкретен публичен ключ принадлежи на конкретен потребител. Сертификатите са валидни за зададен период от време и сертификационната власт може да ги анулира (отнема).

Организациите могат да изграждат свои собствени сертификационни власти като част от *инфраструктурата на публичните ключове (PKI)* на тяхната мрежа. PKI е система за верификация и автентикация на самоличността на страните, вземащи участие в електронните комуникации.

Цифровите сертификати се издават от обществени сертификационни власти като:

- Verisign
- GTE Cybertrust
- Keywitness
- TradeWave

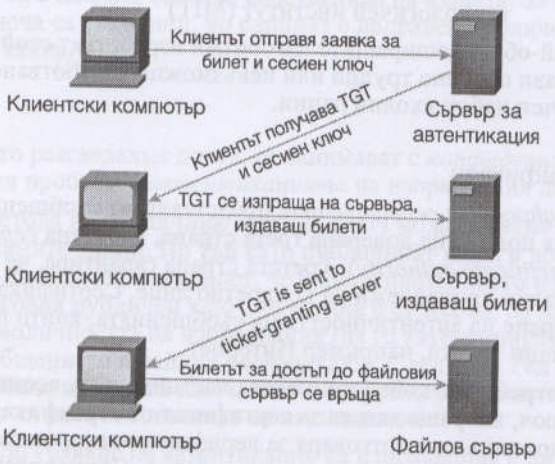
Цифровите сертификати могат да бъдат оприличени на електронни карти за самоличност. Подобно на издаваните от държавата шофьорски книжки, лични карти или други идентификационни документи, които могат да бъдат представяни за доказване на вашата идентичност във физическия свят, така и цифровите сертификати изпълняват тази функция в света на мрежовите комуникации.

Kerberos

Kerberos е протокол за автентикация, който е стандарт в Интернет за верификация на идентичността на потребител или компютърна система. Той е разработен в MIT и е наречен на името на триглавото куче от гръцката митология, което пази вратите на Хадес. Сигурността на Kerberos разчита на три фактора: клиент, сървър и проверен източник, наречен център за разпространение на ключове (KDC). KDC поддържа база данни, която следи участващите в комуникациите единици.

Kerberos е базиран на концепцията на билетите, които представляват криптирани съобщения, използвани за отправяне на заявка за услуга от сървър. Автентикацията се извършва с помощта на симетрично криптиране (означавано още като криптиране със секретен ключ). Вижте Фигура 14-5.

Фигура 14-5 *Процесът на автентикация Kerberos разчита на билети за верификация на идентичността и за предоставяне на достъп до сървъри.*



Ето как работи процесът Kerberos:

1. Първата стъпка включва изпращане на заявка от клиента до сървър за автентикация за билет и *сесиен ключ*. Това е ключ за криптиране, базиран на паролата на отправящия заявката потребител, и се комбинира със

случайна стойност, представяща исканата услуга. Връщаният обратно на клиента билет се нарича *билет за издаване на билет (ticket-granting ticket – TGT)*. Той верифицира самоличността на клиента.

2. TGT се изпраща от клиента на сървъра за издаване на билети (който може да бъде същата физическа машина, като сървъра за автентикация). На базата на TGT, сървърът за издаване на билети връща билет, който се представя на файловия сървър, до чиито ресурси клиентът иска достъп.
3. Билетът е валиден за конкретно количество време, през което клиентът може да отправя допълнителни заявки към сървъра, без да преминава отново през целия процес.

Kerberos се използва от много години в мрежите с UNIX. Microsoft включи поддръжка на Kerberos в Windows 2000, а проверените връзки на домейна Active Directory са базирани на автентикация Kerberos.

Перспективни технологии за идентификация и автентикация

Идентификацията и автентикацията са важни фактори за сигурността, когато корпоративните мрежи станат по-големи и трябва да поддържат хиляди потребители. Установяването на самоличността на потребител, който се опитва да влезе в мрежата или да осъществи достъп до ресурси на компютъра, е основата на плана за силна система за сигурност.

Независимо от интелигентността на технологиите на криптиране на паролите, проблемът при метода с потребителско име/парола е възможността на неоторизирана страна, която е разкрила и използва пълномощията (акредитивите) на легитимен потребител. Технологиите на разширена идентификация и автентикация като следващите се опитват да предотвратят това, като базират идентификацията на фактори, които не могат да бъдат фалшифицирани:

- Смарт карти
- Биометрика, включително разпознаване на пръстови отпечатъци, сканиране на ретината и разпознаване на ириса на окото и верификация на гласа

Макар че тези технологии още не се срещат масово в работното пространство извън държавните агенции, в следващото десетилетие можем да очакваме методите на разширената верификация да станат масово явление и постоянно да нараства тяхната важност за мрежовите администратори, които трябва да са запознати с тяхното реализиране. Всяка от тези технологии е описана в следващите секции.

Смарт карти

Смарт картите са устройства за автентикация, които наподобяват кредитни карти и съхраняват такава информация, каквато са публичните/частните ключове и пароли. Технологията на съхраняване може да бъде проста, например магнитна ивица или по-сложна, като интегрална схема, която се вгражда в картата и функционира подобно на миниатюрен компютър.

ЗАБЕЛЕЖКА Когато картите се разглеждат в контекста на сигурността на мрежите, терминът означава устройство за идентификация и автентикация, което съхранява пълномощията, които позволяват на потребителя да осъществява достъп до системата. Терминът „смарт карта" се използва също в по-общ смисъл за означаване на всяка пластична карта, която съхранява информация на чип или магнитна ивица. Такива карти са кредитните и дебитни карти, картите с медицинска информация и др.

Някои операционни системи, например Windows 2000, имат вградена поддръжка на смарт карти. Ако не работите под операционна система, която има вградена поддръжка, може да се наложи да използвате отделен софтуер за използване на технологиите на смарт картите.

Смарт картите се използват за достъп до компютъра през място в хардуера, наречено *четец на смарт карти*. Смарт картата осигурява допълнителна сигурност, защото потребителят трябва да бъде притежател на физическата карта. Смарт картите могат да бъдат използвани на мястото на – или за по-голяма сигурност, в допълнение към – физически въвежданите пълномощия на потребителя.

В среда с висока сигурност, картата сама по себе си не разрешава достъпа; потребителят трябва да вкара картата в четеца и да въведе правилните логически пълномощия преди да му бъде даден достъп. Това означава, че потенциалният нарушител, който намери паролата на потребителя, пак няма да може да влезе в мрежата без да притежава картата; по подобен начин някой, който намери или открадне картата, не може да получи достъп без да знае правилната парола.

Вариант на смарт картите е устройството *1-key* на Rainbow Technologies. Това е малко устройство, което се поставя на клавиатурата и което комуникира по USB порт вместо да изисква специален хардуер, като четеца.

Биометрика

Все пак е възможно нарушителят да научи паролата и да придобие съответната смарт карта. За да противодейства на тази възможност, започва въвеждането на такива технологии, като разпознаване на пръстовите отпечатъци, сканиране на ретината и верификация на гласа, които представляват стъпка напред в сигурността. Тези технологии са познати като *биометрика,* което е част от биологичната статистика.

Биометриката върши работа, защото статистическата вероятност двама души да имат едни и същи пръстови отпечатъци (или шарки на ретината или тембър на гласа) е толкова малка, че тези технологии се приемат в съда в много държави като доказателство при криминални процеси. Технологиите за биометрична идентификация могат да осигурят положителна идентификация на потребител на базата на биологичните характеристики.

В следващите секции ще опишем как работят различните биометрични методи.

Разпознаване на пръстови отпечатъци

Системата за разпознаване на пръстови отпечатъци често работи съвместно със системата за сигурност, базирана върху карти. Пръстовите отпечатъци на потребителите се снемат и се въвеждат в базата данни, и когато даден потребител иска достъп до компютъра, трябва да постави пръста си (или най-често палеца, макар че някои системи използват цялата длан) върху екрана на четеца. Въве-

деното графично изображение през четеца се сравнява с отпечатъците в базата данни и в зависимост от това се дава или забранява достъп.

Достъпни са различни софтуерни и хардуерни системи за реализиране на автентикация с пръстови отпечатъци. Такива системи са VeriPrint и U.are.U, и двете предлагани от FingerSec Corporation.

Сканиране на ретината и разпознаване на ириса

Друго средство за идентифициране на лица, базирани на техни уникални биологични характеристики, е *сканирането на ретината*. При тази технология светлинен източник с ниска интензивност се използва за сканиране на шарките на ретината, която представлява тънка мембрана, която покрива вътрешната очна ябълка.

Върху характеристиките на човешкото око е базирана и технологията на разпознаване на ириса. Тази технология включва компютърен анализ на шарките в ириса на окото, който представлява пигментирана кръгла мембрана, придаваща цвета на очите. Тези шарки се приемат за по-уникални от пръстовите отпечатъци или ДНК. Дори идентични близнаци имат различни шарки на ириса.

Верификация на гласа

Верификацията на гласа работи на принципа, че тембърът на човешкия глас е уникален за всеки индивид и може да бъде използван за идентифициране на говорещия.

ЗАБЕЛЕЖКА Верификацията на гласа понякога се бърка с *разпознаването на гласа*. Първото се използва за проверка на самоличността на говорещия. Второто не идентифицира говорещия, а разпознава изговаряните думи и с помощта на компютърен софтуер за разпознаване на глас ги транслира под формата на думи на екрана.

Най-общо от потребителя се изисква да запише гласа си, изговаряйки парола или фраза, която се съхранява в базата данни. За да влезе в системата, потребителят изговаря същата дума или фраза, след което мострите се сравняват. Оценяват се такива фактори, като височина, тон и интонация на гласа. Технологията на верификация на глас не се счита за толкова точна като сканирането на ретината, сканирането на ириса и разпознаването на пръстови отпечатъци. Верификацията на глас се използва най-често в ситуации, в които самоличността трябва да бъде проверена по телефонна линия.

Бъдещето на биометриката

В някои части на света, като Австралия, Южна Африка, Южна Америка и Европа технологиите за биометрично разпознаване и автентикация навлизат бързо в практиката. В САЩ тези технологии се реализират по-бавно, вероятно поради проблеми, свързани с конфиденциалността или поради пазарни фактори.

Когато технологиите станат по-прецизни и по-малко натрапчиви и започне да се отделя по-голямо внимание на проблеми като кражба на самоличност, вероятно използването на биометрика ще нарасне и ще стане често явление в мрежите на бъдещето.

Разработка на политики на сигурност

Постоянно се появяват нови технологии за сигурност. За да разработите добър план на сигурността за мрежата, трябва да знаете с какво разполагате. Също така трябва да можете да определите нивото на сигурност, което е необходимо или желателно за вашата ситуация.

ЗАБЕЛЕЖКА Специалистите по биометрика правят разлика между разпознаването и автентикацията. Автентикацията се разглежда като доброволна дейност, в която потребителят сам предоставя име или идентификационен номер, заедно с биометрични входни данни, като пръстов отпечатък, обикновено с цел получаване на достъп до дадена система. Биометричните данни се сравняват с предварително съхранени такива, които се знае, че принадлежат на потребителя. Сравнението се използва за удостоверяване на самоличността на потребителя и ако удостоверяването успее, се предоставя достъп. При разпознаването системата получава само биометрични входни данни (примерен глас, сканирана ретина или пръстов отпечатък) и след това трябва да търси в нейната база данни и да намери съответствие. Например разпознаването се използва, когато съдебните експерти се опитват да идентифицират пръстов отпечатък, оставен на мястото на престъпление. За да направят идентификацията, експертите може да потърсят съвпадение в такава база данни, каквато е Automated Fingerprint Identification System (AFIS) на ФБР.

Политиките на сигурност трябва да бъдат продукт на общите усилия на целия екип. При тяхното разработване трябва да бъде потърсено съдействието на техническия персонал, ръководството и на представителен брой потребители. За да бъде успешна, една политика на сигурност трябва има поддръжката на мениджърите на организацията и на потребителите. Бюджетните и философските съображения трябва да бъдат балансирани добре с конфиденциалността на данните в мрежата и с отклоненията, ако бъде допуснато компрометиране.

Политиките на сигурност трябва постоянно да се променят и да бъдат преразглеждани и преоценявани периодично при промяна на обстоятелствата. Първата стъпка от създаването на политики е извършването на подробен анализ на сигурността. Трябва да определите какви мерки за сигурност се прилагат в момента, дали те постигат тяхната цел и кои от тях трябва да бъдат премахнати, запазени или заменени.

В следващите секции ще разгледаме следните важни фактори, с които трябва да се съобразявате, когато разработвате политики:

- Политики на приемливо използване
- Политики на премахван
- Рейтинги на правителствена сигурност
- Одитинг на сигурността и откриване на нарушения
- Защитни стени и проксита
- Сигурност чрез множество протоколи
- Физическа сигурност

ЗАБЕЛЕЖКА Другите страни имат подобни системи за рейтинг на сигурност. Такива са Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) в Канада, Australian Information Security Evaluation Programme (AISEP) в Австралия и Information Technology Security Evaluation Criteria (ITSEC) в Западна Европа.

Таблица 14-1 съдържа списък на различни операционни системи и техните рейтинги на сигурност.

Таблица 14-1 *NSA рейтинги на сигурност за различни операционни системи*

Операционна система	Производител	NSA сертификация
UNIX XTS-200 и 300	Wang Government Svcs	Оранжева книга B3
UNIX Trusted Xenix 3 и 4	Trusted Information Systems	Оранжева книга B2
UNIX HP-UX 8.04 и 9.0.9	Hewlett Packard	Оранжева книга B1
UNIX UNICOS 8.0.2	Cray Research	Червена книга B1
UNIX RS/6000	IBM	Оранжева книга C2
Windows NT 3.5/SP3 и Windows NT 4.0	Microsoft	Оранжева книга C2
NetWare 4 и 4.11	Novell	Червена книга C2

Само инсталирането на зададената операционна система не гарантира, че отговаряте на показаните критерии за сертифициране на сигурността. Съществуват и други спецификации, като свързването на мрежата и разрешените възможности на операционната система, които също трябва да бъдат взети предвид при общата оценка. Всъщност рейтингът на сигурността не се дава само на операционната система, а на цялата хардуерна и софтуерна конфигурация.

Одитинг на сигурността и откриване на нарушения

Едно изискване за рейтинга на сигурност C2 е възможността за одитинг (проверка) на събитията на сигурността и действията, извършвани от отделните потребители. *Одитингът* е процес на проследяване на действията на потребителите и на системата. Например одитингът включва наблюдение на достъпа до файловете, определяне кога и от кого е осъществен този достъп. Одитингът може да включва информация за това, кой е влязъл или излязъл от системата, кой е осъществявал достъп до обекти и кой е упражнявал потребителски права.

Операционни системи като Windows NT и Windows 2000 имат вграден одитинг, който може да бъде конфигуриран за всеки ресурс или потребител поотделно. Събитията на сигурността не само че биват проследявани, но също се записват във файл-дневник за по-лесното им преглеждане. До дневниците на сигурността трябва да имат достъп само администраторите.

Пасивно откриване

Одитингът на сигурността се означава като *пасивна форма* на откриване на нарушители. Макар че събитията, засягащи сигурността, се записват във файл-дневник, администраторът първо трябва да се усъмни, че има нарушение, и след това да провери файла-дневник, за да определи точния характер на пробива. Примери на програми за пасивно откриване са Tripwire (for UNIX) и вградената възможност за одитинг на сигурността на Windows NT и Windows 2000.

Активно откриване

В работна среда на мрежа с конфиденциални данни не трябва да се разчита само на пасивното отриване на нарушения. Планът на сигурността трябва да включва една или повече форми на *активно откриване*. При активното откриване се използва софтуер, който непрекъснато сканира мрежата за признаци на нарушения, а някои програми дори предупреждават администратора и изключват връзката на подозрителната секция. Примери на такива софтуерни пакети са SATAN (това злокобно име идва от Security Administrator's Tool for Analyzing Networks) и NetRanger.

Беше издадена и обновена версия на SATAN. Тя има по-приятно име – Security Administrator's Integrated Network Tool (SAINT). SAINT може да открие допълнителни уязвими места и е достъпна в лесната за използване версия, наречена WebSaint, която позволява на администраторите да проверяват уязвимите места на системата по Интернет.

Защитни стени и проксита

Засилените мерки за сигурност на периметъра е друго важно съображение при създаване на политики на сигурност. *Защитните стени (firewalls)* и *проксита* могат да бъдат използвани за създаване на бариера между локалната вътрешна мрежа и връзката към външния свят. Тази област може да бъде инсталирана в нейна собствена подмрежа и понякога бива означавана като *демилитаризирана зона (DMZ)* или *прикрита подмрежа (screened subnet)*. Вижте Фигура 14-6.

Фигура 14-6 *В демилитаризираната зона между вътрешната и външната мрежа могат да бъдат конфигурирани защитни стени и проксита.*

Защитната стена може да бъде базирана на хардуер или на софтуер. Тя осигурява средства за филтриране на входящите и изходящите пакети и определя (на

базата на политики, зададени от администраторите на мрежата) дали да разрешава преминаването на пакети до адреса на местоназначението. Защитната стена обикновено се намира на *шлюза* (*gateway*) на мрежата, който представлява точката, в която мрежата се свързва към друга мрежа.

Защитните стени извършват три базови типа филтриране:

- Филтриране на пакети
- Филтриране на вериги
- Филтриране на приложения

При *филтрирането на пакети* пакетите от данни се филтрират на базата на информацията в IP, TCP/UDP и ICMP хедърите. При филтрирането на пакети може да разрешите или блокирате конкретни IP адреси или номера на портове. *Филтрирането на вериги* е базирано на текущата връзка. Ако даден пакет не е част от установена връзка, той няма да бъде пропуснат през защитната стена. Накрая *филтрирането на приложения* филтрира в зависимост от протоколите, използвани за конкретни IP приложения. Например могат да бъдат блокирани само Java аплети или скриптове на Visual Basic.

Хардуерно базираните защитни стени понякога се наричат „черни кутии". Те представляват специализирани компютри, които изпълняват собствени нестандартни операционни системи (или в някои случаи UNIX). Те функционират само като защитна стена и затова са по-бързи и по-стабилни от компютър, който изпълнява софтуер за защитна стена, но едновременно с това осигурява и други функции.

Прокси сървърите работят като „посредници" в мрежата, като изпълняват функции, подобни на защитни стени. Компютрите във вътрешната мрежа комуникират с проксито, което след това комуникира „от тяхно име" с компютрите от външната мрежа (вижте Фигура 14-7).

Фигура 14-7 *Прокси сървърът действа като „посредник" между вътрешната и външната мрежи.*

Прокси сървърите осигуряват също услуги, като *реверсно прокси* и *реверсно хостване*. Реверсното прокси позволява даден прокси сървър да пренасочва външни HTTP заявки само към една специално предназначена за целта машина. Това осигурява сигурност на достъпа до вътрешен Web сървър, без излагане на

сървъра пред външната мрежа. Реверсното хостване позволява на прокси сървъра да пренасочва HTTP заявки към повече от един Web сървър, като асоциира няколко сървъра към един логически адрес (вижте Фигура 14-8). Прокситата осигуряват също кеширане на Web страници за подобряване на производителността в Web.

Фигура 14-8 *Реверсното хостване позволява на прокси сървъра да пренасочва HTTP заявките към множество Web сървъри.*

Маршрутизаторите и Layer 3 суичовете могат да бъдат конфигурирани със *списъци за контрол на достъпа (ACL)*, които забраняват на конкретни машини да използват маршрутизатора или разрешават комуникация само в една посока. В този случай маршрутизаторът играе ролята на защитна стена.

Маршрутизатори с конфигурирани ACL списъци могат да бъдат използвани като „първа линия на отбраната" за вашата мрежа. Те често се използват за защита от намеса в софтуерни защитни стени.

ЗАБЕЛЕЖКА ACL списъците, използвани от маршрутизатора, разрешават или забраняват достъпа на базата на такива фактори, като IP адреси. Това означава, че спуфнат (подправен) IP адрес може да разбие защитната стена на маршрутизатора.

Сигурност чрез множество протоколи

Политиката на сигурност в мрежата трябва също да определя кои протоколи са разрешени или задължителни. Можете да реализирате сигурност за вътрешната мрежа с помощта на протоколен стек, различен от TCP/IP, или в самата LAN, или в подмрежата на демилитаризираната зона (DMZ), която я отделя от външната мрежа.

Ако използвате IPX/SPX като мрежов/транспортен протокол в локалната мрежа вместо да използвате TCP/IP, IP-базираните атаки от Интернет не могат да проникнат в локалната мрежа. Просто конфигурирате маршрутизатора да използва TCP/IP от страната на неговата връзка към Интернет и IPX/SPX от страната на връзката му към локалната мрежа. Ако ви е необходим TCP/IP за комуникация между вътрешни компютри, можете да го използвате в LAN, но трябва

да настроите DMZ, която използва IPX/SPX между локалната мрежа и Интернет.

Физическа сигурност

Политиката на мрежова сигурност трябва да контролира *физическия достъп* до компонентите на мрежата. това е важен, но често пренебрегван фактор при разработване на ефективен план на сигурност. Трябва да определите степента на директен физически достъп, който служителите, предприемачите, клиентите и обществеността ще имат до работните станции, сървърите, кабела или друга преносна среда, маршрутизаторите, суичовете и другите физически компоненти.

В среда с висока степен на сигурност сървърите и устройствата за връзка трябва да се пазят зад заключени врати. Работните станции, които се намират в незащитени области трябва да имат софтуерни средства за контрол, които не допускат достъп до конфиденциални данни в мрежата. Кабелът трябва да бъде защитен със здрави изолационни тръби, без да се полага открито на пода или на тавана. Кабелите с усукана двойка и коаксиалните кабели са особено лесни за разклоняване, но прихващане на данни е възможно също по оптични кабели с използване на оптичен разделител (сплитер). Тъй като нивото на сигнала се влияе при създаване на разклонител по този начин, наблюдателният мрежов администратор може да открие разклонението с помощта на рефлектометър (optical time domain reflectometer – OTDR). Въпреки това експертите могат да вмъкнат разклонител, който не може лесно да бъде открит от OTDR.

В много организации се полагат големи усилия за ограничаване на достъпа на служителите и обществеността до компютърното оборудване – и след това цялото оборудване се оставя широко отворено всяка нощ, когато идва обслужващият персонал за почистване. Ако сигурността е важен въпрос за вашата мрежа, персоналът по почистването и поддръжката трябва да бъде под наблюдението на оторизирано лице, когато се почистват стаите, съдържащи мрежово оборудване.

Защита и възстановяване от сривове

Външните и вътрешните нарушители не са единствената заплаха за мрежата и данните в нея. Също така могат да възникнат хардуерни повреди, природни бедствия и технически грешки, които също довеждат до опустошителни загуби на важни файлове. Ето защо мерките за защита и възстановяване от сривове са важна част от всяка производствена мрежа.

Защитата срещу катастрофални загуби на данни и възстановяването на данните след такива сривове включва няколко линии на защита:

- Аварийно захранване
- Архивиране на данните
- Отказоустойчивост при дисковете
- Отказоустойчивост на ниво сървъри (клъстериране)

Ще разгледаме накратко основните принципи на всяка от тези защити и как всяка от тях може да бъде реализирана в мрежата.

Аварийно захранване

Много компании са се сблъсквали на практика с изгубването на ценни данни при внезапни летни гръмотевични бури, предизвикващи краткотрайно прекъсване на електрозахранването и презареждане на компютрите, или когато авария в елекроснабдителната компания създава пренапрежения с висок волтаж. Всички тези инциденти са още по-страшни поради това, че не могат да бъдат предвиждани.

Всяка година се изгубват или унищожават голямо количество данни вследствие електрически удари или повреди. В тази секция ще разгледаме начините за защита на мрежата от опасни колебания на напрежението с помощта на предпазители от пренапрежения, непрекъсваеми захранващи устройства (UPS) и генератори на напрежение.

Предпазители от пренапрежение

Колебанието на напрежението или пренапрежението може да повреди хардуера на компютъра и да направи данните нечетими. Добрият предпазител от пренапрежение и стабилизатор са абсолютната минимална защита, която трябва да осигурите за всеки важен компютър в мрежата, включително за всички сървъри и критично важни работни станции.

ЗАБЕЛЕЖКА Предпазителите от пренапрежения представляват евтини защитни устройства, но тяхната ефективност е ограничена само до повишаванията на напрежението. Те не защитават системите, ако напрежението падне или изобщо бъде изключено. Много такива стабилизатори не могат да издържат на множество пренапрежения – след като настъпи пренапрежение и уредът свърши своята работа, може да се наложи да бъде заменен. За нещастие, не винаги е възможно да се открие кога е станало това, затова може да попаднете в ситуация, в която вярвате, че имате предпазител от пренапрежение, а фактически той вече не действа.

UPS

Формата на защитено електрозахранване, която е по-добра, но по-скъпа от предпазителя от пренапрежение, е непрекъсваемото захранващо устройство (UPS). UPS представлява тип резервна батерия, която осигурява ограничено количество съхранена електроенергия, с помощта на която системите могат да продължат да работят след прекъсване на основното електрозахранване.

UPS *не* е предназначено за осигуряване на захранване за продължаване на използването на компютърните системи. Неговата цел е да осигури непрекъсвано захранване за няколко минути, давайки ви време да затворите отворените файлове и програми, и да изключите компютрите нормално. Типичният UPS осигурява захранване за 5 до 20 минути, след като се превключи в режим на захранване от батерията.

UPS устройството се включва в контакта на стената, а компютърът се включват в UPS. Много UPS устройства имат множество контакти, така че в един UPS да могат да бъдат включвани няколко системи. В нормален режим устройството се зарежда непрекъснато. При прекъсване на електрозахранването UPS устройството усеща това и често може да бъде конфигурирано да уведомява потребителите, че не приема входящо електрозахранване. Уведомяването може да бъде под формата на аудиосигнал (например писукане) или да бъде използван

софтуер за изпращане на съобщение до административните акаунти в мрежата. Същият софтуер може да бъде конфигуриран да стартира автоматично изключване на свързания компютър, когато UPS премине в режим на батерия.

Всички важни системи в мрежата трябва да бъдат свързани към UPS устройства. Цената на добра UPS система е само част от стойността на нов компютър и си заслужава цената, която може да се окаже много по-малка от тази на изгубените данни (които може дори да бъдат безценни).

ЗАБЕЛЕЖКА Макар че литературата за UPS често използва терминологията „режим на батерия", реално компютърното оборудване постоянно работи на захранване от батерията на UPS. Батерията постоянно се зарежда, докато има електрозахранване от контакта на стената. Ето защо, когато UPS устройството „превключва режимите" няма прекъсване в подаването на електрозахранване към компютрите.

Генератори

Следващата стъпка в защитата на захранването е генераторът на напрежение. Това устройство реално създава електричество с помощта на двигател, захранван с бензин, керосин или друго гориво. Генераторът ви позволява да продължите да използвате електрооборудването (включително компютрите и UPS устройствата) за цялата продължителност на повредата в електрозахранването.

Генераторите са скъпи и тяхната цена не винаги може да бъде компенсирана, освен в случаите, когато електрозахранването е спряно за дълъг период от време, или при работа с оборудване, което се нужда е от постоянно захранване, защото изпълнява животоподдържащи функции или в други спешни случаи.

Архивиране на данните

Независимо от вашите усилия да го предотвратите, винаги е възможно да се случи нещо такова: да настъпи отказ на твърд диск, пожар или наводнение да унищожат сървъра, или злобен вирус да форматира устройството и да направи вашите данни нечетими. Просто данните ще бъдат изгубени. Но ако сте реализирали редовно и изчерпателно архивиране на данните с помощта на програма за архивиране, те не са изгубени завинаги.

Създаването на план за архивиране включва отговори на следните въпроси:

- Кои файлове трябва да архивирате?
- Кога трябва да ги архивирате?
- Как трябва да ги архивирате?
- Защо трябва да ги архивирате?

Отговорът на четвъртия въпрос трябва да бъде ясен от самата формулировка; вашият план за архивиране може да отчита разликата между катастрофална загуба на данни, време и пари, и малкото неудобство от отделянето на няколко часа за възстановяване на файловете от архива до тяхното първоначално състояние. Да видим отговорите на другите три въпроса и как те се вместват във вашия план.

Какво да архивираме

Първата стъпка е да решите какво трябва да бъде архивирано и да зададете приоритети на файловете, които трябва да бъдат архивирани. Идеалната ситуация, разбира се, е да се архивира всичко. Но това не винаги е възможно поради ограничено време и ограничен капацитет на архивния носител.

Не винаги е важно да се архивират операционната система и файловете на приложенията, защото те могат да бъдат инсталирани отново от инсталационните дискове. Много по-важно е да бъдат архивирани оригиналните данни; това са документите от текстообработващите програми, електронните таблици и други данни, създадени в различни потребителски приложения. Творческата работа като графика или писане на оригинални литературни творби трябва да има голям приоритет, защото може да е невъзможно да бъдат пресъздадени точно по същия начин. Разбира се, критично важни данни, като финансова информация, на която разчитат мениджърите в своята работа, стои на първо място в списъка „какво да архивирам".

Вашите политики относно това, какво да се архивира, трябва постоянно да бъдат преразглеждани. Данните, които трябва да бъдат архивирани, трябва да бъдат съхранявани в едно централно местоположение, например на зададено устройство или на сървъра. Ако важните данни са разпръснати из мрежата на отделни твърди дискове, става много трудно да се гарантира, че нещо няма да бъде пропуснато по време на цикъла на архивиране.

Кога да архивираме

Трябва да направите разписание за периодично, *регулярно* архивиране на важни данни. Колко често ще архивирате зависи от това, колко данни можете да си позволите да изгубите: данните, натрупани за един ден или за една седмица.

Архивирането може да бъде извършвано по график след работните часове, така че да не влияе върху производителността на мрежата. Както беше разгледано в последната секция, повечето добър софтуер за архивиране ви позволява да изпълнявате архивиране по график, така че при извършване на архивирането не е нужно да присъства никой.

В повечето случаи графикът за архивиране включва различни типове архивиране. Има три основни типа (макар че някои помощни програми за архивиране ви дават допълнителни възможности за избор):

- **Пълно архивиране** – Всички данни на зададените устройства се архивират независимо от това, дали и кога са архивирани преди, и дали са променени след последното архивиране.
- **Диференциално архивиране** – Архивират се всички файлове, променени след последното *пълно* архивиране.
- **Инкрементално архивиране** – Архивират се всички файлове, променени след последното архивиране от всеки тип (а не просто след последното пълно архивиране).

Пълното архивиране продължава повече време и заема повече пространство на архивния носител, и поради това е най-скъпо. Също така това е най-простият метод, и ако изпълнявате пълно архивиране всяка нощ, ще бъдете сигурни, че всички архивирани данни са актуални. Също така това е типът архивиране, което е най-лесно за възстановяване.

Диференциалното архивиране спестява време. То се прави съвместно с пълно архивиране. Например можете да правите пълно архивиране един път в седмицата или едни път в месеца, а след това да правите диференциално архивиране всяка нощ между пълните архивирания. За да възстановите данните, трябва да възстановите две ленти (последното пълно архивиране и последното диференциално архивиране), за да гарантирате, че всички данни са най-актуалните. Този метод може да бъде предпочетен, ако имате много голямо количество данни, които трябва да бъдат архивирани, и малко време вечер за извършване на архивиране. Диференциалните архивирания отнемат по-малко време. Освен това пълните архивирания могат да бъдат изпълнявани през уикенда, когато има повече свободно време.

Инкременталните архивирания са най-бързите, но възстановяването е по-сложно и отнема повече време от другите методи. Трябва да възстановите последното пълно архивиране и след това да възстановите инкременталното архивиране за *всеки* ден след последното пълно архивиране.

ЗАБЕЛЕЖКА Как на практика архивиращият софтуер „знае" кои данни са променени след последното архивиране? Включва се *архивния бит* на файла. Този бит представлява атрибут на файла, който е подобен на бита, маркиращ файла като скрит (hidden) или само за четене (read only). Този бит се премахва (т.е. се изтрива), когато файлът се архивира по време на пълното архивиране или инкрементално архивиране. Битът *не* се премахва след диференциално архивиране.

Как да архивираме

Начинът за архивиране включва вземането на множество решения:

- Какъв архивен носител трябва да бъде използван?
- Какъв софтуер за архивиране трябва да бъде използван?
- Кой отговаря за извършването на архивирането?
- Архивирането ръчно ли ще бъде направено или автоматично?

Много години лентата беше предпочитан архивен носител и някои видове софтуер за архивиране (като помощната програма за архивиране, вградена в Windows NT) не поддържат никакъв друг носител. Други програми за архивиране ви позволяват да избирате от различни типове носители – сменяеми дискове като Zip и Jaz, CD-R и CD-RW, DVD и магнито-оптичен диск (MO).

Повечето операционни системи включват помощна програма за архивиране. Windows NT и Windows 2000 включват Windows Backup; NetWare включва SBackup, а UNIX притежава вградената архивираща програма *tar*. Има много програми за архивиране на независими производители, които предлагат по-пълен набор от възможности от този на вградените в операционните системи. ARCserve (Cheyenne), Backup Exec (Seagate) и Norton Backup (Symantec) са примери на популярни програми за архивиране под Windows.

Важно е отговорността за архивирането на критично важни данни да бъде зададена конкретно. Уверете се, че операторът по архивирането има съответните позволения за архивиране на данните на всеки потребител. Не е задължително да давате на лицето позволение да чете файлове, за да му позволите да архивира и даже да възстановява файловете. Също така трябва да имате „резервен ар-

хивен оператор" – някой, който е обучен да поеме отговорността, ако първият оператор по архивирането не може да изпълни своите задължения.

Независимо дали архивирането се изпълнява ръчно или автоматично, жизненоважно е периодичната проверка на целостта на архива. Не чакайте да настъпи истинска катастрофа, която да ви накара да възстановите данните, за да разберете, че вашето лентово устройство не е записвало нищо на лентите. Направете тестово възстановяване, когато *не ви* е нужно такова.

Накрая трябва да правите множество архивирания на данни, които са особено важни. Съхранете поне едно от тези копия някъде извън организацията. Не е добре да държите актуалните архивирани данни в чекмедже на бюрото до сървъра, защото пожар, наводнение или торнадо може да унищожи всичко в стаята. Външните архиви могат да бъдат прибрани у дома или при доверен служител, съхранени в банков сейф на депозит, прехвърляни ежедневно в офиса на друг филиал на организацията или качвани на отдалечен сървър по телефонни линии или по Интернет.

Отказоустойчивост при дисковете

Друг начин за защита на вашите данни от повреда на твърдия диск е да реализирате *отказоустойчивост*. (Отказоустойчивостта означава възможността на дадена система да се възстановява след срив.) Това включва комбиниране на множество физически твърди дискове в един *отказоустойчив пакет*, който може да бъде в една от няколко възможни конфигурации.

Отказоустойчивоста при дисковете се нарича също редундантен масив от независими (или нескъпи) дискове (*redundant array of independent* (inexpensive) *disks* – RAID). Най-често използваните отказоустойчиви конфигурации са следните:

- **Дублиране на диск** или **създаване на огледално копие на диск (RAID level 1)** – За дублиране на диска са необходими два физически твърди диска, за предпочитане с един и същ капацитет. Всички данни от единия диск се дублират на втория. На втория диск има точно дублирано копие на всички файлове и структури. Ако единият диск се повреди, другият може да поеме работата. Това става или автоматично, или може да се наложи да укажете на операционната система къде да намери новия диск. Например в Windows NT това се прави чрез редактиране на файла boot.ini.

- **Дуплексиране на диск (RAID level 1)** – Дуплексирането на диск работи по същия начин като дублирането, с изключение на това, че двете физически устройства се свързват към различни дискови контролери. Това повишава нивото на отказоустойчивост, защото ако контролерът на единия диск се повреди, другият диск продължава да функционира, тъй като се управлява от различен контролер.

- **Лентов запис (страйпинг) с дисково устройство за четност (RAID level 3)** – Този метод за конфигуриране се състои в записване на данните на ленти едновременно на множество еднакви устройства и записване на данните за самите записи върху тези устройства на друго устройство, което е запазено само за тази цел. Това изисква минимум три физически диска (два еднакви диска, на които данните се записват на еднакви ленти, и един за информацията за четност). Ако се повреди диск с данни, данните могат да бъдат регенерирани с помощта на информацията за четност.

- **Лентов запис (страйпинг) с ленти за четност (RAID level 5)** – Лентовият запис с ленти за четност работи по начин, подобен на RAID 3, с изключение на това, че четността (подобно на данните) се записва в ленти, които се променят между дисковете. Нито един диск не е предназначен за четност. И тук са необходими поне три диска, но данните могат да бъдат възстановени при повреда на *който и да е* от тях.

ЗАБЕЛЕЖКА Какво представлява четността? Компютърният речник на Microsoft Press дефинира термина като „процедура за проверка за грешки, при която броят на единиците трябва да бъде винаги един и същ – четен или нечетен – за всяка група от битове". В контекста на отказоустойчивостта при дисковете, можете да възстановите липсващите данни на повредения диск, като комбинирате информацията за честността с данните на устройствата, които все още продължават да работят.

Други, по-малко използвани RAID нива на отказоустойчивост са следните:

- **RAID 2** – Прилича на RAID 3 по това, че данните се записват на ленти върху множество устройства и едно устройство се запазва само за информация за четност. Единствената разлика е, че данните се разделят на ленти по битове; при RAID 3 се записват в ленти по байтове.
- **RAID 4** – Това ниво е подобно на RAID 2 и 3, с изключение на това, че данните се записват на ленти по блокове, вместо по битове или байтове.

RAID 0 се използва доста често за увеличаване на производителността при четене и записване на данни, но това не е метод с отказоустойчивост. RAID 2 разделя данните на множество дискове на блокове, но не включва информация за четност; затова ако един от дисковете се повреди, няма начин данните да бъдат възстановени.

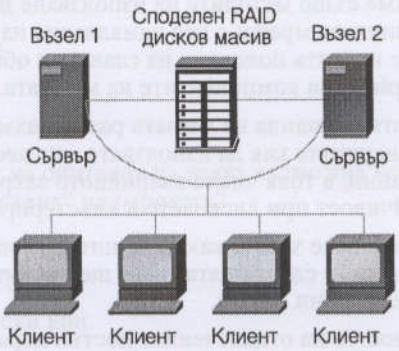
RAID може да бъде реализиран или софтуерно, или хардуерно. Макар че хардуерно базираният RAID е по-бърз и като цяло по-надежден, той е и по-скъп. Някои сървърни операционни системи, като Windows NT и Windows 2000 Server, имат вградена поддръжка за софтуерен RAID.

Технологии за клъстериране

В основата на всички методи за отказоустойчивост стои *редундантността (излишъкът)*. Резервното захранване включва необходимостта от редундантни източници на електрозахранване: контакта на стената и батерията на UPS устройството. Архивирането на данните включва създаване на редундантни копия на важни файлове на архивния носител. Отказоустойчивостта при дисковете включва записване на данните върху множество редундантни дискове. Клъстерирането представлява крайна форма на редундантност.

Клъстериране най-общо означава групиране на сървъри в *клъстери*. При клъстерите група от сървъри се разглежда като един сървър в мрежата. Ако един от сървърите излезе от строя, работата се поема от друг сървър в клъстера. Това прехвърляне е прозрачно за потребителите. Вижте Фигура 14-9.

Фигура 14-9 *Клъстерирането на сървъри е скъп, но високо ефективен начин за осигуряване на отказоустойчивост.*



Поддръжката на клъстериране е вградена в такива операционни системи като Windows 2000 Advanced Server, а отделен софтуер за клъстериране е достъпен за конфигуриране на сървъри, които работят под други операционни системи. Клъстерирането осигурява отказоустойчивост наред с други предимства, каквото е *балансирането на натоварването*.

Обобщение

Нито една отделна мярка за сигурност няма да защити изцяло вашата мрежа. Ефективната сигурност се постига чрез използване на план за сигурност, който обединява множество практики, политики и технологии на сигурност.

В тази глава разгледахме различни начини за защита на мрежата и данните, които се намират в нея или пътуват по преносната ѝ среда. Първо разгледахме много обширната тема за мрежовата сигурност, а след това методите за защита и възстановяване от повреди.

Научихте как можете да удовлетворите нуждите от сигурност във вашата мрежа и какво представляват външните пробиви в сигурността, като неоторизираното използване на пароли или ключове, DoS атаките (включително Ping наводненията, смърф атаките, Ping на смъртта и SYN атаките), IP спуфингът, компютърните вируси и червеи, и злонамерените програми, наречени троянски коне.

След това разгледахме вътрешните заплахи, които могат да бъдат разделени на промишлен шпионаж, вътрешни политики, недоволни служители или бивши служители и случайни пробиви на сигурността.

Направихме общ преглед на криптографските концепции и на начините за кодиране и декодиране на текст с цел осуетяване на опитите на неоторизирани нарушители. Научихте се да разграничавате симетричното криптиране със секретен ключ и асиметричното криптиране с публичен/частен ключ. Също така разгледахме автентикацията, която представлява процес на определяне дали дадено съобщение наистина е от изпращача, който претендира за това.

Научихте за правителствените рейтинги на сигурност и за начините за откриване на информация за текущите рейтинги на популярни операционни системи, след което разгледахме одитинга на сигурността и откриването на нарушения. После се спряхме на защитните стени и прокситата, а също и на това, как те

могат да създадат демилитаризирана зона между вътрешната мрежа и Интернет (или друга външна мрежа), за да защитят ресурсите в локалната мрежа.

Разгледахме също методите на използване на различни протоколи във вътрешната и външната мрежи с цел намаляване на риска от проникване отвън. Завършихме първата половина на главата с обобщение на важността на физическата сигурност за компонентите на мрежата.

Във втората половина на главата разгледахме защитата и възстановяването от повреди; научихте как да използвате множество линии на отбрана срещу загубване на данни, в това число аварийното захранване, архивирането на данни, отказоустойчивост при дисковете и клъстерирането.

Сега, когато вече знаете как да защитите вашата мрежа до известна степен от външния свят, в следващата глава ще научите как да се свържете към външния свят по телефонни линии.

Популярността на отдалеченият достъп нараства ежедневно, защото все повече служители работят като *телекомютъри*, осъществявайки достъп до мрежата на организацията от вкъщи или остават свързани към корпоративната мрежа, докато са на път. От Глава 15, „Отдалечен достъп", ще научите за устройствата за отдалечен достъп и за начините за инсталиране на клиенти и сървъри с отдалечен достъп. Също така ще разгледаме специалните съображения за сигурност, налагани от установяването на dialup конекции към мрежата.

Допълнителни източници

За повече информация относно законите на САЩ, регулиращи експорта на технологии за криптиране, вижте www.bxa.doc.gov/Encryption.

Един чудесен общ преглед на IPSec се намира на Web сайта на Cisco на адрес www.cisco.com/warp/public/cc/techno/protocol/ipsecur/prodlit/ipsec_ov.htm.

Полезна книга, дискутираща много от аспектите по създаването на сигурна мрежа, е *Designing Network Security*, от Merike Kaeo. Публикувана е от Cisco Press.

Един добър ресурс за информация относно сигурността на електронната поща е www.emailtoday.com/emailtoday/dir/email_security.htm.

Няколко полезни връзки към Web сайтове, които представят услуги за сертифициране и други технологии за криптиране, могат да бъдат намерени на www.security-online.com/info/certificates.html.

Опростено обяснение на Kerberos може да бъде разгледано онлайн на адрес www.isi.edu/gost/brian/security/kerberos.html.

За повече информация относно разработката на политики на сигурност в мрежата, вижте www.homex.s-one.net.sg/member/itsecurity/netsec1.htm.

NCSC/NSA Security сертификати са достъпни в Web на адрес www.radium.ncsc.mil/tpep/epl.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Какво е името на числото или шифъра, използван от системата за верификация на интегритета на комуникацията?

a Парола
b Криптография
c Ключ
d Автентикация

2 Какъв е процесът на опитване на всяка възможна комбинация от букви и цифри с цел „кракване" на паролата?

a Декриптиране
b Атака с груба сила
c Атака с троянски кон
d Nuke атака

3 Какво е името на изпращане на потоп от ICMP съобщения с цел забиване или изключване на сървър от мрежата?

a SYN атака
b Червей
c Ping на смъртта
d Ping наводнение

4 Кои от следните представляват често срещани вътрешни заплахи за сигурността на мрежата? (Посочете всички верни отговори.)

a Корпоративен шпионаж
b Случайни пробиви
c IP спуфинг
d Проксита

5 Кое от следните е истина за добра политика на пароли в среда с висока сигурност?

a Позволява на потребителите да създават и използват паролите, които им е най-лесно да запомнят.
b Изисква паролите да бъдат с минимална дължина, например шест знака.
c Забранява използването на числа или символи в паролата.
d Забранява на потребителите да променят своите пароли.

6 Кое от следните описва подразбиращите се позволения на новосъздаден споделен ресурс в Windows 2000 server?

a По подразбиране никой няма позволение за достъп до споделения ресурс.
b По подразбиране всеки има позволение за достъп само за четене до споделения ресурс.
c По подразбиране всеки има позволение за пълен контрол над споделения ресурс.

d По подразбиране членовете на групата на администраторите имат достъп само за четене до споделения ресурс.

7 Кое от следните най-добре описва криптирането на файлове?

a Криптирането на файлове защитава данните, съхранени на твърдия диск.

b Криптирането на файлове защитава данните, изпратени по мрежата.

c Криптирането на файлове защитава данните и докато са на диска, и когато се предават по мрежата.

d Криптирането на файлове е достъпно само чрез независим софтуер.

8 В контекста на сигурността на мрежите, какво означава ESP?

a Extra-Sensitive Packets

b Extended Security Protocol

c Encapsulating Security Payload

d External Security Properties

9 Кой от следните методи за криптиране използва един и същ ключ за криптиране и декриптиране на данните?

a Асиметрично криптиране

b Криптиране с публичен ключ

c Криптиране с частен/публичен ключ

d Криптиране със секретен ключ

10 Какво представлява еднопосочното математическо изчисление, което създава дайджест на съобщение, използван за верификация на автентичността на съобщенията?

a Цифров сертификат

b Хеширащ алгоритъм

c Билет за издаване на билет

d Сканиране на ретината

Глава 15

Отдалечен достъп

В традиционната локална компютърна мрежа (LAN) компютрите се свързват към мрежата по кабел. Но всеки тип кабел има ограничения по отношение на разстоянието, което можете да измине сигналът без значително затихване. Решенията за отдалечен достъп позволяват на потребителите да установяват връзка към мрежата и да изпълняват задачи по такъв начин, както ако са свързани директно по кабел към останалата част от мрежата — дори когато са отдалечени на хиляди километри. В резултат на това отдалеченият компютър става член на локалната мрежа, макар и временно.

При типичната мрежова връзка за отдалечен достъп, осъществявана по телефонна линия с модем (dialup networking), телефонната линия служи за същата функция, както Ethernet кабелът при връзката с директна кабелна връзка, а модемът или друго устройство за отдалечен достъп изпълнява същата основната функция както мрежовата карта. Единствената практическа разлика между отдалечената връзка и кабелната връзка е, че първата по принцип е по-бавна. Една бавна Ethernet връзка има базова скорост на трансфер 10 Mbps; високоскоростните цифрови абонатни линии (DSL) телефонни линии имат средна скорост на трансфер 1,5 Mbps.

Отдалеченият достъп до мрежата може да бъде постигнат също по безжични връзки или по кабелни връзки на кабелните оператори (CATV). В тази глава ще фокусираме върху dialup мрежовите връзки, най-често срещаната форма на отдалечен достъп.

Отдалеченият достъп ви позволява да разширявате мрежата отвъд физическите граници на кабелната мрежа до почти всяка точка на света. Необходим ви е само *сървър за отдалечен достъп*, който се инсталира за приемане на входящите dialup връзки, и *клиент за отдалечен достъп*, който има софтуер, позволяващ му да набира сървъра. Разбира се, и двете системи трябва да имат подходящ хардуер (обикновено модем), свързан към телефонна линия. Освен това компютрите трябва да работят с един и същ протокол.

Повечето модерни операционни системи могат да действат като отдалечени клиенти и отдалечени сървъри. Те могат да действат и по двата начина едновременно, ако има два отделни модема и ако се свържат повече телефонни линии.

В следващите секции ще разгледаме следните важни въпроси, свързани с отдалечения достъп:

- Важността на отдалечения достъп като опция за организиране на мрежа
- Как работи отдалеченият достъп

- Устройства за отдалечено свързване
- Конфигуриране на клиенти и сървъри за отдалечен достъп
- Проблеми на сигурността при отдалечен достъп

Защо да използваме отдалечен достъп?

Отдалеченият достъп става все по-важен с нарастване на мобилността на потребителите на мрежите и с разрастване на бизнеса на организациите до множество места, или отварянето на техните ресурси за избрани външни партньори без поставяне на тези ресурси в Интернет.

