ВИЛЬЯМС

CISCO SYSTEMS



Основы компьютерных сетей

Всеобъемлющее руководство по теории компьютерных сетей, технической реализации сетевых технологий и межоперационному взаимодействию

www.williamspublishing.com
www.ciscopress.ru
ciscopress.com

Дебра Литтлджон Шиндер

ББК 32.973.26-018.2.75
Ш62
УДК 681.3.07

Издательский дом "Вильямс"
Зав. редакцией В.В. Александров

Перевод с английского канд. техн. наук *А.Г. Сысонюка*

Под редакцией *В.В. Александрова*

По общим вопросам обращайтесь в Издательский дом "Вильямс" по адресу:
info@williamspublishing.com, http://www.williamspublishing.com

Шиндер, Дебра, Литтлджон.

Ш62 Основы компьютерных сетей. : Пер. с англ. — М. : Издательский дом "Вильямс", 2002. — 656 с. : ил. — Парал. тит. англ.

ISBN 5-8459-0285-1 (рус.)

Эта книга призвана помочь читателю понять основы, концепции и принципы реализации вычислительных сетей. В книгу включено также краткое введение в выполняющиеся на сетевых компьютерах клиентские и серверные операционные системы. В книге приведена история развития вычислительных сетей, рассматривается принятая терминология, теория сетей, установившиеся стандарты и способы реализации локальных и глобальных вычислительных сетей. Особенное внимание обращается на сетевые протоколы и на работу протоколов на всех уровнях модели вычислительной сети. Детально описаны вопросы совместимости сетей, работающих на разных платформах и в разных протоколах и операционных системах, а также вопросы безопасности и удаленного доступа, частные виртуальные вычислительные сети, сети с тонкими клиентами, администрирование сетей и устранение неполадок. Рассматриваются ближайшие и более отдаленные перспективы развития сетевых технологий.

Книга предназначена главным образом для компьютерных специалистов, начинающих изучать сетевые технологии, а также для тех, кому нужен основательный обзор базовых концепций вычислительных сетей. Книга была задумана как "дружественный интерфейс": она вполне доступна для читателей, которые не обладают достаточной технической подготовкой и могут быть шокированы узкоспециальным жаргоном и обилием технических подробностей в документации коммерческих продуктов.

ББК 32.973.26-018.2.75

Все названия программных продуктов являются зарегистрированными торговыми марками соответствующих фирм.

Никакая часть настоящего издания ни в каких целях не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование и запись на магнитный носитель, если на это нет письменного разрешения издательства Cisco Press.

Authorized translation from the English language edition published by Cisco Press, Copyright © 2001

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Russian language edition published by Williams Publishing House according to the Agreement with R&I Enterprises International, Copyright © 2002

ISBN 5-8459-0285-1 (рус.)
ISBN 1-5871-3038-6 (англ.)

© Издательский дом "Вильямс", 2002
© Cisco Press, 2001

Оглавление

Введение **20**

Часть I. Основные концепции компьютерных сетей **25**

Глава 1. Введение в компьютерные сети 27

Глава 2. Классификация компьютерных сетей 53

Глава 3. Концепции, модели и стандарты компьютерных сетей 89

Глава 4. Методы сетевой коммуникации 117

Глава 5. Локальные сети 137

Глава 6. Глобальные сети 161

Часть II. Сетевое оборудование и программное обеспечение **191**

Глава 7. Физические компоненты сетей 193

Глава 8. Сетевые протоколы и службы 219

Глава 9. Самая глобальная сеть — Internet 253

Глава 10. Сетевые операционные системы 291

Глава 11. Службы каталогов 321

Глава 12. Клиентские операционные системы 339

Глава 13. Гибридные сети 381

Часть III. Специальные вопросы **399**

Глава 14. Защита сети 401

Глава 15. Удаленный доступ 443

Глава 16. Виртуальные частные сети 469

Глава 17. Сети с тонкими клиентами 493

Глава 18. Инструменты мониторинга, управления и устранения неполадок 513

Часть IV. Будущее сетей **545**

Глава 19. Технологии завтрашнего дня 547

Приложение. Ответы на контрольные вопросы **567**

Словарь терминов **595**

Предметный указатель **636**

Содержание

Введение **20**

Часть I. Основные концепции компьютерных сетей **25**

Глава 1. Введение в компьютерные сети **27**

Краткая история компьютерных сетей 27
Первые коммуникационные сети 28
Недостатки изолированных систем 32
Так что же такое *компьютерная сеть* 32
Преимущества объединения 33
Рождение Internet 34
Стоимость технологии: все больше благ за все меньшую цену 36
Сети персональных компьютеров сегодня 37
Домашние компьютеры 37
Web и электронная коммерция 37
Высокопроизводительные коммерческие сети 38
Обучение с помощью сети 38
Будущее компьютерных сетей 38
"Умные" устройства в нашем доме 39
Звонок домой 39
Рабочее место без проводов 40
Школы будущего 41
Компьютерные сети и охрана здоровья 41
Компьютерные сети и юриспруденция 41
Межгалактическая сеть? 42
Краткий обзор терминологии компьютерных сетей 42
Концептуальные термины 43
Термины сетевого оборудования 43
Термины программного обеспечения 44
Термины *топологии* сети 44
Термины единиц измерения 45
Что есть и чего нет в этой книге 46
Сертификация специалистов сетевых технологий 46
Сертификация, ориентированная на конкретного поставщика 46
Сертификаты, не ориентированные на конкретного поставщика 47
Соответствие данной книги программам сертификации 47
Резюме 48
Рекомендуемые источники информации 48
Контрольные вопросы 48

Глава 2. Классификация компьютерных сетей **53**
Классификация сетей по области действия 53
Локальные сети 54
Городские сети 55
Глобальные сети 56
Классификация сетей по способам администрирования 58
Серверы и клиенты 59
Одноранговые сети 63
Сети клиент/сервер 65
Классификация сетей по сетевым операционным системам 67
Сети Windows 68
Сети NetWare 68
Сети UNIX 68
Смешанные сети 69
Классификация сетей по протоколам 69
Сети NetBEUI 70
Сети IPX/SPX 70
Сети TCP/IP 70
Другие протоколы локальных сетей 71
Классификация сетей по топологии 72
Сети с шинной топологией 72
Сети с кольцевой топологией 73
Звездообразные сети 74
Ячеистая топология 76
Смешанные топологии 76
Классификация сетей по архитектуре 78
Сети Ethernet 78
Сети Token Ring 82
Сети AppleTalk 83
Сети ARCnet 83
Резюме 84
Рекомендуемые источники 85
Контрольные вопросы 85
Глава 3. Концепции, модели и стандарты компьютерных сетей **89**
Базовые принципы сетевых коммуникаций 89
Язык компьютеров 90
Системы счисления 90
Пакеты данных 94
Многоуровневый процесс коммуникации 95
Сетевые модели 97
Назначение моделей 97
Модель OSI 97
Модель DoD 108
Модели поставщиков 109
Сетевые стандарты и спецификации 110
Зачем нужна стандартизация 110
Организации, учреждающие стандарты 110

Резюме 113
Рекомендуемые источники 114
Контрольные вопросы 114

Глава 4. Методы сетевой коммуникации 117

Сигналы 117
Аналоговые и цифровые сигналы 117
Модулированные и немодулированные сигналы 120
Мультиплексирование 121
Асинхронная и синхронная передача 122
Симплексный, полудуплексный и дуплексный методы передачи 123
Проблемы, возникающие при передаче сигналов 125
Электромагнитные помехи 125
Радиочастотные помехи 126
Перекрестные помехи 126
Затухание сигналов 126
Пропускная способность 127
Методы доступа к сети 128
Метод CSMA/CD 128
Метод CSMA/CA 129
Передача маркера 130
Приоритеты запросов 131
Резюме 132
Рекомендуемые источники 132
Контрольные вопросы 132

Глава 5. Локальные сети 137

Сети Ethernet 137
10Base2 138
10Base5 139
10BaseT 141
100BaseX 142
1000BaseT 142
Структура кадра Ethernet 143
Правила установки Ethernet 144
Сводка характеристик Ethernet 146
Сети Token Ring 146
Топология Token Ring 147
Процессы коммуникации в Token Ring 147
Сетевое оборудование Token Ring 148
Преимущества Token Ring 149
Недостатки Token Ring 149
Структура кадра Token Ring 149
Правила кольца 150
Сводка характеристик Token Ring 151
Сети FDDI 151
Принцип действия FDDI 151
Спецификации FDDI 152

Преимущества FDDI 152
Недостатки FDDI 153
Структура кадра FDDI 153
Сводка характеристик FDDI 153
Сети AppleTalk 153
Спецификации AppleTalk 153
Принцип действия AppleTalk 154
Преимущества AppleTalk 154
Недостатки AppleTalk 154
Передача данных в LocalTalk 154
Сводка характеристик AppleTalk 154
Сети ARCnet 155
Принцип действия ARCnet 155
Спецификации ARCnet 155
Преимущества ARCnet 156
Недостатки ARCnet 156
Структура пакета ARCnet 156
Сводка характеристик ARCnet 156
Сравнение сетевых архитектур 157
Резюме 157
Рекомендуемые источники 158
Контрольные вопросы 158
Глава 6. Глобальные сети **161**
Оборудование глобальных сетей 162
Модемы 162
Адаптеры ISDN и DSL 166
Оборудование пользователя 167
Топологии глобальных сетей 167
Точечная топология 167
Кольцеобразная топология 168
Звездообразная топология 168
Многоуровневые глобальные сети 169
Типы коммутации 170
Сети с коммутацией каналов 171
Сети с коммутацией пакетов 176
Разрабатываемые технологии глобальных сетей 178
OS-SONET 178
Быстрая ISDN 179
CATV 179
SMDS 180
Беспроводные глобальные сети 181
Соединения между локальными и глобальными сетями 181
Транслируемые соединения 182
Прокси-серверы 184
Маршрутизированные соединения 185
Резюме 186

Рекомендуемые источники 187
Контрольные вопросы 187

Часть II. Сетевое оборудование и программное обеспечение 191

Глава 7. Физические компоненты сетей 193

Сетевые адаптеры 193
Назначение сетевых адаптеров 193
Выбор сетевого адаптера 194
Конфигурирование и использование сетевых адаптеров 195
Сетевые носители 197
Типы кабелей 197
Беспроводные носители 203
Сетевые соединительные устройства 206
Простые соединительные устройства 207
Сложные соединительные устройства 208
Устройства сегментации и создания подсетей 209
Резюме 215
Рекомендуемые источники 216
Контрольные вопросы 216

Глава 8. Сетевые протоколы и службы 219

Протокол NetBIOS/NetBEUI 219
Протокол IPX/SPX 220
Протокол сетевого уровня IPX 221
Протокол транспортного уровня SPX 222
Протокол TCP/IP 222
Пакет протоколов TCP/IP 222
Протокол сетевого уровня IP 222
Протоколы транспортного уровня: TCP и UDP 234
Заголовок пакета: адрес на конверте 236
Разрешение имен 237
Утилиты TCP/IP 241
Протоколы прикладного уровня 248
Резюме 248
Рекомендуемые источники 249
Контрольные вопросы 249

Глава 9. Самая глобальная сеть — Internet 253

Развитие Internet 253
Разработка магистрали 254
Проект Internet2 255
Компоненты Internet 255
Компьютер или локальная сеть 256
Провайдер услуг Internet 256
Региональная сеть 256
Пункты NAP 257
Пункты MAE 257
Взаимодействие компонентов Internet 257

Что делает Internet 259
World Wide Web 260
Электронная почта и списки рассылки 268
Группы новостей 272
Передача файлов 273
Программа Telnet 274
Воспроизведение аудио- и видеопотока данных 275
Беседы 275
Аудио- и видеоконференции 276
Internet-телефония 277
Виртуальные частные сети 277
Internet и маршрутизация TCP/IP 278
Как выполняется маршрутизация IP 278
Пример простой маршрутизированной сети 279
Типы интерфейсов маршрутизации 280
Статическая и динамическая маршрутизация 280
Дистанционно-векторные протоколы и протоколы на основе состояния каналов 282
Распространенные протоколы маршрутизации 283
Кому принадлежит Internet 285
ISOC 285
IAB 286
IETF 286
IESG 286
IANA/ICANN 286
W3C 286
Резюме 286
Рекомендуемые источники 287
Контрольные вопросы 287

Глава 10. Сетевые операционные системы 291

Администрирование сетей 292
Среда клиент/сервер 292
Разделение сетевых ресурсов 295
Обзор сетевых операционных систем 303
Сети Windows NT и Windows 2000 303
Сети NetWare 308
Сети UNIX и Linux 311
Другие сетевые операционные системы 316
Резюме 316
Рекомендуемые источники 317
Контрольные вопросы 317

Глава 11. Службы каталогов 321

Что такое каталоги и службы каталогов 321
Что такое каталог 321
Что такое службы каталогов 323
Стандарты служб каталогов 325

X.500 325
Протоколы DAP и LDAP 326
Сети с каталогами 328
Распространенные службы каталогов 328
Служба каталогов NDS 328
Службы Active Directory компании Microsoft 329
Другие службы каталогов 333
Резюме 334
Рекомендуемые источники 335
Контрольные вопросы 335

Глава 12. Клиентские операционные системы 339

Основы операционных систем 339
Интерфейсы операционных систем 340
Использование команд 342
Файлы и файловые системы 345
Распространенные клиентские операционные системы 357
MS DOS и Windows 3.*x* 357
Windows 9*x* 358
Операционная система Windows NT Workstation 365
Операционная система Windows 2000 Professional 367
Linux/UNIX 370
Macintosh 374
OS/2 376
Резюме 377
Рекомендуемые источники 377
Контрольные вопросы 378

Глава 13. Гибридные сети 381

Характеристики гибридных сетей 381
Невозможность реализации требуемых характеристик на основе компонентов одного поставщика 382
Личные предпочтения пользователей 382
Финансовые соображения 382
Непредсказуемый рост сети 383
Сети на основе многих протоколов 383
Протоколы сетевого/транспортного уровня 383
Протоколы разделения файлов 386
Сети с несколькими операционными системами 387
Сети с несколькими серверными операционными системами 387
Несколько клиентских операционных систем 388
Несколько серверных и клиентских операционных систем 389
Сети на основе нескольких платформ 389
Коммуникация персональных компьютеров с компьютерами Macintosh 389
Коммуникация персональных компьютеров с мэйнфреймами 389
Коммуникация персональных компьютеров с карманными компьютерами 390
Шлюз как еще один способ гибридного соединения 391
Редиректоры Windows–NetWare 391

Соединения между разными платформами 392
Архитектура SNA 392
Резюме 395
Рекомендуемые источники 395
Контрольные вопросы 396

Часть III. Специальные вопросы 399

Глава 14. Защита сети 401

Безопасность сети 401
Оценка требований к безопасности 402
Оценка угроз безопасности 403
Реализация мер безопасности 410
Принцип действия компонентов безопасности 417
Современные средства идентификации и аутентификации 423
Разработка правил безопасности 425
Защита от краха и восстановление 431
Резервирование электропитания 431
Резервное копирование данных 433
Отказоустойчивость дисков 436
Методы кластеризации 437
Резюме 437
Рекомендуемые источники 438
Контрольные вопросы 439

Глава 15. Удаленный доступ 443

Зачем нужен удаленный доступ 444
Филиалы компании 444
Связь в нерабочее время 444
Телекоммуникация 445
Мобильные пользователи 446
Предоставление доступа партнерам и клиентам 446
Принцип действия систем удаленного доступа 447
Протоколы удаленного доступа 447
Аутентификация удаленного доступа 448
Присвоение IP-адресов 449
Группировка пропускных способностей в коммутируемых соединениях 449
Управление использованием пропускной способности 449
Устройства соединений удаленного доступа 450
Модемы 450
Терминальные адаптеры ISDN 456
Кабельные модемы 457
Устройства CSU/DSU 458
Конфигурирование клиентов и серверов удаленного доступа 459
Конфигурирование клиента удаленного доступа 459
Конфигурирование сервера удаленного доступа 460
Безопасность удаленного доступа 460
Метод обратного вызова 461
Служба RADIUS 462

Стратегия удаленного доступа 462
Блокировка учетных записей 462
Хосты безопасности 463
Резюме 463
Рекомендуемые источники 464
Контрольные вопросы 464
Глава 16. Виртуальные частные сети 469
Что такое VPN 469
Виртуальная сеть 469
Частная сеть 470
Принцип действия VPN 470
Создание туннеля 471
Поддержка VPN операционными системами 473
Что дает использование VPN 473
VPN и коммутируемые сети· преимущества и недостатки 474
Сценарии VPN 476
Протоколы VPN 479
Протоколы туннелирования 479
Протоколы шифрования 482
Локальные протоколы 483
Безопасность VPN 483
Аутентификация 483
Авторизация 483
Шифрование 484
Производительность VPN 484
Типы VPN 484
Программные реализации VPN 484
Аппаратные реализации VPN 485
Конфигурирование соединения VPN 485
Резюме 487
Рекомендуемые источники 488
Контрольные вопросы 488
Глава 17. Сети с тонкими клиентами 493
Развитие сетей с тонкими клиентами 494
Технология тонких клиентов 495
Преимущества технологии тонких клиентов 496
Протоколы тонких клиентов 497
RDP 498
ICA 498
X и XDMCP 498
RFB 499
BOOTP, DHCP и TFTP 499
Оборудование тонкого клиента 500
WBT 500
Сетевые компьютеры 501
Сетевые персональные компьютеры 501

Настольные компьютеры 502
Тончайшие клиенты: портативные компьютеры 502
Программное обеспечение тонких клиентов 503
Microsoft Terminal Services 503
Программы Winframe и MetaFrame компании Citrix 504
Система X Window 505
Технологии Web 505
Виртуальные машины Java 506
Модель ASP 506
Инициатива Microsoft .NET 507
Резюме 507
Рекомендуемые источники 508
Контрольные вопросы 508

Глава 18. Инструменты мониторинга, управления и устранения неполадок 513

Анализ и оптимизация производительности сети 514
Узкие места 514
Базовые уровни 515
Положительный опыт 516
Определение пропускной способности соединения с Internet 516
Инструменты мониторинга и управления сетью 518
Программы мониторинга сети 518
Программы управления сетями 523
Программы управления небольшими сетями и сетями средних размеров 527
Провайдеры услуг управления 528
Устройства мониторинга и устранения неполадок 529
Устранение неполадок в сетях 530
Основы устранения неполадок 530
Использование файлов системного журнала 532
Использование утилит TCP/IP 533
Указания по устранению неполадок 539
Резюме 540
Рекомендуемые источники 541
Контрольные вопросы 541

Часть IV. Будущее сетей 545

Глава 19. Технологии завтрашнего дня 547

Вездесущие компьютеры 547
Домашние сети 548
Преодоление ограничений IP 549
Новые направления сетевых технологий 550
Всеобщая связь 552
Интеллектуальные предметы 553
Семейная сеть 553
Развлечения 554
Безопасность всеобщей связи 554
Сетевые технологии на рабочем месте 555

Влияние сетевых технологий на государство 555
Влияние коммуникационных технологий на законодательство 557
Влияние сетевых технологий на медицину 558
Влияние сетевых технологий на издание книг 559
Новые способы обучения 560
Искусственный интеллект 561
Думающие компьютеры 561
Вершина развития сетевых технологий — кибернетические формы жизни 562
Резюме 562
Рекомендуемые источники 563
Заключительные вопросы 563
Приложение. Ответы на контрольные вопросы 567
Глава 1 567
Глава 2 569
Глава 3 570
Глава 4 572
Глава 5 573
Глава 6 575
Глава 7 576
Глава 8 578
Глава 9 579
Глава 10 580
Глава 11 581
Глава 12 582
Глава 13 584
Глава 14 585
Глава 15 587
Глава 16 588
Глава 17 590
Глава 18 592
Словарь терминов 595
Предметный указатель 636

Об авторе

Дебра Литтлджон Шиндер (Debra Littlejohn Shinder), сертифицированный инженер Microsoft (Microsoft Certified Systems Engineer), преподает, пишет программы и консультирует в Далласе (Dallas) и Форт-Уэрте (Ft. Worth), шт. Техас. С 1992 года — преподаватель колледжа округа Даллас (Dallas County Community College District). В настоящее время является также Web-мастером городов Сиговил (Seagoville) и Саннивейл (Sunnyvale), шт. Техас. Ею разработан семейный Web-узел `www.shinder.net`. Прежде чем обратиться к области информационных технологий, Дебра была сержантом полиции, а затем инструктором в полицейской академии Дебра и ее супруг, д-р Томас Шиндер (Dr. Thomas Shinder), познакомились в Internet в 1994 году и с тех пор вместе работают над многочисленными учебными и коммерческими проектами. Дебра — счастливая мать двух взрослых детей. Ее дочь Кристина (Kristen) служит в Военно-морском флоте США, а ее сын Кристофер (Kristoffer) — чемпион одной из школ по шахматам. Дебра опубликовала довольно много статей, причем не только технического характера, но и затрагивающих другие области жизни Связаться с ней можно по адресу: `deb@shinder.net`.

О техническом рецензенте

Д-р Томас У. Шиндер (Dr. Thomas W. Shinder) вместе с супругой является соавтором нескольких книг по компьютерным сетям Windows 2000. Вместе с Деброй они ведут колонку информационных технологий в `Swynk.com`. Томас один из редакторов серии Syngress Media и преподаватель колледжа Истфилд (Eastfield College) в городе Мескит (Mesquite), шт. Техас. Он обучает персонал и консультирует для ряда фирм в округе Даллас, включая Exxon, Computer Learning Center, Xerox, CompUSA и другие. Д-р Шиндер обучался в университете штата Калифорния (г. Беркли) и в медицинском колледже университета штата Иллинойс. Затем несколько лет практиковал в области неврологии, прежде чем сделать карьеру в сфере компьютерных технологий, которые, впрочем, были его хобби всю жизнь. Связаться с ним можно по адресу:
`tshinder@dallas.net`

Посвящения

Моей маме, Крису (Kris), Кики (Khiki) и особенно папе, который всегда будет в моей памяти и в моем сердце.

Нилу (Neal), не оставившему меня, несмотря на мои многочисленные метаморфозы. Джони (Johnnie) и Ирэн (Iren), открывшими мне дверь в новую жизнь

Всем маленьким поросятам, особенно Бобу Бренсону (Bob Brenson) и трем другим из бесстрашной четверки: Шефу Элу (Chief Al), Братцу Лилу — Тому С ("Lil Brother" Tom C.) и Бюргеру Кингу (Buerger King).

И наконец, главное — моему техническому редактору, лучшему другу и мужу, по счастливой случайности оказавшимся одним и тем же лицом. Том, я не смогла бы сделать это без тебя А даже если бы и смогла, то делать это мне совсем бы не хотелось.

Благодарности

Невозможно перечислить всех, благодаря кому эта книга появилась на свет. Спасибо всем авторам и специалистам в области информационных технологий, от которых я так много узнала, особенно Марку Минаси (Mark Minasi) и Томасу Ли (Thomas Lee). Благодарю также всех, кто был терпелив со мной и без нареканий в очередной раз выслушивал "Как только я закончу эту книгу для Cisco Press...". К Джулии (Julie) это относится вдвойне!

Я бесконечно признательна Тому, который не только направлял меня к цели, но и взял на себя дополнительную нагрузку в других областях, чтобы я могла сосредоточиться на книге.

Огромное спасибо Кенту Джоунзу (Kent Jones) и Джерлу Гуднайту (Jearl Goolnight), которые приложили неимоверные усилия, доставая нужную для книги информацию.

Благодарю моих студентов по компьютерным сетям в Eastfield College, сделавших из меня сносного преподавателя. Их поддержка воодушевляла меня, а их вопросы послужили источником многих тем этой книги. Я благодарна моим хорошим друзьям и соратникам в этом деле: Кэшу (Cash), установившему тот первый модем и положившему начало всему этому, и Даркkэту (Darkcat), научившему меня "мыслить". Я высоко ценю поддержку Джима Т. Джоули (Jim T. Jolie) и "деловых дам", особенно Бетти (Beth).

Отдельные благодарности всем, прочитавшим первый черновик, за их бесценные замечания, позволившие значительно улучшить книгу. В этой связи я особенно благодарна Михаэлю Р. Хэнсону (Michael R. Hanson), вышедшему далеко за пределы служебных обязанностей· его советы и предложения значительно повлияли на конечный продукт.

И, разумеется, я глубоко признательна замечательным редакторам Cisco Press, особенно Карлу Линдхольму (Carl Lindholm), благодаря которому я смогла написать эту книгу, и Китти Уилсон Джарретт (Kitty Wilson Jarrett), которая значительно улучшила текст книги.

Введение

Эта книга призвана помочь читателю понять основные концепции и принципы реализации компьютерных сетей. Она содержит краткое введение в клиентские и серверные операционные системы, выполняющиеся на сетевых компьютерах.

В книгу включены история развития компьютерных сетей, принятая в них терминология, теория сетей, установившиеся стандарты и способы реализации локальных и глобальных компьютерных сетей. Особое внимание обращается на сетевые протоколы и их работу на всех уровнях модели сети. Не менее глубоко затрагиваются вопросы совместимости сетей, работающих на разных платформах и в разных протоколах и операционных системах.

Значительное внимание уделено также вопросам безопасности и удаленного доступа, частным компьютерным сетям, сетям с тонкими клиентами, администрированию сетей и устранению неполадок. Рассматриваются ближайшие и более отдаленные перспективы развития сетевых технологий.

Для кого предназначена эта книга

Книга главным образом рассчитана на специалистов в смежных областях, начинающих изучать сетевые технологии, а также для тех, кому нужен основательный обзор базовых концепций компьютерных сетей.

Другой слой читателей книги составят преподаватели учебных заведений и руководители коммерческих организаций, работающие с информационными технологиями и нуждающиеся в широком обзоре концепций, лежащих в основе сетей как малого и среднего бизнеса, так и крупных корпораций

Еще один контингент читателей этой книги — самые широкие круги пользователей, желающих больше узнать о том, как компьютеры сети сообщаются между собой. Книга была задумана как "дружественный интерфейс": она вполне доступна для читателей, не обладающих достаточной технической подготовкой и часто ошеломленных узкоспециальным жаргоном и обилием технических подробностей в документации коммерческих продуктов.

Структура книги

Книга состоит из четырех частей, включающих 19 глав, а также приложения и словаря терминов. В приведенных ниже разделах кратко описывается содержимое каждой части книги.

Часть I. Основные концепции компьютерных сетей

В главе 1, "Введение в компьютерные сети", дается введение в базовые концепции компьютерных сетей, приводится краткая история развития средств электронной коммуникации и обзор сегодняшнего состояния сетевых технологий.

В главе 2, "Классификация компьютерных сетей", рассматривается классификация сетей на основе области действия, административной модели, сетевой операционной системы, используемых протоколов, архитектуры и топологии.

В главе 3, "Концепции, модели и стандарты компьютерных сетей", приводится обзор средств двоичной коммуникации и дано введение в две наиболее распространенные сетевые модели: DoD (Department of Defense), базирующуюся на протоколе TCP/IP, и OSI (Open Systems Interconnection), разработанную Международной организацией по стандартизации ISO (International Standardization Organization). Рассматриваются также спецификации, поддерживаемые IEEE (Institute of Electrical and Electronics Engineers), и модели некоторых поставщиков

Глава 4, "Методы сетевой коммуникации", посвящена основам аналоговой, цифровой, широкополосной, узкополосной, асинхронной, синхронной, симплексной, дуплексной и мультиплексной передач Рассматриваются также методы доступа к сети, включая CSMA/CD (Carrier-sense Multiple Access with Collision Detection), CSMA/CA (Carrier-sense Multiple Access with Collision Avoidance), Token Ring и приоритеты запросов.

В главе 5, "Локальные сети", описываются распространенные типы локальных сетей (Local Area Network — LAN), включая Ethernet, Token Ring, FDDI, AppleTalk и ARCnet

В главе 6, "Глобальные сети", приводится обзор глобальных сетей (Wide Area Network — WAN), таких, как PSTN, ISDN, T-каналы, Frame Relay, X.25 и CATV. Рассматриваются высокопроизводительные решения ATM, SONET, SMDS и межсетевые соединения, включая ICS (Internet Connection Sharing), NAT (Network Address Translation), брандмауэры и маршрутизируемые соединения.

Часть II. Сетевое оборудование и программное обеспечение

В главе 7, "Физические компоненты сетей", рассматриваются такие компоненты, как коаксиальные кабели, витые пары, волоконно-оптические кабели и различные беспроводные технологии — лазеры, инфракрасные средства связи, радиосвязь и спутниковая коммуникация в микроволновом диапазоне. Описываются также соединительные устройства: повторители, концентраторы, маршрутизаторы и коммутаторы

В главе 8, "Сетевые протоколы и службы", рассматриваются распространенные протоколы локальных сетей: TCP/IP, NetBeui, IPX/SPX и пакет протоколов OSI. Представлены протоколы глобальных сетей — PPP и SLIP, а также распространенные протоколы туннелирования.

В главе 9, "Самая глобальная сеть — Internet", обсуждаются вопросы развития Internet и используемые в ней протоколы — HTTP, FTP, NNTP, SMTP, POP и пакет протоколов TCP/IP.

В главе 10, "Сетевые операционные системы", рассматривается практика сетевого администрирования и особенности операционных систем, включая Windows NT, Windows 2000, NetWare, UNIX и Linux.

В главе 11, " Службы каталогов", представлены протоколы DAP (Directory Access Protocol) и LDAP (Lightweight Directory Access Protocol), а также стандарты X.500, разработанные ISO для обеспечения совместимости и взаимодействия служб каталогов различных систем. Значительное внимание уделяется службам каталогов NDS компании Novell, Active Directory компании Microsoft и StreetTalk компании Banyan VINES.

В главе 12, "Клиентские операционные системы", рассматривается клиентская часть вычислительной сети типа клиент/сервер. Приводятся преимущества и недостатки таких распространенных настольных клиентских систем, как DOS, Windows, Linux, Macintosh и OS/2. Рассматривается также их интеграция в распространенные сетевые среды.

В главе 13, "Гибридные сети", описываются способы взаимодействия и протокольные шлюзы, позволяющие компьютерам с разными операционными системами, протоколами и на разных платформах сообщаться друг с другом. В этой же главе рассматривается взаимодействие компьютеров с мэйнфреймом с использованием SNA (Systems Network Architecture).

Часть III. Специальные вопросы

В главе 14, "Защита сети", рассматриваются способы обеспечения безопасности сетей. Приводится обзор базовых концепций шифрования, рассматриваются открытые и закрытые шифры, службы сертификации, межсетевые экраны, брандмауэры и внутренние средства безопасности, такие, как интеллектуальные карты и развитые технологии аутентификации. В этой же главе приводятся советы относительно разработки стратегии безопасности конкретной вычислительной сети. Далее в ней рассматриваются планы аварийного восстановления, включая реализацию системы RAID (Redundant Array of Inexpensive (Independent) Disks). Описываются также расписания регулярного резервного копирования и кластеризация.

В главе 15, "Удаленный доступ", рассматриваются методы установки связи с территориально удаленным сервером с помощью таких устройств связи, как модемы, терминальные адаптеры ISDN и устройства CPE (Customer Premises Equipment) для работы на выделенной линии. Обсуждается также конфигурирование коммутируемого сервера и специализированные средства обеспечения безопасности.

В главе 16, "Виртуальные частные сети", приводится обзор концепций VPN (Virtual Private Network) и протоколы туннелирования, используемые для обеспечения безопасности VPN.

В главе 17, "Сети с тонкими клиентами", рассматриваются терминалы на основе Network Computers, Net PC и Windows. Описываются терминальные службы Windows, система Citrix Metaframe, работа в Web, система X Window, виртуальные машины Java и роль каждой из этих систем в сетях с тонкими клиентами.

В главе 18, "Инструменты мониторинга, управления и устранения неполадок", дается введение в утилиты TCP/IP и другие инструменты, встроенные в различные операционные системы, и анализируются такие коммерческие продукты, как Sniffer Pro, LANanalyzer, Systems Management Server компании Microsoft, ManageWise компании Novell и Tivoli компании IBM.

Часть IV. Будущее сетей

В главе 19, "Технологии завтрашнего дня", сделана попытка заглянуть в будущее вычислительных сетей. Обсуждаются возможные пути преодоления существующих сегодня ограничений протокола IP, в том числе его новая версия — IPv6. Рассматриваются перспективы достижения всеобщей связи, т.е. всех со всеми. В качестве возможных компонентов будущих вычислительных сетей кратко обсуждаются более экзотические системы — искусственный интеллект, квантовые средства вычислений и кибернетические формы жизни.

Условные обозначения

- **Рисунки, листинги и таблицы**. Предназначены для лучшего объяснения концепций, команд и процедур. Сетевые уровни и процессы иллюстрируются с помощью диаграмм. Копии экрана помогут читателю более наглядно представить процедуры конфигурирования. Дополнительно к листингам и таблицам приводятся обзоры и сравнения рассматриваемых средств.
- **Авторские замечания, советы и предупреждения**. В этих элементах текста предоставлена дополнительная информация по обсуждаемым темам, которая очень пригодится читателю в практической работе.
- **Резюме в конце глав**. В конце каждой главы приводится краткое резюме рассмотренных в ней вопросов, призванное помочь читателю лучше усвоить полученную информацию.
- **Рекомендуемые источники** В конце каждой главы приводится список источников, содержащих дополнительную информацию по темам, рассмотренным в главе. Приведенные источники, включающие адреса Web-узлов, книги и статьи, помогут читателю ознакомиться с рассмотренными вопросами более подробно.
- **Контрольные вопросы**. В каждой главе после рекомендуемых источников приводится 10 вопросов, предназначенных для проверки и закрепления полученных знаний. Вопросы помогут читателю оценить степень усвоения изложенного материала, прежде чем двигаться дальше.

В этой книге приняты следующие правила.

- **Полужирным шрифтом** отмечены команды и фразы, которые должны быть введены читателем точно так же, как написаны. В примерах (но не в синтаксисе) полужирным шрифтом выделено то, что должно быть введено читателем (например, команда **show**).
- *Курсивом* отмечены аргументы, которым нужно предоставить значение.
- Квадратные скобки `[ ]` обозначают необязательные элементы.
- Вертикальная черта `|` разделяет альтернативные взаимоисключающие элементы.
- Фигурные скобки и вертикальные черточки внутри квадратных скобок (например, `[x{y|z}]`) означают обязательный выбор внутри необязательного элемента. Содержимое квадратных скобок вводить не обязательно, однако если оно вводится, то необходимо выбрать один из элементов внутри фигурных скобок.

Часть

Основные концепции компьютерных сетей

В этой части...

1. Введение в компьютерные сети
2. Классификация компьютерных сетей
3. Концепции, модели и стандарты компьютерных сетей
4. Методы сетевой коммуникации
5. Локальные сети
6. Глобальные сети

Глава 1

Введение в компьютерные сети

Добро пожаловать в мир компьютерных сетей! В этом мире уже недостаточно всего лишь иметь и использовать персональный компьютер, сегодня нужно быть еще и "подключенным". Реальное преимущество персональных компьютеров проявляется лишь тогда, когда они связаны и могут сообщаться друг с другом. Переход от простого "двухкомпьютерного" дома и небольшой офисной локальной сети к непрерывно растущей глобальной сети Internet — будущее компьютерных технологий, и оно уже присутствует здесь и сейчас.

Во многих регионах США спрос на обученных специалистов по компьютерным сетям значительно превышает предложение. По прогнозам Департамента труда США компьютерные сети как род занятий имеют блестящее будущее. Коммерческие фирмы и отдельные лица покупают компьютеры и связывают их в локальные и глобальные сети с потрясающими темпами. Сетью опутывается буквально весь мир.

Связь с помощью компьютерной сети быстро становится неотъемлемой частью нашей жизни, поэтому даже для тех, кто не занимается информационными технологиями непосредственно, крайне важно хотя бы иметь общее представление о работе компьютерных сетей. Как сегодня невозможно нормально жить, ничего не ведая о телефоне, так и в ближайшем будущем человек, не знающий, как "подключиться", будет на каждом шагу испытывать огромные трудности.

Краткая история компьютерных сетей

Желание общаться с другими людьми для человека всегда было движущей силой и, в отличие от остальных живых существ, он разработал для этого огромное количество самых разнообразных средств коммуникации. С того самого момента, когда люди впервые связали два компьютера, появление Internet стало неизбежным.

В первые годы развития вычислительной техники компьютеры были огромными, занимали несколько комнат, а иногда и зданий. Причем стоили они сотни тысяч долларов. И хотя объем памяти и быстродействие этих дорогостоящих "монстров" были значительно хуже, чем у сегодняшнего компьютера, способного уместиться на ладони,

в 50–60-х годах прошлого столетия они все же были чудом технологии. По сравнению с медлительным и постоянно ошибающимся человеком возможности этих первых компьютеров были потрясающими.

В середине прошлого века компьютеры были редкими, экзотическими и загадочными машинами. Ими владели только большие компании, правительственные учреждения и университеты. В подавляющем большинстве случаев компьютеры были отдельными системами, изолированными друг от друга.

В 1940-х годах председатель IBM Томас Уотсон (Thomas Watson) сказал, что весь мировой рынок способен поглотить приблизительно пять компьютеров. И даже сравнительно недавно, в 1997 году, президент компании Digital Equipment Corporation Кен Олсон (Ken Olson) отметил: "Нет причин полагать, что компьютер может кому-нибудь понадобиться в его доме" (источник: ISBC — International Small Business Consortium, `www.isbc.com/isbc/business/wisdom.cfm`). Конечно, оба они не просто ошибались, а *очень* ошибались. Однако даже десять лет назад никто не предполагал, что компьютеры получат такое потрясающее распространение или что главным направлением развития компьютерных технологий станут компьютерные сети.

Первые коммуникационные сети

К середине 20-го века электронные средства коммуникации, развивавшиеся уже более столетия, были широко распространены как в Европе, так и в США. Эти первые коммуникационные сети были весьма разнообразны, однако все они передавали только закодированные сигналы. Позже они стали способны передавать голос.

В этом разделе приводится краткая история развития первых коммуникационных сетей.

Телеграфные кабели

В начале 19-го века во Франции была создана первая оптическая телеграфная сеть, передававшая информацию с потрясающей для того времени скоростью — 20 символов в секунду. Тогда же Сэмюель Морзе (Samuel Morse) продемонстрировал электрический телеграф, значительно подтолкнувший развитие коммуникационных сетей в США.

Телефонная сеть: технология коммутации каналов

В конце 19-го века началось создание огромной телефонной сети. Однако лидеры этой технологии были не более дальновидны, чем в начале компьютерной эры. В 1876 году во внутренней памятной записке компании Western Union говорилось: "Так называемый *телефон* имеет слишком много недостатков, чтобы его можно было серьезно рассматривать как средство коммуникации. Для нас это устройство бесполезно" (источник: `www.isbc.com/isbc/business/wisdom.cfm`).

Несмотря на такое отношение к телефону, в 1880 году в Соединенных Штатах было 50 тыс. телефонных линий, а к 1960 году телефонные линии покрыли все города и коммуникационная телефонная сеть стала глобальной.

В телефонных системах используется технология коммутации каналов. Когда один телефон посредством сети соединяется с другим телефоном, между ними замыкается электрическая цепь, т.е. устанавливается физический путь. При передаче голоса это работает вполне удовлетворительно, потому что звук переносится по проводу почти с постоянной скоростью передачи информации.

В сети с коммутацией каналов соединение устанавливается так, как показано на рис. 1.1. В течение сеанса связи по этой цепи проходят все сигналы Если связь разрывается и устанавливается снова, то она может установиться по совсем другой цепи (на рис. 1.1 это отмечено пунктирной линией).



Рис. 1 1. Сплошная линия обозначает установленную связь в сети с коммутацией каналов

При передаче компьютерных данных эта технология работает менее удовлетворительно, так как компьютеры передают информацию "взрывообразно": интервалы максимальной интенсивности чередуются с интервалами низкой или нулевой интенсивности.

Технология коммутации пакетов

В 1960-х годах правительство США было заинтересовано в развитии компьютерных сетей, способных обеспечить связь военных организаций и основных учебных центров друг с другом. Поскольку это было в разгар холодной войны, сеть должна была обладать достаточной избыточностью и устойчивостью, чтобы надежно функционировать в условиях реальной ядерной войны.

Исследователи Массачусетского технологического института (Massachusetts Institute of Technology — MIT), Института RAND (RAND Institute) и Национальной физической лаборатории (National Physical Laboratory — NPL, Англия) разработали технологию, названную *коммутацией пакетов*, работавшую с взрывообразными порциями информации лучше, чем традиционная технология коммутации каналов. Таким образом, они заложили фундамент технологии коммуникации, используемой сегодня в Internet.

Как показано на рис 1.2, в сети с коммутацией пакетов соединение не устанавливается на все время сеанса связи Напротив, отдельные пакеты данных могут передаваться различными путями По одной и той же линии могут проходить сигналы различных соединений, в то время как в технологии коммутации каналов линия полностью занимается соединением на протяжении всего сеанса связи.

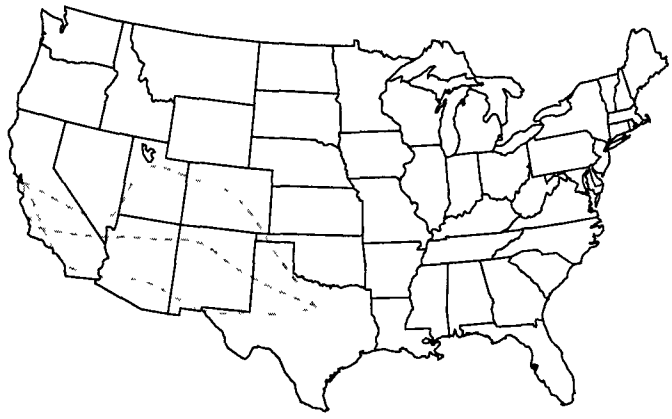


Рис. 1.2. Пути, по которым проходят пакеты данных

Сравнение коммутации каналов и пакетов

Термины *коммутация каналов* и *коммутация пакетов* звучат похоже, однако они означают совершенно разные вещи.

Общедоступная телефонная система, которую иногда называют POTS (plain old telephone service — простая старая телефонная служба), представляет собой коммуникационную сеть с коммутацией каналов. Когда в этой сети абонент набирает телефонный номер, между ним и другим абонентом устанавливается только один физический путь на все время сеанса связи. Этот путь, или *канал*, поддерживается исключительно для двух абонентов, пока один из них не завершит соединение, повесив телефонную трубку.

Однако обратите внимание на то, что если повторно позвонить по этому же номеру с этого же телефона, то отнюдь не обязательно установится этот же путь. Именно потому каналы называются *коммутируемыми*, т.е. плохая, неустойчивая связь между двумя телефонами может улучшиться, если позвонить повторно.

В сети с коммутацией пакетов путь между двумя абонентами не устанавливается. Из-за отсутствия установленного пути технологию коммутации пакетов иногда называют технологией связи *без установления соединения*. При передаче данных, например файла с каким-либо текстом, с одного компьютера на другой по сети с коммутацией пакетов отдельные *пакеты* (т.е. небольшие фрагменты данных) могут передаваться разными маршрутами. И хотя все они прибудут в один и тот же пункт назначения, это не значит, что они прошли по одному и тому же пути. В Internet используется исключительно технология коммутации пакетов.

Технологии коммутации пакетов и каналов можно сравнить с путешествием большой группы туристов из Далласа в Сан-Франциско. Коммутация каналов напоминает перевозку всей группы в одном автобусе, поезде или самолете. Маршрут заранее спланирован, и вся группа едет одним и тем же путем.

В то же время коммутация пакетов похожа на поездку каждого туриста собственным маршрутом. Группа разбивается на отдельные подгруппы, подобно тому как данные разбиваются на пакеты. Некоторые туристы могут поехать на своем автомобиле, другие — на поезде, третьи — в автобусе и т.д. Одни из них поедут прямо в пункт назначения, а другие могут избрать окольные маршруты. Однако со временем все они прибудут в один и тот же пункт, в котором группа опять соберется вместе, аналогично сборке пакетов в конечном пункте коммуникации.

ARPAnet

Первая компьютерная сеть с коммутацией пакетов была разработана в конце 1960-х годов под покровительством Министерства обороны США. Она была названа ARPAnet (Advanced Research Projects Agency network). Первый *узел* ARPAnet (пункт, или точка соединения) был установлен в 1969 году в университете Калифорнии (Лос-Анджелес). Всего за три года сеть "расползлась" по всей территории США, а еще через два года — по всей Европе.

В процессе роста ARPAnet разделилась на две части. Военные назвали свою часть сети *Milnet*, а термин ARPAnet стал обозначать часть сети, соединяющую узлы исследовательских организаций и университетов. В 1980-х годах на смену ARPAnet пришла сеть, образованная из отдельной военной сети Defense Data Network и сети NSFNet (компьютерная сеть научных и университетских узлов, финансируемая Национальным научным фондом США). Со временем эта глобальная сеть выросла в современную Internet.

Компьютерные сети вчерашнего дня

Разработки первых компьютерных сетей не начинались столь масштабно, как проект ARPAnet, — первыми разрабатывались локальные, а не глобальные сети. По мере того как компьютеры становились все более дешевыми и производительными, их стали все шире использовать коммерческие организации самых разных размеров Первые компьютеры были полезны в довольно ограниченных областях обработки данных, однако с бурным ростом производства программных продуктов появляющиеся программные средства обеспечивали пользователей дополнительными функциями, а не только сборкой и сортировкой данных.

С помощью больших универсальных компьютеров (мэйнфреймов) многие пользователи получили доступ к одним и тем же хранимым данным посредством *терминалов*, представлявших собой не более чем устройства для ввода и вывода информации (например, клавиатура и дисплей). Собственные вычислительные возможности терминалов были минимальны — они служили всего лишь пунктами доступа к универсальной вычислительной машине.

В то время большие мэйнфреймы были значительным достижением технической мысли, однако по сравнению с небольшими компьютерами обладали рядом недостатков. Первый — большая стоимость. Мэйнфреймы стоят гораздо дороже так называемых персональных компьютеров, предназначенных для установки на столе и работающих независимо.

Другой недостаток универсальных вычислительных машин — опасность "универсального" краха системы: если машина выходит из строя, то прекращается работа всех пользователей. В этом случае никто не сможет получить доступ к данным, и любой пользователь, зависящий от мэйнфрейма, вынужден будет прекратить работу. В то же время использование персональных компьютеров снимает эту проблему.

Персональные компьютеры появились сразу как полноценные вычислительные машины, выполняющие вводимые в них программы самостоятельно, без использования внешних ресурсов. С их появлением значительно повысилась *отказоустойчивость* системы, т.е. способность функционировать и обеспечивать целостность данных при единичном отказе. Если компьютер одного из служащих выходит из строя, это никак не влияет на других служащих — они могут продолжать работу на своих компьютерах. Фактически служащему достаточно было сохранить данные на гибкой дискете, с которой он мог сесть за любой компьютер и продолжить работу.

Эти факторы привели к быстрому росту популярности персональных компьютеров в коммерческих организациях всех размеров. Однако, когда на столе у каждого служащего появился свой персональный компьютер, возникла проблема обмена информацией между ними. Решением этой проблемы стала компьютерная сеть.

Недостатки изолированных систем

В первые годы после появления настольных персональных компьютеров в продаже еще не было средств коммуникации между ними. В коммерческих организациях компьютеры использовались как изолированные системы. Если, например, нужно было распечатать документы, созданные на разных компьютерах, то сделать это можно было одним из описанных ниже способов.

- Подключить принтер к каждому компьютеру. Это довольно дорогостоящее решение, потому что потребуется приобрести много принтеров, которые вряд ли будут работать одновременно.
- Сохранить файлы с документами на дискете и перенести дискету на компьютер с установленным принтером. Это менее дорогостоящее решение, однако такой способ очень неудобен для исполнителей: как для того, кто пойдет по комнатам искать свободный принтер, так и для того, кому придется прекратить свою работу и ждать, пока на его компьютере будут распечатываться документы, не имеющие к нему никакого отношения.
- Переносить принтер от одного компьютера к другому в зависимости от того, где он сейчас нужен. Весьма обременительное решение. Тем не менее такой способ применялся довольно широко. Были сконструированы даже специальные тележки с установленными на них принтерами. При каждом передвижении нужно было отсоединить и вновь присоединить кабели принтера, а иногда заново конфигурировать программное обеспечение.

Высокая стоимость, неудобства и дополнительные затраты труда — главные недостатки изолированных систем.

Так что же такое *компьютерная сеть*

В словарях *сеть* определена как "система взаимодействующих линий или каналов связи". Телеграфные и телефонные сети коммуникации кратко упоминались в предыдущих разделах. Еще один пример, которого нельзя не заметить, — телевизионная сеть. Пользуясь приведенным выше определением, сетями можно назвать даже системы оповещения на автомобильных и железных дорогах.

И все же, учитывая сказанное, что такое компьютерная сеть? Это два или больше устройств, соединенных для обмена информацией, ресурсами или и тем и другим. Соединение может быть образовано с помощью кабеля (коаксиального, витой пары или, как вы увидите далее в главе, волоконно-оптического) либо с помощью беспроводных средств: радиосигналов, лазерного луча, инфракрасных устройств, спутников связи и т.д. Совместно используемой информацией или ресурсами (которые называются *разделяемыми ресурсами*) могут быть файлы, программы, принтеры, модемы и любое другое оборудование (рис. 1.3).

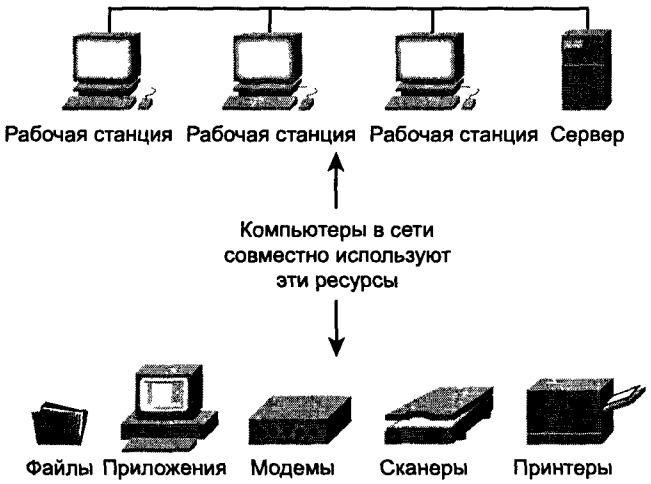


Рис. 1 3 Компьютеры сети совместно используют ресурсы данных, программного обеспечения и оборудования

Зачем объединять компьютеры в сети

Одно из главных преимуществ персональных компьютеров — их независимость друг от друга. Зачем же их объединять? Для того чтобы полнее реализовать преимущества как персональных компьютеров, так и больших универсальных вычислительных машин. Каждый участник сети пользуется преимуществами, с одной стороны, независимости, а с другой — доступа к совместным ресурсам. Совместное использование дорогих и редко применяемых периферийных устройств приносит коммерческим компаниям ощутимую выгоду. Например, дорогостоящий цветной лазерный принтер используется довольно редко, в то же время многим служащим организации иногда нужно что-нибудь распечатать на нем. При доступе к компьютерной сети они могут легко сделать это.

Преимущества объединения

Многие владельцы и управляющие компаниями утверждают, что главной причиной объединения их персональных компьютеров в сеть является необходимость совместного использования принтеров. Однако, когда компьютеры становятся связанными, люди начинают обнаруживать все больше полезных применений сети, помимо совместного использования принтеров.

Стоимость объединения компьютеров в локальную сеть (состоящая из стоимости сетевых адаптеров (Network Interface Card — NIC), кабельных или беспроводных средств связи, концентраторов и других устройств) многократно окупается благодаря уменьшению накладных расходов и трудовых затрат.

Совместное использование устройств вывода

Как отмечалось ранее, в сети можно совместно использовать принтеры, плоттеры и другие устройства вывода. Это экономит время, деньги и устраняет многие проблемы. В качестве устройств ввода-вывода несложно также организовать совместное использование факсов.

Совместное использование устройств ввода

В сети можно совместно использовать сканеры, цифровые камеры и другие устройства ввода. Стоимость этих устройств превышает стоимость принтеров, а частота их использования ниже, поэтому их совместное использование многими участниками сети выгодно.

Совместное использование устройств хранения информации

Компьютеры, объединенные в сеть, могут совместно использовать жесткие диски, дисководы гибких дисков и накопители CD-ROM. Если на одном из компьютеров окажется недостаточно дискового пространства, то можно будет сохранять файлы на жестком диске другого компьютера, подключенного к сети. Кроме того, если на компьютере не установлен накопитель CD-ROM, то можно использовать накопитель CD-ROM другого компьютера. Использовать совместно можно также накопители Zip и Jaz, магнитооптические, ленточные, а также любые другие устройства хранения информации, которые можно подключить к персональному компьютеру.

Совместное использование модемов и подключений к Internet

Еще одним важным свойством сети является способность персональных компьютеров, объединенных в сеть, совместно использовать модемы, кабельные модемы, линии ISDN (Integrated Services Digital Network) и адаптеры DSL (Digital Subscriber Line). Имея соответствующее программное обеспечение (прокси-сервер или NAT, подробно рассматриваемые в главе 9, "Самая глобальная сеть — Internet"), можно посредством одной телефонной линии или учетной записи провайдера Internet (Internet Service Provider — ISP) подключить к Internet всю локальную сеть.

Совместное использование данных и приложений

Использовать в сети совместно можно не только ресурсы оборудования. Файлы данных и программы тоже можно сделать доступными для многих пользователей. В результате будет более эффективно использоваться дисковое пространство и значительно упростится совместная работа нескольких пользователей над одним проектом. Допустим, например, что доступ к электронной таблице, содержащей бюджет отдела, нужен нескольким менеджерам фирмы как для чтения, так и для изменения данных. В этом случае можно разместить файл с таблицей на одном из компьютеров. После этого можно программными средствами предоставить право на изменение данных тем менеджерам, которые должны их изменять, и право на чтение тем, которые должны только читать эти данные.

Приложения, например программы обработки текстовых документов, можно установить на сервере сети. Тогда участники сети смогут использовать их, не занимая свое дисковое пространство громоздкими файлами.

Однако нужно убедиться в том, что лицензионное соглашение с поставщиком программного продукта допускает использование программы на других компьютерах сети даже несмотря на то, что используется лишь одна копия программы.

Рождение Internet

Как уже упоминалось выше в главе, пригодные для использования сетевые технологии появились в середине 1960-х годов. В начале 1970-х совместными усилиями

правительства США (главным образом Министерства обороны) и нескольких университетов была создана сеть ARPAnet.

Роль Министерства обороны США

С усилением политики холодной войны, проводимой между США и СССР в 1960-х годах, Министерству обороны США пришлось всерьез задуматься над необходимостью создания устойчивых связей между основными военными объектами страны. Была поставлена задача обеспечить связь в условиях ядерной войны, когда в результате массовых разрушений традиционные каналы связи окажутся выведенными из строя. Основные научные центры, такие как Массачусетский технологический институт и университет Калифорнии, к этому времени уже занимались разработкой проектов компьютерных сетей.

Министерство обороны начало финансировать исследовательские работы в этом направлении по всей территории США и в 1968 году Управление перспективных исследовательских программ (Advanced Research Projects Agency — ARPA) заключило контракт с частной компанией BNN на создание компьютерной сети на основе технологии коммутации пакетов, разработанной для улучшения характеристик систем передачи компьютерных данных.

1970-е годы: начало бурного роста

Когда проект ARPAnet начинал разрабатываться, никто не ожидал, что компьютерные сети будут расти столь бурно. На протяжении 70-х годов новые узлы сети были установлены как на территории США, так и за рубежом.

1980-е годы: чем больше, тем лучше

В 1983 году ARPAnet была разделена. Из 113 существовавших на то время узлов 68 были выделены в отдельную сеть Milnet, интегрированную с сетью оборонных данных (Defense Data Network — DDN), которая была создана за год до этого.

Служба имен доменов (Domain Name System — DNS), появившаяся в 1984 году, позволила без больших потерь преобразовать имена главных компьютеров в адреса IP (Internet Protocol), более удобный и эффективный метод, чем предыдущие. Эти предыдущие методы рассматриваются в главе 8, "Сетевые протоколы и службы". В 1984 году в сеть были объединены уже более 1000 узловых компьютеров.

Во второй половине 80-х годов компьютерная сеть значительно расширилась. Например, Национальный научный фонд США (National Science Foundation — NSF) создал компьютерные центры в Принстоне, Питсбурге, университете Калифорнии (Сан-Диего), университете Иллинойса (Урбана-Шемпейн) и в Корнелле. В это же время была образована и группа IETF (Internet Engineering Task Force). К 1987 году в сети было 10 000 узловых компьютеров, а к 1989 году их количество увеличилось до 100 000.

1990-е годы: сеть становится большим бизнесом

Феноменальный рост сети в 80-х годах — ничто по сравнению с тем, что произошло в 90-х. Правительство США всерьез занялось разработкой так называемых информационных магистралей, в результате чего система ARPAnet прекратила свое существование и была "изобретена" Internet. Магистраль сети NSFnet (сеть Национального научного фонда США) была усовершенствована до стандарта T3, ее производительность составила 44 736 Мбит/с, и в 1991 году по ней передавалось более одного трил-

лиона байт в месяц. Было образовано общество ISOC, и в 1992 году в Internet входило уже более 1 млн узловых компьютеров.

Это было десятилетие коммерциализации Internet. По мере того как к Internet подключались все больше студентов колледжей, индивидуальных пользователей и компаний всех размеров, бизнесмены осознали появление нового бурно растущего сектора рынка. К 1995 году этот рынок был освоен рекламными компаниями, начали быстро расти масштабы сетевых банковских операций, по Internet уже можно было даже заказать пиццу.

Во второй половине 90-х годов новые средства сетевой коммуникации стали появляться почти ежедневно. Потоковые аудио- и видеоданные, технология принудительной доставки информации, Java, ActiveX, языки сценариев делали компьютерные сети все более доступными и удобными, причем по все более низкой цене. Имена доменов стали предметом большого бизнеса: цены пользующихся наибольшим спросом имен превысили миллион долларов! В декабре 1999 года сеть World Wide Web содержала почти миллиард узлов, к ней были подключены более 50 млн узловых компьютеров по всему миру.

На рис. 1.4 показана диаграмма наиболее существенных событий истории развития компьютерных сетей.