Някои популярни приложения на отдалечения достъп са следните:

- Свързване на офиси на филиали
- Осигуряване на служителите средства за свързване към мрежата след фиксираното работно време
- Предоставяне на служителите възможност за телекомуникация – т.е. на възможността да работят вкъщи в част от работното време или на пълно работно време
- Възможност за служителите, които са на път (например пътуващите търговци или ръководителите на бизнес обиколки), да се свързват към корпоративната мрежа
- Осигуряване на достъп до избрани мрежови ресурси за клиентите на компанията или за нейните партньори

Да разгледаме с какво услугите за отдалечен достъп могат да помогнат на организацията при всяко едно от горните решения.

Офиси на филиали

В разширяващата се глобална икономика, дори на малките бизнес организации често се налага да отварят офиси на много места. Ако тези места имат възможност за връзка към мрежата на централния офис, те ще имат лесен достъп до най-актуалната информация и лесно могат да използват общи ресурси.

Когато не е нужен постоянен или чест достъп, или когато той се извършва само на няколко компютъра, dialup връзката може да е достатъчна. В такъв случай в централния офис един от компютрите в мрежата може да бъде настроен като dialup сървър. Потребителите във филиалния офис могат да избират и да установяват връзка към мрежата, когато това е необходимо.

Възможност за връзка след работно време

За много служители в големите организации работният ден продължава в часовете след работа. Служителите често вземат работа за вкъщи. В този аспект за тях може да бъде полезно или необходимо да имат възможност за връзка към мрежата след работно време, за да довършат своята работа.

При връзка с отдалечен достъп служителят може да набира сървъра за отдалечен достъп на организацията и да влиза в мрежата с неговия обикновен потребителски акаунт. Това дава на служителя достъп до всички ресурси, достъпни и на неговия настолен компютър в офиса.

С помощта на терминални услуги служителят може дори да работи на същия десктоп, който използва през деня в офиса. Работата, която е оставена недовършена, може да бъде продължена по-късно без неудобството от прехвърляне на файлове от един компютър на друг чрез дискети.

Приложенията, достъпни на терминалния сървър, могат да бъдат използвани и от вкъщи дори ако служителят не е инсталирал тези приложения на собствения си домашен компютър. Терминалните услуги ще разгледаме по-детайлно в Глава 17, „Мрежи за тънки клиенти".

Телекомютинг

Голям брой служители, в това число творческият персонал, програмистите на софтуер, търговците и административните служители, работят от вкъщи през част от работното си време или през цялото работно време. Тези работници се наричат *телекомютъри*, защото се свързват отдалеч с офиса и остават във връзка през деня чрез електронна поща, чат на живо и дори аудио и видео конфериране.

Телекомютингът е привлекателен за служителите, защото им спестява време за пътуване и други разходи, свързани с работата в офис, например работно облекло, обеди „извън офиса" и транспортни разходи. Това спестява пари също на организацията, защото не се изисква пространство в офиса за служителите телекомютъри.

Dialup достъпът е най-често срещаният начин за свързване на телекомютърите към LAN мрежата на организацията, макар че в някои случаи може би е по-добре да се използва специално предназначена за целта връзка. Ако организацията има много служители телекомютъри, сървърът за отдалечен достъп ще изисква включване на множество модеми (*банка от модеми*), за да могат да бъдат осъществявани множество връзки едновременно. Разбира се, всеки модем изисква своя собствена отделна телефонна линия, както е показано на Фигура 15-1.

Фигура 15-1 *Dialup достъпът от множество клиенти може да бъде осигурен с помощта на банка от модеми.*

ЗАБЕЛЕЖКА Използването на банка от модеми може да изисква инсталиране на COM порт адаптер на отдалечения сървър. Този адаптер позволява на операционната система да разпознава множество модемни портове. Многопортовите карти осигуряват до 128 порта на един отделен ISA или PCI слот.

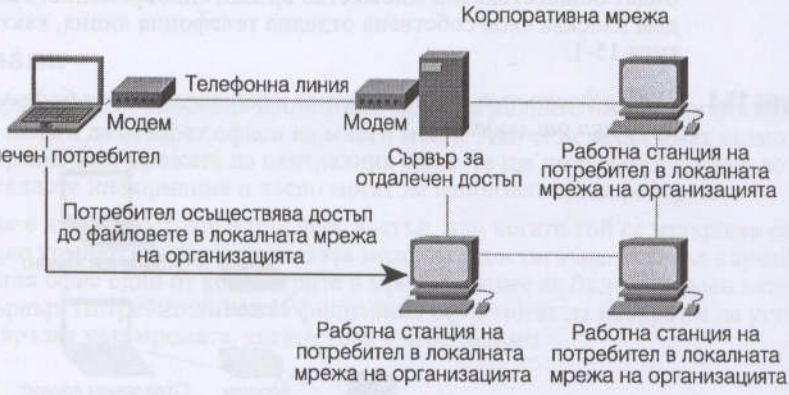
Алтернативна форма на отдалечения достъп, която може да бъде по-ценово ефективна в тази ситуация, е изграждането на виртуална частна мрежа, което е разгледано в Глава 16, „Виртуални частни мрежи“.

Мобилни потребители

Бизнес пътуванията става предпочитана форма на работа, когато организациите започнат да изнасят своите продукти на националния и международния пазар. Търговците, предприемачите, инструкторите, мениджърите от високите нива и други могат да прекарват голяма част от времето си на път. Нуждите от мобилни потребители са подобни на тези на потребителите в извън работно време.

Може да бъде трудно или невъзможно да съхраните всички необходими файлове на лаптоп или нотбук компютър. Също така съществува и заплаха за сигурността, защото лаптопът и неговото съдържание могат да бъдат откраднати физически. По-доброто решение може да бъде мобилният потребител да избира (dial in) LAN мрежата на организацията, където се автентицира неговият потребителски акаунт, и след това да осъществява достъп до данните в мрежата, вместо да копира тези данни на своя собствен твърд диск (вижте Фигура 15-2).

Фигура 15-2 *Мобилният потребител може да влиза в локалната мрежа на компанията, като я избира по телефона, и да осъществява достъп до данните на своя десктоп.*



Осигуряване на достъп за клиенти и партньори

Отдавна утвърдена практика за производителите на хардуер е да осигуряват на своите клиенти възможността да набират сървър и да свалят от него необходимите им софтуерни драйвери. По същия начин производителите на софтуер предоставят обновявания и „кръпки“ за своите програмни продукти.

Концепцията за предоставяне на възможност клиентите (или партньорите – т.е. други компании, с които вашата компания има взаимно изгодно сътрудничест-

во) да избират по телефонните линии корпоративната мрежа и да осъществяват достъп до избрани файлове, непрекъснато нараства по популярност. Но от съображения за сигурност трябва да решите дали искате тези „потребители гости“ да имат достъп до мрежата посредством обикновен акаунт (най-често наричан guest акаунт) или чрез уникално потребителско име и парола. Последният случай увеличава работата на администраторите, но ви позволява да следите кой осъществява достъп до мрежови ресурси и кога и как става това. От друга страна предоставянето на анонимен достъп е опция, подходяща за среда с ниска сигурност, или за такава, в която сървърът за отдалечен достъп е отделен от останалата вътрешна мрежа посредством защитна стена (firewall).

Как работи отдалеченият достъп

Има няколко форми на връзки за отдалечен достъп:

- Най-често използваният тип отдалечен достъп е dialup връзка по аналогова или цифрова телефонна линия.
- *Посветената (dedicated)* връзка представлява връзка от точка до точка, подобно на линия T1, при която от една до друга физическа точка се установява постоянна верига. Обърнете се към Глава 6, „WAN връзки“, за повече информация относно достъпните технологии.

ЗАБЕЛЕЖКА Dialup връзката може да бъде изградена по X.25 мрежа. В този тип мрежа клиентът набира по телефонна линия асемблатор/деасемблатор на пакети (PAD). В Глава 6 ще намерите повече информация относно технологията X.25.

Работата във виртуална частна мрежа е форма на отдалечен достъп, която използва Интернет като преносна среда за изграждане на връзка към частна мрежа. Разбира се, и клиентът на виртуалната частна мрежа (VPN), и самата частна мрежа трябва да бъдат свързани към Интернет.

В следващите секции ще разгледаме следните аспекти на администрирането на отдалечения достъп:

- Протоколи, използвани за отдалечен достъп
- Методи за автентикация при отдалечен достъп
- IP адресът, задаван на отдалечената връзка, която използва TCP/IP
- Обединяване на пропускателната способност за осигуряване на по-бърза връзка
- Управление на степента на използване на пропускателната способност от администратора с цел недопускане на прекомерното ѝ използване

Протоколи, използвани за отдалечен достъп

Отдалеченият клиент и отдалеченият сървър трябва да използват най-малкото един и същ мрежов/транспортен протокол (понякога означаван като *LAN протокол*), например TCP/IP, IPX/SPX, AppleTalk или NetBEUI. Освен това е необходим и протокол за връзка (понякога наричан *WAN протокол*) за изграждане на връзката по телефонната линия или по Интернет от клиентската машина до сървъра.

Протоколите, използвани за изграждане на връзката, са следните:

- Интернет протокол по серийна линия (Serial Line Internet Protocol – SLIP)
- Протокол от точка до точка (Point-to-Point Protocol – PPP)

Ако отдалечената връзка се установява с помощта на VPN, протоколите, използвани за изграждане на връзката, са следните:

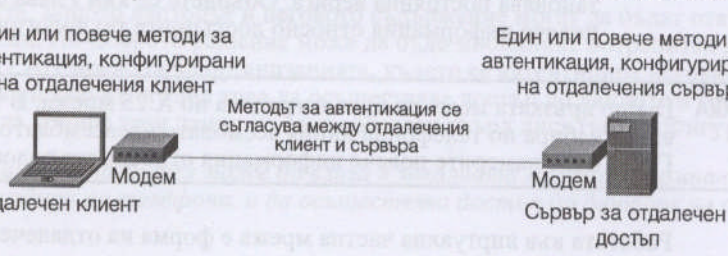
- Тунелен протокол от точка до точка (Point-to-Point Tunneling Protocol – PPTP)
- Тунелен протокол, Слой 2 (Layer 2 Tunneling Protocol – L2TP)

Протоколите за връзка са разгледани в Глава 8, „Мрежови протоколи и услуги".

Автентикация при отдалечен достъп

Сървърът за отдалечен достъп автентицира отдалечените потребители в зависимост от методите за автентикация, зададени от администратора при конфигуриране на връзката за отдалечен достъп (вижте Фигура 15-3).

Фигура 15-3 *Отдалеченият клиент бива автентициран от сървъра за отдалечен достъп.*



Примери на методи за автентикация са:

- Протокол за автентикация чрез парола (Password Authentication Protocol – PAP), който изпраща паролите по мрежата некриптирани
- Shiva PAP (SPAP)
- Протокол за автентикация с предварително съгласуване на повикването (Challenge Handshake Authentication Protocol – CHAP), който криптира паролите
- Разширяем протокол за автентикация (Extensible Authentication Protocol – EAP), който използва MD5, смарт карти или сертификати

EAP със смарт карти е най-сигурният метод на автентикация. Вижте Глава 14, „Защита на мрежата", за да получите повече информация за смарт картите.

ЗАБЕЛЕЖКА Отдалечени клиенти и сървъри с Microsoft Windows могат да използват версия на CHAP, наречена MS-CHAP (Microsoft CHAP). Когато се използва MS-CHAP, може да бъде използван протоколът Microsoft Point-to-Point Encryption (MPPE) за криптиране на данните. MS-CHAP, версия 2, позволява взаимна автентикация (mutual authentication), представляваща двупосочна автентикация, при която на клиента се изпраща верификация да потвърди, че сървърът може да автентицира паролата на потребителя.

Услугата Remote Authentication Dial-In User Service (RADIUS) позволява автентикация на отдалечени потребители и осигурява услуги за управление на акаунти за работа в разпределена dialup мрежа. Вижте секцията „Проблеми на сигурността при отдалечен достъп“ по-нататък в главата, за да научите повече подробности за RADIUS.

Възможно е да конфигурирате сървъра да приема и неавтентициран достъп. В този случай от клиента не се изисква да въвежда потребителско име и парола. Ако имате клиенти, които трябва да осъществяват достъп до мрежата от операционни системи или платформи, които не поддържат отдалечена автентикация, ще трябва да разрешите неавтентициран достъп, защото в противен случай те няма да могат да се свържат.

Назначаване на IP адреси

Ако TCP/IP е протоколът, използван в LAN, всички компютри в мрежата трябва да имат правилни IP адреси, за да могат да комуникират. Това важи със същата сила както за отдалечените клиенти, така и за клиентските компютри, свързани към мрежата по кабел.

Сървърите за отдалечен достъп, като тези, работещи под Windows 2000 Remote Server (RAS), могат да бъдат конфигурирани да установяват контакт с DHCP сървър в мрежата и да придобиват IP адрес за отдалечения клиент. Ако няма DHCP сървър, пак можете да конфигурирате RAS сървър с пул от статични адреси, който се състои от валидни адреси за мрежата. Друг начин за това е клиентът да бъде конфигуриран с валиден статичен IP адрес за отдалечената мрежа.

Ако LAN протоколът, използван от отдалечения клиент и от сървъра, е NetBEUI, AppleTalk или IPX/SPX, не се изисква IP адрес.

Обединяване на пропускателната способност по Dialup връзки

Ако операционните системи на клиента и сървъра поддържат *обединяване на пропускателната способност (bandwidth aggregation)* или *мултилинк*, тогава физически отдалечени връзки (например две телефонни линии) могат да бъдат комбинирани, за да осигурят една обща връзка с по-голяма пропускателна способност. Този метод се използва най-често с BRI (Basic Rate ISDN); в този случай двата канала със скорост 64 Kbps (канали за данни) се обединяват за създаване на една връзка със скорост 128 kbps.

ЗАБЕЛЕЖКА Мултилинкът представлява софтуерно базиран метод за обединяване на пропускателната способност. Два ISDN канала могат да бъдат комбинирани също чрез *бондинг*, който представлява метод, базиран на хардуер.

Мултилинкът може да бъде използван за обединяване на пропускателната способност на два 56 kbps модема (всеки със своя собствена линия). По този начин dialup връзката към доставчик на Интернет услуги (ISP) по аналогови линии може да достигне скорости от 100 kbps или повече (в зависимост от състоянието на линията). Но този метод е подходящ само ако се поддържа от Интернет доставчика.

Контрол на използването на пропускателната способност

Заедно с обединяването на пропускателната способност, може да бъде използван и протоколът Bandwidth Allocation Protocol (BAP) за управление и контрол на използването на допълнителни линии. Това означава, че допълнителните линии се използват само когато е необходимо; ако степента на използване на пропускателната способност спадне, се изключват една или повече обединени линии. Ако изискването за пропускателна способност нарасне, автоматично се добавят допълнителни връзки.

Това е особено полезно при случаите, в които услугата се таксува на единица трансфер, защото освобождаването на неизползваните линии води до по-ниски телефонни такси.

Устройства за свързване при отдалечен достъп

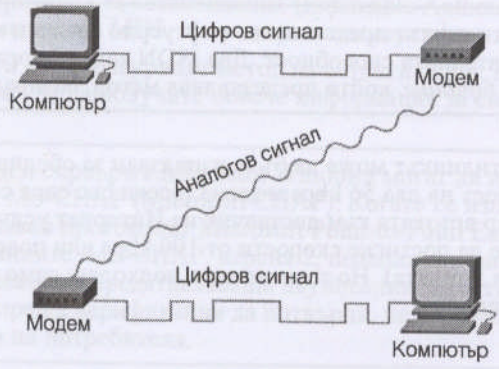
Производителността на отдалечения достъп е относително ниска (сравнена с традиционната кабелна мрежа). Макар че все по-широко достъпни стават алтернативи с висока пропускателна способност като DSL и кабелни модеми, типичните най-високи скорости за тези високоскоростни технологии са от 1 Mbps до 5 Mbps. Най-бавните Ethernet връзки имат скорости на трансфер от 10 Mbps, а най-разпространени са тези със скорост 100 Mbps. Различните технологии за WAN връзки, като DSL или кабелен модем, са разгледани по-детайлно в Глава 6.

Най-популярните средства за изграждане на отдалечена връзка са посредством модем по аналогова телефонна линия. В тази секция ще разгледаме характеристиките на модемите и на другите устройства за отдалечено свързване.

Модеми

Модемът е хардуерно устройство, основната функция на което е да преобразува цифровите сигнали, създавани от предаващия компютър, в аналогови сигнали, които могат да пътуват по телефонната линия. След това модемът на другия край на връзката преобразува тези аналогови сигнали обратно в цифрови, за да могат да бъдат обработени от приемащия компютър, както е показано на Фигура 15-4. Обърнете се към Глава 4, „Методи за комуникация по мрежи“, където е направен общ преглед на разликите между аналоговите и цифровите сигнали.

Фигура 15-4 *Модемите конвертират цифровите сигнали в аналогови и аналоговите сигнали обратно в цифрови.*



Как работи модемът

Процесът на конвертиране на аналогови в цифрови сигнали и обратно се нарича *модулация/демодулация* (оттук идва и терминът *модем*). Спомнете си, че цифровите комуникации са базирани на двоичната бройна система; т.е. цифровите сигнали представят единици и нули. Тези сигнали трябва да бъдат конвертирани във вълнова форма, за да могат да пътуват по аналогови линии.

Когато модемът се опитва да се свърже с друг модем, се изпраща тонален сигнал от извикващия модем. Тоналният сигнал се задава с конкретна модулация, която представлява бързо сменящи се тонове с висока и ниска тоналност. Звуковите тонове съответстват на единиците и нулите на оригиналния цифров сигнал. Ако модемът на приемащия край има възможност да използва този тип модулация, се установява връзка без допълнително съгласуване. Ако не може, изпращащият модем се опитва да използва по-ниска модулация; този процес продължава, докато изпращащият модем открие такава модулация, която се поддържа от приемащия модем. По този начин модемите винаги използват най-високата обща модулация. Този процес се нарича *fallback* (понижаване на скоростта), защото модемът пада на по-ниска модулация, когато е необходимо.

Опитните потребители на модеми могат да идентифицират скоростта, на която се установява връзката между модемите, по височината на тези тонове. Когато модемите установят връзка един с друг, се чува познатото „ръкостискане на модемите", което представлява кулминацията на процеса на съгласуване.

Асинхронни комуникационни портове

Аналоговите модеми използват форма на комуникация, наречена асинхронна комуникация (обърнете се към Глава 4 за повече информация относно асинхронната комуникация). COM портовете, вградени на дънните платки на модерните компютри, поддържат този тип комуникация. Обикновено компютърът има два COM порта – 9-изводен конектор и 25-изводен конектор. Масово разпространени са адаптерите за конвертиране от единия в други вид. Външният модем се свързва към един от тези серийни портове с помощта на сериен кабел.

Чиповете, чрез които се реализират COM портовете, се наричат UART (Universal Asynchronous Receiver/Transmitter) чипове. Типът на UART чиповете определя най-високата скорост, на която могат да комуникират устройствата, използвайки порта. По-старите чипове UART 8259 имат максимална скорост 9600 bps. По-новите чипове UART 16450 и 16550 позволяват скорости до 115 200, а чиповете 16650 поддържат скорост на предаване 230 400 bps.

Вътрешните модеми имат собствени UART чипове и не са ограничени от скоростта на UART на COM портовете на компютъра.

Първите модеми използваха *акустичен съединител*, представляващ устройство, в което поставяте телефонната слушалка на стандартен телефон. Тези модеми нямаха възможност да набират телефонни номера; трябваше ръчно да наберете номера с телефонната шайба. Скоростите на връзката бяха много ниски: модем със скорост 2400 bps се считаше за страхотно бърз. Hayes предложиха на пазара първите „интелигентни модеми", които можеха да избират телефонни номера.

Друг недостатък на по-старите модеми беше тяхното конфигуриране, за което често се налагаше да пишете скрипт, наречен *низ за инициализация на модема*.

Това е поредица от знакове, идентифициращи и конфигуриращи метода, с помощта на който се свързват двата модема.

Днешните модеми са много по-бързи и варират от 14,4 до 56 kbps. Все още се предлагат акустични съединители; те осигуряват достъп с модем, когато телефонната линия е твърдо свързана и не може да бъде изключена от телефона и включена в модема.

Типове модеми

Повечето модерни модеми могат да бъдат класифицирани в следните три типа:

- Вътрешни
- Външни
- PC Card (PCMCA)

И при трите типа включвате телефонната линия в стандартен телефонен конектор RJ-11. Всеки тип има предимства и недостатъци, които ще разгледаме по-долу.

Вътрешни модеми

Вътрешните модеми, както подсказва самото име, се включват в разширителен слот за карти във вътрешността на компютъра. Достъпни са варианти за ISA и PCI. Освен това са достъпни версии PCMCA/PC Card за използване с лаптоп компютри.

Вътрешният модем не отнема допълнително място на бюрото, но трябва да отваряте кутията на компютъра, за да го инсталирате. Най-общо вътрешните модеми са малко по-евтини от същия модел във външна конфигурация.

Конфигурирането на вътрешен модем може да изисква да превключите джъмпери на платката, за да изберете IRQ и I/O адрес. В това отношение конфигурирането на модема наподобява конфигурирането на мрежовата интерфейсна карта, както бе разгледано в Глава 7, „Физически компоненти на мрежата“. Модемът трябва да бъде конфигуриран за използване на COM порт, който не се използва от друго устройство. Устройствата, използващи COM портове, са посочващите устройства, скенерите, кредъли за ръчните компютри и други устройства, които използват серийна връзка. Софтуерните драйвери за модема също трябва да бъдат инсталирани.

Ако модемът е Plug and Play (PnP) модел и PnP се поддържа както от BIOS-а на системата, така и от операционната система, може да не е нужно ръчно конфигуриране.

Външни модеми

Външните модеми обикновено струват малко повече от вътрешните, но те предлагат няколко предимства:

- Не е нужно да отваряте кутията и да инсталирате карта; просто включвате модема в сериен порт с помощта на сериен кабел. При новите USB модеми включвате модемите в USB порт или в концентратор.
- Външният модем използва IRQ и I/O адрес, зададени на серийния порт, към който е свързан модемът, затова обикновено изискват по-малко

конфигурация, макар че това предимство може да бъде отречено при използване на вътрешен PnP модем.

- Обикновено външните модеми имат индикаторни светлини, или *светлини за състоянието*, по които можете да разберете кога модемът е онлайн, кога предава или приема данни и т.н. Някои вътрешни модеми също имат индикаторни светлини; но те не винаги са видими за потребителя, защото са на задния панел на компютъра.

Както при вътрешния модем, трябва да инсталирате софтуерни драйвери, които позволяват на външния модем да комуникира с операционната система. Драйверите за популярните марки, например Motorola и U.S. Robotics, може да бъдат включени и на инсталационните дискове на операционната система.

Модеми PC Card

Модемите PC Card, често наричани PCMCA модеми, представляват малки карти, които се включват в специални слотове, обикновено на лаптоп или нотбук компютри. PC Card интерфейсите са достъпни и за настолни машини. PC Card модемът е конфигуриран по начин, подобен на другите типове модеми. Голямо предимство на PC Card е малкият размер и преносимостта.

Настройка на свойствата на модема

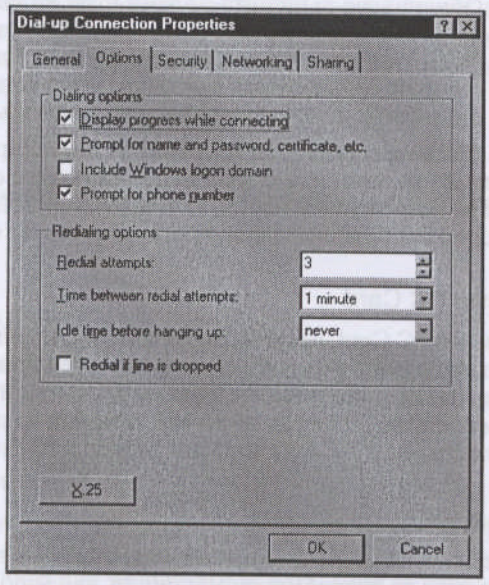
Свойствата на модема често могат да бъдат настройвани според конкретните изисквания на потребителя. Например, ако използвате услугите на определена телефонна компания, да речем, използвате аналогова телефонна линия, по която няма тонален сигнал за набиране, трябва да настроите модема да не изчаква наличие на такъв сигнал, преди да започне набиране на телефонния номер.

Други настройки, които могат да бъдат приспособени (в зависимост от вида на вашия модем и операционна система), са следните:

- Възможността да настроите силата на звука (или да накарате модемът да набира безшумно)
- Възможността да зададете местоположение, от което набирате, за да знае модемът, че трябва да набере код на област преди телефонния номер при междуградски телефонни разговори
- Възможността да зададете автоматично прекъсване на връзката, ако не се използва определен период от време
- Възможността да зададете дали и колко пъти модемът трябва да набира повторно, ако се натъкне на сигнал за заета линия
- Максималната скорост на COM порта, към който е свързан модемът

Дружелюбните операционни системи, като Windows 2000, улесняват конфигуриране на свойствата на dialup връзката, както е показано на Фигура 15-5.

Фигура 15-5 *Свойствата на набирането могат лесно да бъдат конфигурирани от диалоговия прозорец Dial-up Connection Properties на Windows 2000.*



Отстраняване на проблеми при модемите

Проблемите с модемите могат да бъдат доста досадни и варират от модем, който не набира номера, до такъв, който постоянно се свързва на много ниска скорост или често се изключва. Софтуерът, придружаващ модема, може да включва диагностични помощни програми, които да ви помогнат да тествате функционалността на вашия модем; освен това операционни системи като Windows 2000 включват инструменти за диагностика и отстраняване на неизправности на модема.

В следващите секции на тази глава описваме следните проблеми с модемите:

- Модемът не набира номера.
- Модемът набира, но не установява връзка.
- Модемът установява връзка, но след това бързо я прекъсва.
- Модемът установява връзка на много ниска скорост.
- В допълнение ще разгледаме проблемите с COM портовете, които също влияят на възможността на модема за установяване на връзка.

Модемът не набира

Ако модемът не набира телефонни номера, вероятно софтуерът не комуникира с модема. Тази липса на комуникация може да се дължи на това, че операционната система не разпознава COM порта, към който е свързан модемът. Трябва да проверите BIOS-а на компютъра, за да се уверите, че COM портът е разрешен. Също така може да има конфликт между COM порта на вътрешен модем и друго серийно устройство, което използва същото IRQ и същия COM порт.

Промяната на настройките на COM порта в BIOS или промяната на зададено IRQ отстранява този проблем.

Липсата на комуникация може да бъде предизвикана също от драйверите на модема, които не са инсталирани, от неподходящи или неправилно инсталирани драйвери или от това, че самите драйверни файлове са повредени. Тази ситуация може да бъде коригирана с повторно (и правилно) инсталиране на драйверите.

Ако проблемите продължават и модемът е зададен да изчаква тонален сигнал за избиране (dial tone), преди да започне да набира, трябва да помислите за възможността дали самият телефон не е повреден. Освен това обърнете внимание, че някои компании за телефонни услуги, например гласовата поща Call-Notes, използват кратък сигнал, за да ви уведомяват, че имате съобщения. Този сигнал, когато бъде приет, заменя телефонния. Ако имате такава услуга, може да се наложи да настроите модема да не чака тонален сигнал за набиране, а направо да започва набирането.

Накрая една често срещана – и донякъде излагаща – причина за проблема може да бъде тази, че телефонната линия просто не е включена в модема. Обърнете внимание, че модемите имат два женски конектора RJ-11 и те изглеждат идентично. Единият е предназначен за входящата телефонна линия, а другия за изходна линия към телефонен апарат. Уверете се, че телефонът е включен в правилния конектор.

Модемът не установява връзка

Ако модемът набира номера, знаете, че проблемът не е в телефонната линия или кабела, който е свързан с модема. Най-често срещаната причина е, че модемът набира погрешен номер. Проверете дали номерът е правилен и дали е включен кодът на област, ако е необходимо.

Друга възможност е номерът, който набирате, да е зает. Ако звукът на модема е включен, би трябвало да чуете тона за заета линия. Модемът може да бъде настроен автоматично да продължава с повторно набиране, когато приеме сигнал заето.

Ако отговаря друг модем, но не може да бъде установена връзка, може би имате несъвместимост между типовете модеми. Друга възможност е на вашия модем да е зададена по-висока скорост на трансфер на данни, отколкото на модема, който набирате. В този случай трябва да настроите скоростта на порта на по-ниско ниво и това ще реши проблема.

Модемът бързо прекратява връзката

Ако се свързвате с модема на другия край, но веднага след това връзката се разпада, това означава, че сървърът за отдалечен достъп сигурно не може да автентикира вашия акаунт. Проверете дали имат зададени правилни свойства на dialup връзка и въведете правилно потребителско име и парола.

Друга възможност е, че вашият потребителски акаунт е зададен за сигурност с обратно повикване на отдалечения сървър. В този случай сървърът ви изключва след като въведете вашето потребителско име и парола, но трябва веднага след това да ви набере обратно и отново да установи връзката. (Повече информация за сигурността с обратно повикване ще намерите в секцията „Проблеми на сигурността при отдалечен достъп“.) Ако случаят е такъв, уверете се, че вашият модем е конфигуриран да приема входящи повиквания.

Ако бъдете изключвани на равни интервали, когато осъществявате достъп до Интернет през ISP, доставчикът може да е задал ограничения на максималните времена на връзка. Потребителите могат да бъдат „изхвърляни" автоматично след изтичане на определен интервал от време, например 6 часа. Това зависи от политиката и можете да го научите от вашия Интернет доставчик. В много случаи е възможно веднага да наберете отново и да установите връзка.

Модемът установява връзка на ниска скорост

Ако модемът установи връзка, но комуникира на много по-ниска скорост, отколкото очаквате, проблемът може да е причинен от шумни линии. В някои области може да не е възможно да постигнете скорости, по-големи от 35 kbps с модем 56 kbps.

Друга причина за бавните скорости на връзка е модемът от другия край на връзката, който не поддържа високи скорости. Вашият 56 kbps модем се свързва на 28,8 kbps, когато модемът от другия край на връзката има най-висока възможна скорост 28,8 kbps.

Друг проблем представлява несъвместимостта. Първите 56 kbps модеми се произвеждаха в два варианта: 56Kflex, който се поддържаше от производители като Motorola, и технологията X2, която се използваше в модеми то U.S. Robotics. По-новите модеми са проектирани да отговарят на общоприет стандарт, но ако имате по-старо устройство, може да се наложи да ъпгрейднете BIOS-а на модема, за да коригирате проблемите на несъвместимостта.

Ако не успявате никога да постигнете високи скорости с вашия модем, друга възможност е драйверите да са стари или неправилни. Проверете на Web сайта на производителя дали има по-нови драйвери от вашите.

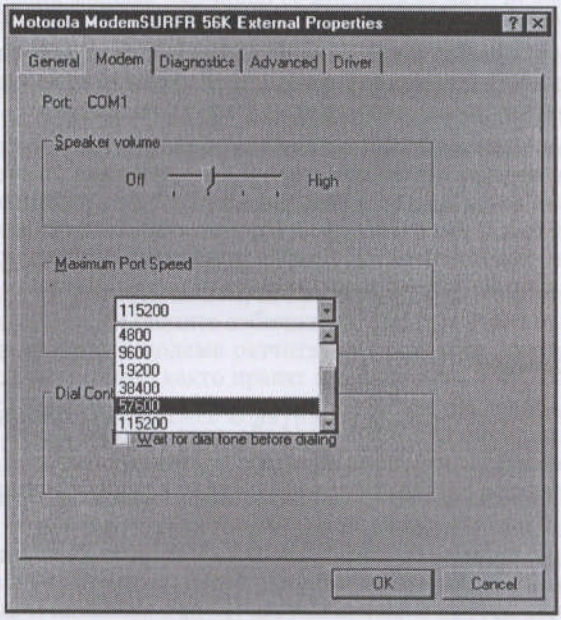
Повреден кабел на външния модем може да доведе до бавен трансфер или изобщо до невъзможност за комуникация. Възможно е също самият модем да е дефектен и да се наложи да го замените.

Проблеми с COM портовете

В някои случаи проблемът не е в модема, а в COM порта, към който е свързан. Ако имате висикоскоростен външен модем, който се свързва само на ниски скорости (например на 9600 bps) трябва да проверите UART чипа на COM порта, към който е свързан модемът.

В някои случаи дори ако COM портът има висикоскоростен UART, подразбиращите се настройки на скоростта на порта в операционната система може да са зададени твърде ниски. В този случай може да се наложи ръчно да промените скоростта на порта. Фигура 15-6 показва настройките на скоростта на порта в диалоговия прозорец на Windows 2000.

Фигура 15-6 *Скоростта на порта може да бъде променена в Windows 2000 от диалоговия прозорец със свойствата на модема.*



ISDN терминални адаптери

ISDN терминалните адаптери понякога се наричат ISDN „модеми", но прилагането на този термин е неточно, защото ISDN терминалните адаптери не модулират и демодулират сигнала; те не правят това, защото ISDN линиите са цифрови.

ISDN адаптерите се произвеждат от същите фирми, които произвеждат модеми, и са достъпни като вътрешни и външни модели. Повечето от тях позволяват използването на един или два канала със скорост 64 kbps, наречени B канали. Най-общо двете линии имат различни телефонни номера, макар че проводниците могат да бъдат затворени в едни кабел.

ISDN адаптерите се инсталират по начин, подобен на инсталирането на модеми. Софтуерът на драйверите трябва да бъде инсталиран и конфигуриран, а при някои адаптери трябва да въведете идентификатори (ID) на *профила на услугата (SPIDs)* и на двете линии. Може да се наложи да конфигурирате и други опции в зависимост от модела на адаптера.

ЗАБЕЛЕЖКА SPID идентификаторът е съставен от 10-цифрен телефонен номер на линията и може да включва префикс или суфикс за идентифициране на възможностите на линията. SPID идентификаторите се назначават от телефонната компания.

ISDN маршрутизаторите могат да бъдат използвани за осигуряване на Интернет достъп до цялата LAN. Това изисква всеки компютър да има регистриран IP адрес. За тази цел Интернет доставчикът може да ви зададе блок от IP адре-

си. Друг начин за това е да използвате NAT софтуер за транслиране на частните вътрешни адреси в един регистриран публичен адрес; в този случай маршрутизаторът не е нужен. Вижте секцията „Как действа адресната транслация“ в Глава 6, за да получите повече информация относно реализацията на NAT.

Често срещан проблем при ISDN е, че понякога се свързва само една от двете линии. В този случай трябва да се уверите, че имате правилно инсталиран и конфигуриран софтуер за мултилинк на линиите.

При повечето ISDN адаптери можете да свържете аналогови телефони за осъществяване на гласови разговори. Адаптерът може да бъде конфигуриран така, че да се свързва към Интернет на 128 kbps, а когато по една линия постъпи повикване и вие отговорите, Интернет връзката да спадне обратно на 64 kbps, докато трае разговорът. Когато затворите телефона, втората линия автоматично се свързва отново и връща скоростта на 128 kbps.

Кабелни модеми

„Кабелен модем“ е друг неправилно употребяван израз. Това устройство действа подобно на LAN интерфейс, като свързва вашия компютър към кабела на мрежата на кабелния оператор посредством същия коаксиален кабел, по който приемате сигналите на кабелната телевизия с вашия телевизор.

Кабелните модеми, за разлика от аналоговите модеми и ISDN адаптерите, най-общо осигуряват само достъп до Интернет. При аналоговите модеми и ISDN адаптери можете да наберете всеки доставчик на Интернет или сървър за отдалечен достъп в частна мрежа. Но при кабелния модем сте свързани по кабела директно към кабелната мрежа и единственият избор за доставчик е кабелната компания.

Услугата кабелен модем е „винаги включена“ технология. Но ако инфраструктурата на кабелната компания е еднопосочна, трябва да установите също dialup връзка, за да можете да изпращате заявки по възходящия поток. За повече информация вижте Глава 6.

Макар че сървърът, с който контактувате, е на отдалечено местоположение, достъпът с кабелен модем прилича повече на директна връзка към LAN, отколкото на отдалечен достъп. Имайте го предвид, когато разглеждаме по-нататък технологията в тази глава, защото те обикновено се използва за същата цел, както разглежданите тук методи за отдалечен достъп.

ЗАБЕЛЕЖКА Някои кабелни компании предлагат или планират да предложат телефонни услуги по техните CATV мрежи.

Кабелни модеми, подобно на техните аналогови и ISDN съответствия, са достъпни като вътрешни и външни устройства. Кабелната компания обикновено ви задължава да използвате даден модел и реално може да се наложи да купите изцяло или на лизинг устройството от тях и да ви бъде забранено сами да си доставите собствено устройство.

Вътрешният кабелен модем представлява малка кутия, към която се свързва коаксиалният кабел на кабелната телевизия. За разделяне на сигнала между телевизора и кабелния модем се използва сплитер. От своя страна кутията се свързва към Ethernet карта в компютъра посредством UTP Ethernet кабел. Достъпни

са също вътрешни USB устройства; те свързват модема към USB порта на компютъра и не изискват Ethernet карта.

Вътрешните кабелни модеми най-общо се инсталират като PCI карти. Те са поевтини, но не работят с всички кабелни мрежи и не могат да бъдат използвани с лаптоп компютри или машини Macintosh.

Кабелният модем включва тунер с вграден дуплексер, за да могат да бъдат осигурени сигналите както на низходящия, така и на възходящия поток. Но инфраструктурите на някои кабелни телевизии поддържат предаване на сигнали само по низходящия поток. В този случай предаването на възходящия поток трябва да бъде изпратено по телефонна линия, и за тази цел в кабелния модем се вгражда телефонен конектор.

Модемът приема цифрово модулирани сигнали. Демодулаторът е вграден в модема, и ако това е двупосочен модем, за предаване на възходящия поток се използва burst модулатор. Външните кабелни модеми включват също микропроцесорен чип, а вътрешните модеми разчитат на процесора на компютъра за обработката на задачите, точно както правят аналоговите „Win модеми".

За нещастие, няколко стандарта се конкурират за надмощие в индустрията за кабелен достъп. Докато един от тях не се наложи като победител, кабелният достъп ще бъде нестандартна технология и услугите, скоростта, надеждността и конфигурациите ще варират значително между различните кабелни компании.

Едно чудесно ръководство по техническите детайли на технологията на кабелните модеми може да бъде намерено в Web на адрес www.cable-modems.org/tutorial/index.htm.

CSU/DSU

CSU/DSU устройството (устройство за обслужване на канала/устройство за връзка с цифровата услуга) се използва при наети цифрови линии (Т-носещи). То преобразува фреймовете на цифровите данни в локалната мрежа във формата, използван от WAN връзката. Самото устройство наподобява външен модем или ISDN терминален адаптер.

И в двата края на връзката трябва да има CSU/DSU. CSU защитава Т-1 линията от електрически смущения и се използва от телефонната компания за излъчване на ехо на тестови сигнали, наречени *обратни връзки (loopbacks)*. DSU изпълнява контролни задачи, които управляват грешките при синхронизация и регенерирането на сигнали. То преобразува данните на входящите сигнали за предаването им по линията.

CSU/DSU комуникира с компютъра през DTE (data terminal equipment) интерфейс. Това е стандартен RS-232 интерфейс или сериен интерфейс.

Конфигуриране на клиенти и услуги за отдалечен достъп

По същия начин, по който трябва да конфигурирате вашия компютър така, че да можете да участвате в кабелна мрежа, така трябва да конфигурирате системите, които комуникират една с друга посредством отдалечен достъп. В следващите секции ще разгледаме как се конфигурира един отдалечен клиент, за да

установи връзка, и как се конфигурира отдалечен сървър за приемане на входящи връзки.

Конфигуриране на клиент за отдалечен достъп

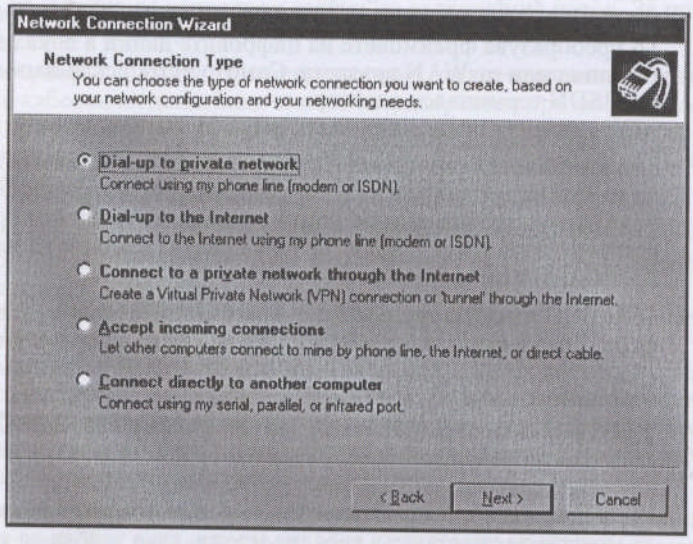
За да можете да набирате и да установите връзка към сървър за отдалечен достъп, като dialup сървър на Интернет доставчик или RAS сървъра на вашата организация, трябва да конфигурирате вашия компютър да функционира като клиент за отдалечен достъп. Това включва няколко стъпки:

1. Инсталиране на правилното хардуерно устройство (обикновено аналогов модем).
2. Инсталиране и конфигуриране на софтуерните драйвери за устройството.
3. Свързване на устройството към телефонната линия.
4. Задаване на свойства за набиране на връзката. Тези свойства включват телефонните номера, които трябва да бъдат набирани, името и паролата на потребителя за достъп до отдалечения сървър, използването на PPP или SLIP за установяване на връзката и други характеристики.

Може да се наложи да инсталирате компонент за dialup мрежа, ако операционната система не инсталира такъв по подразбиране. Възможно е да се наложи да инсталирате RAS като мрежова услуга на компютри с Windows NT. За да комуникирате с отдалечения сървър, трябва също да инсталирате правилни протоколи.

Операционните системи като Windows 9x и Windows 2000 притежават съветници (wizards), които ви водят през процеса на инсталиране, както е показано на Фигура 15-7.

Фигура 15-7 *Съветникът Network Connection Wizard ви води през процеса на инсталиране на новата dialup връзка.*



Конфигуриране на сървър за отдалечен достъп

Сървърът за отдалечен достъп трябва да бъде оборудван с модем или модеми и трябва да бъде конфигуриран за приемане на входящи повиквания. Точните процедури са различни, в зависимост от операционната система.

По отношение на сървъра за отдалечен достъп може да се наложи също да вземете следните решения и да направите съответните промени на настройките:

- Дали да приема Multilink PPP връзки.
- Дали да използва BAP за динамично управление на използването на пропускателната способност. Тази опция е достъпна само при разрешен Multilink.
- Дали да разрешава IP маршрутизация, или за LAN протоколи, различни от TCP/IP, дали да разрешава само достъп до сървъра или до цялата мрежа.
- Когато използва TCP/IP, дали сървърът ще задава IP адреси от комплект от статични адреси или ще използва DHCP сървър.
- Какъв метод за автентикация да се използва за отдалечени връзки.

Политиките за отдалечен достъп могат да бъдат използвани за контрол на достъпа, базиран на членство в групи. За повече информация относно политиките за отдалечен достъп вижте следващата секция на тази глава „Проблеми на сигурността при отдалечен достъп".

Проблеми на сигурността при отдалечен достъп

Независимо дали се свързвате към Интернет като dialup клиент или отваряте ваш сървър за dialin достъп, връзката към външния свят ви излага на определени рискове по отношение на сигурността.

В Глава 14 разгледахме общите насоки на сигурността относно нарушителите по Интернет. Тази секция излага някои от специалните проблеми на сигурността, които възникват, когато разрешите dialup достъп до сървър във вашата мрежа.

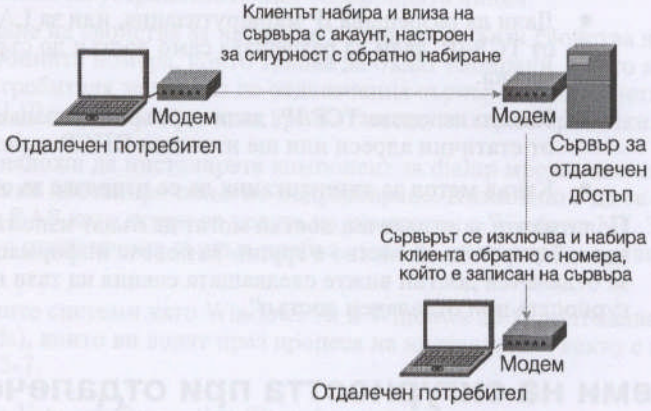
Можете да повишите сигурността по няколко начина, като едновременно с това разрешите на вашите потребители отдалечения достъп, който им е необходим. С помощта на мерки за сигурност в комбинация с позволения за достъп до файлове и споделени ресурси за контрол на достъпа, можете да постигнете сигурна среда и в същото време да осигурите на потребителите удобството на отдалечения достъп. В следващите секции ще разгледаме някои от най-често прилаганите мерки за сигурност:

- Сигурност чрез обратно набиране
- RADIUS
- Политики на отдалечен достъп
- Заключване на акаунт
- Сигурни хостове

Сигурност чрез обратно набиране

Сигурността чрез обратно набиране е възможност на сървъра за отдалечен достъп, която може да разшири сигурността чрез ограничаване на dialup връзки само до тези на одобрени телефонни номера. При включена сигурност с обратно набиране сървърът не вярва на акредитивите (потребителско име и парола), въведени от потребителя. Вместо това сървърът се опитва да проверява идентичността по същия начин, по който можете да направите това, ако ви се струва, че лицето, което се обажда, може да не е това, за което се представя, като затворите телефона и наберете обратно номера на лицето, показан в телефонния указател. Вижте Фигура 15-8.

Фигура 15-8 *Сигурността с обратно набиране ограничава телефонния номер, от който отдалеченият потребител може да набира.*



Ето как работи това:

1. Предварително зададения телефонен номер, съвместно с акаунта на потребителя, е въведен на сървъра за отдалечен достъп.
2. Когато потребителят набере сървъра, той бива запитан за потребителско име и парола. Те идентифицират потребителя на сървъра, който след това проверява дали акаунтът е зададен да използва сигурност с обратно набиране.
3. Сървърът прекъсва връзката и след това веднага набира потребителя обратно на предварително зададения номер и разрешава нормален достъп до мрежата.

Този процес гарантира, че дори ако някой нарушител е научил потребителското име и паролата на легитимен потребител, той няма да може да осъществи достъп до мрежата отдалечено, освен ако не набира от дома на потребителя или от предварително зададено местоположение.

RADIUS

RADIUS е протокол, който стана индустриален стандарт за автентикация на dialup потребители и осигурява услуги за управление на акаунти за dialup сървъри, използвани от ISP доставчиците. Dialup сървърът се конфигурира като RADIUS клиент, а информацията за потребителско име и парола се изпраща от dialup сървъра до RADIUS сървъра. RADIUS сървърът осигурява автентикация.

RADIUS сървърът осигурява централизирана автентикация с помощта на определени протоколи:

- PAP
- CHAP и MS-CHAP
- EAP
- Dialed Number Identification Service (DNIS)
- Automatic Number Identification (ANI) Service

Разгледахме първите три метода по-рано в тази глава. DNIS е базиран на номера, набиран от потребителя, а ANI (използващ идентификатор на повикващия) е базиран на номера, от който се обажда потребителят.

RADIUS също дава информация за влизане и одитинг, и информация за използваемостта и управлението на всички мрежови сървъри за достъп в мрежата от централизирано местоположение. Спецификациите за RADIUS са дадени в RFC 2138 и 2139.

Политики на отдалечен достъп

В зависимост от операционната система, може да имате възможност да контролирате достъпа чрез създаване и прилагане на политиките за отдалечен достъп, които предоставят или забраняват достъп на базата на следните критерии:

- Час от деня (например ограничаване на отдалечения достъп от 8 сутринта до 5 следобед)
- Ден от седмицата (например разрешаване на отдалечен достъп от понеделник до събота, но не и в неделя)
- Членство в група (например забраняването на достъп на всички членове на групата Newbies)
- Тип на отдалечената връзка (например разрешаване на VPN връзки, но забраняване на dialin връзки или обратно)

Политиките също могат да ограничават количеството време, което потребителят може да бъде свързан, или методите на автентикация, които могат да бъдат използвани.

Заключване на акаунт

Заключването на акаунт може да бъде приложено към връзки за отдалечен достъп, за да попречи на неоторизирани потребители да познаят валидната парола чрез изпробване на различни пароли в последователен ред, ръчно или чрез софтуерни атаки с груба сила.

При заключването на акаунта, след определен брой неуспешни опити за логване акаунтът се заключва и системата не приема повече опити. Можете да конфигурирате тази възможност по следните начини:

- Можете да зададете броя на неуспешните опити, които са разрешени преди заключване. Потребител може неволно да сбърка паролата един или дори два пъти, но малко вероятно е да повтаря грешката си непрекъснато, затова можете да зададете тази стойност на 3.

- Можете да зададете дали акаунтът ще бъде освободен след зададен период от време или ще остане заключен, докато администраторът не го отключи. Може да предпочетете да зададете тази стойност на приемлив интервал от време, например на 2 часа. При това положение, ако легитимният потребител се опита да се логне, след като акаунтът е бил заключен вследствие атака на нарушител, потребителят ще може да направи това без проблеми.

Хостове за сигурност

Един хост за сигурност представлява устройство, използвано за автентикация на входящи dialup потребители. То се използва в допълнение към собствените мерки за сигурност на сървъра за отдалечен достъп. Хостът представлява хардуерно устройство, което се инсталира между клиента за отдалечен достъп и сървъра за отдалечен достъп.

Съществуват няколко типа хостове за сигурност; в някои случаи хостът изисква от dialup потребителя да зададе потребителско име и парола, които са отделни и независими от името на акаунта и паролата, използвани за логване в сървъра за отдалечен достъп. Например компанията Security Dynamics предлага модема SecurID, представляващ модем от тип PC card, който включва автоматизирана автентикация за мобилни потребители. Потребителят въвежда PIN номер, който се изпраща автоматично от модема до хоста за верификация.

Обобщение

В тази глава разгледахме нарастващата популярност на отдалечения достъп в света на съвременния бизнес. Разгледахме ситуации, в които отдалеченият достъп е подходящ, в това число свързването на филиални офиси един с друг, осигуряването на достъп в извън работно време за служителите, телекомютинга, свързването към мрежата по време на път и споделянето на ресурси на компанията с клиенти и партньори.

Научихте как работи отдалеченият достъп и разгледахме протоколите, използвани за отдалечен достъп. Научихте, че отдалечените клиенти и сървъри трябва да използват поне едни общ мрежов/транспортен протокол, както и че протокол за връзка като PPP или SLIP се използва за установяване на връзка по телефонна линия.

Разгледахме методите за отдалечена автентикация, като PAP, SPAP, CHAP, MS-CHAP и EAP. Научихте също, че DHCP сървърът може да задава IP адреси на dialup клиенти и че сървърът за отдалечен достъп може да бъде конфигуриран да използва пул от статични адреси, от който да изтегля адресите.

Научихте за обединяването на пропускателната способност с помощта на Multilink PPP или бондинг; и двете ви позволяват да комбинирате две или повече линии за осигуряване на една високоскоростна връзка. В допълнение към това научихте за BAP, който може да бъде използван за динамичен контрол на използването на пропускателната способност по мултилинк връзка.

Направихме общ преглед на устройствата за отдалечено свързване, като модеми, ISDN терминални адаптери, кабелни модеми и CSU/DSU устройства. Научихте, че модемите работят чрез модулиране и демодулиране на сигнала, който се конвертира от цифров сигнал в аналогов и обратно. Разгледахме характеристиките на три типа модеми: вътрешен, външен и PCMCA. Научихте също за

приспособяването на настройките на модема и за начините за отстраняване на проблеми при модемите.

След това разгледахме как се конфигурира клиент за отдалечен достъп и как можете да инсталирате сървър за отдалечен достъп. Накрая разгледахме проблемите на сигурността. Научихте, че са възможни разнообразни мерки за сигурност, в това число сигурност с обратно набиране, RADIUS, политики за отдалечен достъп, заключване на акаунти и хостове за сигурност.

Тази глава се фокусира върху dialup достъпа. В следващата глава ще разгледаме по-отблизо друг тип отдалечен достъп – виртуалната частна мрежа.

Допълнителни източници

Подробно разглеждане на модемите може да бъде намерено на www.teleport.com/~curt/modems.html.

Полезна информация и връзки можете да намерите на Web сайта RADIUS Resources на адрес www.func.com/radius

Заглавната страница на работната група IETF, посветена на RADIUS, се намира на www.ietf.org/html.charters/radius-charter.html.

RFC 2284, който регламентира EAP, се намира на www.rfc-editor.org/rfc/rfc2284.txt.

3Com осигурява добър ресурс за информация относно BAP и Multilink PPP на infodeli.3com.cpm/infodeli/tools/isdn/mlppp/mlppp.html.

За информация относно софтуера на Shiva за управление на сигурността, вижте www.shiva.com/images/t-products.gif.

За обща информация относно проблемите на сигурността при отдалечен достъп вижте www.list.gmu.edu/ras.htm.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Кое от следните може да бъде използвано за осигуряване на dialup достъп до множество клиенти едновременно?
   - **a** Multilink
   - **b** Bandwidth Allocation Protocol
   - **c** Банка от модеми
   - **d** CSU/DSU

2 Какъв е най-разпространеният тип връзка за отдалечен достъп?
   - **a** Посветена цифрова връзка
   - **b** Dialup аналогова връзка
   - **c** Dialup цифрова връзка
   - **d** Безжична връзка

3 Кои от следните се наричат протоколи за връзка и се използват за установяване на връзка по телефонни линии? (Изберете всички верни отговори.)

a SLIP
b IPX/SPX
c NetBEUI
d PPP

4 Кой от следните методи за автентикация изпраща паролите по мрежата некриптирани?

a CHAP
b PAP
c EAP
d SPAP

5 Кое от следните се използва за осигуряване на 128 kbps ISDN връзка?

a Bandwidth Allocation Protocol
b Point to Point Tunneling Protocol
c Multilink PPP
d Мултикастване

6 Кои от следните се отнасят до процеса, използван от модемите по време на процеса на съгласуване на връзка?

a Понижаването на скоростта (fallback)
b Бондинг
c Ремодулация
d Обратното набиране

7 Какви са чиповете, на които се базират COM портовете на компютъра?

a USB чипове
b UART чипове
c UNC чипове
d UDP чипове

8 Кое от следните е предимство на вътрешните модеми пред външните?

a Вътрешните модеми са по-лесни за инсталиране.
b По-лесно се наблюдава състоянието на вътрешните модеми.
c Вътрешните модеми са по-евтини.
d Вътрешните модеми нямат предимства.

9 Кои от следните са най-честите причини за свързване на модемите на ниски скорости? (Изберете всички верни отговори.)

a Потребителското име и паролата са въведени неправилно.
b Повикването идва от телефонна линия, която има услуга за изчакване на повикване.

c Телефонните линии са „нечисти“ или „шумни“.

d Модемът е несъвместим с модема от другия край на връзката.

10 Централизираната автентикация, управлението на акаунти и контролът на сървърите за достъп до мрежата се осигуряват от кое от следните?

a NAT

b RADIUS

c RAID

d RARP

Глава 16

Виртуални частни мрежи

В Глава 15, „Отдалечен достъп“, разгледахме dialup връзките, но те са само една от формите на отдалечения достъп. Друга разновидност — която нараства по популярност, тъй като производителите на софтуер направиха по-лесно нейното реализиране и организациите откриват нейните предимства — е връзката чрез *виртуална частна мрежа (virtual private networking — VPN)*.

В тази глава ще разгледаме тази полезна, ценово ефективна форма на отдалечен достъп. Ще научите какво представлява виртуалната частна мрежа и как работи. Ще разгледаме протоколите, използвани за изграждане на VPN, както и изключително важния проблем за сигурността на VPN. След това ще разгледаме типовете VPN мрежи и проблемите на производителността и ще завършим с практически пример за начина на конфигуриране на VPN връзка.

Какво представлява VPN?

Ако разгледаме термина виртуална частна мрежа, можем да видим, че той е съставен от три думи. Всяка дума е един компонент, от който се изгражда цялата концепция. „Мрежа“ означава компютри, които комуникират един с друг. Да разгледаме другите два компонента — „виртуална“ и „частна“, които дефинират по какво виртуалната частна мрежа се различава от другите типове мрежи.

Виртуална мрежа

Вече разгледахме локалните мрежи (LAN) и глобалните мрежи (WAN). Общ фактор и в двата типа мрежи е някакъв вид *мрежова преносна среда (medium)* — кабелна или безжична връзка — която директно свързва комуникиращите компютри. Виртуалната мрежа не притежава такава директна връзка. Вместо това се създава тунел през обществена мрежа — обикновено Интернет — и двата комуникиращи компютъра се свързват към мрежата, както е показано на Фигура 16-1.

Глава 16

Виртуални частни мрежи

В Глава 15, „Отдалечен достъп“, разгледахме dialup връзките, но те са само една от формите на отдалечения достъп. Друга разновидност — която нараства по популярност, тъй като производителите на софтуер направиха по-лесно нейното реализиране и организациите откриват нейните предимства — е връзката чрез *виртуална частна мрежа (virtual private networking — VPN)*.

В тази глава ще разгледаме тази полезна, ценово ефективна форма на отдалечен достъп. Ще научите какво представлява виртуалната частна мрежа и как работи. Ще разгледаме протоколите, използвани за изграждане на VPN, както и изключително важния проблем за сигурността на VPN. След това ще разгледаме типовете VPN мрежи и проблемите на производителността и ще завършим с практически пример за начина на конфигуриране на VPN връзка.

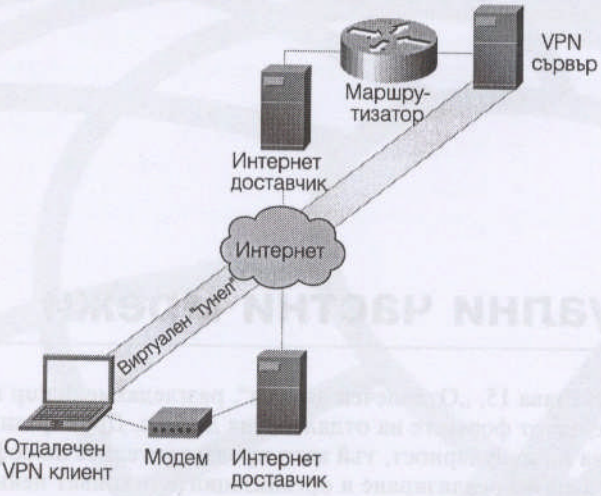
Какво представлява VPN?

Ако разгледаме термина виртуална частна мрежа, можем да видим, че той е съставен от три думи. Всяка дума е един компонент, от който се изгражда цялата концепция. „Мрежа“ означава компютри, които комуникират един с друг. Да разгледаме другите два компонента — „виртуална“ и „частна“, които дефинират по какво виртуалната частна мрежа се различава от другите типове мрежи.

Виртуална мрежа

Вече разгледахме локалните мрежи (LAN) и глобалните мрежи (WAN). Общ фактор и в двата типа мрежи е някакъв вид *мрежова преносна среда (medium)* — кабелна или безжична връзка — която директно свързва комуникиращите компютри. Виртуалната мрежа не притежава такава директна връзка. Вместо това се създава тунел през обществена мрежа — обикновено Интернет — и двата комуникиращи компютъра се свързват към мрежата, както е показано на Фигура 16-1.

Фигура 16-1 *VPN връзката създава тунел през обществена мрежа, например през Интернет.*



Данните се изпращат по обществената мрежа по начин, който емулира връзка от тип „от точка до точка". Това се постига чрез *капсулиране* на данните. По-нататък в тази глава, в секцията „Процесът на капсулация", ще разгледаме как действа този процес. Засега е нужно само да знаете, че VPN ви позволява да създавате логическа мрежа, която е независима от местоположението и от възможността за установяване на директна физическа връзка.

Частна мрежа

Компонентът „частна" от виртуалната частна мрежа е обусловен от криптирането на данните по време на тяхното пътуване през обществената мрежа. Некриптираните данни могат да бъдат изпратени през тунел (изграден с помощта на един от тунелните протоколи, разгледани по-късно в главата), но строго погледнато, по този начин се създава само виртуална мрежа, а не виртуална частна мрежа.

Тъй като данните са криптирани, те остават частни (конфиденциални), макар че се предават по обществена мрежа. Това е важно, защото пакетите, пътуващи по Интернет, са предразположени към прихващане по време на тяхното предаване през всеки възел (сървър), който се намира по пътя между предаващия и приемащия компютър. Когато данните са криптирани, дори ако бъдат прихванати по пътя, те не могат да бъдат прочетени, при условие че този, който ги е прихванал, не разполага с ключа за криптиране. Криптирането ще разгледаме по-детайлно в секцията „Сигурност на VPN" по-нататък в тази глава.

Как работи VPN

VPN може да бъде конфигурирана да работи по dialup връзка, или може да бъде конфигурирана като връзка от типа маршрутизатор-маршрутизатор, която използва маршрутизатори със специално заделени Интернет връзки, например линии T1. Можете да създавате VPN връзка по заявка между маршрутизатори. При този тип връзка отговарящият маршрутизатор има посветена Интернет връзка, а извикващият маршрутизатор използва dialup Интернет връзка.

В следващите секции ще обясним как се изгражда VPN тунел и в какво се състои вградената поддръжка на VPN връзки, предоставяна от модерните операционни системи.

Прокопаване на тунела

Тунелът, създаден в една VPN връзка, реално представлява само логическа връзка от точка до точка, която поддържа автентикация и криптиране на данни от едната крайна точка на тунела до другата.

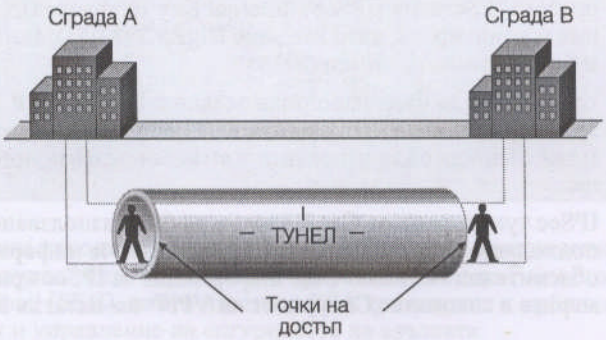
Да предположим, че вашата организация има две сгради, разположени от двете страни на улицата, една срещу друга. Служителите често се налага да пътуват от едната сграда до другата, за да свършат различна работа. За да стигнат до другата сграда, те могат просто да излязат навън, да пресекат улицата и да влязат през входната врата на другото здание. Това може да бъде сравнено с маршрута, който се изминава в една *обществена мрежа*. В обществената мрежа бизнес данните се изпращат по обикновена Интернет връзка, например като атачмънт. Файлът може да бъде изпратен с помощта на електронна поща по Интернет или посредством публичен FTP сървър.

Сега да предположим, че искате да засилите безопасността на служителите от различни въздействия, докато се придвижват от едната сграда до другата, или пък не искате те да бъдат наблюдавани от хора от обществото по време на техните пътувания. Един начин за постигане на това е да прокопаете *частен тунел* под земята от едната сграда до другата. Сега вече имате ситуация, аналогична на виртуалната частна мрежа.

Тъй като не искате хора от обществото да влизат в тунела и да преминават между сградите, може да направите врати във всеки от двата края на тунела, които могат да бъдат отключвани само с помощта на карти с ключ, издавани единствено на упълномощени служители. Тези ключови карти са подобни на процеса на идентификация на потребител, който иска да изпраща данни по VPN връзка, след което или му давате, или му отказвате достъп.

За нещастие, ако някой се промъкне в тунела, той би могъл все пак да заговори служителите, докато преминават напред назад. Можете да решите този проблем (макар и на висока цена), като построите едноместни превозни средства, които се заключват отвътре и превозват служителите през тунела. Това е аналогично на криптирането на данните за защитата им от прихващане по маршрута, както е показано на Фигура 16-2.

Фигура 16-2 *Тунелът предлага частен начин за пренасяне на хора и данни от една точка до друга.*



В следващите секции ще разгледаме процеса на капсулация и характеристиките на два типа тунелиране: Слой 2 и Слой 3.

Процесът на капсулация

Тунелирането скрива оригиналния пакет във вътрешността на нов пакет. За извършване на маршрутизация през тунела, адресът на *крайната точка на тунела* се задава в хедъра на външния (новия) пакет, който се нарича *хедър на капсулацията*. Адресът на крайното местоназначение се намира вътре в хедъра на оригиналния пакет. Когато пакетът достигне до зададената крайна точка на тунела, хедъра на капсулацията се снема. Сега оригиналният пакет може да бъде доставен до крайното местоназначение. Тунелирането е просто термин, използван за описание на капсулацията, която представлява процесът на маршрутизация и декапсулация.

Тунелите могат да бъдат изграждани на различни слоеве на стандартния мрежов модел. В следващите секции ще видим как действа тунелирането в Слой 2 (каналният слой на референтния OSI модел) и Слой 3 (мрежовия слой на референтния OSI модел).

Тунелиране от Слой 2

VPN мрежите често използват тунелни протоколи, които работят в каналния слой. Тези протоколи осигуряват виртуална връзка от една точка до друга. Протоколът Point-to-Point Tunneling Protocol (PPTP) работи на това ниво.

Друг тунелен протокол от каналния слой е Layer 2 Forwarding (L2F), който може да осигурява тунелиране по ATM и Frame Relay, защото не зависи от Internet Protocol (IP). За разлика от PPTP, един L2F тунел може да поддържа повече от една връзка. Cisco Systems разработи технологията L2F, а L2F се поддържа от Internetwork Operating System (IOS), използвана от маршрутизаторите на Cisco. В допълнение продуктите на Nortel и Shiva също поддържат L2F. Най-новият тунелен протокол, който работи на това ниво, е Layer 2 Tunneling Protocol (L2TP), който комбинира елементи на PPTP и L2F. Тези протоколи са разгледани по-детайлно във втората половина на тази глава, в секцията „VPN протоколи".

Тунелиране от Слой 3

Тунели могат да бъдат създавани в мрежовия слой и по този начин да осигуряват IP-базирани виртуални връзки. Тези връзки работят чрез изпращане на IP пакети, капсулирани във вътрешността на специфицирани от Internet Engineering Task Force (IETF) протоколни обвивки (protocol wrappers). Обвивките използват IPSecurity (IPSec), Internet Key Exchange (IKE) и методи за автентикация и криптиране, като Message Digest 5 (MD5), Data Encryption Standard (DES) и Secure Hash Algorithm (SHA).

IPSec може да бъде използван заедно с L2TP; L2TP изгражда тунела, а IPSec криптира данните. В този случай IPSec работи в *транспортен режим*. IPSec може също да бъде използван в *тунелен режим*, при който той осигурява тунела.

IPSec тунелиране от Слой 3 може да бъде използвано в ситуации, в които не е подходящо използването на L2TP. За повече информация вижте следващата обяснителна бележка. Още информация за IPSec криптирането можете да намерите в секцията „Сигурност на VPN" по-нататък в тази глава.

IPSec тунелиране

Важно е да се разбере разликата между VPN мрежите, които използват L2TP за тунелиране и IPSec за криптиране, и VPN мрежите, които използват IPSec в режим на тунелиране.

Една важна разлика е тази, че IPSec може да капсулира само IP пакети. L2TP може да осигурява капсулиране на Internetwork Packet Exchange (IPX) пакети и на пакети на други протоколи по IP мрежа.

Някои шлюзове не поддържат VPN мрежи, базирани на L2TP или PPTP, като в този случай за осигуряване на тунела може да бъде използван IPSec. IPSec тунелите обикновено работят от шлюз до шлюз.

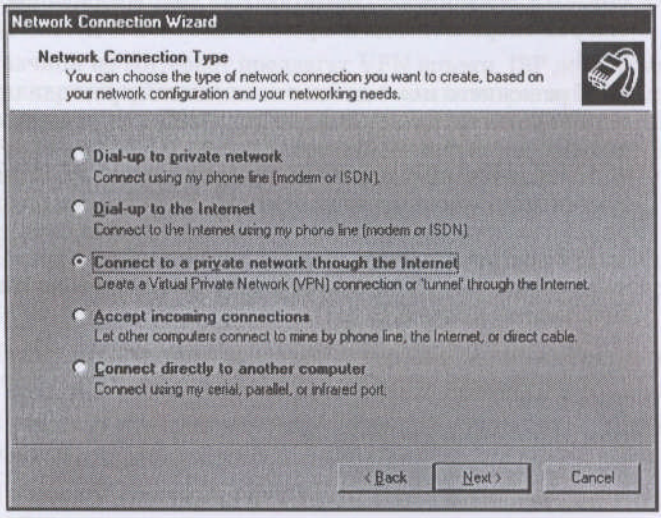
Поддръжка на VPN мрежи от операционната система

Модерните операционни системи включват вградена поддръжка за изграждане на виртуална частна мрежа. Това ви позволява да създавате връзка към VPN сървър толкова лесно, колкото е изграждането на една dialup връзка.

Операционните системи на Microsoft – Windows 95, Windows 98, Windows NT и Windows 2000 – могат да функционират като VPN клиенти, използващи вградените компоненти. Windows 9x и Windows NT поддържат PPTP, а Windows 2000 поддържа използването на PPTP или L2TP.

Потребителите на Windows 2000 използват съветник, който ви превежда през стъпките за инсталиране на VPN връзка, както е показано на Фигура 16-3.

Фигура 16-3 *Network Connection Wizard на Windows 2000 улеснява инсталирането на VPN връзка.*



Linux поддържа използването на IPSec и PPTP. В допълнение можете да създадете „псевдо тунел“ като изпълнявате протокола Point-to-Point Protocol (PPP) през Secure Shell (SSH), който използва RSA технология с публичен ключ за автентикация и управление на сигурността на връзката.

Когато се използва заедно със софтуер на независими производители или с хардуерни решения, виртуалната частна мрежа може да бъде използвана практически с всяка операционна система, а VPN мрежите могат да функционират между различни платформи, точно както при отдалечен достъп.

Защо да използваме виртуална частна мрежа?

Дефинирахме виртуалната частна мрежа като начин за комуникация между два компютъра (или две мрежи), отдалечени една от друга, чрез използване на обществена мрежа. Но не казахме защо може да предпочетете да направите това. В края на краищата бихте могли просто да инсталирате сървър за отдалечен достъп и да накарате потребителите да набират мрежата по dialup връзка. Това ще игнорира обществената мрежа и съображенията за сигурност, които я придружават.

В някои случаи dialup сървърът наистина би могъл да постигне същата цел, както VPN. Но при много други обстоятелства виртуалната мрежа има определени предимства пред услугата на dialup сървъра за отдалечен достъп (RAS).

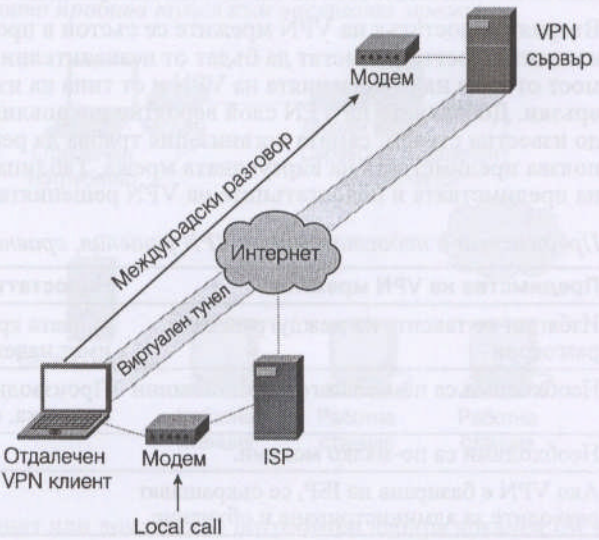
В следващите секции ще разгледаме предимствата и недостатъците на VPN мрежите и dialup мрежите, след което ще обясним някои общо разпространени сценарии за тяхното реализиране.

Сравнение между VPN и Dialup мрежи: предимства и недостатъци

Да вземе предвид ситуациите на отдалечен достъп, които разгледахме в Глава 15. Много служители работят като телекомютъри, вземат работа вкъщи и се нуждаят от достъп до корпоративната мрежа след работно време или искат да бъдат свързани, докато са на път. Тези служители могат да установяват dialup връзка към сървър за отдалечен достъп, но какво ще стане, ако живеят извън областта за набиране или пътуват до друг град или щат? Таксите за междуградски разговори могат да направят отдалечения достъп до мрежата неприемливо скъп.

VPN решението може да спести значителни разходи при този сценарий. Ако корпоративната мрежа е свързана към Интернет и служителят има достъп до локален доставчик на Интернет услуги (ISP), връзката може да бъде установена без плащане на такси за междуградски разговори. В много градове работят ISP доставчици, които могат да осигурят на пътуващите потребители телефонни номера за локален достъп. Потребителят трябва само да набере локалния номер на ISP доставчика и след това да установи тунел през Интернет до LAN мрежата на компанията, която обикновено има специална Интернет връзка, както е показано на Фигура 16-4.

Фигура 16-4 *Използването на VPN позволява на потребителя да избере локален ISP, вместо да провежда междуградски (или международен) разговор до корпоративната LAN.*



VPN мрежите могат да спестят пари чрез редуциране на броя на необходимите телефонни линии. Ако множество потребители искат да осъществяват достъп до мрежата едновременно чрез dialup връзки, компанията ще трябва да задели отделни телефонни линии и модеми за всяка връзка. Но ако същите тези потребители осъществяват достъп до мрежата с помощта на VPN, на организацията е достатъчна само една връзка към Интернет. Намаляването на броя на телефонните линии може да доведе до големи икономи всеки месец.

Някои доставчици на Интернет предлагат VPN връзки. ISP доставчиците осигуряват и поддържат връзката; това намалява административните разходи от страна на компанията, тъй като работата се извършва от ISP. Тези ISP-базирани VPN мрежи може дори да транспортират данните с помощта на гръбначната мрежа на ISP (вместо по Интернет) в качеството на „обществена мрежа".

Ето предимствата на виртуалната частна мрежа пред dialup достъпа:

- VPN мрежите спестяват разходите за междуградските разговори, когато отдалечените потребители се намират извън областта за набиране на локални номера.
- VPN мрежите изискват по-малко телефонни линии за осигуряване на отдалечен достъп до множество потребители едновременно.
- VPN мрежите изискват по-малко хардуерно оборудване, например банки от модеми.
- VPN мрежите, базирани на ISP, редуцират цените за администриране и обучение.

Разбира се, VPN решенията също имат недостатъци. Първо, и двата края на връзката трябва да имат Интернет връзка, за да изградят VPN. Това може да бъде проблем, ако единият или двата края имат ненадеждна Интернет връзка. Например даден потребител, който иска да осъществи достъп до корпоративна-

та мрежа от вкъщи, може да открие, че неговия ISP сървър е изключен за техническа поддръжка. Това би му попречило да използва VPN за свързване към LAN мрежата на организацията; от друга страна при директната dialup връзка към LAN, надеждността на ISP доставчика няма да бъде проблем.

Вторият недостатък на VPN мрежите се състои в проблемите, свързани с производителността. Те могат да бъдат от незначителни до съществени, в зависимост от типа на реализацията на VPN и от типа на използваните Интернет връзки. Добавянето на VPN слой вероятно ще повлияе на производителността до известна степен; самата организация трябва да реши дали си струва да използва предимствата на виртуалната мрежа. Таблица 16-1 представя обобщение на предимствата и недостатъците на VPN решенията.

Таблица 16-1 *Предимства и недостатъци на VPN решения, сравнени с Dialup решения*

Предимства на VPN мрежите	Недостатъци на VPN мрежите
Избягват се таксите на междуградските разговори	И двата края на връзката трябва да имат надеждна Интернет връзка
Необходими са по-малко телефонни линии	Производителността често е по-ниска, отколкото при dialup връзка
Необходими са по-малко модеми.	
Ако VPN е базирана на ISP, се съкращават разходите за администриране и обучение.	

Сценарии на изграждане на VPN мрежи

Виртуалните частни мрежи могат да бъдат използвани по няколко начина, в зависимост от нуждите на компанията. Повечето често използвани VPN мрежи са реализирани за една от следните цели:

- За осигуряване на отдалечен достъп до мобилни служители или такива, работещи от вкъщи.
- За осигуряване на *екстранет* мрежа, до която да имат достъп служители, клиенти и партньори.
- За осъществяване на контакт между два офиса в различни местоположения без за целта да се изгражда специална директна връзка.

В следващите секции ще разгледаме всяка от тези ситуации, начините за реализиране на мрежата и за гарантиране на най-добра конфиденциалност.

VPN мрежи за отдалечен достъп

Използването на VPN за осигуряване на отдалечен достъп до отделни потребители е най-простият сценарий за изграждане – като концепция. Реализацията може да бъде усложнена от такива фактори, като използвани операционни системи и протоколите, инсталирани от страната на клиента.

VPN клиентът трябва да може да използва протоколите, поддържани от VPN сървъра (тунелни, мрежови и транспортни), и протоколите за криптиране, използвани от сървъра. Например не-Microsoft клиентите могат да изградят VPN към сървър за отдалечен достъп с Windows 2000 с помощта на PPTP, но ако връзката трябва да бъде сигурна, клиентът трябва да може да използва протокола Microsoft Point-to-Point Encryption (MPPE).

След инсталиране на конфигуриране на компонентите на VPN, се установява връзката, както е показано на Фигура 16-5.

Фигура 16-5 *Мобилният или домашният потребител набира ISP, за да установи Интернет връзка, през която пробива тунел към частната мрежа.*

1. Мобилният или домашният потребител набира локален ISP и влиза с потребителски акаунт, за да изгради Интернет връзката. (Ако клиентът използва наета (посветена) или „винаги включена“ Интернет връзка, например DSL или кабелен модем, тази стъпка не е необходима).
2. След установяване на Интернет връзката, клиентът извиква сървъра за отдалечен достъп, конфигуриран да приема VPN връзки (използвайки IP адреса на отдалечения сървър); това действие изгражда тунела.
3. Потребителят се автентицира в частната мрежа и му се дава достъп.

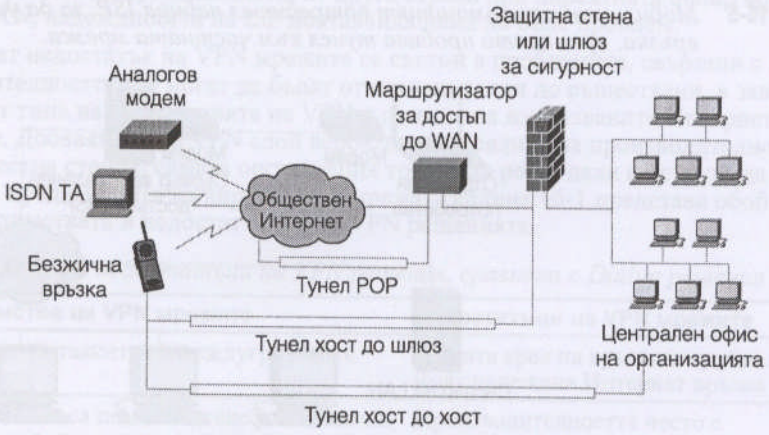
Вариант на този сценарий работи в обратния ред, при който потребител със специализирана връзка може да конфигурира домашен компютър като VPN сървър и след това да се свърже към него от офиса за достъп до файловете, съхранени на домашния компютър.

Виртуален частен екстранет

Този сценарий включва превръщането на част от LAN мрежата на организацията, наречена екстранет, в достъпна за отдалечени потребители по VPN връзка. Екстранет може например да съхранява материали за техническа поддръжка за клиенти или общо използвани бизнес документи за бизнес партньорите.

Важен проблем е защитата на останалата част от вътрешната мрежа от външен достъп. Създаването на отделна подмрежа за екстранет мрежата и поставянето на останалата част от LAN мрежата зад защитна стена може да осигури такава сигурност, както е показано на Фигура 16-6.

Фигура 16-6 *Вътрешната мрежа може да бъде защитена от външен достъп чрез реализиране на защитна стена.*



Обикновено потребителите на екстранет осъществяват достъп до данни през Web браузър, затова в подмрежата с връзка към VPN се инсталира Web сървър. Също така там може да бъдат разположени и файлови сървъри.

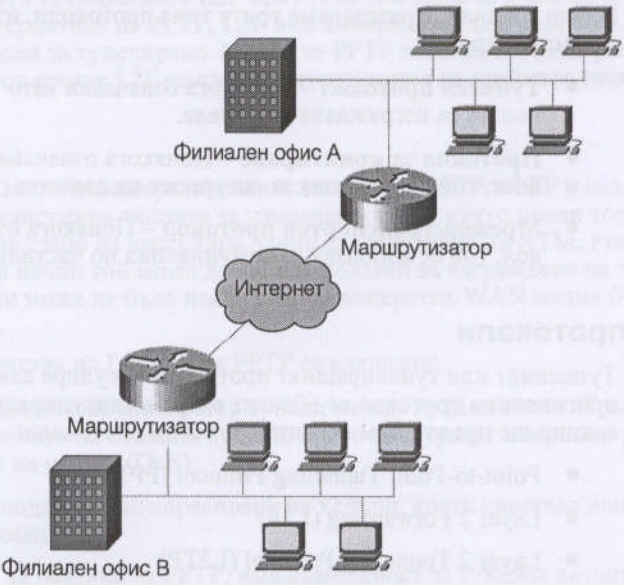
Съществуващите и перспективните стандарти улесняват организациите да използват по екстранет общи данни и приложения, например групуер за разработване на проекти в сътрудничество. Тези перспективни стандарти са следните:

- **Hypertext Markup Language (HTML)** – Позволява споделянето на документи през всеки Web браузър. Потребителите не е нужно да имат конкретна програма за текстообработка или друга програма, за да отварят файловете.
- **Extensible Markup Language (XML) и Commerce XML (cXML)** – Подобно на HTML, тези езици предлагат междуплатформена съвместимост.
- **Open Buying on the Internet (OBI)** – Създава стандарти за транзакции на електронната търговия (e-commerce).

VPN връзки между филиални офиси

При създаването на VPN връзки между офиси на филиали се използва виртуална частна мрежа за свързване на двата офиса във VPN конфигурация маршрутизатор-маршрутизатор. Тази конфигурация се нарича също *шлюз-шлюз*. VPN сървърът може да действа като маршрутизатор с разрешено IP препращане (foewarding), както е показано на Фигура 16-7.

Фигура 16-7 *VPN от тип маршрутизатор-маршрутизатор свързва два филиални офиса.*



LAN мрежата във всеки филиален офис има маршрутизирана връзка към Интернет. Тази връзка може да бъде набирана при необходимост (dial on demand) или постоянна. При връзката с набиране при необходимост, маршрутизаторът, инициращ връзката, използва dialup Интернет връзка. Маршрутизаторът, който се извиква, трябва да има посветена (постоянна) Интернет връзка и трябва да бъде конфигуриран за приемане на връзки от вида набиране при необходимост. На извикващия маршрутизатор се конфигурират две връзки с набиране при необходимост – едната за набиране на ISP и другата за свързване към VPN. Ако и двата маршрутизатора имат постоянни връзки към Интернет, VPN връзката може да бъде установена и оставена непрекъснато открита, ако е необходимо.

VPN връзки от типа маршрутизатор-маршрутизатор могат да бъдат конфигурирани така, че единият маршрутизатор да действа като клиент и да инициира връзката, а другият да функционира като VPN сървър. Това е еднопосочна връзка и представлява добър избор за постоянни връзки. Друга опция е двупосочната връзка, при която всеки от маршрутизаторите може да инициира връзката. В този случай и двата маршрутизатора трябва да имат постоянна връзка към Интернет и трябва да бъдат настроени като LAN и WAN маршрутизатори.

СЪВЕТ При сценария маршрутизатор-маршрутизатор, маршрутните таблици и на двата маршрутизатора трябва да бъдат конфигурирани с необходимите маршрути, за да препращат пакети през връзката. Маршрутите могат да бъдат добавени ръчно или може да бъде използван протокол за динамична маршрутизация, ако интерфейсът набиране при необходимост има постоянна връзка.

Може да бъде използван софтуер от сорта на vpnd (VPNdaemon) за свързване на две локални мрежи, използващи Linux или FreeBSD. За защита на данните, преминаващи през връзката, се използва алгоритъмът за криптиране Blowfish.

VPN протоколи

В тази секция ще разгледаме трите типа протоколи, използвани във виртуалните частни мрежи:

- **Тунелен протокол** – Понякога означаван като VPN протокол, той се използва за изграждане на тунела.
- **Протокол за криптиране** – Понякога означаван като протокол за сигурност, той се използва за сигурност на данните.
- **Мрежов/транспортен протокол** – Понякога означаван като LAN протокол, той се използва за комуникация по частната мрежа.

Тунелни протоколи

Тунелният или тунелиращият протокол капсулира данните така, че хедърите на оригиналния протокол се обвиват вътре в капсулиращите хедъри. В следващите секции ще представим следните тунелни протоколи:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP)
- IPSec
- Secure Shell (SSH) и Secure Shell 2 (SSH2)
- Crypto IP Encapsulation протокол (CIPE)

PPTP

PPTP на Microsoft е установен стандарт, който реално представлява разширение на протокола за връзка PPP, който се използва за изграждане на WAN връзка по връзка с отдалечен достъп. Ето как работи той:

1. PPTP капсулира PPP фрейм, който може да бъде IP, IPX или NetBEUI пакет, във вътрешността на Generic Routing Encapsulation (GRE) хедър. Също така се добавя IP хедър за осигуряване на IP адресите на източника и местоназначението. Адресът на източника е този на VPN клиента, а адресът на местоназначението е този на VPN сървъра.
2. Данните в оригиналната датаграма обикновено са криптирани, за да не могат да бъдат прочетени от неоторизирани лица. VPN мрежите на Microsoft използват протокола MPPE (описан по-долу в тази секция) заедно с PPTP за осигуряване на сигурни комуникации.

PPTP-linux е клиентски софтуер, който се изпълнява на Linux и UNIX машини. Той им позволява да установяват връзка към PPTP сървъри. Софтуерът на PPTP сървъра (наречен PoPToP) е достъпен за Linux, Sun Solaris, FreeBSD и други реализации на UNIX. Той поддържа Windows клиенти, както и PPTP-linux клиенти, и се разпространява като фрийуер.

Macintosh клиенти могат да се свързват към Windows PPTP сървъри с помощта на софтуер на независимо производители, като Network Telesystems TunnelBuilder.

L2F

Cisco разработи технологията L2F през 1996 г. и включи в нея своя софтуер IOS. Като алтернатива на PPTP, L2F има възможност да използва ATM и Frame Relay протоколи за тунелиране. Макар че PPTP изисква IP, за да работи, L2F не изисква. В допълнение L2F осигурява автентикация на крайните точки на тунела.

L2TP

Microsoft и Cisco комбинираха възможностите на PPTP и L2F и създадоха L2TP. L2TP капсулира данните за изпращане по IP, както прави това и PPTP. Но L2TP може също да капсулира данни за изпращане по ATM, Frame Relay и X.25. По този начин той може да бъде използван за изграждане на тунел през Интернет, или може да бъде използван по конкретна WAN медия без необходимост от IP.

Някои предимства на L2TP пред PPTP са следните:

- L2TP поддържа множество тунели между крайни точки. Това позволява създаването на отделни тунели, които осигуряват например различни качества на услуга (QoS).
- L2TP поддържа компресиране на хедъри, което спестява допълнителната информация.
- L2TP, за разлика от PPTP, има възможност за тунелна автентикация.
- L2TP работи по не-IP интермрежи, използващи ATM или Frame Relay виртуални вериги.

IPSec

IPSec може да бъде използван за криптиране на данни, които текат през тунел, изграден от друг протокол, например от L2TP. (Този аспект разглеждаме в секцията „Протоколи за криптиране“.) Той може да бъде използван също за изграждане на тунел, когато действа в режим на тунелиране. В режим на тунелиране IPSec можа да бъде конфигуриран за защита на данните или между два IP адреса, или между две IP подмрежи.

Както научихте в Глава 14, „Защита на мрежата“, IPSec може да използва един или и двата протокола: Authentication Header (AH) и Encapsulating Security Payload (ESP).

В следващите секции ще разгледаме всеки протокол и ще обясним как IPSec може да взаимодейства с различни операционни системи.

AH тунелен режим

AH тунелният режим, използван сам по себе си, не осигурява криптиране на данните, които пътуват през тунела. Но той интегритета на данните, като верифицира, че те не са пипани. Също така той автентицира изпращача. При AH не може да бъде направена никаква промяна на адреса на източника или местоназначението от момента, в който пакетът напусне началната точка на тунела.

ESP тунелен режим

При ESP тунелен режим адресите на първоначалния източник и крайното местоназначение се съдържат в оригиналния (капсулиран) IP хедър. Външният хе-

дър обикновено съдържа адресите на шлюзове. ESP тунелът криптира данните с помощта на алгоритмите DES или 3DES.

Когато се използва ESP, външният IP хедър не е защитен и неговият интегритет не е гарантиран. За постигане на криптиране и автентикация, както и на интегритет на целия пакет, можете да използвате заедно AH и ESP.

Интероперативност на IPSec

Операционната система Windows 2000 включва вградена поддръжка на IPSec. IPSec е стандарт на IETF, който работи също с Linux, Unix, Macintosh и други операционни системи, поддържащи фамилията протоколи IP. IPSec автентикацията може да бъде направена по различни методи, като предварително споделени ключове, Kerberos и сертифициращи услуги.

FreeS/WAN за Linux представлява реализация на IPSec, която е с отворен сорс, и е достъпна за сваляне по Интернет.

SSH/SSH2

Първоначално SSH беше предназначен за осигуряване на сигурна алтернатива на UNIX r команди, като rsh, rlogin и rcp. SSH употребява силно криптиране и автентикация. SSH2 се разви в сигурен тунелен протокол, който може да се използва за създаване на VPN мрежа, работеща под операционни системи Linux или UNIX. Типът на VPN мрежата, изградена с помощта на SSH2, се нарича *VPN на ниво верига*. SSH клиентски софтуер е достъпен също за Windows.

ЗАБЕЛЕЖКА Шлюзовете на ниво верига работят в сесийния слой на референтния OSI модел. Когато данните се предават до отдалечен компютър по шлюз на ниво верига, изглежда, че произлизат от самия шлюз. Това ви позволява да замаскирате информация за защитени мрежи.

SSH може да бъде инсталиран на защитната стена, а тунелът да бъде изграден от SSH клиент с dialup Интернет достъп до защитната стена. Защитната стена може да бъде конфигурирана да препраща трафика до сървър по вътрешната мрежа. Това е просто и лесно решение за VPN връзки, ако не се цели постигане на висока производителност. SSH изисква акаунт за логване, затова е най-подходящ за такива ситуации, като разрешаване на няколко доверени служители да се свържат към малка офис мрежа от вкъщи.

CIPE

CIPE представлява драйвер за ядрото на Linux, който може да бъде използван за осигуряване на сигурен тунел между две IP подмрежи. Данните се криптират в мрежовия слой на референтния OSI модел. Това се нарича криптиране на ниско ниво. То има предимство пред криптирането на високо ниво, защото не трябва да бъдат правени никакви промени на приложния софтуер, когато две мрежи се свързват с помощта на VPN. Освен това CIPE е по-прост и по-ефикасен от IPSec.

Протоколи за криптиране

След изграждане на тунела, данните трябва да бъдат криптирани, за да може връзката да бъде считана за сигурна. Протоколите, използвани за криптиране на данните, са следните:

- MPPE
- IPSec криптиране
- VPNd криптиране
- SSH криптиране

MPPE

MPPE се използва с PPTP-базирани VPN връзки (или PPP dialup връзки) и може да използва криптиращ алгоритъм с 40, 56 или 128-битов ключ. 128 битовият ключ (силно криптиране) може да бъде използван само в САЩ и Канада.

IPSec криптиране

IPSec използва DES или 3DES за криптиране на данните в L2TP тунел. Използването на комбинация от криптографско-базирани алгоритми и ключове прави информацията много сигурна. Алгоритъмът на Дифи-Хелман позволява сигурен обмен на споделен ключ без изпращане на самия ключ по мрежовата връзка.

VPNd криптиране: Blowfish

VPNd за Linux използва криптиращ алгоритъм Blowfish. Това е 64-битов алгоритъм, който може да използва ключове с променлива дължина, от 32 бита до 448 бита. Той е бърз и безплатен: реално неговият сорс код е достъпен. Съществуват няколко варианта, включително GOLDFISH, DOSFISH и TWOFISH.

SSH криптиране

UNIX SSH използва криптография с публичен ключ за криптиране на данните. Обърнете се към Глава 14 за повече информация относно начина на работа на публичния ключ.

LAN протоколи

За да могат VPN клиентът и сървърът да комуникират, те трябва да имат общ стек от мрежови/транспортни протоколи. Това може да бъде TCP/IP, но не е задължително да бъде само той. Дори при PPTP връзка, която изисква IP, приложен в обществената мрежа, през която се изгражда тунелът, частната мрежа може да използва IPX/SPX или дори NetBEUI за комуникации.

Сигурност на VPN

Сигурността на VPN има три компонента:

- Автентикация
- Авторизация
- Криптиране

Тази многокомпонентна реализация осигурява аспекта „частна“ на виртуалната частна мрежа. Ще разгледаме накратко всеки компонент в следващите секции.

Автентикация

Автентикацията на VPN клиента включва проверката за истинност на самоличността на машината и на потребителя, който инициира VPN връзката. Автентикацията може да бъде осъществена на нивото на машината. Например, когато една VPN връзка, базирана на Windows 2000, използва IPSec за L2TP VPN, сертификатите на машините се обменят като част от изграждането на IPSec асоциация за сигурност.

Потребителят може да бъде автентициран с помощта на един от няколкото метода за автентикация, като Extensible Authentication Protocol (EAP), Challenge Handshake Authentication Protocol (PAP) или Shiva PAP (SPAP), изброени в Глава 15.

Авторизация

Авторизацията означава зададените ограничения, на базата на които на едни потребители се предоставя достъп до VPN, а на други се отказва.

Криптиране

За защита на данните във VPN мрежи могат да бъдат използвани най-различни технологии за криптиране. Много VPN реализации ви позволяват да изберете метода на криптиране, който трябва да бъде използван. Криптирането осигурява сигурност за данни, които пътуват по VPN. Без тази сигурност данните биха могли лесно да бъдат прихванати, докато се движат по обществената мрежа.

Проблеми на производителността на VPN

Проблемите на производителността, свързани с VPN мрежите, могат да бъдат категоризирани по два начина: общи проблеми на производителността и проблеми, които са специфични за конкретни VPN реализации.

Повечето сериозни проблеми на производителността се дължат на самата природа на Интернет. Често възникват прекъсвания на достъпността от регионален и всеобщ характер. Тежкият трафик (например по време на голямо Интернет събитие или големи новини) могат да предизвикат забавяния и забивания на системите. Освен това отделни ISP доставчици могат да се сблъскат с изключвания на сървъри, които афектират стотици или дори хиляди потребители.

Технологията на VPN може също да доведе до различни количества допълнителни (служебни) данни, които намаляват производителността. VPN мрежи на ниво вериги не могат да постигнат скоростта на виртуалните мрежи на ниво мрежа. Когато използвате обществената мрежа за установяване на връзката, ще жертвате елемента на контрол, който имате при директна входяща dialup връзка.

Типове VPN мрежи

VPN мрежата може да бъде реализирана софтуерно или хардуерно. В следващите секции накратко ще разгледаме всяка от тези реализации, разликите между тях и начина, по който могат да бъдат комбинирани за повишаване на сигурността.

Софтуерно-базирани VPN

Софтуерно-базираните VPN мрежи включват използването на тунелните протоколи, които разгледахме. Тази категория може да бъде разделена допълнително на продукти на независими производители и VPN софтуер, поддържан от операционната система. Очевидното предимство на последните е тяхната цена. Няма допълнително заплащане, а VPN решенията, включени в модерните операционни системи като Windows 2000, са достатъчни за нуждите на много организации.

VPN софтуерните продукти на независимите производители обикновено предлагат допълнителни възможности и разширяват използваемостта на VPN, като често осигуряват повече опции за сигурност и в някои случаи по-лесно реализиране. Някои софтуерно-базирани VPN мрежи ви позволяват да предавате данни в тунела на базата на протокола или IP адреса. Този тип филтриране обикновено не е достъпен при хардуерно-базираните продукти.

Продуктите на независимите производители включват Safeguard VPN, Checkpoint SVN (Secure Virtual Networking) и NetMAX VPN Suite за Linux.

Хардуерно-базирани VPN

Хардуерно-базираните VPN мрежи се произвеждат от компании като Shiva, 3Com и VPNet Technologies. Поддръжката на VPN е вградена в маршрутизаторите на Cisco, както и в маршрутизаторите на други компании. NTS Tunnel-Builder осигурява сигурни VPN комуникации за Windows, NetWare и Macintosh. Такива производители като Raptor Systems предлагат VPN мрежи, базирани на защитни стени, които са комбинирани със средства за сигурност.