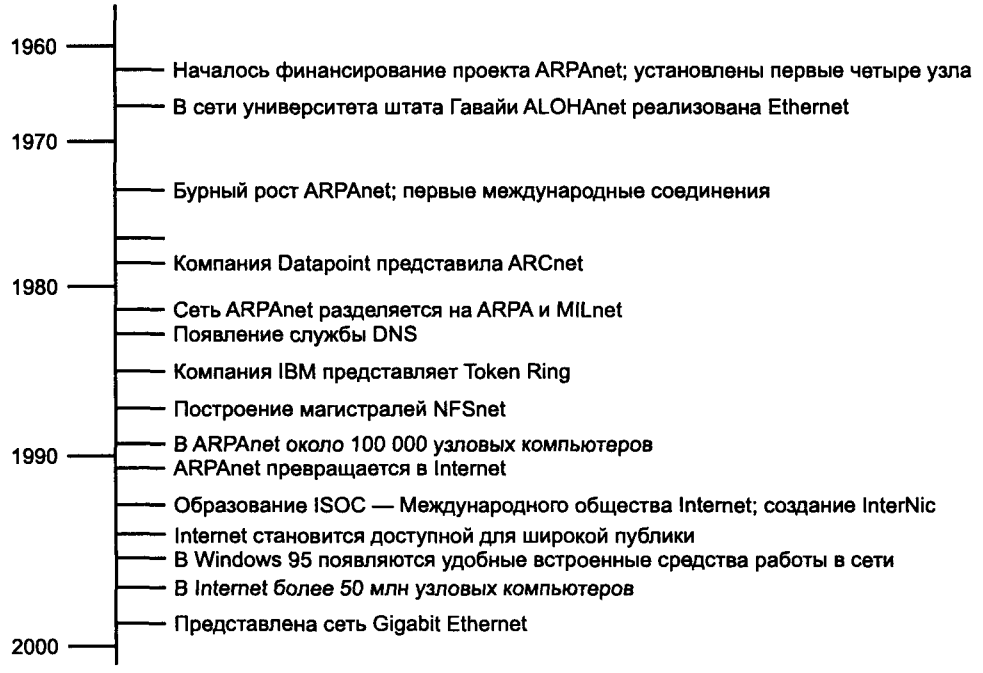


Рис. 1.4. История развития сетей персональных компьютеров

Стоимость технологии: все больше благ за все меньшую цену

По мере развития компьютерных и сетевых технологий на протяжении нескольких последних десятилетий существенно снизилась стоимость постоянно совершенствующихся средств сетевой коммуникации. Именно снижение цен в значительной степени

повлияло на рост популярности компьютерных сетей как в большом бизнесе, так и в личной жизни многих людей.

В 1970–80-х годах персональный компьютер стоил несколько тысяч долларов. На компьютер смотрели как на произведение искусства. И хотя службы доступа к сети существовали, при цене 25 долларов за час позволить себе такую роскошь могли только большие коммерческие организации или очень богатые люди. Ветераны компьютерной техники могут вспомнить удивительное для того времени объявление компании Prodigy о доступе к сети всего за 9,95 $ в час с "потрясающей" пропускной способностью 1 200 и 2 400 бит/с.

Сегодня за 1 000 долларов можно купить компьютерную систему с намного лучшими характеристиками, чем у мэйнфрейма по цене 500 тыс. долларов 20 лет назад. Доступ к Internet с помощью DSL (Digital Subscriber Line) или кабельного модема с пропускной способностью, эквивалентной стандарту T-1 (1,544 Мбит/с), сегодня обойдется в 30–40 долларов в месяц, причем цена продолжает снижаться. Базовый доступ к Internet с пропускной способностью 56 Кбит/с можно получить значительно дешевле, а иногда даже бесплатно, если пользователь согласится терпеть на своем экране рекламу.

Сети персональных компьютеров сегодня

В новом тысячелетии мы становимся свидетелями охвата компьютерными сетями всего мира. Более того, ее величество Сеть начинает проникать во все уголки нашей жизни. Мы пользуемся компьютерами на работе и дома, берем их с собой в самолет и даже на пляж.

И поскольку появляется огромное количество компьютеров, само собой напрашивается решение объединить их в сеть. Действительно, главной задачей большинства этих компьютеров является доступ к Internet. В этом разделе мы коротко остановимся на том, какими путями объединенные в сеть компьютеры способны изменить нашу жизнь.

Домашние компьютеры

Наличие дома собственного персонального компьютера теперь уже никого не удивляет, причем многие компьютеры были специально разработаны как устройства, готовые к подключению к Internet. Во многих домах под одной крышей сосуществует несколько компьютеров, при этом неизбежно появляется желание соединить их. И действительно, в последние годы появился новый и бурно растущий рынок домашних локальных сетей, использующих не традиционные кабели Ethernet, а беспроводные средства связи, телефонные или электрические провода.

Web и электронная коммерция

Коммерческие организации любых размеров и типов все больше убеждаются в том, что иметь собственный Web-узел выгодно и даже жизненно необходимо. Теперь даже небольшие фирмы в целях снижения затрат все больше обращаются к электронной коммерции, т.е продаже своих продуктов и услуг посредством Internet. В больших корпорациях обычными стали *корпоративные сети*, объединяющие компьютеры своих офисов, разбросанных по всему миру, в одну внутреннюю сеть и с Internet.

Высокопроизводительные коммерческие сети

Сегодня обычными становятся волоконно-оптические и другие соединения с высокой пропускной способностью, благодаря которым видеоконференции все чаще приходят на смену личным встречам. Благодаря средствам удаленного доступа и виртуальным частным сетям руководители подразделений получили возможность поддерживать тесный контакт со своими офисами, даже находясь в пути. Посредством сети общаются служащие всех уровней организации, что позволяет более гибко распределять рабочее время. Кроме того, компания экономит средства на оборудовании рабочих мест и других накладных расходах. Передача больших файлов данных сегодня осуществляется быстро и эффективно. Благодаря доступным и высокопродуктивным технологиям сегодня значительно усовершенствованы даже традиционные работы в сети, не требующие высокой пропускной способности, такие как составление расписаний или электронная корреспонденция.

Обучение с помощью сети

В настоящее время сеть все более охватывает обычные средние школы. Колледжи и университеты предлагают курсы в кредит, которые можно пройти частично или полностью в Internet. Обучение в сети становится реальностью. Поставщики оборудования и программного обеспечения, понукаемые ведущими игроками, такими как Microsoft и Cisco Systems, все больше объединяют свои усилия с коммерческими и бесприбыльными организациями, чтобы сделать Internet и другие сети доступными для всех желающих.

Будущее компьютерных сетей

В конце книги рассматриваются новые технологии в области телекоммуникации. Некоторые из них еще только проектируются, другие уже прошли тестирование и признаны годными для лабораторий или, в ограниченных масштабах, для широкой публики.

Государственные органы и большие корпорации стремятся содействовать развитию новых, более совершенных и быстродействующих средств телекоммуникации и внедрению их в повседневную жизнь людей на всех социальных уровнях. Благодаря этому постоянно появляются новые головокружительные разработки как оборудования, так и программного обеспечения. Характер работы и способы проведения досуга людей постоянно изменяются. Средства глобальной коммуникации делают нашу планету все меньше, а ее удаленные уголки — все доступнее. Вследствие развития этих процессов оптимисты предсказывают исчезновение национальных и культурных барьеров. Начинают появляться общедоступные центры коммуникации, услугами которых могут воспользоваться группы и отдельные люди, пока что не имеющие доступа к телекоммуникационным сетям из-за их дороговизны или вследствие недостаточной технической подготовки.

Размышления о будущем компьютерных сетей — это в значительной степени попытка предвидеть непредсказуемое. Двадцать лет назад многие технологии, обычные сегодня, были немыслимы даже для авторов научно-фантастических романов. В последующие двадцать лет развитие компьютерных и телекоммуникационных технологий, скорее всего, пойдет в совершенно новых и непредсказуемых направлениях. Однако на горизонте все же маячат некоторые интересные возможности, которые кратко рассматриваются ниже.

"Умные" устройства в нашем доме

Уже сегодня компьютеризированные домашние устройства если и не широко распространены, то по крайней мере вполне доступны. В продаже есть кухонные приборы со встроенными микропроцессорами, или миниатюрными компьютерами, контролирующими температуру, время приготовления пищи и т.д. Следующий шаг (причем весьма небольшой) — подключение этих устройств к компьютерной сети, чтобы ими можно было управлять на расстоянии. Видимо уже недалеко то время, когда можно будет, находясь в офисе, дать команду своим кухонным приборам начать приготовление ужина.

Эта концепция логически подводит нас к следующему шагу: к "умному" дому, который полностью компьютеризирован и подключен к центральной компьютерной сети. Наглядный пример — личный особняк Билла Гейтса (Bill Gates), президента компании Microsoft, в котором компьютеризованные устройства регулируют микроклимат и перемещают "музыкальные зоны" из одной комнаты в другую, следуя за хозяином.

Многие компании уже сейчас предлагают клиентам сделать их дом "умным", опутав его локальной сетью Ethernet с компьютеризированными телефоном, системой безопасности, домашним театром, системами отопления, кондиционирования и освещения. Всеми этими системами можно управлять щелчком мыши или с помощью голосовых команд. На рис. 1.5 показаны некоторые функции технологии "умного" дома, доступные уже сегодня.

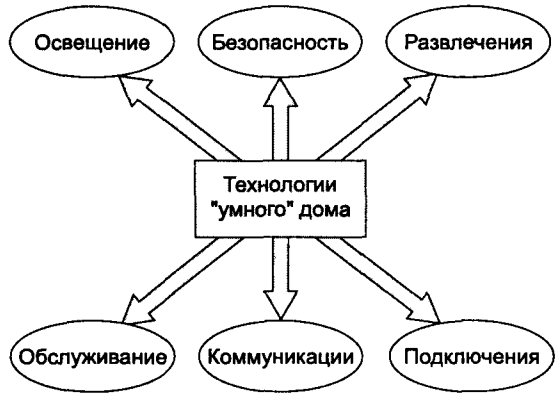


Рис. 1 5. Технология "умного" дома привносит будущее в сегодняшний день

Перспективы технологии "умного" дома обсуждаются более подробно в главе 19, "Технологии завтрашнего дня".

Звонок домой

Между тем на протяжении бурных последних десятилетий продолжала спокойно развиваться технология телефонной связи. Разработки в этой области поступали на рынок и входили в нашу жизнь так гладко и постепенно, что привлекли намного меньше внимания, чем они заслуживают.

Поставщики мобильных телефонов создали сотовые и спутниковые системы телефонной связи, предоставляющие весьма изощренные услуги, например беспроводной доступ к Internet при почти доступной цене. Причем эти технологии постоянно совершенствуются.

Телефонные компании, подстегиваемые компаниями кабельного телевидения, реализуют высокоскоростные услуги передачи данных, такие как ADSL (Asymmetric Digital Subscriber Line), по достаточно низкой для домашнего пользователя цене.

В телефонное оборудование различными способами встраиваются персональные компьютеры. Это предоставляет клиентам дополнительные услуги, например автоматический ответ, хранение сообщений и т.д.

Замечание

В телефонном оборудовании объединяются компьютерные и телекоммуникационные технологии. Техническая реализация совмещенных технологий описывается спецификациями TAPI (Telephony Applications Programming Interface) и стандартами ITC (Internet and Telecoms Convergence Consortium).

Существующее оборудование и программное обеспечение Internet позволяет передавать голос с помощью протокола IP, полностью минуя телефонные линии (если, конечно, с помощью кабеля или беспроводных средств установлено соединение с Internet). Таким способом с помощью компьютера можно побеседовать с приятелем на другом конце Земли, не внося высокую плату за международный звонок.

В настоящее время многие операционные системы, например последние версии Windows, поддерживают не только средства телефонной связи с помощью протокола IP, но и передачу движущихся изображений повышенного качества и данных посредством соединения TCP/IP.

В главе 19, "Технологии завтрашнего дня", перспективы развития систем личной коммуникации рассматриваются более подробно.

Рабочее место без проводов

Складывается впечатление, что в какой бы офис вы ни зашли, вы увидите компьютер (или несколько) на каждом рабочем столе, причем каждый из них подключен к внутренней локальной сети, к Internet и к нескольким удаленным частным компьютерным сетям. Остается только удивляться: неужели можно *еще* больше компьютеризировать и опутать кабелями рабочее место?

Тем не менее в будущем роль компьютерных сетей в офисной работе станет гораздо значительнее. Коммерческая среда все более насыщается волоконно-оптическими и другими высокоскоростными средствами коммуникации, непрерывно растет пропускная способность каналов, телеконференции в реальном времени становятся все более привлекательной альтернативой личных встреч. Все больше служащих смогут выполнять свою работу, не выходя из дома. Однако они не будут изолированы с их маленькими индивидуальными проектами. Напротив, они смогут легко обмениваться по сети документами и чувствовать себя в команде коллег, выполняющих совместную работу.

По мере того как уменьшаются размеры полнофункциональных компьютеров и улучшаются их характеристики, становится все легче "взять с собой офис в дорогу". Умещающиеся на ладони портативные компьютеры, которые сегодня подключены к электронной почте и Web, в ближайшем будущем, несомненно, возьмут на себя функции переносной мультимедийной системы, средства голосовой коммуникации и службы оповещения, которые сейчас реализованы в отдельных устройствах. Больше

не придется носить с собой отдельно переносной компьютер, мобильный телефон и пейджер: все их заменит единственное устройство, помещающееся в кармане.

Став общедоступными и получив связь со всем миром, такие устройства способны существенно повысить эффективность бизнеса любого типа.

Школы будущего

Развитие сетевых технологий, безусловно, повлияет и на систему образования. Уже сегодня почти в каждой библиотеке есть один или несколько подключенных к Internet компьютеров, предназначенных для студентов.

Больше всего на систему образования повлияет доступность информации в немыслимых прежде масштабах. Становятся популярными новые методики, вовлекающие в процесс обучения дополнительные органы чувств. В дошкольном возрасте это интерактивные образовательные игры, привлекающие внимание ребенка и способствующие развитию координации движений.

На уровне колледжей и университетов общей тенденцией, видимо, становится заочное обучение. Студенты смогут "посещать лекции" посредством компьютера, загружая рекомендованные материалы для чтения и возвращая преподавателю ответы на контрольные вопросы и выполненные упражнения с помощью электронной почты. Пользуясь мультимедийными средствами, они смогут также участвовать в дискуссиях. Некоторые университеты уже сегодня предоставляют такой курс обучения по отдельным предметам. В будущем, видимо, этот способ получения образования станет общепринятым.

Компьютерные сети и охрана здоровья

Достижения компьютерных и телекоммуникационных технологий значительно повлияют на медицину и охрану здоровья. Наиболее очевидная выгода от применения компьютерных сетей в системе охраны здоровья вытекает из возможности накапливать, обрабатывать и предоставлять практикующим врачам обширную медицинскую информацию. Врач сможет быстро получить десятки историй болезней с интересующим его заболеванием, что позволит ему проанализировать протекание болезни и эффективность применяемых методик.

Многие другие захватывающие разработки уже сейчас или внедряются в медицинскую практику, или ожидают выхода в свет в ближайшем будущем, например дистанционная хирургия. Хирург получит возможность оперировать больного, находящегося на другом континенте, с помощью подключенных к глобальной сети контрольно-измерительных устройств и управляемых манипуляторов. На сегодняшний день таким образом успешно проведено уже несколько экспериментальных операций.

Родственное этому направление — дистанционная диагностика. Врач получит возможность обследовать пациента с помощью подключенных к сети видеоустройств и диагностических приборов. Эта идея особенно ценна для сельской местности, где всегда ощущался острый недостаток врачей.

Компьютерные сети и юриспруденция

С применением компьютерных сетей юридические исследования и судебная практика становятся все более эффективными вследствие усовершенствования системы хранения юридической информации и упрощения доступа к ней.

Современные сетевые технологии все больше входят в практику полицейских подразделений. В настоящее время на многих патрульных машинах уже установлены мобильные терминалы данных. С их помощью полицейский может быстро получить доступ к базам данных с информацией об уголовном прошлом подозреваемых, о регистрации водительских прав и автомобиля и т.д. Эти устройства позволяют полицейским сообщаться друг с другом и со своим отделением намного быстрее и эффективнее, чем посредством традиционных радиоканалов, не опасаясь при этом прослушивания. В отделениях полиции начинает внедряться технология GPS (Global Positioning System), объединяющая средства автоматической генерации сигналов с патрульных машин и компьютеризированной обработки поступающих сигналов в отделении полиции. Руководство подразделения в любой момент может наблюдать, где находится каждая патрульная машина, что позволяет скоординировать действия полицейских намного эффективнее.

Межгалактическая сеть?

На сегодняшний день глобальная сеть Internet проникла почти во все уголки земного шара. Куда ей расти дальше? Видимо, в космическое пространство. Эта идея не настолько футуристична, как может показаться на первый взгляд. Уже сегодня средства телекоммуникации позволяют обмениваться информацией с орбитальными спутниками и межпланетными автоматическими аппаратами. Довольно давно разрабатываются проекты отправки и приема радиосигналов из далекого космоса в надежде привлечь внимание внеземных цивилизаций, если они, конечно, существуют.

Компьютеры на Земле помогают управлять беспилотными космическими аппаратами. Без компьютеров и средств телекоммуникации были бы невозможны полеты пилотируемых космических кораблей. Благодаря технологиям телекоммуникации становится возможным все более широкое исследование межпланетного пространства.

Краткий обзор терминологии компьютерных сетей

Первое, что нужно сделать, приехав в другую страну, — это выучить хотя бы несколько слов незнакомого языка. Это же справедливо и для тех, кто начинает осваивать новую для себя область знаний.

В сфере компьютерных сетей, как и в большинстве профессиональных областей, сложился собственный жаргон, включающий термины и сокращения. Для непосвященных они выглядят не менее загадочно, чем слова незнакомого языка.

Чтобы можно было понять изложенный в книге материал, необходимо прежде всего хорошо освоить используемую терминологию. В этом разделе приводятся лишь начальные сведения о наиболее часто встречающихся узкоспециальных терминах.

Данный раздел не является исчерпывающим словарем терминов по компьютерным сетям. Здесь лишь приведены определения и короткое объяснение наиболее важных фундаментальных понятий, терминов, фраз и сокращений, без знания которых усвоить материал нескольких следующих глав будет довольно трудно.

Каждый представленный здесь термин подробнее поясняется в последующих главах. Более полный список терминов приведен в конце книги.

Концептуальные термины

Сетевая модель. Графическое представление протекающих в сети процессов. В наиболее распространенных моделях эти процессы представлены как уровни, следовательно, они называются *уровневыми моделями*. Чаще всего встречаются следующие модели сети: семиуровневая модель OSI (Open Systems Interconnection), четырехуровневая модель Министерства обороны США (более известная как модель TCP/IP) и сетевая модель Microsoft Windows. Каждая из них подробно обсуждается в главе 2, "Классификация компьютерных сетей".

Сети клиент/сервер. Компьютер, посылающий запросы на другой компьютер и получающий доступ к хранящимся там данным и ресурсам, называется *клиентским компьютером*. Компьютер, отвечающий на запросы и предоставляющий свои данные и ресурсы другим компьютерам посредством сети, называется *сервером*. В *одноранговой* сети (peer-to-peer) все компьютеры выполняют как клиентские, так и серверные функции. В отличие от этого, в сети *клиент/сервер* (или в *домене* — части сети) выделен компьютер, выполняющий функции сервера. На нем выполняются специальные программы, обслуживающие клиентские компьютеры, выполняющие аутентификацию пользователей и поддерживающие безопасность сети. В главе 2, Классификация компьютерных сетей", рассматриваются как одноранговые сети, так и сети клиент/сервер.

Термины сетевого оборудования

Сетевой адаптер. Плата, установленная в компьютер и соединяющая его с компьютерной сетью. Обычно эта плата вставляется в гнездо типа ISA, PCI, или PCMCIA. Она соединяет компьютер со *средой*, которая, в свою очередь, соединена с другими компьютерами сети.

Среда. Любые средства передачи сигналов от одного компьютера к другому.

Беспроводная среда. Устройства радиосвязи, лазеры, инфракрасные устройства или спутниковые средства связи, по которым сигналы между компьютерами передаются без установки постоянного электрического соединения.

Коаксиальный кабель. Кабель, используемый для связи компьютеров в сеть Подобно телевизионному кабелю, представляет собой медный провод, окруженный металлическим экраном, защищающим передаваемые данные от помех. Используются как тонкие, так и толстые коаксиальные кабели.

Витая пара. Два скрученных медных провода в одной защитной оболочке. Часто применяется также в средствах телефонной коммуникации. В сетевых технологиях используются экранированные и неэкранированные витые пары. Экранированная витая пара окружена металлической защитной оболочкой, предохраняющей от помех. В современных сетях Ethernet чаще всего используются экранированные витые пары. В зависимости от пропускной способности витые пары могут принадлежать к различным категориям вплоть до категории 5, поддерживающей пропускную способность не ниже 100 Мбит/с.

Пленум. Небольшое пространство между фальшь-потолком и перекрытием (или между полом и фальшь-полом), используемое в зданиях для вентиляции и прокладки сетевого кабеля. Пленум-кабель представляет собой кабель с внешней оболочкой из тефлона, или другого пожаробезопасного материала, проложенный в пленуме.

ПВХ (поливинилхлорид). Материал, используемый для изготовления кабелей, не предназначенных для прокладки в пленуме. Он менее дорогой, чем материалы пле-

нум-кабелей, однако при возгорании выделяет ядовитый газ, поэтому устанавливать в пленуме кабели с оболочкой из ПВХ нельзя.

Волоконно-оптический кабель. Представляет собой (в отличие от медного) пучок стеклянных или пластмассовых нитей, по которым предаются импульсы света, несущие полезный сигнал. По сравнению с медными волоконно-оптические кабели имеют ряд преимуществ, среди которых более высокая пропускная способность и лучшее сохранение формы сигнала на большом расстоянии. К их недостаткам относятся большая стоимость и необходимость дополнительного оборудования, преобразующего оптические сигналы в электрические.

Соединительные устройства. Этот термин может означать различные типы устройств, используемых для соединения участков кабелей, двух или более небольших сетей (подсетей) в одну большую сеть, или разделения большой сети на несколько меньших. Сюда относятся повторители, концентраторы, коммутаторы, мосты, маршрутизаторы и мосты-маршрутизаторы. Каждое из этих устройств подробно рассматривается в главе 7, "Физические компоненты сетей".

Термины программного обеспечения

Протокол. Набор правил, обусловливающих способы кодирования передаваемой информации. Иногда протоколы сравнивают с языками, однако по нашему мнению они больше похожи на синтаксис языка, определяющий правила его функционирования. Существует много различных типов компьютерных протоколов. Термин *стек (набор) протоколов* означает два или большее количество протоколов, работающих совместно. *Комплект протоколов* — это несколько протоколов, выполняющих различные функции на разных участках процесса коммуникации.

Сетевая операционная система. Операционная система сервера, например Windows NT Server, Windows 2000 Server, Novell NetWare или UNIX. Этим термином иногда обозначаются также сетевые компоненты клиентских операционных систем, таких как Windows 95 или Macintosh OS.

Клиентская операционная система. Операционная система, выполняющаяся на рабочей станции или на клиентском компьютере, которые имеют доступ к серверу и зарегистрированы в сети в качестве клиента.

Гибридная компьютерная сеть. Сеть, программное обеспечение которой состоит из программ различных поставщиков, особенно программное обеспечение сервера. Например, гибридной является сеть, в которой контроллерами доменов служат системы Windows NT, файловыми серверами — NetWare, а Web-серверами — операционные системы UNIX.

Термины топологии сети

Локальная сеть (Local Area Network — LAN). Сеть, развернутая на небольшой площади. Это может быть комната, этаж, здание или несколько расположенных рядом зданий.

Глобальная сеть (Wide Area Network — WAN). Сеть, составленная из нескольких локальных сетей. Географические пределы глобальной сети ничем не ограничены. С помощью телефонных линий или спутниковых средств связи глобальная сеть может объединять компьютеры в разных городах, странах и даже на разных континентах.

Городская сеть (Metropolitan Area Network — MAN). По площади охвата занимает промежуточное положение между локальными и глобальными сетями. Может покрывать большой город или мегаполис.

Физическая топология. Термин означает физическую раскладку или форму сети. Шинная топология предполагает последовательное (линейное) соединение компьютеров друг с другом. Если при этом последний компьютер соединен с первым, то говорят о кольцевой топологии. При звездообразной топологии все компьютеры соединены с одним концентратором Ячеистая топология предполагает наличие многочисленных избыточных соединений между всеми (или почти всеми) компьютерами. Каждая из этих топологий подробно рассматривается в главе 3, "Концепции, модели и стандарты компьютерных сетей".

Логическая топология Путь прохождения сигналов от одного компьютера к другому Логическая топология тесно связана с физической Например, физическая топология сети может быть звездообразной, в которой каждый компьютер подключен к общему концентратору, однако внутри концентратора данные могут ходить по кругу, образуя таким образом *логическое кольцо.* Разница между физической и логической топологиями обсуждается в главе 3, "Концепции, модели и стандарты компьютерных сетей".

Термины единиц измерения

бит. Наименьшая порция данных. Бит может принимать значение 0, или 1. В двоичном формате данных, обрабатываемых компьютером, информация представлена битами.

байт. Единица количества информации. Равен 8 битам. Размер файлов данных, объем памяти и объем передаваемых по сети данных традиционно определяется в байтах.

Кбайт (килобайт). Объем информации, равный 1 024 байт. Часто его приближенно полагают равным 1 000 байт. Иногда встречается его сокращенное обозначение "К".

Кбайт/с (килобайт в секунду). Единица измерения скорости передачи информации, или пропускной способности канала связи.

Кбит/с (килобит в секунду). То же в битах.

Мбайт (мегабайт) Единица количества информации, равная 1 048 576 байт. Часто приближенно полагают его равным 1 млн байт.

Мбайт/с (мегабайт в секунду). Единица измерения скорости передачи информации, или пропускной способности канала связи.

Мбит/с (мегабит в секунду). То же в битах.

Гц (герц) Единица измерения частоты. Частота в герцах равна количеству циклов повторения какой-либо переменной в секунду В герцах измеряется частота звука, переменного тока и других периодических процессов

МГц (мегагерц). Один миллион циклов в секунду. В мегагерцах традиционно измеряется частота тактового генератора компьютерного процессора.

ГГц (гигагерц) Один миллиард циклов в секунду

Замечание

Довольно распространенная ошибка связана с тем, что килобайты часто путают с килобитами или мегабайты с мегабитами Этому немало способствуют принятые в англоязычной литературе обозначения Kb, kb, KB, Mb или MB, из которых не всегда ясно, что имеется в виду Обычно прописная буква *B* означает байты, а строчная *b* — биты Об этом необходимо помнить, сравнивая скорость передачи данных, выраженную в килобайтах в секунду со скоростью, выраженной в килобитах в секунду. Например, в описаниях программного обеспечения модемов пропускная способность соединения чаще всего приводится в килобитах в секунду, а скорость выгрузки файлов распространенными броузерами — в килобайтах в секунду Таким образом, если модем под-

держивает, например, 45 Кбит/с, то максимальная скорость выгрузки файлов составит 5,76 Кбайт/с. Однако практически эта скорость все же не достигается, потому что на нее влияют и другие факторы, дополнительно загружающие канал. Более подробно скорость передачи данных обсуждается в главе 7, "Физические компоненты сетей".

Замечание

Тактовая частота процессоров персональных компьютеров постоянно растет. В 1980-х годах она редко превышала 10 МГц (первоначально у IBM PC — 4,77 МГц). К 2000 году их тактовая частота приблизилась к 1 ГГц.

Что есть и чего нет в этой книге

В книге приведен обзор основ сетевых технологий и рассмотрены наиболее распространенные на сегодняшний день серверные и клиентские операционные системы. Но, поскольку нельзя объять необъятное, многие вопросы затронуты не так подробно, как в более специализированных изданиях.

На протяжении всей книги в конце каждой главы читателю предоставляются списки дополнительных источников информации по рассмотренным вопросам.

Сертификация специалистов сетевых технологий

Вследствие острой нехватки квалифицированных специалистов и высоких требований к персоналу сертификация стала распространенным средством оценки базовых знаний и квалификации специалистов, особенно при поступлении на работу. Для проверки уровня знаний в области сетевых технологий сертификационные экзамены в настоящее время практикуются во многих организациях.

Сертификация, ориентированная на конкретного поставщика

Некоторые программы сертификации ориентированы на конкретного поставщика. На экзамене проверяется способность претендента работать с конкретным оборудованием или программными продуктами и понимание претендентом технической политики компании-разработчика. Многие сертификаты, например Cisco CCIE или Microsoft MCSE, широко известны и пользуются заслуженным авторитетом.

Замечание

Сертификация, ориентированная на поставщика, выявляет подготовленность к работе с конкретным продуктом. При поступлении на работу сертификат во многих случаях желателен или даже обязателен.

Ниже приведен список наиболее распространенных сертификационных программ, ориентированных на конкретного поставщика.

- CCNA (Cisco Certified Network Associate), CCNP (Cisco Certified Network Professional), CCNE (Cisco Certified Network Expert)
- MCP (Microsoft Certified Professional), MCSE (Microsoft Certified Systems Engineer)
- CNA (Novell Certified NetWare Administrator), CNE (Novell Certified NetWare Engineer)

Такие компании, как Sun, Lotus, IBM, RedHat, и другие поставщики Linux также проводят сертификационные экзамены по своему программному обеспечению компьютерных сетей. Сертификационные экзамены по оборудованию проводят компании IBM, Compaq Computers, Digital Equipment Corporation и др.

Сертификаты, не ориентированные на конкретного поставщика

Программы сертификации, не ориентированные на конкретного поставщика, оценивают общие знания и способности, необходимые для работы с сетевыми продуктами широкого диапазона поставщиков

Наиболее популярная программа сертификации такого типа — Network+, предоставляемая ассоциацией CompTIA (Computing Technology Industry Association). Этой ассоциацией разработан также технический экзамен A+ по оборудованию персональных компьютеров, не принадлежащему конкретному поставщику

Сертификаты, не ориентированные на конкретного поставщика, полезны для оценки фундаментальных знаний в области концепций, практического использования и терминологии компьютерных сетей.

Соответствие данной книги программам сертификации

Эта книга была задумана как широкий обзор наиболее существенных аспектов теории и практики компьютерных сетей Она может служить введением в сетевые технологии как для новичков в области информационных технологий, так и для готовящихся к сдаче сертификационного экзамена, например CCNA, MCSE или CNA

Совместно с другими учебными материалами книга полезна и как руководство по подготовке к экзамену Network+ В книге рассматриваются все вопросы, включенные в программу экзамена Рассматриваются также вопросы, включенные в экзамен *Networking Essentials* компании Microsoft, являющийся первым из шести экзаменов, необходимых для получения сертификата MCSE.

Замечание

Программа сертификации Network+ поддерживается и финансируется такими компаниями, как Microsoft, Novell, IBM, Lotus и многими другими

В новую программу сертификации по Windows 2000 не входит экзамен, посвященный исключительно основным вопросам сетевых технологий, материал книги будет полезен при подготовке к экзамену *70-216 Implementation and Administering a Microsoft Windows 2000 Network Infrastructure*

Резюме

В главе дано введение в мир компьютерных сетей. Приведена история развития компьютерных сетей. Рассмотрено появление первых локальных сетей и развитие ARPAnet — совместного проекта Министерства обороны США и ведущих университетов, превратившегося сегодня в глобальную сеть Internet.

Кратко описано, как сетевые технологии влияют на нашу жизнь и приведен обзор некоторых вопросов, которые будут подробно рассмотрены в следующих главах. Определены наиболее часто встречающиеся термины и рассмотрены программы сертификации специалистов в области сетевых технологий.

Материал, изложенный в этой главе, служит основой следующих глав, из которых читатель узнает о моделях и стандартах, положенных в основу современных компьютерных сетей. Будут подробно рассмотрены как небольшие локальные, так и сложные глобальные сети. Читатель ознакомится с методами сигнализации, архитектурой, оборудованием, протоколами, операционными системами и службами, обеспечивающими работу современных компьютерных сетей.

Будут рассмотрены такие важные темы, как безопасность и устранение неполадок, а также удаленный доступ, виртуальные частные сети и сети с тонкими клиентами. Будут также представлены еще только разрабатываемые в настоящий момент многообещающие технологии, закладывающие основы будущего компьютерных сетей.

Рекомендуемые источники информации

Определения терминов и сокращений, применяемых в области сетевых технологий, можно найти по адресу: `www.whatis.com`.

Дополнительная информация об истории развития компьютерных сетей приведена по адресу: `www.silkroad.com/net-history.html`.

Информация об ассоциации CompTIA и сертификационной программе Network+ есть на Web-узле ассоциации по адресу: `www.comptia.com`.

Дополнительная информация об учебных курсах и экзаменах программ сертификации, ориентированных на конкретного поставщика, есть на Web-узлах соответствующих организаций:

- `www.cisco.com/warp/public/10/wwtraining/certprog` (Cisco);
- `www.microsoft.com/train_cert` (Microsoft);
- `education.novell.com/certinfo` (Novell).

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Какая технология дальней коммуникации была впервые реализована во Франции в начале 19 века?
   а. Телефонная сеть.
   б. Оптическая телеграфная сеть.
   в. Ethernet.
   г. ARPAnet.
2. Какая сетевая технология используется в телефонной сети?
   а. Коммутация пакетов.
   б. Коммутация 2-го уровня
   в. Коммутация 3-го уровня.
   г. Коммутация каналов.
3. Какая технология работает лучше всего при взрывообразном характере передачи данных?
   а. Коммутация пакетов.
   б. Аналоговая передача.
   в. Коммутация каналов
   г. Технология с коммутационными панелями.
4. Какие из приведенных недостатков присущи сетям на основе универсальных вычислительных машин? (Выберите все, что подходит)
   а. Оборудование для мэйнфреймов намного дороже оборудования персональных компьютеров.
   б. Серверы на основе персональных компьютеров могут обрабатывать значительно больший объем данных, чем универсальные машины.
   в. Сбой универсальной машины вызывает крах всей системы.
   г. Терминалы универсальных машин обеспечивают меньший уровень безопасности, чем персональные компьютеры, объединенные в сеть
5. Что из приведенного ниже списка может использоваться компьютерами сети совместно? (Выберите все, что подходит.)
   а. Данные.
   б. Приложения.
   в. Принтеры.
   г. Модемы
6. Какие из этих устройств являются устройствами ввода? (Отметить все подходящие.)
   а. Плоттер.
   б. Факс.
   в. Цифровая камера.
   г. Принтер.
7. Какое из этих имен обозначает разработанный в 1980-х годах метод преобразования имен узлов в адреса IP?
   а. DoD.

б. DHCP.

в. DSL.

г. DNS

8. Как называются технологии, объединяющие телекоммуникационные и вычислительные средства?

а. Мэйнфреймы

б. Телефония.

в. TPI

г. ITC

9. Какой компьютер посылает запросы другому компьютеру для получения доступа к его данным и ресурсам?

а. Сервер.

б. Рабочая станция.

в. Клиентский компьютер.

г. Терминал.

10. Как называется набор правил, которых придерживаются компьютеры в процессе соединения?

а. Протокол.

б. Тип среды.

в. Байт.

г. Топология.

Глава 2

Классификация компьютерных сетей

В зависимости от физических свойств и характеристик программного обеспечения выделяют несколько различных типов сетей. Сети можно классифицировать следующих образом:

- область действия;
- способы администрирования;
- сетевые операционные системы;
- топология;
- архитектура.

В данной главе рассматривается каждый из этих методов классификации.

Классификация сетей по области действия

Классификация компьютерных сетей по области действия учитывает географический район, охваченный сетью, и, в меньшей степени, размер сети. При такой классификации выделяют следующие типы компьютерных сетей:

- локальные (Local Area Network — LAN);
- городские (Metropolitan Area Network — MAN);
- глобальные (Wide Area Network — WAN).

Тип сети в некоторой степени зависит от ее размера, т.е. от количества подключенных компьютеров и пользователей: локальные сети обычно меньше городских, которые, в свою очередь, обычно меньше глобальных. В некоторой степени тип зависит также от финансовых ресурсов: глобальные сети, как правило, стоят дороже и требуют больших затрат на поддержание, чем локальные. Однако наиболее существенным фактором классификации является географическая область, покрываемая сетью.

Локальные сети

В толковом словаре *локальный* означает "местный, но не выходящий за определенные пределы". Аналогично этому термин "локальная сеть" означает сеть, охватывающую ограниченную площадь. Компьютеры, принадлежащие локальной сети, расположены недалеко один от другого. Однако количество компьютеров и пользователей локальной сети может находиться в довольно широких пределах. Например, сеть может состоять из двух рабочих мест с компьютерами, расположенными в нескольких метрах друг от друга, или из сотен компьютеров, разбросанных по этажам небоскреба, а иногда и нескольких расположенных рядом зданий. На рис. 2.1 показано графическое представление простой локальной сети.



Рис. 2.1. Локальная сеть географически ограничена небольшой площадью

Замечание

Количество компьютеров локальной сети может быть ограничено архитектурой сети и типом кабеля. Эти ограничения описываются далее в главе.

Чтобы облегчить управление большими локальными сетями, их иногда разделяют на *рабочие группы*. В этом случае в рабочую группу входят пользователи, имеющие доступ к одним и тем же ресурсам, таким как файлы, принтеры или приложения. Например, локальная сеть некоторой компании может быть разделена на рабочие группы в соответствии с такими ее подразделениями, как финансовый отдел, отдел продаж, отдел кадров и т.д. На рис. 2.2 показана локальная сеть с рабочими группами.

Локальные компьютерные сети могут составить основу более крупных сетей, городских или глобальных, которые образуются путем соединения двух или более локальных сетей.

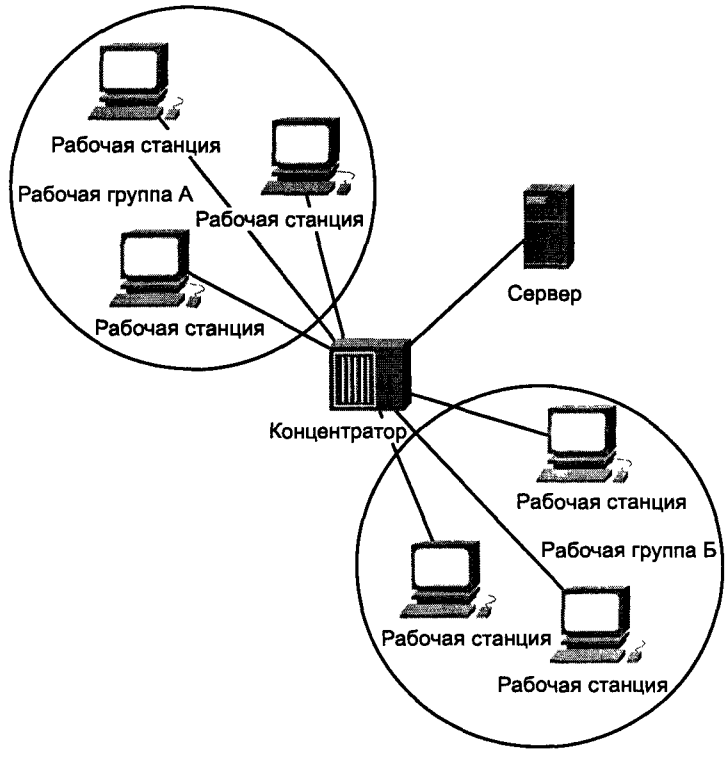


Рис 2 2 Разделение локальной сети на рабочие группы

Городские сети

Городская компьютерная сеть состоит из двух или большего количества локальных сетей, расположенных на площади, приблизительно соответствующей большому городу, откуда и происходит их название Обычно городская сеть представляет собой общедоступную компьютерную сеть с высокими параметрами производительности Городская сеть показана на рис. 2 3

Термин "городская сеть" используется не так часто, как "локальная" и "глобальная", потому что городские сети встречаются значительно реже Большинство сетей ограничены пределами здания или нескольких зданий, следовательно, они попадают в категорию локальных Если же они простираются на большее расстояние, то, скорее всего, их узлы достигают других городов, штатов или стран, переходя таким образом в категорию глобальных сетей Максимальное расстояние между узлами городской сети приблизительно равно 80 километрам.

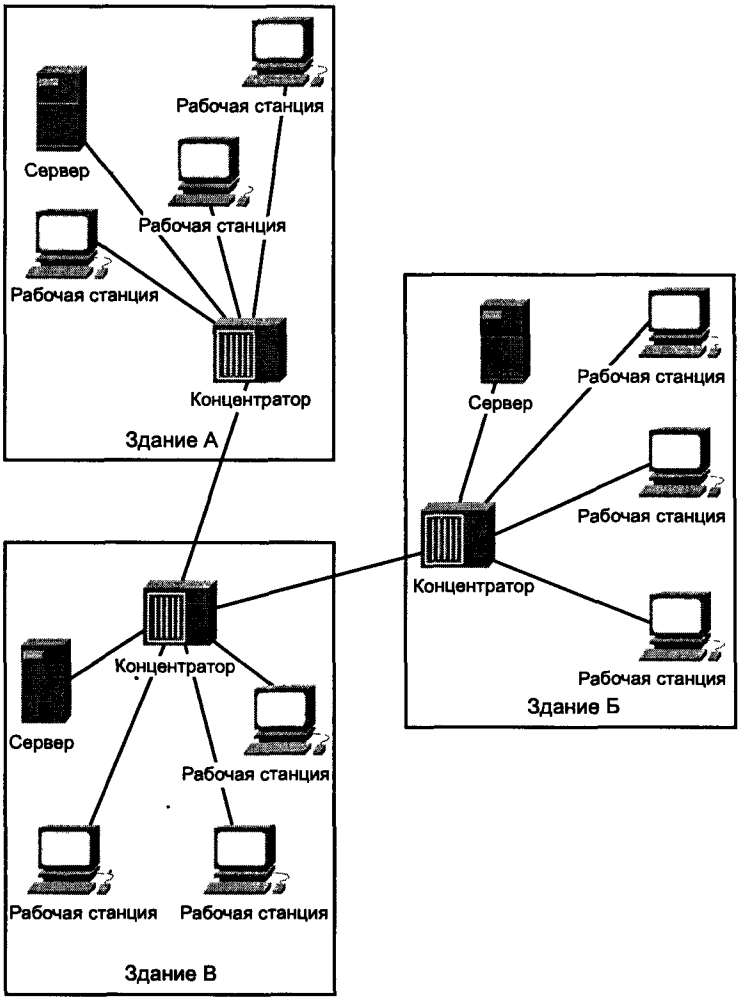


Рис. 2.3. Городская сеть покрывает более широкое пространство, чем локальная, однако, в отличие от глобальной сети, она географически ограничена

Глобальные сети

Глобальными называются компьютерные сети, охватывающие большие географические пространства. Лучшим и наиболее знакомым примером глобальной сети является Internet. Однако существуют и частные глобальные сети. Многие крупные компании с офисами в разных странах имеют корпоративные глобальные сети, соединяющие удаленные офисы посредством телефонных линий, спутниковых и других средств связи. Глобальная сеть всегда состоит из многих соединенных вместе локальных сетей.

Замечание

Несколько сетей, соединенных друг с другом, называют *сетевым комплексом* (*internetwork*, или *internet*). Если слово "internet" написано со строчной буквы, то оно означает сети, соединенные в одну сеть, или сетевой комплекс. Если первая буква прописная, то это слово означает глобальный общедоступный сетевой комплекс, известный всем под именем Internet.

Используются также термины *intranet* (*внутрисетевой*) и *extranet* (*экстрасеть*). Термином "intranet" обозначаются частные локальные сети компаний, использующие протоколы (например, TCP, HTTP и FTP) и технологии Internet. Экстрасетью называется объединение корпоративных сетей различных компаний, взаимодействующих друг с другом посредством Internet

В глобальных сетях для соединения составляющих их частей могут использоваться частные линии, однако чаще всего для этого используются общедоступные средства связи, например система телефонной связи. Поэтому чаще всего скорость передачи данных в глобальных сетях значительно ниже, чем в локальных. Типичная пропускная способность телефонного канала с использованием самого совершенного модема не может превысить 50 Кбит/с. Даже высокоскоростные линии глобальных сетей стандарта T1, кабельные модемы и цифровые абонентские линии DSL могут достичь лишь 1–6 Мбит/с. Между тем в самой медленной локальной сети Ethernet скорость передачи составляет 10 Мбит/с.

Другой характерной особенностью глобальных сетей является то, что их соединения не могут быть постоянными, как в кабельных локальных сетях. Довольно часто, хотя и не всегда, используются коммутируемые связи, т.е. "по вызову". Многие глобальные сети используют выделенные каналы связи, предназначенные исключительно для данной сети, однако в глобальных сетях, в отличие от локальных, значительно чаще используются временные соединения.

Таким образом, в глобальных сетях могут использоваться как частные, так и общедоступные средства связи, как выделенные, так и коммутируемые. Связи глобальных сетей обычно значительно "медлительнее", чем связи локальных сетей.

Глобальные сети подразделяются на распределенные и централизованные. У *распределенных глобальных сетей* (например, Internet) нет центрального пункта управления. С другой стороны, *централизованная глобальная сеть* имеет центральный сервер, или центральный узел (обычно в штаб-квартире компании), к которому подключены остальные сети. На рис. 2.4 показан пример централизованной глобальной сети.

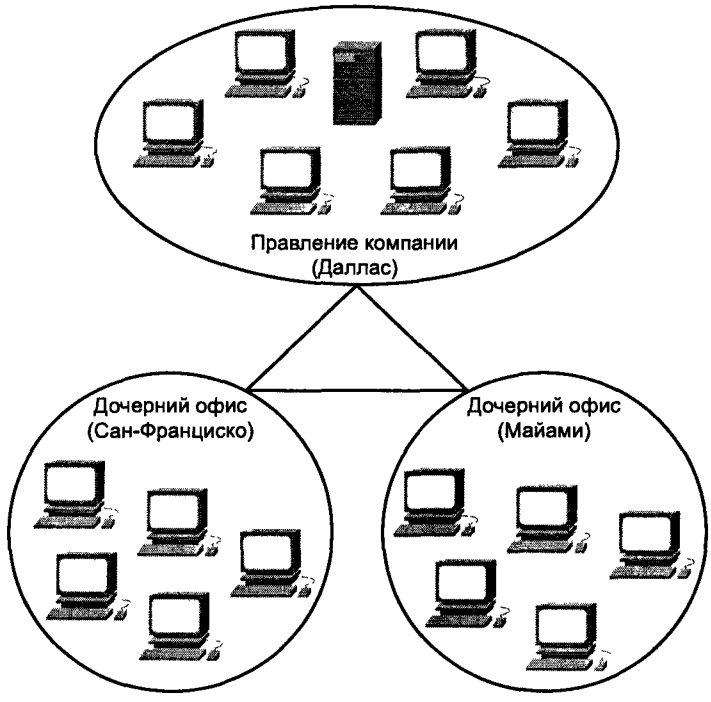


Рис. 2.4. Централизованная глобальная сеть построена вокруг центрального компьютера, или узла, к которому подключены все соединения

Распределенные глобальные сети являются *маршрутизируемыми* сетями. Это значит, что пакеты сообщения, передаваемого из одной локальной сети в другую, должны пройти через шлюзы. *Шлюз* — это маршрутизатор, или компьютер, конфигурированный на выполнение функций маршрутизации. Более подробно маршрутизация описывается в главе 9, "Самая глобальная сеть — Internet".

Классификация сетей по способам администрирования

Компьютерные сети можно классифицировать по способам администрирования, т.е. в зависимости от того, кто и как управляет разделяемыми ресурсами. Компьютерная сеть может быть построена следующим образом:

- как одноранговая рабочая группа, в которой каждый компьютер выполняет функции как сервера, так и клиента, причем каждый пользователь самостоятельно управляет ресурсами своего компьютера;
- как сеть клиент/сервер, в которой функции администрирования сосредоточены на центральном компьютере со специальной сетевой операционной системой; при этом на центральном компьютере выполняется аутентификация пользователей, паролей и другой регистрационной информации для регистрации пользователей и предоставления им доступа к ресурсам.

Выбор оптимального решения зависит от конкретной ситуации. В табл. 2.1 приведены преимущества и недостатки, присущие каждому из этих решений.

Таблица 2.1. Преимущества и недостатки одноранговых сетей и сетей клиент/сервер

Преимущества одноранговой сети	Преимущества сети клиент/сервер
Меньшая стоимость реализации	Обеспечивает большую безопасность
Не требует специальной сетевой операционной системы	Легче управлять большой сетью вследствие централизации функций администрирования
Не нужна должность сетевого администратора	Позволяет создавать резервные копии всех данных в одном центре
Недостатки одноранговой сети	**Недостатки сети клиент/сервер**
Ограниченные возможности наращивания вследствие резкого усложнения задач администрирования	Дорогое программное обеспечение — специальная сетевая операционная система Windows NT/2000 Server или Novell NetWare
Каждый пользователь должен уметь выполнять функции администрирования	Более дорогое и производительное оборудование серверного компьютера
Меньшая безопасность	Нужен профессиональный администратор
Совместное использование ресурсов всеми компьютерами отрицательно влияет на производительность	Опасность краха всей системы при выходе из строя сервера, при этом данные окажутся недоступными для всех пользователей

Таким образом, выбор типа сети зависит от количества компьютеров и пользователей, от требований к безопасности, оборудованию, персоналу и от финансовых ресурсов компании

Серверы и клиенты

Прежде чем приступить к рассмотрению особенностей разных типов сетей, нужно определить термины, обозначающие роли в сети отдельных компьютеров

Сервер — это компьютер, предоставляющий свои ресурсы (данные, программное обеспечение, периферийное оборудование) другим компьютерам сети *Клиент* (*клиентский компьютер*) — это компьютер, получающий доступ к ресурсам сервера

Совет

Это легко запомнить так сервер дает, а клиент получает доступ к ресурсам

Термин "сервер" чаще всего обозначает специально выделенный высокопроизводительный компьютер со специальной серверной операционной системой, централизованно управляющий сетью, однако фактически *каждый* компьютер может предоставлять свои ресурсы, выполняя таким образом функции сервера

Отдельные серверы

Операционные системы, которые обычно считаются клиентскими (Windows 95/98/ME, Windows NT Workstation, Windows 2000 Professional и др), могут выполнять и часто выполняют функции сервера На компьютерах с этими системами могут храниться *разделяемые ресурсы*, предназначенные для использования другими компьютерами

Чтобы ресурсы были доступны для других компьютеров сети, нужно определить их как разделяемые и задать *имена разделяемых ресурсов*, идентифицирующие их в пределах сети Эти имена не обязательно должны совпадать с именами самих ресурсов Например, если в

сети нужно разделять (совместно использовать) каталог `Administration`, ему можно присвоить разделяемое имя `Admin`. На других компьютерах сети, в которых будет использоваться этот каталог, он будет доступен с именем `Admin`. При подключении к этому ресурсу также нужно будет использовать имя `Admin`.

На рис. 2.5 показано диалоговое окно операционной системы Windows 2000, в котором можно создать разделяемый ресурс для каталога `My Documents`.

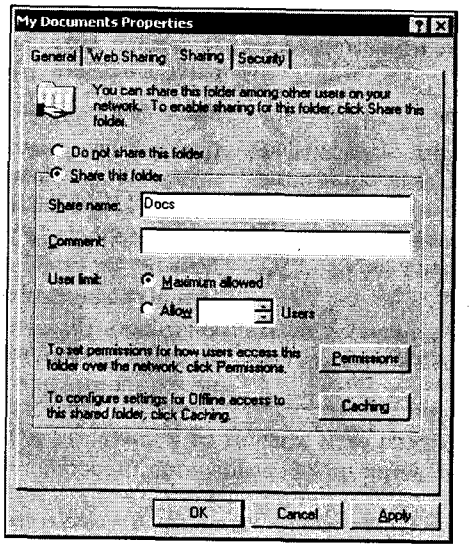


Рис. 2.5. Создание разделяемого ресурса в Windows 2000

Обратите внимание: собственное имя каталога присутствует в заголовке диалогового окна, хотя разделяемое имя определено как `Docs`. Когда к ресурсам сети обращается какой-либо компьютер сети, в его *списке просмотра* (списке доступных разделяемых ресурсов) данный ресурс виден под именем `Docs` (рис. 2.6).

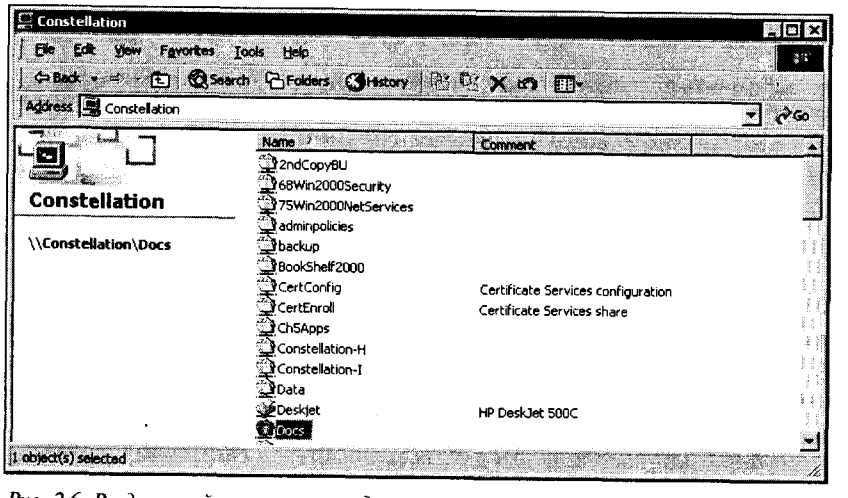


Рис. 2.6. Разделяемый ресурс `Docs` виден в списке просмотра сервера `Constellation`

Замечание

В некоторых сетевых операционных системах разделяемые ресурсы можно "опубликовать" в каталоге. Например, разделяемые каталоги и принтеры в Windows 2000 можно опубликовать в Active Directory, а в Novell NetWare — в дереве NDS. Это позволяет пользователям обращаться к разделяемым ресурсам, не заботясь о том, на каком сервере они расположены физически.

Выделенные серверы

Каждый компьютер, разделяющий свои ресурсы, является сервером. Однако этот термин чаще используется для обозначения именно компьютера, специально *выделенного* для разделяемых файлов, приложений или периферийного оборудования. Обычно *выделенный сервер* представляет собой компьютер с быстродействующим процессором и большим объемом памяти, которые рассчитаны не на выполнение повседневных задач сервера, а для обслуживания клиентских компьютеров. Доступ к серверному компьютеру чаще всего имеют только администраторы сети для выполнения задач управления, мониторинга и поддержки работоспособности сети.

В больших сетях выделенный сервер часто выполняет только одну определенную функцию, как в приведенных ниже случаях.

- Файловым сервером называется сервер, на котором хранятся файлы данных. Пользователи могут хранить данные своих приложений на жестком диске не своего компьютера, а файлового сервера. На сервере файлы легче найти, потому что все они находятся в одном месте, кроме того, легче создавать их резервные копии.
- Серверы печати представляют собой компьютеры, управляющие одним или несколькими принтерами, которые предназначены для распечатки документов, передаваемых пользователями по сети.
- Серверы приложений — это компьютеры, на которых установлены сетевые приложения. Пользователи могут выполнять эти приложения (например, обработку текстов или программы баз данных) посредством сети, несмотря на то что на их компьютерах эти приложения не установлены.
- Регистрационные серверы (в сетях Windows они называются *контроллерами доменов*) предназначены для обеспечения безопасности баз данных. На них содержится информация об учетных записях пользователей. Сервер проверяет права доступа пользователя к базе данных и управляет доступом к сети и ее ресурсам.
- Серверы Web выполняют программное обеспечение Web-серверов (просим извинить за невольную тавтологию) под управлением определенных операционных систем. Например, Microsoft Internet Information Server под управлением Windows NT/2000; Apache под управлением серверов Linux или UNIX; Enterprise Server компании Netscape для различных платформ. Многие операционные системы поставляются с встроенным программным обеспечением Web-сервера. Программное обеспечение Web-серверов часто содержит программы поддержки протоколов FTP (File Transfer Protocol) и NNTP (Network News Transfer Protocol).
- Серверы электронной почты предоставляют "коллекцию" почтовых ящиков, в которые попадают письма, адресованные пользователям сети. Затем эти электронные письма выгружаются на компьютеры пользователей. Примерами

программного обеспечения сервера электронной почты служат программы Microsoft Exchange для сети Windows и Sendmail — распространенный почтовый демон UNIX.

Замечание

В терминологии UNIX *демон* — это программа, которая, работая непрерывно, обрабатывает поступающие запросы.

- Серверы удаленного доступа предоставляют коммутируемое соединение. С их помощью другой компьютер может получить доступ к серверу или к сети по телефонной линии.
- Терминальные серверы предназначены для выполнения клиентских приложений. С их помощью компьютеры тонких клиентов (недорогие малопроизводительные устройства) могут функционировать как терминалы, а не как независимые системы. Серверы этого типа предоставляют пользователям многосеансовую среду и выполняют приложения клиентов.
- Телефонные серверы служат автоответчиками, передают голосовое сообщение и перенаправляют вызовы.
- Кластерные серверы обеспечивают объединение многих серверов в *кластеры*, т.е. в группы независимых компьютерных систем, работающих вместе как одна система. Это делается для решения особенно ответственных задач, когда нужно, чтобы приложения и ресурсы при любых неожиданностях всегда были доступны для клиентов.
- Прокси-серверы служат промежуточными звеньями между рабочими станциями пользователей и Internet. Они повышают безопасность системы и предоставляют средства администрирования и кэширования данных.
- Факс-серверы служат центральной точкой сети, предназначенной для приема и отправки факсов и для распределения поступивших факсов соответствующим пользователям.
- BOOTP-серверы с помощью протокола BOOTP загружают операционные системы клиентских компьютеров, не имеющие жестких дисков, и предоставляют им информацию о конфигурировании сетевого протокола.
- DHCP-серверы (Dynamic Host Configuration Protocol) присваивают IP-адреса и параметры конфигурации TCP/IP компьютерам, конфигурированным как клиенты DHCP. При этом администратору системы не нужно будет вручную присваивать IP-адреса каждому клиентскому компьютеру сети.
- Серверы разрешения имен обслуживают дружественные сетевые имена. Это избавляет пользователей от необходимости помнить числа для идентификации компьютеров. Сервер отображает сетевые имена на IP-адреса, используемые стеком протоколов TCP/IP для локализации компьютера в сети. Сервер разрешения имен содержит также *сервер DNS* (Domain Name System), который отображает иерархическую структуру имен узловых компьютеров на IP-адреса, и *сервер имен NetBIOS* (например, сервер WINS компании Microsoft), отображающий имена NetBIOS на IP-адреса.