Хардуерните VPN мрежи могат най-общо да бъдат категоризирани в следните групи:

- **Базирани на маршрутизатори** – Базираните на маршрутизатори VPN решения представляват маршрутизатори с възможности за криптиране. Те предлагат по-добра производителност на мрежата и като цяло са полесни за инсталиране и използване.
- **Базирани на защитна стена** – Решенията, базирани на защитна стена, осигуряват допълнителни мерки за сигурност, например силна автентикация и детайлно логване. Базираната на VPN защитна стена може да извършва също преобразуване на адреси. Производителността може да бъде проблем, макар че в някои реализации хардуерните криптиращи процесори решават този проблем.

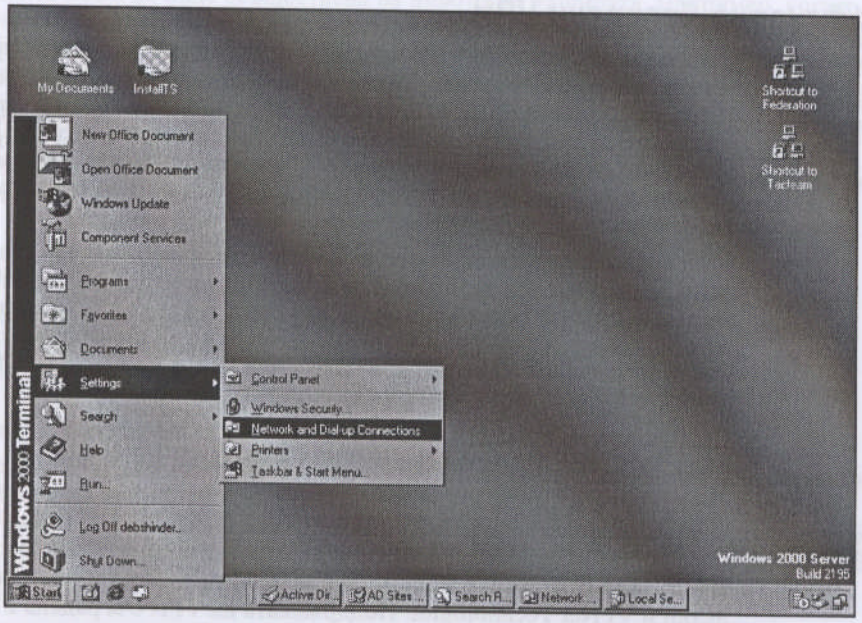
Конфигуриране на VPN връзка

Конфигурирането на една VPN връзка зависи от типа на VPN и от това, дали реализацията е хардуерна или софтуерна.

В тази секция ще представим стъпките за инсталиране на VPN връзка в Windows 2000.

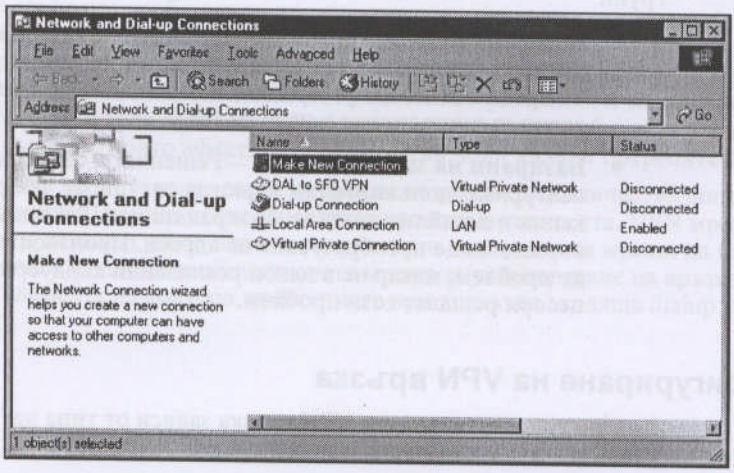
Стъпка 1 Изберете Network and Dialup Connections от менюто Start, както е показано на Фигура 16-8.

Фигура 16-8 *Създаването на VPN връзка в Windows 2000 започва с опцията Network and Dialup Connections.*



Стъпка 2 Щракнете двукратно върху иконата Make New Connection в прозореца Network and Dialup Connections, както е показано на Фигура 16-9.

Фигура 16-9 *Щракнете върху иконата Make New Connection, за да създадете VPN връзка.*



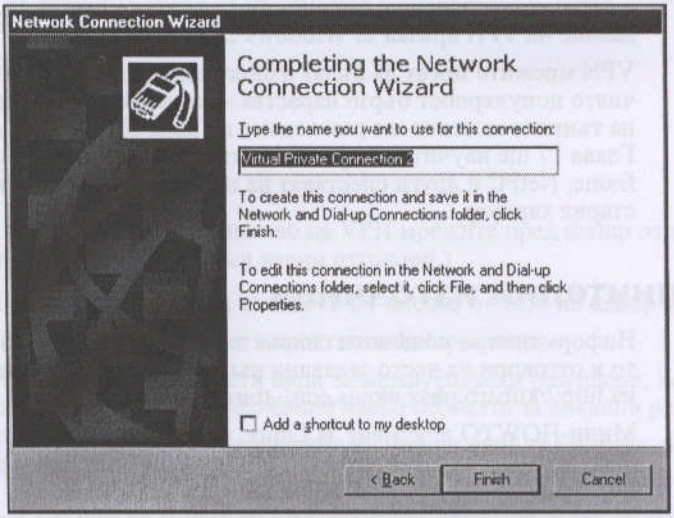
Стъпка 3 Вашето действие стартира съветника Network Connection Wizard. Селектирайте третата опция. Свържете се към частна мрежа по Интернет, както е показано на Фигура 16-3.

Стъпка 4 След това ще ви бъде поискано да зададете следното:

- **Дали да бъде набиран сървър за установяване на първоначална връзка към Интернет** – Ако изберете да направите това, ще ви бъде поискано да конфигурирате или да изберете dialup връзка. Ако имате посветена (постоянна) Интернет връзка, трябва да селектирате „do not dial".
- **Името на хост или IP адрес на VPN сървъра** – Въведете информацията за компютъра или маршрутизатора, към който искате да изградите VPN връзката. Спомнете си, че имената на хостове трябва да бъдат преобразувани в IP адреси, затова обикновено е най-добре да въведете IP адреса, ако го знаете. Това намалява сложността на връзката.
- **Дали връзката трябва да бъде достъпна за всички потребители, които споделят компютъра, или само за потребителя, който я създава** – По подразбиране е достъпно за всички потребители да използват връзката.
- **Дали да разрешите Internet Connection Sharing (ICS), за да споделите VPN връзката по мрежата** – Това позволява на други компютри в LAN да споделят връзката посредством Network Address Translation (NAT). Забележете, че IPSec не работи с NAT.

Стъпка 5 Когато очертаете вашия път през страниците на съветника, отговаряйки на тези въпроси, ще бъдете подканени да въведете име на връзката, както е показано на Фигура 16-10.

Фигура 16-10 *След като завършите съветника, ще ви бъде поискано име на VPN връзката.*



След като VPN връзката е конфигурирана на компютъра на клиента, свързването към VPN мрежата е лесно. Просто щраквате двукратно върху иконата на връзката в Network and Dialup Connections и ще бъдете подканени да въдете

потребителско име и парола за отдалечения VPN сървър. Windows 2000 създава връзката.

Използвайки подразбиращата се конфигурация (при тип VPN, зададен на Automatic), софтуерът открива дали VPN сървърът използва PPTP или L2TP и след това използва подходящия протокол за изграждане на тунела.

По всяко време можете да конфигурирате или промените свойствата на връзката (например кои протоколи за автентикация трябва да бъдат използвани).

Обобщение

В тази глава разгледахме концепцията на изграждане на виртуални частни мрежи в техните различни форми. Научихте, че VPN ви позволява да се свързвате към и да комуникирате сигурно с отдалечена частна мрежа чрез „тунелиране" през Интернет или друга обществена мрежа. Разгледахме начините за реализиране на VPN мрежи – по dialup връзки или като VPN мрежи маршрутизатор-маршрутизатор.

Научихте, че тунелирането може да се осъществява в различни слоеве на референтния OSI модел. Разгледахме тунелирането в Слой 2, извършвано от PPTP и L2TP, и тунелиране в Слой 3, което се използва от IPSec. Научихте също, че повечето модерни операционни системи могат да бъдат използвани за създаване на VPN връзки – или чрез вградената в тях поддръжка на VPN, или чрез софтуер от независими производители.

Разгледахме ценовите предимства на виртуалните частни мрежи, протоколите, използвани при създаването на VPN мрежи, и общоприетите LAN протоколи, използвани за комуникации между VPN клиент и сървър.

Разгледахме сигурността на VPN и трите компонента, включени в нея: автентикация, авторизация и криптиране. След това представихме проблемите на производителността на VPN и разгледахме два типа VPN: софтуерно-базирани и хардуерно-базирани. Главата завършихме с демонстрация на стъпките за създаване на VPN връзка за Windows 2000 VPN клиент.

VPN мрежите могат да бъдат използвани също съвместно с друга технология, чиято популярност бързо нараства – мрежите за тънки клиенти. Концепцията на тънките клиенти ще разгледаме в Глава 17, „Мрежи за тънки клиенти". В Глава 17 ще научите как решения като Microsoft terminal services, Citrix Metaframe, NetPC и други спестяват на организацията пари и вливат нов живот на стария хардуер.

Допълнителни източници

Информация за пощенски списък за VPN мрежи и за начина за абониране, както и отговори на често задавани въпроси за VPN мрежите, можете да намерите на http://kubarb.phsx.ukans.edu/~tbird/vpn/FAQ.html.

Мини-HOWTO документ за Linux, който разглежда детайлно инсталирането на VPN мрежа, базирана на SSH/PPP, може да бъде отворен от http://sunsite.unc.edu/LDP/HOWTO/mini/VPN.html.

За да научите повече за NTS TunnelBuilder и TunnelMaster, вижте www.nts.com/products/index.html.

Кратък доклад за виртуалните частни мрежи може да бъде намерен на www.corecom.com/html/vpn.html.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Какъв е процесът на обвиване на хедъра на един протокол във вътрешността на друг?

a Криптиране
b Капсулация
c Автентикация
d Авторизация

2 Какво е името на логическата връзка от точка до точка, която поддържа автентикация и криптиране на данни от една крайна точка до друга по обществена мрежа?

a Тунел
b Протокол
c Шлюз
d Връзка за отдалечен достъп

3 Кое от следните е истина за PPTP? (Изберете всички верни отговори.)

a PPTP работи заедно с IPSec за осигуряване на сигурна VPN връзка.
b PPTP е базиран на PPP линк протокола.
c PPTP е тунелен протокол от Слой 3.
d PPTP работи съвместно с MPPE за осигуряване на сигурна VPN.

4 Кое от следните може да работи или в транспортен, или в тунелен режим?

a PPTP
b L2F
c IPSec
d SSH

5 Кое от следните е предимство на VPN мрежите пред dialup отдалечения достъп? (Изберете всички верни отговори.)

a Производителността на VPN е по-висока от тази на dialup връзката.
b VPN е по-надеждна от директната dialup връзка.
c VPN може да ви спести пари за междуградски разговори, когато се свързвате от местоположение извън областта за локални разговори.
d При VPN сървърът не е нужно да има по една телефонна линия и модем за всеки едновременно работещ отдалечен потребител.

6 Какво е името на частта от LAN мрежата на компанията, която е направена достъпна за избиране от такива страни, като служители, клиенти или партньори?

a интермрежа

b интранет

c екстранет

d подмрежа

7 За кои от следните цели често се използва VPN от тип маршрутизатор-маршрутизатор?

a За осигуряване на достъп на клиентите до LAN мрежата на организацията.

b За осигуряване на достъп на служителите до мрежата на организацията от вкъщи.

c За осигуряване на достъп на служителите до мрежата на организацията, докато са на път.

d За осигуряване на връзка между два офиса в различни местоположения.

8 Кое от следните е истина както за PPTP, така и за L2TP?

a И двете могат да бъдат използвани за създаване на VPN тунел.

b И двете могат да използват ATM или Frame Relay за тунелиране.

c И двете работят в каналния слой на референтния OSI модел.

d И двете поддържат множество тунели между крайни точки.

9 Кое от следните представлява драйвер на ядрото на Linux, който се използва за осигуряване на сигурен тунел между две IP подмрежи?

a TunnelBuilder

b CIPE

c CIR

d VPN daemon

10 Кое от следните е истина за хардуерно-базираните VPN решения? (Изберете всички верни отговори.)

a Хардуерно-базираните VPN мрежи могат да бъдат разделени на две категории: базирани на маршрутизатори и базирани на защитни стени.

b Хардуерно-базираните VPN мрежи като цяло са по-лесни за инсталиране и използване от софтуерно-базираните VPN мрежи.

c Хардуерно-базираните VPN мрежи като цяло са по-евтини от софтуерно-базираните VPN мрежи.

d Хардуерно-базираните VPN мрежи могат да извършват преобразуване на адреси.

Глава 17

Мрежи за тънки клиенти

При положение че частните мрежи заемат първото място в списъка на популярните технологии, мрежите за тънки клиенти не могат да останат далеч зад тях. „Тънки" означава „икономични", най-малкото когато става въпрос за спестяване на хиляди долари за хардуер с помощта на продукти като Microsoft Terminal Services, Citrix MetaFrame и базирана на Java компютърна обработка.

Решенията за тънки клиенти осигуряват начин за използване на иначе остаряло или маломощно компютърно оборудване за изпълнение на популярни приложения, които нормално изискват много пъти повече памет и процесорна мощ. Тази утилизация се извършва чрез инсталиране на софтуер за тънък клиент, който позволява на клиента да се свързва към сървър (обикновено наричан *терминален сървър*) и да изпълнява програми във виртуален десктоп. Потребителят работи на своята настолна машина, но същинската обработка се извършва на сървъра; екранът се пречертава и след това се предава по мрежата.

В тази глава ще представим предимствата и недостатъците от използването на решения за тънки клиенти, предназначени за редуциране на общата цена на собствеността (total cost of ownership — TCO) в работни среди на големи корпорации и малки бизнес организации. Първо ще представим общата концепция на мрежите за тънки клиенти и след това ще разгледаме начините за тяхното реализиране.

По-специално ще разгледаме опциите за клиентски хардуер: Windows-базирани терминали (WBT), Net PC-та, мрежови компютри, обикновени настолни PC-та и хендхелд или палмтоп компютри. След това ще разгледаме хардуерните и софтуерните съображения при вземане на решение за изграждане на тънки клиенти.

После ще обсъдим най-често използваните протоколи за комуникация между тънкия клиент и сървъра, и ще хвърлим поглед на следните често използвани решения за тънки клиенти:

- Терминални услуги на Microsoft (Microsoft terminal services, включващи както Windows NT Terminal Server Edition, така и Windows 2000 Terminal Server)
- Citrix Winframe и MetaFrame
- X Window терминали
- Web-базирана компютърна обработка и Java desktop

Накрая ще разгледаме доставчиците на приложни услуги (application service provider – ASP) и философията „Интернет е операционна система", която стои в основата на такива инициативи, като новата стратегия Microsoft .Net на Microsoft.

Да започнем с дефиниране на термините и връщане малко назад в историята.

Еволюция на мрежите за тънки клиенти

През последните две десетилетия традиционните настолни операционни системи стават все по-мощни, по-сложни и по-гладни за ресурси. В Таблица 17-1 е дадено сравнение между типичните системни конфигурации за популярните операционни системи на Microsoft. Лявата колона на таблицата показва годините от времето на превръщането на DOS в Windows и следващата еволюция на Windows последователно във Windows 9x, Windows ME, Windows NT и Windows 2000.

Таблица 17-1 *Сравнение на системните конфигурации за операционни системи на Microsoft*.*

Година на издаване	Операционна система	Типична конфигурация на паметта	Типична скорост на процесора
1981	MS-DOS	64 KB	4.77 MHz
1985	Windows	1–2 MB	12 MHz
1990	Windows 3.0	2–4 MB	16–25 MHz
1994	Windows NT	16 MB	33–66 MHz
1995	Windows 95	16 MB	66–90 MHz
1996	Windows NT 4.0	32 MB	100–133 MHz
1998	Windows 98	32 MB	200–233 MHz
2000	Windows ME	32-64 MB	333–450 MHz
2000	Windows 2000	64-128 MB	333–450 MHz

* Тези конфигурации не представляват минималните изисквания към системата. Въпросните операционни системи може да се изпълняват и на по-маломощен компютър. Числата индицират „типичната" системна конфигурация, необходима за постигане на приемлива производителност. Също така забележете, че тези числа са за настолни версии (например Windows NT Workstation, Windows 2000 Professional), а *не* за сървърните продукти.

Това бързо нарастване на изискванията към типичната система (понякога означавана като *bloatware*) имат нежелателен страничен ефект: милиони машини, все още в напълно функционално състояние, се превръщаха в „остарели" при излизането на нови „дебели" операционни системи. Това означава, че тези машини трябва да бъдат ъпгрейдвани или заменени с по-мощни машини; всяка от тези опции може да увеличи разходите на организация, която има стотици или хиляди компютри. Старите системи често се разкарваха по складовете, даряваха се на нетърговски организации, които се радваха, че могат да правят нещо с по-малки машини и по-стар софтуер, или пък се разкомплектоваха за резервни части.

Разбира се, организациите биха могли да продължават да използват своите стари системи и софтуер, или да изберат една от компактните операционни системи, като изданията „тънък Linux", които се побират на една дискета и работят с 4 MB RAM. Но тези решения са неприемливи за повечето бизнес организации,

защото изискват стандартизирани приложения като Microsoft Word и интероперативност със софтуера на клиенти и партньори.

Мрежите за тънки клиенти предлагат начин за използване на тези „остарели" машини и позволяват на техните потребители да се радват на предимствата на модерните операционни системи и приложения. Концепцията на тънкия клиент е проста: Използване на маломощни компютри и терминали за десктоп, докато повечето от работата се извършва от мощен сървър.

Тази концепция не се различава много от света на мейнфрейм компютрите, в който един голям, мощен, централизиран процесор осигурява приложения и данни на множество потребители. Затвори ли се пълният кръг при компютрите? По какво PC реализацията на технологията на тънък клиент се различава от мейнфрейм модела? На тези въпроси ще отговорим в следващите секции.

Технологията тънък клиент

Как работи технологията тънък клиент? При типичната реализация на тънък клиент, софтуерът, работещ на сървъра, предава потребителския интерфейс по мрежата до клиента. Настолната машина, която изпълнява клиентски софтуер, предава въвежданата от потребителя информация (т.е. натисканията на клавиши и щракванията с мишката) обратно към сървъра. Обработката се извършва на сървъра.

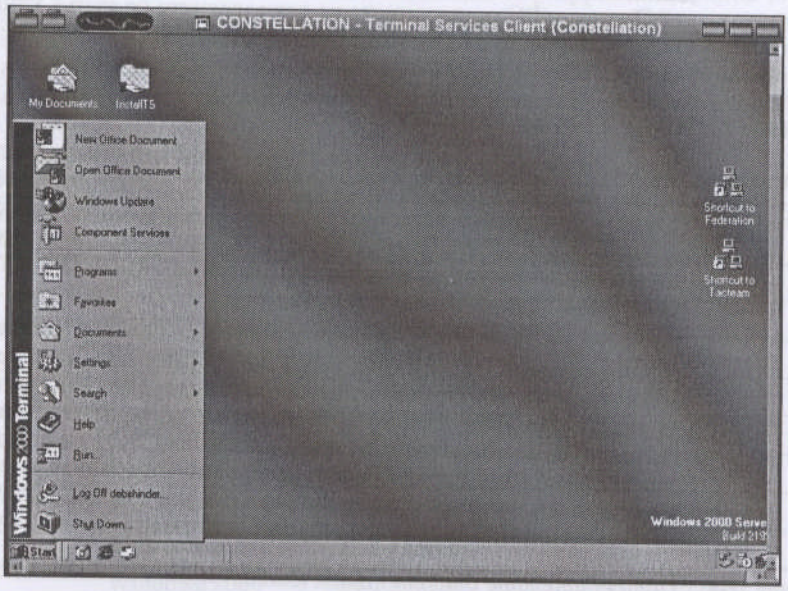
Потребителите се логват на сървъра с индивидуални предварително конфигурирани акаунти; поради това всеки потребител има уникален десктоп, приспособен така, че да отговаря на неговите нужди. Множество потребители могат да влязат едновременно, но потребителите не знаят за сесиите на другите. Инсталирани са многопотребителски приложения, така че всеки потребител може да поддържа свои предпочитани настройки. Потребителите могат да осъществяват достъп до техни собствени локални устройства, да записват на дискети, да печатат по LPT порт и т.н., както е илюстрирано на Фигура 17-1.

Фигура 17-1 *Потребителите от тип тънък клиент могат да имат техни собствени уникални десктопи и настройки.*

Предимства на технологията тънък клиент

Очевидно предимство на модела тънък клиент е спестяването на разходи. Тъй като клиентският софтуер по принцип се изпълнява на разнообразие от различни платформи, това решение предлага висока гъвкавост. Например потребителите могат да работят в десктоп на Windows 2000, в което се изпълняват без проблем приложения като Office 2000, като за целта използват за клиентска машина X386 PC или компютър Macintosh.

Фигура 17-2 *Потребителите могат да изпълняват Windows 2000 в терминален режим, като използват по-старо и по-маломощно оборудване.*



Тази опция често е по-евтина от ъпгрейда на всички настолни компютри до хардуер, на който се препоръчва да се изпълнява Windows 2000. Сървърът за приложения трябва да бъде сравнително мощно PC. Например Microsoft препоръчват за техния Microsoft Terminal Server минимална конфигурация процесор Pentium или еквивалентен с минимум 128 MB RAM, с допълнителни 12–21 MB за всеки потребител. Но модерният сървърен хардуер, който има възможност да поддържа много клиенти, също струва хиляди долари по-малко от мейнфрейм компютрите.

Друго предимство е възможността на потребителя да използва все пак завършена компютърна система за достъп до сървъра за приложения и в същото време да запазва локалната процесорна мощност на компютъра за случаи, в които е по-добре конкретно приложение да бъде изпълнено локално. Терминалите, които обикновено се използват за достъп до мейнфрейм компютри, нямат собствена процесорна мощност. Макар че има шлюзови продукти, като System Network Architecture (SNA), които могат да се използват за осигуряване на достъп на PC до мейнфрейм приложения, тези продукти са скъпи.

За мрежовия администратор инсталирането на тънки клиенти предлага много предимства, в това число:

- Ъпгрейдът на приложения е опростен, защото ъпгрейдвате само многопотребителското приложение на сървъра, вместо да ъпгрейдвате стотици или хиляди отделни десктоп машини.
- В някои случаи може да се спестят пари от такси за лицензи на софтуера. Проверете внимателно лицензните договори; може пак да бъдете задължени да закупите отделен лиценз за всеки потребител на приложението, макар че приложението се изпълнява от терминал.
- Защитата от вируси се извършва на сървъра. Десктопите на потребителите могат да бъдат заключвани, за да се попречи на потребителите да осъществяват достъп до флопидисковите устройства; Също така могат да бъдат използвани WBTs, които нямат флопидискови устройства. В допълнение могат да бъдат зададени политики, които да ограничават потребителите при инсталиране на софтуер.
- Когато се използват терминали, данните се записват на сървъра. Данните могат по-лесно да бъдат осигурявани и архивирани, когато са на сървъра. Ако се използват PC-та, разполагате с опцията да разрешите на потребители да съхраняват данни локално.
- Можете да контролирате терминалните сесии. Контролът може да бъде разширен дори върху поемане на управлението на курсора на потребителя или прекратяване на сесията.
- Могат да бъдат задавани потребителски политики. Тези политики управляват десктопите и действията на потребителите, които могат да бъдат различни от политиките, прилагани към използването на локалната машина.

Протоколи за тънки клиенти

Решенията за тънки клиенти зависят от три компонента: от хардуера (сървърен и клиентски), от софтуера (сървърен и клиентски) и от протоколите, които разрешават на сървъра и клиента да комуникират един с друг.

В тази секция ще разгледаме протоколите, използвани от Windows Terminal Services и Citrix MetaFrame – два от най-популярните продукта за тънки клиенти. Протоколите, използвани от тези продукти, са *Remote Desktop Protocol (RDP) и Independent Computing Architecture (ICA).*

ЗАБЕЛЕЖКА Microsoft разработи RDP за използване с терминални услуги без допълнения на Citrix. ICA върви с Citrix MetaFile.

Също така ще разгледаме протоколите X и XDM, които се използват от X Window терминали в средата на UNIX/Linux. След това ще се спрем на протокола Remote Frame Buffer (RFB) и ще разгледаме протоколите Bootstrap Protocol (BOOTP), Dynamic Host Configuration Protocol (DHCP) и Trivial File Transfer Protocol (TFTP). Всички те се използват за зареждане на мрежови PC и други бездискови работни станции.

RDP

RDP е включен в Windows NT Terminal Server Edition и в Windows 2000 Terminal Services, които пък се включват във всички продукти Windows 2000

Server. RDP работи с WBT, изпълнявани под операционната система Windows CE, и с PC-та, работещи под Windows for Workgroups 3.11, Windows 95, Windows 98, Windows NT и Windows 2000.

RDP поддържа мрежовия транспортен протокол TCP/IP и работи по LAN или WAN връзки и dialup връзки за отдалечен достъп. RDP също позволява печат на локален LPT порт и поддържа пренасочване на клипборда, което се изразява във възможността за изрязване и вмъкване (cut и paste) между терминал и приложения на локалната система.

ICA

Citrix доставя ICA както с Winframe, така и с MetaFrame, а ICA добавя по-пълна функционалност към Windows Terminal Services. Например там, където RDP работи само с Windows клиенти, Citrix поддържа DOS, Macintosh и няколко версии на UNIX и Linux. Той поддържа също използването на Internet Explorer и Netscape браузъри като терминални клиенти. Това разширява терминалните услуги до практически всички среди на персонални компютри.

ICA работи с разнообразни клиентски устройства. В допълнение към PC-тата, той поддържа мрежови компютри, WBT-та, мрежови терминали на Wyse Technology, палмтоп и хендхелд компютри, TV устройства и мрежови домакински електроуреди.

Друго предимство на софтуера Citrix е, че поддържа IPX, SPX и NetBEUI, в допълнение към TCP/IP. ICA се изпълнява върху LAN, WAN, dialup и директни серийни връзки. За разлика от RDP, ICA поддържа 16-битов звук, така че потребителите могат да възпроизвеждат в терминала .wav, .mid и .avi файлове. Протоколът Citrix позволява пренасочване на COM портове и безпроблемно ремапване на устройства.

X и X Display Manager Communication Protocol (XDMCP)

Протоколът X може да разрешава комуникация между X сървър и X терминал. Той донякъде е ограничен като протокол за тънък клиент, защото няма интелигентната сигурност и възможности за компресиране, достъпни при други протоколи. X не се счита за подходящ за WAN връзки, защото му липсват възможности за оптимизация, макар че вариантът, наречен Low-Bandwidth X (LBX) се опитва да реши този проблем.

Протоколът XDM Communication Protocol (XDMCP) се използва от XDM за управление на разпределението на сървърни ресурси на потребители с X терминали.

RFB

Протоколът RFB осигурява на потребителите на терминали отдалечен достъп до графичен потребителски интерфейс (GUI). Той е многоплатформен протокол, който работи с X, Windows и Macintosh.

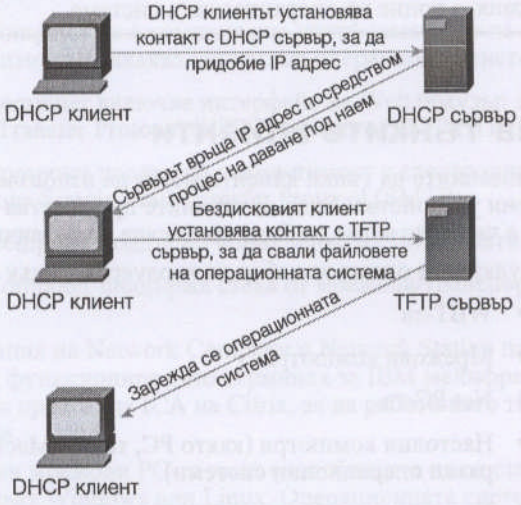
RFB се квалифицира като протокол за тънък клиент, защото неговите изисквания към клиента са минимални. RFB сървърът извършва цялата обработка, а състоянието на сесията се запазва, ако клиентът прекрати връзката. Когато клиентът отново установи връзка към сървъра, интерфейсът е в същото състояние, в което е бил при прекратяването на връзката. Например всички приложения,

които са изпълнявани, продължават да се изпълняват, и всички документи, които са били отворени, пак са отворени на екрана. Това е в сила независимо дали потребителят осъществява достъп до сървъра от същата клиентска машина, или от друга такава.

BOOTP, DHCP и TFTP

BOOTP, DHCP и TFTP не са протоколи за тънки клиенти, но се използват в среда с тънки клиенти, за да позволят на изключително тънък клиент, например бездискова работна станция, да се свързва към мрежата и да зарежда операционната система. Този процес е показан на Фигура 17-3.

Фигура 17-3 *Протоколът BOOTP или DHCP, заедно с TFTP, могат да бъдат използвани за свързване на бездискова работна станция към мрежата и зареждане на операционната система.*



Сега клиентът може да комуникира по мрежата

Първоначално BOOTP беше разработен като начин за контакт на бездискови станции към мрежата, така че да може да им бъде задаван IP адрес. След това те могат да комуникират със сървър с помощта на TFTP, за да заредят файловете на операционната система в паметта. BOOTP сървърът задава IP адреси на компютрите, конфигурирани като BOOTP клиенти.

DHCP е по-нова и по-интелигентна форма на BOOTP. DHCP сървърът може да бъде използван за даване под наем на адреси на DHCP клиентски машини. Процесът, с помощта на който DHCP прави това, е разгледан в Глава 8, „Мрежови протоколи и услуги".

След като тънкият клиент има IP адрес, той може да комуникира по мрежата, използвайки TCP/IP. Това му позволява да установява контакт с TFTP сървър, на който се съхраняват файловете за зареждане (boot image). TFTP сървърът използва протокола User Datagram Protocol (UDP), който е по-бърз от TCP. Бездисковите PC-та могат да зареждат разнообразни операционни системи от boot сървър, включително Windows или Linux. Тъй като нямат твърд диск, обичай-

ните файлове за зареждане на операционната система се записват в ROM. Кодът за първоначално зареждане се записва предварително в ROM чип на мрежовата интерфейсна карта, което отговоря на стандарта Preboot Execution Environment (PXE).

PXE

Intel и други производители използват PXE, за да осигурят код за начално зареждане (bootstrap) за тънки клиенти и други машини, които трябва да зареждат операционна система от мрежата. PXE кодът е записан на ROM чип, който може да бъде включен или към мрежовата карта, или като част от самия тънък клиент.

PXE картата изпраща съобщение до сървъра, за да обяви, че е съвместима с PXE, а след това сървърът, който има възможност за работа с PXE, връща информация, позволяваща на клиента да влезе в контакт с boot сървъра, където се съхранява копие на операционната система.

Хардуер на тънките клиенти

Реализациите на тънки клиенти могат да използват много различни типове хардуерни устройства. Едно от главните предимства на обработката с тънък клиент, е че лесно може да бъде пренасяна на различни платформи.

Популярните опции за избор на хардуер за тънък клиент са следните:

- WBT-та
- Мрежови компютри
- Net PC-та
- Настолни компютри (както PC, така и Macintosh, работещи под разнообразни операционни системи)
- Хендхелд и палмтоп компютри

Сега ще разгледаме накратко всяка опция и начина, по който се интегрира в инфраструктурата на корпоративната мрежа.

WBT-та

Windows-базираните терминали са предназначени за осигуряване на Windows десктоп и Windows приложения на потребители посредством модела „обработка с тънък клиент". Повечето модели на WBT имат или терминален сървърен софтуер на Microsoft и RDP, или предварително зареден ICA клиент на Citrix; те са направени така, че да използват Windows CE или вградена NT операционна система.

WBT терминалите са по-евтини от пълноценните PC-та, при положение че потребителите могат да ги използват за изпълнение на повечето приложения, които се изпълняват на персонални компютри, работещи под Windows. Терминалът на WBT няма твърд диск, което намалява възможността потребителите да се сблъскват с вируси или да правят неоторизирани копия на данните на организацията. Друго предимство на бездисковите машини е, че кражбата е малко

вероятна. Тъй като устройствата са неизползваеми без мрежата, те не са много привлекателни за крадците.

Популярен разпространител на WBT терминали е Wyse Technology, която през 1995 г. беше първата компания на пазара на WBT терминали.

Мрежови компютри

Мрежовият компютър е разработен от Sun Microsystems в средата на 90-те години. IBM и Oracle също се присъединиха към тези усилия. Архитектурата Network Computer беше проектирана като истински тънък клиент, който се състоеше само от минимален хардуер, зареждащ операционна система от мрежата.

Network Computer осигурява Web интерфейс и виртуалната машина Java Virtual Machine (JVM), която осигурява гъвкавост. Спецификациите Network Computer се превърнаха в отворен стандарт, който включва следните основни характеристики:

- Network Computer не е компютърна платформа само на един производител. Не се изисква някаква конкретна операционна система.
- Network Computer включва интерфейс на Web браузър за обработка на Hypertext Transfer Protocol (HTTP) и Secure HTTP (HTTPS) заявки.
- Network Computer поддържа съвместимост с електронна поща с помощта на протокола Simple Mail Transfer Protocol (SMTP).
- Network Computer поддържа изпълнение на Java аплети.
- Network Computer поддържа стека от мрежови/транспортни протоколи TCP/IP.

Модерна реализация на Network Computer е Network Station на IBM. Това устройство може да функционира като терминал за IBM мейнфрейм компютри и може да използва протокола ICA на Citrix, за да работи като терминал за Windows приложения.

Много бездискови мрежови PC-та имат способността да се стартират от мрежата, за да изпълняват Windows или Linux. Операционната система се зарежда от мрежата. Например Sun Ray клиентът може да осъществява достъп до Java и Sun Solaris приложения, както и до NT приложения, изпълнявани на Sun Ray сървър с помощта на MetaFrame.

Net PC-та

Малко след представянето на Network Computer беше разработена и неговата алтернатива – *Net PC* – с общите усилия на Microsoft, Dell, Compaq и Hewlett Packard. Net PC-тата са базови PC-та с ниска процесорна мощност и малко памет, притежаващи възможности като Wakeup on LAN, която позволява да „събуждате" компютрите и да ги управлявате дистанционно дори ако те са изключени.

Тъй като е пълноценен компютър, Net PC може да изпълнява приложения локално и да продължава да функционира като самостоятелна машина, ако мрежата бъде прекъсната. Това е предимство пред терминалните устройства, чието зареждане зависи от мрежата.

Спецификациите на Net PC включват минимум 16 MB RAM, процесор Pentium на 100 MHz (или еквивалент) и Plug and Play (PnP) съвместимост, която под-

държа PnP идентификатори на устройства за всяко хардуерно устройство. Кутията трябва да може да се заключва, за да не се допусне потребителите да сменят компоненти, и трябва да има минимално потребителско въздействие при инсталиране и конфигуриране на устройства. Обикновено няма флопидисково устройство, няма CD-ROM устройство и няма разширителни слотове. Но за разлика от Windows-базираните терминали, Net PC-тата имат локални твърди дискове.

Настолни компютри

Един обикновен настолен компютър, включително най-съвременните модели, може да изпълнява клиента Microsoft Terminal Services или Citrix ICA клиентски софтуер, и да функционира като „дебел тънък клиент". Защо администраторът да се главоболи да инсталира това? Отговорът е, че инсталирането на приложения посредством терминален сървър има много предимства. То ви позволява да контролирате настройки и свойства, и лесно да обновявате приложенията на сървъра. Терминалният клиент се изпълнява подобно на всяко друго приложение от десктопа на PC-то, а в същото време могат да бъдат изпълнявани и локалните програми.

Клиентският софтуер може да бъде използван на DOS, Windows, Macintosh и UNIX/Linux машини. Това решение е особено полезно, ако имате потребители, които работят под не-Windows операционни системи, но които от време на време трябва да изпълняват Windows приложения.

Недостатък на използването на настолни компютри като терминални клиенти е намалената сигурност. Тъй като компютрите имат флопидискови устройства и CD-ROM устройства, потребителите лесно могат да направят пробив в сигурността, като инсталират неоторизирани програми или като копират данни по мрежата на преносима дискета. Но този риск може да бъде редуциран или елиминиран с помощта на политики за заключване на десктопа и ограничаване на действията на потребителите.

Най-тънките клиенти: Хендхелд PC-тата

С помощта на стартиране на клиент на терминални услуги за Windows CE върху хендхелд PC, можете да създадете мобилен WBT. При безжичните мрежови технологии тези преносими устройства могат да бъдат използвани за достъп до приложения и данни „в движение".

Преносимите терминали бяха въведени в болниците, за да осигуряват постоянен достъп до информацията за пациента при визитации. Безжичните хендхелд мрежови устройства ще разгледаме по-подробно в Глава 19, „Технологии на утрешния ден", в секцията „Универсална свързаност".

Софтуер за тънки клиенти

В тази секция ще разгледаме детайлно софтуера, използван за реализиране на решение с тънък клиент. По-специално ще разгледаме терминалните услуги (Terminal Services) на Microsoft, включени в продуктите Windows 2000 Server, допълнителния модул MetaFRame на Citrix за Windows NT 4.0 и Windows 2000, Winframe for Windows 3.51 и софтуера X Window за Unix/Linux. Също така ще разгледаме Web-базираната компютърна обработка и виртуалната машина JVM.

Терминални услуги на Microsoft

Microsoft издаде Terminal Server Edition на Windows NT 4.0, базиран на интегрираната технология на Citrix. В Windows 2000 терминалните услуги се включват във всички сървърни продукти (Windows 2000 Server и Datacenter Server) и вече не се изисква тяхното закупуване като „специално издание" на операционната система.

Както е описано в следващите секции, Windows 2000 Terminal Services могат да бъдат реализирани в един от следните два режима:

- Режим на сървър за приложения
- Режим на отдалечено администриране

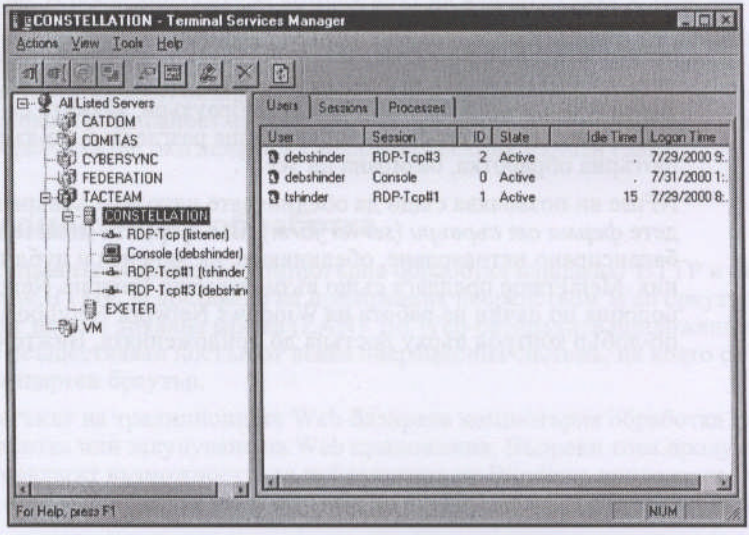
Терминалните услуги на Microsoft в режим на сървър за приложения

Когато е конфигуриран да бъде сървър за приложения, терминалният сървър на Windows 2000 функционира по традиционния модел на тънък клиент. Десктопът на Windows 2000 и Windows приложенията се доставят до клиентските машини, изпълняващи клиентския софтуера за терминални услуги.

Можете да създадете групи от потребители, които са специфични за терминални услуги, и профили на потребители, които се прилагат само за терминални сесии. Могат да бъдат зададени таймаути за изключване на потребителски сесии след зададен период от време. Потребителите трябва да имат валидни акаунти на сървъра или на мрежовия домейн, за да могат да влизат като терминални клиенти. Това ограничение дава повече сигурност.

Мениджърът на терминални услуги (Terminal Services Manager), който се намира на Windows 2000 сървъра, когато изпълнява терминални услуги, ви позволява да разглеждате и управлявате терминалните сесии. Вижте Фигура 17-4.

Фигура 17-4 *Терминалните сесии в Windows 2000 се управляват с помощта на Terminal Services Manager на сървъра.*



Възможността за отдалечен контрол позволява извършване на наблюдение на потребителските сесии. Можете да наблюдавате действията на избран потребител, или да поемете управление на сесията и входа от клавиатурата и действията с посочващото устройство (мишката). Това може да бъде полезно при отстраняване на проблеми от отдалечено местоположение или за демонстриране на правилните процедури на потребителите.

Терминалните услуги на Microsoft в режим на отдалечено администриране

Можете да използвате терминални услуги, за да се свържете към сървъра от някой десктоп и след това да управлявате сървъра от този десктоп. Това е добра алтернатива на софтуера на независими производители, като PCAnyware.

Когато терминалният сървър е в режим на отдалечено администриране, се прилагат някои ограничения:

- Само член на групата на администраторите може да се логва в терминала.
- Разрешени са само две едновременни връзки

Освен тези две ограничения, можете да изпълнявате програми, да управлявате десктопа и да правите всичко друго, което можете да правите и в режим на сървър за приложения.

Winframe/MetaFrame на Citrix

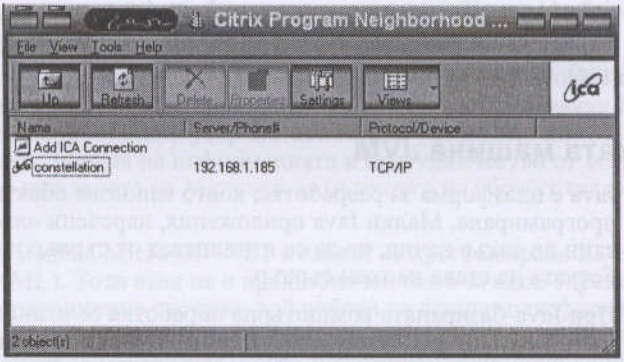
Citrix Winframe беше разработен за изпълнение под Windows NT 3.51 Server с цел осигуряване на функционалност на терминални услуги. По-новата версия на продукта на Citrix – MetaFrame, добавя допълнителни възможности за Windows NT 4.0 Terminal Server Edition и Windows 2000. Citrix също така осигурява MetaFrame за UNIX.

Тъй като Citrix използва протокола ICA, продуктът MetaFrame добавя функционалността, асоциирана с ICA. Тези функционалности разгледахме по-рано в тази глава. В хетерогенна мрежова среда, MetaFile може да свързва към терминалния сървър не-Windows клиенти.

MetaFrame 1.8 за Windows 2000 включва технологията на портал за приложения на Citrix, която се нарича NFuse. Тя ви позволява да интегрирате интерактивни приложения в стандартни Web браузъри, каквито са Netscape или Microsoft Internet Explorer. Тази концепция ще разгледаме по-късно в секцията „Компютърна обработка, базирана на Web“.

NFuse ви позволява също да обединявате няколко сървъра в група, за да създадете *ферма от сървъри* (*server farm*). Във фермата можете лесно да извършвате балансирано натоварване, обединяване на лицензи и публикуване на приложения. MetaFrame предлага също възможността Program Neighborhood, която е подобна по начин на работа на Windows Network Neighborhood и която ви дава по-добър контрол върху достъпа до приложенията. Вижте Фигура 17-5.

Фигура 17-5 *Citrix MetaFrame използва Program Neighborhood за управление на приложения и връзки.*



Системата X Window

X Window (често неправилно наричана X Windows) беше разработена в Масачузетския технологичен институт за осигуряване на графична прозоречна система за операционни системи UNIX (включително Linux).

X създава потребителска среда, подобна на Windows, OS/2, Macintosh OS и други графични операционни системи. Тя позволява едновременно визуализиране на множество приложения в отделни прозорци. Но X се различава от много GUI операционни системи по това, че е мрежов протокол; другите използват извиквания на програмни процедури.

X сървърът приема входна информация по мрежата и изпраща графичния дисплей обратно на клиента. Софтуерът на X клиента може да бъде изпълняван или на същия компютър, на който се намира софтуера на сървъра, или на друг компютър. В последния случай компютърът на клиента става X терминал.

Софтуерът на X сървъра и софтуера на клиента са достъпни за не-UNIX машини, предлагани от такива производители като Hummingbird. Продуктите включват Exceed – X клиент, базиран на Windows, и Exceed Web, който осигурява Web-базирана възможност за свързване на X клиент. Web-базираната компютърна обработка ще разгледаме в следващата секция на тази глава.

Web-базирана компютърна обработка

Web-базираните решения за компютърна обработка използват HTTP и скриптовия език HTML за доставяне на приложения посредством Web браузър по Интернет или по локална мрежа (LAN). До Web-базираните приложения може да бъде осъществяван достъп от всяка операционна система, на която се изпълнява стандартен браузър.

Недостатъкът на традиционната Web-базирана компютърна обработка е скъпата разработка или закупуване на Web приложения. Въпреки това продукти като Citrix предлагат възможността за публикуване на Windows приложения на Web сървър и ги прави достъпни за потребители посредством интерфейса на браузъра.

При публикуване на Citrix приложение, селектираните приложения се вграждат в Web сървъра и достъпът може да бъде ограничен на базата на потребителски или групов акаунт. Тъй като Web браузърът е относително малка програма и понеже цялата обработка се извършва на Web сървъра (който може от своя страна да осъществява достъп до сървъри за бази данни и сървъри за приложения), клиентът може да бъде „тънка" машина.

Виртуалната машина JVM

Java е платформа за разработка, която използва обектно-ориентиран език за програмиране. Малки Java приложения, наречени *аплети*, могат да бъдат написани по такъв начин, че да се изпълняват от сървър и по-голямата част от обработката да става на този сървър.

При Java-базираната компютърна обработка се изпълняват малки JavaScript аплети, които се стартират от сървъра и могат да бъдат изпълнявани на маломощен клиентски компютър или терминално устройство. Run-time средата създава JVM машина, в която се изпълняват аплетите. JVM машината може да бъде изпълнявана на платформи с различни операционни системи. Java поддържа многонишковост и компилиране от вида just-in-time (JIT) на програмите, което позволява висока производителност.

При компютърната обработка с Java кодът за приложението се сваля на клиента по заявка, където се съхранява в кеш или в динамичната RAM памет. Приложенията могат да бъдат изпълнявани в браузър, съвместим с Java, например в текущите версии на Netscape и Internet Explorer. Специализирани Java клиентски устройства могат да работят под прости Java операционни системи и JVM машина, която се съхранява в ROM или се зарежда по мрежата.

Главният недостатък на Java като решение за тънък клиент е ефектът върху пропускателната способност на мрежата при сваляне на приложенията при клиентите. Друг проблем е липсата на стандартизация; реализациите на Java на различните производители не са идентични.

ASP-та

Моделът ASP, в който приложенията се хостват от външна компания, представлява концепция, която е тясно свързана с компютърната обработка от тип тънък клиент. Доставчикът на услуги поддържа приложенията и ги прави достъпни до клиентите по високоскоростна мрежова връзка. Моделът ASP поддържа също лицензиране на софтуера и управлява проблемите по ъпгрейда и поддръжката.

ASP доставчиците могат да бъдат предпочетени от малки и средни бизнес организации, които е възможно да нямат ресурси за собствен IT отдел. Опцията е особено подходяща за Web-базирани услуги,като електронна търговия. Вместо да се купува софтуер, компанията го взема под наем от ASP доставчика. Много ASP доставчици използват Web-базирана компютърна обработка като платформа за доставяне на техните приложения.

Друго предимство на аутсорсинга на приложения са интелигентните мерки за сигурност, които могат да бъдат реализирани от центровете за данни, и отказоустойчивостта, осигурявана от техния редундантен хардуер.

Microsoft .NET

Microsoft .NET инициативата, като част от бизнес плана на компанията за новото хилядолетие, глътна големи инвестиции за нова, Интернет-базирана платформа за софтуер и услуги.

При Microsoft .NET данните и приложенията се съхраняват на сървъри, достъпни по Интернет. До тези сървъри може да бъде осъществяван достъп от всяко местоположение и всяко устройство. Такова разпределение на Web услуги позволява интегриране на информацията и сътрудничество от всяка точка в света. Това е виждането на Microsoft за бъдещето на обработката с персонални компютри.

Основата на модела Microsoft .NET е езикът за програмиране Extensible Markup Language (XML). Този език не е предназначен само за една определена платформа или операционна система; той работи на всички платформи и позволява разпространение на данните до голямо разнообразие от устройства, например безжични хендхелд устройства, които интегрират функционалност на телефон, пейджър и PC. Приложеният софтуер ще бъде предлаган на принципа на абонамента, подобно на услуга, и доставян по Интернет. Microsoft вече обяви плановете си за настолна платформа от следващо поколение, Windows .NET (по време на разработването с кодовото име „Whistler"), която е проектирана специално за тази ориентирана към Интернет работна среда.

Успехът на стратегията Microsoft .NET е още рано да бъде определен, но в бъдеще работата в мрежа вероятно ще играе нарастваща роля в компютърната обработка в бизнеса и у дома, т.е. във всекидневния ни живот.

Обобщение

В тази глава разгледахме концепцията на мрежите за тънки клиенти от няколко гледни точки. Научихте, че тънък клиент може да бъде маломощен компютър или терминал, който има входни устройства, екран и връзка към сървър, извършващ всички задачи по обработката.

Разгледахме предимствата на мрежите за тънки клиенти и протоколите, използвани за комуникация между тънък клиент и сървър за приложения. След това разгледахме хардуера на тънките клиенти, включващ WBT, Net PC и мрежовия компютър; научихме и как обикновени настолни системи се използват като тънки клиенти. Също така изследвахме използването на основен тънък клиент – хендхелд и палмтоп PC-тата, които се свързват към мрежата по безжични преносни среди и които изпълняват олекотени варианти на операционните системи, като Windows CE.

След това разгледахме софтуера за тънък клиент, включващ Windows NT 4.0 Terminal Server Edition и Windows 2000 с терминални услуги, вградени в сървърните продукти. Разгледахме и допълнителните модули Citrix Winframe и MetaFrame за Windows, софтуера X Window System, Web базираната компютърна обработка и JVM като решение за тънък клиент.

Накрая хвърлихме поглед върху перспективните технологии, каквато е ASP, и разгледахме най-новата разработка – Интернет стратегията Microsoft .NET, инициирана от най-голямата софтуерна компания в света.

В последните няколко глави разгледахме много съществуващи технологии, но трябва да помним, че основата на всички тях е висококачествената производителност на мрежата. В следващата глава ще се обърнем към начина, по който можем да използваме инструменти за наблюдение, управление и отстраняване

на неизправности, за да поддържаме нормалната работа на нашите мрежи при пикова работоспособност, използвайки предимствата на тези решения с по-висока интелигентност.

Допълнителни източници

Връзки за информация по многобройни решения за тънки клиенти може да бъде открита на Web сайта на Manchester Thin Client Computing на адрес www.mcc.ac.uk/thin/links.htm.

Един добър ресурс за най-нова информация за решения за тънки клиенти е достъпна на Web сайта Thin Planet на адрес www.thinplanet.com.

Повече информация за Windows 2000 Terminal Services може да бъде намерена на www.microsoft.com/windows2000/guide/server/features/terminalsvcs.asp.

Вижте Web сайта на Citrix за повече информация относно MetaFrame за Windows NT, Windows 2000 и UNIX, на www.citrix.com.

За информация относно системата X Window вижте www.x.org.

Полезни материали за Java-базираната компютърна обработка са достъпни на www.empowermentzone.com/javacomp.txt.

Допълнителна информация за Интернет стратегията на Microsoft за двадесет и първи век може да намерите на www.microsoft.net/net.

Чудесен общ преглед на терминалните услуги съдържа книгата *Windows NT Terminal Server and Citrix MetaFrame* от Тед Харууд, публикувана от New Riders.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1. Кое от следните е предимство на PC-базираните решения за тънък клиент пред обработката с мейнфрейм компютри? (Изберете всички верни отговори.)
   - **a** PC-базираният сървър струва по-малко от мейнфрейма.
   - **b** PC-тата струват по-малко от мейнфрейм терминалите.
   - **c** PC-тата могат да изпълняват приложения локално в допълнение към изпълнението им от сървър.
   - **d** PC-базираните решения за тънък клиент нямат предимства пред обработката с мейнфрейм компютри.
2. Кое от следните е истина за компютърната обработка с тънък клиент?
   - **a** Всички потребители трябва да имат едни и същи настройки на сигурността и позволения за достъп.
   - **b** Използването на терминали прави по-трудно архивирането на данни.
   - **c** Можете да управлявате или да изключвате терминални сесии на потребители.

d Приложенията трябва да бъде ъпгрейдвани на всяка отделна клиентска машина.

3 Кой от следните протоколи за тънък клиент се използва, за да позволи на Macintosh или UNIX клиенти да осъществяват достъп до Windows терминален сървър?

a RDP

b ICA

c X

d DHCP

4 Кое от следните е истина за RDP? (Изберете всички верни отговори.)

a RDP поддържа печат на локален LPT порт.

b RDP поддържа IPX/SPX, NetBEUI и TCP/IP мрежови/транспортни протоколи.

c RDP разрешава пренасочване на COM портове.

d RDP разрешава пренасочване на клипборда.

5 Кой протокол се използва за управление на разпределянето на ресурси, притежавани от X сървър, на потребители на X терминали?

a X

b LBX

c XDMCP

d RFB

6 Какво е предназначението на PXE стандарта?

a PXE (Private X Exchange) се използва за комуникация между X сървър и Windows-базиран клиент.

b PXE (Preboot Execution Environment) е средство за осигуряване на код за начално зареждане на бездискови работни станции.

c PXE (Protocol for Extended Encapsulation) се използва за създаване на VPN връзка между тънък клиент и сървър.

d PXE (Private X Window Emulator) се използва за осигуряване на X интерфейс за Macintosh системи.

7 Кое от следните е истина за архитектурата Network Computer? (Изберете всички верни отговори.)

a Network Computer е нестандартна разработка и използва само операционната система Sun Solaris.

b Network Computer поддържа изпълнение на Java аплети.

c Network Computer поддържа протоколния стек TCP/IP.

d Network Computer включва интерфейс на Web браузър за обработка на HTTP и HTTPS заявки.

8 Кое от следните представлява режим, в който могат да работят терминалните услуги на Windows 2000?

a Режим на отдалечено администриране

b Режим на сървър за приложения

c Режим на локален достъп

d Режим на виртуална машина

9 Кое от следните е истина за Citrix MetaFrame? (Изберете всички верни отговори.)

a Citrix MetaFrame представлява добавъчен продукт за Windows 3.51.

b Citrix MetaFrame може да бъде използван за хостване на приложения на Web сървър, до които да се осъществява достъп с помощта на Web браузър.

c Citrix MetaFrame ви позволява да обединявате множество сървъри във ферма от сървъри.

d Citrix MetaFrame използва Application Neighborhood за управление на приложения и създаване на нови ICA връзки.

10 Кое от следните е истина за Java-базираната компютърна обработка?

a Java аплетите се изпълняват на сървъра и не трябва да бъдат сваляни на клиента.

b Java е стандартизиран език за програмиране и реализациите на всички производители са идентични.

c Виртуалната Java машина (JVM) може да бъде изпълнявана само на UNIX-базирани операционни системи.

d Java поддържа многонишковост и компилация от типа Lust in Time (JIT), които определят нейната висока производителност.

Глава 18

Инструменти за наблюдение, управление и отстраняване на неизправности

На този етап от вашето обучение вече е ясно, че компютърните мрежи — макар и прости като концепция — могат да бъдат доста сложни при изпълнение. Много неща могат да тръгнат неправилно, и като мрежов администратор трябва да бъдете подготвени да откривате, диагностирате и отстранявате проблеми с връзките.

Следвайки поговорката „един грам предвидливост струва колкото килограм лекарство", трябва редовно да наблюдавате мрежата, за да идентифицирате и коригирате потенциални проблеми. В корпоративна работна среда не е достатъчно само да свържете компютрите един с друг. Времето е важен фактор в днешния бизнес свят и от особена важност е оптимизирането на мрежата за постигане на най-висока възможна производителност. Достъпни са различни инструменти, които могат да ви помогнат да наблюдавате, управлявате и отстранявате неизправности в LAN и WAN среди. Те варират от прости TCP/IP помощни програми до интелигентни софтуерни пакети и хардуерни устройства на независими производители.

Но най-важният елемент е човешкият елемент. Мрежовите администратори понякога гледат на потребителите на мрежата като на врагове — хора, които не правят нищо, а непрекъснато се оплакват или създават конспирации, за да саботират перфектно работещите системи. Но винаги трябва да помните, че без мрежови потребители нямаше да има смисъл от съществуване на мрежата. Иначе казано, ролята на мрежовия администратор щеше да бъде излишна.

В тази глава ще разгледаме основите на анализирането и оптимизирането на производителността, управлението на мрежовите услуги и отстраняването на често срещани проблеми. След това ще обсъдим събирането на информация и помощните програми за отстраняване на проблеми, включени в комплекта протоколи TCP/IP. Накрая разглеждаме софтуерните и хардуерните устройства, които можете да използвате за наблюдение и управление на вашата мрежа.

Ще завършим главата, както и тази част на книгата, със списък на указания за решаване на проблеми, които ще ви помогнат да организирате процеса на отстраняване на проблеми.

Анализиране и оптимизиране на производителността на мрежата

Администрирането на компютърна мрежа често е тежка работа, свързана с високо натоварване. Това е в сила независимо дали сте част от голям отдел за техническа поддръжка на мрежа на голяма организация, или единствен администратор на локална мрежа на малка компания.

Тъй като мрежовият персонал не бездейства дълго, много администратори откриват, че действат в *реактивен (противодействащ)* режим; т.е. те са толкова заети за отстраняване на проблеми след тяхното възникване, че не могат да отделят време за реализиране на мерки, които ще възпрепятстват повторното възникване на тези проблеми.

Макар че допускаме, че вие (като администратор) може от време на време да действате в реактивен режим, той все пак е неефикасен и уморителен в дългосрочен план. Поради недостатъците на реактивния режим, трябва да отделите време, за да изготвите *проактивен* план за управление на мрежата. Този план ви позволява да откривате малки проблеми, преди те да прераснат в големи такива. Чрез предвиждане на потенциални източници на проблеми и предприемане на мерки за тяхното отстраняване, ще си спестите голямо количество време и усложнения. Също така в много случаи ще спестите пари на организацията.

Ключовите концепции при анализиране и оптимизиране на производителността на мрежата са следните:

- Тесни места (botlenecks)
- Базови линии (Baselines)
- Оптимални практики

В следващите секции ще хвърлим поглед отблизо на всяка от тези концепции и ще разгледаме още един важен фактор при оценката и оптимизацията на мрежата: скоростта на връзката към Интернет. Също така ще дефинираме някои от термините, които трябва да разберете, докато обсъждаме проблемите по наблюдение на производителността.

Тесни места

Тясното място (bottleneck) е точно това, което подсказва името – точката в системата, ограничаваща *производителността,* която представлява количеството данни, които могат да текат по мрежата. Тясното място в мрежата ограничава данните точно както стеснената горна част на бутилката ограничава количеството течност, която може да се налее или излее от дадена бутилка.

Тясното място може да бъде предизвикано от проблем с компонент или наследени ограничения на този компонент. Например ако вашата мрежа има хъбове и суичове на 10/100 Mbps, и всички ваши компютри имат мрежови карти на 10/100 Mbps, но кабелната инфраструктура е категория 3 с усукана двойка, която не поддържа висока скорост на трансфер на данни, кабелът е тясното място, което забавя мрежата.

Съмнително е, че можете прецизно да настроите всички компоненти на вашата мрежа така, че всички да работят на една и съща скорост. Но оптимизацията на производителността включва откриване на тесни места и ъпгрейдване, преконфигуриране или замяна на компонентите, за да се повиши тяхната производителност до или над нивото на останалите компоненти на мрежата, създавайки по този начин тясно място някъде на друго място. Може никога да не елиминирате тесните места напълно; просто се променя местоположението им.

Базови линии

Първата стъпка при определяне на начина за ефективна работа на мрежата включва сравняване на различни измервания (например броя на байтовете, предавани за секунда, или броя на изпуснатите пакети) със същите измервания, направени по-рано. Производителността подобрена ли е или е спаднала? Какъв е ефектът върху производителността от реализиране на нова услуга или възможност? Единственият начин да научите отговорите е да имате валидни измервания, на базата на които да сравните текущите стойности. Тази точка на сравнение се нарича *базова линия*, представляваща нивото на производителността, което е приемливо, когато системата работи при типично работно натоварване.

Трябва да измерите базовата линия в такъв момент, когато мрежата работи нормално. Не снемайте измервания в най-натовареното време от деня и не чакайте, докато всички си отидат вкъщи вечерта, за да направите измерването, когато мрежата не се използва. За да установите базовата линия, за предпочитане е да измерите производителността на мрежата по време на типичното ѝ използване. Добър начин за това е да направите няколко отделни измервания на равни интервали и след това да вземете тяхната средна стойност.

Освен че ви помагат да определите тесните места в процеса на разработка, базовата линия ви помага да направите следното:

- Да идентифицирате тежки потребители
- Да съпоставяте дневни, седмични или месечни модели на утилизация на мрежата
- Да балансирате цената на ъпгрейд на мрежови компоненти

Сега ще обясним как всяка от тези дейности може да бъде използвана за оптимизация на производителността на мрежата.

Идентифициране на висока степен на използване

В много случаи ще откриете, че шепа потребители на мрежата „изяждат" голям процент от пропускателната ѝ способност. Идентифицирането на тези тежки потребители ви дава благоприятната възможност да направите следното:

- Да ги посъветвате относно начините за спестяване на пропускателна способност
- Да ограничите тяхната работа чрез софтуерен контрол
- Да планирате тяхната тежка работа и да намерите начини, за да предотвратите влиянието на тяхната работа върху ефикасността на мрежата

Разбира се, опцията, която ще изберете, зависи от това, кои са тежките потребители, тяхната роля в организацията и целта на тяхната тежка работа.

ЗАБЕЛЕЖКА Някои софтуерни приложения (например програми за архивиране и сървърно-базирани антивирусни сканирания) също използват голямо количество от пропускателната способност. Те трябва да бъдат разпределени по график за изпълнение в периоди на по-ниско натоварване.

Съпоставяне на модели за утилизация

Наблюдението ви позволява също да съпоставяте модели на утилизация. Можете да определите не само къде възниква тежко използване, но също и кога възниква. Това улеснява заделянето на пропускателна способност за очаквани дни на висока степен на използване или в пикови часове. То улеснява също създаване на график за поддръжка на мрежата и време за изключване на сървъра в такъв момент, когато това няма да влияе на потребителите в мрежата.

Определяне на модели на трафика на конкретни протоколи

Устройствата и софтуерът за наблюдение на мрежата ви позволяват да определите кои портове са използвани. По този начин можете да идентифицирате дали пропускателната способност се използва за сърфиране в Web или за компютърни игри.

Най-добри практики

Най-добрите практики представляват препоръчителни начини за извършване на административни и други мрежови задачи по най-ефикасен и ценово ефективен начин. Например разпространителите на продукти за наблюдение на мрежи препоръчват да записвате прихванати пакети във файл, когато наблюдавате мрежата, за да установите базова линия. Това ви позволява по-късно да ги анализирате или да ги изпратите на професионални анализатори на мрежи. Също така ще получите постоянно документиране на вашите наблюдения.

Програмите за наблюдение на мрежа често се означават като *протоколни анализатори*. Повечето анализатори са софтуерно-базирани и ви позволяват да прихващате отделни пакети (наричани също кадри или *фреймове*), докато пътуват по мрежата. Ще разгледаме начина на работа на анализаторите по-детайлно в секцията „Инструменти за мониторинг и мениджмънт на мрежата“ по-нататък в тази глава. Трябва да прихванете само толкова статистически данни, колкото реално ви трябват за оценка на производителността на мрежата, и да изпълните софтуера за наблюдение (мониторинг) на мрежата по време на периоди с ниска степен на използване, защото самият софтуер за мониторинг влияе върху производителността на системата.

Определяне скоростта на Интернет връзка

Ако вашата мрежа е свързана към Интернет, може да се наложи да определите скоростта на вашата връзка. Фактът, че използвате модем със скорост 56 kbps за връзка, не означава, че реално ще установите връзка на 56 kbps; твърде вероятно е в зависимост от условията скоростта на вашата връзка да бъде 50 kbps или по-ниска. Реално услугите на телефонната компания, като TrueVoice на AT&T, пречат на модеми със скорост 56 kbps да установяват връзка с тяхната оптимална скорост.

ЗАБЕЛЕЖКА Федералната комисия по комуникации (FCC) на САЩ ограничава количеството електроенергия, която може да бъде предавана по телефонни линии. Това ограничава скоростта на модемите със скорост 56 kbps до около 53 kbps дори ако всички други условия са оптимални.

Производителността на трансфера на данни може да варира поради такива фактори, като използването на хардуерно или софтуерно компресиране. Това ком-

пресиране прави възможно постигане на пропускателна способност от 112 kbps с 56-kbps модем по аналогова телефонна линия.

Скоростта на връзката е ограничена от нейния компонент с най-ниска скорост (т.е. от нейното тясно място). Това означава, че ако вашето оборудване има възможност за връзка със скорост 50 kbps и набирате модем, поддържащ само 33,6 kbps, ще установите връзка на по-ниската скорост.

Ако вашата Интернет връзка ви изглежда бавна, може да има много причини, между които:

- Лоша връзка към сървъра за отдалечен достъп на вашия ISP, причинена от проблеми на модемите на всяка от страните, шумни линии и др.
- Бавен Web сървър, FTP сървър или сървър в Интернет, към който се изпращат вашите заявки
- Състояния на задръствания на основни гръбначни (backbone) линии, които могат да възникнат по време на събития от национално или международно значение
- Споделена пропускателна способност по LAN мрежата или в рамките на мрежата на ISP доставчика

Трябва да се очакват моментни временни забавяния (slowdowns), но можете да направите много малко, за да ги избегнете. Ако обаче общата скорост на връзката е неприемлива за дълго време, може да се наложи да направите ъпгрейд от аналогови към цифрови линии или да преминете на широколентово предаване или друг високоскоростен достъп.

Компонентът за dialup networking на вашата операционна система може да индицира скорост на връзка, обикновено в битове за секунда (bps). Например връзката със скорост 50 kbps, която разгледахме по-рано, бива показвана като 50 000 bps. Това не може да ви даде реална индикация за производителността, защото то измерва само първоначалната скорост на връзката между вашия модем и отдалечения модем. Възможно е производителността да се колебае по време на сесията на връзката.

ЗАБЕЛЕЖКА Скоростта на връзката може да бъде визуализирана или като *скорост на порт* (представляваща скоростта модем-компютър, която включва компресия) или *реалната скорост на връзката* (скоростта модем-модем). Windows може да визуализира скоростта във всеки от тези формати, в зависимост от инсталирания от вас драйвер на модема.

Можете да свалите файл по Интернет и да наблюдавате скоростта на сваляне, показвана от вашия браузър или FTP софтуер. Тя често бива показвана като кило*байтове* за секунда. Във всеки байт има осем бита, затова връзка със скорост 50 kbps вероятно ще се визуализира като скорост на сваляне около 6,25 Kbps.

Няколко Web сайта претендират, че тестват точно скоростта на вашата връзка. Резултатите на различни сайтове могат да варират; трябва също да вземете предвид факта, че тези сайтове използват Hypertext Transfer Protocol (HTTP), служебната информация от който ще повлияе върху скоростта на сваляне. Но те са полезни за груби сравнения. Сайтове, които измерват скоростта на връзка, са следните:

- **MSN Speedtest** – Достъпен на http://computingcentral.msn.com/topics/bandwidth/speedtest50.asp

- **Telus.net High-Speed Internet** – Достъпен на http://speedtest.mybc.com
- **Toast.net Internet Service** – Достъпен на www.toast.net

Инструменти за мониторинг и мениджмънт на мрежата

Съществуват много софтуерни пакети, които могат да ви помогнат при наблюдението и управлението на вашата мрежа. Някои са включени в мрежовата операционна система, някои могат да бъдат свалени от Web като фрийуер или шеруер, а някои са скъпи и с богати възможности.

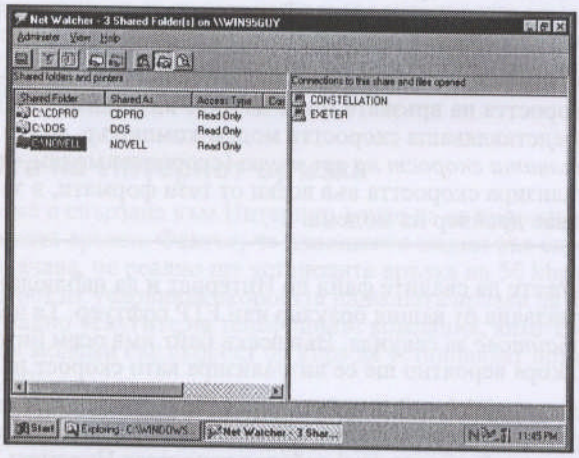
В следващите секции ще разгледаме някои от популярните програми за мониторинг и мениджмънт. Също така ще разгледаме доставчици на услуги за мениджмънт на мрежи, с които можете да сключите договор за управление на ваша мрежа.

Софтуер за мониторинг на мрежи

Софтуерът за мониторинг (наблюдение) на мрежи варира от прост до сложен и от безплатен до скъп. Модерните операционни системи, като Windows NT и Windows 2000, имат вградени инструменти за наблюдение. Те не са толкова интелигентни или богати на възможности, като продуктите на независими производители, но могат да бъдат полезни при определяне на базови линии на производителността или отстраняване на проблеми по мрежата.

Дори Windows 95 има прости инструменти за мониторинг, включени в Net Watcher, показан на Фигура 18-1.

Фигура 18-1 *Windows 95 предлага Net Watcher като опция на системен инструмент.*



Интелигентните средства за мрежов мониторинг се наричат протоколни анализатори. Протоколните анализатори прихващат пакети (т.е. фреймове), които се предават между два или повече компютъра или мрежови устройства. След това анализаторът декодира (интерпретира) пакетите така, че да можете да видите данните на английски (или на друг език), съпоставени с двоичния език. Инте-

лигентният протоколен анализатор осигурява също статистически данни и информация тенденциите за прихванатия трафик.

Терминът *снифър* често се използва за означаване на всяка програма, която позволява да „подслушвате" мрежовия трафик. Network Associates регистрира търговската марка Sniffer (и нейната разширена версия Sniffer Pro). И двата продукта представляват мрежови анализатори.

Подслушващите програми имат лоша репутация в някои кръгове, защото могат да бъдат използвани от хакери и кракери за извличане на потребителски имена и пароли, които се изпращат по мрежата в обикновен текст. Тези пълномощия след това се използват за придобиване на неоторизиран достъп до системи. Въпреки това снифърите имат много законни приложения за мрежови администратори, в това число:

- Анализ на проблеми на свързването
- Анализ на производителността
- Откриване на нарушения

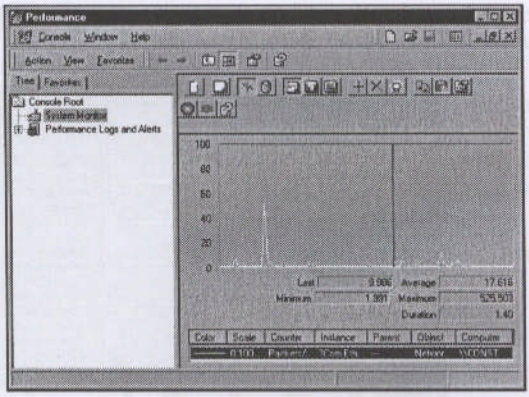
В тази сесия ще разгледаме подробно Microsoft Performance Monitor и Microsoft System Monitor. Също така ще разгледаме Network Monitor. След това ще представим някои продукти за допълнително инсталиране, като Sniffer Pro и LANalyzer на Novell.

Microsoft Performance Monitor и Microsoft System Monitor

Performance Monitor на Windows NT 4.0 (наречен System Monitor в Windows 2000) измерва производителността на голям брой системни компоненти, включвайки броячи на мрежови компоненти.

Мониторът ви позволява да показвате стойности във форма на графика, да записвате данни в дневник и да съставяте отчет. Измерванията могат да бъдат наблюдавани в реално време, да бъдат обновявания автоматично или да бъдат обновявани при поискване.

Фигура 18-2 *System Monitor на Windows 2000 може да бъде използван за измерване на производителността на мрежата.*



Performance Monitor и System Monitor ви позволяват да конфигурирате предупреждения (alerts), които наблюдават зададени броячи и ви уведомяват, когато стойността се покачи над или спадне под предварително дефинирана граница.

За да идентифицирате тесните места в мрежата, трябва да наблюдавате броячи на мрежовия интерфейс, между които:

- Общия брой байтове за секунда
- Изпратени байтове за секунда
- Приети байтове за секунда

Можете също да наблюдавате следните броячи на обекти в протоколния слой:

- Приети сегменти за секунда
- Изпратени сегменти за секунда
- Приети фреймове за секунда
- Изпратени фреймове за секунда

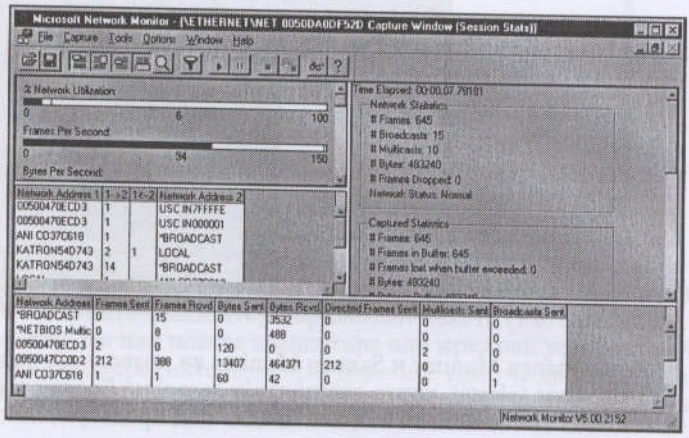
Наблюдението на тези броячи ви позволява да планирате разпределението на капацитета на пропускателната способност. Например ако общия брой байтове, предавани в секунда, е близък или равен на максималния капацитет на преносната среда (media) на вашата мрежа, трябва да помислите или за ъпгрейд на вашето оборудване (например от Ethernet 10 Mbps на Ethernet 100 Mbps), или за намаляване на натоварването на мрежата.

Microsoft Network Monitor

System Monitor измерва стойностите, свързани с производителността на мрежата, но за да прихващате реално пакети, докато пътуват по мрежата, и след това да ги анализирате, трябва да използвате един друг инструмент. Windows NT 4.0 и Windows 2000 включват „олекотена" версия на Microsoft Network Monitor, която е част от System Management Server (SMS) на Microsoft. SMS ще разгледаме в секцията „Софтуер за мениджмънт на мрежи" на тази глава.

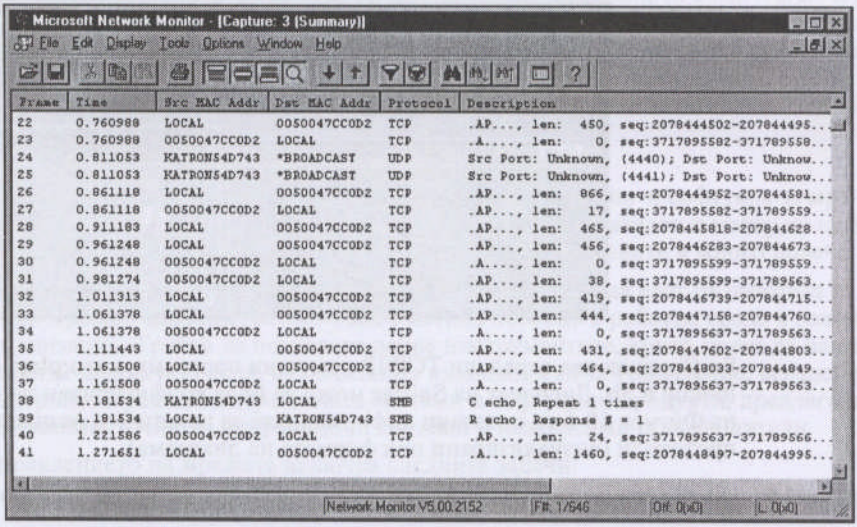
Network Monitor, който се разпространява с Windows NT и Windows 2000, е функционален и полезен инструмент за извършване на анализ на протоколите за маршрутизация. Фигура 18-3 показва момент, в който Network Monitor наблюдава степента на използване на мрежата, фреймовете в секунда и допълнителни статистически данни за мрежата.

Фигура 18-3 *Microsoft включва „олекотена" версия на Network Monitor в операционните системи Windows NT и Windows 2000.*



Можете да използвате Network Monitor, за да визуализирате отделните фреймове на прихванатите данни, както е показано на Фигура 18-4. Обърнете внимание, че има пакети за няколко различни прихванати протокола, като TCP, UDP и SMB.

Фигура 18-4 *Данните, прихванати от Network Monitor, могат да бъдат анализирани фрейм по фрейм.*



Снифър технологии

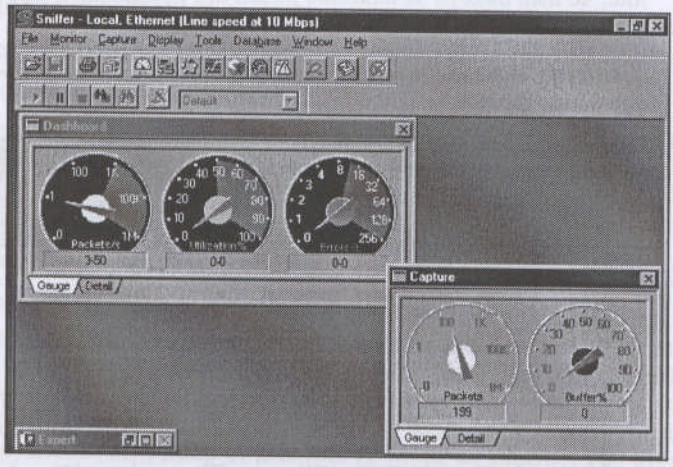
Популярният мрежов анализатор Sniffer прерасна в сложен комплект от мрежови инструменти, в това число:

- Sniffer Pro LAN и Sniffer Pro WAN
- Sniffer Pro High-Speed
- Gigabit Sniffer Pro
- Sniffer Distributed Analysis Suite

Продуктите Sniffer разрешават интелигентно филтриране, базирано на съвпадения в моделите, IP/IPX или DLC адреси. Sniffer Pro включва генератор на трафик, спомагащ тестването на нови устройства или приложения; можете да го използвате, за да симулирате мрежов трафик и да измервате времената за отговор и броя на скоковете (hops).

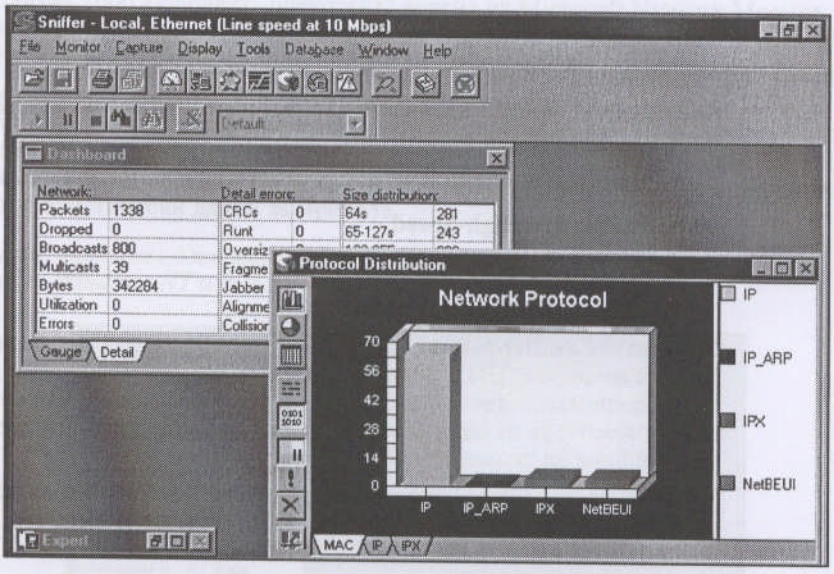
Sniffer използва интерфейс във формата на контролен панел, както е показано на Фигура 18-5.

Фигура 18-5 *Sniffer Pro визуализира прихванатата информация в интерфейс с формата на контролен панел.*



Sniffer включва вградени TCP/IP помощни програми, като **ping**, **tracert**, DNS lookup и др. Дисплеят на Sniffer може да бъде конфигуриран по много начини; на Фигура 18-6 са показани информацията за пакетите и разпределението по протоколи (визуализирани под формата на диаграма).

Фигура 18-6 *Дисплеят на Sniffer Pro може да се конфигурира по няколко начина*



Sniffer включва Expert Analyzer, който ви помага при диагностициране на мрежови проблеми; можете да стартирате множество инстанции на програмата или отделни инструменти.

Novel LANalyzer

Инструментът за анализ на мрежата LANalyzer на Novell се изпълнява в Windows и притежава основни възможности за мониторинг и отстраняване на проблеми за мрежи Ethernet и Token Ring. В допълнение към прихващането на пакети, продуктът прави конкретни препоръки за отстраняването на проблеми и оптимизирани на производителността на мрежата.

LANalyzer поддържа Novell Directory Services (NDS) и работи с NetWare, Apple Talk, NFS, SNA и TCP/IP. Графичният интерфейс на LANalyzer използва стил на контролен панел, подобен на Sniffer Pro, и индицира мрежовите компоненти по име и по MAC адрес.

Софтуер за мениджмънт на мрежи

Каква е разликата между софтуера за мрежов мониторинг и софтуера за мрежов мениджмънт? Последният по принцип е по-изчерпателен и макар че включва компоненти за мониторинг, той ви позволява да правите и много повече.

Управлението на мрежовите услуги представлява голяма част от работата на всеки мрежов администратор. Това е истина особено в работна среда в голяма организация. Трябва да познавате добре инструментите, които могат да направят тази задача по-лесна, включително възможности за управление, вградени в модерните мрежови операционни системи и софтуерни продукти, предлагани от производители на операционни системи и независими производители.

Управлението на мрежата включва следните задачи:

- Документиране на устройствата в мрежата и състоянието на всяко от тях
- Създаване на инвентарен списък на мрежовия софтуер, който ви позволява да инсталирате софтуер и да извършвате обновявания по мрежата
- Измерване на софтуера за осигуряване на данни за използваните приложения и как, кога и от кога са използвани
- Управление на софтуерните лицензи
- Отдалечено управление на клиентски машини и сървъри по мрежата и управление на отдалечени десктопи
- Уведомяване на администраторите за събития като отказ на мрежови компоненти или предварително дефиниран капацитет, който е достигнат или надхвърлен

На пазара съществуват няколко програми за мрежов мениджмънт (или по-точно комплекти от програми). В тази секция ще разгледаме няколко от най-популярните, а именно:

- Microsoft SMS
- Novell ManageWise
- IBM Tivoli Enterprice
- Hewlett Packard OpenView

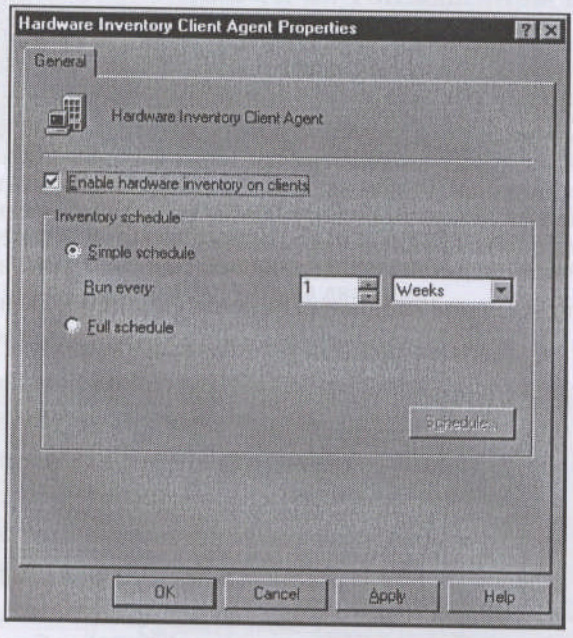
Тези продукти са проектирани за мрежа на голяма организация с голям брой сайтове.

Също така ще разгледаме софтуера за мениджмънт на мрежи, който е подходящ за малки до средни LAN мрежи. Този софтуер включва LANExplorer и Network Monitoring Suit на Lanware.

Microsoft SMS

Microsoft SMS е модерен пакет за мрежов мениджмънт, който прави подробен опис (inventory) на хардуера и софтуера (вижте Фигура 18-7), има възможности за отдалечена диагностика и отдалечен контрол на десктопа и отдалечено инсталиране на софтуер.

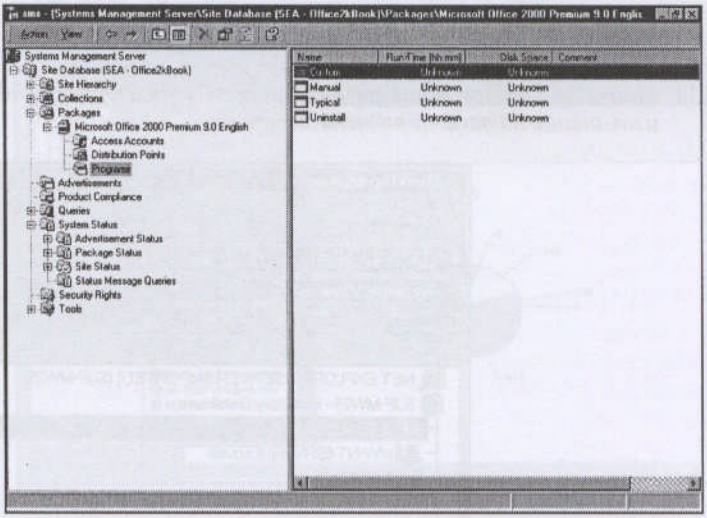
Фигура 18-7 *Microsoft SMS ви позволява да събирате данни за създаване на опис на хардуера чрез инсталиране на клиентски агенти на набелязани компютри.*



Също така SMS включва по-силна версия на Microsoft Network Monitor от тази, вградена в операционните системи Windows NT и Windows 2000. Например SMS Network Monitor добавя възможността за откриване на маршрутизатори в мрежата и преобразуване на от имена в адреси.

Една от най-полезните възможности на SMS е неговата възможност за разпространение на софтуер. С нея се създава *дистрибутивен пакет*. Пакетът съдържа информация, използвана от SMS за координиране на разпространението на софтуера (вижте Фигура 18-8).

Фигура 18-8 *SMS използва дистрибутивни пакети за инсталиране на софтуера из цялата организация.*

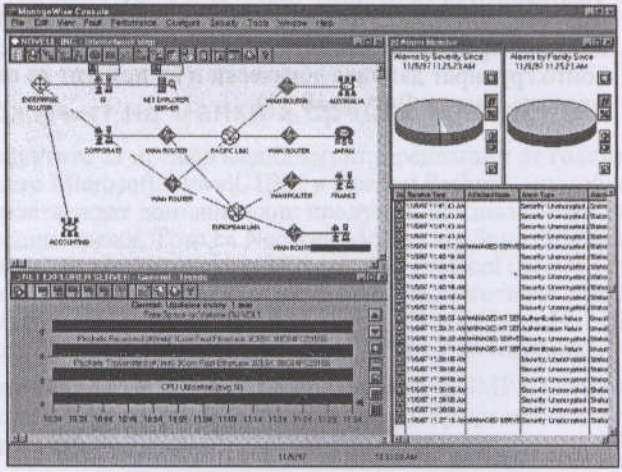


SMS използва SQL server на Microsoft, което означава, че можете лесно да експортирате данни към Microsoft Access. SMS включва поддръжка на Macintosh клиенти и може лесно да бъде интегриран в среда на Novell NDS.

Novell ManageWise

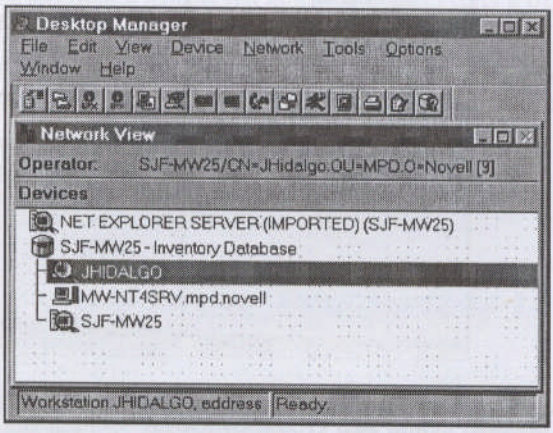
ManageWise на Novell се състои от интегрирана група от услуги за мрежов мениджмънт, които могат да бъдат използвани за управление на сървъри NetWare или с добавянето на допълнителен агент, на Windows NT сървъри. Компонентите включват анализ на мрежовия трафик, контрол на работните станции и сървъри и администриране на мрежови приложения. Фигура 18-9 показва конзолата на ManageWise.

Фигура 18-9 *ManageWise на Novell включва възможности за картографиране на мрежата.*



Подобно на SMS, ManageWise може да създава опис на мрежовите устройства; в допълнение той включва възможност за алармиране/уведомяване. ManageWise включва агента NetWare LANalyzer – агентът за мениджмънт, LANDesk Manager на Intel и LANDesk защита от вируси. ManageWise включва и модула Desktop Manager, показан на Фигура 18-10.

Фигура 18-10 *Модулът Desktop Manager на ManageWise осигурява графичен интерфейс за изпълнение на задачи по мениджмънта.*



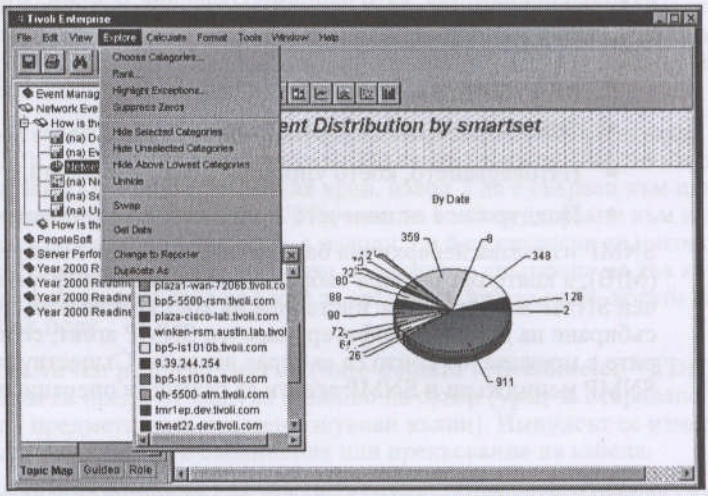
Desktop Manager ви позволява да преглеждате описите на хардуера и софтуера на работната станция, да извършвате трансфер на файлове към и от нея, да управлявате отдалечен неин десктоп, да провеждате чат с потребителя и да рестартирате компютъра.

IBM Tivoli Enterprise

Tivoli Enterprise е популярен пакет за мрежов мениджмънт, който съдържа инструменти, проектирани за осигуряване на управление на активи, достъпност, промени, операции, сигурност, услуги и съхранение. Tivoli Enterprise улеснява реализирането на тези компоненти на фази.

Tivoli Enterprise има възможност да осигури пълен изглед на топологията на мрежата. Инструментите за отчети ви позволяват да приспособявате изгледа, в който се представят данните, и можете да създавате „интелигентни набори", които групират данните логически и ви помагат да анализирате състоянието на мрежата (вижте Фигура 18-11).

Фигура 18-11 *Tivoli Enterprise позволява да приспособявате представянето на събраните данни.*



Tivoli предлага също решения за малки бизнес организации (с Tivoli IT Director) и за организации със среден размер (комплектите за мениджмънт Tivoli).

Hewlett Packard OpenView

Инструментите за мениджмънт OpenView на Hewlett Packard включват OpenView Enterprise за широкомащабни корпоративни решения, и OpenView Express за организации със среден размер. OpenView Enterprise е предназначен за мрежи, които имат хиляди сървъри и повече от 5000 работни станции, и които работят под мрежови операционни системи Windows NT, Windows 2000 или UNIX. OpenView Express осигурява мениджмънт на Web сървъри, мениджмънт на Exchange пощенски сървъри и мрежи в смесен режим с Windows NT и Windows 2000.

Компонентът ManageX на OpenView представлява инструмент за мениджмънт на сървъри и производителност, който може да бъде използван в среди на NT и NetWare.

Софтуер за мениджмънт на малки и средни мрежи

Наред с продуктите за мрежов мениджмънт, предлагани от големи софтуерни компании, като Microsoft, Novell, IBM и Hewlett Packard, многобройни по-малки фирми произвеждат допълнителни продукти, предназначени за пазара на малки до средни мрежи. Това са Network Monitoring Suite (NMS) на Lanware, който използва Simple Networking Management Protocol (SNMP) и осигурява такива възможности, като рестартиране на сървъри, изготвяне график за изпълнение на събития и презареждане на сървъри. ViewLAN на NuLink е друг относително прост SNMP инструмент за мениджмънт и мониторинг.

В следващите секции ще разгледаме протоколите SNMP и Common Management Information Protocol (CMIP), на които са базирани много от тези прости софтуерни решения.

SNMP

SNMP е помощна програма, включена в повечето реализации на TCP/IP. Тя има няколко предимства, като например решение за мениджмънт на мрежи:

- Проста е
- Не е скъпа
- Относително лесна за реализиране
- Натоварването, което упражнява върху мрежата, е малко
- Поддържа се от повечето мрежови хардуерни устройства

SNMP използва йерархична база данни, наречена Management Information Base (MIB), в която организира събраната за мрежата информация. Софтуер, наречен SNMP мениджър, се инсталира на хост компютъра, който се използва за събиране на данните. Софтуер, наречен SNMP агент, се инсталира на компютрите в мрежата, от които се събират данните. Съществуват фрийуер версии на SNMP мениджъри и SNMP агенти за различни операционни системи.

CMIP

CMIP беше предназначен за подобряване на SNMP и разширяване на неговата функционалност. Той работи почти по същия начин като SNMP, но има подобри възможности за сигурност и дава възможност за уведомяване, когато възникнат конкретни грешки.

Служебната информация (overhead) за CMIP е значително по-голяма от тази, която се изисква за SNMP; поради това този протокол не се реализира толкова широко. CMIP е базиран на OSI комплекта от протоколи; CNMP се счита за част от комплекта TCP/IP.

Доставчици на услуги за мениджмънт

В Глава 17, „Мрежи за тънки клиенти“, разгледахме концепцията за доставчиците на услуги за приложения (ASP) – компании, които доставят софтуерни приложения по мрежата. Една нова разработка в мрежовия мениджмънт е вариант на същата тема: доставчик на услуга за мениджмънт (MSP).

Дадена организация се абонира за услуга MSP, която осигурява наблюдение на производителността и мениджмънт на мрежата. Това спестява на организацията разходите по закупуване, инсталиране и обучение по използването на софтуер за мониторинг и мениджмънт.

Пример за компания, която осигурява аутсорсинг на задания за мрежов мениджмънт, е компанията Luminate.Net, която осигурява Web-базиран интерфейс за взаимодействие с клиентите по Интернет.

Устройства за мониторинг на хардуера и отстраняване на проблеми

Повечето хардуерни устройства, които се използват за наблюдение и управление на мрежата, са просто специално предназначени за целта компютри (често преносими), които изпълняват собствен софтуер за протоколен анализ и управ-

ление на мрежата. Ето някои устройства, които могат да бъдат полезни при отстраняване на проблеми в мрежата:

- **Тон генератор/локатор** (наричан също *лисица и хрътка*) – Частта „лисица" може да бъде свързана към единия край на кабела и да бъде генериран тонален сигнал. Локаторът („хрътката") в други край приема тона, което индицира, че имате изправен кабел.
- **Кръстосан кабел** – Това е Ethernet неекраниран кабел с усукана двойка (UTP), в който двойките проводници са кръстосани. Вместо извод 1 да е свързан към извод 1 на другия край, извод 2 да е свързан към извод 2 и т.н. (както при нормалния UTP), изводи 1 и 2 са свързани към изводи 3 и 6 на противоположния край, а изводи 3 и 6 са свързани към изводи 1 и 2. Кръстосаният кабел се използва за директно свързване на два компютъра без преминаване през хъб или за свързване на два хъба, когато няма uplink порт.
- **Динамичен рефлектометър (time-domain reflectometer – TDR)** – По кабела се предават импулс подобно на сонар (уред за откриване на потънали предмети чрез отразени звукови вълни). Импулсът се измерва, за да бъдат открити къси съединения или прекъсвания на кабела.
- **Хардуерна обратна връзка (loopback)** – Това устройство се свързва към серийния порт за предаване на данни, които след това се връщат обратно, за да бъдат приети от същия компютър. Това ви позволява да определите дали серийният порт функционира правилно и ви дава възможност да направите това, без да свързвате модем или друго устройство.
- **Цифров волт/ом метър** – Волт/ом метърът (или волтметър) се използва за измерване на електронни импулси по кабела и за определяне дали има къси съединения или прекъсвания по кабела.
- **Кабелен тестер** – Кабелният тестер се използва за откриване на прекъсвания и къси съединения, а *усъвършенстваният кабелен тестер* може да визуализира допълнителна информация за състоянието и свойствата на кабела.
- **Осцилоскоп** – Осцилоскопите се използват за калибриране на електроника и за измерване на нивото на напрежението на сигнала, който преминава по кабела за зададен период от време. Информацията се визуализира на малък монитор във вълнова форма. Осцилоскопът може да индицира къси съединения и прекъсвания в кабела, нагънати проводници и затихване.
- **LAN метър** – LAN метърът може да проверява за бродкасти, колизии, нива на използване и грешки на локални мрежи Ethernet и Token Ring, както и да измерва производителността в WAN мрежи. Той може също да идентифицира устройства, свързвани към мрежата.