Замечание

В главе 8, "Сетевые протоколы и службы", службы разрешения имен и протоколы BOOTP и DHCP рассматриваются более подробно

Клиенты, рабочие станции, хосты и узлы

Как уже упоминалось, клиентами сети являются компьютеры или другие сетевые устройства, имеющие доступ к ресурсам сети Чаще всего клиентом является компьютер Обратите внимание принтер или другое сетевое устройство, получающее доступ к ресурсам, технически тоже может быть клиентом

Термин *клиент* может также обозначать программы, имеющие доступ к программам сервера Например, программа поддержки электронной почты, выполняющаяся на настольном компьютере и передающая запросы для загрузки поступивших сообщений с сервера, называется *клиентом электронной почты*

Клиентская операционная система обычно устанавливается на настольных компьютерах, или *рабочих станциях*, которые либо подключены к сети как одноранговые компьютеры рабочей группы, либо зарегистрированы на сервере аутентификации Примерами клиентских операционных систем могут служить Windows 95/98/ME, Windows NT Workstation и Windows 2000 Professional

Термин *рабочая станция* имеет много значений Им обозначается клиентская операционная система NT/2000 или любой настольный компьютер, на котором установлена любая клиентская операционная система Другое значение термина *рабочая станция* — высокопроизводительный компьютер, на котором выполняются приложения, интенсивно загружающие ресурсы Такой компьютер обычно служит графической рабочей станцией, или рабочей станцией системы автоматизированного проектирования

Еще один термин, обозначающий компьютеры сети, — *основной компьютер*, или *хост* Этот термин часто используется в сетях на основе протоколов TCP/IP, где он может обозначать любое сетевое устройство, которому присвоен IP-адрес

Узел — это точка соединения в сети Часто этим термином обозначается любой компьютер или другое сетевое устройство В общем случае узел представляет собой точку перераспределения, или устройство, запрограммированное или спроектированное для распознавания и обработки запросов на передачу информации другим узлам

Одноранговые сети

Одноранговая структура хорошо подходит для небольших сетей, у которых требования к безопасности не очень высоки В большинстве книг по сетевым технологиям рекомендуется включать в одноранговую сеть не более 10 компьютеров

Стоимость небольшой одноранговой сети невелика Ее несложно реализовать на основе таких операционных систем, как Windows 95/98/ME, Windows NT Workstation, Windows 2000 Professional и различных версий Linux (все они имеют встроенные сетевые компоненты)

Если нужно подключить к одноранговой сети компьютер с установленными Windows 9*x*, Windows NT или Windows 2000, то его следует конфигурировать на соединение с *рабочей группой* в диалоговом окне свойств сетевой конфигурации В этом окне всем компьютерам, разделяющим с другими свои ресурсы, должно быть присвоено одно и то же имя рабочей группы

Администрирование одноранговых сетей

В одноранговых сетях администрирование пользователей и ресурсов *децентрализовано*. Каждый компьютер сети может быть как клиентом, так и сервером. Другими словами, каждый компьютер сети может предоставлять свои ресурсы другим компьютерам и получать доступ к ресурсам других.

Пользователь каждого компьютера полностью отвечает за управление доступом к своим ресурсам: он создает учетные записи пользователей, создает разделяемые ресурсы и присваивает права доступа к этим ресурсам. Каждый пользователь отвечает также за резервное копирование данных на своем компьютере. К сожалению, если одноранговая сеть содержит несколько компьютеров, то найти в ней нужные ресурсы довольно трудно.

Безопасность в одноранговых сетях

В одноранговых сетях нет центральной базы данных, в которой хранилась бы регистрационная информация пользователей. Все средства обеспечения безопасности в этих сетях локальны. Учетные записи и пароли пользователей создаются и поддерживаются на каждом компьютере. Это довольно неудобно, к тому же менее безопасно, чем в централизованной модели безопасности, используемой в сетях клиент/сервер.

Допустим, рабочая группа состоит из четырех компьютеров с операционными системами Windows NT Workstation, принадлежащих Мэри, Джо, Джону и Джейн. Чтобы Мэри получила доступ к файлам, хранящимся на компьютере Джо, он должен создать для нее учетную запись на своем компьютере. Если Мэри хочет получить доступ к разделяемому принтеру, установленному на компьютере Джейн, то Джейн должна создать учетную запись пользователя для Мэри и т.д.

Если Джо, Джейн и Джон присвоят этим учетным записям разные имена пользователей и пароли, то Мэри вынуждена будет помнить, что для доступа к ресурсам Джо, например, нужно использовать имя *maryjohnson* и пароль *tree*, для доступа к ресурсам Джейн — имя *maryj* и пароль *Shelton*, для доступа к ресурсам Джона — имя *mjohnson* и пароль *flute*. Можете себе представить, как это выглядит, если в сети больше 10 компьютеров!

Безопасность на уровне ресурсов и на уровне пользователей

В рабочих группах Windows for Workgroups и Windows 95/98 средства безопасности реализованы не на уровне пользователей, а на уровне ресурсов. В табл. 2.2 приведены основные отличия между этими уровнями безопасности.

Таблица 2.2. Обеспечение безопасности на уровне ресурсов и на уровне пользователей

Безопасность на уровне ресурсов	Безопасность на уровне пользователей
Используется в Windows for Workgroups 3.11 и Windows 95/98	Используется в Windows NT и Windows 2000
Пароль присваивается каждому разделяемому ресурсу	Пароль присваивается каждому пользователю
Для получения доступа к ресурсу пользователь должен ввести пароль этого ресурса	Для получения доступа к ресурсу учетная запись пользователя должна иметь право доступа к этому ресурсу
Пользователь должен помнить много паролей	Пользователь должен помнить только один пароль

Вернемся к примеру небольшой рабочей группы. Если на компьютерах Мэри, Джо, Джейн и Джона установлена Windows 95, то им не нужно создавать учетные записи пользователей для каждого, кто будет получать доступ к их ресурсам. Все, что им нужно сделать, — это присвоить пароль каждому своему разделяемому ресурсу. Если Мэри хочет, чтобы к папке *Documents* имела доступ Джейн, но не Джон или кто-либо еще, то она должна присвоить этой папке пароль (например, *health*) и сообщить его только Джейн. При попытке обратиться к папке *Documents* система спросит пароль, который знает только Джейн.

Если Мэри хочет, чтобы к другой ее папке *Pix* имели доступ Джон и Джейн, но не Джо, то она должна присвоить этой папке другой пароль (например, *crate*) и сообщить его только Джону и Джейн.

Допустим, на диске Мэри расположены 20 совместно используемых папок. В этом случае ей придется помнить 20 разных паролей. Другим пользователям тоже придется помнить немалое количество паролей, причем нужно будет постоянно следить за соответствием паролей и папок. Если же количество компьютеров такой сети превысит 10, то работать в ней будет невозможно. Система безопасности на уровне ресурсов показана на рис. 2.7.

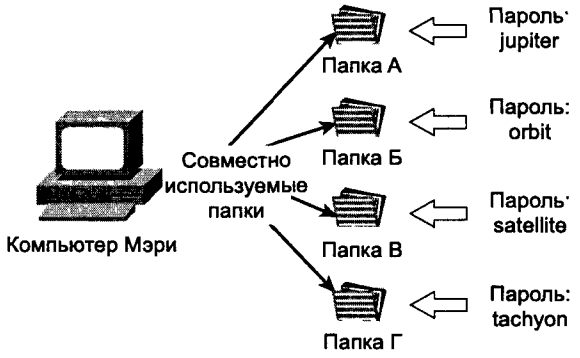


Рис 2 7 В системе безопасности на уровне ресурсов количество паролей, которые нужно помнить, быстро растет

Поскольку при увеличении размеров сети такая ситуация быстро становится невыносимой, большинство пользователей рабочих групп Windows 9*x* прибегают к простейшему решению — вообще не присваивают ресурсам пароли. Естественно, для сети с дорогими или конфиденциальными данными, доступ к которым должен быть ограничен, такое решение неприемлемо. В этом случае следует использовать сеть клиент/сервер, рассматриваемую в следующем разделе.

Сети клиент/сервер

Наиболее характерной особенностью сети клиент/сервер является *централизованное управление* сетью. В такой сети как минимум на одном компьютере (называемом сервером) установлена сетевая операционная система, например Windows NT, Windows 2000 Server или NetWare. На сервере создаются учетные записи пользователей, и администратор сети может управлять ею из одного центра.

В сетях клиент/сервер решается также проблема снижения производительности, которое происходит в компьютерах рабочей группы, когда другие пользователи загружают системные ресурсы компьютера одного из пользователей. Производительность и пропускная способность сетей клиент/сервер в общем случае лучше, чем одноранговых.

Операционная система сервера часто предоставляет дополнительные услуги. Например, сервер Windows NT/2000 может функционировать как сервер удаленного доступа (коммутируемый доступ), к которому можно по телефонной линии подключить много пользователей. Обратите внимание: Windows 9*x* и Windows NT Workstation допускают только одно входящее соединение в один момент времени.

Администрирование сети клиент/сервер

Модель сети клиент/сервер значительно упрощает задачи администрирования, особенно в сетях с большим количеством компьютеров и разделяемых ресурсов. В этой модели разделяемые файлы хранятся на сервере, поэтому задачи их поиска и резервного копирования существенно упрощаются.

Одна из важных особенностей сетей клиент/сервер (которая может оказаться как обузой, так и облегчением) — это необходимость в специально подготовленном сетевом администраторе. Это, конечно, увеличивает стоимость поддержания сети, однако в конечном счете вследствие квалифицированного управления сетью накладные расходы все же окажутся меньше.

Управление безопасностью в сети клиент/сервер

Сети клиент/сервер обладают большей безопасностью, чем одноранговые. Чтобы зарегистрироваться в сети, пользователь должен знать учетную запись и пароль, созданные на сервере. Когда пользователь успешно зарегистрировался, он получает доступ ко всем ресурсам, на которые у него есть право. При этом от него не требуется помнить многочисленные имена и пароли для разных компьютеров, как в рабочей группе Windows NT Workstation и Windows 2000 Professional. Не нужно также помнить пароли разделяемых ресурсов на разных компьютерах, как в рабочей группе Windows 9*x*. Сеть клиент/сервер предоставляет пользователю доступ к ресурсам на основе *аутентификации пользователя* и *прав доступа*.

Сетевой администратор может присвоить право доступа к определенному ресурсу как отдельному пользователю, так и группе. Права доступа могут предоставлять различные уровни доступа для разных пользователей. Допустим, на сервере хранится разделяемый каталог *Sales*. Нужно, чтобы Мэри (секретарь отдела продаж) могла читать в этом каталоге документы, но не могла вносить в них изменения. Нужно также, чтобы Джейн (начальник отдела продаж) могла читать, изменять, удалять и вообще полностью контролировать содержимое каталога *Sales*. В сети Windows 2000 это можно сделать, отредактировав свойства разделяемых ресурсов: нужно присвоить учетной записи Мэри право доступа на чтение и учетной записи Джейн — право неограниченного доступа.

Замечание

Присваивать права доступа учетным записям каждого пользователя может оказаться довольно хлопотным занятием, особенно если их много и время от времени их нужно изменять. Эту задачу можно упростить, организовав учетные записи пользователей в *группы*. Тогда права доступа можно присваивать сразу всей группе Группы рассматриваются более подробно в главе 10, "Сетевые операционные системы".

Если права доступа к каталогу *Sales* присвоены Мэри и Джейн (или группам к которым они принадлежат), то необходимо сначала удалить права доступа к ресурсам, установленные по умолчанию (рис 2 8)

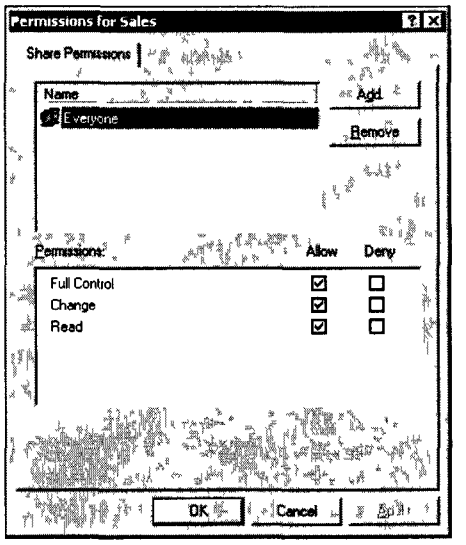


Рис 2 8 В сетях Windows неограниченный доступ (право Full Control) по умолчанию предоставлен всем (группа Everyone)

Как видно из рис 2 8, при создании нового разделяемого ресурса группе Everyone (Все) автоматически присваивается неограниченный доступ (право Full Control) В эту группу включены все пользователи, имеющие действительную учетную запись для регистрации в сети Описанное право доступа несложно удалить, ограничив доступ к ресурсу только теми пользователями, которым этот ресурс нужен

Замечание

Это объяснение несколько упрощено, оно предназначено только для иллюстрации отличий *прав доступа к разделяемым ресурсам* в сетях клиент/сервер и одноранговых сетях В системе Windows 2000 можно реализовать несколько разных уровней безопасности, в зависимости от используемых протоколов и файловой системы Права доступа, присвоенные разделяемому ресурсу, — это только один замок на дверях к этому ресурсу

Классификация сетей по сетевым операционным системам

Иногда сети классифицируют по установленным на серверах сетевым операционным системам, которые используются для управления сетью Приведем примеры типов сетей, выделенных по этому признаку

- Windows (Windows NT и Windows 2000),

- NetWare;
- UNIX.

Во многих сетях на серверах установлены разные сетевые операционные системы. Они называются *смешанными сетями.*

Сети Windows

Сети клиент/сервер на основе Windows называются *доменами.* В домене Windows NT 4.0 главный компьютер, называемый *первичным контроллером домена*, содержит только копию (с правом чтения и записи) базы данных учетных записей (Security Accounts Manager — SAM). После выхода в свет Windows 2000 компания Microsoft рекомендует называть домены NT 4.0 *доменами нижнего уровня.*

Домены Windows 2000 реализованы на базе активного каталога (Active Directory), копии которого, содержащие регистрационную информацию и объекты представления сетевых ресурсов, хранятся на всех контроллерах доменов. В сети может быть много контроллеров доменов, все они имеют право доступа к основной базе данных как для чтения, так и для записи.

Системы Windows 2000 Professional, Windows NT Workstation, Windows 95/98, Windows for Workgroups и MS DOS могут быть клиентами серверов Windows NT или Windows 2000. Операционные системы, не принадлежащие Microsoft, например Macintosh или Linux, после установки дополнительного программного обеспечения тоже могут получать доступ к ресурсам серверов Windows

Замечание

Все распространенные сетевые операционные системы подробно рассматриваются в главе 10, "Сетевые операционные системы".

Сети NetWare

Довольно распространенная сетевая операционная система NetWare компании Novell предоставляет регистрационную систему безопасности и поддерживает функции хранения файлов и печати. При установке соответствующего программного обеспечения клиентские операционные системы Windows тоже могут получать доступ к серверам NetWare. Компания Novell также поставляет добавляемую клиентскую программу Client32, которую можно установить в 32-разрядных операционных системах Windows для расширения их функциональных возможностей.

Версии NetWare 4.*x* и 5.*x* содержат службы каталогов, использующие иерархическую базу данных NDS (NetWare Directory Services), аналогичную системе Active Directory компании Microsoft. (Справедливости ради, следует отметить, что NDS появилась раньше, чем Active Directory.) Более ранние версии NetWare (3.*x* и раньше), все еще установленные во многих сетях, для организации сетевых объектов используют базу данных *Bindery.*

Сети UNIX

В свое время на большинстве узловых компьютеров сети ARPAnet (предшественницы Internet) была установлена сетевая операционная система UNIX. Она была разработана компанией Bell в 1969 году и завоевала большую популярность благодаря свободному и

бесплатному распространению. Это весьма мощная сетевая операционная система, однако большинство реализаций UNIX основаны на текстовом вводе-выводе, поэтому неудобны и довольно сложны для изучения

Система Linux представляет собой "вариацию на тему" UNIX. В последнее время Linux становится все более распространенной в качестве как сервера, так и настольной операционной системы Как и ее старшая сестра UNIX, она основана на открытом стандарте, поэтому многие компании поставляют на рынок собственные версии. Распространенные версии Linux — RedHat, Caldera и Corel.

Смешанные сети

В настоящее время большинство сетей, служащих промежуточным звеном для связи с большими сетями, можно рассматривать как смешанные. Они реализованы на основе программного обеспечения различных поставщиков, используют разные протоколы и могут даже объединять принципы построения доменов и рабочих групп.

Сеть Microsoft, в которой клиенты регистрируются на контроллере домена Windows NT, может иметь файловый сервер NetWare, к которому эти же клиенты получают доступ. В этой же сети компьютер с UNIX может выполнять функции Web-сервера Персональный компьютер можно даже подключить к мэйнфрейму IBM AS/400 для доступа к его приложениям

Большинство поставщиков предоставляют специальные инструменты для взаимодействия с разными системами Для облегчения интеграции в другую среду эти инструменты могут быть или добавляемыми, или встроенными в операционную систему Например, операционные системы Windows NT и Windows 2000 Server компании Microsoft содержат службы доступа к сетям NetWare и Macintosh.

Ниже приведены некоторые популярные средства взаимодействия.

- **Client Services for NetWare (CSNW) и Gateway Services for NetWare (GSNW).** Средство CSNW позволяет компьютеру-клиенту Microsoft получить непосредственный доступ к серверам NetWare. Средство GSNW позволяет клиентам сервера Microsoft получить доступ к ресурсам сервера NetWare посредством программного шлюза, установленного на сервере Windows NT или Windows 2000.
- **Файловые службы и службы печати для NetWare** Позволяют компьютерам NetWare получить доступ к файлам и принтерам сети Microsoft.
- **Файловые службы и службы печати для Macintosh.** Позволяют компьютерам Macintosh получить доступ к файлам и принтерам сети Microsoft
- **Systems Network Architecture (SNA)** Позволяет подключить сеть персональных компьютеров к мэйнфрейму IBM.
- **SAMBA** Набор утилит, с помощью которых компьютер Microsoft может получить доступ к файловым службам и службам печати серверов UNIX.

Эти средства взаимодействия подробно рассматриваются в главе 13, "Гибридные сети".

Классификация сетей по протоколам

Иногда компьютерные сети классифицируют на основе используемых ими протоколов. Сетевой протокол — это набор правил, которых придерживаются связанные компьютеры при установке и поддержании связи посредством сети В следующих раз-

делах рассматриваются три наиболее распространенных протокола локальных сетей — NetBEUI, IPX/SPX и TCP/IP, а также два менее распространенных набора протоколов — AppleTalk и OSI.

Сети NetBEUI

Протокол NetBEUI (NetBIOS Extended User Interface) обычно используется в небольших простых локальных сетях на базе операционных систем Microsoft. Протокол NetBEUI основан на протоколах NetBIOS (Network Basic Input/Output System), разработанных компанией IBM для использования в рабочих группах. Обратите внимание: сеть NetBEUI не может быть маршрутизирована. Это значит, что если сеть разделена на подсети, то для коммуникации с компьютерами другой подсети нужно использовать другой локальный сетевой протокол.

Разделение сети на подсети подробно рассматривается в главе 8, "Сетевые протоколы и службы".

Преимуществами сетей NetBEUI являются простота, высокое быстродействие и низкие накладные расходы.

Сети IPX/SPX

Стек протоколов IPX/SPX (Internet Package Exchange/Sequenced Packet Exchange) используется в качестве протокола локальных сетей Novell. Для сетей NetWare до версии 5.0 этот протокол является обязательным.

Замечание

Версия NetWare 5.0 — первая версия NetWare, поддерживающая "чистый" протокол IP стека протоколов TCP/IP и не требующая IPX/SPX.

Протокол IPX/SPX обычно используется в сетях NetWare, однако он может использоваться и в других сетях. Рабочая группа или домен компьютеров Microsoft тоже могут использовать протокол IPX/SPX. Компания Microsoft включила в операционные системы Windows 9*x*, Windows NT/2000 собственную реализацию IPX/SPX-совместимых протоколов под названием NWLink. Для подключения клиента Microsoft к серверу NetWare с операционной системой NetWare 4.0 и ниже на этом клиенте должен быть установлен протокол NWLink или IPX/SPX.

Конфигурирование протокола IPX/SPX не очень сложное (сложнее, чем NetBEUI, но проще, чем TCP/IP), его быстродействие выше, чем у TCP/IP. Протокол IPX/SPX иногда используется во внутренних сетях Microsoft, подключенных к Internet в целях повышения безопасности. Более подробно этот вопрос рассматривается в главе 13, "Гибридные сети".

Сети TCP/IP

Из всех распространенных протоколов локальных сетей протоколу TCP/IP присущи наименьшее быстродействие и наибольшая сложность конфигурирования. Несмотря на это, он все же получил широкое распространение. Это объясняется следующими причинами.

- В протоколе TCP/IP используется гибкая схема адресации, исключительно удачная для маршрутизации даже в самых больших сетях.
- Протокол TCP/IP поддерживается практически во всех операционных системах и на всех платформах.
- К настоящему времени разработано и применяется огромное количество инструментов и утилит для мониторинга и управления комплектом протоколов TCP/IP.
- Протокол TCP/IP де-факто является протоколом глобальной сети Internet. В любой системе, подключаемой к Internet, должен быть реализован протокол TCP/IP.

Другие протоколы локальных сетей

В подавляющем большинстве локальных сетей используется один из трех описанных протоколов. Однако в некоторых сетях применяются менее распространенные протоколы, которые описывается далее в разделе.

Протокол AppleTalk

Представляет собой набор протоколов, разработанных компанией Apple для объединения в сеть компьютеров Macintosh. Пакет протоколов AppleTalk включает три протокола.

- **LocalTalk**. Используется для объединения компьютеров Macintosh в небольшие рабочие группы. Его быстродействие относительно невелико (230,4 Кбит/с), и он поддерживает не более 32 устройств.
- **EtherTalk**. Используется для подключения рабочих групп Macintosh к сетям Ethernet.
- **TokenTalk**. Используется для подключения рабочих групп Macintosh к сетям Token Ring.

В сетях AppleTalk для отображения адресов AppleTalk на адреса Ethernet и на физические адреса MAC (Media Access Control) сетей Token Ring используется протокол AARP (AppleTalk Address Resolution Protocol).

Пакет протоколов OSI

Пакет протоколов OSI (Open System Interconnection) был разработан с целью замены TCP/IP. Международная организация стандартизации ISO (International Organization for Standardization), разработавшая этот протокол, намеревалась устранить путаницу и облегчить стандартизацию сетевых продуктов многочисленных поставщиков.

Замечание

Название организации ISO — это не сокращение полного названия. Оно произведено от древнегреческого слова *isos*, означающего "равенство".

Намерение заменить TCP/IP пакетом OSI хорошо выглядело в теории, однако TCP/IP оказался намного более стойким, чем ожидалось. В свое время правительство США поспешило форсировать процесс замены. В 1980 году Министерство обороны США объявило, что к августу 1990 года все его сети будут использовать протокол OSI. Однако этого не случилось. Сети не были изменены, и TCP/IP продолжает властвовать как король Internet. Позиции TCP/IP по-прежнему неуязвимы. Развиваясь, он оказался способным удовлетворить все требования бурного роста, что демонстрирует планируемый переход на IPv6.

Классификация сетей по топологии

Сети можно классифицировать также по их физической или логической *топологии*. *Физическая топология* означает форму сети, т.е. путь прокладки кабеля. *Логическая топология* означает путь, по которому сигналы проходят из одной точки сети в другую.

Физическая и логическая топологии могут совпадать. Например, в сети, физически реализованной в виде шины, данные проходят от одного компьютера к следующему "по прямой линии". Однако физическая и логическая топологии могут и не совпадать. Например, в звездообразной топологии все компьютеры соединены кабелями с одним концентратором, образуя звезду, однако внутри концентратора соединения могут быть построены так, что сигнал проходит по кругу от одного порта к другому, образуя логическое кольцо.

Перечислим наиболее распространенные топологии локальных сетей:

- шинная;
- кольцевая;
- звездообразная;
- ячеистая;
- смешанная.

Эти топологии подробно рассматриваются в следующих разделах.

Сети с шинной топологией

Шина представляет собой сеть, проложенную по линии. Кабель проходит от одного компьютера к следующему, затем к следующему и т.д. Шинная топология показана на рис. 2.9.

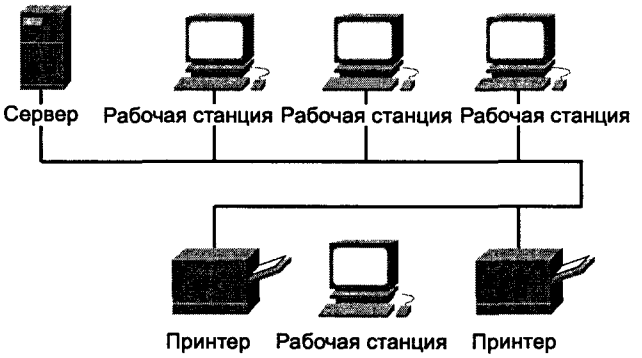


Рис. 2.9. Компьютеры в сети с шинной топологией соединены линейно: каждый компьютер соединен с предыдущим и следующим

Поскольку у каждой линии есть начало и конец, на каждом конце шины должен быть *терминатор* (оконечное устройство, оконечная нагрузка шины). Если оба конца кабеля не подключены к терминаторам, то происходит *отражение сигнала*, нарушающее нормальную работу сети. Один из концов шины (но не оба) обязательно должен быть заземлен.

Замечание

Для завершения шины терминатор подключается к "пустой" стороне Т-образного разъема сетевого адаптера в первом и последнем компьютерах.

В сетях с шинной топологией может использоваться как толстый, так и тонкий коаксиальный кабель. Обычно в таких сетях используется архитектура 10Base2 или 10Base5. Параметры различных кабелей подробно рассматриваются в главе 7, "Физические компоненты сетей".

Принцип действия сети с шинной топологией

В сети с шинной топологией сообщения, посылаемые каждым компьютером, поступают на все компьютеры, подключенные к шине. Каждый сетевой адаптер анализирует заголовки сообщений и таким образом определяет, предназначено ли сообщение для этого компьютера. Если да, то сообщение обрабатывается, в противном случае отбрасывается.

Преимущества сети с шинной топологией

Шинную топологию очень просто реализовать. Она относительно дешевая, потому что требует меньше кабелей, чем другие топологии. Это решение особенно пригодно для небольших сетей, которые будут использоваться всего несколько дней или недель, например в классной комнате.

Недостатки сети с шинной топологией

Шинная топология называется *пассивной*, поскольку компьютеры не регенерируют сигналы, а просто передают их дальше. Поэтому сигналы в такой сети подвержены *затуханию*, т.е. интенсивность сигнала с расстоянием уменьшается. Эту проблему можно решить с помощью *повторителей*, рассматриваемых в главе 7, "Физические компоненты сетей"

Другой недостаток шинной топологии состоит в том, что если происходит разрыв кабеля (или один из пользователей вынимает разъем из гнезда, чтобы отключиться от сети), то вся сеть разрывается. При этом происходит не только разрыв связи между двумя группами изолированных компьютеров, но и возникает отражение сигнала из-за отсутствия терминаторов на концах, вследствие чего вся сеть выходит из строя.

Сети с кольцевой топологией

Если соединить последний в магистрали компьютер с первым, то получится *кольцевая* топология. В кольце каждый компьютер соединен с двумя другими и сигнал может проходить по кругу (рис. 2.10). Поскольку кольцо не имеет конца, терминаторы не нужны (и даже невозможны).

Физически в кольцевой сети, как и в шинной, используется коаксиальный кабель. В сети Token Ring, представляющей собой логическое кольцо, согласно спецификациям IEEE 802.5 используется кабель STP (типа IBM).

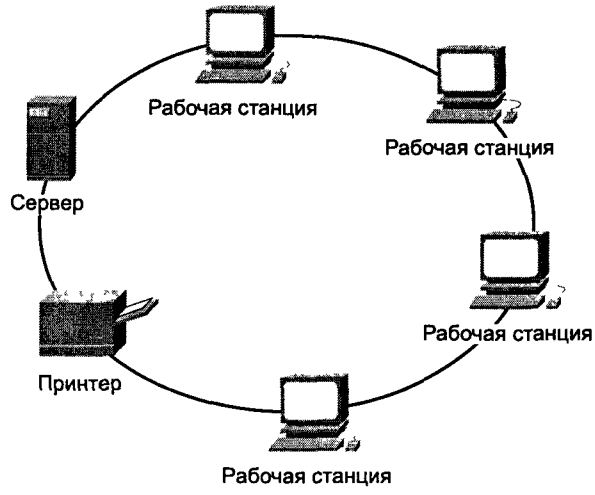


Рис 2 10 В кольцеобразной сети компьютеры соединены по кругу, при этом последний компьютер соединен с первым

Принцип действия кольцевой сети

В кольцевой сети сигнал проходит в одном направлении. Каждый компьютер принимает сигнал от *верхнего по течению соседа* и посылает сигнал *соседу, нижнему по течению*. Кольцевая топология называется *активной*, потому что каждый компьютер, прежде чем передать сигнал дальше, регенерирует его.

Чаще всего кольцевая топология используется в архитектуре Token Ring. В этой архитектуре кольцо всегда является *логическим* кольцом, круг реализуется в концентраторе Token Ring, который называется MSAU (Multistation Access Unit).

Преимущества кольцевой сети

В кольце сравнительно легко устранять неполадки. Как и шину, кольцо просто реализовать. Для установки кольца требуется больше кабеля, чем для шины, и меньше, чем в звездообразной топологии.

Недостатки кольцевой сети

Кольцевой топологии присущи некоторые недостатки шинной топологии. Если круг не разрывается, то это надежная топология. Однако если где-либо происходит разрыв или разъединение, то вся сеть выходит из строя.

Другой недостаток кольца состоит в том, что в сеть трудно добавить новый компьютер. Поскольку кабель проходит по кругу, для добавления нового компьютера кольцо нужно разорвать, при этом сеть становится неработоспособной.

Звездообразные сети

Звезда — одна из наиболее распространенных топологий локальных сетей. Звезда образуется путем соединения каждого компьютера с центральным концентратором (рис. 2.11).

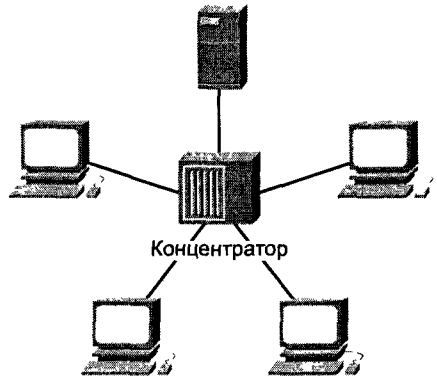


Рис. 2 11 В звездообразной топологии все компьютеры соединены с центральным концентратором

Концентратор может быть *активным*, *пассивным* или *интеллектуальным* Пассивный концентратор представляет собой всего лишь точку соединения. Он не потребляет электрическую энергию. Активный концентратор (наиболее распространенный) фактически является *повторителем* со многими портами. Прежде чем передать сигнал другому компьютеру, активный концентратор усиливает его. Интеллектуальный концентратор представляет собой активный концентратор с возможностями диагностики. Для этого в нем есть специальная встроенная микросхема. Концентраторы подробно рассматриваются в главе 7, "Физические компоненты сетей".

При звездообразной топологии обычно используются неэкранированные витые пары и архитектура Ethernet 10BaseT или 100BaseT.

Принцип действия звездообразных сетей

В типичной звездообразной сети сигнал передается от сетевого адаптера, установленного в компьютере, к концентратору. Здесь сигнал усиливается и передается обратно на все порты. В звезде, как и в шине, сообщение получают все компьютеры. Получив сообщение, компьютер анализирует его заголовок и принимает решение: обработать или отбросить сообщение.

Преимущества звездообразных сетей

По сравнению с шинной и кольцевой звездообразная топология имеет два больших преимущества. Во-первых, она значительно устойчивее к сбоям. Другими словами, если один из компьютеров отключается или разрывается кабель, то это влияет только на него, в остальной сети продолжается нормальный процесс коммуникации. Во-вторых, легко изменить конфигурацию сети. Добавление в сеть нового компьютера или удаление компьютера из сети состоит всего лишь в подсоединении или отсоединении разъема кабеля. В звездообразной сети легко устраняются неполадки на уровне оборудования, особенно если используется интеллектуальный концентратор, предоставляющий диагностическую информацию. Физические и другие уровни, определяемые стандартными моделями сети, рассматриваются в главе 3, "Концепции, модели и стандарты компьютерных сетей".

Недостатки звездообразных сетей

Недостатки звездообразной топологии связаны главным образом с финансовыми затратами. Для звездообразной сети нужно больше кабелей, чем для шинной или кольца, потому что отдельный кабель проходит от каждого компьютера к концентратору, который может находиться далеко. Кроме кабелей приходится покупать довольно дорогой концентратор. К счастью, используемые в звезде витые пары стоят недорого, к тому же отпадает необходимость в терминаторах.

Ячеистая топология

Эта топология распространена не так широко, как три предыдущие. При ячеистой топологии каждый компьютер соединен непосредственно с каждым другим компьютером сети (рис. 2.12).

Благодаря избыточным соединениям ячеистая топология более устойчива к сбоям. Если один путь прохождения сигнала выходит из строя, сигнал может пройти по другому пути.

К сожалению, это преимущество нивелируется высокой стоимостью кабелей, которых нужно огромное количество, и сложностью сети, если в ее состав входит много компьютеров. При добавлении каждого нового компьютера количество соединений растет экспоненциально. Видимо, недаром в английском языке термин "ячейка" (mesh) звучит как "путаница" (mess) — это именно то, что получается при наращивании сети.

Смешанные топологии

В сетевой терминологии слово *смешанный* может иметь два разных значения. В главе 13, "Гибридные сети", термин *смешанные сети* означает сети на основе разных протоколов, операционных систем или платформ. В данной главе слово *смешанный* обозначает топологию, объединяющую элементы двух или более стандартных топологий (например, ячеистой и звезды).

Смешанные ячеистые сети

Поскольку ячеистая топология с ростом сети быстро становится слишком сложной и неуправляемой, во многих сетях используется *полуячеистая* топология, в которой соединения установлены не между всеми компьютерами. Такую сеть иногда называют *смешанной ячеистой*. Избыточные соединения устанавливаются только между наиболее ответственными компьютерами. Пример смешанной ячеистой сети приведен на рис. 2.13.

Смешанная ячеистая топология имеет большинство преимуществ чистой ячеистой топологии при меньшей стоимости. При этом реализовать ее и управлять ею значительно легче.

Комбинированные топологии

Смешанными могут называться не только топологии, но и сети, использующие несколько топологий. Такие сети распространены довольно широко. Смешанная сеть получается если, например, соединить несколько концентраторов с помощью шины и подключить к каждому концентратору несколько компьютеров (рис. 2.14). Специально для этого во многих концентраторах предусмотрены разъемы BNC для тонких коаксиальных кабелей и несколько портов RJ-45 для витых пар.

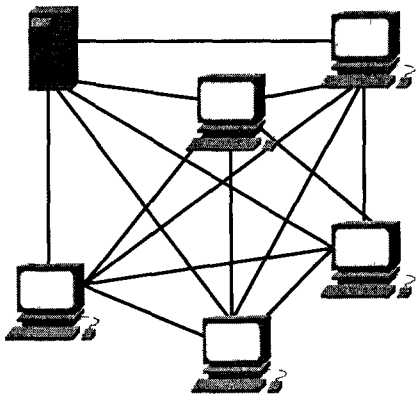


Рис 2 12 В ячеистой сети каждый компьютер соединен с каждым другим компьютером

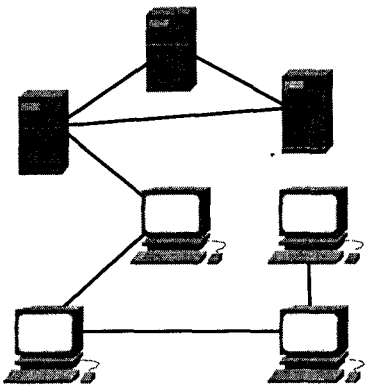


Рис 2 13 В смешанной ячеистой сети соединения устанавливаются только между некоторыми компьютерами

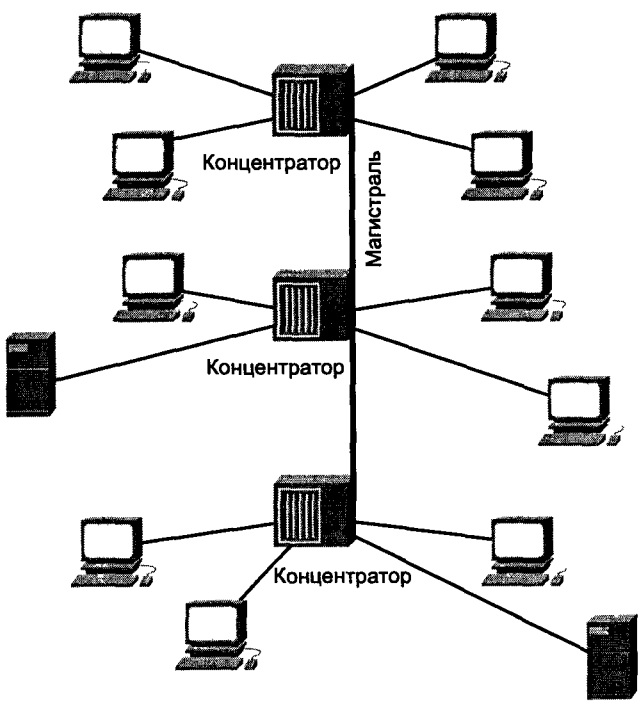


Рис 2 14 Коаксиальный кабель, соединяющий концентраторы, называется магистралью сети

При такой топологии (см рис 2 14) коаксиальный кабель, соединяющий концентраторы, называется *магистральным* или *магистралью* В этом случае магистраль является компонентом сети, объединяющим ее части, называемые *сегментами* Путем подключения к магистрали новых сегментов можно создать довольно большую сеть

Классификация сетей по архитектуре

Еще один способ классификации сетей — по архитектуре. В общем случае понятие *сетевой архитектуры* подразумевает набор спецификаций, определяющих физическую и логическую топологии, типы кабелей, ограничения на расстояние, методы сетевого доступа, размер пакетов, структуру заголовков и другие факторы. Иногда эти спецификации называются *протоколами канального уровня.*

В настоящее время наиболее популярными архитектурами локальных сетей являются Ethernet и Token Ring. Архитектуры AppleTalk и ARCnet получили меньшее распространение. Все эти архитектуры рассматриваются в следующих разделах.

Сети Ethernet

Архитектура Ethernet, разработанная в 1960-х годах и усовершенствованная компаниями Xerox, Digital и Intel с целью соответствия спецификациям IEEE 802.3, на сегодняшний день является наиболее распространенной сетевой архитектурой. (Роль спецификаций IEEE рассматривается в главе 3., "Концепции, модели и стандарты компьютерных сетей".)

Сети Ethernet физически конфигурируются как шины или звезды. В качестве метода сетевого доступа в Ethernet используется множественный доступ с контролем несущей и обнаружением конфликтов (Carrier Sense Multiple Access Collision Detect — CSMA/CD). Пропускная способность стандартной Ethernet ограничена 10 Мбит/с. В настоящее время уже довольно распространена *Fast Ethernet* с пропускной способностью 100 Мбит/с и в ближайшем будущем на рынке должна появиться *Gigabit Ethernet*, перешагнувшая рубеж 1 Гбит/с.

В зависимости от используемого типа кабеля выделяются следующие архитектуры Ethernet:

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

В следующих разделах приведены характеристики каждой архитектуры Ethernet.

Замечание

Спецификации максимальной и минимальной длины сегмента в большинстве литературных источников приведены в метрах, так как в научной литературе стандартом служит метрическая система единиц, а не принятая в США. В этой книге везде используется метрическая система. Однако в некоторых распространенных программах сертификации системы единиц смешиваются. Например, в одном вопросе длина кабеля может быть в метрах, а в другом — в футах. Поэтому необходимо помнить их соотношение: 1 метр равен 3,28 фута.

Ethernet 10Base5

Сеть 10Base5 иногда называют стандартной Ethernet, хотя в настоящее время она уже не так распространена, как некоторые другие типы Ethernet В сети 10Base5 используется толстый коаксиальный кабель RG-8 или RG-11 (толщиной немного больше сантиметра), поэтом ее называют *толстой сетью*

Число 10 в названии 10Base5 означает максимальную пропускную способность 10 Мбит/с Число 5 означает максимальную длину сегмента 500 метров В толстых сетях используется шинная топология

По ряду причин с толстыми сетями труднее работать, чем с Ethernet, в которых используются другие типы кабелей Во-первых, толстый кабель менее гибок из-за большого диаметра Во-вторых, в соединении используется специальное устройство — пронзающий ответвитель, или "зуб вампира", при этом для соединения с разъемом в кабеле нужно просверлить небольшое отверстие В сетях 10Base5 используются *внешние трансиверы* Трансивер представляет собой устройство, генерирующее и принимающее сигналы данных В других архитектурах Ethernet трансиверы встроены в сетевой адаптер Для подключения трансивера к сетевому адаптеру в сетях 10Base5 используется разъем DIX и кабель AUI

Замечание

Сетевые адаптеры и различные типы разъемов подробно рассматриваются в главе 7, "Физические компоненты сетей"

Толстые сети часто используются совместно с другими типами кабелей Ethernet для построения *магистрали*, соединяющей тонкие сегменты сети

Ethernet 10Base2

Довольно распространены коаксиальные сети 10Base2, в которых используется более тонкий кабель (приблизительно полсантиметра диаметром) Эти сети дешевле, а кабель более гибкий, чем у 10Base5 Число 2 в названии сети означает округленное значение максимальной длины сегмента, которая равна 185 метров Как и в 10Base5, в тонких сетях используется шинная топология с терминаторами на каждом конце

На физическом уровне сеть 10Base2 легче установить, чем толстую сеть Для подсоединения кабеля к Т-образному разъему сетевого адаптера используется поворотный разъем BNC (рис 2 15) Трансивер встроен в сетевой адаптер

Замечание

Хотя кабель RG-58 внешне и похож на RG-59, используемый в кабельных телевизионных сетях, путать их нельзя Кабель RG-59 имеет сопротивление 59 Ом и его *нельзя* применять в компьютерных сетях Кабель RG-58U принадлежит к тому же типу, что и RG-58, однако он не отвечает требованиям спецификаций IEEE, поэтому использовать его не рекомендуется

Кабели тонких сетей иногда называются *дешевыми*, потому что с ними установка сети обходится дешевле, чем с толстыми кабелями Погонная стоимость (стоимость одного метра) тонкого кабеля обычно выше, чем витой пары, однако благодаря шинной топологии в коаксиальной сети расход кабеля меньше

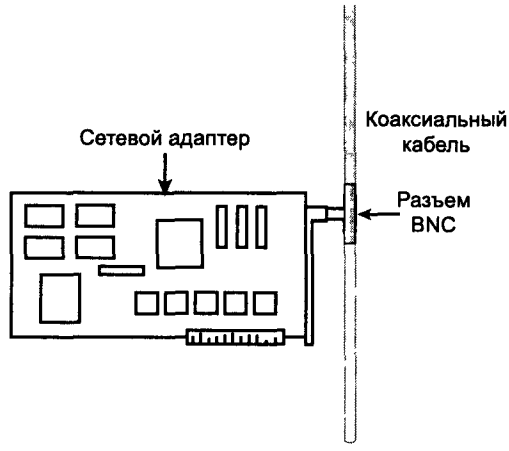


Рис. 2 15 Тонкая сеть подсоединяется к Т-образному разъему сетевого адаптера с помощью поворотного устройства BNC

Ethernet с витыми парами

В настоящее время при установке новых локальных сетей чаще всего используются витые пары, в частности в сетях 10BaseT (буква T означает *twisted — скрученный*). Большинству читателей витые пары хорошо знакомы, поскольку они используются в телефонных линиях.

Существует несколько категорий витых пар: 1, 2 и т.д. В табл. 2.3 приведены характеристики и области применения различных категорий витых пар.

Таблица 2.3. Используемые категории витых пар

Категория	Максимальная пропускная способность	Характеристики и область применения
Cat 1	Только для голоса	Только в телефонных сетях
Cat 2	4 Мбит/с	Для передачи данных не рекомендуется
Cat 3	16 Мбит/с	Низший уровень распознавания данных, используется главным образом в телефонных сетях
Cat 4	20 Мбит/с	Пригоден для Ethernet с пропускной способностью 10 Мбит/с
Cat 5	100 Мбит/с–1 Гбит/с	Наиболее распространенная категория в локальных сетях, используется в Fast Ethernet (100 Мбит/с)
Cat 5e (Enhanced)	155 Мбит/с	Используется в Fast Ethernet и сетях ATM 155 Мбит/с
Cat 6 и 7	1 Гбит/с и выше	Используется в новых технологиях Gigabit Ethernet

Кабели категории 5, 7 и улучшенной категории 5e пока что встречаются не часто, поскольку их спецификации определены сравнительно недавно.

Как видно из табл. 2.3, витые пары могут обеспечить большую пропускную способность, чем коаксиальные кабели. К тому же витая пара очень гибкая и ее легко

монтировать Они используются с разъемами RJ — типовыми модульными разъемами в телефонных линиях В телефонных линиях обычно используются меньшие по размерам разъемы RJ-11, в то время как в сетях Ethernet большинство соединений выполняется с помощью больших разъемов RJ-45

В сети с витыми парами каждый компьютер соединен с центральным концентратором в топологии звезды Различные типы концентраторов рассматриваются в главе 7, "Физические компоненты сетей"

Сети 10BaseT

Спецификация 10BaseT популярна в локальных сетях любых размеров В них могут использоваться кабели категории 3, которые уже установлены во многих зданиях в качестве телефонных линий Однако новые сети 10BaseT обычно устанавливаются с кабелями категорий 5 и 5е, чтобы в дальнейшем было легче модернизировать сети до пропускной способности 100 Мбит/с

Сети 100BaseT

Спецификация 100BaseT определяет сети Ethernet с пропускной способностью 100 Мбит/с, выполненные на кабелях категорий 5 и 5е В этих сетях используются те же топология и методы доступа, что и в 10BaseT И действительно, единственное их отличие — требования к пропускной способности кабеля, сетевых адаптеров и концентраторов, которые должны обеспечивать скорость передачи 100 Мбит/с

Многие сетевые адаптеры и концентраторы сконструированы таким образом, что они могут поддерживать скорость передачи как 10 Мбит/с, так и 100 Мбит/с, что значительно облегчает задачу модернизации сетей Кроме того, при наличии соответствующего оборудования часть сети может работать со скоростью 100 Мбит/с, а другая часть — со скоростью 10 Мбит/с

Сети 1000BaseT (Gigabit Ethernet)

Первые стандарты высокоскоростной Ethernet, чаще всего называемой Gigabit Ethernet, были разработаны организацией IEEE в 1996 году и опубликованы как спецификации 802 3z Эти стандарты предусматривают передачу данных со скоростью 1 000 Мбит/с, в них используются формат кадра Ethernet 802 3 и метод доступа CSMA/CD

Замечание

Стандарт IEEE 802 3ab определяет требования к режимам работы, тестовым проверкам и правилам эксплуатации сетей Gigabit Ethernet на расстоянии до 100 метров с использованием четырех медных витых пар категории 5 К этой категории принадлежит большинство кабелей уже установленных в зданиях для сетей 10BaseT и 100BaseT

Большим преимуществом Gigabit Ethernet является их способность работать с разными операционными системами и совместимость с предшественниками Gigabit Ethernet — прекрасная магистраль для объединения локальных сетей 10BaseT и 100BaseT

В продаже есть сетевые адаптеры и концентраторы, удовлетворяющие стандартам 1000BaseT, однако их стоимость в несколько раз выше, чем у компонентов Ethernet на 100 Мбит/с

Сети 100BaseVG-AnyLAN

Технология 100BaseVG-AnyLAN разработана компанией Hewlett Packard. Это быстродействующая и надежная архитектура. В ней используется специальный тип концентраторов, выполняющих функции интеллектуального центрального контроллера. Такой концентратор управляет доступом к сети путем быстрого карусельного сканирования запросов к портам в целях выявления служебных запросов от присоединенных к нему узлов. Концентратор принимает поступающие к нему пакеты данных и направляет их только в порты с соответствующими целевыми адресами. Такое сопоставление адресов существенно повышает безопасность сети.

Концентраторы могут быть связаны, причем каждый из них можно конфигурировать на поддержку форматов кадра как Ethernet 802.3, так и Token Ring 802.5. Однако все концентраторы одного и того же сегмента сети должны быть конфигурированы на одни и те же форматы кадров.

Сети 100BaseVG-AnyLAN часто причисляют к категории Ethernet, однако в них используется другой метод доступа к сети, который определен спецификацией IEEE 802.12 и называется *приоритетом требований*.

Сети 10BaseFL и 100BaseFL

Буквы FL в названии сетей означают *fiber link — волоконно-оптическая связь*. В этих сетях используется немодулированная передача сигналов по волоконному оптическому кабелю. Методы передачи рассматриваются в главе 4, "Методы сетевой коммуникации".

В волоконно-оптических кабелях для представления нулей и единиц информации, используемой компьютерами, применяется не электрический сигнал, а световые импульсы. Большим преимуществом волоконной оптики по сравнению с медными кабелями является отсутствие помех и *затухания* (т.е. уменьшения мощности сигнала с расстоянием). Длина участка волоконно-оптического кабеля, удовлетворяющего спецификациям, может достигать 2 000 метров, что в 4 раза превосходит максимальную длину в 10Base5, в 10 раз — 10Base2 и в 20 раз — 10BaseT!

Сети Token Ring

Сетевая архитектура Token Ring была разработана компанией IBM в 1980-х годах. Она была задумана для преодоления некоторых трудностей, присущих сетям *конкурентного* типа, таким как Ethernet, в которых компьютеры "состязаются" за доступ к сети. Более подробно этот вопрос рассматривается в главе 4, "Методы сетевой коммуникации".

В сети Token Ring используется кольцеобразная логическая топология. Сигнал, называемый *маркером* (*token*), проходит по кругу, и компьютер не может получить доступ, пока к нему не придет маркер. Следовательно, в отличие от Ethernet, в сети Token Ring невозможны *конфликты данных*, происходящие при одновременном начале передачи данных двумя компьютерами.

Хотя логически в сетях Token Ring используется кольцевая топология, физически они имеют звездообразную топологию. Компьютеры подключены к центральному концентратору, который называется MSAU (Multistation Access Unit). Фактически кольцо находится внутри концентратора, в котором порты соединены в непрерывный круг и данные проходят по круговому пути.

Требования к сетям Token Ring определяются стандартами IEEE 802.5. В сети используются экранированные витые пары типа IBM. Сетевые адаптеры и другие компоненты

Token Ring в общем случае дороже, чем в сетях Ethernet. Несмотря на это, архитектура Token Ring очень надежна и все еще используется во многих локальных сетях.

Более старые компоненты Token Ring поддерживают скорость передачи не более 4 Мбит/с, однако в настоящее время выпускаются все компоненты, обеспечивающие 16 Мбит/с.

Замечание

В настоящее время предпринимаются значительные усилия для разработки эффективной быстродействующей технологии Token Ring под стандарт FDDI (Fiber Distributed Data Interface) и в режиме ATM (Asynchronous Transfer Mode) Подробную информацию по этому вопросу можно найти на Web-узле организации High-Speed Token Ring Alliance по адресу: `www.hstra.com/whitepapers.html`.

Сети Token Ring обладают рядом преимуществ.

- Когда сеть Token Ring перегружена, ее производительность плавно понижается. Неожиданный крах, как случается в Ethernet, произойти не может.
- В сетях Token Ring используется *активная топология*, в которой каждый компьютер в кольце регенерирует сигнал, проходящий по кругу. В то же время в Ethernet для усиления сигналов, передаваемых с большого расстояния, нужны повторители.

Сети AppleTalk

Пакет протоколов AppleTalk был разработан компанией Apple Computers с целью объединения компьютеров Macintosh для разделения (т е. совместного использования) различных ресурсов (файлов, принтеров и т.д.) рабочей группы. Эта задача решается с помощью пакета AppleShare, представляющего собой набор протоколов уровня приложений. Пакет AppleShare состоит из следующих компонентов, встроенных в операционную систему Macintosh

- **Файловый сервер AppleShare**. Предоставляет пользователям доступ к ресурсам компьютера.
- **Принтерный сервер AppleShare**. Позволяет совместно использовать принтеры.

Пакет AppleShare включает служебную программу, выполняющуюся на компьютерах, на которых установлена DOS. Эта программа обеспечивает компьютеру доступ к файловому серверу или серверу печати AppleShare.

Сети AppleTalk иногда называют *LocalTalk*. В них используется базовый протокол LLAP (Local Talk Link Access Protocol), поддерживающий динамическую адресацию.

Сеть AppleTalk можно разделить на группы, называемые *зонами*. Они выполняют роль, аналогичную рабочим группам в больших сетях. Пользователи имеют доступ только к разделяемым ресурсам своей зоны. Для связи между зонами маршрутизаторы используют протокол ZIP (Zone Information Protocol).

Сети ARCnet

В ARCnet (Attached Resource Computer Network) используется довольно старая архитектура. Почти все они уже вытеснены сетями Ethernet и Token Ring. В ARCnet применяется метод доступа с маркерами, однако топология ARCnet представляет собой шину или звезду, а не кольцо.

В ARCnet маркер проходит в порядке возрастания по адресам узлов, представляющим собой восьмеричные числа, установленные на сетевом адаптере ARCnet с помощью перемычек. Если карты пронумерованы недостаточно тщательно и не обеспечена рациональная последовательность прохождения сигнала или если компьютер перенесен в другое место без изменения адреса, то сигнал будет проходить расстояние, большее чем необходимо. Описанная проблема проиллюстрирована на рис. 2.16.

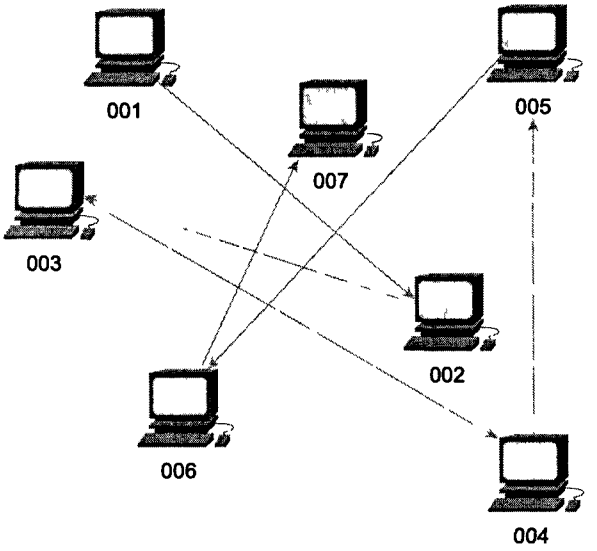


Рис. 2 16. Если на сетевом адаптере ARCnet адреса установлены непродуманно, то путь маркера может оказаться неэффективным

Замечание

Скорость передачи в ARCnet по сравнению с другими локальными сетями невелика: 2,5 Мбит/с для стандартной ARCnet. В новом стандарте ARCnet Plus скорость передачи увеличена до 20 Мбит/с.

В ARCnet можно использовать коаксиальные кабели, витые пары и даже волоконно-оптические кабели. Однако чаще всего используется коаксиальный кабель RG-62/U сопротивлением 90 Ом. Один из недостатков ARCnet, служащий причиной ее все меньшей популярности, — ее "крайне собственническая натура" (другими словами, это "вещь в себе"). Тем не менее архитектура ARCnet устойчива и надежна

Резюме

В этой главе были рассмотрены различные способы классификации сетей, включая следующие:

- по географическому региону, охваченному сетью;
- по административной модели, используемой для управления сетью;

- по сетевым операционным системам, выполняющимся на серверах;
- по используемым в сети протоколам;
- по топологии (раскладке, форме) сети;
- по архитектуре, охватывающей стандарты и спецификации, обусловливающие работу сети.

Существуют, конечно, и другие способы классификации сетей. Например, сети UNIX можно разделить на HP-UX, SUN Solaris, AIX, SCO и т.д. Сети Microsoft можно разделить на сети на основе Windows 2000, Windows NT 4.0, Windows NT 3.51 и т.д., не говоря о рабочих группах Windows 9*x*.

Рассматривая различные методы классификации, вы видимо обратили внимание, что определенные архитектуры связаны с определенными топологиями, некоторые сетевые операционные системы используют конкретные модели администрирования, а некоторые протоколы применяются чаще в сетях определенного размера. В следующих главах мы еще вернемся к этим зависимостям.

Будут также рассматриваться сигналы, используемые в различных топологиях, и типы кабелей, ассоциированные с разными методами доступа к сети. В главе 3, "Концепции, модели и стандарты компьютерных сетей", вы познакомитесь с популярной моделью, описывающей сложные процессы с участием всех этих компонентов. Будут рассмотрены также спецификации и стандарты, определяющие построение и функционирование сетей.

Рекомендуемые источники

Хорошим источником информации о Gigabit Ethernet служит Web-страница консорциума Gigabit Ethernet Consortium: `www.iol.unh.edu/consortiums/ge/main.html`.

Gigabit Ethernet регулярно обсуждается на ежегодной весенней конференции в Сан-Хосе, Калифорния (`www.etherconference.com/English/Main_Splash.html`)

Прекрасный источник информации о сети 100BaseVG-AnyLAN компании Hewlett Packard — Web-узел `www.100vg.com`.

Общая информация по работе локальных сетей приведена по адресу: `www.net-engineer.com/lanbasics1.html`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Что из приведенного ниже является типом сети в классификации по физической области действия?
   - **а.** 10Base2.
   - **б.** WAN (глобальная сеть).
   - **в.** IPX/SPX.
   - **г.** Кольцо.
2. Какие из приведенных утверждений справедливы для типичной локальной сети?

а. Локальная сеть — это большая сеть, состоящая из множества малых сетей.

б. Локальная сеть охватывает широкую географическую область с узлами в разных городах, штатах и странах.

в. Локальная сеть охватывает ограниченную площадь, ее компьютеры расположены недалеко друг от друга.

г. Для упрощения задач управления локальную сеть можно разделить на рабочие группы.

3. Как называется группа сетей, соединенных друг с другом?

а. internet.

б. intranet.

в. extranet.

г. Рабочая группа.

4. Какие из приведенных утверждений верны для сетей клиент/сервер?

а. Установка сетей клиент/сервер обходится дешевле.

б. В сетях клиент/сервер данные хранятся централизованно, что облегчает создание резервных копий.

в. Для обслуживания сетей клиент/сервер нужен сетевой администратор.

г. Сети клиент/сервер обеспечивают большую безопасность.

5. Как называется сервер, выполняющий регистрационную аутентификацию в сети Microsoft типа клиент/сервер?

а. Демон.

б. Security Accounts Manager.

в. Контроллер домена.

г. Кластерный сервер.

6. Какие из этих утверждений о безопасности в одноранговой сети верны?

а. Средства обеспечения безопасности централизованы и контролируются сетевым администратором.

б. Безопасность выше, чем в среде клиент/сервер, нарушить целостность и конфиденциальность данных труднее.

в. В каждом компьютере рабочей группы хранится своя база данных с параметрами безопасности.

г. Безопасность обеспечивается не на уровне пользователей, а на уровне разделяемых ресурсов.

7. Какие из этих утверждений о доменах Windows 2000 верны?

а. Основой доменов Windows 2000 является служба каталогов, которая называется Active Directory.

б. Основой доменов Windows 2000 является служба каталогов, которая называется Bindery.

в. Домены Windows 2000 называются доменами нижнего уровня.

г. Домен Windows 2000 может содержать много контроллеров доменов, причем все они могут читать и записывать в базу данных, содержащую информацию о каталогах.

8. Какие из этих утверждений о сетях TCP/IP верны?
   а. Сети TCP/IP представляют собой сети средних и больших размеров, содержащие много подсетей.
   б. Глобальная сеть Internet является сетью TCP/IP.
   в. Количество инструментов и утилит, разработанных для сетей TCP/IP, невелико.
   г. Сети TCP/IP легче администрировать, чем NetBEUI.
9. Как называется сетевая топология, в которой сеть имеет начало и конец, а для предотвращения отражения сигналов используются терминаторы?
   а. Звездообразная.
   б. Смешанная ячеистая.
   в. Шинная.
   г. Token Ring.
10. В каких сетевых архитектурах используются неэкранированные витые пары?
   а. 10Base2.
   б. 10BaseT.
   в. 100BaseFL.
   г. Token Ring.

Глава 3

Концепции, модели и стандарты компьютерных сетей

Изучать новый предмет, особенно такой сложный, как компьютерные сети, легче всего, начав с теории и лежащих в его основе концепций, переходя затем к конкретным вопросам реализации. Подобно тому как начинающий врач, прежде чем заняться пациентами, должен изучить биохимию, анатомию и другие теоретические дисциплины, начинающий специалист по сетям должен сначала изучить теорию построения и принципы функционирования компьютерных сетей.

В этой главе представлены базовые концепции построения и функционирования компьютерных сетей. Обсуждаются сетевые модели, стандарты, спецификации (а также организации, учреждающие их) и основные принципы работы сетей, которые необходимо помнить, знакомясь в следующих главах с оборудованием и программным обеспечением сетей.

Базовые принципы сетевых коммуникаций

Независимо от размера и области действия сети, топологии, архитектуры, типа среды или модели администрирования, компьютеры связываются в сеть всегда с одной и той же целью: для обмена информацией. Это звучит просто, однако в действительности процессы коммуникации очень сложны. Прежде чем приступить к изучению процессов коммуникации в компьютерной сети, нужно понять, как компьютеры обрабатывают информацию.

В этой главе рассматриваются базовые концепции, лежащие в основе процессов коммуникации.

- Двоичный язык, применяемый для коммуникации с компьютерами (называемый *машинным языком*).
- Модели сетей, предназначенные для графического представления процессов коммуникации.

- Стандарты и спецификации, разработанные для того, чтобы сетевые системы разных поставщиков могли сообщаться друг с другом.

В первую очередь рассмотрим *код*, или язык, на котором "разговаривают" компьютеры, и то, как с его помощью можно *запрограммировать* компьютер, т.е. заставить его сделать нужную работу.

Язык компьютеров

Современные компьютеры — это сложнейшие машины, способные выполнять разнообразные задачи. Если с помощью программы текстового процессора в компьютер ввести письмо или отчет, то он не только сохранит сделанную работу, но и автоматически отметит грамматические ошибки, отформатирует документ и даже передаст его на другой компьютер, расположенный в соседней комнате или на другом конце Земли.

Если на компьютере установлено соответствующее программное обеспечение, то он может, отслеживая заданное расписание, выполнить в определенное время необходимые действия или напомнить пользователю, что нужно сделать. С помощью определенных утилит компьютер может автоматически поддерживать порядок в операционной и файловой системах, регистрироваться в Internet (самостоятельно или с помощью пользователя) и обновлять свое программное обеспечение. Компьютер может даже выиграть в шахматы у чемпиона мира!

Все эти задачи (и многие другие) компьютер решает, оперируя исключительно нулями и единицами. Все процессы внутри компьютера — это команды, исходными данными и результатами которых являются *двоичные числа*, которые, как будет видно дальше, великолепно подходят для электронной коммуникации. Сами команды тоже представляют собой двоичные числа. Двоичный код команд называется *машинным языком*.

Системы счисления

Существует несколько систем счисления. В своих повседневных делах люди пользуются *десятичной* системой, однако в компьютерных и коммуникационных технологиях чаще используются *шестнадцатеричная* и *двоичная* системы. Рассмотрим каждую из них.

Десятичная система

Десятичную систему счисления называют также *системой счисления с основанием 10*, потому что она основана на десяти цифрах (от 0 до 9), с помощью которых можно представить любое число.

Замечание

Десятичное число не обязательно содержит десятичную точку.

В десятичном числе 342 цифра "3" представляет *три сотни*, "4" — *четыре десятки*, а "2" — *две единицы*. Таким образом, каждая цифра представляет величину, определенную значением цифры и ее положением в числе.

Шестнадцатеричная система

Еще одна система счисления, используемая в компьютерных технологиях, — *шестнадцатеричная* (система счисления с основанием 16). Число 16 не имеет какого-либо магического значения, однако операции с ним для непосвященных могут пока-

заться не менее загадочными, чем черная магия Главная причина, по которой число 16 удостоено столь высокого звания, — его равенство целой степени двойки Для представления шестнадцатеричных чисел используется десять цифр десятичной системы и шесть символов латинского алфавита от A до F

В шестнадцатеричной системе цифры от 0 до 9 имеют то же значение, что и в десятичной Символ A (здесь он уже называется цифрой) представляет число, равное 10 в десятичной системе Соответственно цифра B равна 11 и так далее вплоть до цифры F, равной 15 Дальнейшие числа уже нельзя представить одной цифрой Десятичное число 16 в шестнадцатеричной системе записывается как 10, десятичное 17 — как 11 и т д Другими словами в шестнадцатеричной системе, как и в десятичной (и во всех других), величина, представленная цифрой, определяется значением цифры и ее позицией в числе

Замечание

В английском языке "шестнадцатеричный" звучит как *hexadecimal* Это слово-гибрид происходит из двух языков в древнегреческом "hexa" означает "шесть", а в латинском "decimal" означает "десять"

Как преобразовать число из одной системы счисления в другую? Проще всего это сделать с помощью калькулятора Windows в научном режиме или карманного калькулятора Все арифметические операции над шестнадцатеричными числами выполняются точно так же, как над десятичными, за исключением того, что в них участвуют дополнительные шесть цифр В табл 3 1 приведено соответствие шестнадцатеричных и десятичных чисел

Таблица 3.1. Соответствие шестнадцатеричных и десятичных (в скобках) чисел

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)

Шестнадцатеричная запись используется в компьютерах потому, что в двоичное число легче преобразовать шестнадцатеричное, чем десятичное Поскольку *баит* состоит из восьми битов, а шестнадцатеричное число можно выразить четырьмя битами, следовательно, в одном байте можно записать две шестнадцатеричные цифры В следующих разделах этой главы мы еще вернемся к байтам и битам

В табл 3 1 обратите внимание на то, что некоторые шестнадцатеричные числа выглядят точно так же, как десятичные, хоть и не равны им Как же узнать, в какой системе записано число, если, например, написано "12"? Ведь оно может представлять десятичное число 12, или шестнадцатеричное 18' Следовательно, нужен какой-то способ обозначения шестнадцатеричных чисел (но не десятичных, потому что люди давно уже привыкли писать десятичные числа, никак не отмечая, что они десятичные) Обозначать шестнадцатеричные числа принято одним из следующих двух способов

- добавить символ "H" в конец числа, например 12H;
- добавить символы "0x" в начало числа, например 0x12.

Второй способ (символы 0x) является стандартным способом обозначения шестнадцатеричных чисел в C++ и большинстве других языков программирования.

Двоичная система

С одной стороны, двоичная система счисления чрезвычайно проста: в ней используются только две цифры — 0 и 1. Однако с другой стороны, использование только двух цифр приводит к настолько быстрому росту размеров чисел, что человек не в состоянии работать с ними. Например, десятичное число 519 в двоичной системе равно 10000000111.

Английское слово *binary* (двоичный) происходит от латинского *bi*, означающего "два". Другое название двоичной системы — *система счисления с основанием 2.*

Нули и единицы

Если вы никогда не работали с двоичными числами, то вас может удивить: как можно представить любое число, используя только нули и единицы? Этот же вопрос можно задать и о десятичной системе счисления, однако нас это не удивляет, поскольку десятичную систему мы используем всю жизнь. Для любого человека кажется совершенно нормальным использовать позицию цифры для указания представляемой этой цифрой величины. Например, в третьей позиции справа записываются сотни. Точно так же записывается и двоичное число.

Замечание

Помните: в двоичной системе счисления существуют только нули и единицы.

Биты и байты

Двоичная цифра (0 или 1) называется битом. Один байт равен восьми битам. Байт — это строка битов, сгруппированных для удобства в группы по восемь битов. В компьютерах байт используется для представления *символа*, т.е. буквы, цифры или какого-либо другого символа.

Замечание

Слово "байт" (по-английски *byte*) происходит от *binary term* — "двоичный терм". В одном байте компьютерной памяти хранится один символ. Стандарт устанавливает размер байта равным 8 битам, однако в прошлом иногда байтом называли 16 битов В настоящее время байт всегда считается равным 8 битам, хоть некоторые символы и записываются в 16 битах.

Преобразование двоичного числа в десятичное

Рассмотрим двоичное число 01001100. Чтобы определить значение этого числа, нужно знать, какую величину представляет каждая цифра в зависимости от ее позиции.

Каждый бит в двоичном числе "включен" или "выключен". Цифра 0 означает, что бит выключен, а 1 — включен. Как и в других системах счисления, номер позиции в числе отсчитывается справа.

В двоичном числе (как и в десятичном) первая позиция справа представляет величину, равную 1. Однако на этом сходство двоичной и десятичной систем заканчивает-

ся. В двоичной системе счисления вес каждой следующей позиции в два раза больше веса предыдущей (в десятичной системе — в десять раз, в шестнадцатеричной — в шестнадцать). В табл 3.2 приведены десятичные эквиваленты каждой позиции двоичного числа (т.е. вес позиции, или ее значение, когда бит равен 1).

Таблица 3.2. Вес позиции (десятичное значение бита, равного 1, в разных позициях)

Двоичный бит	1	1	1	1	1	1	1	1
Десятичное значение	128	64	32	16	8	4	2	1

Если двоичная цифра равна 0, значит, бит в этой позиции выключен и значение позиции равно нулю Чтобы преобразовать двоичное число в десятичное, нужно просуммировать десятичные значения каждого бита. В табл. 3.3 показано преобразование двоичного числа 01001100 в десятичное.

Таблица 3.3. Преобразование двоичного числа в десятичное

Двоичный бит	0	1	0	0	1	1	0	0
Десятичное значение	0	64	0	0	8	4	0	0

Итак, чтобы получить десятичный эквивалент двоичного числа 01001100, вычислим сумму 64+8+4. В результате получим десятичное значение, равное 76. Этот результат можно проверить с помощью научного калькулятора Windows. введите двоичное число 01001100, щелкните на кнопке Dec (Преобразование в десятичное число) и убедитесь, что результат преобразования равен 76.

Почему используются двоичные числа

Пока что все это было похоже на светскую беседу (когда на вечеринке собрались компьютерщики) Однако вы, возможно, все еще удивляетесь, зачем нужны двоичные числа? Почему не шестнадцатеричные? А еще лучше — десятичные, чтобы не нужно было тратить время на изучение других систем счисления!

Использование двоичной системы обусловлено весьма вескими причинами Компьютеры представляют собой электронные устройства, в которых данные представлены электрическими импульсами, т е. в них используются *цифровые* сигналы. В главе 4, "Методы сетевой коммуникации", мы еще вернемся к тому, что такое цифровые сигналы и чем они отличаются от *аналоговых*, используемых в телевидении и радиовещании.

Цифровые сигналы представляют собой *дискретные состояния* какого-либо устройства (ячейки памяти или канала связи). Проще всего реализовать устройство, у которого есть только два дискретных состояния. Например, участок магнитного материала, служащий ячейкой памяти, может быть или намагничен или размагничен Если бы этих состояний было больше (например, намагничен в разных направлениях или в разной степени), то конструкция ячейки памяти была бы значительно сложнее Поскольку для обозначения двух состояний лучше всего подходят 0 и 1, двоичная система счисления в компьютерных технологиях стала базовой.

Двоичная система счисления и цифровые сигналы — базовые понятия в области компьютерных и коммуникационных технологий. Более глубоко с этими вопросами можно ознакомиться с помощью источников, приведенных в конце главы

Пакеты данных

Прежде чем передать данные по сети как электрические импульсы, их нужно разделить на небольшие части, с которыми смогут работать сетевые устройства. Текстовый документ или сообщение электронной почты нельзя передать по сети как один длинный непрерывный поток, потому что он "свяжет" сеть на неопределенное время и другие компьютеры окажутся отключенными от сети. Чтобы многие компьютеры могли работать в сети одновременно, прежде чем передать большие файлы по кабелю или по какому-либо другому каналу, нужно разбить их на маленькие фрагменты.

Рассмотрим такую аналогию. Допустим, вам нужно послать своему коллеге по обычной почте отчет, объемом 100 страниц. Однако почтовое оборудование способно обрабатывать только конверты, в которых помещается всего несколько страниц отчета. Очевидное решение — вложить отчет в разные конверты, написать на них одинаковый адрес и бросить их все в почтовый ящик. Когда все конверты дойдут до адресата, он сможет собрать из них полный отчет.

В идеальном мире все конверты пришли бы один за другим в правильном порядке. Однако почтовая служба так не работает. Адресат может даже не получить все конверты в один день. Возможно, конверт с первой страницей отчета прибудет последним. Сможет ли коллега сложить страницы отчета в правильном порядке? Вы значительно облегчите ему эту работу если пронумеруете страницы отчета.

Далее в главе рассматривается, как протоколы обеспечивают составление целостного документа из разрозненных пакетов на принимающем конце канала связи.

Небольшие легкопередаваемые порции информации, на которые компьютерные данные разбиваются для передачи по сети, называются *пакетами*. В зависимости от архитектуры сети и этапа процесса коммуникации, пакеты могут называться *кадрами* или (в протоколе TCP) *сегментами*. В этой книге используется главным образом термин *пакет*.

Преимущества разбивки данных на пакеты

Разделение передаваемых данных на небольшие пакеты предоставляет ряд преимуществ.

- Сетевые компьютеры могут передавать данные по очереди. Один компьютер, передающий большое количество данных, не монополизирует канал связи.
- Если в сети происходит сбой и пакет теряется, то потребуется передать заново только один небольшой пакет, а не весь файл.
- В зависимости от топологии сети и типа соединения, каждый пакет может проходить к адресату разными путями. Следовательно, если один из путей перегружен или вышел из строя, пакеты могут достичь адресата другими путями. Эффективность и надежность передачи при этом существенно повышаются.

Сбор данных из пакетов

Если данные разбиты на фрагменты и каждый фрагмент передается отдельно, то что с ними происходит у получателя? Вспомним нашу аналогию с почтой. Компоненты сети делают с данными нечто подобное. В каждом пакете, кроме передаваемых данных, есть *заголовок пакета* (как адрес на конверте). Заголовок содержит информацию об адресе пакета, чтобы он мог попасть к нужному адресату. Кроме адреса, в заголовке содержится информация о месте пакета в последовательности других пакетов, чтобы в принимающем компьютере пакеты могли быть аккуратно собраны вместе.

Замечание

Видимо, вы заметили, что сигналы, передаваемые по сети, обозначаются словом "данные" Термины "информация" и "данные" во многих случаях взаимозаменяемы, однако это не одно и то же *Информация* — это данные в форме, пригодной для использования, например сообщение, отображаемое программой электронной почты *Данные* — это закодированная информация в форме последовательности электрических импульсов в канале связи

Заголовок размещается в начале пакета, перед данными Пакет может также содержать *трейлер*, присоединенный к концу пакета, т е после передаваемых данных Информация в трейлере чаще всего предназначена для обнаружения ошибок передачи На рис 3 1 показана структура типичного пакета данных

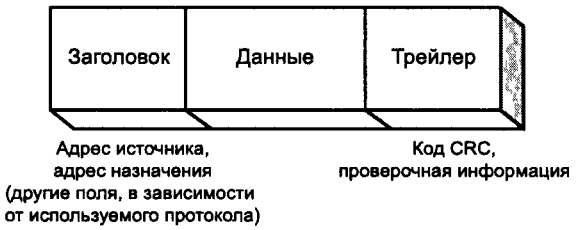


Рис 3 1 Типичный пакет данных содержит заголовок и трейлер

Замечание

В трейлере находится код *CRC (cyclical redundancy check)*, представляющий собой короткую последовательность нулей и единиц Вычисления с кодом CRC выполняются дважды перед отправкой пакета в сеть специальная процедура формирует код CRC, а после получения пакета адресатом такая же процедура вычисляет его еще раз Если результаты этих двух вычислений отличаются, значит, данные в процессе передачи изменились В этом случае пакет отбрасывается и посылается запрос на его повторную передачу

Конкретное положение в пакете и размеры полей заголовка и трейлера зависят от сетевой архитектуры и протоколов Например, в Ethernet кадр (так здесь называется пакет) может иметь размер от 64 до 1 518 байт, причем 18 байт всегда используются под заголовок и трейлер Поэтому в одном кадре Ethernet можно передать не более 1 500 байт данных Пакеты Token Ring немного больше — обычно в них находится 4 202 байта данных

Многоуровневый процесс коммуникации

Компьютер преобразует данные в нули и единицы, а затем обрабатывает их При передаче данных в другой компьютер нужно учесть, что на нем может быть загружена другая операционная система или установлены другие программы приложений Например, нужно передать электронное письмо, созданное с помощью программы Microsoft Outlook Express на компьютере с операционной системой Windows NT, причем на принимающем компьютере установлена система Apple, а электронные письма обрабатываются программой Eudora Pro

Процесс сетевой коммуникации сложен. Чтобы получатель смог принять сообщение, все введенные пользователем слова с графической информацией и файлами должны быть правильно преобразованы в последовательность нулей и единиц, которую принимающий компьютер должен правильно расшифровать.

Замечание

В локальных сетях физическим носителем двоичной информации чаще всего служат электрические импульсы. Однако могут использоваться также импульсы света или радиоимпульсы. Различные типы сетевой среды рассматриваются в главе 7, "Физические компоненты сетей".

Данные в виде электрических сигналов должны по кабелю дойти до нужного компьютера, затем их необходимо правильно преобразовать в исходную форму. Этот процесс выполняется в несколько этапов, которые называются *уровнями* процесса коммуникации.

Согласованность сетевого оборудования

Изготовление автомобиля, как и передача данных в компьютерной сети, представляет собой *процесс*, состоящий из отдельных этапов. Один человек *может*, имея соответствующие инструменты, собрать автомобиль. Однако так автомобили не делают. Почему?

Опыт показывает, что производительность труда на сборочном конвейере значительно выше. На конвейере автомобили собираются поэтапно. Каждый рабочий на определенном участке конвейера выполняет отдельную операцию. Процесс сборки разбит на небольшие этапы: один рабочий вставляет колесо, другой накладывает гайки, третий завинчивает эти гайки. Такой метод имеет ряд преимуществ.

- Каждый рабочий может сосредоточиться исключительно на своей операции.
- Поскольку рабочий повторяет одно и то же действие много раз, он приобретает прочный навык, что позволяет ему выполнять это действие с высокой производительностью.
- Работая в команде, рабочие производят конечный продукт быстрее и эффективнее, чем это смог бы сделать один человек или группа людей без определенных функций.
- Очень просто выполнять учет работы. Если на одном из этапов работа выполнена неправильно (например, не закручена гайка), то несложно определить, кто отвечает за эту операцию.

Нечто подобное происходит и в многоуровневом процессе коммуникации. На каждом уровне (т.е. каждым компонентом сети) выполняется определенная задача. В результате процесс коммуникации выполняется быстрее и эффективнее. Если на каком-то этапе происходит ошибка, то, как и в примере с автомобильным конвейером, администратор сети может сузить область поиска компонента, вызывающего неполадки.

Процессы и протоколы

В многоуровневой модели процесс сетевой коммуникации разбит на отдельные этапы. Вернемся к примеру с автомобилем. Каждый рабочий выполняет определенную операцию. В компьютерной сети роль рабочих играют *протоколы*: один "рабочий" принимает данные от приложения, другой сжимает и шифрует данные, третий формирует пакеты и т.д. И наконец, в принимающем компьютере последний "рабочий" формирует из пакетов исходный документ.

Каждый протокол используется на определенном уровне модели коммуникации. В следующих разделах модели коммуникации рассматриваются более подробно. Вам необходимо хорошо понимать, как протоколы соотносятся с уровнями. Уровень не только определяет функции протокола, но и служит источником ценной информации для устранения неполадок в случае их возникновения.

Сетевые модели

Восприятие информации человеком в значительной степени зависит от ее визуализации. Мы лучше понимаем что-либо, когда видим это своими глазами. Абстрактные концепции не имеют конкретных форм, однако, чтобы их было легче понять, используется *модель*, т.е. визуальное представление, например структуры, процессы или отношения.

Мы встречаемся с наглядными моделями на каждом шагу. Генетики представляют структуру молекулы ДНК в виде двойной спирали. В физической модели атома электроны и протоны представлены в виде шариков. Элементарные частицы не являются шариками, однако эта модель позволяет наглядно представить то, что нельзя увидеть непосредственно.

Назначение моделей

Слово "модель" имеет много значений, например: "модель — схематическое описание предмета (системы, теории или явления), которое включает известные свойства предмета и может быть использовано для его дальнейшего изучения". В этом определении присутствует одно из назначений сетевых моделей: помочь нам описать и понять процесс сетевой коммуникации.

Другое значение слова "модель" — "пример для подражания или сравнения" — тоже неплохо подходит для сетевых моделей, поскольку они служат основой *стандартизации* оборудования и программного обеспечения сети. Если разные поставщики сетевых продуктов используют одну и ту же модель, то их продукты будут совместимы друг с другом. В модели представлено, как *должны* происходить процессы коммуникации. Если поставщики придерживаются стандартов на каждом уровне, то их оборудование будет совместимо с оборудованием других поставщиков на других уровнях. Далее в главе рассматриваются различные вопросы стандартизации, а также организации, которые их разрабатывают и поддерживают.

Модель OSI

В мире компьютерных сетей модель OSI (Open System Interconnection) — это "модель моделей". Она обсуждается практически в каждой книге по компьютерным сетям. Разработана эта модель Международной организацией стандартизации (International Organization for Standardization — ISO).

Замечание

В некоторых книгах название модели OSI расшифровывается как Open System *Interconnect*. Это название используется на Web-узле организации ISO. Им, конечно, виднее.

Структура модели OSI

Модель OSI состоит из семи уровней, каждый из которых представляет определенный этап процесса сетевой коммуникации. Семиуровневая модель OSI показана на рис. 3.2.

Протоколы, входящие в состав *пакета протоколов*, работают на разных уровнях. Дополнительная информация о сетевых протоколах приводится в главе 8, "Сетевые протоколы и службы".

Каждый уровень модели OSI выполняет определенную задачу процесса коммуникации, а затем передает данные вверх или вниз на следующий уровень (в зависимости от того, передает или принимает компьютер данные). По мере прохождения данных по уровням, каждый уровень добавляет свою информацию в виде *заголовков* перед исходными данными. На рис. 3.1 показано, как присоединяются заголовки.

Взаимодействие одноранговых уровней

Процесс коммуникации протекает следующим образом. На передающей стороне приложение создает данные, которые должны быть переданы по сети. Затем данные поступают на уровень приложений сетевого компонента операционной системы.

Когда данные проходят по уровням, они *инкапсулируются* (вкладываются) во все больший блок, по мере того как каждый уровень добавляет заголовочную информацию. Когда данные поступают на принимающий компьютер, этот процесс выполняется в обратной последовательности. Информация передается вверх по уровням. При этом каждый уровень удаляет инкапсулирующую информацию.

Канальный уровень на принимающем конце считывает и удаляет заголовок, добавленный канальным уровнем на передающей стороне. Таким образом, каждый уровень на принимающей стороне обрабатывает заголовочную информацию, добавленную соответствующим уровнем на передающей стороне. Другими словами, каждый уровень взаимодействует с таким же уровнем на другой стороне. Этот процесс показан на рис. 3.3.

Когда данные прошли все уровни в принимающем компьютере, вся заголовочная информация оказывается удаленной и данные принимают исходную форму (как они были созданы приложением на передающей стороне). В этом виде они предоставляются принимающему приложению.

На рис. 3.4 показано, как добавляется заголовочная информация по мере продвижения по уровням.

Обратите внимание на то, что физический уровень не добавляет заголовочную информацию. Функции физического уровня не требуют этого, потому что это уровень сетевого оборудования. Его задачей является обработка электрических сигналов.

Замечание

Процесс коммуникации начинается в передающем компьютере с вершины модели. Однако во многих руководствах уровни OSI отсчитываются "снизу вверх". Иногда встречаются термины "уровень 1", "уровень 2" и т.д. Стандартом обусловливается нумерация, начиная с нижнего уровня, т.е. физический уровень называется уровнем 1.

Прикладной уровень

Первое и главное, что нужно хорошо запомнить о прикладном уровне, — это то, что он не является пользовательским приложением, создающим сообщение. Напро-

тив, прикладной уровень обеспечивает взаимодействие между пользовательским приложением и сетью. Протоколы прикладного уровня выполняют такие функции, как передача файлов, доступ к принтеру и служба сообщений



Рис 3 2 Модель OSI состоит из семи уровней

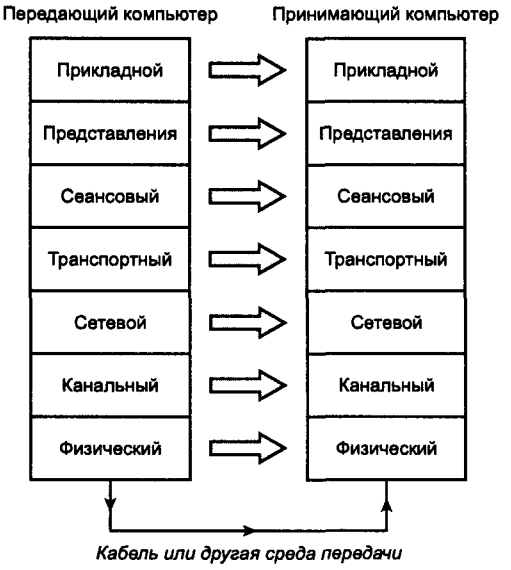


Рис 3 3 Каждый уровень взаимодействует с аналогичным одноранговым уровнем на другой стороне

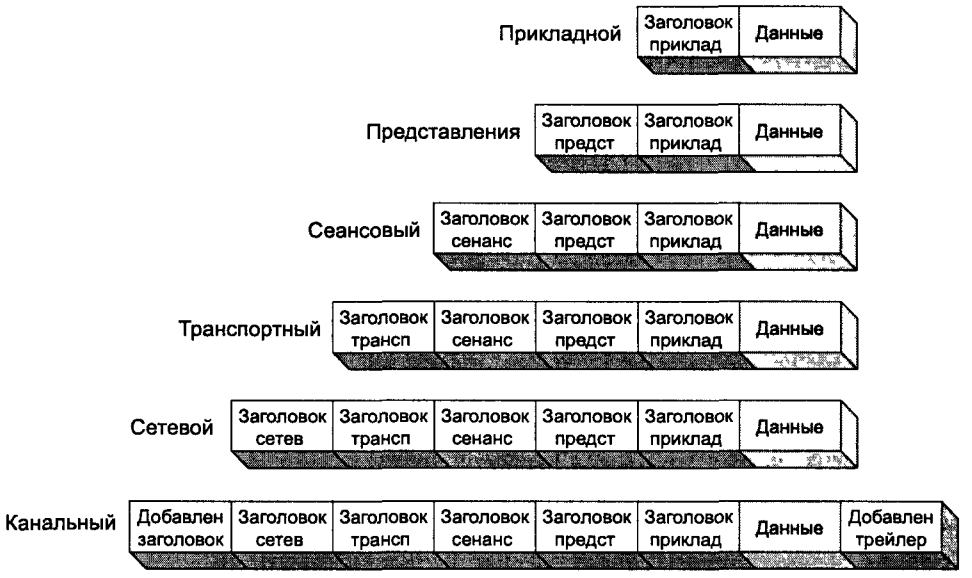


Рис 3 4 По мере продвижения данных по уровням каждый уровень добавляет заголовочную информацию

На прикладном уровне работают перечисленные ниже протоколы.

- **FTP (File Transfer Protocol)**. Используется для передачи файлов между компьютерами, на которых могут быть установлены разные операционные системы или платформы. Программное обеспечение FTP-сервера выполняется на компьютере, передающем файлы, а *клиентская программа* FTP используется для организации соединения и загрузки файлов с сервера. Клиентская программа FTP, вызываемая из командной строки, включена почти во все реализации пакета протоколов TCP/IP. Широко распространены графические клиентские программы FTP, например WSFTP, CuteFTP и FTP Voyager. В последних версиях Web-броузеров, таких как Microsoft Internet Explorer и Navigator/Communicator компании Netscape, тоже содержатся встроенные средства FTP.
- **Telnet**. Используется для эмуляции терминала и для предоставления доступа к приложениям и файлам на другом компьютере. В отличие от FTP, протокол Telnet нельзя использовать для копирования файлов с одного компьютера на другой. Его можно использовать только для чтения и для выполнения приложений на удаленном узле. Программное обеспечение Telnet состоит из программного обеспечения сервера Telnet, выполняющегося на удаленном компьютере, к которому предоставляется доступ, и программного обеспечения клиента Telnet, выполняющегося на компьютере, который получает доступ.
- **SMTP (Simple Mail Transfer Protocol)**. Представляет собой простой протокол ASCII, не ориентированный на конкретного поставщика и используемый для передачи посредством Internet электронных сообщений. Протокол SMTP используется многими популярными программами отправки электронных сообщений и программами выгрузки писем из пользовательского почтового ящика на сервере (например, Post Office Protocol, текущая версия — POP3, или Internet Message Access Protocol).
- **SNMP (Simple Network Management Protocol)**. Используется для получения информации о сети. Можно применять с разными платформами и операционными системами. Протокол SNMP входит в состав пакетов TCP/IP, IPX и OSI. В протоколе SNMP используется MIB (Management Information Base), которая представляет собой базу данных с информацией о компьютерах сети. Протокол SNMP состоит из двух частей: программного обеспечения *агента*, выполняющегося на контролируемом компьютере, и программного обеспечения *управления*, выполняющегося на контролирующем компьютере.

Кроме перечисленных, существует довольно много других протоколов прикладного уровня. В главе 9, "Самая глобальная сеть — Internet", рассматриваются такие протоколы, как HTTP (Hypertext Transfer Protocol) и NNTP (Network News Transfer Protocol).

Не следует путать приложения с протоколами под тем же именем, служащими основой этих программ. Например, существует много приложений различных поставщиков с именем FTP (таких, как FTP Voyager, FTP Explorer, Fetch для Macintosh и GREED для Linux). В этих программах FTP используется для передачи файлов, однако, кроме этого, в них включены некоторые дополнительные средства, такие как графические интерфейсы (отличающиеся в разных реализациях) или драйверы поиска файлов.

Уровень представления

Протокол прикладного уровня принимает данные от пользовательского приложения и передает их вниз по стеку протоколов на уровень представления. На этом уровне решаются задачи, связанные с *представлением* данных, т.е. с формированием пакетов.

- **Сжатие данных**. Уменьшение размера данных с целью их быстрой передачи по сети. Различные типы данных могут сжиматься в разной степени.
- **Шифрование данных**. Преобразование данных в закодированную форму таким образом, чтобы они не могли быть прочитаны посторонними лицами.
- **Трансляция протоколов**. Преобразование данных из одного протокола в другой для передачи их между разными платформами и операционными системами.

Уровень представления на принимающем компьютере обеспечивает распаковку, расшифровку и другие преобразования данных в формат, пригодный для пользовательских приложений и передачи данных на прикладной уровень.

На уровне представлений работают шлюзы. *Шлюз* — это устройство или программа, служащие точкой соединения между двумя разными сетями. Ниже приведен список наиболее распространенных шлюзов.

- **GSNW (Gateway Services for Netware)**. Программное обеспечение, поставляемое с операционными системами Windows NT и Windows 2000 Server. Позволяет клиентам сервера получить доступ к файлам на сервере Netware компании Novell. Этот шлюз выполняет необходимые преобразования данных между SMB (Server Message Block), используемым в системах Microsoft, и NCP (Netware Core Protocol) — протоколом разделения (совместного использования) файлов в сетях Netware.
- **Шлюз электронной почты**. Преобразует сообщения от различных несовместимых систем электронной почты в один из общепринятых форматов Internet, например в SMTP. Это позволяет передавать сообщения, например, от компьютера Macintosh с почтовым клиентом Eudora в систему Lotus Notes в сети Netware. Несмотря на отличия систем электронной почты, сообщения успешно проходят и могут быть прочитаны.
- **Шлюз SNA (Systems Network Architecture)**. Входит в состав архитектуры IBM, используемой в мэйнфреймах, таких как AS/400. С помощью программного обеспечения шлюза SNA компьютеры локальной сети могут получить доступ к файлам и приложениям мэйнфрейма.

На уровне представления работает также *редиректор* (программа, определяющая, чем должен быть обработан запрос — локальным компьютером или устройством сети).

Сеансовый уровень

Следующий уровень вниз по стеку в модели OSI — сеансовый. Протоколы этого уровня отвечают за установление сеанса связи между передающим и принимающим компьютерами. Сеансовый уровень устанавливает и разрывает диалоги приложения с приложением. На этом же уровне устанавливаются *точки проверки* для синхронизации потока данных к приложению, т.е. в потоке данных размещаются маркеры. Если в канале связи произошел сбой, то повторно передаются только данные, начиная с последнего маркера, или *точки проверки*.

На сеансовом уровне проверяется режим связи — дуплексный или полудуплексный. В дуплексном режиме осуществляется двунаправленная коммуникация, т.е. каждая сторона может быть передающей и принимающей одновременно. Полудуплексный режим тоже может быть двунаправленным, однако в один момент времени сигнал может передаваться только в одном направлении.

Коммуникация в дуплексном режиме похожа на разговор по обычному телефону. Обе стороны могут говорить одновременно и при этом слышать, что говорит другой. В то же время полудуплексный режим похож на двустороннюю радиосвязь: когда один из участников связи держит кнопку микрофона, он может говорить, но не может слышать, что говорит другой. Другими словами, в полудуплексном режиме сигналы могут передаваться в обоих направлениях, но не одновременно.

Замечание

Режим *однонаправленной* коммуникации, в котором сигналы могут проходить только в одном направлении, называется *симплексным*. Наиболее очевидные примеры симплексной коммуникации — системы радиовещания и телевидения. В появившихся в последнее время системах "интерактивного телевидения" осуществляется двунаправленная коммуникация. Многие компании кабельного телевидения активно модернизируют свою инфраструктуру для поддержки двунаправленных режимов.

На сеансовом уровне выполняются многие функции, например установлены правила обмена данными между приложениями на протяжении сеанса. Это похоже на работу спортивного судьи, который должен проследить, чтобы оба участника состязания знали правила игры и придерживались их, как минимум, на протяжении сеанса.

Что еще делает такой занятой уровень? Сеансовый уровень определяет категории (приоритеты) услуг и генерирует сообщения о неполадках у себя и на вышестоящих уровнях.

На сеансовом уровне используется два протокола.

- **Интерфейс NetBIOS (Network Basic Input/Output System)**. В режиме сеанса NetBIOS отвечает за установление соединения между двумя компьютерами, за обработку длинных сообщений и за обнаружение и устранение ошибок. На этом уровне приложение освобождается от необходимости учитывать все детали работы сети.
- **Интерфейс Winsock (Windows Sockets)**. Обрабатывает запросы ввода-вывода для приложений Internet в среде Windows. Интерфейс Winsock происходит от интерфейсных сокетов UNIX, которые использовались для установки соединения и обмена данными между двумя программными процессами на одном и том же компьютере или в сети.

На сеансовом уровне могут также выполняться задачи обеспечения безопасности и распознавания имен.

Транспортный уровень

Этот уровень является весьма важным элементом сетевой коммуникации. На транспортном уровне выполняется несколько функций. Главная задача — обеспечение сквозного контроля ошибок. Протоколы транспортного уровня обрабатывают структурированные сообщения.

На транспортном уровне отслеживается целостность и последовательность пакетов данных и обрабатываются дубликаты пакетов. Принимающая система с помощью

транспортного уровня может отправить на передающий компьютер подтверждение о приеме пакета. Эта операция выполняется, если на транспортном уровне для передачи сообщения используется *протокол с установлением логических соединений.*

Существует два типа протоколов транспортного уровня: *протоколы с установлением логических соединений* и *протоколы без установления соединения.* Важными атрибутами транспортного уровня являются также *разрешение имен*, *порты* и *сокеты.*

Протоколы с установлением логических соединений

К этому типу принадлежит TCP, использующийся на транспортном уровне как часть стека протоколов TCP/IP. Служебные программы протоколов этого типа перед передачей данных устанавливают логическое соединение. Для проверки получения данных используется механизм *подтверждения.*

Приведем такую аналогию. Если вам нужно послать по почте своему другу ценный пакет, то это можно сделать двумя способами. Первый — позвонить ему и сообщить, что выслан пакет. Это похоже на то, что делает протокол с установлением соединения: перед отправкой пакета устанавливается соединение. Второй способ — послать заказной пакет. В этом случае почтовая служба уведомит вас об успешном получении пакета адресатом. Эта операция тоже выполняется протоколом с установлением соединения: на передающий компьютер посылается *подтверждение* успешного приема пакета.

Протоколы без установления логического соединения

К протоколам этого типа принадлежит UDP (User Datagram Protocol), входящий в состав пакета TCP/IP. Работа протоколов этого типа похожа на обычную почтовую службу. Отправляя письмо, человек полагает, что оно дойдет до адресата, однако подтверждения того, что это действительно произошло, нет.

Протоколы без установления соединения используются для передачи не очень важных сообщений, а также в том случае, если сообщение достаточно короткое и при его потере пользовательское приложение может послать повторный запрос. Например, UDP используется для передачи широковещательных сообщений всем компьютерам подсети.

Несмотря на низкую надежность, протоколы без соединения все же имеют некоторые преимущества: их простота и скорость передачи обусловливают более низкую стоимость коммуникации.

Разрешение имен

Еще одной обязанностью транспортного уровня является разрешение имен (узлов) компьютеров, т.е. отображение их имен на логические сетевые адреса. Как TCP/IP, так и IPX/SPX присваивают сетевым компьютерам логические имена, а для идентификации компьютеров в сети используют присвоенные им логические адреса.

На транспортном уровне работает служба DNS (Domain Name System), которая вместе с другими службами разрешения имен рассматривается в главе 9, "Самая глобальная сеть — Internet".

Порты и сокеты

В отличие от старых операционных систем (например, MS DOS), современные сетевые операционные системы являются *многозадачными.* Это позволяет пользователям выполнять несколько сетевых программ одновременно. Например, пока Web-броузер обращается к Web-узлу, можно выгружать из почтового ящика электронные письма.

На транспортном уровне есть механизмы разделения ответа броузеру от приходящих по сети одновременно с ним электронных сообщений. Чтобы различить их, в протоколах TCP и UDP используются порты. (Не путайте с портами устройств, в частности компьютера! Здесь говорится о логических портах и сокетах.)

Номера портов связаны с сетевыми адресами. В главе 9, "Самая глобальная сеть — Internet", подробно рассматриваются IP-адреса, используемые протоколом TCP/IP для маршрутизации данных. Сейчас вам нужно лишь знать, что IP-адрес, представляющий собой логический сетевой адрес компьютера, состоит из двух частей: адреса сети и адреса компьютера в сети.

Близкая аналогия IP-адреса — название улицы и номер дома в почтовом адресе: название улицы позволяет найти нужную улицу, а номер дома — нужный дом. То же самое и в IP-адресе: адрес сети позволяет найти локальную сеть, в которую входит компьютер, а адрес компьютера — конкретный компьютер в локальной сети. Однако на компьютере может выполняться несколько приложений и нужно решить, какому из них адресовано сообщение. Это делают протоколы транспортного уровня (например, TCP или UDP), которые присваивают каждому приложению номера портов, чтобы сообщение приложению А не попало к приложению Б.

Сетевой уровень

Этот уровень отвечает за доставку пакетов данных адресату. На нем выполняется *маршрутизация* пакетов. Сетевой уровень можно сравнить с штурманом, планирующим наиболее эффективный путь корабля, или самолета. На сетевом уровне работает большинство протоколов маршрутизации (рассматриваются в главе 9, "Самая глобальная сеть — Internet"). На этом уровне также обрабатываются приоритеты типов данных (основа службы QoS — Quality of Service), обеспечивающие выделение сетевых ресурсов для широкополосных приложений, таких как передача видеосигналов в реальном времени.

Устройства сетевого уровня

Устройства, работающие на сетевом уровне, включают маршрутизаторы и *коммутаторы сетевого уровня*, т.е. уровня 3. (Как вы помните, уровни нумеруются снизу, поэтому сетевой уровень имеет номер 3.) Эти устройства сетевого соединения подробно рассматриваются в главе 7, "Физические компоненты сетей".

Канальный уровень

Уровень 2 (канальный уровень) делится на следующие два подуровня:

- MAC (Media Access Control) — управление доступом к сети;
- LLC (Logical Link Control) — управление логическими связями.

MAC-адресация

Подуровень MAC работает с физическими адресами, которые называются *MAC-адресами*. В сетях Ethernet и Token Ring MAC-адреса представляют собой шестнадцатеричные числа, записанные в микросхему сетевого адаптера.

MAC-адрес сети Ethernet (иногда его называют адресом Ethernet) — это 12 шестнадцатеричных цифр, каждая пара из которых отделена двоеточием (например, 17:A4:2C:43:2F:09).

Эти 12 шестнадцатеричных цифр представляют двоичное число длиной 48 бит (или 6 байт). Первые три байта содержат код производителя, присвоенный организацией

IEEE (Institute of Electrical and Electronics Engineers). Последние три байта присваиваются производителем.

Замечание

MAC-адрес, или физический адрес, иногда называют адресом устройства. Он отличается от логического адреса (т.е. IP-адреса в сети TCP/IP) тем, что его нельзя изменить. Логический адрес присваивается программным обеспечением, изменить его очень просто. Оба адреса служат для идентификации компьютера в сети. Логический адрес похож на название улицы, которое можно изменить указом городских властей. MAC-адрес аналогичен координатам широты и долготы, которые всегда остаются неизменными.

Теоретически во всем мире не должно быть двух сетевых адаптеров с одинаковыми MAC-адресами. Однако на практике иногда происходят ошибки у производителей, присваивающих адаптерам уже использованные адреса. Кроме того, некоторые поставщики исчерпали выделенные им номера и начали нумерацию сначала. Повторяющиеся MAC-адреса вызывают проблемы, если два сетевых адаптера с одинаковым MAC-адресом принадлежат одной и той же сети, как два дома с одинаковыми номерами на одной и той же улице. В этом случае почтальон не будет знать, в какой дом нести письмо с этим адресом.

Если два сетевых адаптера в одной и той же сети имеют одинаковый адрес, то нужно заменить один из них или изменить у одного MAC-адрес. В сетевых адаптерах некоторых поставщиков MAC-адрес можно изменить программно — с помощью "перезаписываемой" микросхемы.

Метод сетевого доступа, управляющий доступом компьютеров к сети, выполняется на подуровне MAC. Принципы работы некоторых методов сетевого доступа рассматриваются в главе 4, "Методы сетевой коммуникации".

Подуровень LLC и логическая топология

На подуровне LLC определяется логическая топология сети. Как уже упоминалось, она может не совпадать с физической топологией. Подуровень LLC отвечает также за связь (или интерфейс) между подуровнем MAC и расположенным выше сетевым уровнем.

Устройства канального уровня

На канальном уровне работают *мосты* и *коммутаторы уровня 2* (которые называют также *коммутирующими концентраторами*). Оба эти устройства рассматриваются в главе 7, "Физические компоненты сетей".

Физический уровень

И наконец, уровень 1 — физический. Здесь данные и заголовки, поступившие со всех верхних уровней, транслируются в сигнал, передаваемый в сеть. Протоколы физического уровня преобразуют все эти нули и единицы в электрические импульсы, которые по проводам или по воздуху отправятся в далекое путешествие.

Физический уровень имеет дело с различными аспектами формирования сигналов, включая следующие:

- аналоговые и цифровые сигналы;
- модулированные и немодулированные сигналы;
- синхронные и асинхронные методы передачи;
- мультиплексирование.

В главе 4, "Методы сетевой коммуникации", подробно рассматриваются методы формирования сигналов и их характеристики.

Протоколы физического уровня имеют дело с физической топологией сети, в отличие от протоколов канального уровня, имеющих дело с логической топологией. В главе 2, "Классификация компьютерных сетей", описаны наиболее распространенные типы физической топологии локальных сетей — шина, звезда, кольцо и ячейки.

Устройства физического уровня (сетевые адаптеры, повторители и концентраторы) обрабатывают электрические сигналы. Концентраторы делятся на пассивные, активные и интеллектуальные. Примером может служить сетевой концентратор Token Ring, который называется MSAU (Multistational Access Unit). В некоторых источниках это название пишется как MAU. Обратите внимание на то, что к концентраторам не относятся *коммутирующие концентраторы*, поскольку они работают на канальном уровне.

Сетевые адаптеры

Представляют собой базовый компонент сетевого оборудования. При подключении компьютеров к сети они необходимы *почти* всегда. Однако в некоторых случаях компьютер в сети может обойтись без сетевого адаптера; например, при удаленном доступе, когда компьютер подключен к сети посредством модема и телефонной линии. Еще один пример — простое соединение двух компьютеров с помощью кабеля последовательной связи без модемов. В общем случае сетевой адаптер подготавливает и передает данные в среду сети.

Существует много различных типов сетевых адаптеров. Выбрать оптимальный довольно сложно. При выборе сетевого адаптера необходимо учитывать ряд аспектов.

- **Архитектура сети**. Адаптер должен быть предназначен для работы с конкретной архитектурой, используемой в сети. Например, адаптеры Token Ring не работают в сетях Ethernet.
- **Тип носителя сигналов**. В Ethernet может использоваться тонкий или толстый коаксиальный кабель, витая пара или волоконно-оптический кабель, для подключения к которым в сетевом адаптере должен быть предусмотрен соответствующий разъем. Если используется беспроводное соединение (инфракрасный луч, лазер, радиоканал), в адаптере должна быть предусмотрена возможность подключения к соответствующему каналу.
- **Шина компьютера**. В зависимости от типа шины компьютера, выделяются соответствующие типы сетевых адаптеров — PCI, ISA и PC Card.

Замечание

Желательно приобрести комбинированный адаптер с разъемами для двух или трех типов кабелей Ethernet. Это очень пригодится в случае модернизации сети, например при замене тонких коаксиальных кабелей на витые пары.

- **Скорость передачи**. Пропускная способность сетевого адаптера должна соответствовать пропускной способности других компонентов сети. Например, Ethernet, в которой используются неэкранированные витые пары категории 5, может иметь пропускную способность 10 Мбит/с или 100 Мбит/с. Сеть Token Ring с кабелями типа IBM может иметь пропускную способность 4 Мбит/с или 16 Мбит/с.

Замечание

Сетевые адаптеры Ethernet с разъемом для неэкранированной витой пары могут иметь пропускную способность 10, 100 и 10/100 Мбит/с. Адаптер на 10/100 Мбит/с дороже, однако его преимущества очевидны. Если адаптер подключается к концентратору с пропускной способностью 100 Мбит/с, то его пропускная способность должна быть 100 или 10/100, но не 10 Мбит/с, иначе адаптер окажется несовместимым и работать не будет.

Сетевые трансиверы

Слово *transceiver* состоит из двух слов: *transmit* (передавать) и *receive* (принимать). В русском языке трансивер иногда называют *приемопередатчиком*. В сети 10Base5 (толстой сети) используется *внешний трансивер*, который представляет собой устройство, подключенное к сетевому адаптеру с помощью разъема AUI (другое название — разъем DIX). Разъем AUI — это 15-контактный разъем типа DIN. С его помощью можно подключать компьютер к различным типам носителей путем присоединения внешнего трансивера к кабелю желаемого типа.

Трансиверы используются всеми сетевыми адаптерами. В сетях 10BaseT, 10Base2 и 100BaseT трансивер встроен в сетевой адаптер.

Повторители

Усиливают сигналы, прошедшие большое расстояние и ослабленные вследствие неизбежного *затухания*. Применение повторителей позволяет проложить сетевой кабель на значительно большее расстояние, чем без них.

Повторители не фильтруют сигналов. Они передают дальше как данные, так и шум. Поэтому на линии можно установить лишь ограниченное количество повторителей. Использование повторителей в сети с коаксиальными кабелями обусловливается правилом 5-4-3, которое рассматривается в главе 5, "Локальные сети".

Концентраторы

Служат центральной точкой соединения. Большинство концентраторов фактически являются *многостанционными повторителями*. Обычно повторитель имеет только два порта, а концентратор — от четырех до двадцати и больше. Чаще всего концентраторы можно встретить в сетях Ethernet 10BaseT и 100BaseT, однако в других архитектурах они тоже иногда используются.

Существует три базовых типа концентраторов.

- **Пассивные**. Служат лишь точкой физического соединения. Они не потребляют электрическую энергию, потому что не усиливают и не фильтруют сигнал, а всего лишь пропускают его через себя. В настоящее время используются редко.
- **Активные**. Должны быть подключены к источнику энергии, потому что, прежде чем передать сигнал в другие порты, усиливают его. Активные концентраторы фактически представляют собой повторители с несколькими выходами. Это наиболее распространенный тип концентраторов в настоящее время. Концентраторы Ethernet потребляют электрическую энергию и, следовательно, причисляются к типу активных.
- **Интеллектуальные**. Эти устройства работают как активные концентраторы, однако дополнительно содержат микросхему, выполняющую диагностические функции. Несмотря на то что они чаще всего дороже активных концентраторов, они очень полезны при устранении неполадок.

Устройство, которое часто называют концентратором Token Ring фактически является устройством MSAU. Уникальной особенностью MSAU является то, что топологически оно имеет внутри себя логическое кольцо. Если соединить несколько устройств MSAU, как показано на рис. 3.5, то образуется непрерывный внешний кольцевой маршрут, по которому проходит сигнал.

Модель DoD

Хотя модель OSI широко распространена, это отнюдь не самая первая сетевая модель и далеко не единственная. Модель DoD (иногда ее называют моделью TCP/IP) была разработана в 70-х годах, т.е. приблизительно на десять лет раньше, чем OSI. Расшифровывается DoD как Department of Defense (Министерство обороны США).

Модель DoD разрабатывалась вместе с протоколом TCP/IP как часть проекта ARPAnet. Это более простая модель, чем OSI. Она содержит только четыре уровня, которые можно приближенно отразить на семь уровней модели OSI. Как показано на рис. 3.6, верхний и нижний уровни модели DoD объединяют функции нескольких уровней модели OSI.

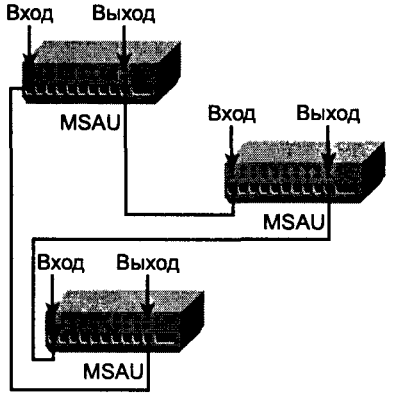


Рис. 3.5. В сети Token Ring несколько MSAU образуют для сигнала непрерывный кольцевой путь

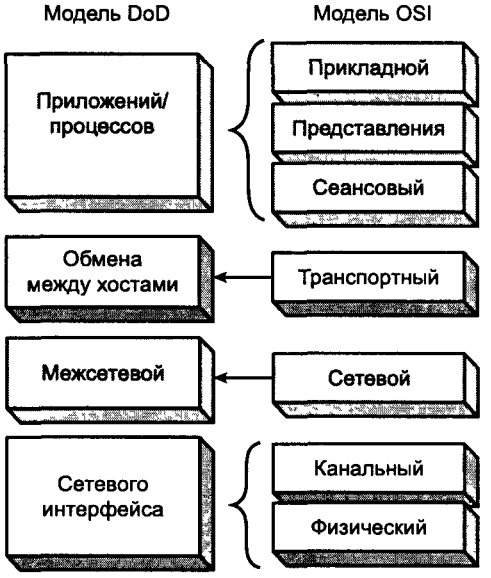


Рис. 3.6. Соответствие четырех уровней модели DoD уровням модели OSI

Уровни модели DoD выполняют описанные ниже функции.

- **Уровень приложений/процессов**. Верхний уровень модели DoD выполняет функции трех верхних уровней модели OSI: прикладного, представления и сеансового. В источниках по TCP/IP можно встретить утверждение, что уровень приложений (прикладной) шифрует данные, создает точки проверки и управляет сеансом связи. Если вы будете помнить, что речь идет *не* о прикладном уровне модели OSI, то избежите путаницы.

- **Уровень обмена между хостами (транспортный уровень)**. Во многих источниках, включая четырехуровневые диаграммы DoD, этот уровень называется так же, как соответствующий ему уровень модели OSI — транспортный. На этом уровне работают протоколы TCP, UDP и служба DNS.
- **Межсетевой уровень**. Этот уровень довольно точно соответствует сетевому уровню модели OSI. На межсетевом уровне выполняется маршрутизация сигнала на основе логических адресов. Протокол ARP (Address Resolution Protocol) преобразует логические адреса в MAC-адреса. Это преобразование необходимо потому, что расположенные ниже уровни могут работать только с MAC-адресами.
- **Уровень сетевого интерфейса** Этот уровень выполняет функции канального и транспортного уровней модели OSI На уровне сетевого интерфейса работают протоколы физического и канального уровней стандартных реализаций Ethernet и Token Ring.

Модели поставщиков

Некоторые поставщики сетевых операционных систем используют для описания работы компонентов этих систем собственные сетевые модели В качестве примера на рис. 3.7 показана сетевая модель Microsoft Windows для Windows NT/2000.

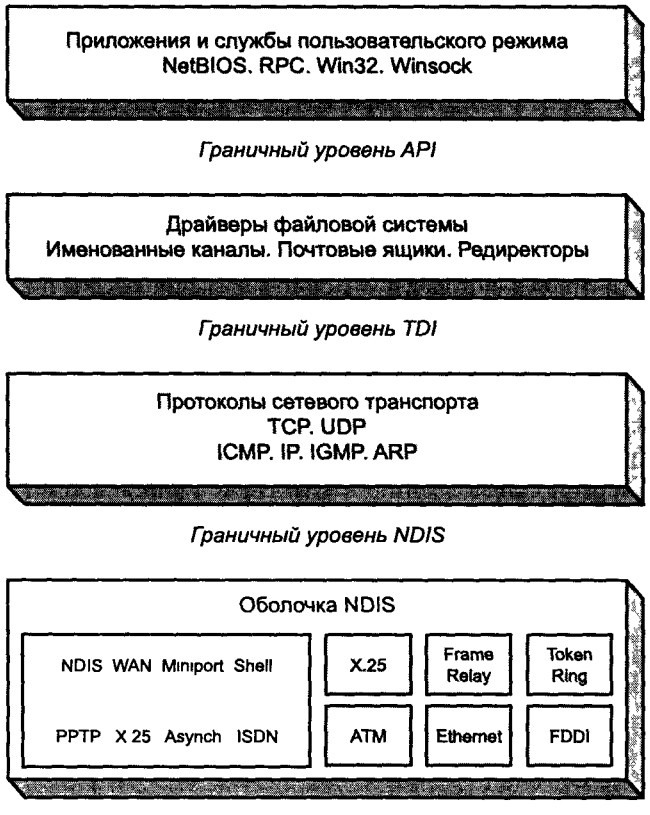


Рис 3 7 Модель сетевой коммуникации, разработанная компанией Microsoft для сетей Windows

Как видно из рис. 3.7, непосредственно отразить модель Microsoft на другие модели довольно сложно. В эту модель входят новые типы уровней, названные *граничными уровнями*. Они служат интерфейсом между фактическими уровнями сетевых компонентов. Граничные уровни имеют открытые спецификации, в то время как лежащие между ними компонентные уровни специфичны для каждой операционной системы.

Сетевые стандарты и спецификации

Компоненты сетей стандартизируются и специфицируются не только сетевыми моделями. Многочисленные организации разрабатывают и публикуют спецификации сетевого оборудования и программного обеспечения. Конечно, спецификации не являются *законом*. Организации, разрабатывающие стандарты, не входят в состав правительства и не могут принуждать к соблюдению стандартов. Поставщик может отклоняться от стандартов как ему заблагорассудится, однако это не в его интересах. Собственные продукты, работающие только с продуктами этого же поставщика, непопулярны. В первые годы развития сетевых технологий производители могли не обращать внимания на стандарты, однако в настоящее время совместимость с другими продуктами является одним из основных требований.

Зачем нужна стандартизация

Организация ISO (`www.iso.ch`) определяет стандарты как "документированные соглашения, содержащие технические спецификации, или другие точные критерии, которых следует придерживаться в качестве правил, директив или необходимых параметров, определяющих соответствие материалов, продуктов, процессов и услуг своему назначению".

Требования рынка — весьма существенный фактор, побуждающий поставщиков придерживаться стандартов, однако такая политика приносит и другие преимущества. Например, стандарты облегчают процесс разработки и производства коммерческих продуктов. С точки зрения потребителя, стандартизация обеспечивает надежность и качество продуктов и услуг.

Организации, учреждающие стандарты

Признанным органом стандартизации является ISO, однако это далеко не единственная организация, разрабатывающая и публикующая стандартизирующие спецификации на компьютеры и сетевые компоненты. Ниже приведен список основных международных органов стандартизации, которые описываются далее в главе.

- ISO.
- IEC.
- ITU.
- IETF.
- IEEE.

Организация ISO

ISO (International Standardization Organization) представляет собой всемирную федерацию национальных органов стандартизации. В нее входят по одному полномочному представителю более чем от 100 стран. ISO была создана в 1947 году для разра-

ботки международных стандартов в самых разных областях. Один из стандартов ISO, с которым люди сталкиваются на протяжении многих лет, — "номер ISO" на коробках с фотопленкой, означающий светочувствительность пленки. Другой пример работы ISO — международные коды стран.