Отстраняване на проблеми в мрежите

Независимо от това, че полагате най-добрите усилия за превенция на проблеми, като администратор неизбежно ще се сблъскате с проблеми по мрежата. Те варират от постепенни забавяния, които дразнят потребителите, до пълно изгубване на връзка по цялата мрежа, като това прекъсва работата на хиляди служители.

Всички продукти, които разгледахме, могат да бъдат използвани за отстраняване на проблеми в мрежата. Тъй като повечето съвременни мрежи работят с TCP/IP, имате на разположение няколко полезни помощни програми за отстраняване на проблеми. Те могат да бъдат използвани без необходимостта от закупуването, инсталирането и изучаването, свързани с един сложен и скъп продукт за мрежов мениджмънт.

В тази секция ще разгледаме някои от основите на отстраняването на проблеми и начините за използване на файлове-дневници при отстраняването на проблеми, а също инструментите и помощните програми, включени в повечето реализации на TCP/IP. След това ще разгледаме как могат да бъдат използвани за отстраняване на проблеми в мрежовите връзки. Накрая ще представим списък с по-подробни указания за отстраняване на проблеми в мрежите, за да ви помогнем при откриване и решаване на проблемите, свързани с производителността и връзките на мрежите.

Основи на отстраняването на проблеми

Най-основният мрежов проблем е невъзможността на един компютър да комуникира с друг компютър. За изгубването на връзката може да има много причини и те могат да бъдат свързани както с хардуера, така и със софтуера.

Първото правило при отстраняване на проблеми е да проверите физическата връзка. Не пренебрегвайте най-простата причина. Не един мрежов професионалист е загубил часове за преконфигуриране на протоколи, преинсталиране на софтуер и дори преинсталиране на операционната система, за да открие накрая, че причината компютърът да не комуникира по мрежата е, че някой е изключил кабела от мрежовата карта. Следователно, преди да се впуснете в сложни действия по отстраняване на проблеми, се уверете, че кабелите са правилно включени *и в двата* края, че мрежовият адаптер функционира (проверете светлинната индикация на връзката на самата мрежова карта), че светят светлините за състоянието на хъба и че комуникационният проблем не е просто повреда на хардуера.

Друга често срещана причина за проблеми на мрежата е меко казано „грешката на оператор". Вероятно причината дадена работна станция да не вижда останалата част от мрежата е, че потребителят се е логнал на локалната машина, но не и в мрежата. Уверете се, че потребителите използват правилното потребителско име и парола, и че техните акаунти не са ограничени по начин, който им забранява да установяват логическа връзка с мрежата. Например броят на логванията може да бъде ограничен само до работните часове през дните от седмицата, или потребителят може да бъде ограничен да се логва само от конкретна работна станция.

ЗАБЕЛЕЖКА Една от най-популярните причини, поради които паролата на даден потребител „не работи", се дължи на факта, че при записване на паролите повечето операционни системи отчитат разликата между главни и малки букви. Случайното включване на клавиша Caps Lock преди въвеждане на паролата ще доведе до нейното отхвърляне. Дори операционна система, която няма файлови системи, отчитащи разликата между главни и малки букви, например Windows, обикновено налага такава по отношение на паролите на потребителите.

Хардуерните проблеми са сравнително прости за отстраняване, след като бъдат открити. Трябва да включите устройството, и ако то е повредено, да го ремонтирате или замените.

Софтуерните проблеми могат да бъдат по-трудни за проследяване. Най-честият виновник е погрешното конфигуриране на софтуера. Настройките на софтуера могат да бъдат променени от инсталационната програма на наскоро инсталиран софтуер, или потребителят може да е експериментирал с настройките. Липсващи или повредени файлове могат да причинят всевъзможни проблеми, включително проблеми с възможността за връзка с мрежата. Потребителите неволно (или по друг начин) изтриват файлове, а пикове в захранващото напрежение или внезапно изключване на компютъра могат да повредят данни във важни файлове. Не пренебрегвайте също възможността за наличие на вирус.

Каквато и да е предполагаемата причина за проблема, следването на определен набор от предварително планирани стъпки за всеки сценарий на отстраняване на проблеми ще ви гарантира, че сте обхванали всички основни пунктове. Програмата за сертифициране Network+ препоръчва следната последователност от стъпки при отстраняване на проблеми:

1. Идентифицирайте проблема, събирайки колкото е възможно повече информация.
2. Опитайте се да пресъздадете проблема. Определете дали проблемът може да бъде пресъздаден на друг компютър или е специфичен за въпросната машина.
3. Опитайте се да изолирате причината за проблема. Формулирайте възможни обяснения за проблема и ги елиминирайте една по една.
4. Формулирайте отговор за коригиране на проблема, като се базирате на вашия опит и проведеното изследване.
5. Реализирайте вашия план за отстраняване на проблема.
6. Тествайте, за да проверите дали планът ви действа.
7. Документирайте проблема и решението, за да могат да бъдат правени справки в бъдеще. Документацията трябва да включва дневник на всички направени промени в конфигурацията.
8. Осъществете обратна връзка с потребителя.

Първите шест стъпки се изпълняват почти интуитивно, но много професионалисти по мрежи пропускат стъпки 7 и 8. След като проблемът е „отстранен", те вярват, че работата е свършила. Но последните две стъпки са критично важни при работа в мрежова среда.

След като отделите два дни в отстраняване на проблем, може би си мислите, че никога няма да забравите измъчилите ви подробности. Но животът на мрежовия администратор е доста наситен и е твърде вероятно, когато същият проблем възникне отново, може би година по-късно, да не си спомните, че това е ставало и преди, и че *някак* сте успели да го разрешите. Документирането на стъпките, които сте предприели, ще ви спести не само време, но и много главоболия.

Също е важно осигуряване на обратна връзка с потребителите. Не пропускайте възможността да ги обучавате; на първо място това е ключов елемент при предотвратяване на проблеми. Може би за вас е важно, че потребителят не го е грижа *какъв* е възникналият проблем, а само че е бил отстранен. Но повечето хора оценяват информацията – особено ако тази информация може да им помогне да променят техните навици или да разберат за какви признаци на пов-

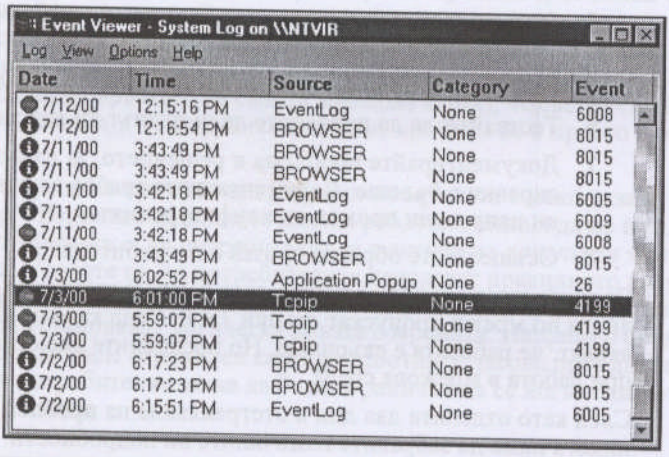
реди да следят и да докладват, преди проблемът да се е превърнал в катастрофа. Когато давате обратна информация, трябва да внимавате да използвате ниво на езика, подходящо за техническите познания на потребителя.

ЗАБЕЛЕЖКА Когато давате обратна информация на потребителя, се уверете, че сте казали ясно какво трябва да се направи, ако проблемът възникне отново. Ако това нещо е много просто и вие мислите, че потребителят може да го коригира сам, задайте му подробни инструкции от вида „стъпка по стъпка"; дори можете да му ги дадете в писмен вид. В противен случай укажете ясно, че вие му давате само информация и че политиката на организацията изисква потребителят да ви уведоми, ако отново възникнат проблеми.

Използване на файловете-дневници на операционната система

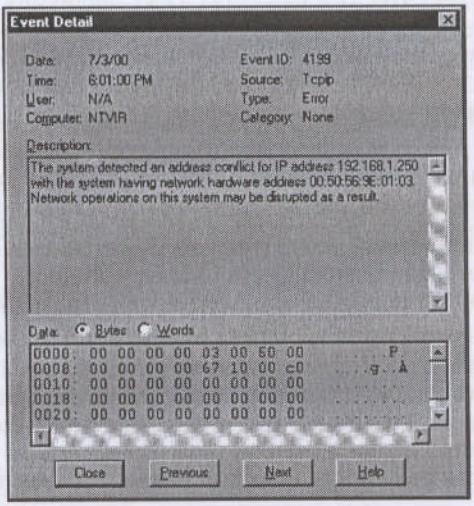
Повечето операционни системи осигуряват средства за водене на дневник на повредите на устройства, провалени опити за комуникации и други състояния на грешки. Информацията е полезна стартова точка за отстраняване на проблеми. Например Windows NT и Windows 2000 осигуряват програмата за преглед Event Viewer (вижте Фигура 18-12), която ви позволява да преглеждате списък от системни събития.

Фигура 18-12 *Event Viewer в Windows NT Server визуализира състояния на възникване на грешки.*



Селектирайки конкретно събитие, например грешката на TCP/IP, показана на Фигура 18-12, можете да получите още подробности за събитието, показани на Фигура 18-13. Информацията за този сървър ви указва, че е настъпил конфликт на IP адреси, който обяснява защо компютърът не комуникира по мрежата.

Фигура 18-13 *Когато селектирате конкретно събитие, се визуализира по-детайлна информация за това събитие.*



Други операционни системи също имат механизми за водене на дневници. Файлът SYS$LOG.ERR на NewWare е дневник на сървърни грешки. Файлът CONSOLE.LOG съдържа грешки и информиращи съобщения, които се визуализират на сървърната конзола. Също така NewWare води дневник, наречен ABEND.LOG; тя записва грешки от типа Abnormal End, които карат сървъра да прекрати своята работа или да изключи зареждаем NewWare модул (NewWare Loadable Module – NLM).

Използване на помощни програми за TCP/IP

Макар че могат да се различават до известна степен по име и функционалност, повечето реализации на TCP/IP включват комплект от помощни програми, които могат да бъдат използвани за събиране на конфигурационна информация, тестване на връзката и отстраняване на проблеми в мрежата.

В следващите секции ще разгледаме няколко категории TCP/IP помощни програми: такива, които тестват връзката, такива, използвани за конфигурация, и такива, осигуряващи информация, която може да бъде полезна за отстраняване на проблеми в мрежите.

Помощни програми за тестване на връзката

Първата стъпка при отстраняването на проблеми, свързани с изгубване на връзка, е да определите дали тя наистина е изгубена. По-неопитните потребители на мрежи бързо решават, че нямат връзка към сървъра, ако не виждат името на сървъра в Network Neighborhood в Windows. Често това е просто проблем на преминаването в дървовидната структура от ресурси; сървърът не се регистрира сам в главния браузър (master browser) (компютърът, който следи мрежовите ресурси, за да ги визуализира в списъка за браузване [browse list]). Но ако се опитате да осъществите достъп до сървъра чрез въвеждане на неговия път, спазвайки конвенцията за универсално именуване (UNC), ще откриете, че връзката е налице.

TCP/IP инструментите, които ви позволяват да тествате връзката до друга машина и да определяте пътя, който изминава пакетът, за да достигне до местоназначението, са следните:

- **ping** и **pathping**
- Помощни програми за трасиране

Тези инструменти ще разгледаме в следващите секции.

ping и pathping

ping е съкращение на *packet internetwork grooper*. Тази команда е проста помощна програма, която изпраща съобщение, наречено Echo Request, използвайки протокола Internet Control Message Protocol (ICMP), до зададен компютър местоназначение. Компютърът местоназначение отговаря с изпращане на ICMP exo.

Първата стъпка при проверка за предполагаем проблем на връзката е ping-ването на хоста. Ако искате да проверите вашата връзка към Интернет, трябва да ping-вате надежден хост в Интернет, например www.yahoo.com. Ако получите отговор, ще знаете, че физическата връзка между двата компютъра е незасегната и работи. Пример 18-1 показва пример на заявка и отговор на **ping**.

Пример 18-1 *Командата ping се използва за тестване на връзката между два компютъра.*

```
G:\>ping www.yahoo.com

Pinging www.yahoo.akadns.net [216.32.74.52] with 32 bytes of data:

Reply from 216.32.74.52: bytes=32 time=110ms TTL=241
Reply from 216.32.74.52: bytes=32 time=141ms TTL=241
Reply from 216.32.74.52: bytes=32 time=100ms TTL=241
Reply from 216.32.74.52: bytes=32 time=100ms TTL=241

Ping statistics for 216.32.74.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 100ms, Maximum =  141ms, Average =  112ms
```

Командата **ping** може да бъде подадена с използване или на IP адрес, или на името на компютъра местоназначение. За тестване на връзката използвайте IP адреса. Ако успеете да ping-вате с IP адрес, но не получите отговор, когато ping-вате същия компютър по име, това означава, че има проблем с вашия сървър или конфигурацията за преобразуване на имена. Такъв проблем може да възникне, когато вашият компютър не използва DHCP и няма адрес на DNS сървър, въведен в свойствата на TCP/IP. От друга страна, когато вашият компютър е DHCP клиент, DHCP сървърът може да зададе адреса на DNS сървъра.

ЗАБЕЛЕЖКА Терминът ping time се отнася до количеството време, което изминава между изпращането на заявка за exo (Echo Request) и приемането на exo отговор (Echo Replay). Късото време на ping-ване показва бърза връзка.

Командата **ping** може да бъде използвана също за тестване дали TCP/IP стекът на компютъра е инсталиран правилно и функционира. За да извършите теста, изпълнете ping до адреса за обратна връзка 127.0.0.1. (За този адрес говорихме

в Глава 8, „Мрежови протоколи и услуги“.) Ако получите отговор, това означава, че стекът работи.

Версията на ping от командния ред е включена в TCP/IP стековете на всички операционни системи Windows, както и с различните издания на UNIX и Linux. На NetWare сървърите са включени две версии: **ping** и **tping** (което означава *trivial ping*). Те се зареждат като NLM модули от сървърната конзола.

Програмата **pathping** е включена в Windows 2000, но не и в Windows 9x или NT. Тя комбинира възможностите на **ping** с тези на **tracert** и осигурява допълнителна информация, която иначе не се визуализира от тези програми. С **pathping** можете да откриете кои маршрутизатори предизвикват проблеми по мрежата и да измерите колко пакета се губят при конкретен маршрутизатор.

Помощни програми за трасиране

Помощните програми за трасиране се използват за откриване на маршрута на движение на даден пакет за достигане на неговото местоназначение. Таблица 18-1 показва командите за трасиране, използвани в различни операционни системи.

Таблица 18-1 *Помощни програми за трасиране в различни операционни системи**

Операционна система	Команда за трасиране
Windows 9x, NT и 2000	Въведете **tracert** от командния ред
Linux/UNIX	Въведете **traceroute** от командния ред
NetWare	Въведете **load iptrace** от конзолата на сървъра

* Спомнете си, че за да осъществите достъп до командния ред на Windows 9x, трябва да въведете **command** в реда на прозореца Run. В Windows NT и Windows 2000 въвеждате **cmd**.

Помощната програма за трасиране показва всичките маршрутизатори, през които преминава пакетът, докато пътува по мрежата от предаващия компютър до компютъра местоназначение (вижте Пример 18-2). Помощната програма за трасиране на маршрути може да бъде полезна за определяне на точката, в която се губи връзката или в която има забавяне.

Пример 18-2 *Командата tracert показва маршрута, изминат от пакет, изпратен от един хост до друг*

```
G:\>tracert www.yahoo.com

Tracing route to www.yahoo.akadns.net [216.32.74.52]
over a maximum of 30 hops:

  1   <10 ms   <10 ms   <10 ms  STARBLAZER [192.168.1.16]
  2   131 ms    60 ms    60 ms  dal-isdn0.august.net
[216.87.128.117]
  3    60 ms   110 ms    61 ms  dal-gw-eth0.august.net
[216.87.128.126]
  4    60 ms    60 ms    60 ms  dal-gw2-fe2-0.august.net
[216.87.128.86]
  5   100 ms    70 ms    90 ms  500.Serial2-7.GW6.DFW9.ALTER.NET
[157.130.216.157]
```

```
  6   110 ms    70 ms   111 ms  158.at-5-0-0.XR1.DFW9.ALTER.NET
[152.63.100.186]

  7    60 ms   100 ms    61 ms  285.at-1-0-0.XR1.DFW7.ALTER.NET
[152.63.96.205]

  8    60 ms    80 ms    91 ms  191.ATM6-0.GW6.DFW7.ALTER.NET
[146.188.242.81]
  9    90 ms    60 ms    70 ms  exodus-oc3-dfw.customer.alter.net
                                 [157.130.141.74]
 10    60 ms   130 ms    60 ms  bbr01-g4-0.dlls01.exodus.net
[216.34.160.205]
 11    90 ms   120 ms   110 ms  bbr02-p5-0.atln01.exodus.net
[209.185.9.38]
 12    90 ms    90 ms   130 ms  bbr01-g6-0.atln01.exodus.net
[216.35.162.19]
 13   110 ms   120 ms   120 ms  bbr02-p5-0.stng01.exodus.net
[209.185.9.42]
 14   110 ms   110 ms   120 ms  dcr04-g9-0.stng01.exodus.net
[216.33.96.146]
 15   130 ms   431 ms   170 ms  csr22-ve243.stng01.exodus.net
[216.33.98.26]
 16   150 ms   210 ms   240 ms  216.35.210.126
 17   120 ms   151 ms   120 ms  www3.dcx.yahoo.com [216.32.74.52]
```

Помощни програми за конфигуриране

Проблемите на връзката често се оказва, че са проблеми на конфигурацията. Възможно е IP адресът, зададен на компютъра, да не е в правилния подмрежов обхват, или вероятно са въведени неправилно подмрежова маска, подразбиращ се шлюз, DNS адрес или други части от конфигурационната информация. Ако някоя от тези стойности е погрешна или случайно изтрита, компютърът не може правилно да комуникира по TCP/IP мрежата.

Всяка операционна система включва възможност за визуализиране на IP конфигурацията, използвана от системата или мрежовия адаптер. Таблица 18-2 показва списък на командите, използвани от различни операционни системи.

Таблица 18-2 *Команди за конфигуриране на IP в различни операционни системи.*

Операционна система	Команда за визуализиране на конфигурацията
Windows 9x, NT и 2000	**winipcfg**
Linux/UNIX	**ifconfig**
Windows NT и 2000	**ipconfig**
NetWare	**config**

Макар че форматът и точната информация могат да се различават до известна степен, всяка помощна програма визуализира основна информация за конфигурацията, като използвания IP адрес, мрежовата маска (подмрежовата маска) и шлюз, а също допълнителна информация, като DNS сървъри, MAC (физически) адрес и др.

config на NetWare

Командата **config** на NetWare въвеждате от сървърната конзола. Разгледайте Пример 18-3 като илюстрация на действието на командата **config** на NetWare.

Пример 18-3 *Командата config в сървърната конзола на NetWare показва информация за IP конфигурацията.*

```
File server name: NETGUY
IPX internal network number: 394CEC29
    Node address: 000000000001
    Frame type: VIRTUAL_LAN
    LAN protocol: IPX network 394CEC29
Server Up Time: 1 Minute 22 Seconds

AMD PCNTNW
    Version 3.20   June 27, 1996
    Hardware setting: Slot 2, I/) ports 1000b to 101Fh. Interrupt 9h
    Node address: 005056AC01BA
    Frame type: ETHERNET_802.2
    Board name: PCNTNW_1_E82
    LAN protocol: IPX network 66745DBA

AMD PCNTNW
    Version 3.20   June 27, 1996
    Hardware setting: Slot 2, I/) ports 1000b to 101Fh. Interrupt 9h
    Node address: 005056AC01BA
    Frame type: ETHERNET_802.3
    Board name: PCNTNW_1_E82
    LAN protocol: IPX network 66745DBA

<Press ESC to terminate or any other key to continue>
```

ipconfig на Windows NT и Windows 2000

Командата **ipconfig** се използва в Windows NT и Windows 2000 за визуализиране на IP адреса, подмрежовата маска и подразбиращия се шлюз, за които е конфигуриран мрежовият адаптер. За да видите по-детайлна информация, използвате ключа **/all**. Пример 18-4 показва резултатите от използването на **ipconfig /all** на Windows NT сървър.

Пример 18-4 *Командата ipconfig с ключ /all се използва за визуализиране на подробна конфигурационна информация в Windows NT и Windows 2000.*

```
C:\>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : DS2000
        Primary DNS Suffix  . . . . . . . : tacteam.net
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : Yes
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : tacteam.net

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 3Com EtherLink XL 10/100
PCI TX NIC
                                            (3C905B-TX)
        Physical Address. . . . . . . . . : 00-50-04-7C-C0-D2
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.201
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

```
        Default Gateway . . . . . . . . . : 192.168.1.16
        DNS Servers . . . . . . . . . . . : 192.150.87.2
                                            216.87.128.131
        Primary WINS Server . . . . . . . : 192.168.1.185
```

Ако компютърът е конфигуриран като DHCP клиент, с **ipconfig** могат да бъдат използвани два допълнителни ключа. Първият е **/renew**. Той предизвиква подновяване на арендата за зададения IP адрес. Вторият е ключът **/release**, който предизвиква освобождаване на IP адреса, така че DHCP сървърът да може да го назначава отново.

ifconfig на Linux/UNIX

Командата **ifconfig** можете да използвате на компютър с UNIX/Linux, за да прегледате информацията за конфигурацията. Конфигурацията може да бъде променена с тази програма и с помощта на аргументи на командата.

СЪВЕТ За разлика от командите на Windows и NetWare, командата **ifconfig** в UNIX и Linux е чувствителна към разликата между главни и малки букви. Ако въведете **IFCONFIG** с главни букви, командата няма да бъде разпозната.

Пример 18-5 показва резултатите от изпълнението на командата **ifconfig** на Linux машина.

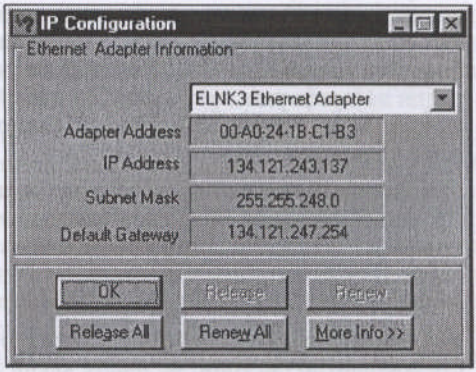
Пример 18-5 *Linux и UNIX използват командата ifconfig за визуализиране на конфигурационна информация.*

```
[root@noname /root]# ifconfig
eth0      Link encap: Ethernet   HWaddr 00:50:56:8Z:01:C9
          inet addr:192.168.1.128 Bcast:192.168.1.255
Mask:255.255.255.128
          UP BROADCAST RUNNING MULTICAST  MTU:1500   Metric:1
          RX packets:154 errors:0 dropped: 0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 frame:0
          collisions:0 txqueuelen:100
          Interrupt:9 Base address:0x1000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING   MTU:3924   Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

winipcfg на Windows 9x

Операционните системи Windows 95 и Windows 98 реализират помощната програма за конфигурация с графичен интерфейс. Въвеждането на **winipcfg** от командния ред визуализира екрана, показан на Фигура 18-14. **winipcfg** може да бъде използван с ключа **/all** за получаване на по-детайлна информация.

Фигура 18-14 *Операционните системи Windows 9x използват winipcfg – помощна програма, базирана на GUI.*



Други TCP/IP помощни програми

Тестването на възможността за връзка и проверката на информацията за конфигурацията са най-честите приложения на TCP/IP помощните програми при отстраняване на проблеми в мрежата. Но наред с тях могат да бъдат използвани и няколко допълнителни инструмента за събиране на конкретна информация:

- **Netstat и Nbtstat** – Те визуализират TCP/IP и NetBIOS статистическа информация.
- **ARP** (или „arp" в Linux и UNIX) – Използва се за визуализация и управление на кеша на протокола Address Resolution Protocol (ARP).
- **ROUTE** (или „route" в Linux и UNIX) – Използва се за преглеждане и промяна на елементите, записани в маршрутните таблици.

Указания за решаване на проблеми

Отстраняването на проблеми в мрежата изисква умения. Вашите шансове за успех са най-големи, ако използвате структуриран метод за откриване, анализиране и решаване на всеки проблем, когато го срещнете. Отстраняването на проблеми трябва да бъде осъществявано на принципа стъпка по стъпка.

Добрите умения за решаване на проблеми не са специфични за компютърните мрежи. Вземете например начина, по който докторът се опитва да реши сложен медицински проблем, или начина, по който инспекторът разкрива престъпление. Независимо от сферата, стъпките са едни и същи, а именно:

1. **Съберете информация** – Лекарят взема медицинския картон и кара пациента да му опише симптомите. Полицейският детектив задава въпроси на потърпевшите и на свидетелите. И двамата разчитат на техни собствени наблюдения и може да се обърнат към книги или други експертни документи, за да потърсят конкретни факти, свързани със случая. При отстраняване на проблеми в мрежата трябва да се научите да изслушвате потребителите, когато описват случилото се, и да формулирате уместни въпроси, за да съберете цялата информация, която ви е необходима за диагностициране на проблема.

2 **Анализирайте информацията** – Това е моментът, в който в играта влизат вашите знания и опит. Първо елиминирайте най-очевидните възможни причини. Ако пациентът се оплаква от главоболие, докторът не започва с извършване на мозъчна операция, а първо взема под внимание най-простите фактори, от които могат да произлизат симптомите. Както беше отбелязано по-рано, трябва да се уверите дали кабелът е включен, преди да преформатирате твърдия диск и да преинсталирате операционната система. Когато елиминирате възможности, всъщност стеснявате вашето търсене.

3 **Формулирайте и реализирайте план за „третиране" на проблема** – На базата на направения анализ, направете план за отстраняване на проблема. Вашият план трябва да включва и резервен план, в случай че първият опит не успее. Пристъпете към изпълнение на плана по организиран начин. Изпробвайте възможните решения *едно по едно*.

4 **Тествайте, за да проверите резултатите от третирането** – Дори ако сте абсолютно сигурни, че знаете какви са проблемите, решението и необходимите корекции, важно е да потвърдите успеха на вашите действия. Също така трябва да се уверите, че вашето „лекарство" няма някакви странични ефекти, които предизвикват допълнителни или различни проблеми.

5 **Документирайте всичко** – Отделете време да запишете подробностите на проблема и стъпките, които сте предприели за неговото коригиране. Добра идея е да запазите копие и на хартия. Помнете, че дори ако имате превъзходна фотографска памет, може един ден да преминете на друга работа. Вашият наследник може да ви бъде признателен за това, че няма да му се налага да повтаря вашите опити и грешки.

Когато отстранявате проблеми в мрежи или се стремите да оптимизирате производителността, не забравяйте да зададете реални цели и приоритети. Направете ценови анализ, ако не сте сигурни на кои проблеми трябва да дадете приоритет. Имайте предвид, че „разходите" не винаги са финансови; макар че вашите приоритети могат да зависят от бюджетни фактори, те трябва да бъдат повлияни също от въпросите на ефективността, графиците на времето и сроковете, и дори от вътрешните политики.

Отстраняването на проблеми е една от най-трудните задачи на мрежовия администратор. Това е също областта, в която добрият администратор доказва своята цена и правото на заплатата и званието, което носи.

Обобщение

В тази глава разгледахме важността на превантивната поддръжка и начина за наблюдение, управление и отстраняване на проблеми на нашите натоварени мрежови среди. Научихте как да идентифицирате тесните места в мрежата и как да установявате базови линии, по които може да бъде измерена производителността на мрежата.

Разгледахме как можете да измерите скоростта на вашата Интернет връзка и как да използвате софтуер за мрежов мониторинг, като Network Monitor на Microsoft, LANalyzer на Novell и решения на независими производители, като Sniffer Pro, за събиране на информация за производителността на мрежата.

След това разгледахме софтуера за мениджмънт на мрежата и за начина, по който може да бъде използван за документиране на хардуера, софтуера и топо-

логията на мрежата. Също така разгледахме начина за инсталиране на софтуера, управлението на лицензирането, отдалечения контрол на десктопите на потребителите и уведомяването на администраторите за значителни събития в мрежата. По-конкретно разгледахме популярни пакети за управление, като SMS на Microsoft, Manage Wise на Novell, Tivoli на IBM и Open View на Hewlett Packard. Разгледахме също помощната програма SNMP, включена в протоколния комплект TCP/IP, и CMIP – OSI братовчед на TCP/IP.

Изучихте хардуерните устройства, които могат да бъдат използвани за наблюдение и отстраняване на проблеми в една връзка. Тези устройства включват тон генератори и локатори, кръстосани кабели, TDR, хардуерни обратни връзки, кабелни тестери и осцилоскопи. След това се обърнахме към софтуерните инструменти и разгледахме използването на файлове-дневници и помощните програми на TCP/IP, за да изолираме проблемите в мрежата. Тези помощни програми включват ping, pathping, програмите за трасиране, помощните програми за конфигурация и други. Накрая дадохме някои указания за решаване на проблеми, за да ви помогнем да организирате вашите усилия за оптимизация и отстраняване на проблеми.

В тази книга научихте как можете да изградите мрежа от самото начало, започвайки от физическия слой. Научихте за хардуера и софтуера, които се събират, за да образуват модерната компютърна мрежа. В следващата и последна глава ще изложим насоките, в които се развива и разраства работата на мрежовия администратор в процеса на изграждане на един по-свързан свят с технологиите на бъдещето.

Допълнителни източници

Едно добро разглеждане на снифър софтуера е достъпно на http://secinf.net/info/misc/sniffingfaq.html.

Повече информация за решенията за мрежов мениджмънт Tivoli можете да намерите на адрес www.tivoli.com.

Демонстрация на Open View на Hewlett Packard можете да свалите от www.openview.hp.com.

Ръководство за помощната програма ping можете да разгледате онлайн на адрес www.hgmp.mrc.ac.uk/Embnetut/Universl/ping.html.

Въпроси за преговор

Следващите въпроси тестват вашите знания по материала, разгледан в тази глава. Прочетете всеки въпрос внимателно и изберете *най-правилния* от отговорите.

1 Какво е името на количеството данни, които реално могат да бъдат предадени по мрежа?

- **a** Пропускателна способност
- **b** Производителност
- **c** Скорост на подаване на информация
- **d** Базова линия

2 Кои от следните са софтуерно-базирани инструменти, които ви позволяват да прихващате отделни фреймове или пакети, докато пътуват по мрежата?

- **a** Протоколни анализатори
- **b** Монитори на производителността
- **c** Динамични рефлектометри
- **d** Филтри на пакети

3 Кое от следните е протоколен анализатор? (Изберете всички верни отговори.)

- **a** Network Monitor на Microsoft
- **b** Simple Network Management Protocol
- **c** Sniffer Pro
- **d** TCPCON на Novell

4 Кое от следните съдържа пълноценна, мощна версия на Network Monitor на Microsoft?

- **a** Open View
- **b** Tivoli
- **c** SMTP
- **d** SMS

5 Кои от следните програми за мониторинг използват интерфейс във формата на контролен панел? (Изберете всички верни отговори.)

- **a** Network Monitor
- **b** LANalyzer
- **c** Sniffer Pro
- **d** Performance Monitor

6 Кое от следните е истина за SMS? (Изберете всички верни отговори.)

- **a** SMS може да бъде използван за разпространение на софтуер.
- **b** SMS е включен в Windows NT и Windows 2000, но не и в Windows 9x.
- **c** SMS се използва за осигуряване на връзка между Windows мрежа и IBM мейнфрейм мрежа.
- **d** SMS включва мощна версия на Network Monotor на Microsoft.

7 Кое от следните използва MIB за организиране на информацията, която събира за мрежата?

- **a** Network Monitor
- **b** SNMP
- **c** Protocol Analyzer
- **d** ASP

8 Кое от следните е познато също като „лисица и хрътка“?

a Динамичен рефлектометър

b Осцилоскоп

c Тон генератор и локатор

d Цифров волт-ом метър

9 Кое е първото нещо, което трябва да проверите, когато срещнете проблем с връзката към мрежата?

a Конфигурацията на протоколите

b Файловете на операционната система за изправност

c Сървъра, за да се уверите, че потребителският акаунт е валиден

d Физическата връзка

10 Ако използвате система UNIX, кое от следните се използва за определяне на пътя, който пакетът изминава от изпращащия компютър до компютъра местоназначение?

a TRACERT

b TRACEROUTE

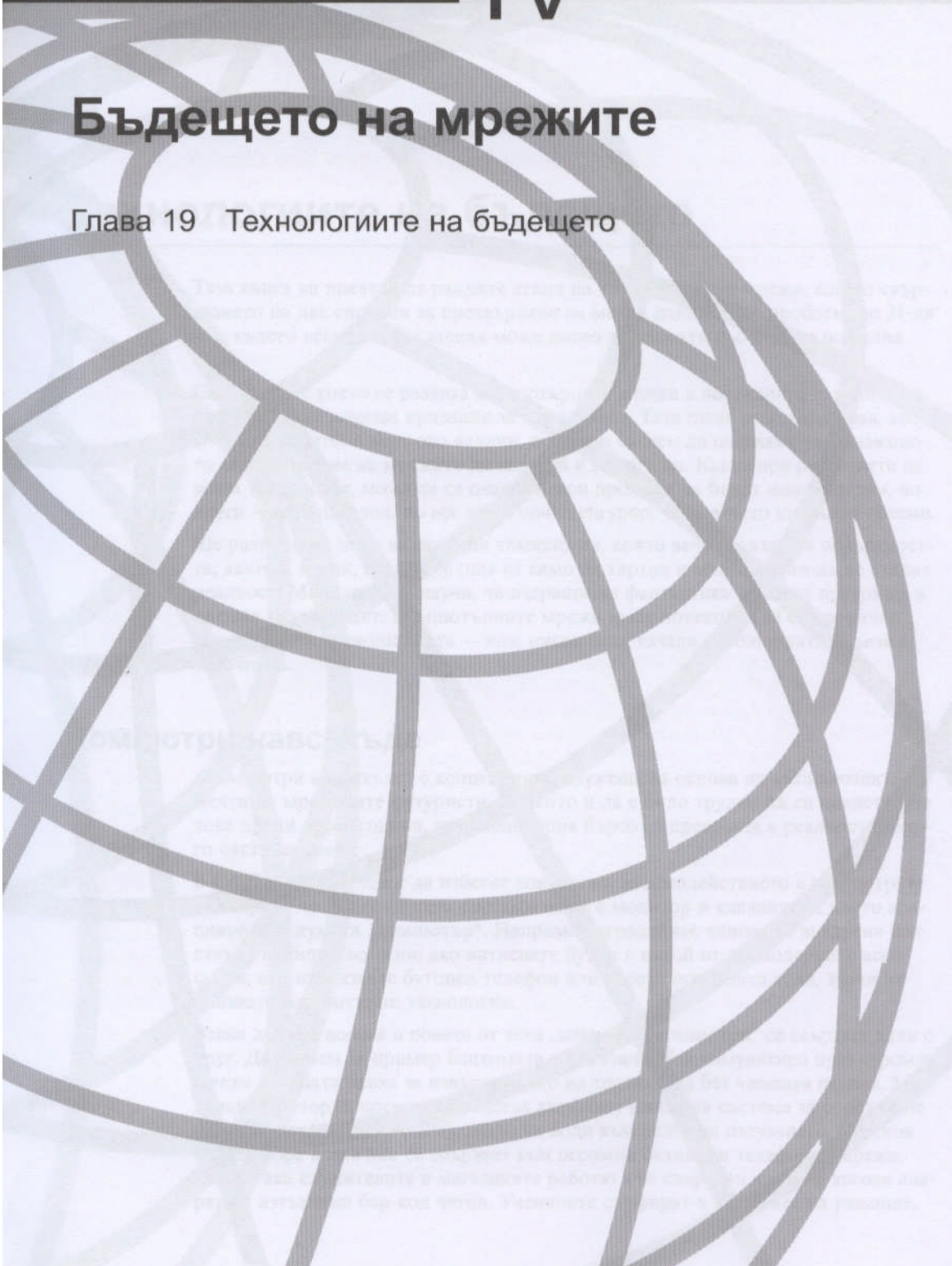
c tracert

d traceroute

Част IV

Бъдещето на мрежите

Глава 19 Технологиите на бъдещето



Глава 19

Технологиите на бъдещето

Тази книга ви преведе от ранните етапи на компютърните мрежи, когато свързването на две системи за прехвърляне на малко данни беше проблем, до 21-ви век, където всеки второкласник може лесно да изпрати съобщение по целия свят.

Скоростта, с която се развиха компютърните мрежи в последните години, е поразяваща и не показва признаци за намаляване. Тази глава разглежда това, което е в бъдещето, и многото начини, по които можем да очакваме увеличаващото се присъствие на мрежите да навлиза в живота ни. Както при развитието на всяка технология, може да се очаква някои промени да бъдат положителни, но други — отрицателни, но все пак е почти сигурно, че повечето ще бъдат големи.

Ще разгледаме нови вълнуващи технологии, които вече излизат на повърхността, както и някои, които все още са само на хартия и може никога да не станат реалност. Миналото ни научи, че вчерашната фантастика често се превръща в днешен научен факт. Компютърните мрежи имат потенциал за безгранични възможности, а еволюцията — или, някои биха казали революцията — вече е започнала.

Компютри навсякъде

„Компютри навсякъде“ е концепцията, служеща за основа на амбициозните мечти на мрежовите футуристи. Колкото и да е било трудно да си представите това преди десет години, тази концепция бързо се превръща в реалност в много части на света.

В САЩ е трудно човек да избегне контакта и взаимодействието с компютрите — въпреки че много от тези системи не са с монитор и клавиатура, които асоциираме с думата „компютър“. Например вградените чипове са внедрени навсякъде в обществото ни; ако натиснете бутон в някой от по-модерните асансьори, ако използвате бутонен телефон или карате нов модел кола, значи използвате компютърни технологии.

Всеки ден все повече и повече от тези „невидими компютри“ се свързват един с друг. Да вземем за пример банкомата в магазина. Той комуникира през огромна мрежа с вашата банка за извършването на транзакция без човешка намеса. Модерните моторни превозни средства включват глобална система за определяне на местоположението (GPS), която ви води към целта на пътуването. Стотици хиляди хора всеки ден се свързват към огромни безжични телефонни мрежи. Също така служителите в магазините работят със свързани в мрежа касови апарати с изтънчени бар-код четци. Учениците сърфират в Интернет на училище,

след което се прибират у дома, за да гледат любимите си телевизионни програми по мрежата на местната кабелна телевизия. Целта за компютри навсякъде е по-близко до реалността, отколкото мнозина си мислят.

В следващите секции на тази глава ще разгледаме следните аспекти на мрежовите технологии:

- Мрежите в дома
- Преодоляване на ограниченията на IP
- Нови насоки в мрежовите технологии

Мрежите в дома

Една от най-горещите нови маркетингови идеи в компютърната индустрия е за мрежа в дома. Навсякъде се рекламират продукти, предназначени да свържат лесно и просто два или повече компютъра в дома.

Много от тези решения за мрежи в дома използват традиционни Ethernet кабели. Напоследък дори някои строителни компании вграждат Ethernet кабели като част от инфраструктурата, точно както водопровода, електрическата инсталация и телефонните кабели.

Други технологии за мрежи в дома са базирани на по-иновативни идеи, като използване на съществуващите телефонни кабели или кабелите на електроинсталацията за предаване на сигнал. Безжичната мрежа е друга възможност, която се предлага на потребителя на домашна мрежа; тази алтернатива е особено атрактивна за хора, които не желаят да прокарват нови кабели през стените.

Засега най-честата форма на домашна мрежа е dialup връзката до доставчика на Интернет услуги. Много хора дори не осъзнават, че когато наберат доставчика си, техните компютри се превръщат в отдалечени възли на локалната мрежа на доставчика. Именно тази глобална връзка с Интернет е базата за появяващите се технологии.

Преди да стане възможно компютрите да са навсякъде обаче, трябва да бъдат преодолени някои технически ограничения. Най-неотложен е недостигът на IP адреси. Интернет е TCP/IP мрежа и всеки компютър, комуникиращ през TCP/IP, трябва да има уникален IP адрес.

Както беше обсъдено в предишните глави, текущата версия на IP, IPv4, използва 32-битови адреси. Това означава, че има „само“ 4 294 967 296 възможни адреса. Може да изглежда, че над 4 милиарда адреса трябва да са достатъчни; обаче тези, които са проектирали протокола в ранните дни на ARPAnet не са взели предвид, че необходимостта от адреси ще нарасне в такива размери.

Сега населението на света е над шест милиарда и се увеличава бързо. Ако се сбъдне мечтата на футуристите за универсална свързаност и ако всеки на земята има връзка с глобалната мрежа (да не говорим, че ще има отделна връзка за смарт тостерите, смарт хладилниците и т.н.), ограничението на IPv4 трябва да бъде преодоляно.

Преодоляване на ограниченията на IP

Плановете за реализация на следващото поколение на IP – IPv6 (наречено също IPng, от IP next generation) – е на хартия от няколко години. Internet Engineering Task Force (IETF) работят по спецификацията на новия IP от 1994 г.

Както обсъдихме в Глава 8, „Мрежови протоколи и услуги“, – използването решения със CIDR (Classless interdomain routing) и IP-sharing, като Network Address Translation (NAT) забави изчерпването на достъпните адреси. Но все пак това са само временни решения. Въпреки трудностите, които несъмнено ще произлязат от промени с такъв мащаб, Интернет в края на краищата ще направи прехода към новата версия на IP.

За да бъде преходът колкото се може по-безболезнен, фокусът е IPv6 да се разработи с максимална съвместимост със сегашната система. Идеята е IPv4 и IPv6 системи да могат да комуникират през междинния период преди новият IP да бъде напълно разгърнат. Това е критично важно за успеха на всички усилия по IPv6. Неуспехът на пакета OSI да замени TCP/IP беше основно заради липсата на правилен план за преход.

Колко по-добър е IPv6 от IPv4?

Най-значителната разлика между старата и новата версия на IP е адресното пространство. За разлика от 32-битовите адреси, използвани от IPv4, следващото поколение на IP ще използва 128-битово адресно пространство. Това ще даде 3.4^{38} IP адреса. Трудно е да възприемете обхвата на това число. Когато бъде изписано, то изглежда така:

340 282 366 920 938 463 463 374 607 431 768 211 456

С други думи, ще има по 3 911 873 538 269 506 102 адреса за всеки квадратен метър от повърхността на Земята. Това адресно пространство би трябвало да позволи достъп за предвидимото бъдеще, дори ако всеки човек на Земята има десетки устройства, изискващи отделни IP адреси.

Колко сигурен е IPv6?

Новият IP поддържа нови механизми за сигурност, като IPng Authentication Header (AH) и IPng Encapsulating Security Header. Може да разпознаете AH от нашата дискусия за IPSec в Глава 14, „Защита на мрежата“. IPv6 също така намалява бродкаст съобщенията в мрежата, което подобрява и производителността, и сигурността.

Реализация на IPv6

Не е възможно Интернет да бъде спрян за няколко дена или седмици, за да бъде направен преходът към IPv6. Затова са предложени няколко метода, които най-вероятно ще бъдат използвани в комбинация, за да бъде осъществен преходът от IPv4 към IPv6. Те включват постепенното въвеждане на промяната, и по-конкретно:

- **Двоен стек** – този метод позволява двете версии на IP да работят на едни и същи устройства в една и съща мрежа. IPv6 софтуерът работи паралелно IPv4 по начин, подобен на начина, по който различни протоколи (например IPX и TCP/IP) работят на едно и също устройство.
- **Транслиране** – С този метод IPv6 ще комуникира с IPv4 устройства чрез процес на конверсия на комуникациите на новия IP в стария формат. Това е сравнимо с начина, по който NAT транслира частните IP адреси в публични.

- **Тунелиране** – Чрез този метод IPv6 пакетите могат да бъдат тунелирани в IPv4. Това ще позволи на новата версия да работи в мрежа с IPv4 устройства, докато те бъдат обновени. Всъщност това създава виртуална IPv6 мрежа по IPv4 Интернет.

6bone е тестова IPv6 мрежа, която започна като виртуална мрежа, тунелирана през Интернет. Тя беше реализирана като част от проекта IPng на IETF. 6bone е широкообхватна мрежа с възли в повечето големи държави. Експериментите с IPv6 адресирането и маршрутизирането продължава чрез тази мрежа.

IPv6 Forum е организация, посветена на въпросите, касаещи новата версия на IP. Нейният Web сайт www.ipv6forum.com съдържа богата информация за следващото поколение на IPv6.

Нови насоки в мрежовите технологии

Новата версия на IP, колкото и да е вълнуваща, все още е базирана на традиционните мрежови технологии. Като поглеждаме напред в бъдещето, трябва да предвидим вероятността утрешните мрежи да бъдат базирани на изцяло нови компютърни или мрежови технологии. Въпреки че много от идеите днес звучат като научна фантастика, има сериозни изследвания в областта на невронните мрежи, базирани на начина, по който човешкият мозък комуникира с „възлите“ из тялото, както и в областта на квантовите мрежи, базирани на теорията на квантовата физика, работеща на атомно и субатомно ниво. Следващите секции описват някои от тези възможности.

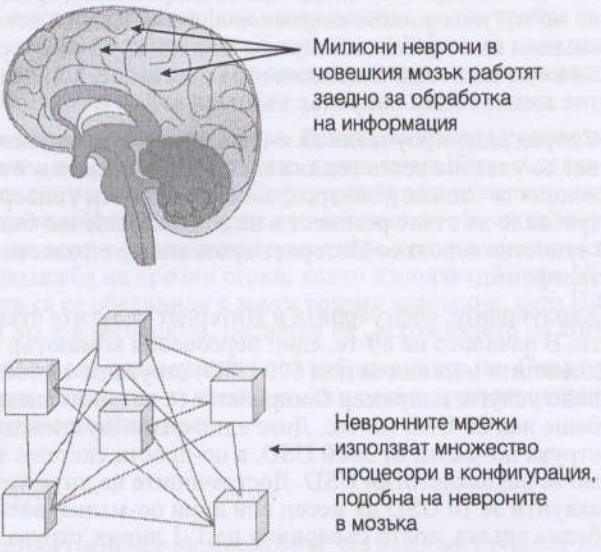
Невронни мрежи

Невронни мрежи вече е нашумял термин в компютърната индустрия; първоначалният замисъл за създаването на изкуствена невронна мрежа е базиран на моделиране на компютърна и мрежова архитектура по подобие на човешкия мозък. Това включва свързване на множество сравнително прости процесори в конфигурация, емулираща невроните в мозъка.

Моделът на невронната мрежа е изграден по идеята за паралелна обработка. Начина, по който използва голям брой малки процесори вместо един или два много мощни такива, е много различен от традиционната компютърна архитектура.

невронните мрежи биха дали основите за разработката на истински изкуствен интелект, който можем да считаме за върхово постижение в компютърната технология. (Ще разгледаме идеята за *изкуствения интелект* по-подробно в последната секция на главата.) Вижте Фигура 19-1.

Фигура 19-1 *Невронните мрежи използват множество малки процесори, които работят заедно като невроните в човешкия мозък.*



Квантови мрежи

Квантовата теория е базирана на идеята, че законите на физиката, приложими към макро света, който виждаме, не е задължително да са валидни в микро света на невероятно малките частици материя, съставящи атомите.

Основна предпоставка в квантовата механика е това, че субатомните частици, като електрони и протони, могат да съществуват едновременно в множество състояния. Тази концепция може драстично да промени начина, по който компютрите обработват информация. Традиционните компютри са базирани на двоичен код и зависят от факта, че даден бит може да бъде в едно от две състояния: включено (представяно чрез 1) и изключено (представяно чрез 0).