ISO тесно сотрудничает с другими международными организациями, такими как IEC (International Electrotechnical Commission), WTO (World Trade Organization) и ITU (International Telecommunications Union).

Подробную информацию об ISO можно найти на ее официальном Web-узле по адресу: `www.iso.ch`.

Организация IEC

IEC (International Electrotechnical Commission — Международная комиссия по электротехнике) существует с 1906 года, т.е. дольше чем ISO, однако ее специализация более узкая. В то время как ISO учреждает стандарты любого вида, целью IEC является стандартизация в области электротехники и электроники.

В состав IEC входят 47 национальных комиссий. В 1967 году IEC заключила соглашение с ISO о совместной разработке стандартов и спецификаций.

Официальный Web-узел IEC:
`www.hike.te.chiba-u.ac.jp/ikeda/IEC/home.html`.

Организация ITU

ITU (International Telecommunications Union — Международный союз телекоммуникаций) занимается финансированием конференций, публикацией документов и учреждением стандартов на продукты и услуги в области телекоммуникации.

На Web-узле ITU по адресу `www.itu.int` приводится информация о структуре и деятельности этой организации.

Организация IETF

IETF (Internet Engineering Task Force) входит в состав IAB, который, в свою очередь, является технической консультативной группой в составе ISOC (Internet Society).

Организация IETF разделена на *рабочие группы*, каждая из которых занимается различными вопросами стандартизации Internet. Членство в IETF открытое, участие в ней может принять любая заинтересованная организация.

Основной задачей групп IETF является разработка и подача проектов Internet, которые затем преобразуются в официальные документы RFC (Requests for Comments — запросы на комментарии). Документы RFC, пройдя процесс официального утверждения, становятся стандартами Internet.

Документы RFC и стандарты Internet

Как будущий специалист по сетям, вы еще не раз встретите выражение "RFC*номер*", служащее ссылкой на более подробную информацию о параметрах сетевых служб и протоколов. Эти службы и протоколы включают такие элементы:

- реализация DNS (Domain Name System);
- расширения TCP/IP;
- спецификации программного обеспечения NAT (Network Address Translation).

Хотя обычно документы RFC исходят от IETF, любая заинтересованная организация может подать свои предложения RFC. Не каждый документ RFC является стандартом. Чтобы стать стандартом, он должен пройти три этапа:

- предложение стандарта;
- проект стандарта;
- стандарт Internet.

Существует даже документ RFC 2226, "Инструкция авторам", содержащий информацию о том, как писать и форматировать проект. Поданный проект поступает на рассмотрение в IESG (Internet Engineering Steering Group), входящую в состав IETF. Более подробная информация об этом процессе содержится на Web-узле IETF по адресу: `www.ietf.org/home.html`.

Если проект одобрен IESG, он редактируется и публикуется. Редактор RFC, нанятый организацией ISOC, утверждает и публикует проект RFC. Редактор также отвечает за окончательную редакцию документов. Головная страница редактора RFC находится по адресу: `www.rfc-editor.org`.

После рецензирования исполнительным комитетом и техническими экспертами каждый документ RFC причисляется к одной из следующих категорий:

- **Required Status** — соблюдение обязательно;
- **Recommended Status** — соблюдение настоятельно рекомендуется;
- **Elective Status** — соблюдение рекомендуется, но не обязательно;
- **Limited Use Status** — не предназначен для всеобщей реализации;
- **Not Recommended Status** — применять не рекомендуется.

Если вам нужна более подробная информация о процессе рассмотрения и принятия документов RFC, можете выгрузить документ RFC 2026, находящийся по адресу: `ftp://ftp.isi.edu/in-notes/rfc2026.txt`.

Организация IEEE

IEEE (Institute of Electrical and Electronics Engineers — Институт инженеров по электротехнике и электронике) занята содействием обмену информацией и разработкой стандартов и спецификаций для нижних уровней сетевых технологий (т.е. физического и канального).

Особый интерес для специалистов в области сетевых технологий представляют спецификации, составляющие проект IEEE 802. Его название отражает дату заседания комитета: число 80 означает год (1980), а 2 — месяц (февраль). Ниже перечислены стандарты комитета 802, определяющие реализацию физических и канальных протоколов и других сетевых компонентов нижнего уровня.

- **802.1**. Введение в стандарты: управление локальными и городскими сетями; мосты подуровня MAC; алгоритм Spanning-Tree, предотвращающий *зацикливание мостов.*
- **802.2**. LLC (Logical Link Control). Целью этих спецификаций является предотвращение "забивания" принимающего компьютера отправителем. Стандарт определяет разделение канального уровня OSI на два подуровня: LLC и MAC, из которых LLC обеспечивает интерфейс подуровня MAC и сетевого уровня.

- **802.3**. CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением конфликтов). Эта спецификация определяет использование в Ethernet метода доступа к сети (CSMA/CD). Спецификация устанавливает также стандарт на формат пакетов Ethernet. В первоначальном виде спецификация определяла использование в шине коаксиального кабеля, однако позже в спецификацию была включена архитектура 10BaseT (топология звезды) на основе витой пары.
- **802.4**. Token Bus. Спецификация устанавливает стандарты на реализацию физической и логической шинной топологии с использованием 75-омного коаксиального телевизионного или волоконно-оптического кабеля с методом доступа на основе маркеров.
- **802.5**. Token Ring. Спецификация определяет физические стандарты и метод доступа для топологии физической звезды и логического кольца с использованием экранированных и неэкранированных витых пар и доступа на основе маркеров. Этот стандарт основан на технологии Token Ring.
- **802.6**. Городские сети. Спецификация устанавливает стандарты на сети, которые больше локальных, но меньше глобальных.
- **802.7**. Широкополосные системы. Спецификация предназначена для сетей, использующих широкополосные передающие системы, такие как абонентское телевидение, в котором разные сигналы передаются на разных частотах по одному кабелю методом FDM (Frequency Dividing Multiplexing — мультиплексная передача с частотным разделением или уплотнением каналов).
- **802.8**. Волоконная оптика. Спецификация предназначена для сетей на основе волоконно-оптических кабелей, включая FDDI (Fiber Distributed Data Interface).
- **802.9**. Совместная передача голоса и данных. Специфицируется передача голоса и данных посредством сети ISDN (Integrated Services Digital Network).
- **802.10**. Безопасность локальных сетей. Специфицируются методы безопасного соединения сетей VPN (Virtual Private Network) посредством общедоступной сети Internet.
- **802.11**. Беспроводная связь. Специфицируется реализация беспроводных (некабельных) локальных сетей.
- **802.12**. 100 VG AnyLAN. Этот стандарт определяет требования к методу доступа к сети на основе приоритетов, разработанному компанией Hewlett Packard с целью объединения преимуществ технологий Ethernet, Token Ring и ATM в быстродействующей локальной сети.

Материалы IEEE (включая каталог стандартов, на которые можно подписаться) находятся по адресу: `standards.ieee.org`.

Резюме

В этой главе рассмотрены концепции, служащие основой построения компьютерных сетей. Глава начинается с базовых "догматов" компьютерных технологий: рассматриваются двоичная, шестнадцатеричная и десятичная системы счисления и раскрываются преимущества двоичной системы для хранения и обработки данных. В главе описано, как при передаче по сети данные предварительно разбиваются на не-

большие части, как в процессе передачи данных участвуют различные уровни сети и как поддерживается целостность передаваемой по сети информации.

В главе рассмотрено также назначение сетевых моделей и отображение четырех уровней модели DoD на семь уровней модели OSI. Представлены преимущества стандартизации сетевого оборудования и программного обеспечения. Рассмотрены некоторые стандарты, такие как документы RFC и спецификации IEEE 802, которые вы обязательно встретите в своей практической деятельности.

В следующей главе мы вернемся к самому началу, т.е. рассмотрим сигналы, представляющие передаваемые по сети данные. Мы обсудим типы и параметры сигналов, методы доступа к сети и то, каким образом сигналы от многочисленных компьютеров смогут не заблудиться, не перепутаться и каждый из них достигнет своей цели.

Рекомендуемые источники

Более глубокое изложение о систем счисления можно найти в руководстве *A Practical Guide to Binary, Decimal and Hexadecimal Numbers* по адресу:
`www.myhome.org/pg/numbers.html`.

Материалы по сетевым стандартам и спецификациям находятся на общедоступном Web-узле WSSN (World Standards Services Network), принадлежащем органам стандартизации всего мира, по адресу: `www.wssn.net/WSSN`.

Хороший краткий учебник по модели OSI с контрольными вопросами есть на Web-узле `www.lex-con.com/osimodel.htm`.

Диаграмму отображения протоколов на модель OSI можно найти по адресу:
`www.lex-con.com/osimodel.htm`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Как называется система счисления, в которой для представления числовых значений используется 16 цифр?
   - **а.** Десятичная.
   - **б.** Шестнадцатеричная.
   - **в.** Двоичная.
   - **г.** Машинный код.
2. Как называется цифра в двоичной системе счисления?
   - **а.** Бит.
   - **б.** Байт.
   - **в.** q-бит .
   - **г.** Гигабайт.
3. Какое число в десятичном исчислении равно двоичному числу 10010001?
   - **а.** 256.
   - **б.** 128.
   - **в.** 145.

г. 64.

4. Как называются небольшие части данных, на которые компьютер разбивает данные, прежде чем передать их в сеть?

   а. Шестнадцатеричные числа.

   б. Пакеты.

   в. Заголовки.

   г. Биты.

5. Как называется компонент, который помещается в трейлер пакета данных с целью обнаружения ошибок?

   а. Проверочный бит.

   б. Кадр.

   в. UDP.

   г. CRC.

6. "Схематическое описание системы, теории или явления, включающее его известные или изучаемые свойства и используемое в целях дальнейшего изучения его характеристик". Что здесь определяется?

   а. Протокол.

   б. Модель.

   в. Процесс.

   г. Уровень.

7. Какой уровень модели OSI разделен на два подуровня?

   а. Физический.

   б. Канальный

   в. Сетевой.

   г. Транспортный.

8. Какой уровень модели OSI не добавляет в пакет данных заголовочную информацию при продвижении пакета вниз по стеку?

   а. Физический.

   б. Канальный.

   в. Сеансовый.

   г. Прикладной.

9. Какой протокол относится к сеансовому уровню?

   а. TCP.

   б. IPX.

   в. NetBIOS.

   г. Telnet.

10. Как еще называется многостанционный повторитель?

    а. Мост.

    б. Маршрутизатор.

    в. Коммутатор.

    г. Концентратор.

Глава 4

Методы сетевой коммуникации

В предыдущих главах рассматривалось, как можно соединить компьютеры с целью передачи данных от одного из них к другому. Теперь вы знакомы с тем, как компьютеры обрабатывают данные в двоичном формате и как двоичные цифры преобразуются в электрические сигналы, которые отправляются в путешествие по сети. Эта глава посвящена основе процесса коммуникации — сигналам. Кроме того, здесь рассматриваются методы управления доступом в сетевую среду, используемые в различных архитектурах.

Сигналы

Как упоминалось раньше, существует много способов физического создания и передачи сигнала: электрические импульсы могут проходить по медному проводу, импульсы света — по стеклянному или пластмассовому волокну, радиосигналы передаются по воздуху, так же передаются и лазерные импульсы в инфракрасном, или видимом диапазоне. Преобразование единиц и нулей, представляющих данные в компьютере, в импульсы энергии называется *кодированием* (*модуляцией*).

Подобно классификации компьютерных сетей, сигналы можно классифицировать на основе их различных характеристик. Сигналы бывают следующие:

- аналоговые и цифровые;
- немодулированные и модулированные;
- синхронные и асинхронные;
- симплексные, полудуплексные, дуплексные и мультиплексные.

Аналоговые и цифровые сигналы

В зависимости от формы электрического напряжения (которую можно увидеть на экране осциллографа), сигналы делятся на аналоговые и цифровые. Скорее всего, вы уже знакомы с этими терминами, так как они довольно часто встречаются в документации различного электронного оборудования, например магнитофонов, телевизоров, телефонов и т.д.

В некотором смысле аналоговое оборудование представляет уходящую эпоху электронной техники, а цифровое — новейшую, приходящую ей на смену. Однако следует

помнить, что один тип сигналов не может быть лучше другого. Каждый из них имеет свои достоинства и недостатки, а также свои области применения. Хотя цифровые сигналы используются все более широко, они никогда не вытеснят аналоговых.

Параметры аналоговых сигналов

Аналоговые сигналы плавно и непрерывно изменяются во времени, поэтому их можно графически представить в виде плавной кривой (рис. 4.1).

В природе подавляющее большинство процессов принципиально аналоговые. Например, звук — это изменение давления воздуха, которое с помощью микрофона можно преобразовать в электрическое напряжение. Подавая это напряжение на вход осциллографа, можно увидеть график, аналогичный приведенному на рис. 4.1, т.е. можно проследить, как изменяется давление воздуха во времени.

Чтобы нагляднее представить себе аналоговую информацию, вспомните традиционный спидометр в автомобиле. Когда скорость автомобиля увеличивается, стрелка плавно проходит по шкале от одного числа к другому. Еще один пример — настройка на станцию в радиоприемнике: при повороте ручки принимаемая частота плавно изменяется.

Большинство аналоговых сигналов имеют циклический, или периодический характер, например радиоволны, представляющие собой колебания электромагнитного поля с высокой частотой. Такие циклические аналоговые сигналы принято характеризовать тремя параметрами.

- **Амплитуда**. Максимальное или минимальное значение сигнала, т.е. высота волны.
- **Частота**. Количество циклических изменений сигнала в секунду. Частота измеряется в герцах (Гц); 1 Гц — это один цикл в секунду.
- **Фаза**. Положение волны относительно другой волны или относительно некоторого момента времени, служащего началом отсчета. Фазу принято измерять в градусах, причем считается, что полный цикл равен 360 градусам.

Параметры цифровых сигналов

Другое название цифровых сигналов — дискретные Довольно часто встречается термин дискретные состояния Цифровые сигналы изменяются от одного дискретного состояния к другому почти мгновенно, не останавливаясь в промежуточных состояниях (рис. 4.2).

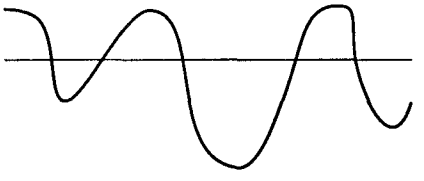


Рис. 4.1. Аналоговый сигнал представляет собой непрерывно изменяющуюся физическую величину, например электрическое напряжение или интенсивность электромагнитного поля

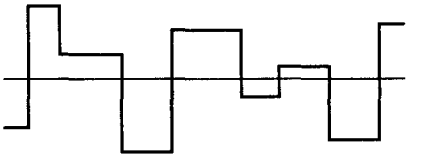


Рис. 4.2. Цифровой сигнал представляет собой последовательность фиксированных дискретных состояний

Примером цифрового сигнала могут служить показания новейшего цифрового спидометра в автомобиле (сравните с примером аналогового спидометра в предыдущем разделе). Когда скорость автомобиля увеличивается, цифры, показывающие значение скорости в километрах в час, переключаются скачками, причем величина сиг-

нала принципиально дискретна: например, между дискретными состояниями "125 км/ч" и "126 км/ч" нет промежуточных значений. Другой пример цифровой информации — новейший радиоприемник, в котором для настройки на определенную станцию пользователь вводит точное число, равное частоте радиостанции.

Сравнение аналоговых и цифровых сигналов

Компьютеры являются цифровыми машинами. Обрабатываемая ими информация представлена нулями и единицами. Двоичная цифра равна или 0, или 1, причем между ними или за их пределами нет ничего. Благодаря такой четкой определенности цифровые сигналы очень удобны для представления и передачи компьютерных данных, поэтому они используются в подавляющем большинстве сетей.

Замечание

Интересно то, что изначально аналоговую информацию можно представить в цифровом виде и наоборот. Вернемся к нашим примерам со спидометрами Обратите внимание скорость автомобиля изменяется от 125 до 126 км/ч не скачком, а плавно, т е. существуют промежуточные, дробные значения скорости. Однако в цифровом спидометре эти дробные значения игнорируются, что, впрочем, не мешает водителю, поскольку ему не нужна столь высокая точность.

Обратный пример — электроэнцефалограмма, представляющая собой аналоговый график электрической активности участков головного мозга человека Электрическая активность мозга порождается нейронами, имеющими дискретные состояния (т е в данный момент времени импульс или проходит по нейрону, или не проходит, других состояний нет) Таким образом, электроэнцефалограф преобразует дискретные (цифровые) сигналы нейронов в аналоговый сигнал.

В некотором смысле цифровые сигналы проще аналоговых. Проиллюстрируем это утверждение на примере экзамена. Если к вопросам прилагаются варианты ответов (например, А, Б, В и Г, другими словами, дискретные состояния), то оценить ответ очень легко: достаточно сопоставить его с правильным ответом. В то же время, если предметом экзамена является, например, написание эссе, такой ответ не может быть правильным или неправильным, "качество" эссе всегда находится где-то посередине, поэтому оценить его намного сложнее.

Благодаря простоте технологии цифровые сигналы имеют ряд преимуществ

- Цифровое оборудование в общем случае дешевле аналогового Например, цифровые часы намного дешевле своих аналоговых конкурентов.
- Цифровые сигналы менее чувствительны к помехам Чтобы перевести устройство из одного дискретного состояния в другое, требуется значительное воздействие В то же время на аналоговый сигнал, в силу его непрерывности, могут иметь воздействие даже самые малые помехи

Тем не менее аналоговые сигналы имеют некоторые преимущества.

- Их легко мультиплексировать, т е. передавать большое количество сигналов по одному каналу.
- Они меньше подвержены затуханию (ослаблению сигнала с увеличением расстояния), поэтому при той же мощности передающего устройства их можно передавать на большее расстояние.

В общем случае полезными являются как аналоговые, так и цифровые сигналы. Однако в компьютерных сетях цифровые сигналы позволяют достичь большего уровня безопасности, пропускной способности и надежности. Кроме того, цифровые линии значительно меньше подвержены ошибкам, чем аналоговые.

Локальные сети практически всегда основаны на передаче цифровых сигналов по кабелю. Аналоговые сигналы используются в некоторых глобальных сетях.

Модулированные и немодулированные сигналы

Важной характеристикой метода передачи является пропускная способность канала, непосредственно связанная с модулированием сигнала. Цифровой сигнал называется немодулированным, если переходы из одного дискретного состояния в другое представляют собой скачки напряжения в кабеле или другом носителе. В то же время в модулированном сигнале переход между дискретными состояниями — это изменение амплитуды так называемого несущего сигнала, представляющего собой высокочастотные колебания напряжения.

Немодулированный сигнал занимает весь канал связи. Кроме него, по каналу связи нельзя передать больше ничего. Примером немодулированных сигналов являются сигналы в кабеле Ethernet.

Если используется модулирование, то по одному каналу можно передать несколько цифровых сигналов на разных несущих частотах. Кроме того, на разных несущих частотах можно передавать не только цифровые, но и аналоговые сигналы. Примером может служить система кабельного телевидения, в которой один кабель обслуживает десятки телевизионных каналов, по каждому из которых идут разные передачи.

Немодулированные сигналы

Немодулированные сигналы довольно просты: по кабелю в один момент времени передается только один сигнал. Немодулированным чаще всего является цифровой сигнал, хотя может быть и аналоговый.

В компьютерной и коммуникационной технике применяются главным образом немодулированные цифровые сигналы. Например, компьютер обменивается немодулированными цифровыми сигналами с мониторами, принтерами, клавиатурой и т.д. Примером применения модулированных цифровых сигналов является система ISDN (Integrated Services Digital Network), в которой многие сигналы передаются на разделенных каналах по одному кабелю. Немодулированные сигналы могут передаваться в двух направлениях, т.е. на каждом конце кабеля можно установить как передатчик, так и приемник, работающие одновременно.

Модулированные сигналы

С помощью модулированных сигналов можно организовать несколько каналов связи по одному кабелю, при этом каждый канал связи может работать на своей несущей частоте, не мешая другим каналам.

Модулированные сигналы являются однонаправленными. Это значит, что сигнал передается только в одном направлении: на одном конце кабеля установлен передатчик, а на другом — приемник. Однако на одном кабеле могут одновременно работать несколько каналов в разных направлениях.

Кроме кабельного телевидения, модулированные сигналы используются в системе DSL (Digital Subscriber Line), в которой данные и голос передаются одновременно по одной и той же линии, возможно через спутник или посредством радиоволн.

Для размещения на одной линии нескольких каналов связи используются методы мультиплексирования, рассматриваемые в следующем разделе.

Мультиплексирование

Мультиплексированием называется одновременная передача многих сигналов по одной линии. На принимающей стороне мультиплексированные сигналы восстанавливаются, т.е. отделяются друг от друга. Вернемся к примеру с кабельным телевидением. В телевизор встроено устройство декодирования сигналов, которое выделяет один канал и отбрасывает остальные. Благодаря этому зритель может выбрать желаемую программу.

Во многих литературных источниках о методах мультиплексирования говорится только применительно к аналоговым сигналам, однако мультиплексировать можно и цифровые сигналы. Применяются следующие основные методы мультиплексирования:

- частотное разделение каналов (Frequency Division Method — FDM);
- временное разделение каналов (Time Division Method — TDM);
- по длине волны высокой плотности (Dense Wavelength Division Multiplexing — DWDM).

Частотное разделение каналов

При частотном разделении каналов, занимающих одну и ту же линию, каждый канал работает на своей частоте (рис. 4.3). Обычно этим методом мультиплексируются аналоговые сигналы. Чтобы при частотном разделении каналов была возможна двусторонняя коммуникация, необходимо установить на каждой стороне как мультиплексор, так и демультиплексор.



Рис. 4 3 Частотное разделение каналов

Временное разделение каналов

Обычно этот метод используется для мультиплексирования цифровых сигналов. При временном разделении каждому каналу выделяются свои промежутки времени. На принимающем конце сигналы разных каналов отделяются демультиплексором (рис. 4.4).



Рис. 4.4. Временное разделение каналов

Мультиплексирование по длине волны высокой плотности

Этот метод мультиплексирования используется при передаче сигналов по волоконно-оптическим кабелям. Сигналы каждого канала передаются световым лучом со своей длиной волны. Физически этот метод совпадает с частотным разделением каналов, так как длина волны светового луча однозначно связана с его частотой. Однако отличия аппаратных реализаций этих методов настолько велики, что они все же рассматриваются как отдельные методы. Как показано на рис. 4.5, по одному оптическому волокну могут одновременно передаваться различные данные, причем разными методами (например, SONET и ATM).

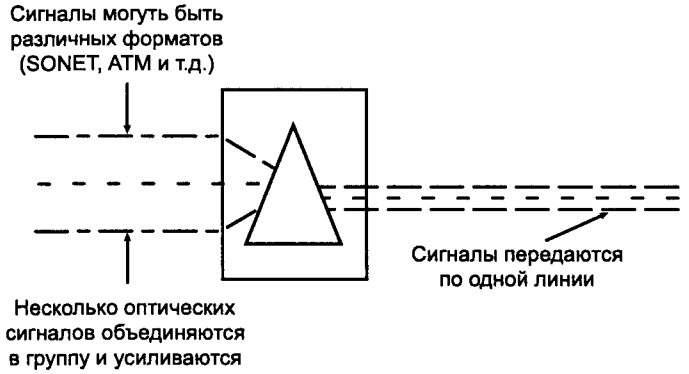


Рис. 4.5. Мультиплексирование по длине волны высокой плотности

Асинхронная и синхронная передача

Данные, заложенные в цифровом сигнале, фактически представлены изменениями дискретных состояний сигнала. Можно восстановить наши исходные нули и единицы, измеряя напряжение вольтметром в определенные моменты времени. Однако нужно точно знать, в какие именно моменты времени следует выполнять измерения. Синхронизация, т.е. согласование по времени, в коммуникационных технологиях не менее важна, чем во всех других областях нашей жизни.

В сетевых технологиях такое согласование по времени называется *битовой синхронизацией*. Электронные устройства синхронизируют отдельные биты с помощью *асинхронного* или *синхронного* методов.

Асинхронная передача

В этом методе для синхронизации используется *стартовый бит*, расположенный в начале каждого сообщения. Когда стартовый бит попадает в принимающее устройство, оно в этот момент синхронизирует свои внутренние часы с часами передающего устройства

Синхронная передача

При синхронной передаче внутренние часы передающего и принимающего устройств координируются встроенными механизмами. Например, информация о времени может быть встроена в сигналы данных. Такой метод называется синхронизацией с *гарантированным изменением состояний*. Среди синхронных методов это наиболее распространенный.

Другой синхронный метод — синхронизация с помощью *отдельного временного сигнала*, в котором информация о времени передается между передатчиком и приемником по отдельному каналу Еще один синхронный метод — *стробирование* В этом случае синхронизация выполняется с помощью специальных строб-импульсов

Симплексный, полудуплексный и дуплексный методы передачи

Каналы, по которым передаются сигналы данных, могут работать в одном из трех режимов: *симплексном*, *полудуплексном* и *дуплексном*. Отличаются эти методы направлениями, в которых передаются сигналы.

Симплексная передача

Как видно из названия, это самый простой метод передачи. Иногда его называют *однонаправленным*, потому что сигналы проходят только в одном направлении, как автомобили по улице с односторонним движением (рис. 4.6).

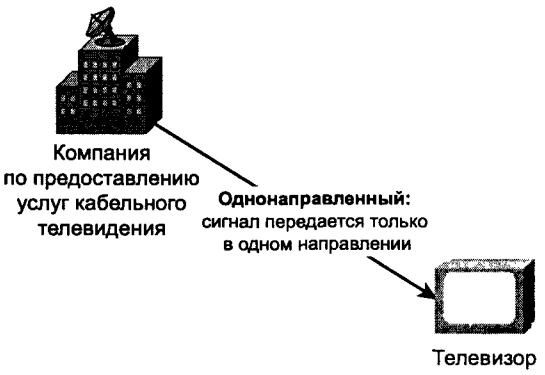


Рис 4 6 При симплексном методе передачи сигналы передаются только в одном направлении

Примером симплексной коммуникации может служить телевидение. Данные (телевизионные программы) передаются на телевизор От телевизора обратно в студию или в кабельную компанию никакие сигналы не передаются Поэтому в состав телевизора входит только *приемник* сигналов, но не передатчик.

В настоящее время все большее распространение получают системы интерактивного телевидения, позволяющие передавать сигналы не только из студии к телевизору, но и в обратном направлении. Однако кабельное оборудование большинства компаний по-прежнему поддерживает только симплексную передачу. Это создало серьезную проблему при появлении сети Internet. Существующая кабельная система оказалась способной передавать данные только в одном направлении, к пользователю.

Этот недостаток делает невозможным, например, доступ пользователя к Web-страницам, потому что броузер пользователя должен передать на Web-узел свой запрос. Кабельные компании предлагают два способа решения этой проблемы:

- передавать запросы пользователей (которые всегда намного короче, чем Web-страницы) по телефонным линиям, а Web-страницы — по телевизионным кабелям;
- установить новое кабельное оборудование с двусторонней передачей.

Большинство компаний использовали первый способ как временную альтернативу второго, более совершенного. Если оставить кабельную систему передачи симплексной, то пользователю придется нести расходы только на покупку кабельного и телефонного модемов (с пропускной способностью последнего не более 56 Кбит/с.) При этом ресурсы высокоскоростного кабельного канала будут использоваться полностью.

Многие кабельные компании сразу модернизируют свое оборудование для поддержки двусторонней коммуникации, в то время как другие все еще предоставляют только одностороннюю передачу данных Internet по телевизионному кабелю. В этих районах клиенты вынуждены использовать как кабельные, так и аналоговые модемы, подключенные к телефонной линии.

Полудуплексная передача

По сравнению с симплексной преимущества полудуплексной передачи очевидны: сигналы могут передаваться в обоих направлениях. Однако, к сожалению, эта дорога недостаточно широка, чтобы сигналы проходили в обоих направлениях одновременно. В полудуплексном методе в каждый момент времени сигналы передаются только в одном направлении (рис. 4.7).

Полудуплексный метод используется во многих системах радиосвязи, например, в устройствах связи в полицейских автомобилях. В этих системах при нажатой кнопке микрофона можно говорить, но услышать что-либо нельзя. Если пользователи нажмут кнопки микрофонов в обоих концах одновременно, то ни один из них ничего не услышит.

Замечание

Модемы являются полудуплексными устройствами. Они могут как передавать, так и принимать сигнал, но не одновременно. Однако можно создать дуплексное соединение с помощью двух модемов и двух телефонных линий.

Дуплексная передача

Работа дуплексной системы коммуникации похожа на улицу с двусторонним движением: автомобили могут двигаться в обоих направлениях одновременно (рис. 4.8).

Примером дуплексной коммуникации является обычный телефонный разговор. Оба абонента могут говорить одновременно, при этом каждый из них слышит, что говорит другой на другом конце линии (правда, при этом не всегда можно разобрать, что было сказано).



Рис 4 7. В полудуплексном методе сигналы передаются в обоих направлениях по очереди, а не одновременно

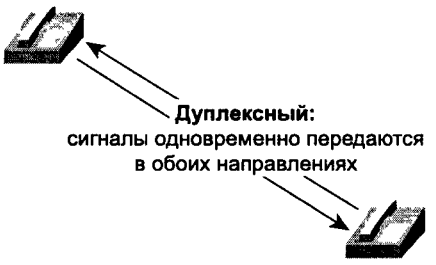


Рис 4 8 В дуплексном методе сигналы передаются в обоих направлениях одновременно

В сетевых технологиях дуплексный метод увеличивает производительность системы, потому что данные и передаются и принимаются одновременно. В дуплексном режиме работают системы DSL (Digital Subscriber Line), в которых используются двусторонние кабельные модемы. С помощью DSL можно, например, одновременно выгружать данные на свой компьютер и передавать голосовое сообщение.

Проблемы, возникающие при передаче сигналов

Сигналы, с помощью которых сообщаются компьютеры, подвержены различным помехам и ограничениям Разные типы кабелей и методы передачи обладают разной чувствительностью к помехам. В этом разделе рассматриваются вопросы, которые необходимо учитывать при устранении неполадок в сетевых соединениях

Электромагнитные помехи

Электромагнитные помехи представляют собой вторжение постороннего электромагнитного сигнала, нарушающего форму полезного сигнала. Когда в полезный сигнал добавляются внешние помехи, принимающий компьютер не может правильно интерпретировать сигнал.

Представьте себе, что вы проезжаете в автомобиле рядом с мощной промышленной установкой и слушаете в это время радио Чистый и разборчивый сигнал вдруг покрывается шумом и треском Это происходит потому, что к сигналу радиостанции добавляются сильные сигналы, создаваемые установкой, которая расположена ближе, чем радиостанция. Поэтому электромагнитные помехи иногда называют шумами

Довольно часто помехи поступают из неизвестного источника. Существует множество устройств, в которых электрические сигналы не выполняют информационные функции, а являются побочным продуктом различных производственных процессов Создаваемые ими помехи могут распространяться на расстояние вплоть до нескольких километров.

Электромагнитные помехи порождают проблемы не только в компьютерных коммуникационных технологиях В городах есть много устройств, передающих и принимающих

электромагнитные сигналы: мобильные телефоны, средства радиосвязи, телевизионные передатчики и приемники. Электромагнитные помехи могут стать причиной многих неприятностей, таких как плохое телевизионное изображение, крушение самолета вследствие нарушения связи с диспетчером, смерть пациента из-за нарушения работы медицинского оборудования и т.д. Существуют также долговременные побочные эффекты электромагнитного излучения, например рак или лейкемия могут быть вызваны длительным пребыванием человека рядом с мощным источником электромагнитных полей.

В коммуникационных технологиях особенно чувствительны к электромагнитным помехам неэкранированные медные провода. Металлическая внешняя оболочка коаксиальных кабелей в значительной степени защищает их от помех. Эту же функцию выполняет металлическая оболочка экранированной витой пары. Неэкранированная витая пара довольно сильно подвержена помехам. Совершенно нечувствительны к электромагнитным помехам волоконно-оптические кабели, потому что в них сигналами служат не электрические импульсы, а луч света. Поэтому в условиях сильных электромагнитных помех лучше всего работают волоконно-оптические каналы связи.

Радиочастотные помехи

Радиочастотные помехи представляют собой сигналы радиопередатчиков и других устройств, генерирующих сигналы на радиочастотах. К ним относятся также процессоры и дисплеи компьютеров. Радиочастотным считается электромагнитное излучение на частотах от 10 КГц до 100 ГГц. Излучение на частотах от 2 до 10 ГГц называется также микроволновым.

Влияние радиочастотных помех устраняется с помощью помехозащитных фильтров, применяемых в различных типах сетей.

Перекрестные помехи

К этому типу помех относятся сигналы проводов, расположенных на расстоянии нескольких миллиметров друг от друга. Протекающий по проводу электрический ток создает электромагнитное поле, которое генерирует сигналы в другом проводе, расположенном рядом. Довольно часто, разговаривая по телефону, можно услышать приглушенные разговоры других людей. Причиной этого являются перекрестные помехи.

Перекрестные помехи значительно уменьшаются, если скрутить два провода, как это сделано в витой паре. Чем больше витков приходится на единицу длины, тем меньше влияние помех. Применение волоконно-оптического кабеля полностью устраняет эту проблему. Внутри одной оболочки можно расположить сколько угодно оптических волокон, и они не будут мешать друг другу, потому что сигналами в них служат не электрические импульсы, а световые лучи.

Затухание сигналов

Проходя по кабелю, электрические сигналы становятся все слабее. Чем больше расстояние до источника, тем слабее сигнал. Это нетрудно представить себе, вообразив, будто вы пытаетесь что-то сказать человеку, находящемуся на некотором расстоянии от вас. Если до него 5 метров, то он услышит ваш голос (сигнал) четко и громко, однако если до него 50 метров, то он с трудом поймет, о чем вы ему кричите. Такое ослабление сигнала с расстоянием называется затуханием сигнала

Затухание является причиной того, что в спецификациях различных сетевых архитектур указывается ограничение на длину кабеля. Если это ограничение соблюдается, то эффект затухания не повлияет на нормальную работу канала связи.

Замечание

Для увеличения максимально допустимого расстояния сигнал можно *усилить*. Для усиления цифровых сигналов используются *повторители*. Аналоговые сигналы усиливают с помощью *усилителей*. Эти устройства рассматриваются в главе 7, "Физические компоненты сетей".

При увеличении частоты затухание увеличивается, потому что, чем выше частота сигнала, тем интенсивнее рассеивание его электромагнитной энергии в окружающее пространство. При увеличении частоты сам провод превращается из носителя сигнала в антенну, рассеивающую его энергию в пространство.

Сигналы в волоконно-оптическом кабеле тоже подвержены затуханию Две главные причины — поглощение светового луча примесями в стекле и рассеиваниелуча вследствие небольших изменений оптической плотности стекла, образовавшихся при его производстве. Однако волоконно-оптические кабели могут передавать сигнал на значительно большее расстояние, чем медные кабели, причем без уменьшения его мощности до недопустимого уровня.

Пропускная способность

Пропускная способность канала коммуникации обычно измеряется в мегабитах в секунду (Мбит/с). На пропускную способность влияет тип сигнала, тип среды и расстояние, на которое передается сигнал.

Понятия высокой и низкой пропускной способности весьма относительны. Например, пропускная способность Ethernet 10BaseT, равная 10 Мбит/с, кажется очень высокой по сравнению с пропускной способностью телефонного модема (50 Кбит/с), в то же время она кажется удручающе низкой по сравнению Gigabit Ethernet (1 Гбит/с) или с высокоскоростными соединениями глобальных сетей, такими как SONET и ATM.

Важным критерием при выборе типа кабеля и архитектуры сети является требующаяся (как сейчас, так и в будущем) пропускная способность.

Планирование роста сети

На этапе планирования сети необходимо помнить, что пропускная способность — это такой ресурс, которого всегда оказывается недостаточно. Покупка оборудования с более высокой пропускной способностью, чем необходимо сейчас, является хорошим вложением капитала: дополнительные затраты обязательно окупятся.

Компьютерные и коммуникационные технологии развиваются быстрыми темпами. В 1980-х годах типичные каналы глобальных сетей имели пропускную способность 10 Кбит/с, а локальных — 2,5 Мбит/с. Тогда никто даже не предполагал, что когда-нибудь понадобится передавать что-нибудь со скоростью, большей 100 Мбит/с Ведь еще не существовали такие технологии, как видеоконференции, передача голоса, или передача больших файлов, которые сейчас широко распространены.

Проложить кабель с увеличенной пропускной способностью значительно легче и дешевле, чем потом заменять кабель новым. Допустим, вы устанавливаете сеть 10BaseT, для которой достаточно кабеля категории 3 с пропускной способностью 10 Мбит/с Купив кабель ка-

тегории 3, а не категории 5, вы сэкономите несколько долларов. Однако через несколько лет, когда понадобится модернизировать сеть до 100 Мбит/с (а это случится почти наверняка), вам придется заменять все кабели. Это обойдется значительно дороже, чем если бы вы сразу купили и установили кабель категории 5.

Методы доступа к сети

Теперь, когда вы знакомы с различными типами сигналов и их параметрами, рассмотрим, каким образом сеть обрабатывает сигналы от многих компьютеров и как все они попадают в пункт назначения.

Представьте себе загруженную автомобильную дорогу. Если бы не было правил дорожного движения и контролирующих приборов, водителям пришлось бы на свой страх и риск прорываться в нужном направлении. Количество столкновений было бы намного большим, а дороги стали бы такими переполненными, что скорость движения упала бы почти до нуля.

Светофоры, дорожные знаки, полицейские на перекрестках, правила, которые мы должны выучить, чтобы получить водительские права, — все это методы доступа, определяющие, какой автомобиль должен уступить дорогу, а какой может сейчас проехать беспрепятственно. Методы доступа разрабатываются для того, чтобы упорядочить движение и чтобы каждый достиг своего пункта назначения как можно быстрее.

Аналогичная ситуация и в коммуникационных технологиях: чтобы сигналы не "налезали" друг на друга, нужны методы доступа к сети. Существует несколько различных методов доступа, соответствующих разным архитектурам и топологиям сети Наибольшее распространение получили следующие методы:

- CSMA/CD;
- SCMA/CA;
- передача маркера (эстафетный доступ);
- приоритеты запросов.

В следующих разделах рассматривается каждый из этих методов.

Метод CSMA/CD

В настоящее время самый распространенный метод управления доступом в локальную сеть — это CSMA/CD (Carrier Sense Multiple Access with Collision Detection – множественный доступ с контролем носителя и обнаружением конфликтов). Язык можно сломать, не правда ли? Поэтому название этого метода чаще всего сокращают до начальных букв, что, впрочем, не легче. Распространенность метода CSMA/CD в значительной степени обусловлена тем, что он используется в наиболее распространенной в настоящее время архитектуре Ethernet.

Это весьма быстродействующий и эффективный метод предоставления доступа к кабелю Ethernet. Чтобы понять, как он работает, рассмотрим отдельно фрагменты его названия.

- **Контроль носителя**. Когда компьютер собирается передать данные в сеть методом CSMA/CD, он должен сначала проверить, передает ли в это время по это-

му же кабелю свои данные другой компьютер. Другими словами, проверить состояние носителя: занят ли он передачей других данных.

- **Множественный доступ**. Это означает, что несколько компьютеров могут начать передачу данных в сеть одновременно.
- **Обнаружение конфликтов**. Это главная задача метода CSMA/CD. Когда компьютер готов передавать, он проверяет состояние носителя. Если кабель занят, компьютер не посылает сигналы. Если же компьютер не слышит в кабеле чужих сигналов, он начинает передавать. Однако может случиться, что кабель прослушивают два компьютера и, не обнаружив сигналов, начинают передавать оба одновременно. Такое явление называется конфликтом сигналов.

Когда в сетевом кабеле сигналы конфликтуют, пакеты данных разрушаются. Однако еще не все потеряно. В методе CSMA/CD компьютеры ждут на протяжении случайного периода времени посылают эти же сигналы повторно. Почему промежуток времени должен быть случайным? Если оба компьютера будут ждать некоторое фиксированное количество миллисекунд, то их времена ожидания могут совпасть и все повторится сначала. Компьютер, который первым повторяет передачу пакета (у которого случайный период времени оказался меньшим), как бы "выигрывает" доступ к сети в рулетку.

Вероятность конфликтов невелика, так как они происходят, только если совпадают начала пакетов, т е. весьма короткие отрезки времени Поскольку сигналы передаются с высокой скоростью (в Ethernet — 10 или 100 Мбит/с), производительность остается высокой.

Реализация метода CSMA/CD определяется спецификациями IEEE 802.3.

Метод CSMA/CA

Название метода расшифровывается как Carrier Sense Multiple Access with Collision Avoidance (множественный доступ с контролем носителя и предотвращением конфликтов) Как видите, по сравнению с предыдущим методом заменено лишь одно слово — "обнаружение (конфликтов)" на "предотвращение". Ничем не отличается также первый шаг при попытке передать пакет: компьютер прослушивает кабель и определяет, свободен ли он.

Однако CSMA/CA — более "недоверчивый" метод. Если компьютер не находит в кабеле других сигналов, он не делает вывод, что путь свободен и можно отправлять свои драгоценные данные Вместо этого компьютер сначала посылает сигнал запроса на передачу — *R*TS (*R*equest to Send). Этим он объявляет другим компьютерам, что намерен начать передачу данных Если другой компьютер сделает то же самое в тот же момент времени, то произойдет конфликт сигналов *R*TS, а не пакетов данных. Таким образом, пакеты данных никогда не смогут конфликтовать Это называется предотвращением конфликтов

На первый взгляд, метод с предотвращением конфликтов значительно совершеннее, чем с обнаружением Однако его производительность ниже из-за того, что дополнительно к данным приходится посылать сигналы *R*TS, подавляющее большинство которых не нужны Фактически количество поступающих на кабель сигналов почти удваивается.

Метод CSMA/CA используется в сетях AppleTalk.

Замечание

Как CSMA/CD, так и CSMA/CA называются *конкурентными* методами, потому что в них сигналы разных компьютеров как бы конкурируют, или состязаются за доступ к кабелю.

Передача маркера

Существует ли метод доступа, работающий вообще без конфликтов сигналов? Такой метод существует: это метод с передачей маркера.

Метод с передачей маркера неконкурентный В нем два компьютера не могут начать передавать сигнал одновременно. Работа метода похожа на семинар, участник которого не может начать говорить, пока ему не предоставлено слово. Аналогично этому, компьютер в сети с передачей маркера не передает сигнал, пока маркер не перейдет к нему.

Передача маркера — весьма вежливый, "интеллигентный" метод управления доступом. Сигнал, называемый маркером, передается по сети от одного компьютера к другому, пока не достигнет компьютера, который хочет начать передачу данных. Чаще всего этот метод используется в кольцевой топологии, однако ничто не мешает передавать маркер и в шинной. Процесс передачи маркера показан на рис. 4.9.

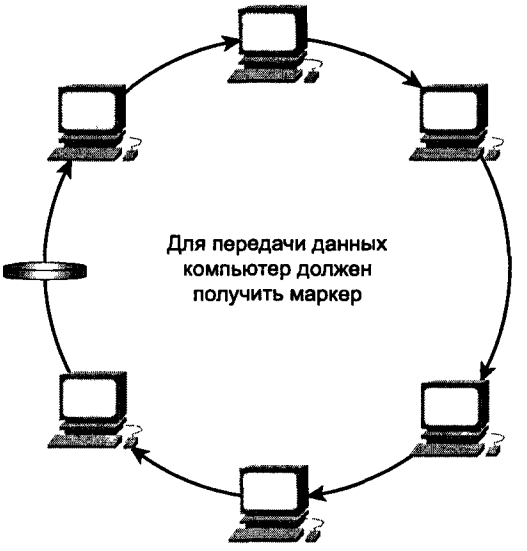


Рис. 4.9. В сети с передачей маркера компьютер не может начать передачу сигналов, пока не получит маркер

Наиболее распространенная сеть с передачей маркера — Token Ring. В ней управление доступом выполняется следующим образом. Маркер передается по сети от одного компьютера к другому. Когда он попадает в компьютер, готовый передавать данные, этот компьютер захватывает управление маркером. Он добавляет данные к сигналу маркера и передает его обратно в сеть. В пакете данных содержится адрес назначения пакета. Когда пакет проходит по сети, компьютеры, адреса которых не совпадают с адресом назначения, передают его дальше.

Когда маркер и пакет достигают компьютера, адрес которого указан в заголовке, сетевой адаптер компьютера копирует данные, добавляет в маркер подтверждение об успешном приеме и передает маркер дальше по кругу. Компьютер, передавший эти данные, получает маркер с подтверждением, после чего или передает с ним еще один пакет, или освобождает маркер, т.е. передает дальше с отметкой, что он свободен.

В некоторых архитектурах с передачей маркера, например в FDDI (Fiber Distributed Data Interface), по сети могут циркулировать несколько маркеров одновременно. Архитектуры Token *R*ing и FDDI подробно рассматриваются в главе 5, "Локальные сети". Стандарты Token *R*ing содержатся в спецификации IEEE 802.3.

Приоритеты запросов

Метод доступа с приоритетами запросов был разработан компанией Hewlett Packard для локальной сетевой архитектуры 100VG-AnyLAN. Иногда ее называют архитектурой VG-AnyLAN, или AnyLAN. Архитектура VG-AnyLAN была задумана как высокоскоростная, гибкая и эффективная сетевая архитектура, призванная заменить Ethernet.

В методе доступа с приоритетами запросов используются многопортовые повторители (концентраторы), выполняющие карусельный обзор подключенных узлов (компьютеров, маршрутизаторов или других сетевых устройств) для обнаружения запросов на передачу данных. В сетях VG-AnyLAN используется древовидная топология, аналогичная звездообразной. В целях централизации управления сетью концентраторы можно подключать каскадами, начиная с корневого концентратора. На рис. 4.10 показана сеть VG-AnyLAN.

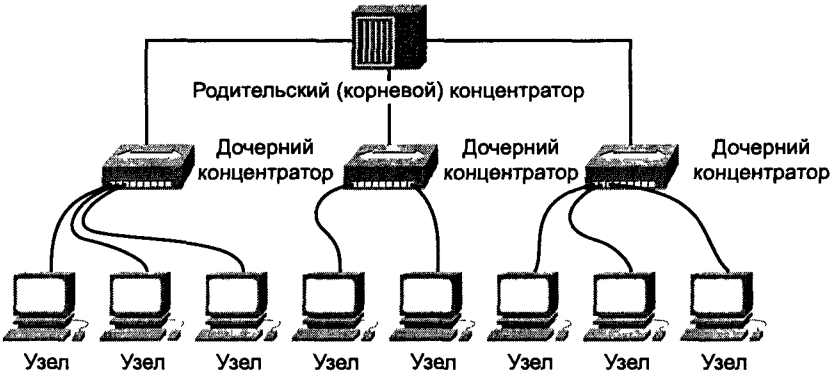


Рис. 4.10. В сети VG-AnyLAN для реализации метода доступа с приоритетами запросов используется каскадное подключение концентраторов

Слово приоритеты в названии метода означает, что определенным типам данных может быть присвоен приоритет, в результате чего концентратор обработает их в первую очередь, если несколько запросов на передачу поступили одновременно. Это гарантирует необходимую пропускную способность для высокоскоростных приложений в реальном времени, таких как видеоконференции или голосовая связь.

Метод доступа с приоритетами запросов более эффективен, чем CSMA/CD, потому что в нем используются пары кабелей (четыре провода к каждому компьютеру), по которым можно одновременно как передавать, так и принимать сигналы. Кроме того, в отличие от CSMA/CD, в этом методе сигналы не передаются во всю сеть. Напротив, сигналы попадают только в компьютеры, подключенные к одному концентратору. Концентраторы сообщаются друг с другом. Каждый концентратор работает только с подключенными к нему узлами и ничего не знает об остальных узлах, подключенных к другим концентраторам.

Поскольку не все данные проходят через все компьютеры (как в архитектурах Ethernet и Token Ring), безопасность сетей VG-AnyLAN тоже значительно выше.

В сетях VG-AnyLAN можно использовать две или четыре неэкранированные витые пары, две экранированные витые пары либо волоконно-оптический кабель. Спецификации метода с приоритетами запросов содержатся в IEEE 802.12.

К сожалению, оборудование и программное обеспечение 100VG-AnyLAN в настоящее время предлагается весьма ограниченным кругом поставщиков. Эта архитектура еще не получила широкого распространения. Большинство сетевых администраторов пока что не встречались с сетями VG-AnyLAN.

Резюме

В этой главе рассмотрены процессы передачи компьютерных данных на уровне сигналов и представлены различные способы классификации сигналов.

Мы рассмотрели, чем отличаются аналоговые сигналы от цифровых и модулированные от немодулированных. Описаны синхронные и асинхронные методы коммуникации, симплексный, полудуплексный и дуплексный методы передачи данных. Рассмотрены сложности, возникающие при передаче данных: электромагнитные, радиочастотные и перекрестные помехи, а также явление затухания сигналов.

Обсуждались наиболее распространенные методы управления доступом к сети, включая CSMA/CD, CSMA/CA, методы с передачей маркера и с приоритетами запросов.

В следующих главах рассматривается реализация различных типов сетей: в главе 5, "Локальные сети", — соединения локальных сетей Ethernet, Token Ring и AppleTalk, а в главе 6, "Глобальные сети", — соединения ATM, FDDI и SONET, используемые в глобальных сетях.

Рекомендуемые источники

С обзором систем коммуникации и методов передачи данных можно ознакомиться на Web-узле по адресу: `www.cs.ucl.ac.uk/staff/S.Bhatti/D51-notes/node1.html`.

Страница института Tech Broadband Institute штата Джорджия, содержащая полезную информацию о широкополосных технологиях и ссылки на дополнительные источники, расположена по адресу: `www.broadband.gatech.edu/top.html`.

Великолепный учебник по сетям 100VG-AnyLAN можно найти по адресу: `www.iol.unh.edu/training/vganylan`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите наиболее правильный ответ или ответы.

1. Как называется процесс превращения нулей и единиц, представляющих компьютерные данные, в электрические или световые импульсы?
   а. Шифрование.
   б. Кодирование.

в. Обеспечение безопасности.

г. Цикличность

2. Какие из этих утверждений справедливы для цифровых сигналов?

   а. Цифровой сигнал представляет собой постоянно изменяющуюся электромагнитную волну.

   б. Параметрами цифрового сигнала являются амплитуда, частота и фаза.

   в. Единицей измерения цифровых сигналов служит герц.

   г. Цифровой сигнал — это сигнал с дискретными состояниями.

3. Какие из приведенных ниже утверждений о преимуществах аналоговых сигналов над цифровыми справедливы? (Выберите все подходящие)

   а. Аналоговые сигналы менее чувствительны к помехам

   б. Аналоговые устройства дешевле цифровых.

   в. Аналоговые сигналы легче мультиплексировать.

   г. Аналоговые сигналы меньше подвержены затуханию

4. Как называется технология, в которой все возможности среды используются для передачи данных по одному каналу?

   а. Передача немодулированных сигналов.

   б. Модулирование сигналов

   в. Мультиплексирование

   г. Мультисоединения

5. Какие из этих утверждений справедливы для немодулированных сигналов? (Выберите все подходящие.)

   а. Немодулированные сигналы можно передавать в обоих направлениях

   б. Немодулированные сигналы используются в кабельном телевидении.

   в. Немодулированные сигналы являются однонаправленными

   г. Цифровые сигналы чаще всего являются немодулированными

6. Какой тип мультиплексирования используется в волоконно-оптических сетях, в которых каждый сигнал передается на своей длине волны светового луча?

   а. Частотное разделение каналов.

   б. Временное разделение каналов.

   в. По длине волны высокой плотности.

   г. По частоте длины волны

7. Какие из этих утверждений об асинхронной передаче данных справедливы?

   а. При асинхронной передаче внутренние часы передающего и принимающего устройств координируются встроенными механизмами

   б. При асинхронной передаче используется синхронизация с гарантированным изменением состояний

   в. При асинхронной передаче используется стробирование

   г. При асинхронной передаче для синхронизации передающего и принимающего устройств используется стартовый бит.

8. В каких системах используется полудуплексный метод?

а. Телевидение.

б. Радиовещание.

в. Телефонная связь.

г. DSL.

9. Какой носитель сигналов наиболее чувствителен к электромагнитным помехам?

а. Неэкранированная витая пара.

б. Коаксиальный кабель.

в. Волоконно-оптический кабель.

г. Экранированная витая пара.

10. Какой метод доступа используется в Ethernet?

а. CSMA/CA.

б. CSMA/CD.

в. Передача маркера.

г. Приоритеты запросов.

Глава 5

Локальные сети

В первых четырех главах вы ознакомились со структурой и назначением сетей, с сетевыми моделями, стандартами, методами передачи сигналов по сети и с методами управления доступом к сети.

В этой главе речь пойдет о реализации этих методов в конкретных спецификациях, определяющих тип сетевого соединения, т.е. *архитектуру* сети.

Сетевые соединения можно разделить на две категории:

- соединения локальных или городских сетей, т.е. охватывающих географически ограниченное пространство;
- соединения глобальных сетей, которые могут охватывать города, страны и целые континенты.

В этой главе описаны характеристики первого типа соединений. Вы узнаете, как в конкретной ситуации выбрать оптимальный тип сети, позволяющий выполнять поставленные задачи наиболее просто и с наименьшими затратами. Соединения второй категории рассматриваются в главе 6, "Глобальные сети".

Для подключения компьютеров к локальным и городским сетям используется несколько типов соединений. Поскольку в этих сетях расстояние между компьютерами небольшое, в них используются кабели, которые не смогли бы работать в глобальных сетях вследствие затухания.

Из предыдущих глав вы уже знакомы с большинством типов архитектур локальных сетей, однако, поскольку в этой главе мы рассматриваем стандарты и спецификации каждой архитектуры отдельно, перечислим их еще раз:

- Ethernet;
- Token Ring;
- FDDI (Fiber Distributed Data Interface);
- AllpeTalk;
- ARCnet.

Сети Ethernet

В настоящее время архитектура Ethernet — наиболее распространенный тип локальных сетевых соединений. Согласно спецификации 802.3 в сетях Ethernet

используется метод управления доступом CSMA/CD, шинная или звездообразная топология и передача немодулированных сигналов по коаксиальным кабелям или витым парам. Стандартная пропускная способность — 10 или 100 Мбит/с. Новые стандарты определяют также *Gigabit Ethernet* с пропускной способностью 1 Гбит/с, в которой используются волоконно-оптические кабели или другие типы высокоскоростных носителей.

Архитектура Ethernet берет свое начало от глобальной сетевой архитектуры ALOHA, разработанной университетом штата Гавайи, в которой используется метод управления доступом CSMA/CD. В 1970-х годах Исследовательский центр Пало Альто, принадлежащий компании Xerox, разработал архитектуру Ethernet с пропускной способностью 2,95 Мбит/с. Вскоре после этого Xerox в сотрудничестве с Intel и Digital разработали стандартную Ethernet на 10 Мбит/с.

Среди многочисленных топологий Ethernet, используемых в настоящее время, наиболее распространены следующие:

- 10Base2 (тонкая сеть);
- 10Base5 (толстая сеть);
- 10BaseT (с неэкранированными витыми парами);
- 100BaseT (Fast Ethernet);
- 100BaseFX (Ethernet на волоконно-оптических кабелях);
- 1000BaseT (Gigabit Ethernet).

10Base2

В топологии Ethernet 10Base2 согласно спецификации IEEE 802.3 реализованы метод доступа CSMA/CD и шинная топология с использованием тонкого коаксиального кабеля. Эта топология иногда называется также *тонкой сетью*.

Число 10 в названии означает, что пропускная способность тонкой сети равна 10 Мбит/с. Для передачи данных между компьютерами используются немодулированные импульсы. Число 2 в названии топологии означает максимальную длину сегмента кабеля (более точно она составляет 185, а не 200 метров).

В сети 10Base2 на один 185-метровый сегмент может приходиться не более 30 *узлов* (компьютеров или других сетевых устройств). В этих сетях используются цилиндрические или Т-образные разъемы (оба типа называются разъемами BNC). На каждом конце шины устанавливается терминатор типа BNC. На рис. 5.1 показано использование цилиндрического разъема для наращивания длины кабеля.

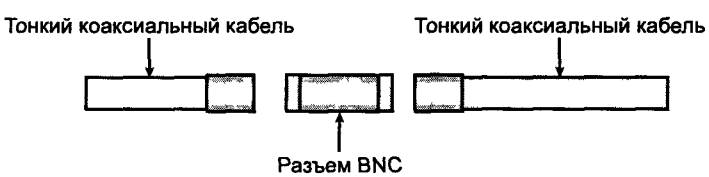


Рис. 5.1. Тонкий коаксиальный кабель можно нарастить с помощью цилиндрического разъема BNC

Замечание

Среди специалистов по сетевым технологиям существуют разногласия относительно того, как расшифровывается BNC. В некоторых источниках можно встретить расшифровку *British Naval Connector* (разъем британского флота). В других — *Bayonet Nut Connector* (шипообразный, или штыкообразный разъем). Многие утверждают, что это сокращение происходит от фамилий изобретателей разъема: Neil (Нейл) и Concelman (Консельман). Среди приверженцев последней гипотезы тоже нет единодушия относительно того, как правильно пишется — Neil или Neill. После некоторых исследований нам удалось установить, что Поль Нейлл (Paul Neill), сотрудник лаборатории Bell, разработал так называемый N-разъем, который использовался на британском флоте. Позже Карл Консельман на основе N-разъема создал разъем, который назвал C-разъемом. В конце концов Нейл и Консельман вместе разработали окончательный малогабаритный вариант разъема — BNC.

Преимущества 10Base2

Сеть 10Base2 легко установить и конфигурировать. Поэтому эта архитектура хорошо подходит для небольших временных сетей, например в классных комнатах, где сеть нужно периодически снимать и устанавливать. В сети 10Base2 используется меньше кабеля, чем в 10BaseT. Тонкий кабель сети 10Base2 дешевле, чем толстый кабель, используемый в 10Base5. В топологии 10Base2 не нужны дополнительные компоненты, такие как концентраторы или внешние трансиверы. Поэтому установка сети 10Base2 обходится довольно дешево.

Недостатки 10Base2

К сожалению, топология 10Base2 не предназначена для больших сетей из-за ограничений на длину сегмента кабеля и количество узлов на сегмент. К тому же пропускную способность 10 Мбит/с сегодня вряд ли уже можно считать высокой.

Замечание

Сетевые спецификации определяют максимальную длину сегмента исходя из допустимого уменьшения сигнала вследствие затухания. В спецификациях определяется также минимальная длина кабеля между двумя компьютерами. Если расстояние между ними слишком малое, то сигналы двух устройств, перекрываясь, создадут в кабеле недопустимо высокое напряжение. Это явление называется *коллизией*.