В света на квантовата физика, един квантов бит (наречен квабит), може да бъде едновременно и във включено, и в изключено състояние. Освен това множество квабитове могат да бъдат съединявани, за да можете да обработвате едновременно множество стойности. Технологиите за изображения с лазер и магнитен резонанс са разработени на базата на изследванията в квантовата физика.

Квантовата теория приема идеята за разклоняване на вселени (наречени мултивселени) и парадоксални идеи, като принципа на Котката на Шрьодингер, в който физикът Ървин Шрьодингер твърди, че котка в кутия е едновременно жива и мъртва. Сред другите учени, които допринасят за квантовите изследвания, са Макс Планк (основоположник на квантовата теория), Вернер Хайзенберг и Нилс Бор (който е помогнал за приемането на квантовата теория в научните среди, въпреки че Алберт Айнщайн се противял на възгледите).

Детайлна дискусия за квантовата теория е далеч отвъд обсега на тази книга, но тя допринася за невероятните предположения за бъдещето на компютрите и компютърните мрежи. Прегледайте секцията „Допълнителни източници“ в края на тази глава за повече информация.

Универсална свързаност

Ако „компютри навсякъде“ ще става реалност, трябва да постигнем състояние на почти *универсална свързаност*, в което всеки човек, който желае да бъде свързан към глобалната мрежа, има достъп до Интернет връзка. Въпреки че може да изглежда невъзможно за постигане, дори само в последното десетилетие имаме голям напредък към тази цел.

Според едно проучване на e-land, броят на потребителите на глобалния Интернет се удвоява всяка година след 1995 г. (вижте www.e-land.com). Ако тази тенденция се запази, универсалната – или почти универсалната – свързаност би трябвало да стане реалност в не толкова далечно бъдеще. В следващите две десетилетия вероятно Интернет връзката ще е толкова стандартна, колкото е днес телефонът.

Хардуерните, софтуерните и Интернет услугите стават все по-евтини с времето. В началото на 80-те, един персонален компютър (много по-маломощен от днешните машини за под 500 USD) струваше 10 000 USD, а dialup връзка за онлайн услуги, например CompuServe (с ослепителната скорост 900 – 1200 bps) беше над 20 USD на час. Днес едно силно мултимедийно PC с всички екстри струва по-малко от 3000 USD, а по-прости системи за Интернет се продават само за неколкостотин USD. Доставчиците на интернет услуги предлагат dialup акаунти за 10 USD на месец или дори по-малко, високоскоростна DSL или кабелна връзка, която съперничи на T-1 линия, струва по-малко от 50 USD на месец, а на много места има рекламно подпомагани безплатни Интернет услуги.

Утрешният Интернет вероятно ще бъде много по-интегрирана част от живота ни в сравнение с днешния Интернет. Вече няма да е необходимо да сядаме пред клавиатурата и монитора и да пускаме компютъра, за да влезем в киберпространството. Всъщност при най-новите технологии това не е необходимо дори днес. Безжичният Интернет, до който се осъществява достъп чрез клетъчни телефони и малки палм компютри, е в своето ранно детство, но расте бързо. Някои пейджъри са всъщност миниатюрни компютри, които могат да получават e-mail. Можем да очакваме утрешният Интернет да е съставен от разнообразни свързани устройства, много от които няма да приличат на традиционните компютри.

В следващите секции ще разгледаме „смарт“ уредите и това, как мрежите променят нашия живот и индустрията на забавленията. Ще разгледаме и проблемите с поверителността, изникнали в нашето глобално свързано общество.

„Смарт“ уреди

Терминът *Интернет уред* описва компактна специализирана система, която изпълнява само конкретен софтуер, като Web браузър или e-mail клиент, и осигурява лесен начин за достъп до Интернет – за сърфиране и изпращане на съобщения. Необходимо (или възможно) е само малко конфигуриране, а дружелюбността е най-важен приоритет.

Все пак терминът може да приеме ново значение в контекста на бъдещите технологии. Софтуерните компании, като Microsoft и Sun Microsystems, си сътрудничат с производителите на уреди, като Maytag и Whirlpool, за да създадат смарт хладилници и смарт микровълнови фурни. Според техните виждания за бъдещето, тези стандартни кухненски уреди ще бъдат снабдени с микропроцесори и ще бъдат свързани помежду си – и с Интернет.

За какво ѝ е на кафе-машината ви Интернет? Да предположим следния сценарий: в студен зимен ден се прибирате от офиса към дома и жадувате за чаша горещо кафе. Няма ли да е хубаво, ако при пристигането ви очаква готово горещо кафе? В нашата футуристична визия всичко, което трябва да направите, е да използвате свързания с Интернет безжичен телефон, за да осъществите контакт със свързаната с Интернет кафе-машина и да ѝ кажете да започне приготвянето на любимото ви кафе.

Смарт кафе-машината е само началото. Идеята за смарт уредите е част от по-амбициозна цел: „смарт къща". Emware, компания в Юта, създава мрежов софтуер за уредите с вградени чипове. Софтуерът прави възможно свързването на тези устройства към Интернет и дава възможност за обмен на информация. Това може да стане дори с уреди като термостати, поливна система за градината, автомати за продажба на дребни стоки, които използват 8- или 16-битови процесори. Emware са се обединили с други големи компании, като Hitachi, Phillips, SAP, Sybase и др. в консорциум, посветен на „вграждането на Интернет".

Възможностите са ограничени само от въображението ни. Смарт хладилниците вече са реалност – те могат да познават кога даден продукт свършва и да го поръчат автоматично по Интернет.

Мрежа в семейството

Широкото разпространение на мрежовите технологии променя живота ни по някои неуловими и други не толкова неуловими начини. Голяма част от вниманието на медиите е съсредоточено върху отрицателните неща, като проваленитe бракове поради „пристрастяването към Интернет" на единия съпруг или поради онлайн изневяра. Все пак Интернет е и основен фактор за сплотяването на семействата.

Технологиите за E-mail, чат на живо, видео конференции, Интернет телефония правят възможен близкия контакт между членовете на семейството и приятелите независимо от географското им местоположение. Домашната мрежа осигурява споделяне на файлове, принтери и Интернет връзка. Общият интерес към мрежите е тема за разговор и е дал тласък за не един семеен бизнес.

Преди 10 години никой не си е представял, че е възможно – освен за безумно богатите – да наблюдават бавачката или чистачката в реално време от работното си място. Днес това е икономически изпълнимо и е въведено в някои области. В бъдеще можем да очакваме мрежите да проникнат в домашния живот в още по-голяма степен и по начини, които понастоящем не можем да си представим.

Това е забавление

Една област, в която Интернет вече има голяма роля, е забавлението. Правни спорове вече се разгорещиха за споделянето на MP3 музикални файлове. Други правни въпроси касаят онлайн казината. Тези и подобни на тях случаи са усложнени от неопределеността на юрисдикцията, в която съществуват Web сайтовете. Често те се поддържат в страни, в които техните действия са законни, но са достъпни от страни, в които действията им са против закона. Разрешението на тези конфликтни закони е едно от най-големите предизвикателства пред глобално свързания свят.

Свалянето на електронни варианти на книги вече е нещо нормално, а с високоскоростните връзки през мрежата могат да бъдат прехвърляни дори филми.

Големите фирми за видеокасети под наем вече тестват пилотни програми със сваляне на филми, което би елиминирало нуждата да излизате от дома, за да си вземете филм.

Web е основен източник на забавления и онлайн са сайтове като ITEN (Internet Talk and Entertainment Network) и десетки сайтове с традиционни забавни публикации, като *Variety* и *Hollywood Reporter*. Всъщност Интернет е задвижваща сила в нарастващата популярност на концепцията за „инфозабавления". Терминът се отнася за представянето на информация и новини в забавен формат.

Въпроси за поверителността: Големият брат гледа

Универсалната свързаност води със себе си много въпроси за правото на поверителност, особено в правителствените институции и използването на информация, предадена по Интернет и други мрежи. Системата за наблюдение на e-mail на ФБР Carnivore и наблюдението на Интернет трафика от Великобританското разузнаване MI5 повдигнаха въпроси сред защитниците на поверителността.

Използването на информация, събрана от корпорации чрез Интернет с търговска цел е друг много обсъждан въпрос. Технологията позволява събирането на информация и следенето на посетителите на Web сайтове без тяхното знание или съгласие. Възможно е да се получи достъп до твърдия диск на потребителите и до данните там и да се получи контрол върху техните системи чрез тайно инсталиране на зловредни програми, които могат да бъдат разпространявани чрез e-mail или чрез скриптове на Web страници.

Много работодатели следят Интернет активността на своите работници, а и съдът в много случаи е определял, че имат право на това, когато е свързано със собственост и време на компанията.

Формирани са множество организации, посветени на запазването на онлайн поверителността, а законодателната власт[1] е формулирала закони като Children's Online Privacy Protection Act. Този закон влезе в сила през април 2000 г. Той е насочен към регулирането на събирането на информация за потребителя. Някои щати прокараха закони, защитаващи Интернет потребителите от кибер-измамници, използващи електронните комуникации за тормоз и заплахи. Възможно е 21-ви век да види много нови закони за прихващането, събирането и използването на предаваните данни – и от частни, и от публични лица.

Мрежа в дома

В допълнение към повдигнатите въпроси за наблюдаването на онлайн комуникациите на работника от страна на работодателя, мрежовите технологии промениха лицето на модерното работно място по много начини. Това е особено така за някои професии, както ще видим в следващите секции, а присъствието на мрежите ще се усеща във все повече сфери с времето.

Е-търговията засяга търговията на дребно, а Web-базираните реклами засягат бизнеса от всякакъв тип. Сега потребителите могат да пазаруват и да правят големи и малки покупки чрез компютърния си екран без да напускат дома си. Работещите у дома си и зависимите от компютри компании стават нещо нормал-

[1] Б. пр. В САЩ.

но. Мрежите променят начина на работа – от едноличния офис до подпомагана от правителството програма за изследване на космоса.

В следващите секции ще разгледаме как модерната технология е засегнала правителствените институции, правните и медицинските професии и издателската индустрия.

Влиянието на мрежовите технологии върху правителството

Местните, щатските и федералните правителства (в САЩ – б.пр.) все по-усилено използват Интернет за разпространение на информация до гражданите и за оползотворяване на вътрешните мрежи с цел увеличаване на продуктивността на служителите си. Следващите секции разглеждат тези въпроси.

Осигуряване на по-добри услуги на гражданите

Много градове поставят формуляри, например за смяна на местожителството и разрешителни за строеж, в Web във формат, подходящ за сваляне и отпечатване. Това спестява на гражданите пътуването до общината и спестява на служителите времето за раздаване на формулярите. Други услуги, осигурявани през Web от общините са:

- Справочници с телефонни номера за различни общински отдели
- E-mail адреси за оплаквания и въпроси от гражданите
- Обяви за свободни работни места
- Карти и упътвания за устройството на града
- Календари за събития в града
- Информация за данъците
- Бази данни с възможност за търсене в постановленията, наредбите и други публични документи

Щатските правителства публикуват подобна информация. Те публикуват също информация за пътуване и туризъм, онлайн версии на щатските закони, информация за контакти за избраните и назначени официални лица, ресурси за получаване на копия от свидетелства за раждане, информация за свидетелства за правоуправление на МПС, както и данни, генерирани от други програми и услуги.

Отделните институции на федералното правителство предлагат Web сайтове, FTP сайтове и Telnet достъп за гражданите. Например Internal Revenue Service предлага формуляри за данъчни декларации във формат, подходящ за сваляне. Добра отправна точка за информация за федералното правителство в САЩ е www.fedword.gov.

Намаляване на бремето за правителствените служители

Технологията засегна някои действия на правителствените офиси и процеси. Задачите с интензивно използване на данни, като събиране и обработка на информация за преброяване на населението и поддръжката на данни за данъците, са опростени чрез мрежата от компютри, използвани за съпоставяне на данните. Членовете на законодателни институции, от местно до национално ниво,

могат да използват частните и публични мрежи за бързо събиране на информация в помощ на определяне на държавната политика.

Компютърните войни и тероризмът

Докато страните по света стават все по-зависими от технологиите, как ще се отрази това на тъмната страна на национализма – воденето на война? Някои предричат, че в бъдеще войните ще се водят в киберпространството вместо на бойното поле. Свързани в мрежа роботи, вместо граждани, могат да бъдат изпращани за завземане на чужди брегове.

За оптимиста, новите технологии предлагат възможността за войни без кръв. Битките може да се водят изцяло между виртуални войници в мрежата. Тази практика вече е реалност в контекста на компютърните игри. Но заради човешката същност – такава, каквато е – амбициозната мечта за напълно безкръвни войни може никога да не се сбъдне. Все пак е напълно възможно технологическото развитие силно да намали броя на изгубените на бойното поле човешки животи. Например Space and Naval Warfare Center в Сан Диего са разработили безпилотни наземни, въздушни и подводни превозни средства, както и автономни наземни роботи и контролирани чрез виртуалната реалност „манипулатори", които могат да бъдат използвани за „ръчен бой" и други задачи на дълги разстояния.

За по-песимистичните, технологическият прогрес създава възможност кибертеристите да правят опустошения в напълно реалния свят. Те посочват, че универсалният достъп и усъвършенстването на технологиите може да доведе до сценарий със „Страшния съд". Хакери биха могли да проникнат в компютъризираните контролни пултове на ядрените ракети и да задържат цели нации като заложници. Враждебни сили биха могли да получат достъп до важни военни тайни. Деспотични правителства биха могли да наблюдават и контролират всеки аспект от живота на гражданите.

Мрежовите технологии могат да бъдат и част от „смарт бомби" и ракети, изискващи и използващи информация по време на полета си за коригиране на курса към целта си. Военните експерти и футуристи предвиждат, че хората-войници в недалечно бъдеще ще носят GPS устройства и друга свързана в мрежа апаратура.

Компютърните мрежови технологии – и по-специално безжичните комуникации – осигуриха начин за събиране на информация и за изпращането и на командващите. Подобно събиране на информация винаги е основно изискване за успешното водене на война. В бъдеще, вместо войните да бъдат печелени на базата на размера на армията, могат да бъдат печелени на базата на това, коя страна по-стратегически използва технологиите.

Правителствена подкрепа за разработка на технологии

Правителството на САЩ спомогна в развитието и поддръжката на Интернет инфраструктурата след като Department of Defense (DoD) спонсорира създаването на ARPAnet. В последните години създаването на информационна супермагистрала, осигуряваща широколентов достъп за цялата нация, е високо в приоритетите на федералното правителство.

На 15 февруари 2000 г. Камарата на представителите прокара The Networking and Information Technology Research and Development Act, който отрежда 126 милиона USD за специализирани федерални изследвания в областта на компютрите за фискалната 2000 г. В допълнение администрацията на Клинтън по-

иска 2,3 милиарда USD от бюджета за фискалната 2001 г. за изследвания и разработки в областта на новите технологии.

Ако миналото е индикатор, можем да очакваме правителствата по света да бъдат въвлечени в разработките на нови технологии и за използването им след тяхната поява.

Влиянието на мрежовите технологии върху закона

Голямата достъпност на информация през компютърните мрежи дълбоко засегна ежедневния живот на практикуващия адвокат. Правните изследвания, навремето времеотнемаща задача, сега са бързи, по-пълни и по-точни. Компютрите могат да претърсят хиляди страници случаи и изисквания на закона за малка част от времето, необходимо на човек да прочете текста.

Както е описано в следващите секции, новите технологии променят не само как се практикува законът, но също и как се прилага.

Информационно-базирано законодателство

Информацията е базата за законодателните и регулиращи решения, а универсалната свързаност носи още повече информация, при това по-бързо, на тези, от които зависят решенията. Членовете на Конгреса в САЩ, щатските законодателни власти, градските съвети и други законодателни органи могат да използват Интернет и частните мрежи за следното:

- Да изследват въпроси, свързани с конкретни законопроекти преди да гласуват за тях
- Да комуникират бързо и ефективно помежду си
- Да получават в реално време отзиви от избирателите

В някои щати законодателите имат достъп до компютър и мрежова технология още от входа на Конгреса. Представителите могат да проверяват Web анкети и e-mail, докато участват в законодателни сесии.

В бъдеще е възможно онлайн да става не само регистрацията на гласуващите, но дори самото гласуване. Преди това трябва да бъдат решени няколко въпроса за сигурността и удостоверяването, но в едно напълно свързано общество електронните урни може да носят много предимства.

Еволюцията в действие

Процесът на създаване на закони не е единствената област в правото, която се адаптира към новите технологии. Света на прилагане на законите също е силно засегнат, особено от настъпването на безжичните мрежи.

Много съвременно полицейски управления имат патрулни коли, снабдени с мобилни терминали с дисплеи (mobile display terminals – MDT) и лаптоп компютри с всички екстри. Те се използват за комуникации през безжична медия с други MDT и с мрежата на полицейското управление. Полицаите могат да използват терминалите, за да се свързват със щатските и националните бази данни за проверка на контролни номера, свидетелства за правоуправление и криминални проявления. В миналото полицаят трябваше да се обади по радио на диспечера в управлението, който на свой ред използваше компютри за получаване на информацията, след което устно я предаваше на полицая.

Сега полицейските превозни средства могат да са снабдени с GPS за осигуряване на прецизна информация за местоположението и за подобряване на времето на реакция при спешни случаи. Друга интересна употреба на технологията, комбинираща прилагане на закона и търговски интереси, е системата LoJack, в която на колите се монтира скрит предавател, за да може полицията да следи и открива откраднати превозни средства. в бъдеще можем да очакваме още подобни технологии при усилията за прилагане на закона.

Влиянието на мрежовите технологии върху медицината

Медицинската област е една от първите, възприели в голям мащаб мрежовите миниатюрни компютри. Докторите и медицинските сестри могат да записват данни в диаграмите на клиентите, а тези данни се синхронизират веднага в други системи в мрежата, като по този начин се увеличава ефективността на медицинските записи. Клинически справочници, като Merck и *Physician's Desk Reference*, също могат да бъдат достъпни в системата.

Дистанционно лекуване

Хирурзите вече изпълняват „дистанционни операции" чрез мрежа от свързани в мрежа компютри, като дистанционно контролират роботизирани устройства. Телемедицината – концепцията докторът да извършва предварителни прегледи на пациентите си с видеоконференция – е вълнуваща, дори и спорна, нова възможност.

Лекари в Интернет

Публикации като *MD netguide* са посветени на осигуряването на информация за онлайн ресурсите за лекари, като има няколко частни услуги за данни, в които лекарите могат да влязат и да намерят медицинска информация или да получат кибер-консултация с друг лекар.

Много лекари създават собствени Web сайтове, като осигуряват на пациентите си достъп до себе си посредством e-mail или чат на живо. Тези сайтове се използват за предоставяне на информация на пациентите за стандартни медицински условия, какво да очакват в случай на хоспитализация, стандартни медицински процедури, предупреждения за наркотици и други съвети за здравето. Целта е да се благоприятстват по-добри отношения лекар-пациент и да се отворят комуникациите, които биха довели до по-добро диагностициране и лечение.

Пациенти в Интернет

Има множество групи за онлайн поддръжка за тези, които имат нужда от помощ при справянето с хронически болести – и психологически, и физиологически. Пациентите и техните семейства могат да комуникират с други сърфисти в същото състояние и да обменят опита си и информацията за собствените програми за лечение, лекари и болници. Популярни организации като Alcoholics Anonymous, спонсорират Web сайтове и поддържат пощенски списъци и нюзгрупи за членовете си. В допълнение съществуват много търговски и некомерсиални Web сайтове, насочени към здравето. Те предлагат на болните много възможности и здравна информация, до които те нямаха достъп в миналото.

Съгласие за пълна информираност

Пациентите не само че могат да изследват медицинското си състояние с помощта на огромно количество информация, достъпно в медицинските училища и лаборатории, но могат и да получават информация за своите лекари. Множество Web сайтове събират и класифицират информация за лекари, болници и проблеми, на които са се натъкнали пациентите.

в бъдеще бази данни като National Physicians Database, която съдържа информация за действия срещу лекари във всеки щат, може да бъдат отворени публично в Интернет. Освен това бъдещите компютърни мрежови технологии обещават повече начини, по които медицинските лица ще могат да се свързват с пациентите.

Влиянието на мрежовите технологии върху издателската дейност

Последната нашумяла думичка в издателската индустрия е „e-book" (е-книга) и нарастващото предлагане на електронни книги, списания и онлайн вестници бавно, но сигурно променя издателската индустрия.

Продукти като Glassbook Reader for PCs и Microsoft Reader (с версии за PC и миниатюрни компютри) улесняват четенето на роман или консултирането със справочник в електронен формат. Предимствата на технологията са очевидни:

- Стотици хиляди книги могат да бъдат съхранени на минимално пространство. Същият брой отпечатани книги би заел цели стаи.
- Много електронни книги могат лесно да бъдат пренасяни от едно място на друго. Създаването на електронни книги не изисква рязането на дървета и по този начин те са по-дружелюбни към околната среда.
- Електронните публикации могат да бъдат продавани на по-ниска цена, тъй като разходите за отпечатване и разпространение са спестени.
- Грешките в електронните версии на даден книга могат да бъдат коригирани лесно и почти моментално.
- Авторите могат лесно сами да публикуват електронни, книги.
- Световното разпространение на електронни книги през Web и FTP е бързо и лесно.

Разбира се, електронното публикуване има и недостатъци. Например нарушенията на авторските права са по-лесни за извършване, а и на някои хора им е физически неудобно да четат от екран.

ЗАБЕЛЕЖКА Много от въпросите относно издателската индустрия са в сила и за музикалната индустрия. За да получат широка подкрепа, издателите и читателите трябва да преговарят за условията на всеки нов модел на достъп. Потребителите, които могат спокойно да изхвърлят книга или CD, след като са ги купили, не могат да разберат какво пречи законно да ги подарят, или да продадат електронно-записана музика, за която са си платили.

Има и други, по-практични недостатъци. Например някои от миниатюрните устройства се четат трудно на дневна светлина, и ако батерията им се изтощи, книгата вече не е достъпна. Все пак някои пуристи предвиждат, че в следващия

век хартиените книги ще остареят, а повечето или всички данни ще бъдат в електронен формат.

Нови начини за обучение

Технологията променя не само начина, по който четем; тя предлага нови начини за получаване на официално или неофициално образование. Мрежите и Интернет улесняват и опростяват взимането на даден клас или степен дори без да напускате дома си.

Онлайн университетите, акредитирани и неакредитирани, изобилстват. Много традиционни училища, от Ivy League до местния колеж, предлагат възможности за *дистанционно обучение*. Например Harvard University Extension School предлага курсове по информатика през Интернет.

Виртуалните часове могат да бъдат провеждани през Web сайтове, в които преподавателите публикуват задания и поддържат онлайн чат сесии. Студентите изпращат работата си по e-mail, а технологиите за аудио- и видео-конференции дават възможност за участие в часа „на живо". „Класната стая без стени" вероятно ще стане нещо обичайно за бъдещето. Образователният модел предлага на студентите удобството да учат по собствен график вместо да се налага да пътуват до мястото на занятията, а и е повече ценово-ефективно за обучаващите, които няма да се налага да поддържат специални за обучението сгради.

Според изследвания (Moore & Thompson, 1990 г., Penn State American Center for the Study of Distance Education; и Verduin & Clark, 1991 г., *Distance Education: The Foundations of Effective Practice*, Jossey-Bass), дистанционното обучение може да бъде точно толкова ефективно, колкото традиционните методи, когато технологиите са подходящи и когато има връзка студент-студент и обратна връзка учител-студент.

Изкуствен интелект

Изкуственият интелект (Artificial intelligence – AI) се дефинира като „симулация на човешките процеси на интелигентност чрез машини, и по-специално компютърни системи. Тези процеси включват научаване, разсъждаване и самокритика" (от IT енциклопедията Whatis.corn).

Компютърна програма, която може да емулира преценките и поведението на човек с опит в дадена област или сфера, се нарича *експертна система*. Системата разчита на огромна база данни и включва множество програмирани правила, дефиниращи как да се прилага базата знания в предварително дефинирани ситуации. Експертните системи включват програмата за игра на шах Deep Blue, разработена от IBM за среща със световния шампион по шах Гари Каспаров. Във фантастиката, пример за експертна система е холографският лекар на кораба *Voyager* в телевизионните серии на филма *Star Trek: Voyager*.

Компютрите могат да мислят

Истинският изкуствен интелект е способен не само да сортира данни и да осигурява предварително програмирани отговори, но също да се учи от опита си. С други думи, машината ще може да мисли и да разпознава отношения, да прави обобщения и да различава нюанси – умения, които засега никой компютър не е овладял.

Усилията за създаване на интелигентен компютър станаха по-интензивни през последното десетилетие. Повечето големи университети, включително престижни училища като MIT, имат програми, посветени на тази цел. Военните агенции (например, U.S. Navy's Center for Applied Research in Artificial Intelligence) са силно „замесени" в проекти за изкуствен интелект. За изследвания са изхарчени милиарди долари. Да, колкото и да са удивителни възможностите на модерните компютри, засега те са много далеч от човешкия мозък.

Компютрите правят едно нещо много добре и много бързо: обработката на числа. Обаче компютрите, както ги познаваме днес, са роби на програмистите; не могат да вземат решения или да изпълняват действия, за които не са програмирани. Мислещият компютър ще бъде изцяло нов и различен вид устройство.

Ако и когато такива машини станат реалност, е неизбежно те да бъдат свързани в мрежа за споделяне на информацията. Някои изследователи вярват, че в края на краищата тези машини не само ще се присъединят една към друга, но ще бъдат свързани и с човешки същества за създаването на полуорганични, полутехнологични същества.

Кибернетични форми на живот: абсолютната мрежа

Кибернетични форми на живот – човеци, или *киборги*, с електронни и механически импланти – свързани за споделяне на „колективно съзнание" – това е честа тема в научната фантастика. В допълнение, кибернетиката е област със сериозни изследвания в университетите по света. Всъщност някои изследователи вярват, че свързването на тяло и компютър може да бъде начин хората най-накрая да постигнат безсмъртие.

Обобщение

В тази глава разгледахме бъдещето на мрежите и това, как утрешните технологии ще променят света, в който живеем днес.

Започнахме с дискусия на това, как целта за „компютри навсякъде" бързо става реалност и как тази концепция ще промени начина на работа на Интернет и на другите мрежи. Научихте начините, по които могат да бъдат преодолени ограниченията на Internet Protocol, включително временните решения, като NAT и CIDR, които вече са вградени широко.

След това разгледахме крайното решение за недостатъка на IP адреси: нова версия на IP, наречена IPv6. научихте характеристиките на новия протокол и методите за осъществяване на плавен преход от текущата версия, IPv4.

След това се докоснахме до някои от новите насоки в мрежовите технологии и бъдещи възможности, като невронните мрежи и мрежите, базирани на квантови компютри. После разгледахме концепцията за универсална Интернет свързаност и това, как тя ще повлияе на нашия живот вкъщи и на работа. Научихте за проектите за „смарт уреди" и „смарт дом", които вече са на път, като разгледахме социалните и правни въпроси, които със сигурност ще изскочат, когато светът стане по-„свързан".

По-конкретно, очертахме някои от начините, по които днешните мрежови технологии са повлияли в сферите на държавното управление, правото, медицината и издателската дейност. Погледнахме също как някои бъдещи технологии биха могли да променят тези професии още повече. В допълнение, обърнахме

внимание на новите начини на обучение през Интернет и на това, как традиционните модели за обучение се адаптират по новите технологии.

Накрая завършихме главата и книгата с поглед в бъдещето и разгледахме усложненията, ако настоящите „невъзможни мечти", като истински изкуствен интелект и кибернетични форми на живот, станат реалност.

Тази книга ви преведе от основите на компютърните мрежи до области които, понастоящем, са теоретични. Завършваме с един принцип, в който сме се убедили от самото създаване на персоналните компютри и мрежите: Днешните технологии, колкото и сложни и усъвършенствани да изглеждат, ще бледнеят в сравнение с утрешните технологии.

Допълнителни източници

Отлична статия за IPv6 има на адрес http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html#CH1.

Задълбочена дискусия за IPv6 мрежата 6bone има на адрес www.6bone.net.

Добро, кратко, просто обяснение на квантовата физика има онлайн на адрес www.jracademy.com/~jtucek/science/what.html.

За повече информация относно въпросите за поверителност в Интернет, вижте Web сайта Electronic Privacy Information Center на адрес www.epic.org.

Web сайтът за технологиите в правителството има на адрес www.govtech.net.

подробен обзор на китайските възгледи за войните на 21-ви век можете да намерите в Web сайта на Institute for National Strategic Studies на адрес www.ndu.edu/inss/books/chinview/chinapt4.html.

За повече информация относно миниатюрните компютри за медици вижте www.handheldmed.corn.

Добър ресурс за информация и връзки за дистанционното обучение има в Distance Learning Resource Network (DLRN) на адрес www.dlrn.org.

Journal of Artificial Intelligence Research е онлайн на адрес www.cs.washington.edu/research/jair/home.html.

Сайтът на American Society for Cybernetics е на адрес http://gwis.circ.gwu.edu/~asc/asc-cyber.html.

Въпроси

Като завършвате тази фаза от обучението си и преминавате напред към кариера в областта на компютърната мрежова технология, ето няколко провокиращи мисълта въпроси, над които може да помислите:

- Как ще използвате компютрите в работата си след три години? Какво ще е по-различно в сравнение със сега?
- Как ще бъдат засегнати личните ви взаимоотношения от компютрите? Въобще ще бъдат ли засегнати?
- Какви промени, ако има такива, ще настъпят в живота ви – емоционално, физически, финансово или по друг начин – поради развитието на компютърната технология?

- Колко време ще отделите в следващото десетилетие за изучаване на компютърна технология?
- Колко от това, което сега знаете за компютрите, ще бъде полезно след три години? А след десет години?
- Как можете да спечелите пари от Интернет с личния си бизнес до една година? Какъв Интернет бизнес бихте могли да развиете за една година, така че да ви осигури поне средно, но все пак достатъчно допълнителни доходи?
- Каква работа в компания в компютърната индустрия бихте могли реално да задържите в следващата една година, която би ви осигурила добър живот?
- Бихте ли гласували за президент киборг?
- Ще станете ли следващия Бил Гейтс или Стив Джобс и ще постигнете ли слава и богатство като изключително успешен предприемач в областта на информационните технологии?

Приложение А

Отговори на преговорните въпроси от главите

Това приложение съдържа отговори на преговорните въпроси от книгата, намиращи се в края на всяка глава.

Глава 1

1 **B.** Оптичната телеграфна мрежа е разработена от французите в началото на 19-ти век и е била способна да предава по 20 знака в секунда. По това време Самюел Морз демонстрира електрическия телеграф в САЩ. Телефонната мрежа започва развитието си едва към края на 19-ти век, а Ethernet мрежите се реализират за пръв път в изследователския център на Xerox в Пало Алто (Palo Alto Research Center — PARC) през 1960-те. ARPAnet също се заражда през 1960-те години.

2 **D.** Телефонните комуникации се предават по комутируеми вериги. Това означава, че дадена верига се установява за времетраенето на сесията, но ако тази верига се разпадне и после се възстанови, може да се използва напълно различна верига. Комутирането на пакети е по-нова технология, използвана в компютърните мрежи. Layer 2 и Layer 3 комутирането се отнасят до технологии, използвани в LAN мрежите за подобряване на производителността чрез създаване на специализирани пътища от един компютър до друг.

3 **A.** Технологията за комутиране на пакети, разработена от изследователи в MIT, института RAND и NPL, беше проектирана да обработва пикови предавания, при които данните се предават на пресекулки. Комутирането на вериги е по-подходящо за предаване на глас, което е по-постоянно. Терминът „аналогово“ се отнася до използвания метод на предаване на сигналите, а комутиращите централи се използват за ръчно изграждане на вериги.

4 **A** и **C.** Мейнфрейм хардуерът по принцип е по-скъп от PC-тата. Мейнфрейм компютрите по традиция са с по-ниска отказоустойчивост, защото един мейнфрейм представлява единична точка на прекъсване. Терминалите не притежават собствена изчислителна мощ и са безполезни, ако мейнфреймът не работи. Мейнфрейм компютрите са способни да обработват огромни количества данни и са подходящи при интензивна обра-

ботка. PC-тата са по-несигурни от мейнфреймовете, защото съдържат локални харддискове и флопидискови устройства, позволяващи на потребителите да зареждат програми (вероятно вкарвайки вируси) или да копират важна информация.

5 **A**, **B**, **C** и **D.** Мрежовите компютри могат да споделят както хардуерни, така и софтуерни компоненти. Потребителите могат да изпращат данни на принтерите по мрежата, да споделят модемни връзки (с помощта на подходящ софтуер), да осъществяват достъп до данни, съхранени някъде в мрежата (ако техните потребителски акаунти притежават необходимите позволения за достъп), както и да стартират приложения, инсталирани на приложни сървъри.

6 **B** и **C.** Факс машините могат да бъдат класифицирани и като входни, и като изходни устройства в зависимост от това, дали факс данните пристигат или се изпращат. Цифровите фотоапарати са входни устройства, използвани за заснемане на цифрови изображения, след което прехвърлят тези изображения на компютъра. Плотерите и принтерите са изходни устройства; те получават данни от компютъра и създават хартиено представяне на данните.

7 **D.** Системата за имена на домейни (Domain Name System – DNS) беше разработена през 1980-те, когато броят на хост компютрите в ARPAnet нарасна до ниво, при което трябваше да се намери ефективен начин за преобразуване на имената на хост компютрите в IP адреси. DoD е съкращение от Department of Defense (Министерство на отбраната на САЩ) – главният „виновник" за създаването на ARPAnet. DHCP означава Dynamic Host Configuration Protocol (протокол за динамично конфигуриране на хостове) – метод за автоматично назначаване на IP адреси на компютри. DSL означава Digital Subscriber Line (цифрова абонатна линия), високоскоростна широколентова услуга, предлагана от телефонните компании в много области за трансфер на данни и глас.

8 **B.** Приложенията за телефония комбинират телекомуникациите и компютърните технологии, като например реализираните според TAPI (Telephony Applications Programmers Interface) на Microsoft. Консорциумът ITC установява стандартите, свързани с телефонията.

9 **C.** В една клиент/сървър мрежа, компютърът, заявяващ данни от друг компютър, се нарича клиент. Компютърът, който споделя своите данни с клиента, се нарича сървър. Работната станция също може да бъде клиент, но някои работни станции представляват самостоятелни компютри, които не осъществяват достъп до мрежови ресурси. Терминалът не е компютър, а по-скоро комплект от входни и изходни устройства, свързани към компютър (често пъти централен мейнфрейм).

10 **A.** Правилата, конектор които компютрите комуникират един с друг, се наричат протоколи. Тези правила определят формáта на изпращаните данни и последователността на тяхната обработка. Преносната среда представлява физическите средства, по които се предават данните – кабели, ефир, светлинни вълни и т.н. Байтът е единица за измерване, описваща размера на файл с данни или изпратена единица данни, и се състои от осем бита (един бит е по-малка единица). Топологията представлява плана на мрежата.

Глава 2

1 **B.** Категориите, използвани за класифициране на една мрежа според физическия ѝ обхват, са WAN, LAN и MAN. 10Base2 е класификация, използвана при категоризиране според архитектурата. IPX/SPX се използва при категоризиране по използвания протокол. Кръговата мрежа е тип, който се дефинира при категоризиране според топологията.

2 **C** и **D.** LAN мрежите са най-малките мрежи, категоризирани по физически обхват, и обикновено се ограничават до неголяма географска площ, в която компютрите се намират близо един до друг. Големите мрежи, съставени от множество малки мрежи се наричат MAN, или по-скоро WAN. Една WAN мрежа, но не и LAN, обикновено има възли в различни градове, щати или държави.

3 **A.** Една интермрежа представлява група от мрежи, които са свързани помежду си. Най-добрият пример за това е глобалният Интернет. Интернет и екстранет мрежите използват Интернет технологии като Web браузъри и FTP, но те са частни мрежи, ограничени до специфични потребители. Работната група е група от компютри, чиито потребители често осъществяват достъп до едни и същи ресурси.

4 **B**, **C** и **D.** Клиент/сървър мрежите осигуряват централизирано хранилище за данни на мрежови сървъри, което улеснява архивирането на данните. В такива случаи обикновено се изисква назначаване на мрежов администратор, тъй като клиент/сървър мрежите работят със сложни мрежови операционни системи, инсталирани на сървърите. Централизираният клиент/сървър административен модел осигурява по-добра сигурност. Клиент/сървър мрежите обаче са по-скъпи за реализация, тъй като се налага използване на специализиран сървърен софтуер и назначаване на един или повече мрежови администратори.

5 **C.** Клиент/сървър мрежите на Microsoft се разделят на групи от компютри и ресурси, наречени *домейни*, а сървърът, в който потребителите се логват, за да осъществят достъп до домейна, се нарича домейн контролер (или контролер на домейн). Демонът е UNIX термин за програма, която работи непрекъснато и обслужва заявки за услуги. SAM (security accounts manager) е базата данни, която съдържа информация за сигурността за потребителите и групите на един Windows NT компютър. Един клъстерен сървър изпълнява софтуер, позволяващ на множество сървъри да бъдат обединени в група, работеща като един компютър с цел отказоустойчивост и балансиране на натоварването.

6 **C** и **D.** В една група всеки компютър поддържа индивидуална локална база данни за сигурност. Даден потребител трябва да има акаунт на всяка машина, до която иска да осъществи достъп. За всеки споделен ресурс се задава парола; това се нарича сигурност на ниво споделен ресурс. За разлика от клиент/сървър средата, сигурността не е централизирана и не може да се контролира от мрежов администратор, а се управлява локално от потребителя на всяка машина, която има споделени ресурси. Поради тази причина сигурността не е толкова голяма, колкото при клиент/сървър мрежите.

7 **A** и **D.** За разлика от Windows NT, който беше базиран на SAM (security account manager) база данни, разположена в главния домейн контролер, Windows 2000 домейните са базирани на Active Directory. В една Windows 2000 мрежа може да съществуват множество домейн контролери,

като всеки от тях има възможност да чете и записва в директорийната база данни. Windows NT позволява само на PDC да извършва запис в базата данни за сигурност. Bindery е базата данни за сигурност, използвана от по-старите NetWare сървъри (версия 3.*x*). *Windows NT домейните понякога се наричат домейни от по-долно ниво.*

8 **A** и **B.** TCP/IP е подходящ избор за протокол при мрежи със среден и голям размер. За малките мрежи е по-добре да работят с по-прости и по-бързи протоколи като NetBEUI или IPX/SPX. Глобалният Интернет е TCP/IP мрежа. Съществуват множество инструменти и помощни програми за наблюдение, отстраняване на проблеми и администриране на TCP/IP мрежи. Въпреки това е по-трудно да се администрира TCP/IP мрежа, отколкото такава, която работи с NetBEUI. Причината е в сложността на схемата за адресиране, въпроса с маршрутизирането и по-големият типичен размер на мрежата.

9 **C.** Линейната шинна топология се разполага като линия, като кабелът преминава от един компютър към следващия. Кабелът изисква във всеки от краищата да има устройство, наречено терминатор, който да неутрализира отразяваните сигнали. Мрежата тип звезда представлява компютри, вързани към централен хъб. Мрежата тип хибридна решетка притежава излишни връзки между някои, но не и между всички компютри. Една Token Ring мрежа представлява по-скоро архитектура, отколкото топология, и обикновено се реализира като физическа звезда.

10 **B.** Спецификациите за 10BaseTмрежи включват звездна топология и UTP кабел, обикновено Cat 5. Една 10Base2 мрежа използва тънък коаксиален кабел в конфигурация тип шина. 100BaseFL мрежите работят с влакнесто-оптичен кабел. Token Ring мрежите обикновено използват IBM екраниран кабел тип усукана двойка.

3

1 **B.** Шестнадесетичната бройна система използва цифри от 0 до 9 и букви от A до F, за да представя числени стойности. Често се използва в компютърната индустрия, защото конвертирането от шестнадесетични в двоични числа е по-лесно, отколкото от десетични в двоични. Десетичната бройна система е тази, която използваме ежедневно. Машинният код се отнася до потока от битове (двоични цифри), които се обработват от компютъра.

2 **A.** Двоичната цифра се нарича бит. Байтът обикновено се равнява на 8 бита (в света на микрокомпютрите). Кубитът е бит, който е в неопределено състояние. Гиг е съкращение от гигабайт.

3 **C.** В двоичното число 10010001, битовете за стойностите 1, 16 и 128 са включени (единиците). Сумата на тези стойности дава 145. Изключените стойности (нулите) имат стойност 0 и поради тази причина не засягат резултата. Преобразуването на двоично в десетично число включва сумирането на всички стойности, представени 1-ци. Десетичното число 256 в двоична форма ще бъде 100000000, 128 двоично е 10000000, а 64 двоично е 1000000.

4 **B.** Единица данни, която може да се управлява и да се изпраща по мрежата, се нарича пакет, или алтернативно – фрейм (кадър) или сегмент. Хексадецимал (прочетено буквално от английски) е шестнадесетичната бройна система. Хедърите са информация, намираща се в началото на

всеки пакет с данни и съдържат служебни данни. Въпреки че по мрежата наистина се предават битове, файловете с данни не се разделят на индивидуални битове, а на групи от битове (пакети).

5 **D.** Компонентът за проверка за грешки в трейлъра на пакета с данни се нарича cyclical redundancy check (CRC). Тя е средство за извършване на двоични изчисления върху пакета при компютъра източник и компютъра местоназначение, след което резултатите се сравняват, за да се гарантира, че данните не са променяни. В трейлъра няма бит за верификация. Един фрейм представлява единица данни, като например пакет, която се изпраща по мрежата. UDP означава User Datagram Protocol, безвръзково-ориентиран протокол от транспортния слой, който е част от TCP/IP.

6 **B.** Моделът е „схематично описание на система, теория или явление, което представя нейни познати или предполагаеми свойства и може да бъде използвано за допълнително изучаване на нейните характеристики". Мрежовите модели се използват за графично представяне на процеса на мрежовите комуникации. Протоколите са набори от правила, позволяващи на компютрите да комуникират. Процесът е серия от действия, промени или функции, довеждащи до резултат. Слоевете са различни нива, на които работят протоколите в даден комплект; популярните OSI и DoD мрежови модели се наричат слоести модели.

7 **B.** Каналният слой (Layer 2) е разделен на подслоевете Media Access Control (MAC) и Logical Link Control (LLC). Физическият, мрежовият и транспортният слой не се разделят на подслоеве.

8 **A.** Физическият слой не добавя хедърна информация, защото той се занимава с мрежовия хардуер и предаването на сигналите. Каналният, сесийният и приложният слой (както и представителният и мрежовият слой) добавят цялата хедърна информация, която се обработва от съответния слой на приемащия компютър.

9 **C.** NetBIOS и Winsock са два популярни протокола от сесийния слой. NetBIOS позволява на два компютъра да установят връзка и осигурява откриване на грешки и възстановяване. TCP (Transmission Control Protocol), подобно на UDP, е протокол от транспортния слой. IPX, както IP, е протокол от мрежовия слой. Telnet е протокол от приложния слой.

10 **D.** Един активен хъб представлява повторител, притежаващ портове, към които могат да се свържат множество станции. Той регенерира сигнала, преди да го изпрати кум останалите компютри в мрежата. Мостът е Layer 2 устройство, използвано за сегментиране на мрежата и намаляване на трафика. Маршрутизаторът е Layer 3 устройство, което препредава пакети от една подмрежа към друга. Суичът е устройство (Layer 2, 3 или 4, в зависимост от реализацията), което изпраща сигнала навън само към компютъра, за който е предназначен пакетът.

Глава 4

1 **B.** Процесът на превръщане на двоичните данни в импулси (електрически или светлинни) се нарича модулация или кодиране. Криптираните данни са такива, които се разбъркват, за да се защити съдържанието от неоторизиран достъп. Защитените данни могат да бъдат криптирани, защитени с права за достъп или други методи. Пулсацията е просто ритмично разширяване и свиване или туптене.

2 **D.** Цифровите сигнали се наричат сигнали в дискретно състояние, защото тяхното състояние се променя от едно в друго почти моментално, без постепенно изменение. Електронната вълна, която се променя постоянно е аналогов сигнал, а аналоговите сигнали се измерват в цикли според три характеристики: амплитуда, честота и фаза.

3 **C** и **D.** Аналоговите сигнали по принцип са по-лесни за мултиплексиране (комбинират се за увеличаване на честотната лента) от цифровите и са по-неподатливи към ефекта на затихване (отслабването на сигнала с нарастване на разстоянието). Аналоговите сигнали обаче са по-податливи на смущения като EMI (електромагнитни смущения), а цифровите устройства за по-евтини за производство, защото предаването на цифрови сигнали е по-просто.

4 **A.** Теснолентови технологии като Ethernet използват целият капацитет на кабела, за да изпращат данните в един канал. Широколентовите технологии като DSL разделят сигнала на множество канали. Мултиплексираните предавания комбинират сигналите, за да увеличат пропускателната способност, а многосвързаната (мултилинк) технология може да се използва, за да осигури по-висока обща пропускателна способност по аналогови телефонни линии или ISDN.

5 **A** и **D.** Теснолентовото предаване на сигнали е двупосочно; сигналите могат да пътуват и в двете страни, така че можете да изпращате и приемате по един и същ канал. Теснолентовото предаване обикновено се асоциира с технологиите за предаване на цифрови сигнали, макар че може да се използва и при аналогови предавания. CATV е широколентова технология; сигналът се разделя на десетки различни сигнали. Широколентовото предаване е еднопосочно, въпреки че честотната лента може да бъде разделена на два канала, като единият се използва за предаване, а другият за приемане.

6 **C.** С оптичен кабел се използва мултиплексирането DWDM (Dense Wavelength Division Multiplexing), като всеки сигнал се пренася по различна дължина на светлинната вълна. FDM (Frequency Division Multiplexing) комбинира множество канали по една линия за предаване, като на всяка линия се назначава различна честота. TDM (Time Division Multiplexing) разбива всеки сигнал на сегменти с кратко времетраене и ги изпраща по линията в редуващи се времеви отрязъци. MPPE е протоколът Microsoft Point to Point Encryption, който няма нищо общо с мултиплексирането.

7 **D.** Асинхронните предавания се характеризират със старт и стоп бит, които да идентифицират началото и края на предаването и да синхронизират тактуването. Синхронните предавания включват вграден механизъм за синхронизация и могат да използват различни типове синхронизиране, включващи гарантирана промяна на състоянието (най-често използваното) и овърсемплинг.

8 **B.** Честотите на градските радиостанции, полицейските и таксиметровите радиостанции и подобните двупосочни радио технологии са примери за полудуплексно предаване, защото сигналът може да пътува и в двете посоки, но не едновременно. Традиционните телевизионни предавания са симплексни – сигналът се предава само в една посока. Обикновените телефонни комуникации и DSL технологиите са пълнодуплексни предавания; при тях сигналите могат да пътуват и в двете посоки едновременно.

9 **A.** UTP кабелът е най-податлив на електромагнитни смущения (EMI), въпреки че усукването на двойката проводници вътре в кабела спомага за намаляване на тази уязвимост. Коаксиалните кабели и STP са екранирани, което ги предпазва от EMI, въпреки че всички медни кабели са податливи на смущения до известна степен. Влакнесто-оптичният кабел, който вместо електрически импулси за предаване на сигналите използва светлина, не е податлив на EMI и е най-добрият избор в среда, в която има голямо количество електромагнитна енергия.

10 **B.** CSMA/CD е методът за достъп, указана за Ethernet мрежи. CSMA/CA се използва в AppleTalk мрежи. Предаването на маркер е методът за достъп в Token Ring мрежите, а приоритетът по заявка е метод за достъп, използван от рядко реализираната 100VG-AnyLAN мрежа.

Глава 5

1 **B.** 802.3 спецификациите се отнасят за метода за достъп CSMA/CD, използван от Ethernet мрежите. Token Ring и FDDI са базирани на спецификациите 802.5, а ARCnet се базира на спецификациите 802.4. Инженерите от IEEE разработиха спецификациите 802, за да дефинират стандарти за протоколите от физическия и каналния слой.

2 **A.** CSMA/CD е методът за достъп, използван от Ethernet мрежи. При този метод компютърът, който иска да предава данни, „подслушва“ преносната среда и изпраща данните, ако по кабела няма трафик. Ако едновременно с него и друг компютър направи същото, двете машини усещат колизията, след което всеки изчаква произволен интервал от време, след което пак изпраща данните. CSMA/CA се използва от AppleTalk мрежите; Предаването на маркер се използва от Token Ring, ARCnet и FDDI, а приоритетът по заявка се използва от 100VG-AnyLAN.

3 **A.** Спецификациите за 10Base2 Ethernet мрежите, използващи тънък коаксиален кабел, ограничават броя на възлите на един кабелен сегмент (дължината на кабела между повторителите) до 30. Възелът е компютър или друго мрежово устройство, което предава и приема данни по мрежата.