10Base5

Сеть 10Base5 иногда называют *стандартной* или *толстой* Ethernet. В ней используется довольно толстый коаксиальный кабель диаметром около 1 см, т.е. в два раза толще, чем в тонкой сети. В толстой сети используется шинная топология. Поскольку используется толстый кабель, максимальное допустимое расстояние между компьютерами составляет 500 метров. Спецификации толстой сети определяют минимальную длину сегмента равной 2,5 метра.

Устанавливать толстую сеть сложнее, чем тонкую. В сетях 10Base5 используются внешние трансиверы, которые передают и принимают сигналы. Они подключаются к сетевым адаптерам с помощью *трансиверного кабеля* и 15-контактного разъема AUI

(DIX). К коаксиальному кабелю трансивер подключается с помощью специального разъема, который называется *зуб вампира* (рис. 5.2).

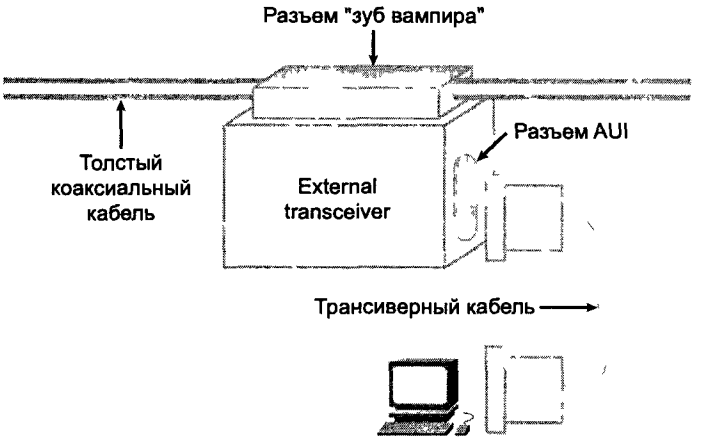


Рис 5 2 Сетевой адаптер подключается к толстой сети посредством внешнего трансивера и разъема "зуб вампира"

Архитектура 10Base5 часто используется как *магистраль*, соединяющая расположенные на большом расстоянии сегменты тонкой сети. В этой схеме к толстому кабелю подключены повторители, расположенные на разных этажах здания. К повторителям с помощью тонкого кабеля подключены компьютеры тонкой сети (рис 5.3).

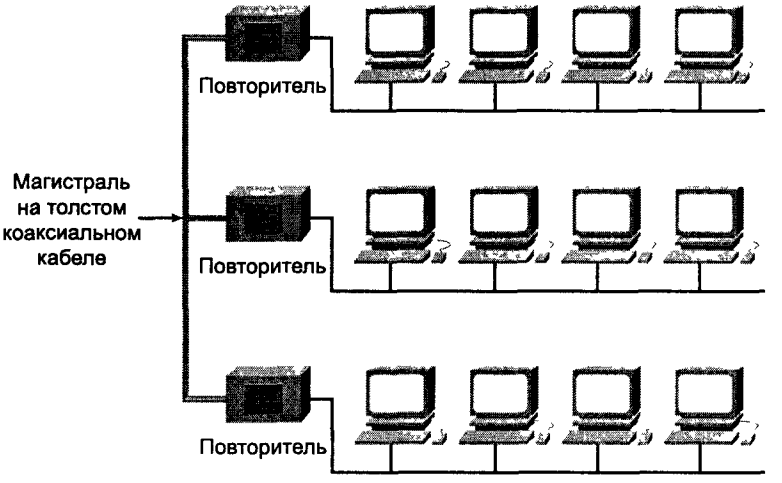


Рис. 5 3 Толстый коаксиальный кабель можно использовать как магистраль для сегментов тонкой сети

Как и в других сетях Ethernet, в 10Base5 используются немодулированные сигналы и метод доступа CSMA/CD. Длина кабеля может быть увеличена с помощью цилиндрических N-разъемов. Магистраль должна заканчиваться N-терминаторами.

Преимущества 10Base5

Толстые сети имеют по сравнению с тонкими два больших преимущества

- большее допустимое расстояние без применения повторителей,
- большее допустимое количество узлов (компьютеров) на сегмент

Преимуществом толстых (и тонких) коаксиальных кабелей по сравнению с неэкранированной витой парой является относительно меньшая чувствительность к электромагнитным помехам, обусловленная наличием внешнего защитного экрана

Недостатки 10Base5

Из-за малой гибкости кабеля толстую сеть труднее устанавливать, чем тонкую Кроме того, для добавления в сеть узлов (компьютеров) в кабеле нужно просверливать отверстие, необходимое для установки разъема "зуб вампира"

Установка толстой сети обходится относительно дорого Не только потому, что толстый кабель стоит дороже тонкого или неэкранированной витой пары, но и потому, что для каждого сетевого компьютера нужно покупать дополнительное оборудование (трансивер и трансиверный кабель)

10BaseT

В настоящее время 10BaseT — одна из наиболее популярных архитектур Ethernet Можно сказать, что это "звезда" коммуникационных технологий, потому что в ней используется топология звезды

Замечание

Внутри концентратора Ethernet сигналы проходят по шине, поэтому считается, что в 10BaseT реализована логическая шинная топология, как и в архитектурах Ethernet с коаксиальными кабелями

Довольно часто встречается выражение *кабель Ethernet*, означающее неэкранированную витую пару, которая используется в 10BaseT (можно использовать также экранированную витую пару) Сеть 10BaseT и ее сестру 100BaseX легко устанавливать и расширять

Преимущества 10BaseT

Сети 10BaseT относительно дешевы Несмотря на то что в них нужны концентраторы (если соединяются более двух компьютеров), на стоимость сети это почти не влияет, потому что небольшие концентраторы довольно дешевы Сетевые адаптеры 10BaseT тоже недороги и широко доступны

Замечание

Согласно спецификациям для сети 10BaseT нужен концентратор Однако если в сеть объединяются только два компьютера (например, в домашней сети) и витая пара предпочтительнее тонкого кабеля, то вместо концентратора можно использовать *перекрученный кабель*

С витыми парами (особенно неэкранированными, которые используются чаще всего) легче работать, чем с коаксиальными кабелями, потому что они тонкие и гиб-

кие. Для них используются модульные гнезда и разъемы RJ-45, поэтому подключить кабель к сетевому адаптеру или концентратору очень просто.

Еще одно преимущество 10BaseT — легкость модернизации. Ее пропускная способность составляет 10 Мбит/с, однако если проложен кабель категории 5 или выше и установлены сетевые адаптеры, поддерживающие 10 и 100 Мбит/с, то для модернизации сети на 100 Мбит/с нужно всего лишь заменить концентраторы.

Недостатки 10BaseT

Максимальная длина сегмента 10BaseT (без повторителей) составляет всего 100 метров. Используемые в этой сети неэкранированные витые пары более подвержены электромагнитным помехам и затуханию, чем другие типы кабелей. Кроме того, из-за дополнительных расходов на концентраторы установка сетей 10BaseT обходится несколько дороже, чем сетей с тонкими коаксиальными кабелями.

100BaseX

В настоящее время для многих приложений (таких, как видеоконференции или голосовая связь) сеть должна обладать значительно большей пропускной способностью, чем 10 Мбит/с. Ее может обеспечить архитектура 100BaseX, которая называется *Fast Ethernet.*

Сеть 100BaseX может быть реализована в нескольких вариантах: на четырех неэкранированных витых парах категории 3, 4 или 5 (100BaseT), на двух экранированных или неэкранированных витых парах категории 5 (100BaseTX) или на двужильном волоконно-оптическом кабеле (100BaseFX).

Преимущества 100BaseX

Независимо от реализации, пропускная способность 100BaseX составляет 100 Мбит/с, что в 10 раз выше, чем у 10Base2, 10Base5 или 10BaseT.

Поскольку используются витые пары, 100BaseX имеет все преимущества архитектуры 10BaseT: низкая стоимость, гибкость, простота установки и расширения.

Недостатки 100BaseX

Архитектура 100BaseX разделяет также и недостатки сетей 10BaseT, обусловленные использованием витых пар: повышенную чувствительность к электромагнитным помехам и затухание сигнала. Сетевые адаптеры и концентраторы на 100 Мбит/с стоят дороже, чем на 10 Мбит/с, однако цены на них неуклонно снижаются.

Установка волоконно-оптической сети продолжает оставаться весьма дорогим удовольствием, причем не столько из-за стоимости кабеля, сколько из-за сложности установки, требующей квалифицированных специалистов.

1000BaseT

Раз уж 100BaseT называется *Fast Ethernet*, то как назвать 1000BaseT? Дьявольски быстрой? Однако ее название звучит довольно скромно: *Gigabit Ethernet.* Ее пропускная способность составляет 1 Гбит/с, что почти в семь раз превышает пропускную способность линии T-1. Пока что сети 1000BaseT не получили широкого распространения. Архитектура Gigabit Ethernet предназначена главным образом для локальных сетей, однако с помощью волоконно-оптических кабелей ее можно реализовать и в городской сети.

Преимущества 1000BaseT

Основным преимуществом 1000BaseT является, конечно, высокая производительность. Ее пропускная способность в 10 раз больше, чем у Fast Ethernet и в 100 раз больше, чем у стандартной Ethernet. Это позволяет реализовать в сетях 1000BaseT такие высокоскоростные технологии, как, например, видеоконференции в режиме реального времени.

Недостатки 1000BaseT

Недостатки сетей 1000BaseT обусловлены главным образом применением неэкранированных витых пар, поэтому они полностью совпадают с недостатками сетей 10BaseT и 100BaseT, перечисленными в предыдущих разделах.

Структура кадра Ethernet

Пакеты, или порции, на которые данные разбиваются для передачи по сети, в терминологии Ethernet называются *кадрами*. Кадр состоит из заголовка, передаваемых данных и трейлера.

Типы кадров Ethernet

Существует четыре различных типа кадров: Ethernet_802.2, Ethernet_802.3, Ethernet II и Ethernet_SNAP. Кадры Ethernet II и Ethernet_SNAP (Subnet Access Protocol) используются в сетях TCP/IP. Тип кадра определяется его структурой, т.е. количеством байтов, выделенных для каждого поля заголовка, поля данных и поля трейлера. Например, наиболее простой заголовок Ethernet II содержит только четыре поля. Заголовок Ehernet_SNAP содержит девять полей.

На рис. 5.4 показана структура кадра Ethernet II.

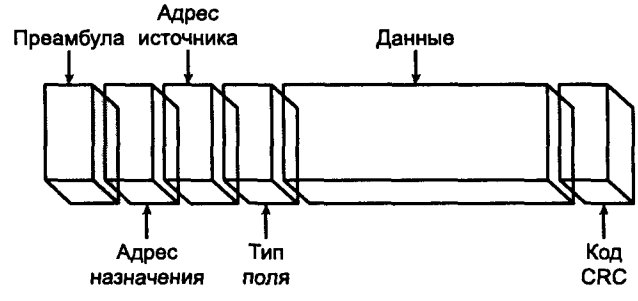


Рис. 5 4. Кадр Ethernet II содержит четыре заголовочных поля и трейлер

Первое заголовочное поле, которое всего лишь отмечает начало кадра, называется *преамбулой*. Следующие два поля содержат целевой адрес и адрес источника (адреса передающего и принимающего компьютеров). Четвертое поле используется для идентификации протокола сетевого уровня (обычно это IP или IPX). После заголовка расположены данные, которые могут занимать от 46 до 1 500 байт. В Ethernet используются дополнительные 18 байт в качестве элементов конструкции самого кадра. Трейлер содержит код CRC (Cyclic Redundancy Check), который используется для проверки правильности кадра, поступившего на принимающий компьютер.

Выявление ошибок с помощью CRC

Метод CRC — это стандартный метод обнаружения ошибок в данных после их передачи по сети. Работает метод следующим образом. Компьютер, передающий данные, трактует их как один длинный полином — алгебраическое выражение, которое равно сумме слагаемых, причем каждое слагаемое равно произведению коэффициента (бита данных) на номер позиции в целой степени. Передающий компьютер вычисляет этот полином, а затем делит его на предопределенный 16- или 32-битовый полином. Результат деления — это и есть код CRC, который добавляется в кадр перед отправкой данных в сеть. Принимающий компьютер выполняет над полученными данными те же операции, после чего сравнивает результат с кодом CRC, находящимся в трейлере. Если результаты совпадают, принимающий компьютер делает вывод, что данные переданы правильно. В противном случае на передающий компьютер передается извещение о том, что он должен передать этот кадр повторно.

Правила установки Ethernet

Чтобы сеть правильно и эффективно функционировала, при ее установке необходимо придерживаться некоторых правил, определяемых спецификациями для каждой архитектуры. Эти ограничения накладываются главным образом характеристиками носителей сигналов. Ограничения не являются абсолютно жесткими, иногда при небольшом их нарушении сеть может нормально работать, однако это будет все же нарушением стандартов и может вызвать серьезные неполадки.

В этом разделе рассматриваются два важных ограничения:

- правило 5-4-3;
- ограничение количества узлов 10BaseT.

Правило 5-4-3

Правило определяет ограничения сетей Ethernet, использующих коаксиальный кабель. Числа означают следующее:

- **5** — максимально допустимое количество сегментов кабелей в тонких и толстых сетях равно пяти (в тонкой сети длина каждого сегмента не должна превышать 185 метров, а в толстой — 500 метров);
- **4** — максимальное количество повторителей, соединяющих сегменты, равно четырем;
- **3** — максимальное количество *заселенных* сегментов (содержащих узлы) равно трем. Два остальных сегмента могут использоваться только для увеличения расстояния.

Замечание

Когда правило 5-4-3 применяется к сети 10Base5 (толстой сети) длиной сегмента считается длина толстого кабеля. Длина трансиверного кабеля не учитывается.

Правило 5-4-3 в архитектуре 10BaseT

Применимо ли правило 5-4-3 к сетям Ethernet с витыми парами? Читая некоторые книги, можно прийти к выводу, что неприменимо. Однако ограничение на количест-

во концентраторов, которые можно соединить в 10BaseT, фактически является применением этого же правила.

По отношению к звездообразной топологии с неэкранированными витыми парами правило 5-4-3 означает, что максимальное количество каскадированных населенных концентраторов равно трем, т.е. "заселенный" концентратор засчитывается как заселенный сегмент.

Внутри каждого концентратора есть магистраль, к которой подключены компьютеры (рис. 5.5). Это аналогично подключению компьютеров к сегментам кабеля между повторителями в шинной сети.

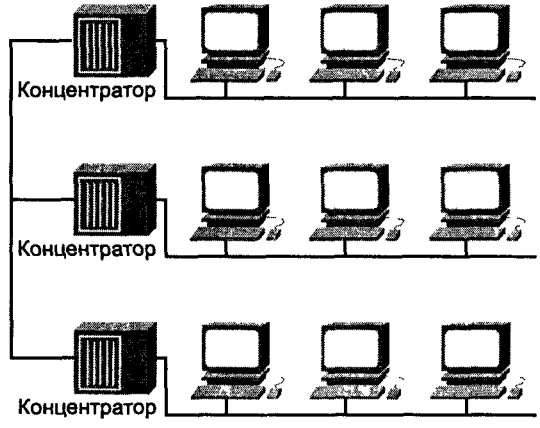


Рис. 5.5 Каждый концентратор, к которому подключены компьютеры, засчитывается как заселенный сегмент

Правило 5-4-3 и расширение сети

Насколько большой можно сделать сеть Ethernet в пределах ограничений, накладываемых этим правилом? Посредством витых пар или коаксиальных кабелей к сети можно подключить сотни компьютеров. Как же это согласуется с ограничениями 5-4-3?

Рассмотрим это правило внимательнее. В выражении "...не более пяти сегментов, четырех повторителей и трех заселенных сегментов на *сеть*" слово *сеть* означает не всю локальную сеть, а *домен конфликтов*, т.е. ту часть сети, в которой будут происходить конфликты при одновременной передаче данных.

При создании сети с количеством устройств, большим, чем позволяет правило 5-4-3, понятие домена конфликтов является ключевым. С помощью концентраторов и маршрутизаторов в сети можно создать отделенные друг от друга домены конфликтов. Эти устройства подробно рассматриваются в главе 7, "Физические компоненты сетей".

Ограничение количества узлов в 10BaseT

В топологии звездообразной магистрали на витых парах количество узлов на сегмент всегда точно равно двум: один узел — компьютер или другое устройство на одном конце провода, а другой узел — сам концентратор на другом конце. Количество узлов, подключенных к концентратору, не должно превышать 100, потому что после 100 вероятность конфликтов данных резко увеличивается. Однако это ограничение

можно преодолеть с помощью таких сетевых устройств, как мосты и коммутаторы. Теоретически максимальное количество сетевых устройств в сети 10BaseT равно 1 024.

Сводка характеристик Ethernet

В табл. 5.1 приведена краткая сводка спецификаций наиболее распространенных архитектур Ethernet.

Таблица 5.1. Спецификации Ethernet

	10Base2	10Base5	10BaseT	100BaseX
Тип кабеля	Тонкий коаксиальный RG-58 A/U	Толстый коаксиальный RG-8 или RG-11	Неэкранированная витая пара категории 3, 4, 5 или 5e	Неэкранированная витая пара категории 3, 4, 5 или 5e
Тип разъемов	BNC	AUI/DIX (к трансиверу)	Модульный RJ-45	Модульный RJ-45
Максимальная длина сегмента, м	185	500	100	100
Максимальная длина сети, м	925	2 500	Топология звездообразной магистрали	Топология звездообразной магистрали
Количество узлов на сегмент	30	100	2 (1 024 на сеть)*	2 (1 024 на сеть)*
Пропускная способность, Мбит/с	10	10	10	100

** В сетях 10BaseT и 100BaseX на витых парах концентратор используется как центральная точка соединения, поэтому формально к каждому сегменту подключаются только два устройства концентратор и компьютер (узел).*

Ethernet — широко распространенная архитектура, работающая почти со всеми серверными и клиентскими операционными системами, включая Windows for Workgroups, Windows 9*x*, Windows NT, Windows 2000, Novell NetWare, AppleTalk/AppleShare и UNIX/Linux.

Сети Token Ring

Архитектура Token Ring, разработанная компанией IBM, была задумана как надежная сетевая архитектура на основе метода управления доступом с передачей маркера. Довольно распространена интеграция в сеть Token Ring мэйнфреймов IBM, таких как AS/400. Архитектура Token Ring предназначена для персональных компьютеров, мини-компьютеров и универсальных вычислительных машин. Она хорошо работает с SNA (Systems Network Architecture), которая представляет собой архитектуру IBM, используемую для соединения с сетями мэйнфреймов.

Стандарты Token Ring определяются спецификациями IEEE 802.5.

Топология Token Ring

Сначала топология Token Ring может привести в замешательство. Это отличный пример архитектуры, в которой физическая топология не совпадает с логической. Топология Token Ring называется *звездообразным кольцом*. Внешне сеть похожа на звезду: компьютеры подключены к центральному концентратору, который называется MSAU (Multistation Access Unit — устройство доступа ко многим станциям). Однако внутри MSAU данные проходят по кругу, образуя логическое кольцо.

Таким образом, название Token Ring отражает логическую топологию и метод управления доступом к сети — передача маркера. Пропускная способность Token Ring может составлять 4 или 16 Мбит/с.

В Token Ring используются немодулированные цифровые сигналы. Этим она напоминает Ethernet, однако процессы коммуникации в них существенно различаются Топология Token Ring *активная*: переходя по кругу от одного сетевого адаптера к другому, сигналы регенерируются.

Процессы коммуникации в Token Ring

В Ethernet все компьютеры физически равны. На уровне программного обеспечения некоторые из них могут работать как серверы и управлять доступом и учетными записями сети, однако физически серверы сообщаются с сетью точно так же, как и клиентские компьютеры

Управление кольцом

В сети Token Ring первый подключенный компьютер становится управляющим Он должен отслеживать, сколько раз каждый кадр проходит по кругу. Он же отвечает и за то, чтобы только один маркер ходил по кругу в определенный момент времени.

Управляющий компьютер периодически посылает специальный сигнал, который называется *маяком* Маяк проходит по кольцу так же, как и другие сигналы. Каждый компьютер ожидает маяк. Если компьютер не получает маяк от своего верхнего по течению соседа (т.е. компьютера, передающего маркер), он передает в сеть сообщение, информирующее управляющий компьютер о том, что маяк не получен. В сообщении указан также адрес этого компьютера и адрес его верхнего соседа, от которого он не получил маяк. Тогда управляющий компьютер автоматически конфигурирует систему заново и во многих случаях нормальный процесс коммуникации восстанавливается.

Передача данных

В Token Ring для управления доступом к кабелю используется специальный сигнал, называемый *маркером*. Маркер генерируется, когда первый компьютер подключается к сети. Как упоминалось в главе 4, "Методы сетевой коммуникации", когда компьютер ожидает права передавать данные, он ожидает маркер. Дождавшись его, компьютер захватывает управление маркером.

Маркер может переходить по кольцу в любом направлении, однако в каждый момент времени направление его движения может быть только одним. Направление движения маркера определяется конфигурацией оборудования.

Сетевое оборудование Token Ring

В сетях Token Ring используется специальное оборудование. Одной из причин меньшей распространенности этих сетей по сравнению с Ethernet является более высокая стоимость компонентов Token Ring.

MSAU

Концентраторы Token Ring называются MSAU или SMSAU (Smart MSAU). Отличительной особенностью MSAU является его внутренняя кольцевая конфигурация. Допускается соединение друг с другом произвольного количества MSAU, однако каждый выходной порт MSAU должен быть подключен ко входному порту следующего MSAU (рис. 5.6). Это условие обеспечивает сохранение логического кольца. Данные должны передаваться по непрерывному кругу.

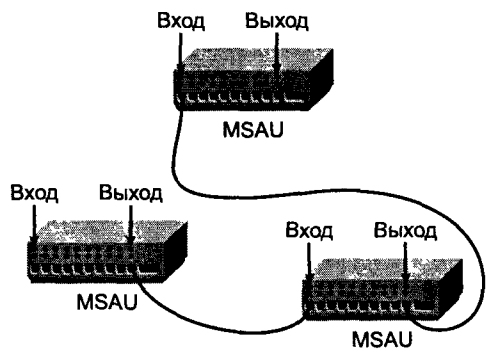


Рис. 5.6. Можно соединить между собой много MSAU, однако, чтобы не нарушилось логическое кольцо, кабели должны правильно соединять входные и выходные порты

Кабели и сетевые адаптеры

В сетях Token Ring используются кабели IBM типов 1, 2 и 3. Компания IBM обозначает свои витые пары как "типы", а не как "категории". В табл. 5.2 приведено описание кабелей IBM.

Таблица 5.2. Типы кабелей IBM

Тип	Описание
1	Две экранированные витые пары с внешней оболочкой
2	Экранированные витые пары; две пары для данных и четыре пары для голоса
3	Четыре экранированные витые пары; разъемы RJ-45 или RJ-11
5	Волоконно-оптический кабель
6	Экранированная витая пара; используется как перемычка
9	Экранированная витая пара класса "пленум"

Замечание

С кабелями IBM используются специальные разъемы IBM, которые называются разъемами типа A Со стандартными разъемами BNC они несовместимы.

Сетевые адаптеры Token Ring, как и адаптеры Ethernet для витых пар, выпускаются двух типов: на 4 и на 16 Мбит/с. Если сеть работает со скоростью 4 Мбит/с, то можно использовать адаптер на 16 Мбит/с (естественно, она будет работать с меньшей скоростью).

Внимание!

Если сеть работает со скоростью 16 Мбит/с, то использовать адаптер на 4 Мбит/с нельзя Соединение между компьютерами не установится вообще

Другие компоненты

В сетях Token Ring используются также некоторые другие компоненты. Например, для соединения кабелей типа 1 и 2 используются разъемы MIC (Media Interface Connector). Для подключения сетевого адаптера Token Ring к модульному гнезду и для уменьшения шумов на линии используются специальные фильтры.

Как и в Ethernet, для увеличения длины кабеля можно регенерировать цифровой сигнал с помощью повторителей.

Преимущества Token Ring

Архитектура Token Ring весьма надежна, так как метод доступа с передачей маркера делает конфликты данных невозможными. Устройства MSAU могут обнаруживать выход из строя сетевого адаптера, который в этом случае автоматически отключается от кольца и не мешает нормальному прохождению маркера. Следовательно, выход из строя одного компьютера не нарушает нормальной работы других компьютеров сети

Еще одно преимущество — простота взаимодействия персональных компьютеров с мэйнфреймами.

Недостатки Token Ring

Основные недостатки архитектуры Token Ring — высокая стоимость по сравнению с 10BaseT и 100BaseT при меньшей пропускной способности.

Структура кадра Token Ring

В сетях Token Ring используются три типа кадров.

- **Кадр данных**. Переносит информацию от одного компьютера к другому
- **Кадр маркера**. Передается по кругу, пока не перехватывается компьютером, готовым передавать информацию
- **Кадр управления** Передает информацию об ошибках или другую управляющую информацию.

Структура кадра данных Token Ring (рис 5 7) несколько сложнее, чем кадра данных Ethernet II. Иногда кадр данных Token Ring называют кадром LLC (Logical Link Control).

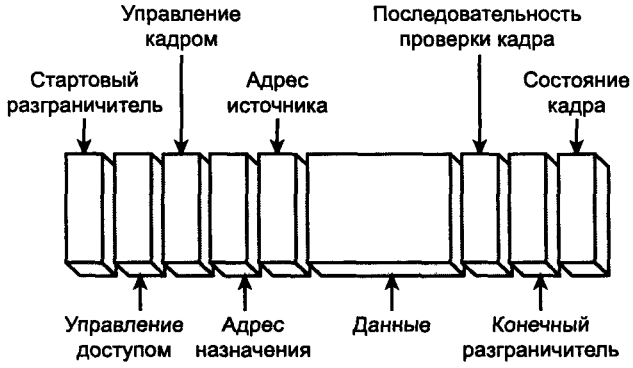


Рис. 5.7. Кадр данных Token Ring

- **Стартовый разграничитель**. В кадре Token Ring играет ту же роль, что и преамбула в кадре Ethernet.
- **Поле управления доступом**. Указывает, является ли кадр маркером или кадром данных. Определяет также приоритет кадра.
- **Поле управления кадром**. Содержит информацию об управлении доступом.
- **Целевой адрес**. Адрес компьютера, на который передается этот кадр.
- **Адрес источника**. Адрес передающего компьютера.
- **Данные**. Передаваемая информация (например, содержимое передаваемого файла).
- **FCS (Frame Check Sequence — последовательность проверки кадра)**. Проверочное поле с битами CRC.
- **Конечный разграничитель**. Отмечает конец кадра.
- **Поле состояния кадра**. Указывает, был ли адрес распознан, а кадр скопирован (заполняется принимающим компьютером перед отправкой кадра обратно в кольцо).

Замечание

Кадр маркера (иногда он называется просто маркером) переходит по кругу, пока его не перехватит компьютер, готовый передавать данные. В кадре маркера есть только три поля: стартовый разграничитель, поле управления доступом и конечный разграничитель.

Правила кольца

Спецификации накладывают на реализацию сетей Token Ring ряд ограничений.

- Расстояние между MSAU не может превышать 365 метров для кабеля типа 3 и 730 метров для типов 1 и 2.
- Максимальная длина кабеля сегмента зависит от типа кабеля и находится в пределах от 45 до 200 метров.
- Максимальная длина перемычки на кабеле типа 6 составляет 46 метров.

- Согласно спецификациям IBM, максимальное количество компьютеров на сегмент для неэкранированного кабеля составляет 72, а для экранированного — 260
- Согласно спецификациям IBM, максимальное количество сегментов (устройств MSAU), которые можно соединить друг с другом, составляет 33

Сводка характеристик Token Ring

Для сетей Token Ring характерны высокая надежность и устойчивость, однако вследствие более высокой стоимости и меньшей пропускной способности они менее популярны, чем Ethernet В настоящее время разрабатываются спецификации для Token Ring с пропускной способностью 100 Мбит/с и для Gigabit Token Ring Следовательно, эта архитектура считается перспективной

Сети FDDI

Архитектура FDDI (Fiber Distributed Data Interface — распределенный интерфейс передачи данных по волоконно-оптическим каналам) причисляется к типу Token Ring, однако ее реализация и топология отличаются от локальной сетевой архитектуры Token Ring, разработанной IBM и определяемой спецификациями IEEE 802 5 Архитектура FDDI часто используется в городских или больших локальных сетях, развернутых в нескольких зданиях

Принцип действия FDDI

Как указано в названии, в сетях FDDI используются волоконно-оптические кабели Поэтому в них высокая производительность сочетается с преимуществами кольцевой топологии с передаваемым маркером Пропускная способность FDDI равна 100 Мбит/с Топология сети представляет собой *двойное кольцо* Внешнее кольцо называется *первичным*, а внутреннее — *вторичным*

В нормальном режиме данные передаются по первичному кольцу, однако, если оно выходит из строя, данные автоматически переходят на вторичное кольцо и передаются в обратном направлении Когда это происходит, говорят, что сеть находится в *свернутом состоянии* Этим обеспечивается высокая устойчивость соединения к ошибкам Работа сети FDDI показана на рис 5 8

Компьютеры в сетях FDDI делятся на два класса

- **Класс А** Компьютеры, подключенные к кабелям обоих колец
- **Класс Б** Компьютеры, подключенные только к одному кольцу

Сети FDDI и Token Ring 802 5 отличаются также количеством кадров, циркулирующих по кольцу одновременно По кольцу FDDI одновременно может циркулировать много кадров Следовательно, несколько компьютеров могут осуществлять передачу одновременно Такой способ передачи называется *разделяемой сетевой технологией*

Как и в Token Ring 802 2, в сетях FDDI для обнаружения неполадок в кольце используются маяки

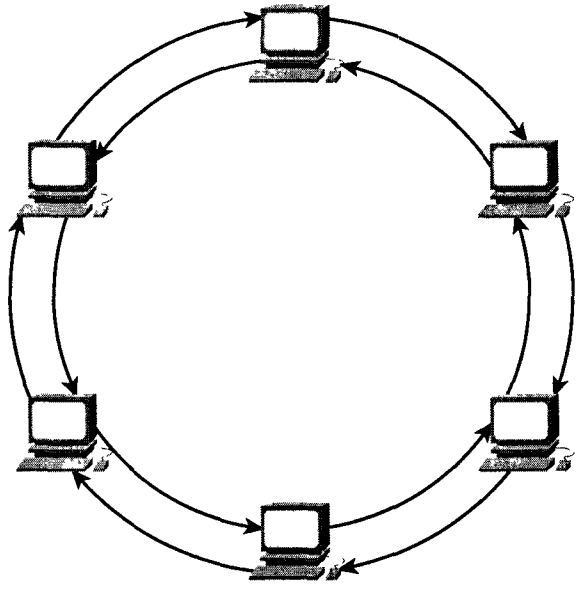


Рис. 5.8. В сетях FDDI используется отказоустойчивая топология с двойным кольцом

Спецификации FDDI

Двойное кольцо FDDI может содержать до 500 узлов. Общая длина кольца не должна превышать 100 км, однако на каждые 2 км нужен повторитель. Поэтому сети FDDI нельзя считать глобальными.

Замечание

Эти спецификации относятся к FDDI на волоконно-оптических кабелях. Однако сеть FDDI можно построить также на медных кабелях. В этом случае она называется CDDI (Copper Distributed Data Interface). Максимальные расстояния в сетях CDDI значительно меньше, чем в FDDI.

Кольцевая топология FDDI может быть реализована как физическое кольцо или как звездообразное логическое кольцо, образованное подключением компьютеров к центральному концентратору.

Преимущества FDDI

В архитектуре FDDI объединяются преимущества метода передачи маркера в кольцевой топологии с высокой пропускной способностью волоконно-оптических кабелей. Топология с избыточным двойным кольцом обеспечивает высокую устойчивость к сбоям. Волоконно-оптический кабель нечувствителен к электромагнитным помехам и шумам. Кроме того, он обеспечивает высокую безопасность, потому что к нему трудно подключиться незаметно. Максимальное расстояние между повторителями значительно больше, чем в Ethernet или традиционной Token Ring.

Недостатки FDDI

Как всегда, за высокую скорость и надежность нужно платить. Установка сети FDDI обходится относительно дорого. Кроме того, ограничения расстояний, хоть и менее жесткие, чем в других локальных сетевых архитектурах, делают архитектуру FDDI непригодной для построения глобальных сетей.

Структура кадра FDDI

Кадр FDDI имеет такую же структуру, как и кадр традиционной Token Ring. Однако в FDDI используется хронометрированный протокол маркера, в то время как в Token Ring передаваемый по кольцу маркер принадлежит одному из компьютеров. Максимальный размер кадра FDDI составляет 4 500 байт.

Маркер FDDI представляет собой специальный кадр, состоящий из трех октетов. Компьютер, готовый передавать данные, ожидает кадр маркера, затем захватывает его, передает один или больше кадров данных и освобождает маркер.

Сводка характеристик FDDI

Архитектура FDDI хорошо приспособлена для сетей средних размеров — городских и больших локальных, а также для сетей, в которых требуется большая пропускная способность для высокоскоростных приложений, таких как графические или видеоданные.

Сети AppleTalk

Архитектура AppleTalk разработана для объединения в сеть компьютеров Apple, ее программное обеспечение встроено в операционные системы Macintosh Различают две разновидности AppleTalk. фаза 1, включенная в ранние версии Mac OS, и фаза 2 — современная версия.

Термин *LocalTalk* употребляется применительно к оборудованию, кабелям и протоколам канального уровня, используемым в сетях AppleTalk.

Спецификации AppleTalk

В AppleTalk/LocalTalk для управления доступом в сеть применяется метод CSMA/CA. Чаще всего используются экранированные витые пары, однако возможно также использование волоконно-оптических кабелей и неэкранированных витых пар Сетевая топология AppleTalk шинная или древовидная. В сети LocalTalk (с компонентами Apple) максимальное количество узлов равно 32

Разделение (совместное использование) файлов и принтеров в сетях AppleTalk обеспечивается протоколом AppleShare.

Замечание

Кабели и оборудование некоторых поставщиков, отличных от Apple, позволяют включать в сеть AppleTalk больше компьютеров, чем 32.

Принцип действия AppleTalk

В сетях AppleTalk используется адресная схема. Каждый компьютер, подключаемый к сети, ищет хранимый адрес, который он использовал в предыдущем сеансе. Если компьютер находит этот адрес, то использует его. В противном случае он присваивает себе адрес, случайно выбранный из набора предлагаемых адресов. Затем компьютер сообщает этот адрес всем другим компьютерам, чтобы определить, использует ли его еще кто-нибудь. Если да, то процесс поиска адреса повторяется. Если нет, то компьютер сохраняет этот адрес для использования в следующих сеансах.

Архитектура AppleTalk разрабатывалась для небольших сетей. Однако отдельные сети можно соединять друг с другом. Каждая подсеть называется *зоной*. Для идентификации ей присваивается имя. Работают зоны аналогично рабочим группам. Чтобы получить доступ к ресурсам другой зоны, нужно указать ее имя.

Сети AppleTalk можно подключать к сетям с другими архитектурами, такими как Ethernet или Token Ring. Компания Apple предоставляет сетевые адаптеры EtherTalk и TokenTalk, с помощью которых компьютеры Macintosh можно подключать к сетям, определенным спецификациями 802.3 и 802.5 соответственно.

Преимущества AppleTalk

Программное обеспечение AppleTalk включено компанией Apple в операционную систему Macintosh, поэтому сети AppleTalk легко устанавливать и конфигурировать. Установить небольшую рабочую группу компьютеров Macintosh просто и недорого.

Недостатки AppleTalk

Архитектура AppleTalk не предназначена для больших сетей. Ее пропускная способность (230,4 Кбит/с) по сравнению с другими локальными архитектурами невелика, поэтому в ней трудно или вообще невозможно реализовать высокоскоростные приложения.

Передача данных в LocalTalk

LocalTalk представляет собой протокол канального уровня, который первоначально использовался в сетях AppleTalk. Компьютеры Macintosh, использующие LocalTalk, соединяются друг с другом посредством принтерных портов.

Замечание

В сетях AppleTalk первоначально использовались кабели LocalTalk, однако соединение может быть реализовано также посредством Ethernet. Такое решение становится все более популярным, потому что сама LocalTalk обладает низкой пропускной способностью (230,4 Кбит/с) и разрабатывалась для небольших рабочих групп с низкой загрузкой сети.

Сводка характеристик AppleTalk

Главным недостатком AppleTalk является низкая производительность. Однако пакет протоколов AppleTalk позволяет быстро и легко объединить компьютеры Macintosh в небольшие рабочие группы для разделения файлов, принтеров и других ресурсов.

Сети ARCnet

Архитектура ARCnet (Attached Resource Computer Network) старше других локальных сетевых технологий. В ней используется специальный метод доступа с передачей маркера в звездообразной шинной топологии.

В некоторых книгах ARCnet ассоциируется со спецификациями 802.4, в которых маркер передается по магистрали, однако ARCnet фактически была разработана до появления стандартов 802 и не полностью им соответствует. Простая и недорогая архитектура ARCnet предназначена для небольших рабочих групп.

Принцип действия ARCnet

Метод передачи маркера, используемый в ARCnet, отличается от используемого в Token Ring. В сетях ARCnet маркер проходит не по физическому пути на основе расположения компьютеров, а от одного компьютера к другому согласно предопределенной их нумерации (рис. 5.9). Поэтому ARCnet является довольно неэффективной средой: для достижения адресата данные могут проходить намного больший путь, чем необходимо.

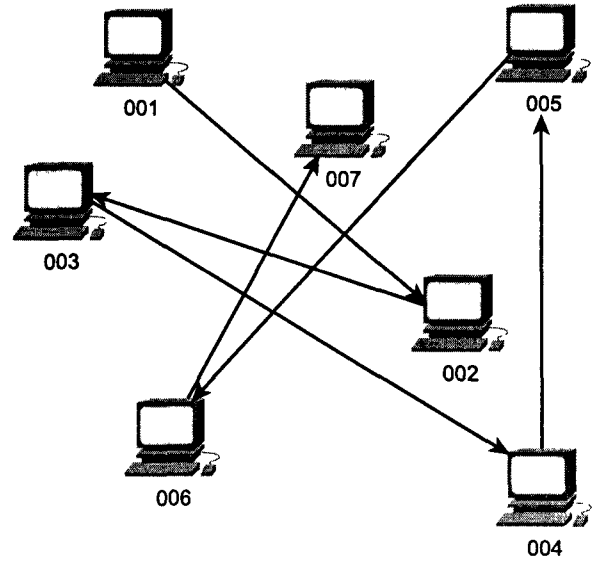


Рис. 5.9 Используемый в ARCnet метод передачи маркера может привести к неэффективному маршруту передачи данных

Спецификации ARCnet

Для соединения компьютеров в звездообразную магистраль в ARCnet используются концентраторы и 95-омные коаксиальные кабели RG-62 A/U. Однако сеть ARCnet может работать также на витых парах и волоконно-оптических кабелях.

Если используется коаксиальный кабель (что более распространено), то максимальная длина сегмента от компьютера к концентратору составляет 610 метров. Если

используется неэкранированная витая пара, то максимальная длина сегмента уменьшается до 244 метров.

Замечание

В ARCnet на коаксиальном кабеле может использоваться не звездообразная, а шинная топология. В этом случае максимальная длина сегмента равна 305 метрам.

Стандартная ARCnet обладает низкой производительностью: ее пропускная способность равна всего лишь 2,5 Мбит/с. Пропускная способность более поздней версии ARCnet Plus составляет 20 Мбит/с.

Преимущества ARCnet

Архитектура ARCnet недорогая и хорошо работает в небольших сетях. Архитектура ARCnet Plus обладает более высокой пропускной способностью, чем стандартная Ethernet.

Недостатки ARCnet

Технология ARCnet старше и менее популярна, чем Ethernet или Token Ring. Ее сетевые компоненты сложно достать. Трудно также найти специалистов, хорошо знакомых с ARCnet. Даже ее более быстрая версия ARCnet Plus по производительности весьма далека от 100BaseT, поэтому она не предназначена для высокоскоростных приложений.

Структура пакета ARCnet

Порция данных, передаваемая по сети ARCnet, называется *пакетом* (в Ethernet и Token Ring — *кадром*). Структура стандартного пакета ARCnet очень проста (рис. 5.10).



Рис. 5.10. В пакете ARCnet содержатся только адреса и данные

Как видно из рис. 5.10, поля заголовка и трейлера содержат адреса передающего и принимающего компьютеров. Между заголовком и трейлером располагаются данные. Длина стандартного пакета ARCnet ограничена 506 байтами данных, пакет ARCnet Plus может содержать до 4 096 байт.

Сводка характеристик ARCnet

Простые сети ARCnet в настоящее время во многих местах и средах заменяются сетями Ethernet и Token Ring. Хотя архитектура ARCnet относительно недорогая и ее производительность достаточна для небольших и слабо загруженных сетей, тем не менее ограниченная пропускная способность и неэффективный метод передачи маркера служат причиной неуклонного падения популярности ARCnet.

Сравнение сетевых архитектур

В табл. 5.3 приведены характеристики наиболее распространенных сетевых архитектур.

Таблица 5.3. Сравнение характеристик сетевых архитектур

Архитектура	Тип кабеля	Пропускная способность	Метод доступа	Топология
Ethernet 10Base2	Тонкий коаксиальный	10 Мбит/с	CSMA/CD	Шинная
Ethernet 10Base5	Толстый коаксиальный	10 Мбит/с	CSMA/CD	Шинная
Ethernet 10BaseT	Неэкранированная витая пара категорий 3–5	10 Мбит/с	CSMA/CD	Звезда
Ethernet 100BaseT	Неэкранированная витая пара категории 5	100 Мбит/с	CSMA/CD	Звезда
Ethernet 100BaseFX	Волоконно-оптический	100 Мбит/с	CSMA/CD	Звезда
Ethernet 1000BaseT	Неэкранированная витая пара категории 7	1 Гбит/с	CSMA/CD	Звезда
Token Ring	Экранированная или неэкранированная витая пара	4 или 16 Мбит/с	Передача маркера	Физическая звезда, логическое кольцо
FDDI	Волоконно-оптический	100 Мбит/с	Передача маркера	Двойное кольцо
AppleTalk	Экранированная или неэкранированная витая пара	LocalTalk 230,4 Мбит/с, Ethernet 10 Мбит/с	CSMA/CA	LocalTalk шинная, Ethernet звезда

Резюме

В этой главе рассмотрены характеристики и спецификации нескольких наиболее популярных архитектур локальных сетей.

Одна из наиболее распространенных локальных сетевых архитектур — Ethernet — определяется спецификациями IEEE 802.3. В ней используется метод доступа CSMA/CD. Были описаны следующие варианты Ethernet:

- 10Base2 (тонкая сеть);
- 10Base5 (толстая сеть);
- 10BaseT, 100BaseT и 1000BaseT.

Кроме того, обсуждалась архитектура Token Ring, определяемая спецификациями IEEE 802.5, и принцип действия сетей на ее основе. Затем была представлена архитектура FDDI, в которой используются волоконно-оптические кабели и метод переда-

чи маркера. Архитектура FDDI предназначена для городских и больших локальных сетей. Далее рассматривалась архитектура AppleTalk и ее составляющие: LocalTalk, AppleShare, EtherTalk и TokenTalk. Описана также архитектура ARCnet: более старая технология, в которой используется уникальная схема передачи маркера по логическому, а не физическому пути.

В следующей главе мы расширим горизонт за пределы локальных сетей и рассмотрим концепции и практическую реализацию глобальных сетевых архитектур. Будет рассмотрена реализация наиболее распространенных типов глобальных сетей, а также способы объединения локальных сетей в глобальную (включая самую глобальную сеть — Internet).

Рекомендуемые источники

Дополнительную информацию о соединениях локальных сетей можно найти в следующих источниках.

- Web-узел Чарльза Сперджена (Charles Spurgeon) с информацией об Ethernet 802.3 находится по адресу: `wwwhost.ots.utexas.edu/ethernet/ethernet-home.html`.
- Web-узел Консорциума Token Ring находится по адресу: `www.iol.unh.edu/training/fddi/htmls/index.html`.
- С официальными документами *Core Competence AppleTalk* (Ключевые сведения по AppleTalk) можно ознакомиться по адресу: `www.corecom.com/html/appletalk.html`.
- Web-узел Ассоциации поставщиков ARCnet имеет адрес: `www.arcnet.com/home.html`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Какая архитектура определяется спецификацией IEEE 802.3?
   - **а.** Token Ring.
   - **б.** Ethernet.
   - **в.** ARCnet.
   - **г.** FDDI.
2. Какой метод доступа к сети используется в Ethernet?
   - **а.** CSMA/CD.
   - **б.** CSMA/CA.
   - **в.** Передача маркера.
   - **г.** Приоритеты запросов.
3. Чему равно максимальное количество узлов на сегмент кабеля в Ethernet 10Base2?
   - **а.** 30.
   - **б.** 100.
   - **в.** 185.

г. 1 024.

4. С каким типом кабеля используется разъем BNC?
   а. Неэкранированная пара.
   б. Толстый коаксиальный кабель.
   в. Тонкий коаксиальный кабель
   г. Волоконно-оптический кабель.
5. Какая архитектура называется стандартной Ethernet?
   а. 10BaseT.
   б. 100BaseT.
   в. 10Base2.
   г. 10Base5.
6. Какая максимальная длина кабеля специфицирована для сетей 10Base5?
   а. 100 метров.
   б. 500 метров.
   в. 100 футов.
   г. 500 футов.
7. Какое из приведенных утверждений справедливо для архитектуры Token Ring? (Выберите все подходящие.)
   а. Топология Token Ring является пассивной.
   б. Пропускная способность сети Token Ring равна 4 или 16 Мбит/с
   в. Концентраторы Token Ring называются устройствами многостанционного доступа.
   г. В сетях Token Ring используются модулированные сигналы.
8. Как называется проходящий по кругу сигнал, посылаемый управляющим компьютером в сети Token Ring для обнаружения вышедшего из строя узла и повторной конфигурации сети с целью восстановления коммуникации?
   а. Маркер.
   б. Кадр данных.
   в. Маяк.
   г. NAUN.
9. Как называется протокол канального уровня, первоначально разработанный для сетей AppleTalk?
   а. Ethernet.
   б. LocalTalk.
   в. EtherTalk.
   г. TokenTalk.
10. Чему равна пропускная способность стандартной ARCnet?
    а. 2,5 Мбит/с.
    б. 25 Мбит/с.
    в. 16 Мбит/с.
    г. 10 Мбит/с.

Глава 6

Глобальные сети

Носители, оборудование и программное обеспечение, хорошо работающие на небольших расстояниях в локальных и городских сетях, совершенно непригодны для глобальных сетей с их большими расстояниями. В современном мобильном мире необходимы все более производительные, эффективные и дешевые технологии глобальных сетей. Этому есть несколько причин.

- Руководителям и работникам компаний нужен доступ к корпоративным сетям, когда они находятся в дороге или дома.
- Появляется все больше компаний с офисами, разбросанными по всему миру, с которыми нужно поддерживать постоянную и надежную связь.
- Многие организации нуждаются в информации других организаций, удаленных на большие расстояния.
- Коммерческим, правительственным и учебным учреждениям, а также отдельным лицам нужен доступ к ресурсам всемирной сети Internet.

Очевидно, невозможно протянуть кабель Ethernet от центрального офиса в Москве к филиалу компании во Владивостоке. А тем более к узлам, расположенным на другом континенте.

Для глобальных сетей нужны совершенно другие носители, оборудование и сетевые спецификации. В этой главе рассматриваются основные концепции компьютерной коммуникации на больших расстояниях и технологии, используемые для соединения компьютеров, расположенных в разных странах и даже на разных континентах. Эти технологии варьируют от хорошо всем знакомой общедоступной телефонной сети PSTN (Public Switched Telephone Network — коммутируемая телефонная сеть общего пользования) до таких новейших технологий, как спутниковая коммуникация, с помощью которой можно "разговаривать" с компьютерами на космической орбите.

Разработчикам глобальных сетей пришлось преодолеть многие трудности, которых не было при реализации локальных сетей в географически небольших регионах. Глобальная сеть — это не просто большая локальная сеть. Это набор отдельных локальных сетей, соединенных каналами связи, совершенно отличными от каналов локальных сетей. В глобальных сетях, пересекающих границы стран должны быть учтены многие факторы, такие как разные часовые пояса и языковые отличия.

Конструирование глобальной сети — комплексная задача. При выборе оптимальных технологий нужно учитывать назначение сети, количество пользователей, требо-

вания к пропускной способности, сложившуюся практику пользователей и другие факторы. Вопросы, которые при этом нужно рассмотреть, классифицированы следующим образом.

- Оборудование глобальной сети.
- Топология сети.
- Типы сетевых коммутаторов.
- Новые технологии глобальных сетей.
- Соединения локальных сетей с глобальной.

В следующих разделах рассматривается каждый из этих вопросов.

Оборудование глобальных сетей

Оборудование, необходимое для реализации соединения глобальной сети, может быть очень простым и дешевым — достаточно телефонной линии и модемов на каждом конце. Однако оно может быть также весьма сложным и дорогим. В общем случае стоимость сетевого оборудования возрастает с ростом пропускной способности и надежности.

В следующих разделах рассматриваются наиболее распространенные устройства глобальных сетей, включая модемы, терминальные адаптеры ISDN (Integrated Services Digital Network) и DSL (Digital Subscriber Line), а также оборудование пользователя, необходимое для работы с выделенными каналами, такими как T-соединения и X.25.

Модемы

Чтобы установить сетевое соединение (с провайдером услуг Internet или с сервером удаленного доступа частной сети) по общедоступной телефонной линии, используются *модемы*.

Замечание

Слово "модем" отражает выполняемые им операции: *мо*дулирование и *дем*одулирование сигналов. На передающем конце модем преобразует сгенерированный компьютером цифровой сигнал в аналоговый, который можно передать по телефонной линии. На принимающем конце модем преобразует аналоговый сигнал обратно в цифровой.

Физически существует два типа модемов: *внутренние* и *внешние*. Каждый из них имеет свои достоинства и недостатки. Конфигурирование модема тоже зависит от типа.

Модем любого типа является устройством *последовательного действия*. Это означает, что биты информации передаются по одному — один за другим. В устройствах *параллельного действия* многие биты информации могут передаваться одновременно, например сигналы от компьютера к принтеру. Последовательная передача сигналов похожа на группу партизан, движущихся гуськом, а параллельная — на группу солдат, марширующих в шеренге.

Внутренние модемы

Одно из главных преимуществ внутреннего модема — компактность. Он представляет собой электронную плату, помещаемую внутри компьютера в стандартный

разъем ISA (Industry Standard Architecture) или PCI (Peripheral Component Interconnect), как показано на рис 6 1 Поэтому модем не занимает места на столе и его кабели не путаются под ногами

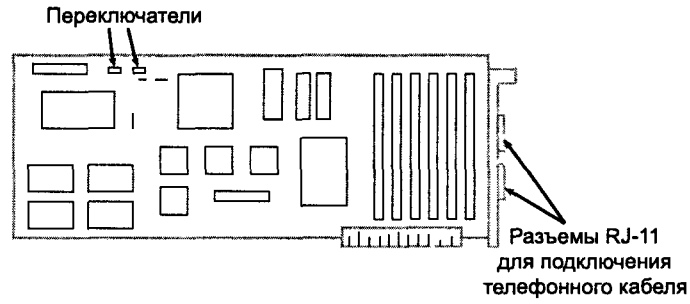


Рис 6 1 Внутреннии модем — это электронная плата, которая помещается в разъем компьютера

Параметры конфигурирования внутреннего модема

Внутренние модемы труднее конфигурировать, чем внешние Нужно установить номера IRQ, адреса ввода-вывода и виртуальные коммуникационные порты, причем необходимо, чтобы эти установки не конфликтовали с установками других устройств компьютера Рассмотрим каждый параметр подробнее

- **Номера IRQ (Interrupt Request)** Номер канала, по которому операционная система ожидает сигнал прерывания от этого устройства Если сигналы прерывания от разных устройств поступают на процессор по одной и той же линии, то они будут конфликтовать Поэтому каждому устройству должен быть присвоен свой IRQ
- **Адреса ввода-вывода** Адрес, по которому записываются принятые данные или откуда считываются передаваемые данные Как и для IRQ, этот адрес не должен совпасть с адресами ввода-вывода других устройств компьютера, иначе произойдет конфликт данных
- **Виртуальный коммуникационный порт** Номер логического порта, по которому операционная система идентифицирует последовательный порт Каждое устройство последовательного действия должно быть конфигурировано на использование своего коммуникационного порта

Все распространенные операционные системы содержат средства просмотра ресурсов С помощью этих средств можно проанализировать использование ресурсов и выделить для нового устройства свободный ресурс

Изменение установок внутреннего модема

Конфигурацию внутреннего модема можно изменить физически В зависимости от производителя и модели, установки IRQ, ввода-вывода и коммуникационного порта можно изменить с помощью следующих средств

- **Переключатель DIP** Впаянный в печатную плату пакет миниатюрных переключателей, рычажки которого можно передвигать в разные позиции Позиция переключателя определяет значение устанавливаемого параметра

- **Перемычки**. Пары металлических контактов, встроенных в плату. Перемычки конфигурируются путем вставки небольших заглушек, замыкающих электрическую цепь. В инструкции к внутреннему модему обычно указывается, какие перемычки нужно замкнуть, чтобы установить желаемые IRQ, адреса ввода-вывода и коммуникационные порты.
- **Программное обеспечение**. В некоторых модемах нет физических переключателей или перемычек. Чтобы конфигурировать такой модем, нужно запустить специальную программу, прилагаемую к модему.

Конфигурирование устройств Plug and Play

Во многих современных модемах поддерживается технология *PnP* (*Plug and Play*). Это означает, что операционная система самостоятельно обнаруживает новое устройство, устанавливает необходимые драйверы, определяет свободные ресурсы компьютера и автоматически присваивает их новому устройству. При этом вмешательство пользователя сведено к минимуму или вообще не требуется.

Технология PnP великолепна! Однако, только если она работает и если пользователь кое-что предусмотрит. А именно следующее: если вы купили модем или другое устройство, на коробке которого написано "Plug and Play", то автоматическое конфигурирование произойдет *только* при выполнении двух условий:

- система BIOS компьютера должна поддерживать PnP;
- операционная система компьютера должна поддерживать PnP.

Должны быть удовлетворены оба критерия. Системные платы компьютеров, выпущенные после 1995 года, обычно поддерживают PnP. Поддерживают PnP также операционные системы Windows 95/98/ME и Windows 2000/XP.

Замечание

Операционная система Windows NT *не поддерживает* PnP. Однако в ней все же есть некоторые ограниченные средства PnP, с помощью которых можно автоматически конфигурировать некоторые типы модемов.

Внешние модемы

По сравнению с внутренними внешние модемы имеют некоторые преимущества.

- В большинстве внешних модемов на переднюю панель выведена индикация состояния модема, т.е. включен ли он и передает ли данные (рис. 6.2).
- Внешние модемы легче устанавливать и конфигурировать. В них нет внутренних переключателей и перемычек. Кроме того, для их установки не нужно открывать компьютер.

Для внешних модемов нужен кабель питания для подключения к электрической сети, однако внутренние модемы питаются по шине компьютера. Внешний модем подключается к одному из последовательных портов на задней стенке компьютера с помощью последовательного кабеля.

Последовательные порты

Для подключения внешнего модема нужен свободный *последовательный порт*. В большинстве компьютеров есть два встроенных последовательных порта: COM1 и COM2. Их разъемы расположены на задней стенке компьютера.

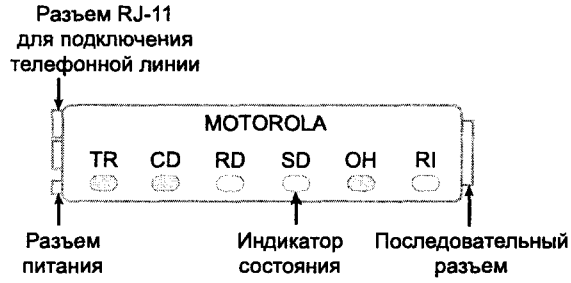


Рис. 6.2. Индикация состояния внешнего модема

Последовательные порты используются многими устройствами, такими как сканеры, цифровые камеры и устройства указания. Если в компьютере нет свободного последовательного порта, то можно поступить одним из следующих способов:

- использовать внутренний модем;
- установить на компьютер карту расширения, которая добавляет последовательные порты;
- если системная плата компьютера поддерживает USB (Universal Serial Bus), то к одному последовательному порту можно подключить несколько устройств последовательной связи. Однако для этого может понадобиться добавить карту с разъемом USB или использовать модем USB.

Микросхемы UART

Для обработки сигналов в последовательных портах используются микросхемы UART (Universal Asynchronous Receiver/Transmitter). Существуют различные типы микросхем UART, определяющих скорость передачи данных в последовательном порту.

В первых персональных компьютерах стояли микросхемы UART 8250 с максимальной скоростью передачи 9 600 бит/с. Это значит, что если к одному из портов подключен модем, например, на 56 Кбит/с, то скорость передачи все равно будет ограничена пропускной способностью UART и составит 9 600 бит/с.

В современных компьютерах устанавливаются микросхемы UART серии 16450 или 16550, обеспечивающие пропускную способность последовательных портов до 115 200 бит/с.

Микросхемы UART 16650 и 16750 могут поставляться как добавляемые карты расширения последовательных портов. Внутренние модемы имеют собственные микросхемы UART, поэтому быстродействие коммуникационных портов компьютера для них не имеет значения.

Замечание

Если к вашему современному компьютеру подключен быстродействующий модем, а скорость передачи все же невелика, проверьте конфигурацию коммуникационных портов. Некоторые операционные системы по умолчанию устанавливают быстродействие портов 9 600 бит/с. Для реализации ожидаемого быстродействия нужно изменить этот параметр.

Драйверы модемов

Драйвер — это программа, служащая связующим звеном между операционной системой и устройством. Обычно драйвер поставляется вместе с устройством. Его можно также загрузить с Web-узла производителя. Для устройства желательно использовать его "родной" драйвер.

Конфигурирование модема

Итак, необходимо установить драйвер, позволяющий операционной системе "увидеть" модем, и конфигурировать IRQ, адрес ввода-вывода и коммуникационный порт, используемый модемом. Однако, кроме этого, нужно конфигурировать модем на набор телефонного номера и поддержку соединения. В современных операционных системах есть встроенные средства набора номера. Если при установке операционной системы модема еще не было, то может также понадобиться установка службы удаленного доступа.

Пулы модемов

Компьютер можно сконфигурировать как *сервер удаленного доступа*. Это позволит другим компьютерам, набрав номер телефона, на котором установлен сервер удаленного доступа, установить с ним соединение. Серверное программное обеспечение может одновременно поддерживать множество входных соединений удаленного доступа, например Windows NT Server поддерживает до 256 соединений.

Как же подключить к серверу удаленного доступа 256 модемов? Если нужно устанавливать много коммутируемых соединений (например, когда сервер принадлежит компании, где большинство сотрудников работают дома), то можно использовать *пул модемов*.

Пул модемов позволяет использовать группу модемов (обычно установленных вместе в стойке) и один сервер для одновременного обслуживания многих удаленных соединений. Стойка с модемами может быть подключена к серверу, маршрутизатору или непосредственно к локальной сети. Естественно, для каждого соединения нужна своя телефонная линия.

Адаптеры ISDN и DSL

Устройства, используемые для подключения компьютера к телефонной линии ISDN (Integrated Services Digital Network — цифровая сеть связи с комплексными услугами) или DSL (Digital Subscriber Line — цифровая абонентская линия), иногда называют модемами. Однако более правильное название — *терминальные адаптеры*, потому что они не модулируют и не демодулируют сигнал, так как линии ISDN и DSL цифровые (в отличие от обычных аналоговых телефонных линий).

Адаптеры ISDN

Адаптеры ISDN, как и модемы, поставляются во внутреннем и внешнем исполнении. Их конфигурирование аналогично конфигурированию модемов. Типичная линия ISDN на 128 Кбит/с состоит из двух каналов по 64 Кбит/с каждый. Для обеспечения пропускной способности 128 Кбит/с два канала обычно используются в *многоканальной* конфигурации. Технология ISDN рассматривается далее в главе.

В большинстве случаев два канала данных имеют отдельные телефонные номера. В конфигурацию адаптеров ISDN входит информация о *SPID* (*Service Profile Identifier — идентификатор услуги и линии*) для каждого канала, т.е. номер телефона, двухцифровой

идентификатор разделяемого терминала и двухцифровой идентификатор терминала TID (Terminal Identifier). Некоторые современные адаптеры ISDN обеспечивают автоматический выбор параметров SPID и не требуют ручного ввода этой информации.

Адаптеры DSL

На обоих концах соединения DSL должно быть установлено конечное устройство, которое иногда называют *модемом DSL*. Это устройство подключается к сетевому адаптеру Ethernet, установленному в компьютере. Конечное устройство может быть как внешним, так и встроенным в сетевой адаптер компьютера.

Оборудование пользователя

Этот термин может обозначать несколько различных устройств, установленных у пользователя. На узле пользователя это оборудование применяется для обработки данных, поступающих по каналам связи глобальных сетей, таким как Т-линии, соединения X.25 и соединения Frame Relay.

Обычно используются следующие типы пользовательского оборудования.

- Устройства CSU/DSU (Channel Service Unit/Digital Service Unit — модуль обслуживания канала и данных) используются в коммутируемых соединениях, например с линией Т-1. Устройство CSU принимает и передает сигналы по линии глобальной сети. Устройство DSU управляет линией, обрабатывает ошибки и регенерирует сигналы.
- Устройство PAD (Packet Assembler/Disassembler — сборщик/разборщик пакетов) используется в соединениях с коммутацией пакетов, таких как X.25. Это асинхронное устройство. Оно позволяет многим терминалам использовать одну линию сети одновременно. Пользователь может, набрав номер PAD, подключиться к нему с помощью модема.

Топологии глобальных сетей

В главе 2, "Классификация компьютерных сетей", рассматривались топологии локальных сетей, во многом аналогичные топологиям глобальных сетей. Однако применительно к глобальным сетям термин *топология* означает размещение средств передачи данных.

Простейшей топологией глобальной сети является точечное соединение. В глобальных сетях используются также традиционные топологии локальных сетей, такие как звезда или кольцо.

Точечная топология

Топология точечной глобальной сети похожа на шинную топологию локальной сети. Линия удаленного доступа (любая, от модема на 56 Кбит/с вплоть до выделенной линии Т-1) соединяет каждую точку глобальной сети со следующей точкой (рис. 6.3).

Это относительно простой и недорогой способ соединения небольшого количества узлов глобальной сети. Однако его устойчивость к отказам невелика. Если в сети, изображенной на рис. 6.3, выйдет из строя оборудование в Далласе, то Сан-Франциско и Бостон не смогут сообщаться друг с другом. Другим недостатком точечной топологии является ограниченная возможность "плавного" наращивания, т.е. на-

ращивания без прекращения эффективной работы сети. Если в эту сеть добавить еще одну точку между Далласом и Бостоном, то увеличится количество транзитных передач между Бостоном и Далласом или Сан-Франциско.

Замечание

Транзитная передача — это передача данных от одного маршрутизатора к другому. *Количество транзитных передач* — это количество маршрутизаторов на пути пакета от источника к адресату.

Точечная топология удовлетворительно работает только в небольших глобальных сетях с двумя или тремя точками.

Кольцеобразная топология

Кольцеобразная топология образуется, если замкнуть линию точечной топологии (рис. 6.4).

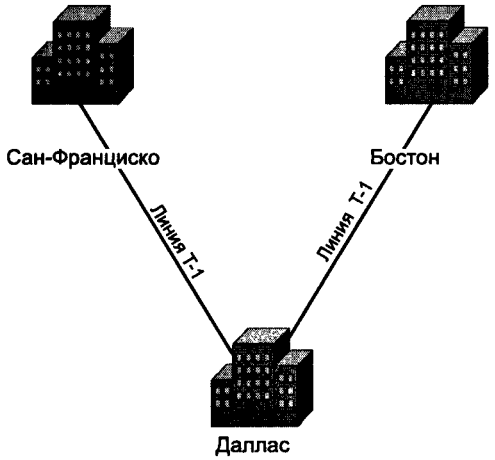


Рис. 6.3. В поточечной глобальной сети непосредственно соединены две точки

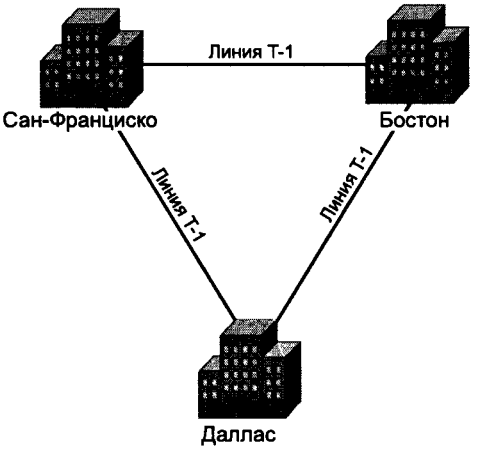


Рис. 6.4. Глобальная сеть с кольцеобразной топологией

Кольцеобразная топология избыточна. Если в сети, показанной на рис. 6.4, выйдет из строя линия между Далласом и Сан-Франциско, данные смогут проходить через Бостон.

Реализация кольцеобразной топологии более дорогая, чем точечной. Кроме того, возможности наращивания сети с кольцеобразной топологией так же ограниченны, как и с точечной.

Кольцеобразная топология рекомендуется для глобальных сетей с повышенными требованиями к надежности, однако содержащих не более нескольких точек.

Звездообразная топология

В глобальной сети с топологией звезды используется *концентратор-маршрутизатор*, служащий центральной точкой, к которой подключаются маршрутизаторы всех локальных сетей. В примере глобальной сети, изображенной на рис. 6.5, концентратор-маршрутизатор расположен в Далласе.

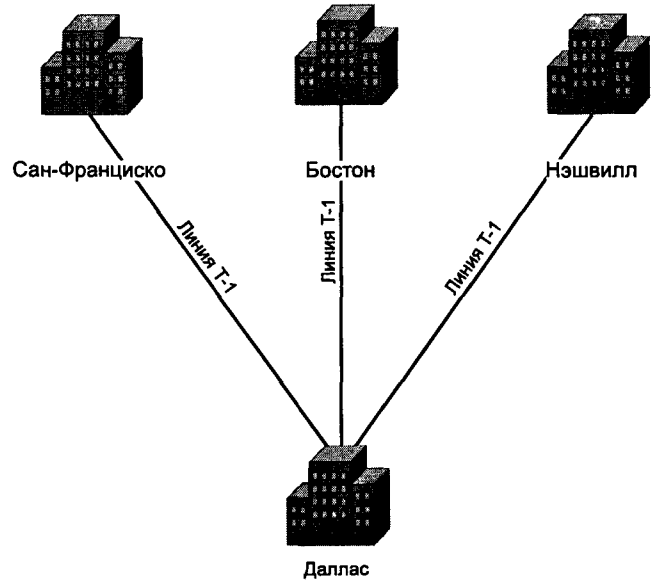


Рис 6 5 Глобальная сеть с топологией звезды

Возможности расширения сети с топологией звезды выше, чем сети с кольцевой или точечной топологией В нее легче добавлять новые точки

Недостатком звездообразной топологии является критическая для отказа точка В примере на рис 6 5 такая критическая точка — концентратор-маршрутизатор в Далласе Если он выходит из строя, то прекращается коммуникация между всеми точками сети

Полностью и частично ячеистые топологии

В ячеистой топологии соединения существуют между всеми точками сети Это наиболее надежная и отказоустойчивая топология К сожалению, она также и наиболее дорогая Кроме того, с увеличением числа узлов количество соединений растет ужасающими темпами

В полностью ячеистой топологии каждый узел сети должен быть соединен с каждым другим узлом В частично ячеистой топологии это требование не обязательно Надежность сети с частично ячеистой топологией почти такая же, как и с полностью ячеистой, причем ее стоимость значительно ниже

Примеры сетей с полностью и частично ячеистой топологией приведены в главе 2, "Классификация компьютерных сетей", на рис 2 10 и 2 11

Многоуровневые глобальные сети

Как и в звездообразной, в многоуровневой глобальной сети используются концентраторы-маршрутизаторы, однако эта сеть значительно надежнее благодаря тому, что в ней концентраторы соединены с другими узлами каскадно (рис 6 6)

Многоуровневая глобальная сеть легко расширяется, потому что в нее легко добавлять новые узлы и даже уровни Эта топология используется в больших быстрорастущих сетях

В больших многоуровневых глобальных сетях серьезной проблемой может стать чрезмерная загрузка отдельных линий Чтобы избежать этого, нужно тщательно анализировать загрузку линий и размещать оборудование оптимальным образом

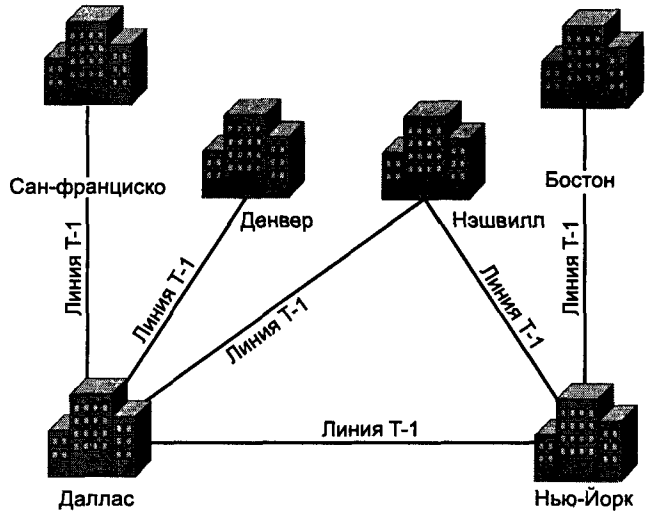


Рис. 6.6. Многоуровневая глобальная сеть более надежна, чем простая звезда

Типы коммутации

Данные могут проходить на пути к адресату по нескольким различным типам линий, однако при этом используется только один из двух типов коммутации:

- коммутация каналов;
- коммутация пакетов.

Далее в этом разделе оба типа коммутации рассматриваются подробнее.

Коммутация каналов и пакетов

Многие не знают, чем отличается коммутация каналов от коммутации пакетов. Примером сети с коммутацией каналов служит телефонная сеть. Если набрать номер филиала компании в Бостоне, то на все время разговора электрическая цепь, соединяющая с Бостоном, остается замкнутой. Сигнал проходит по этому каналу (пути) до тех пор, пока один из говорящих не повесит телефонную трубку. Если завтра позвонить по этому же номеру, то, возможно, сигнал будет проходить по другому пути.

Примером сети с коммутацией пакетов является Internet. Если отправить электронное письмо в Бостон, то оно будет разбито на небольшие части, называемые *пакетами*. Каждый пакет может пройти по другому пути, однако в принимающем компьютере все они собираются вместе и компьютер составляет из них посланное письмо.

Сети с коммутацией каналов

Сначала рассмотрим сети, построенные на основе коммутации каналов.

Коммутируемые и выделенные соединения

В сетях с коммутацией каналов могут устанавливаться как коммутируемые, так и выделенные соединения. Коммутируемое соединение — это *временное* соединение, установленное только на период одного сеанса связи. Однако коммутируемое соединение может быть "вечным" — набрав номер удаленного сервера и установив с ним соединение, можно не заканчивать сеанс связи сколь угодно долго. Коммутируемое соединение позволяет также в любой момент прервать сеанс связи и установить соединение с другим абонентом. Например, можно прервать соединение с одним провайдером Internet и установить с другим.

В противовес этому выделенное соединение устанавливается между двумя пунктами "навсегда", т.е. пока не будет демонтирована линия.

Технология коммутируемых каналов имеет долгую историю, она значительно старше технологии коммутируемых пакетов. Коммутация каналов работает удовлетворительно, когда данные должны передаваться в реальном времени, например для телефонного разговора. Можно сказать, что сети с коммутацией каналов ориентированы на соединение, потому что соединение устанавливается для каждого сеанса связи.

В следующих подразделах кратко рассматриваются такие технологии коммутации каналов:

- PSTN;
- ISDN;
- DSL;
- выделенные линии;
- DDS;
- T-носители;
- Switched 56.

PSTN

Сеть PSTN (Public Switched Telephone Network — коммутируемая телефонная сеть общего пользования) является традиционной аналоговой телефонной сетью. Для установки связей в глобальных сетях она используется довольно часто.

Использование PSTN имеет два существенных преимущества:

- линии PSTN есть практически везде;
- эта связь недорогая.

Коммутируемое соединение по обычной телефонной линии просто установить Кроме модема не требуется никакого дополнительного оборудования. Аналоговые модемы широко доступны и недороги, их легко конфигурировать.

Первоначально телефонная система создавалась не для передачи данных, а для голосовой связи. Поскольку высокая скорость передачи не требовалась, телефонным линиям присуще "врожденное" ограничение пропускной способности.

Важным фактором является также качество телефонной линии. Высококачественные модемы рассчитаны на максимальную пропускную способность 56 Кбит/с, однако из телефонной линии редко можно "выжать" более 40–45 Кбит/с. Обычная же скорость передачи — около 20 Кбит/с, а то и меньше.

ISDN

Технология ISDN (Integrated Services Digital Network — цифровая сеть связи с комплексными услугами) разработана для постепенной замены PSTN. Она обеспечивает более надежное цифровое соединение, предназначенное как для голоса, так и для данных. Замена PSTN не состоялась и, видимо, уже не состоится, поскольку появились более быстродействующие технологии по более низкой цене, однако ISDN все же имеет весьма существенные достоинства.

Для сетей ISDN характерны следующие особенности.

- ISDN — это цифровая связь. Поскольку при передаче данных их не нужно преобразовывать в аналоговый сигнал, а затем обратно в цифровой, производительность и надежность линии повышается.
- Линии ISDN более распространены, чем их новый конкурент DSL.
- Хотя это коммутируемая технология, линии ISDN могут быть выделенными.
- Услуги ISDN дороже услуг PSTN. Для ISDN требуется специальное оборудование (цифровые коммутаторы) как на телефонной станции, так и у пользователя (терминальные адаптеры ISDN).

Цепь ISDN состоит из одного или большего количества каналов, переносящих данные (каналы-носители, или B-каналы), и управляющего канала (дельта-канал, или D-канал).

Каждый B-канал имеет пропускную способность 64 Кбит/с. Несколько B-каналов могут быть агрегированы (объединены) методом *инверсного мультиплексирования*. При этом пропускные способности агрегируемых каналов суммируются и образуется высокоскоростное соединение. В зависимости от реализации интерфейса, пропускная способность D-канала составляет 16 или 64 Кбит/с.

Большинство телефонных компаний предлагают услуги ISDN с двумя интерфейсами доступа.

- **BRI (Basic Rate ISDN)**. Интерфейс состоит из двух B-каналов на 64 Кбит/с (агрегированный канал — 128 Кбит/с) и одного D-канала на 16 Кбит/с.
- **PRI (Primary Rate ISDN)**. Интерфейс состоит из 23 B-каналов на 64 Кбит/с (агрегированный канал — 1,472 Мбит/с) и одного D-канала на 64 Кбит/с.

Интерфейс BRI чаще всего устанавливается на телефонных станциях в жилых кварталах, небольших компаниях, а PRI — для цифровой передачи голоса посредством телефонных систем PBX (Private Branch Exchange).

Замечание

Система PBX — это частная телефонная станция, работающая внутри организации (другое название — офисная телефонная станция). Ее внутренние пользователи имеют обычный доступ к внешним линиям. Для установки соединения внутри организации нужно набрать несколько цифр. В системе PBX на старом оборудовании нужен был оператор на коммутационной панели, отвечающий на внешние звонки и переключающий их на внутренние линии. В системах на современном оборудовании этот процесс автоматизирован.

DSL

Технология DSL относительно новая. Услуги DSL предлагаются телефонными станциями дополнительно к обычной телефонной связи. При этом используются уже существующие телефонные провода. По сравнению с другими типами соединений, использование в глобальной сети системы DSL предоставляет некоторые преимущества.

Ниже приведен список основных характеристик системы DSL.

- Пропускная способность DSL приближается (или выше) к пропускной способности линий T-1 при значительно меньшей стоимости. Во многих регионах услуги DSL стоят меньше, чем ISDN.
- Система DSL подключена всегда. Для установки соединения нет необходимости набирать телефонный номер.
- По одной линии могут одновременно передаваться как данные, так и голос.
- В настоящее время доступность системы DSL ограниченна. На телефонной станции, обслуживающей регион, должно быть установлено оборудование DSL, и — особая "прелесть" системы DSL — клиент должен находиться на небольшом расстоянии от этой станции.

Существует несколько разновидностей системы DSL.

- **ADSL (Asymmetric DSL — асимметричная DSL)**. Наиболее распространенная реализация. Ее пропускная способность может находиться в пределах от 384 Кбит/с до 6 Мбит/с (или больше) в направлении от телефонной станции к пользователю. В обратном направлении пропускная способность ниже.
- **SDSL (Symmetric DSL — симметричная DSL)**. Поддерживает одинаковую пропускную способность в обоих направлениях.
- **HDSL (High Data Rate DSL — DSL с высокой пропускной способностью)**. Поддерживает пропускную способность 768 Кбит/с в обоих направлениях.
- **VDSL (Very High Data Rate DSL — DSL с очень высокой пропускной способностью)**. Пропускная способность этой реализации находится в пределах от 13 до 52 Мбит/с.
- **IDSL**. Предоставление услуг DSL по линиям ISDN. Максимальная пропускная способность этой реализации может достигать 144 Кбит/с, однако она доступна в регионах, в которых другие реализации DSL не работают.

Общее обозначение всех реализаций DSL — *xDSL*.

Наиболее распространенная в настоящее время реализация ADSL обеспечивает высокую пропускную способность в направлении от телефонной станции к пользователю (чаще всего 1,5 Мбит/с) и более низкую пропускную способность в обратном направлении. Такое соотношение скоростей передачи вполне оправдано, поскольку подавляющее большинство пользователей Internet передает на Web-узлы короткие запросы и принимает от них длинные ответы. Однако если вы захотите установить на своем компьютере Web- или FTP-сервер, то низкая пропускная способность в направлении к телефонной станции станет серьезным препятствием для загрузки ваших данных.

Для создания нескольких каналов в ADSL используется мультиплексирование с разделением по частоте, т.е. каждый канал работает на своей частоте. В некоторых реализациях ADSL используется метод *удаления эха*. Этот метод более эффективен, однако он сложнее и дороже.

В табл. 6.1 приведены результаты сравнения доступных в настоящее время реализаций DSL.

Таблица 6.1. Сравнение реализаций DSL

Тип DSL	Пропускная способность	Преимущества	Недостатки
ADSL	От 384 Кбит/с до 6 Мбит/с (к пользователю)	Относительно низкая цена; большая распространенность	Может быть установлена не далее 5 300 метров от телефонной станции, пропускная способность в направлении к станции значительно ниже
SDSL	До 3 Мбит/с	Одинаковая пропускная способность в обоих направлениях	Более дорогая и менее доступная, чем ADSL
IDSL	144 Кбит/с	Может быть установлена там, где DSL недоступна из-за расстояния	Более дорогая, чем ADSL; меньшая пропускная способность
HDSL	До 768 Кбит/с (к пользователю)	Пропускная способность выше, чем у IDSL и некоторых реализаций ADSL	Ограниченная доступность
VDSL	От 13 до 52 Мбит/с	Высокая пропускная способность, удовлетворяющая передачу аудио- и видеоданных в реальном времени	Ограниченная доступность, наиболее дорогой тип DSL

Выделенные линии

Для соединений глобальных сетей, требующих высокой производительности и надежности, можно арендовать линии у телефонных компаний. Выделенная линия обеспечивает постоянное соединение двух точек, например двух офисов или локальной сети компании с провайдером Internet.

DDS

Служба DDS (Digital Data Service) — одна из первых общедоступных цифровых систем коммуникации в США. Ее пропускная способность составляет 56 Кбит/с. В конкурентной борьбе с Т-носителями технология DDS проигрывает, потому что линии Т-1 предоставляют большую пропускную способность в пересчете на доллар.

Т-носители

Это выделенные цифровые цепи, арендуемые большими компаниями для передачи больших объемов данных с высокой скоростью, например для надежной аудио- и видеокоммуникации между двумя точками.

Обычно физическими носителями в Т-линиях являются медные провода, однако это могут быть коаксиальные кабели, волоконно-оптические кабели или беспроводные средства связи.

Для кодирования и декодирования данных, передаваемых по Т-носителям, обычно используются устройства CSU/DSU (Channel Service Unit/Digital Service Unit) на каждом конце соединения.

За последнее десятилетие цены на линии T-1 значительно упали, однако продолжают оставаться довольно высокими Например, аренда типичной линии T-1 в 10–20 раз дороже службы DSL при одной и той же скорости передачи 1,5 Мбит/с

Почему же пользователи соглашаются платить больше? Одна из причин — доступность линии T-1 Системы DSL появились на рынке недавно и установлены пока что не везде, но даже там, где они установлены, многие жилые кварталы и компании оказываются вне области их действия вследствие ограничений на расстояние

Другая причина — гарантированная пропускная способность, которая называется CIR (Committed Information Rate — согласованная скорость передачи информации) Когда телефонная компания предоставляет услуги DSL с 1,5 Мбит/с, то это значит, что 1,5 Мбит/с составляет максимально возможную скорость передачи Реально линия DSL может и не обеспечить эту скорость В то же время, если арендуется линия T-1, то телефонная компания гарантирует пропускную способность 1,544 Мбит/с Если решение задач корпорации, арендующей линию, существенно зависит от производительности сети, то это весьма важный фактор

В термине "T-носители" буква "T" означает *transmission — передача данных* Иногда этот тип линии называют DS (Data Signal) В табл 6 2 приведен список наиболее распространенных реализаций T-носителей

Таблица 6.2. Реализации T-носителей

Носитель	Обозначение DS	Скорость передачи, Мбит/с
T-1	DS-1	1,544
T-2	DS-2	6,312
T-3	DS-3	44 736
T-4	DS-4	274,760

Линии на основе T-носителей состоят из отдельных каналов на 64 Кбит/с Поэтому если пропускная способность всей линии не нужна, то можно арендовать часть линии T-1 (порциями по 64 Кбит/с)

Switched 56

Сеть Switched 56 представляет собой расширенную версию сети PSTN (традиционной аналоговой телефонной сети), в которой цифровые данные передаются по коммутируемым каналам со скоростью 56 Кбит/с на канал Аренда линий Switched 56 дешевле, чем линий T-1, однако их пропускная способность намного ниже Соединения Switched 56 коммутируемые, поэтому они используется в тех случаях, когда выделенное соединение не нужно

В сетях PSTN скорость передачи теоретически может достигнуть 56 Кбит/с, однако на практике довольно редко достигается скорость 50 Кбит/с, а чаще всего — значительно меньше В отличие от этого, пропускная способность линии Switched 56 гарантированно составляет 56 Кбит/с Поскольку это цифровое соединение, количество возникающих в нем ошибок значительно меньше, чем в аналоговых линиях PSTN

Соединение называется Switched (переключаемое) потому, что в нем используется (переключается на пользователя) отдельный канал линии T-1 с пропускной способностью 56 Кбит/с

Популярность сетей Switched 56 падает по мере распространения более дешевых и скоростных линий ISDN и DSL

Сети с коммутацией пакетов

В этих сетях пакеты данных могут проходить от передающего компьютера к принимающему разными маршрутами. На принимающем конце пакеты собираются в правильном порядке. Сети с коммутацией пакетов иногда сравнивают с облаками, потому что точный маршрут передачи данных неизвестен.

Существуют следующие технологии передачи пакетов:

- X.25;
- Frame Relay;
- ATM (Asynchronous Transfer Mode).

Далее рассматривается каждая из этих технологий.

X.25

Сети X.25 — один из первых типов сетей с коммутацией пакетов. Они были разработаны для связи с мэйнфреймами, такими как IBM 360. В сетях X.25 используется аналоговая передача данных.

Замечание

Довольно часто употребляется термин *сети X.25*, однако более правильное название — *PSDN (Public Switched Data Network — общедоступная сеть с коммутацией данных)*. Для передачи данных между терминальным оборудованием и сетью используется протокол X.25

Первоначально протокол X.25 назывался ARPAnet 1822. Название X.25 пришло из спецификаций протоколов этой технологии, утвержденных в 1976 году организацией CCITT (Comite Consultatif Internationale de Telegraphique et Telephonique).

Замечание

В 1993 году название организации CCITT было изменено на ITU (International Telecommunications Union).

Технология PSDN работает на первых трех уровнях модели OSI. Протокол X.25 фактически состоит из нескольких протоколов.

- На физическом уровне PSDN используется протокол X.21. (В США используется X.21bis — вариация протокола физического уровня X.21.)
- На канальном уровне используется протокол LAPB (Link Access Procedure Balanced).
- На сетевом уровне для сборки кадров канального уровня в пакеты используется протокол PLP (Packet Layer Protocol).

При разработке протокола X.25 главной целью было обеспечение надежности. В 1970-х годах, когда он разрабатывался, тогдашние компьютеры и телефонные линии были подвержены частым сбоям. Поэтому система PSDN на основе протокола X.25 была создана избыточной с целью обнаружения ошибок. В результате было создано надежное средство передачи данных, однако его производительность была существенно понижена из-за дополнительных процедур обнаружения ошибок. Пропускная способность PSDN обычно составляет 64 Кбит/с или ниже.

В настоящее время системы PSDN продолжают использоваться. Установить соединение глобальной сети посредством PSDN можно одним из трех способов.

- Приобрести и установить асинхронный модем и набрать номер PAD (Packet Assembler/Disassembler).
- Установить синхронное соединение с помощью протокола X.32.
- Установить соединение непосредственно с PSDN с помощью "интеллектуальной" карты X.25.

Frame Relay

Это более новая технология коммутации пакетов, чем X 25. Она была разработана на основе технологии X.25 для использования с цифровыми линиями. Таким образом, технология Frame Relay представляет собой усовершенствованный вариант технологии X 25, разработанный организацией CCITT. В ней используются только два первых уровня OSI, а не три, как в X 25. Целью разработки Frame Relay была реализация преимуществ современных компьютеров и телефонных линий, гораздо более совершенных и надежных, чем во времена разработки X.25. Глобальные соединения Relay Frame становятся все более популярными вследствие более высокой производительности и меньшей стоимости по сравнению с X.25.

В технологии Frame Relay используются только два нижних уровня модели OSI — физический и канальный. В этой технологии по каналам передается намного меньше протокольной информации, чем в X.25, поэтому она намного производительнее. Пропускная способность сетей Frame Relay находится в пределах от 1,5 до 45 Мбит/с, т е на уровне линий T-1 и T-3. Frame Relay называют технологией *быстрых пакетов*.

В большинстве реализаций Frame Relay для обеспечения постоянного соединения используется *PVC (Permanent Virtual Circuit)*. Благодаря PVC заказчики могут избежать затрат на аренду выделенной линии, поскольку провайдеры услуг обычно взимают плату за фактическое использование линии (за так называемую *пропускную способность по требованию*).

Высокая производительность Frame Relay в значительной степени обусловлена тем, что в ней не выполняются дополнительные процедуры обнаружения и коррекции ошибок, как в X.25. Кадры с ошибками попросту отбрасываются, программы приложений сами должны обнаруживать пропущенные пакеты и посылать запросы на их повторную передачу. Поскольку передаются цифровые сигналы, количество ошибок невелико и технология Frame Relay работает в соединениях глобальных сетей по линиям T-1 вполне удовлетворительно.

ATM

ATM (Asynchronous Transfer Mode) — популярная технология с коммутацией пакетов — была разработана для поддержки приложений, требующих высокой пропускной способности, таких как аудио- и видеоданные в реальном времени. Важным элементом сетей ATM является QoS (Quality of Service). QoS означает способ управления выделением каналов с необходимой полосой пропускания для гарантирования нормальной работы приложений, требующих высокой скорости передачи данных.

Все сетевое оборудование должно быть предназначено для работы с ATM. Преимуществом такого подхода является высокая скорость обработки данных и коммутации. Стандартная скорость передачи ATM может быть следующей: 25, 155,520 или

622,080 Мбит/с. Скорость передачи ATM может составлять 10 Гбит/с, однако по значительно более высокой цене. Установка соединений ATM обходится дорого, потому что все сетевое оборудование должно поддерживать ATM, а стоимость сетевых адаптеров, концентраторов и другого оборудования, совместимого с ATM, довольно высока.

В системе ATM данные разбиваются на части с фиксированной длиной по 53 байта, которые называются *ячейками*. Для заголовка ATM, содержащего адресную информацию, используется 5 байт.

Соединения ATM применяются как в локальных, так и в глобальных сетях. Для одновременной передачи по сети голоса, данных и видео используется мультиплексирование сигналов. Коммутацию ячеек выполняет оборудование ATM (в отличие от Frame Relay, где это делает программное обеспечение).

Соединение пользователя с сетью ATM может быть прямым или по требованию. Соединение между двумя сетевыми компьютерами называется *виртуальным каналом*. Существует два типа виртуальных каналов: PVC (Permanent Virtual Circuit) и SVC (Switched Virtual Circuit). Как для PVC, так и для SVC в системе ATM используются предопределенные каналы (в отличие от Frame Relay или X.25, где виртуальные каналы устанавливаются только на время соединения). Это экономит много времени и служит одним из факторов высокого быстродействия ATM.

Многие специалисты по компьютерным сетям предсказывают, что в будущем ATM станет одной из лучших технологий как локальных, так и глобальных сетей.

Разрабатываемые технологии глобальных сетей

Новые, более быстрые и более эффективные технологии глобальных сетей разрабатываются постоянно. Многие из них создаются с учетом взаимодействия друг с другом в целях поддержки приложений, требующих высокой пропускной способности.

Далее рассматриваются новые высокоскоростные технологии OC-SONET, быстрая ISDN, CATV и SMDS.

OS-SONET

Буквы OS означают *optical carrier* (оптический носитель), а SONET — *Synchronous Optical Network* (синхронная оптическая сеть). Протокол SONET используется на физическом уровне для высокоскоростной передачи данных по волоконно-оптическим носителям. Пропускная способность SONET достигает 20 Гбит/с. Протокол SONET может использоваться в ATM для достижения высокой пропускной способности.

Замечание

За пределами США технология SONET иногда называется SDH (Synchronous Digital Hierarchy).

Скорость передачи сигналов SONET определяется стандартами OC. В табл. 6.3 приведены наиболее распространенные стандартные скорости передачи (иногда они называются уровнями оптических носителей).

Таблица 6.3. Скорости передачи сигналов оптическими носителями

Уровень оптического носителя	Скорость передачи
OC-1 (базовая скорость)	51,84 Мбит/с
OC-3	155,52 Мбит/с
OC-12	622,08 Мбит/с
OC-48	2,488 Гбит/с

Технология SONET используется как физическая основа быстрой ISDN, рассматриваемой в следующей главе.

Быстрая ISDN

В технологии быстрой ISDN (Broadband ISDN — BISDN) для передачи данных по волоконно-оптическим кабелям и радиолиниям используются методы SONET, FDDI (Fiber Distributed Data Interface) и Frame Relay.

Высокоскоростные технологии, позволяющие передавать одновременно данные, видео и голос по многим каналам одного и того же носителя, получают все большее распространение в качестве соединений Internet и других скоростных глобальных сетей. Другие высокоскоростные технологии — DSL и кабельные модемы.

CATV

У компаний кабельного телевидения CATV (Community Antenna TeleVision) неожиданно появились впечатляющие перспективы. К настоящему времени в больших городах и даже сельских районах уже создана огромная инфраструктура коаксиальных кабелей, которые можно использовать для передачи не только телевизионных сигналов, но и компьютерных данных. Доступ к Internet посредством кабелей CATV предлагают все больше провайдеров.

Система CATV не разрабатывалась как технология глобальной компьютерной коммуникации. Первоначально CATV предназначалась только для передачи информации (телевизионных программ) от телевизионных компаний к зрителю. И хотя все пользователи соединены одной и той же сетью коаксиальных кабелей, опутавших окрестности, сеть не предназначалась для коммуникации пользователей друг с другом. Фактически кабельная сеть даже не предназначалась для передачи данных от пользователей, они могли только принимать информацию. Однако появление кабельных модемов радикально изменило ситуацию.

Для доступа к Internet по кабелю нужен кабельный модем, соединяющий входящий коаксиальный кабель и сетевой адаптер персонального компьютера. Чаще всего для этого используется сетевая карта Ethernet 10BaseT.

Фактически кабельная компания одновременно является провайдером — поставщиком услуг Internet. В такой схеме не имеет смысла отделять предоставление носителя от услуг доступа в Internet, подобно тому как это произошло с провайдерами услуг Internet по телефонным линиям.

Кроме того, когда пользователь оплачивает услуги телефонной компании (как линии PSTN, так и выделенной линии T-1), он может одновременно оплатить учетную запись Internet, зарегистрированную у любого провайдера, в том числе и телефонной компании, которой принадлежит линия. Технически это возможно и для телевизион-

ных кабелей, однако телевизионные компании предоставляют эти две услуги в пакете. Контракт с телевизионной компанией обычно предусматривает, что она одновременно является провайдером Internet.

Кабельная инфраструктура может поддерживать одностороннюю или двустороннюю передачу. Односторонняя передача означает, что сигналы передаются по коаксиальному кабелю только в одном направлении — от телевизионной компании к пользователю. При этом передача данных в обратном направлении должна выполняться по обычной аналоговой телефонной линии, которая, впрочем, тоже подключается к кабельному модему. Если используется односторонняя передача по телевизионному кабелю, то скорость передачи данных от пользователя ограничена пропускной способностью линии PSTN, которая составляет до 56 Кбит/с. В то же время скорость передачи к пользователю составляет от 364 Кбит/с до 1,5 Мбит/с.

Если установлен двусторонний кабель, то в обоих направлениях скорость передачи высокая. Однако многие кабельные компании ограничивают скорость передачи от пользователя величиной 128 Кбит/с, чтобы пользователи не устанавливали у себя Web-серверы. Довольно часто установка Web-сервера запрещается условиями контракта с компанией CATV.

Кабельная технология предполагает постоянное соединение, однако если установлен односторонний кабель, то соединение в направлении от пользователя все же остается наборным. Большим преимуществом соединений CATV является низкая цена. К недостаткам можно отнести то, что во многих регионах пользователи сталкиваются с проблемой надежности соединения. В кабельной технологии используется "разделение пропускной способности" между пользователями (т.е. полная пропускная способность кабеля в текущий момент времени делится между всеми пользователями данного сегмента кабеля), поэтому по мере подключения соседей скорость передачи для каждого пользователя снижается. Существуют также проблемы с безопасностью данных. Поэтому системы CATV больше подходят не для коммерческих организаций, а для жилых кварталов.

SMDS

SMDS (Switched Multimegabit Data Service — служба коммутации мегабитовых данных) представляет собой новую технологию с коммутацией пакетов, разработанную специально для глобальных сетей со "взрывообразным" характером загрузки. *Взрывообразность* означает, что при передаче данных периоды слабой загруженности сети чередуются с "пиковыми" периодами, когда сеть с трудом справляется с потоком данных.

В технологии SMDS соединение не устанавливается, т.е. перед началом передачи данных между двумя компьютерами устанавливать между ними соединение нет необходимости. В этой технологии используются относительно большие пакеты, вплоть до 7 168 байт. Адреса SMDS (десятизначные числа, как и телефонные номера) используются для идентификации подсети SMDS. Каналы SMDS (обычно это каналы OC-3 SONET) подключаются к коммутаторам магистральной сети телефонной компании.

SMDS разрабатывалась как технология общедоступной сети, предоставляющей услуги, аналогичные услугам локальных сетей. Отличие заключается лишь в том, что SMDS может охватывать большие города. Скорость передачи находится в пределах от 1,544 до 45 Мбит/с. Сеть SMDS легко расширяется. Ее можно использовать совместно с ATM. Однако SMDS пока что распространена значительно меньше, чем Frame Relay или другие технологии, поэтому оборудование SMDS трудно достать.

Беспроводные глобальные сети

Во многих случаях установить постоянное соединение по кабелям между узлами глобальной сети невозможно или, по крайней мере, неудобно и дорого Беспроводная связь особенно подходит для случаев, когда необходима коммуникация в реальном времени или когда пользователь передвигается Беспроводные технологии предназначены главным образом для передачи небольших объемов данных

Ниже перечислены беспроводные технологии, используемые в глобальных сетях

- **Радиочастотные технологии**. Система SMR (Specialized Mobile Radio — специализированная мобильная радиосвязь) обеспечивает пропускную способность от 1 200 бит/с до 19,2 Кбит/с Ее расширенная версия ESMR (Enhanced SMR) является цифровой системой
- **Спутниковые технологии** Пропускная способность лежит в пределах от 4 800 до 9 600 бит/с Используется как коммутация каналов, так и коммутация пакетов
- **Микроволновые технологии** В этой технологии для обеспечения высокой пропускной способности используется техника сотовой связи на микроволновых частотах
- **Сотовые технологии** Используются соединения с коммутацией каналов на основе аналоговых или цифровых сотовых линий
- **Технологии пакетов данных** В этих технологиях соединения образуются на основе коммутации пакетов без установки вызовов.

По сравнению с проводными технологиями беспроводная коммуникация часто более дорогая и медленная Например, типичная аналоговая сотовая система связи обеспечивает скорость передачи не более 14,4 Кбит/с, а цифровая сотовая — до 64 Кбит/с

Соединения между локальными и глобальными сетями

В современном мире, опутанном проводами, локальной связи часто бывает недостаточно Ни одна локальная сеть не является изолированным островом, по крайней мере их становится все меньше и меньше Для коммерческих организаций жизненно важно иметь устойчивую связь с внешним миром Это означает, что локальные сети должны объединяться в корпоративную глобальную сеть, или подключаться к Internet, или и то и другое

Подключить локальную сеть к внешнему миру можно несколькими способами, зависящими от бюджета и потребностей организации Наиболее очевидный метод предоставления пользователям доступа к другим сетям — оборудовать каждый персональный компьютер модемом и подключить его к телефонной линии Тогда каждый пользователь сможет при необходимости устанавливать коммутируемое соединение с провайдером или с удаленным сервером. Однако такому методу присущи некоторые недостатки

- При увеличении количества пользователей расходы растут слишком быстро Для каждого компьютера придется покупать отдельный модем и платить за каждую телефонную линию Кроме того, если пользователи подключаются к Internet, то придется платить за учетные записи провайдера отдельно для каждого пользователя

- Если разрешить пользователям устанавливать соединение посредством набора телефонного номера, то могут возникнуть серьезные проблемы с безопасностью конфиденциальных данных. У компании не будет почти никаких средств контроля за тем, к каким сетям подключаются ее служащие и куда передаются данные компании.
- Такой метод требует относительно высокой квалификации пользователей. Компании придется понести расходы на обучение своих служащих тому, как конфигурировать коммутируемое соединение и как с ним работать.

Однако есть лучшие способы выхода во внешний мир. Преимуществами по сравнению со старомодным методом обладают сразу несколько альтернативных методов подключения к глобальным сетям. Их достоинства и недостатки определяются конкретной ситуацией и характером решаемых компанией задач.

Далее рассматриваются такие способы соединения локальных и глобальных сетей:

- транслируемые соединения;
- прокси-серверы;
- маршрутизированные соединения.

Транслируемые соединения

Трансляция адресов — один из наиболее дешевых методов подключения всех компьютеров небольшой локальной сети к Internet или к другой глобальной сети. В этом методе доступ к глобальной сети обеспечивается посредством одного главного компьютера, при этом используется только одна телефонная линия, одна учетная запись провайдера (или другое соединение глобальной сети) и один зарегистрированный публичный IP-адрес.

Как транслируются адреса

Компьютер, выполняющий программу трансляции адресов, находится между общедоступной глобальной сетью и частной локальной сетью. На нем установлены интерфейсы к обеим сетям. Этому компьютеру присвоены: частный IP-адрес, используемый для коммуникации с другими компьютерами локальной сети, и публичный IP-адрес, который может быть присвоен сервером провайдера с помощью службы DHCP (Dynamic Host Configuration Protocol) во время установки соединения с глобальной сетью. Будем называть этот компьютер *хостом трансляции адресов.*

Замечание

Служебная программа DHCP автоматически присваивает компьютерам, конфигурированным на ее использование, IP-адреса и другие параметры TCP/IP. Подробнее DHCP рассматривается в главе 8, "Сетевые протоколы и службы".

Трансляция адресов выполняется путем отображения IP-адресов каждого компьютера локальной сети, передающего данные "наружу", на номера портов хоста трансляции адресов. Эта информация добавляется в IP-заголовок пакета. Затем пакет передается в глобальную сеть. При этом адресом источника служит IP-адрес хоста (компьютера, имеющего физическое соединение с глобальной сетью).

Когда на компьютере локальной сети пользователь запускает броузер и передает, например, запрос на просмотр Web-страницы, хост присваивает запросу номер порта, с помощью которого можно будет идентифицировать передающий компьютер (не хост!). Затем хост передает запрос на Web-сервер провайдера. Когда на хост (чей IP-адрес содержится в заголовке как адрес источника запроса) возвращается запрошенная страница, хост находит в таблице трансляции адресов компьютер, пославший запрос, и передает Web-страницу на этот компьютер.

Таблица трансляции адресов содержит следующую информацию.

- IP-адреса первоначального источника и адресата, служащие для идентификации передающего компьютера внутри сети и принимающего компьютера вне сети.
- Номера портов источника и адресата, служащие для идентификации передающего или принимающего приложения. Например, запросы HTTP на Web-страницы обычно передаются через порт TCP номер 80.
- Последовательность номеров пакетов, с помощью которых из пакетов собирается запрос или ответ.
- Метка времени — число, однозначно идентифицирующее момент передачи с точностью до миллисекунды.

Понятие NAT (Network Address Translation — трансляция сетевых адресов) означает стандартизированную процедуру, определяемую спецификациями RFC 1631. Однако этому стандарту удовлетворяют не все методы трансляции адресов. На рис. 6.7 проиллюстрированы этапы процесса трансляции адресов.

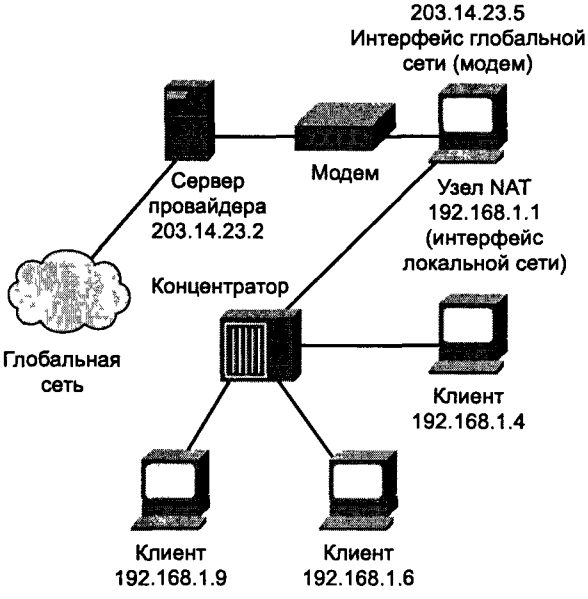


Рис. 6 7. Процесс NAT представляет собой трансляцию частных адресов в публичные

Процесс NAT состоит из ряда этапов.

1. Пользователь, сидя за клиентским компьютером с IP-адресом 192.168.1.9, открывает броузер и вводит в адресном поле следующий URL: `www.tacteam.net`. Броузер передает HTTP-запрос по IP-адресу, ассоциированному с именем, "дружественным" по отношению к `www.tacteam.net`.
2. Хост NAT клиентской локальной сети отображает запрос от 192.168.1.9 к `www.tacteam.net` на номер порта в таблице трансляции адресов. Таблица содержит IP-адреса первоначального источника и адресата, а также их номера портов TCP или UDP.
3. Хост NAT изменяет заголовок таким образом, что для внешней сети пакет кажется пришедшим не от 192.168.1.9, а от публичного IP-адреса, присвоенного провайдером внешнему сетевому адаптеру хоста.
4. Хост NAT передает запрос к `www.tacteam.net` на сервер провайдера. Служба DNS (Domain Name Service) отображает имя запрашиваемого Web-сервера на IP-адрес сервера, в котором хранится основная страница `www.tacteam.net`.
5. Сервер `www.tacteam.net` принимает запрос, обрабатывает его и возвращает требуемую страницу по IP-адресу хоста NAT.
6. Хост NAT, обратившись к таблице трансляции адресов, определяет адрес клиента, пославшего запрос (192.168.1.9), и номер порта TCP или UDP, куда нужно направить ответ.

Программное обеспечение NAT

Некоторые операционные системы (например, Windows 98/2000 и текущая версия Linux) содержат встроенные средства трансляции адресов. В Linux они называются *IP-маскированием*, в Windows 98 и 2000 Professional — *ICS* (*Internet Connection Sharing*). Программа ICS используется также для разделения соединений частной удаленной сети или виртуальной частной сети (Virtual Private Network — VPN). В Windows 2000 Server поддерживается более гибкая и устойчивая версия трансляции адресов — NAT. Если в операционную систему не включена поддержка трансляции адресов, то можно использовать программу NAT сторонних разработчиков, например:

- **Sygate** компании Sybergen Software (`www.sygate.com`);
- **NAT32** компании A.C.T.Software (`www.nat32.com`).

Другой, более сложный (и более трудный в конфигурировании) тип программ, позволяющих разделять сетевые соединения — прокси-серверы.

Прокси-серверы

Прокси-серверы служат не просто посредником между локальной сетью и внешним миром, они обеспечивают защиту данных путем фильтрации входящих и выходящих пакетов. Они же выполняют *кэширование* часто запрашиваемых Web-страниц.

В прокси-серверах используется метод трансляции адресов, который, однако, не обязательно отвечает спецификациям RFC 1631, определяющим NAT.

Принцип действия прокси-сереверов

Как и хост трансляции адресов, прокси-сервер принимает запросы на ресурсы Internet от прокси-клиентов. Получив запрос, прокси-сервер сверяет его с параметрами

фильтрации, предварительно сконфигурированными администратором. Если запрос удовлетворяет требованиям фильтра, сервер ищет в своем кэше хранимые страницы Если требуемая страница есть, прокси-сервер возвращает ее клиенту. В этом случае нет необходимости передавать запрос на сервер провайдера Если в кэше нет нужной страницы, прокси-сервер запрашивает ее у сервера провайдера, принимает ее и возвращает клиенту.

Как и в случае NAT, внутренние клиенты, получающие доступ к Internet посредством прокси-сервера, невидимы из Internet. Вся коммуникация с внешним миром выполняется через прокси-сервер.

Программное обеспечение прокси-серверов

Обычно программы прокси обеспечивают более высокую производительность и безопасность данных, чем NAT. Однако их использование обходится несколько дороже. Их также труднее установить, потому что на всех клиентских компьютерах приложения Internet (такие, как Web-броузеры) должны быть индивидуально сконфигурированы на взаимодействие с прокси-сервером. Практически вся необходимая информация автоматически передается клиентам сервером DHCP.

Во всех популярных операционных системах общедоступны многочисленные программы прокси-серверов; некоторые из них перечислены ниже.

- **Rideway** компании DGL (`dgl.com/rideway`).
- **Winproxy** компании Ositis (`www.winproxy.com/toc`)
- **Microsoft Proxy Server** компании Microsoft (`www.microsoft.com`)
- **Squid для UNIX** компании SCO (`www.sco.com`).

Некоторые программы прокси выполняются только в определенных сетевых операционных системах, например Microsoft Proxy Server — только в Windows NT и Windows 2000 Server. В то же время Rideway может выполняться почти во всех настольных операционных системах — Windows 95/98, Windows NT Workstation и Windows 2000 Professional.

Программы серверов, объединяющие свойства NAT и прокси, иногда называют *прозрачными прокси.*

Маршрутизированные соединения

Еще один способ предоставления компьютерам локальной сети доступа в глобальную сеть — *маршрутизированные соединения.* В отличие от соединений NAT и прокси, в которых индивидуальные компьютеры нуждаются в компьютере-посреднике, маршрутизированные соединения позволяют каждому компьютеру подключаться к Internet непосредственно.

Для конфигурирования маршрутизированных соединений нужно хорошо знать принципы адресации TCP/IP. Необходимо купить и конфигурировать *маршрутизатор* Кроме того, каждый компьютер локальной сети, соединяемый с внешней сетью, должен иметь действительный публичный IP-адрес.

Замечание

В главе 8, "Сетевые протоколы и службы", приведена более подробная информация об адресации TCP/IP Маршрутизация рассматривается в главе 9, "Самая глобальная сеть — Internet"

Зачем нужны маршрутизированные соединения

Большим преимуществом NAT и прокси является возможность подключения небольшой локальной сети к публичной глобальной сети с использованием только одного действительного IP-адреса. Однако во многих случаях это не лучшее решение.

Использование трансляции адресов приводит к тому, что протоколы, не хранящие адресную информацию в IP-заголовках, в системах NAT не работают. Иногда эту проблему можно обойти, добавив *редактор NAT*, модифицирующий пакеты IP. Однако во многих случаях (например, когда пакеты аутентифицируются и шифруются с помощью системы IP Security) трансляция адресов невозможна.

Конфигурирование маршрутизированного соединения

Для маршрутизированного соединения нужен или отдельный маршрутизатор, или программное обеспечение передачи данных по IP-адресам (в этом случае компьютер работает как маршрутизатор).

В компьютерах, использующих для коммуникации протоколы TCP/IP, нужно сконфигурировать следующие параметры:

- IP-адрес компьютера в сети, к которой он подключается;
- маску подсети, определяющую, какая часть IP-адреса идентифицирует компьютер, а какая — сеть.

В компьютерах, участвующих в маршрутизированной сети, должен быть конфигурирован также *шлюз по умолчанию*. Другими словами, должен быть установлен адрес маршрутизатора с двумя сетевыми соединениями: одно с локальной сетью, а другое с внешней.

Замечание

Если вместо IP-адресов используются имена хостов (например, `www.tacteam.net`), то нужно ввести адрес сервера DNS. Служба DNS рассматривается в главе 8, "Сетевые протоколы и службы".

Для установки маршрутизированного соединения с Internet в протоколе TCP/IP маршрутизатора конфигурируются следующие параметры: IP-адрес, маска подсети и адрес сервера DNS, предоставленный провайдером. Кроме того, статический маршрут по умолчанию должен быть сконфигурирован на использование интерфейса Internet.

Точно так же в компьютере локальной сети, подключаемом к Internet, должны быть верно настроены IP-адрес, маска подсети и адрес сервера DNS. Адрес шлюза по умолчанию должен быть установлен как IP-адрес маршрутизатора, служащего интерфейсом локальной сети.

Резюме

В этой главе рассмотрены традиционные и развивающиеся технологии глобальных сетей, используемые для установки соединения компьютеров, удаленных на большое расстояние.

Кроме того, описано оборудование и топологии глобальных сетей, а также преимущества и недостатки таких топологий, как точечная, кольцо, звезда, полная или частичная сетка и многоуровневые глобальные сети.

Далее была показана разница между сетями с коммутацией каналов и коммутацией пакетов, а также характеристики сетевых технологий на основе PSTN, ISDN, xDSL, T-носителей, x.25, Frame Relay, ATM, OC-SONET, BISDN, CATV, SMDS и беспроводных средств связи.

Затем были рассмотрены способы подключения компьютеров локальной сети к глобальной. Значительное внимание было уделено способам предоставления компьютерам локальной сети доступа к Internet и другим внешним сетям. Представлены соединения с трансляцией сетевых адресов, которую иногда называют разделением подключений. Описано, как установить маршрутизированное соединение в случаях, когда трансляция адресов нежелательна или невозможна.

Эта глава заканчивает часть I, "Основные концепции компьютерных сетей" Теперь вы знакомы с базовыми понятиями сетевых технологий. В части II, "Сетевое оборудование и программное обеспечение", рассматривается оборудование и программное обеспечение сетей. В главе 7, "Физические компоненты сетей", рассматриваются физические компоненты сетей

Рекомендуемые источники

Прекрасный источник информации о технологиях и узлах глобальных сетей — `www.networkcomputing.com/wansites/default.html`.

Тщательное, ясное изложение различных технологий глобальных сетей можно найти на Web-узле High Performance Networking Unleashed по адресу: `www.officewizard.com/books/network`.

Подробное обсуждение технологии NAT можно найти по адресу: `www.suse.de/~mha/linux-ip-nat.diplom`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Какие из приведенных параметров должны быть сконфигурированы для внутреннего модема?
   - **а.** Адрес ввода-вывода.
   - **б.** IP-адрес.
   - **в.** IRQ.
   - **г.** Коммуникационный порт.
2. Что такое CSU/DSU или PAD?
   - **а.** Терминальный адаптер ISDN.
   - **б.** Оборудование пользователя.
   - **в.** Терминальный идентификатор
   - **г.** Концентратор-маршрутизатор
3. В каких сетях используются линии PSTN, ISDN, DSL, DDS и T-носители?
   - **а.** В сетях с коммутацией каналов.

б. В сетях с коммутацией пакетов.

в. В сетях Switched 59.

г. В локальных сетях.

4. Какие из приведенных утверждений об ISDN справедливы? (Выбрать все, что подходит.)

а. Это аналоговая связь.

б. ISDN дороже, чем PSTN.

в. Для ISDN требуется специальное оборудование на телефонной станции и у пользователя.

г. Линия ISDN содержит только один канал.

д. По линии ISDN можно передавать как голос, так и данные.

5. Какая топология глобальных сетей обеспечивает наиболее легкую расширяемость?

а. Точечная.

б. Кольцо.

в. Звезда.

г. Все перечисленные одинаково расширяемы.

6. Как называлась самая первая технология с коммутацией пакетов на основе протокола ARPAnet 1822?

а. Frame Relay.

б. X.25.

в. ATM.

г. DSL.

7. Какие из приведенных характеристик Frame Relay отличаются от характеристик X.25? (Выбрать все, что подходит.)

а. Frame Relay обеспечивает высокую производительность.

б. В Frame Relay используется коммутация пакетов.

в. В Frame Relay используются цифровые сигналы.

г. В Frame Relay нет постоянной проверки ошибок.

8. Что из приведенного справедливо для ATM? (Выбрать все, что подходит.)

а. Используются пакеты переменной длины.

б. Используются порции данных длиной 53 байта, которые называются ячейками.

в. Видео, голос и данные можно передавать одновременно.

г. Используются предопределенные каналы.

д. Это самая дешевая технология глобальных сетей.

9. Какая из приведенных технологий обеспечивает передачу данных со скоростью до 2,488 Гбит/с?

а. ADSL.

б. T-1.

в. ISDN BRI.

г. OC-SONET

10. Какое из приведенных утверждений о NAT справедливо? (Выбрать все, что подходит)

а. Каждый компьютер внутренней сети, использующий NAT, должен иметь зарегистрированный IP-адрес

б. NAT совместима со всеми приложениями

в. NAT не совместима с технологиями, шифрующими данные IP

г. Для отображения частных внутренних IP-адресов на один или несколько публичных внешних адресов в NAT используется специальная таблица

Часть II

Сетевое оборудование и программное обеспечение

В этой части...

7. Физические компоненты сетей
8. Сетевые протоколы и службы
9. Самая глобальная сеть — Internet
10. Сетевые операционные системы
11. Службы каталогов
12. Клиентские операционные системы
13. Гибридные сети

Глава 7

Физические компоненты сетей

Теперь, когда вы знакомы с основными понятиями компьютерных сетей, можно приступить к изучению физических компонентов, используемых для соединения персональных компьютеров таким образом, чтобы они могли разделять свои ресурсы.

В некоторых случаях для соединения компьютеров требуются всего лишь несколько недорогих карт сетевого интерфейса (которые чаще всего сокращенно называются сетевыми адаптерами) и кабель Ethernet. С другой стороны, разработка сети может оказаться настолько сложной, что потребует усилий немалой команды специалистов в области компьютерных сетей с бюджетом, выраженным шестизначным числом.

В этой главе рассматриваются некоторые наиболее распространенные сетевые устройства и носители, включая сетевые адаптеры, кабели, беспроводные носители и соединительные устройства.

Сетевые адаптеры

Сетевой адаптер — базовое сетевое устройство, необходимое для подключения компьютера к сети. Существует несколько разновидностей сетевых адаптеров. Они рассматриваются далее в главе.

Сетевой адаптер называют устройством физического уровня, однако драйверы сетевых адаптеров (программы, служащие интерфейсом между сетевыми адаптерами и операционными системами компьютеров) работают на канальном уровне модели OSI.

В следующих разделах рассматривается назначение сетевых адаптеров, выбор оптимального сетевого адаптера и конфигурирование сетевых адаптеров для передачи и приема данных.

Назначение сетевых адаптеров

Для коммуникации посредством сети всегда нужен какой-либо интерфейс между сетью и компьютером. Если компьютер подключен к удаленной сети с помощью телефонной линии, то роль интерфейса играет модем, выполняющий функции сетевого адаптера при подключении к локальной сети.