4 **C.** BNC конекторите се използва с тънък коаксиален кабел в Ethernet 10Base2 мрежи. Кабелът с неекранирана усукана двойка (UTP) в 10BaseT мрежите използва RJ конектори, обикновено RJ-45. Дебелият коаксиален кабел в 10Base5 мрежите използва 15-изводен AUI конектори за свързване към външен приемопредавател, който пък се свързва към кабела посредством „вампирски зъб“. Оптичните кабели използват SMA или FSMA конектори.

5 **D.** терминът стандартен Ethernet се отнася до 10Base5 мрежи (thicknet). Въпреки че thicknet е по-малко популярна от останалите Ethernet архитектури (днес UTP-базираните архитектури са най-масово използваните), 10Base5 беше „стандарт“, когато Ethernet мрежата беше разработена (през 1960-те), поради което тя все още се води за стандарт в индустрията.

6 **B.** 10Base5 спецификациите за мрежи, използващи дебел коаксиален кабел, ограничават дължината на сегмента до 500 метра, като за сравнение това ограничение е 100 метра за 10BaseT и 185 метра за 10Base2. Това по-голямо разстояние прави thicknet мрежата подходящ избор за „гръб-

начни“ сегменти. Спецификациите на IEEE за дължините на кабелите се дават в метри.

7 **B** и **C.** Token Ring мрежите могат да работят със скорост 4 или 16 Mbps (в зависимост от мрежовата карта и хъба). Token Ring хъбът, или концентраторът, се нарича multistation access unit (MAU или MSAU). Token Ring е активна топология, в която всяка станция регенерира сигнала, преди да го предаде по кръга. Подобно на Ethernet, Token Ring е тесно-лентова архитектура; цялата честотна лента на кабела се използва за предаване на един сигнал.

8 **C.** Наблюдаващият компютър изпраща фрейм, наречен маяк, като всеки компютър очаква приемането на маяка. Ако той не пристигне, когато е очакван, компютърът уведомява наблюдаващия за собствения си адрес и този на своя най-близък възходящ съсед (nearest active upstream neighbor – NAUN). MSAU устройството може след това да реконфигурира пътя на сигнала, за да изключи нефункциониращата станция, а комуникациите се възстановяват за останалата част от кръга. маркерът е сигнал, който циркулира и всяка станция трябва да чака за него, преди да може да предава данни. кадърът с данни съдържа предаваната информация.

9 **B.** LocalTalk е оригиналният протокол от каналния слой, предназначен за бързо и лесно изграждане на (за съжаление, бавни) мрежи от Macintosh компютри чрез кабели, свързани към техните паралелни портове. LocalTalk предава със скорост само 230,4 Kbps и в много Macintosh мрежи е заменен от Ethernet. EtherTalk е протокол, позволяващ на Macintosh-и, работещи с AppleTalk протоколи, да участват в Ethernet мрежа с коаксиален кабел. TokenTalk позволява на Macintosh-ите да се свързват към Token Ring мрежи.

10 **A.** Стандартната ARCnet е относително бавна, работейки само със скорост 2,5 Mbps. От популярните мрежови архитектури само LocalTalk е по-бавна. Беше разработена подобрена версия на ARCnet, която да преодолее това ограничение; ARCnet Plus работи със скорост 20 Mbps, което е два пъти по-бързо от скоростта на стандартния Ethernet и по-бързо от „високоскоростните“ Token Ring мрежи, работещи на 16 Mbps.

6

1 **A**, **C** и **D.** За вътрешни не-Plug and Play модеми обикновено трябва да се конфигурират I/O адрес, IRQ и виртуален com порт. Тези настройки могат да се променят чрез джъмпери, dip ключета или софтуер. IP адресите могат да се задават на модемна връзка, когато компютърът участва в TCP/ IP мрежа, но това не е хардуерна конфигурация.

2 **B.** CSU/DSU и PAD са примери за оборудване на страната на клиента. CSU/DSU устройството се използва за осигуряване на интерфейс към T-носеща линия. CSU приема и предава сигнали от и към WAN линия. DSU управлява линията, грешките при синхронизация и регенерирането на сигнала.

3 **A.** Изброените технологии са все такива с комутиране на веригата. В една мрежа с комутиране на вериги се установява връзка, по която се изпращат данните за времетраенето на сесията. При мрежите с комутиране на пакети отделните пакети могат да поемат по различни маршрути, за да достигнат местоназначението. Switched 56 е тип мрежа с комутиране на пакети. Всички споменати технологии са WAN.

4 **B**, **C** и **E.** ISDN линиите трябва да се инсталират от телефонната компания и по принцип са по-скъпи от обикновените аналогови линии. В централата на телефонната компания трябва да се инсталира специално оборудване, което да обработва цифровото предаване, а от страната на клиента трябва да се инсталира ISDN терминален адаптер (неправилно наричан понякога ISDN модем). ISDN може да предава както глас, така и данни. При една BRI линия, състояща се от два B канала, гласовото предаване се извършва по единия от каналите, докато по другия продължават да се предават данни.

5 **C.** Топологията тип звезда е най-мащабируема, защото добавянето на още възли към мрежата не изисква нейното преконфигуриране. Кръговата топология е най-трудна за „уголемяване“, защото добавянето на нов възел означава прекъсване на връзката между два съществуващи възела. Топологията от точка до точка по дефиниция не може да се разширява.

6 **B.** Първата технология за комутиране на пакети беше X.25. Frame Relay е по-нова технология, разработена на базата на X.25 схемата, но с добавени подобрения. ATM е най-новата технология за комутиране на пакети и осигурява висока скорост. DSL е технология с комутиране на вериги.

7 **A**, **C** и **D.** Frame Relay предлага по-висока производителност от X.25 – до 45 Mbps. Тя не включва широката проверка за грешки, използвана от X.25, което и не се налага, защото тя използва по-надеждни цифрови сигнали. X.25 използваше аналогово предаване. Както Frame Relay, така и X.25 използват комутиране на пакети.

8 **B**, **C** и **D.** Отличителна характеристика на ATM е дължината на клетката, която е фиксирана на 53 байта. Това е високоскоростна технология, способна да предава видео, глас и данни едновременно, като използва предварително дефинирани вериги.

9 **D.** OC-SONET с ранг OC-48 има върхова скорост на предаване от 2,488 Gbps. ADSL реализациите варират от 384 до около 6 Mbps. T-1 има максимална скорост на предаване 1,544 Mbps. ISDN BRI предава с максимална скорост от 128 Kbps (два свързани 64 Kbps канала).

10 **C** и **D.** NAT използва таблица, за да асоциира множество частни вътрешни IP адреси с един или повече външни публични адреси, като по този начин се избягва регистрирането на публични адреси за всеки компютър във вътрешната мрежа. NAT обаче не може да се използва с технологиите за криптиране, които не позволяват смяната на IP хедъра, а също така технологията не е съвместима с някои приложения.

Глава 7

1 **C.** Мрежовата карта (NIC) е най-основният хардуерен компонент. Мрежов интерфейс се изисква за всеки компютър, който се свързва в мрежа. Повечето мрежови карти са предназначени за ISA/EISA, PCI или PCMCIA (PC card) шини. някои мрежови адаптери са вградени директно на дънната платка на компютъра. Маршрутизатор се използва за препредаването на пакети от една мрежа към друга. Кабелът е преносната среда, използвана от традиционните мрежи; безжичните мрежи обаче не се нуждаят от кабел. Хъбът свързва компютрите, когато се използва топология звезда.

2 **B.** Мрежите, използващи thicknet кабел в съответствие с 10Base5 спецификацията, използват външен приемопредавател, който се свързва към мрежовата карта посредством AUI конектор, а към кабела посредством вампирски зъб. 10Base2 (thinnet) и 10BaseT (UTP) мрежите използват мрежови карти с вграден приемопредавател.

3 **A.** IRQ 5 често пъти се използва за звукови карти; само че звуковата карта на този компютър е установена на IRQ 10. IRQ 7 е подразбиращото се IRQ за основния паралелен (принтерски) порт (LPT1), който е зает. IRQ 12 е подразбиращото се IRQ за PS/2 мишка. Главният IDE контролер на компютъра използва IRQ 14. Не се споменава за втори паралелен порт на компютъра, рака че IRQ 5 трябва да е свободно за мрежовата карта.

4 **D.** Терминът за пространството между етажните плочи и окачените тавани се нарича пленум, така че за инсталирането в това пространство кабелът трябва да е огнеупорен (от клас plenum), т.е. да е опакован в тефлон или друг негорим материал (вместо поливинилхлорид).

5 **B.** За 10Base2 мрежите е указан RG-58 A/U – тънък коаксиален кабел със стандартна сърцевина. На външен вид RG-58 /U е подобен, но има плътна медна сърцевина и не отговаря на спецификациите на 10Base2. RG-58 C/U е военен еквивалент на RG-58 A/U и притежава по-дебела външна обвивка. Той може да се използва за 10Base2 мрежи, но не е типичният избор. RG-59 е кабел за кабелна телевизия.

6 **C.** Дебелият коаксиален кабел (thicknet) се използва в 10Base5 мрежите, които използват външен приемопредавател; той се свързва към мрежовата карта посредством AUI конектор, а към кабела чрез вампирски зъб. UTP, STP и тънкият коаксиален кабел използват мрежови карти с вграден приемопредавател.

7 **D.** Смесването е преминаването на сигнала от един проводник в друг, когато проводниците са в близост един до друг. Усукването на проводниците един около друг намалява или предотвратява това. Степента на защита от смесване се увеличава с нарастване броя на усукванията на фут. RFI означава радиочестотни смущения, идващи от радиосигналите. Затихването представлява загуба на сигнала с увеличаване на разстоянието. Изкривяването е липсата на качествено приемане или нежелано изменение във вълновата форма на сигнала.

8 **A.** Ethernet Cat 5 кабелите по принцип използват RJ-45 конектори, подобни на телефонните (RJ-11), само че са по-големи. BNC конекторите се използват с тънък коаксиален кабел в 10Base2 мрежи. F конектор се използва за свързване на два кабелни сегмента в кабелната телевизия.

9 **B** и **D.** Влакнесто-оптичният кабел е по-сигурен от медния, защото е по-трудно за нарушителите да се прикачат към него, за да прихващат сигналите, тъй като самите сигнали представляват светлина, а не електрически импулси. Еднорежимният оптичен кабел е по-бърз от многорежимния, защото при втория има разлика във времената на пристигане на отделните светлинни импулси. С оптичен кабел се работи по-трудно и е по-неудобен за инсталиране от медния, поради което се изисква квалифициран персонал. Влакнесто-оптичният кабел е по-неподатлив на затихване от медния, поради което и дължината на един сегмент може да е значително по-голяма.

10 **C.** Повторител се използва за свързване на два кабелни сегмента и повтаряне (регенериране) на сигнала при преминаването му от единия сегмент в другия. Това елиминира ефекта на затихване и удължава мрежата.

Цилиндричните конектори, панелите за свързване и пасивните хъбове са прости устройства за свързване, които не регенерират сигнала. Активните хъбове обаче работят като многопортови повторители.

Глава 8

1 **C.** NetBEUI е високопроизводителен протокол с малко служебна информация и е лесен за установяване. Тъй като той не използва логическо адресиране, той не може да бъде маршрутизиран към други мрежи/подмрежи. Използва се в малки работни групи, компютрите в които работят под операционни системи на Microsoft.

2 **A.** IPX нарича частта от адреса, която идентифицира устройството и включва MAC адреса, номер на възел. Той се отбелязва като шестнадесетичен запис и се използва, заедно с мрежовия номер, да маршрутизира IPX пакет към правилното местоназначение.

3 **A** и **D.** И TCP, и SPX работят в транспортния слой на референтния OSI модел, осигурявайки установяване на връзка преди изпращането на данни. UDP е безвръзково-ориентиран протокол от транспортния слой, а IP и IPX са безвръзково-ориентирани протоколи от мрежовия слой.

4 **B** и **C.** Един IP адрес представлява 32-битово двоично число, съставено от четири октета, които съдържат по осем бита. Въпреки че компютърът ги обработва като двоични числа, IP адресите обикновено се записват в точково-десетичен формат.

5 **C.** Класовото адресиране позволява 16 384 мрежи от Клас B, всяка от които може да съдържа 65 535 хост компютъра. Могат да съществуват 126 мрежи от Клас A с над 16 милиона хоста всеки, и 2 097 152 мрежи от Клас C. ограничени до 254 хост компютъра.

6 **B.** В една Клас C мрежа първите три октета идентифицират мрежата. Битовете за мрежовия идентификатор се „маскират“ с 1-ци, т.е. по осем единици за всеки от трите октета: 11111111.11111111.11111111. В десетичен запис това е 255.255.255. Битовете за идентификатора на хоста (последният октет) са „отворени“, като това се посочва от нулите: 00000000. Десетичната стойност на това е 0. И така, десетичният запис за подмрежовата маска е 255.255.255.0.

7 **B.** Старшите битове в един Клас B адрес са 10. Това означава, че десетичният диапазон за първия октет е 128–191. Клас A адресите използват диапазона 0–127, Клас C адресите използват диапазона 192–223, а Клас D адресите използват диапазона 224–239.

8 **C.** CIDR спомага за по-ефективното използвана на IP адреси, като се разделя със старите адресни класове и позволява размерите на мрежите да попадат навсякъде в Клас A, B и C.

9 **D.** DHCP служи за автоматично назначаване на IP адреси на компютри, конфигурирани като DHCP клиенти, като това става чрез четиристъпков процес на договаряне за наем (откриване, предлагане, заявяване и потвърждение).

10 **C.** ARP преобразува IP адреси във физически хардуерни (MAC) адреси. Помощната програма ARP ви позволява да разглеждате кеша с преобразуваните адреси, да изтривате записи и да добавяте перманентни съответствия между IP и MAC адреси.

9

1 **B.** Точките на свързване, изграждащи гръбнаците, се наричат възли. Хостовете са индивидуални компютри в Интернет. Подмрежите са частите, на които се разделят мрежите. Сървърите са компютри, които споделят ресурси с останалите компютри в мрежата.

2 **D.** NAP точките са местата, където доставчиците на достъп се свързват един с друг. Интернет доставчиците (ISP) са компании, които се свързват с гръбнака на Интернет и осигуряват на клиентите dial-in или посветен достъп до своята мрежа. vBNS е част от проекта Internet2 – съвместна инициатива на университетите на САЩ, насочена към разработката на високоскоростен гръбнак, който може да се използва за тестване на нови технологии. Услугата vBNS е изградена чрез свързване на пет суперкомпютърни центъра.

3 **C.** Хипертекстът се отнася до способността за вграждане на връзки в документите към други текстови файлове, графики, звуци и т.н. Хипертекстовите файлове могат, но не е задължително да бъдат разположени на Web сървър и до тях да се достига чрез URL адрес. (HTML Help е пример за хипертекст.) Хипертекстовите файлове могат и често съдържат вградени графики.

4 **C.** http://bigserver.acme.com/ има правилния синтаксис за достъп до подразбиращата се Web страница на Web сървър с име bigserver в домейна от второ ниво, наречен acme, който се намира в домейна от най-високо ниво – .com. Въпреки че много Web сървъри имат име „www," то *не е задължително*. В този случай се използва протоколът HTTP; HTML е език за форматиране, в който се кодират страниците.

5 **B.** Порталите са Web сайтове, предназначени да служат като стартова точка за Web потребителите. Една машина за метатърсене комбинира резултатите от множество машини за търсене, а подразбиращият се шлюз е IP адресът на маршрутизатор в една TCP/IP мрежа. Хипервръзките са указатели към други файлове, кодирани в HTML документи.

6 **D.** IMAP е сложна услуга, позволяваща на потребителите да гледат и да манипулират съобщенията, без да ги свалят на локалната машина. SMTP е протоколът, използван за изпращане на поща по Интернет. SNMP е помощно средство за наблюдаване, събиране на информация и управление от комплекта TCP/IP. POP се използва за сваляне на e-mail съобщения от пощенски сървър към e-mail клиентска програма на компютъра на потребителя.

7 **C.** NNTP (понякога наричан Usenet) се използва за хостване и осъществяване на достъп до нюзгрупи. За управление на пощенските списъци се използва софтуер като Listserv и Majordomo. Telnet е протоколът, използван за свързване към отдалечен сървър с цел разглеждане на файлове и стартиране на приложения. NetWare 5.*x* е способна да работи с TCP/IP без IPX/SPX.

8 **A.** Системата IRC позволява на потребителите да се свързват с IRC сървъри и да се присъединяват към канали, в които могат да провеждат текстово-базирани дискусии в реално време с един или повече потребители. Telnet се използва за свързване към отдалечен сървър с цел разглеждане на файлове и стартиране на приложения. IGMP се използва в мултикаст комуникации. FTP се използва за валяне на файлове от други компютри и за качване на файлове от вашия компютър към други компютри в мрежата.

9 **B.** Стандартът H.323 на ITU спада към мултимедийните комуникации по IP и IPX, което включва технологии за видео конференции, не осигуряващи QoS.

10 **A** и **D.** RIP за IP е дистанционно-векторен протокол с динамична маршрутизация; той е подходящ за малки и средни мрежи, но е по-неефективен и по-малко мащабируем от OSPF, който е динамично маршрутизируем протокол за състояние на връзките, разделящ мрежата на области.

Глава 10

1 **C.** Клиент/сървър приложенията използват така наречения front end софтуер (т.е. клиент), представляващ потребителско приложение на клиентска машина, което заявява данни от back end машината – сървърът за бази данни. Сортирането и обработката на заявките се извършва на сървъра, а на клиента се връщат само резултатите.

2 **B.** Един ресурс, като например файл, папка или принтер, който е направен достъпен за останалите потребители в мрежата, се нарича споделен ресурс.

3 **A.** Сигурността на ниво потребител, която изисква от потребителя да помни само една парола за логване, е по-добра и по-лесна за администриране от сигурността на ниво споделен ресурс, при която за всеки споделен ресурс трябва да се помни отделна парола.

4 **A**, **C** и **D.** Главният административен акаунт се създава по време на инсталиране на операционната система и се използва за логване в операционната система за пръв път. Главният акаунт има пълен достъп до всички мрежови ресурси; ето защо за него трябва да се подбира силна парола. Административният акаунт се използва, когато искате да изпълнявате управленски задачи, като например да създавате нови потребителски акаунти.

5 **A** и **D.** Буквите в горен и долен регистър (главните и малките букви), както и цифровите знакове, по принцип са приемливи при задаването на имена на акаунти, но интервалите и знакове като + например трябва да се избягват. Някои операционни системи ограничават броя на знаковете, които могат да бъдат използвани, но име с осем знака се разпознава дори от MS-DOS машини.

6 **C.** Windows домейните са сбор от потребители, компютри и ресурси, върху които администраторът упражнява административна (управленска) власт. Домейните в Windows 2000 (но не и в Windows NT) могат да бъдат организирани в йерархични структури, наречени дървета, които пък се групират в гори.

7 **B.** User Manager for Domains е инструментът, използван за създаване на потребителски акаунти в един Windows NT 4.0 домейн контролер. Един инструмент, наречен User Manager, е наличен за Windows NT 4.0 Workstation и самостоятелни сървърни машини, но се използва за създаване на локални потребителски акаунти, валидни само за конкретната машина.

8 **C.** Active Directory е новата директорийна услуга на Microsoft, върху която се изграждат Windows 2000 мрежите. AD до известна степен е по-

добна на NDS – директорийните услуги на Novell, като и двете са съвместими с LDAP стандартите.

9 **D.** NetWare 3.*x* сървърите използват плоска база данни, наречена bindery, която съхранява информация за сигурността за сървъра, на който се намира. Тя не се репликира на останалите сървъри в мрежата. NetWare 4.x и по-новите версии използват NDS – йерархична дистрибутирана база от данни, позволяваща достъп от един потребителски акаунт до всички ресурси в мрежата.

10 **A** и **C.** UNIX операционните системи, за разлика от Windows и NetWare, са чувствителни към регистъра. Сървърните услуги, като например услугата за принт сървър, се наричат демони. Главният административен акаунт в UNIX се нарича root, а групите в една UNIX система работят много подобно на локалните групи в Windows NT 4.0, които са валидни само на този сървър.

1

1 **C.** Директорията (справочникът) е база данни, която може да съдържа най-различни типове информация. В една обектно-ориентирана система директорията съдържа обекти, а всеки обект има атрибути.

2 **B.** Когато данните се разпростират на две или повече физически машини в мрежата, базата данни е дистрибутирана.

3 **B** и **C.** NTDS на Windows NT и базата данни bindery на Novell, използвана в NetWare 3.*x*, са плоски бази данни; NDS на Novell и Active Directory на Microsoft са йерархични.

4 **D.** Едно родствено пространство от имена е такова, в което имената на дъщерните обекти съдържат в себе си името на родителския обект. Едно дърво от Windows 2000 домейни е пример за родствено пространство от имена.

5 **C.** Стандартите OSI X.500 указват директория, построена на DSA агент, който управлява директорийните данни, DUA агент, който дава на потребителите достъп до директорийните услуги, и DIB база, където се съхранява директорийната информация.

6 **C.** Отличителното име (distinguished name – DN) е средството за идентифициране на пълния път до директориен обект, което използва атрибути като DC (DomainComponentName – име на компонент на домейн), OU (OrganizationalUnit – организационна единица) и CN (CommonName – общо име).

7 **A.** NDS има два основни типа обекти: контейнерни обекти (които могат да съдържат други обекти) и листови обекти, които представляват ресурсите в края на клона.

8 **D.** SysVol (Shared System Volume) файлът съхранява скриптовете и обектите за групови политики, които се използват от администраторите за контролиране средата на потребителя и ограничаване на потребителските права.

9 **B.** В едно дърво от Windows 2000 домейни, всички домейни споделят двупосочни транзитивни доверителни отношения. Това означава, че потребителите, принадлежащи на един домейн, могат да осъществяват достъп до ресурси в друг домейн, стига да разполагат с подходящите позволения за достъп.

10 **C.** ACL е сборът на всички позволения за достъп, назначени на един Active Directory обект.

Глава 12

1 **A** и **B.** Текстово-базираните операционни системи като DOS и UNIX по принцип са по-бързи от графичните операционни системи като Windows, защото се използват по-малко ресурси. Графичните потребителски интерфейси обаче са по-лесни за научаване и използване от повечето потребители, а освен това се осигурява и многозадачност.

2 **C.** командата **winipcfg** извиква графично представяне на информацията за конфигурацията на TCP/IP в Windows 95 и Windows 98. **ifconfig** се използва за същите цели на Linux и UNIX компютрите; **ipconfig** се използва в Windows NT и 2000 машини, а **config** е командата, използвана на NetWare сървъри, работещи с TCP/IP.

3 **D.** Суфиксът, който може да се използва за идентифициране на типа на файловете, се нарича файлово разширение. Файловите клони са двете части на един Macintosh файл. Файловите таблици са бази данни, поддържани от файловите системи, за да могат да следят къде върху физическия диск са разположение данните на всеки файл.

4 **A.** За разлика от FAT32 и NTFS, FAT16 може да се използва от всички операционни системи на Microsoft, включващи DOS, Windows 3.*x*, Windows 9*x*, Windows NT и Windows 2000. FAT16 не предлага сигурността на ниво файл, налична в NTFS, а и е по-малко надеждна, защото не включва възможности като гореща поправка. Въпреки че FAT16 използва по-малко служебна информация и поради това се представя по-добре при малки дялове, в повечето случаи FAT32 и NTFS осигуряват по-добра производителност.

5 **D.** NTFS поддържа дялове до 16 ексабайта. 2 GB е ограничението за дял в DOS, а FAT16 не може да използва дялове над 4 GB независимо от операционната система. 4 TB е максималният размер на дял, поддържан от FAT32.

6 **C.** В UNIX главната (root) директория се представя като наклонена черта (/) и не използва буква на устройство като част от пътя. Всяко ниво от йерархията се разделя от наклонена черта, вместо обратно наклонена черта (\), използвана във файловите системи FAT и NTFS.

7 **B.** Файловата система на UNIX използва вътрешен номер, наречен i-възел (i-node), за да идентифицира всеки файл или директория и асоциира номера с местоположението на данните върху физическия диск. Останалите файлови системи не използват тази система, макар че HFS на Macintosh каталогизира записите по подобен начин.

8 **C.** Услугата CSNW е включена в Windows NT Workstation, макар че не се инсталира по подразбиране. Веднъж инсталирана, тя ви позволява да се логвате в NetWare сървър и да осъществявате достъп до неговите файлове. Gateway Services for NetWare се инсталира на NT Server, за да позволи на неговите клиенти да осъществяват достъп до NetWare файлове по индиректен начин. File and Print Services for NetWare е продукт, който може да се купи от Microsoft, за да позволи на NetWare клиенти да осъ-

ществяват достъп до файлове на NT или Windows 2000 сървър. Макар че трябва да се използва IPX/SPX-съвместим протокол за комуникация с NetWare сървъра, NWLink се инсталира автоматично, когато инсталирате CSNW; поради това не се налага да го инсталирате изрично.

9 **A.** Файловата система SMB (Server Message Block), базирана на кода на Samba, може да се инсталира на Linux, за да осигури достъп до Microsoft ресурси. NCP означава NetWare Core Protocol – протоколът за споделяне на файлове, използван от NetWare сървърите. Въпреки че Linux машините могат да комуникират по мрежата, като използват TCP/IP за мрежов транспортен протокол, те не могат да осъществяват достъп до файловете на Microsoft сървър без SMB клиент, работещ в приложния слой. Протоколът PPP (Point to Point Protocol) се използва за установяване на връзка през dialup достъп и не е протокол за споделяне на файлове.

10 **C.** OS/2 използва операционната система High Performance File System (може да използва и FAT16). Windows NT 3.*x* включваше поддръжка на HPFS, но по-късните версии на NT и другите операционни системи на Microsoft не го правят.

13

1 **C.** Протоколът за споделяне на файлове се нарича и същински протокол, защото споделянето на ресурси се намира в същината на компютърните мрежи; свързваме компютрите в мрежи, за да могат да споделят ресурси. Мрежовият/транспортният протокол е набор от протоколи (наречени протоколен стек), използвани за LAN/WAN комуникации. Каналният протокол се използва за установяване на връзка между компютрите. Layer 2 е просто каналният слой в референтния OSI модел, така че Layer 2 протоколите са канални протоколи (протоколи от каналния слой).

2 **B.** Както TCP/IP (и за разлика от NetBEUI), протоколът IPX/SPX е маршрутизируем. Макар че често се асоциира с NetWare мрежи, той може да се използва и в мрежи на Microsoft, а понякога се реализира във вътрешните мрежи с цел сигурност. NetWare 5.*x* е първата версия, която работи с чист IP и не използва IPX/SPX; последният обаче все още се поддържа и трябва да се използва, ако в мрежата работят по-стари NetWare сървъри (преди 5.x). IPX/SPX е по-бърз и по-лесен за конфигуриране от TCP/IP, но е по-бавен и по-труден за установяване от NetBEUI.

3 **A** и **D.** Спецификацията NDIS (Network Driver Interface Specification), създадена от Microsoft, и интерфейсът ODI (Open Driver Interface) позволяват свързването на множество протоколи с един мрежов адаптер или на един протокол с множество мрежови адаптери. Winsock е приложен програмен интерфейс (API), а TDI (Transport Driver Interface) е граничен слой в мрежовия модел на Windows NT.

4 **B.** Протоколът SMB (Server Message Block) се използва за споделяне на файлове в мрежи на Microsoft. SMB клиентският и сървърният софтуер са налични и за други мрежови операционни системи, за да осигурят интеграция с Microsoft компютрите. NCP означава NetWare Core Protocol и се използва от мрежите на Novell. NFS означава Network File System и се използва за споделяне на файлове при UNIX машините. DLC е Data Link Control протокол, който може да се използва за комуникиране с лазерни принтери и IBM мейнфрейм машини, свързани в мрежата.

5 **B** и **D.** Софтуерът GSNW е включен в Windows NT и Windows 2000 Server, и се инсталира на Windows сървъра, за да позволи на Microsoft клиентите да осъществяват достъп до ресурси на NetWare сървър през шлюз. На страната на клиента не се изисква допълнителен софтуер; NetWare сървърът обаче трябва да е конфигуриран с група, наречена NTGATEWAY, и потребителски акаунт в тази група, който се използва от всички шлюзови клиенти. GSNW не се инсталира на NetWare сървъра.

6 **B.** Samba позволява SMB клиенти (като Windows компютрите) да осъществяват достъп до файлове на UNIX сървъри, и включва SMB клиент, за да позволи на UNIX машини да осъществяват достъп до SMB споделени ресурси. CDFS е файловата система, използвана от CD-ROM устройствата. Такова нещо като Client Services for UNIX не съществува. Systems Network Architecture (SNA) е протоколен набор, разработен от IBM, за да позволи на различни архитектури (като мейнфреймове и PC-та) да комуникират помежду си.

7 **C.** Шлюзът е софтуерен пакет, свързващ два различни типа мрежи, използващи напълно различни протоколи, при което извършва транслация между протоколите, за да позволи на компютрите от всяка страна да комуникират един с друг. Мостът осигурява средства за сегментиране на една мрежа с цел намаляване на трафика. Сървърният софтуер, или NOS, е операционната система, работеща на даден сървър; тя осигурява автентикация при логване, централизирано хранилище и администриране. Маршрутизиращият софтуер позволява на пакетите да се препращат от една мрежа (подмрежа) към друга, като използват устройство (например специализиран маршрутизатор или PC, работещо като маршрутизатор), притежаващо мрежов интерфейс и към двете мрежи.

8 **D.** Редиректорният софтуер прихваща заявките за ресурси и ги пренасочва към мрежата, вместо към локалната шина на компютъра. Платформата е хардуерна архитектура (като Macintosh, IBM мейнфрейм или PC). Клиентът е програма, която осъществява достъп до ресурсите на даден сървър. В компютрите няма такова нещо като директор.

9 **A** и **C.** CIFS, базирайки се на протокола SMB за споделяне на файлове, осигурява преобразуване на имена, услуги за споделяне на файлове и принтери, автентикация и авторизация, и услуга за браузване на мрежата. Dialup достъпът и сигурността на ниво файлове не са услуги, осигурявани от CIFS.

10 **A.** SMB демонът, SMBd, е един от двата главни компонента на SAMBA. Той осигурява автентикация, авторизация и споделяне на файлове и принтери. Вторият главен компонент, NMBd, осигурява услуги за браузване и преобразуване на имена. Не съществува MBXd. SMBFS е продукт, позволяващ на Linux машини да мапват мрежови устройства към SMB ресурс. Той се дистрибутира със SAMBA, но не е част от SAMBA.

Глава 14

1 **C.** Ключовете са числа или шифри, използвани за верифициране на интегритета на електронните комуникации. Паролата е поредица от буквени, цифрови и символни знакове, използвани за верифициране на това, дали даден потребител наистина е собственик на акаунта, асоцииран с паролата. Криптографията е наука за изучаване на секретни записи. Ав-

тентикацията се отнася до целия процес на верификация на идентичността.

2 **B.** Една атака с груба сила непрекъснато опитва различни възможности за пароли, докато някоя не проработи. Паролите могат да се въвеждат ръчно или от програма или скрипт. Декриптирането е действието по използване на криптиращ код, за да върне разбърканото съобщение обратно в неговата оригинална форма. Троянският кон е програма, представяща се за нещо друго, и обикновено съдържа злонамерен код. Nuke атаката е още един термин за DoS атака.

3 **D.** Едно ping наводнение (или ICMP наводнение) изпраща „потоп" от ICMP пакети, които в крайна сметка заливат системата. Когато ICMP съобщенията се изпращат към бродкастен адрес с намерението да се засегне цял мрежов сегмент, това се нарича Smurf атака. Една SYN атака използва трикратната последователност за хендшейк на TCP, за да запълни опашката на сървъра така, че той да не може да приема нови легитимни заявки за връзка. Червеят е вид злонамерен код, който се саморазпространява. Атаката ping на смъртта (Ping of Death) включва изпращане на ICMP пакет, надвишаващ границите на максималната единица за трансфер (Maximum Transfer Unit – MTU).

4 **A** и **B.** Както промишленият шпионаж, така и случайните пробиви в сигурността, предизвикани от некомпетентността на работниците са често срещани вътрешни заплахи. IP спуфингът по-често е външна заплаха, в която някой от Интернет емулира вътрешен IP адрес, за да получи достъп.

5 **B.** По-дългите пароли са по-трудни за отгатване, така че една добра политика е да се изискват пароли с дължина, не по-мака от минималната. паролите, които се запомнят от потребителите най-лесно, са и най-често пробивани. Включването на цифри и знакове в паролата (заедно с комбинация от букви в горен и долен регистър) прави по-трудно отгатването и е добре да се изисква. В една среда с висока сигурност паролите трябва да се сменят редовно.

6 **C.** По подразбиране Windows 2000 дава на всички позволение за пълен контрол над нов споделен ресурс. Това позволение може да бъде премахнато или променено. По подразбиране NetWare сървърите работят точно по обратния начин; никой няма позволение за използване на споделения ресурс. При NetWare ресурсите трябва изрично да назначите позволение,за да можете да осъществявате достъп до тях.

7 **A.** Криптирането на файлове защитава данните при записа им на диска, а не при предаването им по мрежата. За да защитите данните по време на прехвърляне, трябва да използвате друг метод, като например IPSec. Макар че за целта съществува независимо разработен софтуер, функцията за криптиране е вградена в някои операционни системи, като например Windows 2000.

8 **C.** ESP е протоколът Encapsulating Security Payload, който заедно с AH (Authentication Header) се използва от IPSec, за да защити данните при пътуването им по мрежата. ESP гарантира конфиденциалността на самите данни, а AH се използва само за да автентицира идентичността на изпращача. ESP и AH могат да се използват независимо или в комбинация един с друг.

9 **D.** Криптирането със секретен ключ, наречено също симетрично криптиране, използва само един ключ (наречен споделена тайна), за да криптира и декриптира данните. Криптирането с публичен ключ (наречен също асиметрично криптиране) използва два ключа: публичен, който се публикува и разпространява свободно, и частен ключ, известен само на притежателя на двойката ключове. Криптирането с публичен ключ се нарича ще криптиране с криптиране с частен/публичен ключ.

10 **B.** Хеш алгоритъмът е математическо изчисление, което не може да бъде анализирано до изходното му състояние; то се изпълнява върху съобщение при изпращащата и приемащата страна. Ако резултатите са еднакви, съобщението не е било променяно. За верификация на идентичността на притежателя на двойка ключове се използва цифров сертификат от доверена трета страна. При Kerberos автентикацията се издава билет за издаване на билет, за да се провери идентичността на даден потребител или система спрямо сървър.

Глава 15

1 **C.** Модемната банка позволява множество входящи телефонни линии към сървър за отдалечен достъп, по този начин могат да се свържат едновременно множество клиенти. Multilink е средство събиране на пропускателна способност. BAP работи с multilink, за да позволи динамично управление на използването на пропускателната способност. CSU/DSU е устройство, използвано при T-носещи линии.

2 **B.** Аналоговата dialup връзка, използваща модем и обикновени телефонни линии, е най общата форма на отдалечен достъп. Цифровите dialup връзки, посветените цифрови връзки и безжичните връзки могат да се използват за осъществяване на достъп до мрежата отдалечено; всички те обаче са по-скъпи и оборудването се намира, конфигурира и поддържа по-трудно.

3 **A** и **D.** SLIP (Serial Line Internet Protocol) и PPP (Point to Point Protocol) за протоколи, използвани за установяване на връзка по телефонна мрежа. IPX/SPX и NetBEUI са мрежови/транспортни протоколи, които отдалеченият клиент или сървър може да използва, за да комуникира, след като WAN връзката е установена.

4 **B.** Протоколът PAP (Password Authentication Protocol) изпраща в чист текст некриптирани пароли по мрежата, поради което той е най-несигурният от изброените методи. Протоколите CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol), и SPAP (Shiva PAP) използват криптиране, за да защитят интегритета на паролите при преминаването им по мрежата.

5 **C.** Multilink PPP комбинира капацитета на два 64-Kbps B канала, снабдени с услугата Basic Rate ISDN, в една 128-Kbps връзка. Отдалеченият сървър, с който се свързвате, трябва да е конфигуриран да приема multilink връзки. BAP се използва за динамично отпускане на пропускателна способност при една multilink връзка. PPTP се използва за създаване на тунел през Интернет за целите на виртуалните частни мрежи. Мултикастването е средство за изпращане на едно и също съобщение едновременно до всички компютри, които са членове на дадена мултикаст група.

6 **A.** Процесът на намаляване на модулацията, докато позвъняващият модем не открие модулация, която да се поддържа от приемащия модем, се нарича понижаване на скоростта (fallback), защото модемът непрекъснато понижава модулацията. Бондингът е хардуерен метод за събиране на

пропускателна способност. Ремодулацията не е термин, използван в модемните „преговори“. Обратното повикване е форма на сигурност при отдалечен достъп.

7 **B.** UART (Universal Asynchronous Receiver/Transmitter) чипът контролира COM порта и определя неговата максимална скорост. USB означава Universal Serial Bus – интерфейс, осигуряващ по-голямо удобство и скорост от стандартните серийни и паралелни портове. UNC означава Universal Naming Convention (конвенция за универсални имена), която дефинира синтаксиса за указване на път до мрежов ресурс. UDP е User Datagram Protocol – безвръзково-ориентиран протокол от транспортния слой, използван за комуникации, когато допълнителното натоварване, свързано с използването на TCP, не е желателно.

8 **C.** Вътрешните модеми по принцип са по-евтини от външните. Външните са по-лесни за инсталиране, защото не трябва да отваряте компютъра или да конфигурирате джъмпери. Освен това външните са по-лесни за наблюдение, тъй като включват индикаторни светлини.

9 **C** и **D.** Шумните телефонни линии могат да попречат на модема ви да се свърже на максималната скорост, на която е способен. Друга възможност е подемът да е несъвместим с този от другия край, особено ако имате по-стар 56-kbps модем, използващ 56Kflex или X2 технология. Ако въведеното потребителско име и парола са сгрешени, въобще няма да можете да се свържете. Входящ разговор по линия, за която е разрешено изчакването на повикване може да накара модема да прекрати връзката, но самото изчакване не я забавя.

10 **B.** RADIUS (Remote Authentication Dial-In User Service) е стандартен за индустрията протокол, осигуряващ централизация на автентицирането, управлението на акаунти и NAS контрола. Dialup сървърът се конфигурира като RADIUS клиент, а автентикацията се изпълнява от RADIUS сървър. Network Address Translation (NAT) е средство за споделяне на Интернет връзка с цялата LAN мрежа чрез транслиране на частните вътрешни адреси към един външен публичен адрес. RAID (Redundant Array of Independent Disks) е метод за осигуряване на дискова отказоустойчивост и висока производителност. RARP (Reverse Address Resolution Protocol) се използва от даден компютър, за да научи своя IP адрес, базиран на физическия MAC адрес.

16

1 **B.** Когато хедърът на протокола е обвит или скрит в друг, това се нарича капсулация и е процесът, по който се създава тунелът. Криптирането е процесът на разбъркване на данни, така че те да не могат да се четат от неавторизирани личности. Автентикацията е процесът на установяване на идентичността на даден потребител или машина. Авторизацията е позволяването само на потребителите с предефинирани акаунти да осъществяват достъп до мрежовите ресурси.

2 **A.** Тунелът е логическа връзка от точка до точка, която поддържа автентикация и криптиране на данни от едната крайна точка до другата. Протоколът е набор от правила, по които компютрите си комуникират помежду си. Терминът шлюз се използва за маршрутизатора, през който преминават пакетите, предназначени за други мрежи. Шлюз като Gateway Services for NetWare е и средство за транслиране от един протокол в

друг. Въпреки че една връзка за отдалечен достъп е логическа връзка от точка до точка, тя не е задължително да осигурява автентикация и криптиране, нито пък е необходимо да преминава през обществена мрежа. VPN мрежата е един вид връзка за отдалечен достъп.

3 **B** и **D.** PPTP е разширение на каналния протокол PPP. В това си качество той работи в каналния слой (Слой 2) на референтния OSI модел. PPTP използва протокола MPPE (Microsoft Point-to-Point Encryption), за да предостави сигурност чрез криптиране на данни; той не използва IPSec. IPSec се използва заедно с L2TP.

4 **C.** IPSec може да работи в транспортен режим, например когато осигурява криптиране на данни, докато L2TP осигурява капсулация. Той може да работи и в тунелен режим, по време на което той самият извършва капсулация. PPTP и L2F са тунелни протоколи, които не работят в два режима. SSH е Secure Shell и се използва за създаване на VPN връзки в UNIX среди.

5 **C** и **D.** Най-голямото преимущество на VPN връзките е пестенето на средства, което идва от премахването на необходимост за провеждане на разговори на далечни разстояния. VPN производителността обаче обикновено е по-ниска от директната връзка заради служебната информация, създаваща тунела. VPN мрежите, разчитащи на Интернет, особено използващите dialup връзка, обикновено не са толкова надеждни, колкото една директна dialup връзка.

6 **C.** Една екстранет мрежа е част от LAN мрежата на дадена компания, която е направена достъпна за външен достъп. Когато достъпът се осигурява от тунел през обществената мрежа, имате VPN екстранет. Една интернет мрежа (с малко *и*) е всяка мрежа от мрежи. Интранет мрежата е подобна на екстранет, но по принцип достъпът до нея се установява вътре в корпоративната мрежа. Тя е предназначена за използване от работниците, а не от външни клиенти. Всяка подмрежа е част от по-голяма мрежа.

7 **D.** Конфигурацията маршрутизатор към маршрутизатор свързва две отделни LAN мрежи една с друга и позволява на потребителите да осъществяват достъп до ресурси от всяка страна. В останалите три сценария е по-вероятно потребителят да инициира VPN връзката от dialup Интернет връзка, вместо да минава през маршрутизатор.

8 **A** и **C.** PPTP и L2TP могат да се използват за създаване на VPN тунели, като и двата работят в каналния слой (Слой 2) на референтния OSI модел. Само че PPTP изисква IP и не може да използва виртуални ATM или Frame Relay вериги за тунел през не-IP мрежи. Само L2TP поддържа множество тунели между крайните точки.

9 **B.** Протоколът CIPE (CryptoIP Encapsulation protocol) е реализиран като драйвер в ядрото на Linux и може да се използва за сигурен тунел между две IP подмрежи. TunnelBuilder е независим VPN продукт. CIR е съкращение от Committed Information Rate и не се отнася директно за VPN мрежите. VPN демонът (VPNd) е тунелизиращ софтуер за Linux/UNIX, който използва алгоритъма за криптиране Blowfish.

10 **A**, **B** и **D.** Хардуерно-базираните VPN мрежи съществуват в две разновидности: базирани на маршрутизатор и базирани на защитна стена (firewall). Базираните на маршрутизатор VPN мрежи по принцип са доста лесни за установяване и използване – нещо близко до технологията „plug-and-play“. Базираните на защитни стени VPN мрежи могат да из-

вършват транслиране на адреси. Само че много софтуерно-базирани VPN решения са безплатни и са включени в операционната система. Хардуерно-базираните VPN мрежи са по-скъпи.

17

1 **А и С.** Дори един сървър, базиран на PC от висок клас и използван като приложен сървър, струва хиляди долари по-малко от един мейнфрейм компютър. Използване на PC-та като клиенти дава на потребителите възможност да изпълняват някои приложения локално, докато другите се стартират на сървъра. PC-тата са по-скъпи от мейнфрейм терминалите, но пък са по-функционални.

2 **С.** При повечето реализации на тънки клиенти, като например Microsoft Terminal Services, имате контрол над потребителските сесии и можете да поемете входа от клавиатурата и мишката, или да прекратите сесията. Използването на терминали всъщност улеснява архивирането на данните, защото всички те се намират на централно място на сървъра. Приложенията се ъпгрейдват само на сървъра, а не на индивидуалните клиентски машини.

3 **В.** Протоколът ICA (Independent Computing Architecture), който се използва от Citrix за техния MetaFrame продукт, позволява на не-Windows клиенти да се свързват с Windows терминален сървър. Протоколът RDP (Remote Desktop Protocol), който се използва от Microsoft и е включен в Windows NT и Windows 2000 Terminal Services, позволява само на Windows клиенти да осъществяват достъп до терминалния сървър. Протоколът X обикновено се използва от UNIX клиенти за достъп до UNIX X сървъри. Протоколът DHCP (Dynamic Host Configuration Protocol) се използва за назначаване на IP адреси на компютри (включително тънки клиенти), когато те се свържат към TCP/IP мрежа.

4 **А и D.** Протоколът RDP (Remote Desktop Protocol), който се използва от Microsoft Terminal Services, поддържа печатане на локален LTP (паралелен) порт от клиенти; той позволява и клипборд пренасочване – копиране и вмъкване на данни между терминалните прозорци и локалния десктоп. Само ICA поддържа COM порт пренасочване и протоколите IPX/SPX и NetBEUI.

5 **С.** Протоколът XDMCP (X Display Manager Communication Protocol) се използва за назначава не на X сървърни ресурси на X терминалните клиенти. X е протоколът, използван за комуникация между клиент и сървър. LBX (Low Bandwidth X) е вариация на X, предназначена за бавни WAN връзки. RFB е протоколът Remote Frame Buffer, който се използва за осигуряване на отдалечен достъп до GUI интерфейс.

6 **В.** Preboot Execution Environment е стандарт, реализиран от Intel и други производители, който дефинира средствата за осигуряване на зареждащ код за бездисковите работни станции, които зареждат операционна система от мрежата. Останалите три дефиниции на PXE са грешни.

7 **В, С и D.** Мрежовият компютър, който беше разработен от Sun Microsystems съвместно с Oracle и IBM, поддържа протоколния стек TCP/IP и изпълнението на Java аплети. Мрежовите компютри (т.е. създадените по технологията Network Computer) включват Web браузър за обработка на HTTP и HTTPS заявки. Network Computer е фирмена разработка, която не изисква специфична платформа или операционна система.

8 **А и В.** Софтуерът Windows 2000 Terminal Services може да работи или в режим на отдалечено администриране, което ви позволява да управлявате сървъра от отдалечена работна станция, или в режим на приложен сървър, в който множество потребители могат да се свързват към терминалния сървър, за да стартират приложения на Windows 2000 десктоп. Терминалните услуги нямат режими на локален достъп или виртуална машина.

9 **В и С.** Citrix MetaFrame се характеризира с технологията Nfuse – технология за портал за приложения, позволяваща интегриране на приложения в стандартния интерфейс на Web браузър. Друга характеристика на MetaFrame е възможността за групиране на сървъри във ферма с цел балансиране на натоварването и пул за лицензи. MetaFrame е допълнителен продукт за Windows NT 4.0 и Windows 2000; Citrix продуктът за NT 3.51 е Winframe. MetaFrame използва Program Neighborhood за управление на приложения създаване на нови ICA връзки.

10 **D.** Високата производителност на Java се базира от части на нейната способност за многонишкова работа и поддръжка на JIT компилация. Java аплетите трябва да се свалят на клиентската машина, макар че част или цялата обработка може да се извърши на сървъра. Java стандартите все още не са универсални; реализациите при отделните производители могат значително да се различават. JVM може да работи на почти всички платформи, включително Windows и Macintosh; тя не е ограничена до UNIX-базирани машини.

Глава 18

1 **В.** Количеството данни, което може в действителност да бъде предадено от компютъра източник до компютъра местоназначение по мрежа се измерва в пропускателна способност. Честотната лента е теоретичното количество на наличните сигнали, но терминът е взаимозаменяем с пропускателната способност. CIR (Committed Information Rate) е гаранция от доставчика, че вашата връзка ще има указаната минимална трансферна скорост. Базовата линия е установен стандарт за производителност, спрямо който се извършват бъдещи измервания.

2 **А.** Протоколният анализатор (наричан понякога мрежов монитор) е инструмент, обикновено софтуерен пакет, който прихваща индивидуални фреймове или пакети за анализиране. Мониторите на производителността са софтуерни инструменти, използващи броячи, за да измерват специфичен критерий, като например броя байтове, предавани за една секунда. Динамичните рефлектометри (TDRs) са хардуерни устройства, използвани за засичане на повредени или дадени накъсо кабели. Филтрите на пакети са компоненти, които могат да се използват с протоколни анализатори, за да се разглеждат пакети на специфичен протокол, или такива, изпратени на или от специфичен адрес.

3 **А и С.** Network Monitor на Microsoft, LANalyzer на Novell и Sniffer Pro на Network Associates са софтуерни протоколни анализатори. SNMP (Simple Network Management Protocol) е TCP/IP помощна програма, използвана за изпълнение на управленски задачи, но не осигурява анализиране на пакети и протоколи. TPCON на Novell представлява NetWare Loadable Module (NLM), използван за гледане на TCP/IP конфигурацията и статистики.