Как упоминалось, сетевой адаптер — это базовое сетевое устройство. Оно преобразует *параллельные* сигналы компьютера в *последовательные*, передаваемые в сетевой кабель. Нули и единицы данных, сгенерированные компьютером, превращаются сете-

вым адаптером в электрические или световые импульсы, радиоволны, а также в любой другой сигнал, поступающий на сетевой носитель.

Важной частью сетевого интерфейса является *трансивер (transmitter/receiver — приемник/передатчик сигналов)*. В некоторых сетях (например, в 10Base2 или 10BaseT) трансивер встроен непосредственно в сетевой адаптер. В других типах сетей используется внешний трансивер. Например, в 10Base5 трансивер подключается к кабелю с помощью разъема AUI (Attachment Unit Interface).

Таким образом, сетевой адаптер отвечает за подготовку данных к передаче их на сетевой носитель, за прием поступающих данных и за управление потоком данных между компьютером и носителем.

Выбор сетевого адаптера

При выборе сетевого адаптера необходимо учесть ряд факторов.

- **Архитектура сети**. Сетевой адаптер должен быть специально разработан для данной архитектуры. Однако в некоторых случаях с помощью *фильтра носителя* можно использовать адаптер, разработанный для другой архитектуры. Например, сетевой адаптер Token Ring в сети Ethernet. Распространенные архитектуры локальных сетей рассматриваются в главе 5, "Локальные сети".
- **Тип носителя**. В Ethernet может использоваться толстый коаксиальный кабель (10Base5), тонкий коаксиальный кабель (10Base2) или витая пара (10BaseT). Разъем сетевого адаптера должен быть совместим с разъемом на кабеле. Это же относится и к волоконно-оптическим и беспроводным сетевым адаптерам. Кабели и беспроводные носители рассматриваются далее в главе.
- **Скорость передачи данных**. Если концентратор Ethernet рассчитан на 100 Мбит/с, то сетевой адаптер на 10 Мбит/с работать не будет. Однако на рынке существуют компоненты с двойной пропускной способностью (концентраторы и сетевые адаптеры), работающие со скоростью как 10, так и 100 Мбит/с. Аналогично этому, сетевые адаптеры Token Ring на 4 Мбит/с не будут работать в сети с пропускной способностью 16 Мбит/с. Тем не менее сетевой адаптер Token Ring на 16 Мбит/с *работает* в сети с пропускной способностью 4 Мбит/с, хотя и с меньшей скоростью.
- **Тип шины компьютера**. Есть ли в компьютере свободный разъем ISA или PCI? Нужен ли специальный переходник для подключения к компьютеру через последовательный порт или через порт SCSI? Если используется портативный компьютер, то необходим интерфейс PCMCIA.

Типы шин персонального компьютера

Шина компьютера — это путь передачи сигналов на системной плате. Физически шина представляет собой 16 или 32 металлические дорожки на плате, к которым подключены процессор, память, дисководы и другие устройства компьютера. Каждое устройство подает сигналы на шину или принимает сигналы от нее. Существует несколько различных типов шин, на которые рассчитаны сетевые адаптеры.

- ISA (Industry Standard Architecture). Предоставляет для сетевого адаптера 16-разрядное гнездо. Пластмасса гнезда обычно черного цвета, а само гнездо (фактически два гнезда — одно позади другого) длиннее, чем гнездо PCI.

- EISA (Extended ISA). Трехразрядная архитектура, совместимая с ISA. Большинство современных гнезд, называемых ISA, фактически являются гнездами EISA
- PCI (Peripheral Component Interconnect). Используемая в современных компьютерах (класса Pentium и выше, а также Macintosh) 32-разрядная шина Архитектура PCI поддерживает устройства PnP (Plug and Play). Гнездо на плате, более короткое, чем в ISA/EISA, обычно из бежевой или светлой пластмассы
- MCA (Micro Channel Architecture). Шина, используемая в компьютерах IBM Может быть как 16-, так и 32-разрядной. В настоящее время почти не используется
- PCMCIA (Personal Computer Memory Card International Association, другое название — PC Card) Шина ввода-вывода для устройств с размерами и формой кредитной карточки. Обычно используется в портативных компьютерах Выпускаются также адаптеры PC Card для настольных компьютеров.

Существуют также сетевые адаптеры, подключаемые посредством шины SCSI Есть несколько типов сетевых адаптеров для шины USB (Universal Serial Bus — универсальная последовательная шина), однако они встречаются редко. Системные платы некоторых компьютеров содержат *встроенный сетевой адаптер*.

- **Операционная система**. К сетевому адаптеру должен прилагаться драйвер, предназначенный для используемой операционной системы. Если используется одна из операционных систем Windows, то нужно обратиться к списку совместимого оборудования (Hardware Compatibility List — HCL), предоставляемому компанией Microsoft на Web-узле по адресу: `www.microsoft.com`. В списке HCL следует найти сетевые адаптеры, которые были протестированы в данной операционной системе и гарантированно в ней работают. Популярные настольные операционные системы рассматриваются в главе 12, "Клиентские операционные системы".

Конфигурирование и использование сетевых адаптеров

Конфигурирование сетевого адаптера во многом аналогично конфигурированию модема, рассмотренному в главе 6, "Глобальные сети". Сетевые адаптеры и модемы выполняют в сущности одинаковые функции.

При конфигурировании сетевого адаптера необходимо установить следующие параметры:

- IRQ;
- адрес ввода-вывода;
- адрес в памяти.

Эти параметры можно установить с помощью миниатюрных переключателей на плате адаптера, перемычек или программы конфигурации, поставляемой с адаптером. Сетевые адаптеры, поддерживающие PnP, автоматически обнаруживаются и конфигурируются операционной системой, если, конечно, BIOS компьютера тоже поддерживает PnP.

Если используется *комбинированный* сетевой адаптер, т.е. пригодный для разных типов носителей, то может понадобиться конфигурирование дополнительных параметров. Обычно в комбинированном сетевом адаптере есть разъем BNC для тонкого коаксиального кабеля, разъем RJ-45 для витой пары, а иногда и разъем AUI для толстого коаксиального кабеля. Благодаря этому один и тот же адаптер может работать в

сетях 10Base2, 10BaseT и 10Base5. Однако в каждый момент времени используется, естественно, один тип носителя Поэтому тип носителя нужно выбрать вручную. Некоторые адаптеры могут автоматически определять тип подключенного носителя.

На рис. 7.1 показан комбинированный сетевой адаптер, рассчитанный на три типа носителей

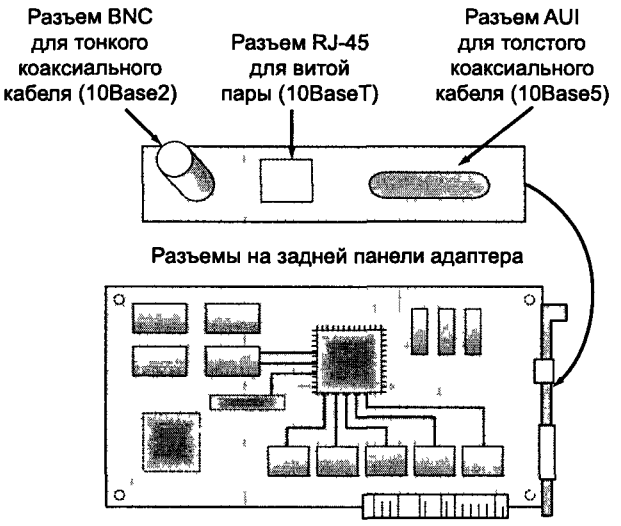


Рис 7 1 Комбинированный сетевой адаптер для сетей 10Base2, 10Base5 и 10BaseT

Конфигурирование IRQ

Обычно для сетевых адаптеров выделяется IRQ 3 или IRQ 5. Во многих сетевых адаптерах один из этих IRQ предполагается по умолчанию. Если предопределенная линия IRQ уже занята другим устройством компьютера, то во избежание конфликтов нужно изменить конфигурацию одного из этих устройств

В табл. 7 1 перечислены стандартные установки IRQ для различных устройств типичного персонального компьютера. Обратите внимание· в ранних версиях персональных компьютеров доступными были только восемь первых IRQ Поэтому IRQ 2 используется как контроллер IRQ, т е. для передачи запроса на прерывание на IRQ 9, через который реализуется доступ к IRQ с номерами, большими чем 9

Таблица 7.1. Стандартные установки IRQ по умолчанию

Устройство	IRQ по умолчанию
Графический адаптер VGA	2 (9)
COM 2 и COM 4 (вторичный последовательный порт)	3*
COM 1и COM 3 (первичный последовательный порт)	4
Вторичный параллельный порт LPT2 или звуковой адаптер	5*
Контроллер дисковода	6
Первичный параллельный порт LPT1	7
Часы	8

Окончание табл 7 1

Устройство	IRQ по умолчанию
Первичный контроллер SCSI	10*
Вторичный контроллер SCSI	11*
Мышь PS/2	12
Математический сопроцессор	13
Первичный контроллер IDE	14
Вторичный контроллер IDE	15*

** Эти устройства необязательны и могут не входить в состав компьютера. Если их нет, соответствующие IRQ свободны Например, если в компьютере нет контроллеров SCSI, то IRQ 10 и IRQ 11 свободны (если, конечно, не заняты другими устройствами) и могут быть присвоены сетевому адаптеру.*

Конфигурирование порта ввода-вывода и адреса памяти

Кроме уникальных IRQ, каждое устройство должно иметь уникальную установку порта ввода-вывода. *Порт ввода-вывода* — это канал, по которому данные передаются между устройствами и процессором. Номера портов представляют собой шестнадцатеричные числа. Обычно сетевые адаптеры используют следующие порты:

- от 300 до 30F;
- от 310 до 31F.

Можно использовать и другие. Чаще всего нормально работают установки порта ввода-вывода по умолчанию, присвоенные сетевому адаптеру на заводе-изготовителе.

Адрес памяти — это место в оперативной памяти, где хранятся передаваемые и принимаемые данные. Как и в случае с номерами портов, адрес памяти, присвоенный сетевому адаптеру на заводе-изготовителе, практически всегда работает нормально. В некоторых сетевых адаптерах для промежуточного хранения данных оперативная память не используется, поэтому для них не нужно устанавливать адрес памяти.

Сетевые носители

По сетевым носителям сигналы передаются от одного сетевого устройства к другому. Чаще всего носителем служит кабель, однако в настоящее время используются также беспроводные носители: радиоволны, световые и инфракрасные лучи, спутниковые и микроволновые средства связи и т.д.

В этом разделе сначала рассматриваются различные типы кабелей, используемых для соединения сетевых устройств, а затем беспроводные носители.

Типы кабелей

В настоящее время в качестве сетевых носителей чаще всего используются кабели. Наиболее распространенными являются коаксиальные кабели, витые пары (которые тоже причисляются к кабелям) и волоконно-оптические кабели.

Коаксиальные кабели

С коаксиальными кабелями знаком любой человек, у которого есть телевизор. Коаксиальный кабель представляет собой медный сердечник (одножильный или многожильный), окруженный слоем изоляционного материала, металлическим экраном (из фольги или сплетенным) и еще одним слоем изоляции. Сигнал передается по медному сердечнику, а металлический экран заземляется на одном из концов. Название "коаксиальный" образовано из слов *со — вместе* и *axial — осевой*, т.е. оно означает "вокруг одной оси". Металлический экран кабеля защищает передаваемый по сердечнику сигнал от внешних электромагнитных помех. Внешняя оболочка, защищающая всю эту конструкцию от влаги, пыли, механических повреждений и других неблагоприятных воздействий, делается из пластмассы или резины. Внешняя оболочка *пленум-кабеля* делается из тефлона или других негорючих материалов.

Замечание

Пленум — это пространство между полом и фальшь-полом, или между потолком и фальшь-потолком, используемое для прокладки кабелей. Согласно строительным нормам и правилам, прокладка в пленуме кабеля, не являющегося пленум-кабелем, запрещена. Это обусловлено тем, что внешняя оболочка стандартного кабеля сделана из поливинилхлорида, который при высокой температуре выделяет ядовитые газы.

Благодаря металлическому экрану коаксиальный кабель менее чувствителен к внешним электромагнитным помехам, чем витая пара.

Заглянув в каталог любого производителя, можно увидеть тысячи различных типов и марок коаксиальных кабелей. Многие из них используются только в узкоспециальных целях, например для соединения научных приборов или технологического оборудования. В табл. 7.2 приведены характеристики только тех кабелей, которые используются в локальных сетях.

Таблица 7.2. Типы и характеристики коаксиальных кабелей

Тип	Название	Описание	Область применения
RG-8, RG-11	Толстый	Внешний диаметр около 1 см	10Base5
RG-58 A/U	Тонкий	Внешний диаметр около 0,5 см	10Base2
RG-58 C/U	Тонкий (военная спецификация)	Внешний диаметр около 0,5 см	10Base2 (военное применение)
RG-62	ARCnet	Тонкий коаксиальный кабель	Сети ARCnet

В ранних реализациях Ethernet использовались главным образом коаксиальные кабели, однако со временем они все больше вытесняются витыми парами. В Ethernet используются коаксиальные кабели двух базовых типов: тонкие и толстые. Соответственно этим названиям выделяются два типа сетей Ethernet: *тонкие* и *толстые*.

Замечание

Телевизионный коаксиальный кабель выглядит почти так же, как и кабель, используемый в тонких сетях, однако они не взаимозаменяемы. В кабельном телевидении используется 75-омный кабель RG-59.

Тонкий коаксиальный кабель

Диаметр тонкого коаксиального кабеля составляет приблизительно 0,5 сантиметра. Он более гибкий, чем толстый. Используется этот кабель в сетях Ethernet 10Base2. Максимальное расстояние передачи сигнала по тонкому коаксиальному кабелю равно 185 метрам. При большем расстоянии сигнал ослабевает вследствие затухания и соединение становится ненадежным.

Тонкий коаксиальный кабель обозначается как RG-58. Его *импеданс*, т.е. волновое сопротивление протекающему току, равен 50 Ом.

Основные термины электроники

Электрический ток — это поток электронов, или заряженных атомов по проводнику. *Ампер* — единица измерения интенсивности электрического тока. *Сопротивление* — характеристика проводника тока, степень "трудности протекания", или "сопротивления", оказываемого проводником протекающему току. Для высокочастотных токов сопротивление называется *импедансом* (другое название — *волновое сопротивление*) Сопротивление измеряется в *омах*. Единица измерения сопротивления названа так в честь немецкого ученого Георга Симона Ома, открывшего закон, гласящий: "Электрический ток пропорционален напряжению и обратно пропорционален сопротивлению". Этот закон впоследствии был назван именем открывателя. Иногда единица сопротивления Ом обозначается греческой буквой Ω.

Напряжение (другие названия — *электрический потенциал, электродвижущая сила*) — это избыток или недостаток электронов на двух концах проводника, вызывающий протекание электрического тока. Единица измерения напряжения — *вольт*

Циклические (повторяющиеся) аналоговые сигналы характеризуются *частотой* — количеством полных циклов (повторений) сигнала в единицу времени. Единица измерения частоты — *герц (Гц)*. Сигнал имеет частоту 1 Гц, если за секунду происходит один цикл его повторения.

Коаксиальные кабели стандартизированы спецификациями RG (Registered Grade). В компьютерных сетях используется всего несколько из сотен типов коаксиальных кабелей.

В сетях 10Base2 используется тонкий коаксиальный кабель RG-58 A/U, имеющий многожильный медный сердечник. Военный кабель этого же типа обозначается RG-59 C/U. От обычного он отличается немного более толстой внешней оболочкой, делающей кабель более устойчивым к жаре, холоду, влаге и другим неблагоприятным факторам.

Кабель RG-58 /U внешне похож на RG-58 A/U, однако его медный сердечник одножильный. Он не удовлетворяет спецификации 10Base2, поэтому использовать его в компьютерных сетях *нельзя*. Обычно этот кабель используют для подключения антенн и в других целях. На рис. 7.2 показана разница между этими кабелями.

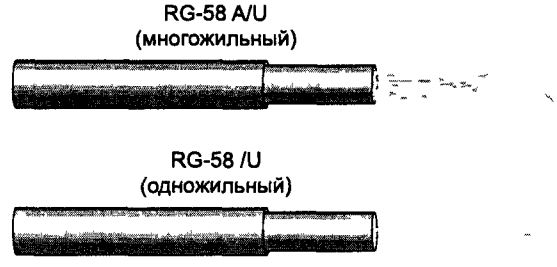


Рис 7 2 Многожильный и одножильный коаксиальные кабели

Тонкий коаксиальный кабель подключается к сетевому адаптеру с помощью Т-разъема типа BNC (рис 7 3)

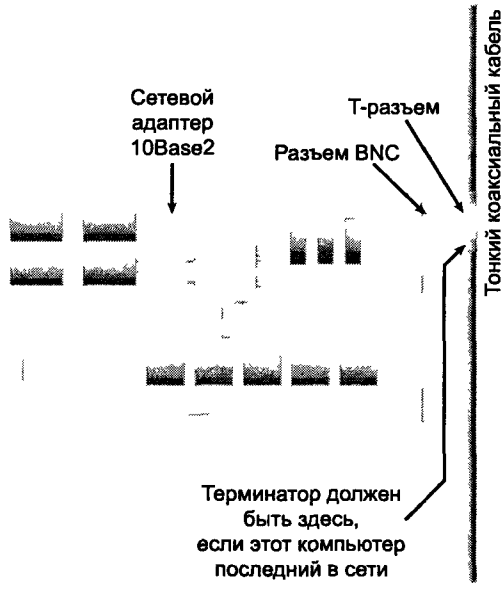


Рис 7 3 Подключение тонкого кабеля к сетевому адаптеру с помощью Т-разъема BNC

На каждом конце шины тонкой сети должен быть установлен терминатор, который подключается к пустой стороне Т-разъема

Толстый коаксиальный кабель

Толстый коаксиальный кабель приблизительно в два раза толще, чем тонкий Его диаметр составляет около 1 см Первоначально в сетях Ethernet использовался именно толстый кабель, поэтому толстая сеть называется *стандартной Ethernet*

В компьютерных сетях используется два типа толстого кабеля RG-8 и RG-11 Благодаря более толстому сердечнику по толстому кабелю можно передавать сигналы на большее расстояние, чем по тонкому, — до 500 метров без затухания сигнала Однако толстый кабель дороже и с ним труднее работать, чем с тонким, из-за его малой гибкости В сетях с толстым кабелем используются внешние трансиверы, которые подключаются к кабелю с помощью специального устройства, называемого *зуб вампира* (рис 7 4) Чтобы подключить к кабелю зуб вампира, в кабеле нужно просверлить отверстие, поэтому устанавливать толстый кабель сложнее, чем тонкий, для которого используются Т-разъемы BNC

Замечание

В прошлом были распространены главным образом сети ARCnet, в которых использовался 90-омный коаксиальный кабель RG-62 В настоящее время архитектура ARCnet становится все менее популярной (см главу 5, "Локальные сети")

Витые пары

Под *кабелем Ethernet* большинство подразумевает витые пары, используемые в настоящее время почти во всех сетях Ethernet Витая пара представляет собой два скрученных изолированных медных провода в защитной оболочке Скручивание проводов уменьшает *перекрестные помехи* чем больше витков приходится на единицу длины, тем меньше влияние перекрестных помех

Телефонные компании прокладывают витые пары чаще всего внутри зданий Этот фактор немало способствует росту популярности витых пар во многих зданиях они уже проложены для телефонной связи

Витые пары бывают двух типов экранированные и неэкранированные (рис 7 5) В системах телефонной связи и в большинстве сетей Ethernet используются неэкранированные витые пары, а в сетях Token Ring и AppleTalk — экранированные

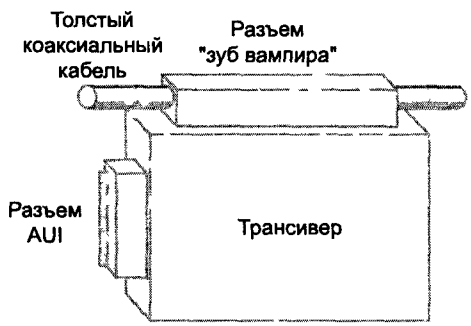


Рис 7 4 В сетях 10Base5 используется внешний трансивер, подключенный к толстому кабелю с помощью зуба вампира

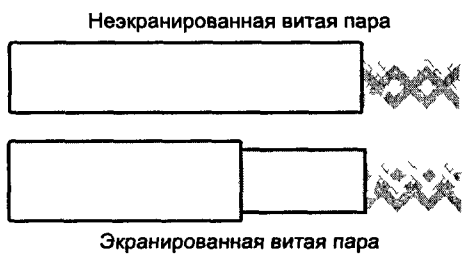


Рис 7 5 Экранированная и неэкранированная витые пары

Внешний металлический экран, окружающий витую пару, уменьшает влияние электромагнитных помех Однако в экранированных витых парах затухание сигналов больше, чем в неэкранированных

Неэкранированные витые пары

Популярность неэкранированных витых пар в локальных сетях обусловлена следующими факторами

- Дешевизна
- Гибкость и легкость установки
- Для подключения неэкранированной витой пары используются хорошо знакомые и распространенные разъемы RJ-45, которые внешне выглядят аналогично меньшим модульным телефонным разъемам RJ-11
- Неэкранированные витые пары используются в топологии звезды, имеющей многочисленные преимущества (см главу 2, "Классификация компьютерных сетей")

В соответствии с областью применения и пропускной способностью витые пары делятся на категории В табл 2 3 главы 2, "Классификация компьютерных сетей", перечислены категории неэкранированных витых пар, для каждой из которых приведены пропускная способность и области применения

Замечание

Неэкранированные витые пары телефонных линий проложены внутри стен и выведены наружу с помощью гнезда RJ-11. Обычный телефонный провод от стены до телефонного аппарата чаще всего представляет собой *нескрученную* медную пару.

Как и коаксиальные кабели, неэкранированные витые пары поставляются в стандартном исполнении и как пленум-кабель.

Экранированные витые пары

Экран, сделанный из плетеных медных жилок или из фольги, окружает два скрученных изолированных медных провода. В свою очередь, экран заключен в защитную изоляционную оболочку. Экран уменьшает влияние внешних электромагнитных помех, однако при этом появляются другие неблагоприятные факторы. В частности, увеличивается стоимость кабеля и становится более интенсивным затухание сигналов.

Чаще всего экранированные витые пары используются в сетях AppleTalk и Token Ring.

Волоконно-оптические кабели

Волоконно-оптические кабели — относительно новый тип сетевых носителей. Их пропускная способность выше, чем у традиционных кабелей, однако стоят они дороже. Популярность волоконно-оптических кабелей неуклонно растет. В настоящее время реализованы волоконно-оптические кабели с пропускной способностью 100 Мбит/с, однако для этого типа носителя она может достигать 1 Гбит/с и выше.

Замечание

В исследовательской лаборатории Lucent Technologies для волоконно-оптического кабеля с помощью нескольких лазеров достигнута пропускная способность 3 Тбит/с. Один терабит равен тысяче гигабит.

Вместо медного провода в волоконно-оптическом кабеле используются стеклянные или пластмассовые нити, по которым передаются сигналы в виде световых импульсов.

Кроме высокой пропускной способности, волоконно-оптические кабели обладают следующими преимуществами:

- безопасность данных выше, чем при использовании коаксиальных кабелей или витых пар, потому что незаметно подключиться к оптической нити почти невозможно;
- волоконно-оптические кабели меньше подвержены затуханию, поэтому по ним можно передавать сигналы на большее расстояние — до 2 км и более;
- волоконно-оптические кабели совершенно нечувствительны к электромагнитным помехам.

По сравнению с традиционными типами кабелей волоконно-оптические кабели дорогие. Значительно дороже сам кабель, а кроме того, приходится нести дополнительные расходы на установку волоконно-оптических кабелей, потому что это могут делать только квалифицированные специалисты.

Режимы передачи оптических сигналов

Волоконно-оптические кабели могут работать в двух режимах передачи сигналов

- **Одномодовый режим** Световые импульсы проходят вдоль оси оптической нити
- **Многомодовый режим** Световые импульсы многократно отражаются от стенок оптической нити

В одномодовом режиме пропускная способность выше (до 10 Гбит/с) В многомодовом луч света состоит из многих лучей, проходящих разными путями, поэтому световой импульс "размазывается" вдоль кабеля В то же время в одномодовом режиме импульс не размазывается и поэтому может быть более коротким, а пропускная способность, соответственно, выше

Источники световых импульсов

Для генерации световых импульсов, передаваемых по оптической нити волоконно-оптического кабеля, используется два типа источников света

- **Светодиоды** Обычно используются в *одномодовом* режиме, т е в каждый момент времени генерируется (или отсутствует) только один импульс Интенсивность импульсов невелика
- **Полупроводниковые лазеры** Генерируют интенсивный, хорошо сфокусированный световой импульс заданного цвета Используются в *многомодовом* режиме, т е когда по одной нити одновременно передается много световых импульсов разного цвета

В современной технике светодиоды широко используются в самых разных устройствах, например в цифровых часах, в приборах индикации, в устройствах телеуправления и т д Светодиод представляет собой полупроводниковый прибор, аналогичный обычному диоду Когда через светодиод проходит электрический ток, он светится Цвет свечения обычно красный, однако в зависимости от материала светодиода и силы тока цвет может изменяться в широком диапазоне, вплоть до фиолетового Существуют светодиоды, генерирующие инфракрасное излучение

Полупроводниковый лазер, как и светодиод, конструктивно представляет собой миниатюрный кристаллик полупроводникового материала Однако, в отличие от светодиода, он испускает более мощный монохроматический луч (луч со строго определенной длиной волны) Полупроводниковые лазеры используются также в портативных лазерных сканерах

Беспроводные носители

Беспроводные средства сетевой коммуникации становятся все более популярными По сравнению с кабелями пропускная способность беспроводных носителеи намного меньше, однако во многих случаях они обладают значительными преимуществами (см главу 6, "Глобальные сети") Базовые понятия беспроводных носителей в глобальных сетях относятся также и к локальным сетям

Следует отметить, что "беспроводная" сеть практически никогда не обходится без кабелей Напротив, беспроводные средства связи, как правило, встроены в традиционные кабельные сети Для обмена сигналами между беспроводными и традиционными сетевыми устройствами используются трансиверы (рис 7 6) Другое название трансиверов — *точки доступа*

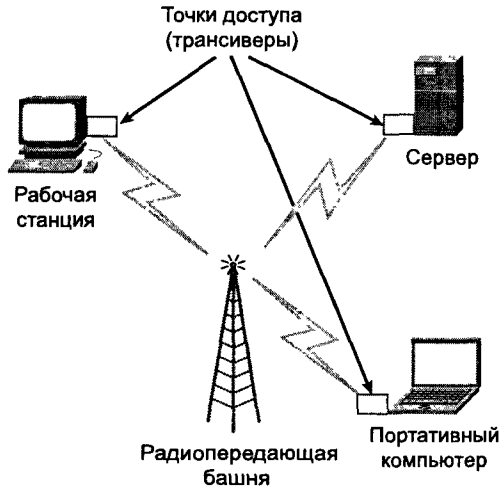


Рис. 7.6. В беспроводной сети для передачи и приема данных без кабелей используются трансиверы

Замечание

Компания Cisco Systems в содружестве с другими компаниями (Motorola, EDS, Samsung и Texas Instruments) является ведущим разработчиком высокоскоростных, надежных и доступных средств беспроводной компьютерной коммуникации.

В беспроводных соединениях локальных сетей используются следующие носители сигналов:

- лазерные лучи;
- инфракрасные лучи;
- радиоволны.

Далее рассматриваются характеристики каждого из них.

Лазеры

Слово *лазер* представляет собой сокращение от light amplification by stimulated emission of radiation — усиление света путем возбуждения эмиссии излучения. Лазер излучает мощный когерентный луч света, все волны которого имеют строго одинаковую частоту и согласованы по фазе. *Фаза* — это положение электромагнитной волны на оси времени. Если две волны одинаковой частоты совпадают, значит, они согласованы по фазе (находятся в фазе). Если одну из них сдвинуть на половину цикла, то их интенсивность в каждый момент времени будет иметь противоположный знак. В этом случае говорят, что волны находятся в противофазе. Компоненты лазерного луча всегда строго согласованы по фазе.

Различные типы лазеров генерируют световые лучи с разной длиной волны, т.е. разного цвета.

Замечание

Многие представляют себе лазерный луч как "красную точку". Однако существуют лазеры, генерирующие лучи самых разных цветов. Например, аргоновый лазер (назван так потому, что его рабочей средой является газ аргон) испускает голубые или зеленые лучи. Криптоновый лазер испускает красные лучи. В некоторых лазерах рабочей средой служит смесь газов. Тогда испускаемый луч состоит из нескольких монохроматических лучей, в результате чего его цвет может быть белым или самых разных оттенков.

Лазеры используются в разнообразнейших устройствах — в школьных лазерных указках, в прицелах, в системах наведения ракет, в принтерах, в электронных играх, в средствах удаленного контроля, в хирургических инструментах, в том числе и в средствах сетевой коммуникации.

В лазерных сетях сигналы данных представлены импульсами света. Большим недостатком лазерных средств коммуникации является необходимость обеспечения *прямой видимости* между передатчиком и приемником. Если между ними находится здание, дерево или облако, то связь, естественно, невозможна.

Инфракрасные лучи

Многим людям инфракрасные средства связи знакомы благодаря устройствам дистанционного управления телевизором. В беспроводных средствах коммуникации на основе инфракрасных лучей сигналы данных передаются лучом или конусом инфракрасного излучения. Длина волны инфракрасного излучения немного превышает длину волны видимого света.

Разработкой стандартов на оборудование и программное обеспечение средств коммуникации на основе инфракрасного излучения занимается организация IrDA (Infrared Data Association — Ассоциация методов передачи данных в инфракрасном диапазоне). Устройства, отвечающие стандартам IrDA, разрабатываются таким образом, что, когда пользователь прерывает инфракрасное соединение, оно автоматически восстанавливается при повторном помещении приемника в область действия передатчика.

В инфракрасных средствах коммуникации трансиверы используются на обоих концах линии. Иногда применяется синхронизация сигналов с помощью специального программного обеспечения. Некоторые операционные системы, например Windows 98 и Windows 2000, содержат встроенные средства поддержки коммуникации в инфракрасном диапазоне. Пропускная способность инфракрасных средств коммуникации изменяется от 4 до 16 Мбит/с.

Как и лазерные, инфракрасные лучи обычно переносят сигналы в пределах прямой видимости. Однако в некоторых реализациях приемники могут принимать рассеянный или отраженный инфракрасный сигнал. Но даже в этом случае инфракрасные лучи не могут проникать сквозь непрозрачные предметы, например стены.

К недостаткам инфракрасных методов коммуникации относятся следующие.

- **Ограниченное расстояние**. Расстояние передачи сигналов с помощью инфракрасных лучей в принципе может быть более одного километра, однако в настоящее время реализованы лишь устройства с максимальным расстоянием до 30 метров.
- **Чувствительность к помехам**. Помехами может стать тепловое излучение окружающих предметов.

Радиоволны

Как известно, телефонные линии первоначально были разработаны для передачи голоса, однако по ним можно передавать и цифровые данные. Это же справедливо и для радиоволн — вплоть до последнего времени радиоволны использовались только для передачи звуковых сигналов, однако с их помощью можно передавать и сигналы данных.

Методы передачи и приема радиосигналов можно разделить на две категории:

- узкополосные;
- широкополосные.

Каждый из этих методов рассматривается ниже.

Узкополосная радиосвязь

С этим методом радиосвязи хорошо знаком каждый из нас. Передатчик посылает сигналы на определенной частоте, а приемник, настроенный на эту частоту, принимает сигналы. Так работают традиционные системы радиовещания и средства мобильной двусторонней связи.

Однако если по узкополосному каналу передаются данные, то их легко может перехватить кто угодно. Поэтому для повышения безопасности данных интенсивно разрабатываются широкополосные методы радиосвязи.

Широкополосная радиосвязь

В этом методе сигналы передаются не на одной частоте, а в некоторой заранее определенной полосе частот. Что касается загрузки эфира, то широкополосные методы менее эффективны, так как занимают более широкую полосу частот, в которой могло бы разместиться много узкополосных каналов связи. Однако безопасность широкополосных методов существенно выше, чем узкополосных. Методы широкополосной радиосвязи можно разделить на две категории.

- **Скачкообразное переключение частот (FHSS)**. В этом методе передатчик быстро переключается с одной частоты на другую. На принимающей стороне нужно знать последовательность и время переключений, поэтому перехватить такой сигнал очень сложно.
- **Непосредственное расширение спектра (DSSS)**. Используется специальная техника кодирования (*ращепление*), в которой для каждого бита передаваемых данных создаются избыточные фрагменты на других частотах.

Сетевые соединительные устройства

Термин *соединительное устройство* означает любое устройство, соединяющее различные части сети. К соединительному устройству подключены два кабеля (в некоторых случаях больше).

В следующих разделах рассматриваются три типа соединительных устройств:

- простые соединительные устройства;
- сложные соединительные устройства;
- соединительные устройства, предназначенные для сегментации и образования подсетей.

Простые соединительные устройства

Простое соединительное устройство — это всего лишь точка соединения. В нем сигнал не усиливается и не изменяется каким-либо иным образом. Здесь рассматриваются такие типы простых соединительных устройств:

- разъемы BNC;
- разъемы RJ;
- разъемы волоконно-оптических кабелей;
- коммутационные панели;
- пассивные концентраторы.

Разъемы BNC

В сетях 10Base2 для подключения сетевого адаптера к тонкому коаксиальному кабелю используется разъем BNC. Это небольшое устройство цилиндрической или Т-образной формы, в котором контактный штырек припаян к сердечнику кабеля. Разъем укрепляется на гнезде путем вращения внешнего кольца.

Существует два типа разъемов BNC.

- **Т-разъем BNC**. Разъем имеет Т-образную форму К сетевому *адаптеру* подключается нижняя ножка, а две боковые подключаются к двум кабелям. Если нужно подключить только один кабель, то к другому концу Т-разъема подключается терминатор.
- **Цилиндрический разъем BNC**. Представляет собой цилиндрическое устройство, к каждому концу которого подключается по кабелю. С его помощью можно нарастить общую длину кабеля.

Внимание!

Использование цилиндрических разъемов для наращивания кабеля нужно свести к минимуму, потому что в каждом из них происходят потери сигнала

Терминатор BNC — это 50-омное оконечное устройство, которое устанавливают на каждом конце коаксиальной магистрали Если на конце магистрали не поставить терминатор, то сигналы будут отражаться от "висящего" конца кабеля, внося помехи в другие сигналы Терминаторы должны быть установлены на каждом конце. Кроме того, один из концов должен быть *заземлен*, т е. подключен к проводу с нулевым электрическим потенциалом. Термин "заземление" используется потому, что во многих случаях проводником с нулевым потенциалом служит именно земля или металлические конструкции, имеющие с ней надежный контакт — батареи отопления, арматура зданий и т д.

Разъемы RJ

Разъемы RJ (Registered Jack) называются так потому, что их тип зарегистрирован и утвержден комиссией FCC (Federal Communication Commission) Разъем RJ состоит из *розетки* и *штепселя*. Иногда розетку называют *гнездом*

Разъемы RJ-11 используются повсеместно в обычных аналоговых телефонных системах. Почти в каждом доме телефонный провод оканчивается модульным штепселем.

Внутри стены розетка подключена к неэкранированной витой паре категории 3 или 5 (в большинстве современных зданий). Разъемы RJ-11 используются также для подключения модемов.

В Ethernet для подключения неэкранированных витых пар используются разъемы RJ-45. Штепсель и розетка RJ-45 выглядят так же, как и RJ-11, однако у RJ-45 они немного больше. Для подключения пары проводов к розетке RJ-45 используется специальный набор инструментов.

Существует много других марок разъемов RJ, однако в компьютерных сетях обычно используются RJ-11 и RJ-45.

Разъемы волоконно-оптических кабелей

Устанавливать разъемы волоконно-оптических кабелей довольно трудно, потому что положение торца каждой оптической нити должно быть тщательно подогнано. После подгонки кабель укрепляется на разъеме с помощью эпоксидных смол или специальных цементирующих веществ.

В компьютерных сетях обычно используются следующие типы волоконно-оптических разъемов:

- **SC** — вставляемый разъем;
- **ST** — штыкообразный разъем с ключом;
- **FC** — разъем с резьбой и ключом;
- **SMA** — разъем с резьбой;
- **FSD** — устройство с фиксированным экраном. Используется в сетях FDDI.

Коммутационные панели и пассивные концентраторы

На *коммутационной панели* устанавливаются постоянные соединения кабелей, проложенных к ней из различных мест. Она похожа на старую телефонную панель, в которой соединения устанавливаются путем вставки штепселей в определенные розетки.

В сетях с звездообразной топологией кабели от компьютеров, расположенных в различных зданиях, проведены в специальную комнату, в которой находится коммутационная панель. Кабели от компьютеров подключены к монтажному блоку на задней стенке панели. На передней стенке расположены розетки RJ-45, от которых отрезки кабелей ведут к концентратору.

Коммутационная панель выполняет те же функции, что и пассивный концентратор, представляющий собой центральное соединительное устройство, в котором сходятся кабели от всех компьютеров или других сетевых устройств. В коммутационной панели нет электронных устройств, и она не потребляет электрическую мощность. Она не регенерирует сигналы, а только передает их на все свои порты.

Сложные соединительные устройства

Простые соединительные устройства служат только для установки электрического контакта с кабелем. В то же время функции сложных соединительных устройств значительно шире. Например, они могут усилить сигнал, прежде чем передать его дальше, или даже преобразовать тип сигнала для другого типа носителя.

В следующих подразделах рассматриваются такие типы сложных соединительных устройств:

- преобразователи,
- повторители,
- активные/интеллектуальные концентраторы

Преобразователи

Используются при соединении сегментов носителей разных типов, например 10BaseT с 10Base2, Ethernet 100BaseT с волоконно-оптическим кабелем или Token Ring с волоконно-оптическим кабелем

Повторители

Повторитель соединяет два сегмента сети или два участка кабеля В отличие от разъемов, он не только передает сигнал от одного кабеля к другому, но и *регенерирует* его Сигнал, ослабленный вследствие затухания, усиливается повторителем и передается дальше Поэтому с применением повторителя максимальное расстояние между компьютерами может быть увеличено

Замечание

Иногда с помощью повторителей можно соединять разные типы носителей например сегменты 10Base2 и 10Base5 Обе архитектуры принадлежат Ethernet и в обеих используется один и тот же метод доступа к сети Однако с помощью повторителей нельзя соединять сегменты разных типов сетей или сети, использующие разные методы доступа Например, нельзя соединить сегмент Ethernet (метод доступа — CSMA/CD) и сегмент Token Ring (метод доступа — передача маркера)

Повторители не фильтруют проходящие через них данные Они регенерируют *все* сигналы, включая компьютерные данные, шумы и помехи Повторители работают на физическом уровне модели OSI

Активные и интеллектуальные концентраторы

Активные концентраторы иногда называют *многопортовыми повторителями*, потому что они имеют много портов, как пассивные концентраторы, и, подобно повторителям, регенерируют сигналы, поступающие на один из портов, прежде чем передать их на другой порт Активные концентраторы потребляют электрическую мощность

Интеллектуальные концентраторы — это специальный тип активных концентраторов Они не только регенерируют сигналы, но и с помощью встроенного микропроцессора диагностируют порты Концентраторы работают на физическом уровне модели OSI

Устройства сегментации и создания подсетей

Соединительные устройства сегментации и создания подсетей — наиболее сложные из всех сетевых соединительных устройств *Сегментация* сети — это деление сети на сегменты, являющиеся частями этой сети *Создание подсетеи* — это деление сетей на отдельные сети, называемые *подсетями*, на основе адресной информации Термины "сегментация" и "создание подсетей" в некоторых случаях взаимозаменяемы В главах 8, "Сетевые протоколы и службы", и 9, "Самая глобальная сеть — Internet", создание подсетей рассматривается подробнее

Мосты

Обычный мост (*простой прозрачный мост*) объединяет два сегмента сети и выполняет *фильтрацию* передаваемых данных на основе MAC-адресов, записанных в пакетах. Это позволяет уменьшить загрузку сегментов сети. На рис. 7.7 показано, как сеть делится на два сегмента с мостом между ними. MAC-адреса представляют собой шестнадцатеричные числа.

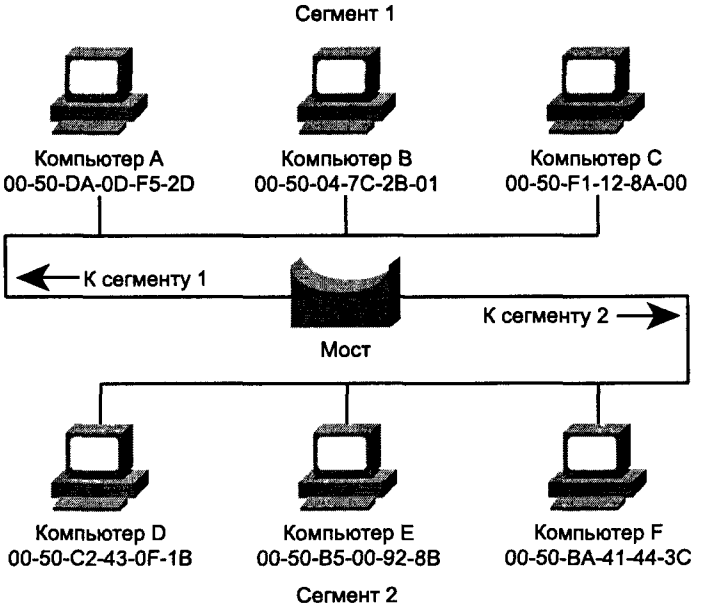


Рис. 7.7. Мост делит сеть на два сегмента

Мост создает таблицу адресов в несколько этапов.

1. Когда пакет передается в сеть, мост проверяет MAC-адреса источника и пункта назначения (адресата) данных. В таблице адресов записано, в каком сегменте (т.е. с какой стороны моста) расположен каждый адрес.
2. Если адрес назначения пакета в таблице отсутствует, то мост передает пакет в оба сегмента. Если в таблице отсутствует адрес источника, то мост добавляет его в таблицу.
3. Если адрес назначения в таблице есть, то мост передает пакет в соответствующий сегмент (только в том случае, когда передающий и принимающий пакет находятся в разных сегментах).
4. Если из таблицы адресов видно, что источник и адресат находятся в одном и том же сегменте, то мост не передает пакет никуда, поскольку в сегменте с адресатом этот пакет уже циркулирует.

Замечание

Таблицу адресов, созданную мостом, называют также *таблицей маршрутизации*, потому что она используется для определения того, на какую сторону моста следует передать пакет Не путайте ее с таблицей маршрутизации, используемой маршрутизатором! Таблица маршрутизации моста содержит адреса оборудования (т е MAC-адреса), а таблица маршрутизации маршрутизатора — IP-адреса

Рассмотрим пример сети, приведенный на рис 7 7 Если компьютер B посылает сообщение на компьютер F, то мост передает пакет в сегмент 2 Он делает это независимо от того, есть ли в таблице адрес компьютера F, потому что если в таблице нет адреса назначения, то пакет передается всем сегментам

Если компьютер B посылает сообщение на компьютер A, то мост сверяет адреса в пакете с адресами в таблице B том случае, если адрес компьютера A в таблице отсутствует, мост передает пакет в сегмент 2 Если же адрес компьютера A в таблице есть (поскольку компьютер A раньше посылал сообщения), то пакет *не передается* через мост Благодаря этому уменьшается объем передаваемых по сетевым каналам данных

Такой мост называется *прозрачным*, потому что компьютеры сети Ethernet его не видят, они даже ничего не знают о существовании моста

Мосты передают также широковещательные сообщения, имеющие *широковещательный адрес* FF-FF-FF-FF-FF-FF

Транслирующие и инкапсулирующие мосты

В отличие от повторителей, мосты могут соединять сегменты сети в которых используются разные методы доступа, например сегменты Ethernet и FDDI Однако в этих сегментах должен использоваться один и тот же протокол, например TCP/IP Такие мосты называются *транслирующими* или *инкапсулирующими*

Транслирующий мост преобразует, например, адреса Ethernet в адреса FDDI В то же время инкапсулирующий мост *инкапсулирует* кадр Ethernet, т е заключает его в кадр FDDI

В сетях Token Ring используются специальные мосты, которые называются *мостами с маршрутизацией источника* От обычных прозрачных мостов они отличаются тем, что зависят от главного компьютера, управляющего маршрутизацией

Мосты работают на канальном уровне модели OSI Поэтому пакеты с *немаршрутизируемыми* протоколами, например NetBEUI, могут пересекать мосты беспрепятственно Более подробно маршрутизируемые и немаршрутизируемые протоколы рассматриваются в главе 8, "Сетевые протоколы и службы" Как и повторители, мосты регенерируют данные, однако делают это на уровне пакетов

В сети может быть больше одного моста Это повышает отказоустойчивость сети, но может привести к *зацикливанию мостов* (рис 7 8), загружающему сеть ненужными потоками информации Зацикливание мостов происходит, когда между двумя точками сети существует несколько путей и пакет данных получает возможность ходить по кругу

Для решения проблемы зацикливания мостов был разработан алгоритм покрывающего дерева (Spanning-Tree Algorithm — STA) Технические подробности явления зацикливания и алгоритма STA выходят за рамки данной книги, однако с ними можно ознакомиться по дополнительным источникам, приведенным в конце главы

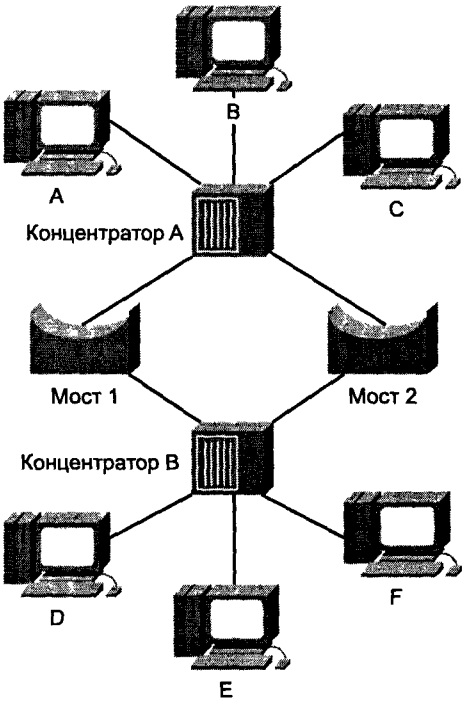


Рис. 7.8. Если между мостами существует несколько маршрутов, то может возникнуть зацикливание мостов

Маршрутизаторы

Передвигаясь вверх по модели OSI, мы дошли до соединительных устройств, работающих на сетевом уровне, — *маршрутизаторов*. С помощью маршрутизаторов соединяются отдельные сети (или подсети). Маршрутизаторы могут работать как внутри локальных сетей (в этом случае они соединяют подсети), так и в глобальных сетях, соединяя составляющие их локальные сети.

Как и мосты, маршрутизаторы фильтруют передаваемые данные. Однако в отличие от мостов, маршрутизаторы используют логические сетевые адреса (IP- или IPX-адреса), а не физические адреса устройств. Маршрутизаторы устроены сложнее, чем мосты. Они принимают серьезные решения: выбирают оптимальный маршрут передачи пакета среди немалого количества других возможных маршрутов.

Замечание

Фактически маршрутизаторы являются небольшими специализированными компьютерами. В их состав входят микропроцессоры, выполняющие специальные программы маршрутизации под управлением собственной операционной системы. Персональный компьютер также можно конфигурировать на выполнение функций маршрутизатора, однако его операционная система должна поддерживать IP- и IPX-адресацию.

Маршрутизаторы поддерживают таблицы маршрутов, в которых хранятся адреса других маршрутизаторов. Маршрутизатор должен иметь, как минимум, два сетевых

интерфейса, потому что он выполняет функции *шлюза* между сетями. Адрес интерфейса, обслуживающего отдельную подсеть, называется *шлюзом подсети по умолчанию* Обратите внимание: термин "шлюз" используется также для обозначения программ или устройств, работающих на более высоких уровнях OSI.

Задачи маршрутизаторов

Маршрутизаторы могут использоваться для объединения многих сетей в одну или для разделения большой сети на несколько меньших. В главе 9, "Самая глобальная сеть — Internet", рассматривается, зачем может понадобиться разделение сети на подсети.

Когда пакет данных передается от одного маршрутизатора к другому, заголовки канального уровня (фрагменты адресной информации) удаляются и создаются заново. Это позволяет маршрутизаторам передавать пакеты между разными сетями, например между Ethernet и Token Ring Этот процесс несколько замедляет передачу данных и снижает производительность сети.

Если в сети существует несколько маршрутов передачи пакета, то маршрутизатор выбирает оптимальный и впоследствии всегда использует его для передачи данных определенному адресату. Маршрутизатор рассматривает все возможные маршруты и принимает решение об оптимальном маршруте для каждого поступившего пакета. Следовательно, если некоторый маршрут в данный момент времени перегружен, маршрутизатор выбирает другой, более эффективный.

Маршрутизаторы могут фильтровать широковещательные пакеты как по уровню 2, так и по уровню 3. По умолчанию маршрутизаторы *не передают* пакеты, отправленные по широковещательному адресу 255.255 255 255 Это уменьшает загрузку сети и предотвращает распространение *широковещательного шторма*, когда большое количество широковещательных сообщений нарушает нормальную работу сети

Маршрутизируемые протоколы и протоколы маршрутизации

Маршрутизаторы работают только с *маршрутизируемыми* протоколами (IP, IPX, OSI, XNS, DECnet и DDP). В немаршрутизируемом протоколе, например в NetBEUI, нет адресной схемы, позволяющей маршрутизатору идентифицировать сеть, следовательно, такой протокол нельзя маршрутизировать.

Необходимо различать маршрутизируемые протоколы и протоколы маршрутизации. Для работы с маршрутизируемыми протоколами используется *динамическая маршрутизация.*

Далее сравниваются различные типы маршрутизации и маршрутизируемые протоколы, включая:

- статическую и динамическую маршрутизацию;
- внутренние и внешние протоколы маршрутизации.

Статическая и динамическая маршрутизация. Существует два основных способа маршрутизации.

- **Статическая маршрутизация**. Администратор вводит адреса в таблицу маршрутизации вручную и постоянно поддерживает их обновленными
- **Динамическая маршрутизация** Маршрутизаторы автоматически обмениваются адресной информацией с помощью протоколов RIP (Routing Information Protocol), OSPF (Open Shortest Path First) или NLSP (NetWare Link Services Protocol).

Динамическая маршрутизация и эти протоколы подробнее рассматриваются в главе 9, "Самая глобальная сеть — Internet".

Внутренние и внешние протоколы маршрутизации. Протоколы маршрутизации делятся на *внутренние* (Interior Gateway Protocol — IGP) и *внешние* (Exterior Gateway Protocol — EGP). Они подробно рассматриваются в главе 9, "Самая глобальная сеть — Internet".

Протоколы маршрутизации IGP используются в *автономных системах*, т.е. в сетях отдельных компаний или организаций.

Мосты-маршрутизаторы

В зависимости от используемого протокола транспортного уровня, мосты-маршрутизаторы могут работать или как мосты, или как маршрутизаторы. Сообщения, посланные с протоколом NetBEUI или с другим немаршрутизируемым протоколом, мост-маршрутизатор обрабатывает как мост, а сообщения с маршрутизируемыми протоколами (например, TCP/IP) — как маршрутизатор. Современные маршрутизаторы способны выполнять функции как мостов, так и маршрутизаторов.

Коммутаторы

Главное назначение коммутатора может показаться обманчиво простым: выбор пути, по которому следует послать данные.

Коммутаторы становятся все более популярными в сетях Ethernet. Они увеличивают производительность и к тому же сравнительно дешевы.

В коммутаторах используется один из следующих методов коммутации.

- **Без буферизации пакетов**. Коммутатор начинает передавать пакет по назначению, не дожидаясь, пока к нему поступит весь пакет. Такой метод более быстродействующий, однако при этом через коммутатор могут проходить испорченные пакеты.
- **С буферизацией пакетов**. Коммутатор *не начинает* передавать пакет, пока не получит его полностью и не проверит его целостность. Такой метод менее быстродействующий, но более надежный.

Существуют различные типы коммутаторов. Иногда коммутаторы классифицируют на основе уровней модели OSI, на которых они работают. В следующих подразделах описываются отличия коммутаторов уровней 2, 3 и 4.

Коммутаторы уровня 2

Стандартные коммутаторы уровня 2 работают как концентраторы, но с одним существенным отличием. Концентратор передает пакет на все свои порты, в то время как коммутатор (называемый в этом случае *коммутирующим концентратором*) определяет, какой порт подключен к компьютеру, которому адресован пакет, и передает пакет только на этот порт. Такой метод дает ряд преимуществ.

- Уменьшается количество ненужных пакетов, "гуляющих" по сети. Следовательно, снижается загрузка сетевых каналов.
- Создаются отдельные домены коллизий. Это предотвращает коллизии данных, которые ухудшают производительность и приводят к необходимости повторной передачи пакетов.
- Увеличивается безопасность данных вследствие того, что пакеты не передаются на все порты (если сообщения передаются на все порты, то их легче перехватить посторонним лицам).

Коммутирующие концентраторы еще называют *коммутаторами портов*, потому что к каждому порту подключается компьютер или сетевое устройство. Каждое устройство имеет собственный выделенный путь к коммутатору.

Другой тип коммутаторов — *сегментные*. К порту сегментного коммутатора подключается целый сегмент сети.

Коммутаторы можно использовать для создания *виртуальных локальных сетей*. В этом случае коммутаторы делят физическую сеть на несколько логических сетей, увеличивая таким образом производительность сети и безопасность данных.

Коммутаторы уровня 3

Как видно из названия, коммутаторы уровня 3 работают на сетевом уровне модели OSI. Устройства этого типа впервые были разработаны компанией 3Com в 1992 году с целью уменьшения количества управляемых сетевых устройств путем интеграции коммутаторов и маршрутизаторов.

Коммутаторы уровня 3 фактически являются маршрутизаторами, однако не обычными, а специального типа. Коммутатор уровня 3 (другое название — *коммутируемый маршрутизатор*) выполняет те же функции, что и выделенный маршрутизатор. В нем используются такие протоколы маршрутизации, как RIP или OSPF.

Устанавливать и конфигурировать коммутаторы уровня 3 легче, чем маршрутизаторы. В локальной сети их можно использовать вместо маршрутизатора почти всегда. К тому же, несмотря на более широкие возможности и легкость применения, коммутаторы уровня 3 стоят меньше, чем маршрутизаторы.

Коммутаторы уровня 4

В последнее время функциональные возможности коммутаторов уровня 3 были существенно расширены в целях использования дополнительной информации, содержащейся в заголовках TCP и UDP, например о номерах портов. Такие коммутаторы стали называться *коммутаторами уровня 4*, потому что протоколы TCP и UDP работают на транспортном, четвертом, уровне модели OSI. Однако, несмотря на название, эти коммутаторы часто используют информацию и более высоких уровней.

Наиболее важным результатом применения коммутаторов уровня 4 является повышение безопасности данных путем фильтрации списка контроля доступа (Access Control List — ACL) Традиционные маршрутизаторы тоже могут использовать информацию уровня 4 (некоторые маршрутизаторы, например Cisco 7500, могут также выполнять функции уровня 4), однако выполнение ими фильтрации ACL существенно снижает производительность. В то же время коммутаторы уровня 4 обрабатывают пакеты на уровне оборудования, поэтому производительность не снижается.

Коммутаторы уровня 4 могут управлять выделением пропускной способности для различных типов пакетов. Это позволяет реализовать службы QoS и выравнивать загрузку сетевых каналов.

Функции коммутаторов уровня 4 может выполнять большинство современных маршрутизаторов.

Резюме

В этой главе представлена широкая гамма сетевых устройств, а также выбор некоторых из них, установка, конфигурирование и устранение неполадок.

Рассмотрены доступные в настоящее время типы сетевых носителей, как кабельных, так и беспроводных. Особое внимание было уделено техническим характеристикам трех наиболее распространенных типов кабелей: коаксиальных (толстых и тонких), витых пар (экранированных и неэкранированных) и волоконно-оптических ка-

белей. Описаны преимущества и недостатки каждого из них, а также их использование в различных архитектурах локальных сетей.

Рассмотрены наиболее распространенные устройства, используемые для соединения сегментов сетей и подсетей. Сначала представлены простые устройства, не содержащие электронных компонентов: кабельные разъемы, коммутационные панели и пассивные концентраторы; затем более сложные устройства: повторители, активные и интеллектуальные концентраторы. После этого обсуждались вопросы сегментирования сетей и создания подсетей с помощью мостов, маршрутизаторов и коммутаторов.

Теперь вы знакомы с принципом действия основных компонентов сетевого оборудования, поэтому в следующей главе можно приступить к более глубокому рассмотрению сетевых протоколов и служб.

Рекомендуемые источники

Прекрасный учебник по беспроводным сетям можно найти на Web-узле по адресу: `www.proxim.com/wireless/whiteppr/whatwlan.shtml`.

Более подробная информация о мостах, зацикливании мостов и алгоритме покрывающего дерева приведена по адресу: `www.officewizard.com/books/network/ch07.htm`.

Великолепное разъяснение принципов коммутации на уровне 3 можно найти по адресу: `www.3com.com/technology/tech_net/white_papers/500660.html`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Какой базовый компонент сетевого оборудования подключается к компьютеру?
   - **а.** Маршрутизатор.
   - **б.** Кабель.
   - **в.** Сетевой адаптер.
   - **г.** Концентратор.
2. В каком типе сетей используется внешний трансивер?
   - **а.** 10Base2.
   - **б.** 10Base5.
   - **в.** 10BaseT.
   - **г.** Во всех перечисленных.
3. Допустим, сетевой адаптер нужно установить в компьютер с мышью PS/2, клавиатурой, принтером и двумя контроллерами ID. Все эти устройства используют IRQ по умолчанию. Звуковому адаптеру присвоен IRQ 10. Какой IRQ следует присвоить сетевому адаптеру?
   - **а.** 5.
   - **б.** 7.
   - **в.** 12.
   - **г.** 14.

4. Какой кабель удовлетворяет требованиям пожарной безопасности при установке в пространстве между фальшь-потолком и потолком?
   а. Категории 5.
   б. Толстый коаксиальный кабель.
   в. Военной спецификации
   г. Пленум-кабель
5. Какой тип кабеля определен спецификациями сетей 10Base2?
   а. RG-58 /U
   б. RG-59 A/U
   в. RG-58 C/U
   г. RG-59.
6. С каким типом кабеля используется разъем "зуб вампира"?
   а. Неэкранированная витая пара
   б. Экранированная витая пара
   в. Толстый коаксиальный кабель
   г. Тонкий коаксиальный кабель
7. Как называется утечка сигнала с одного провода на другой, которую можно уменьшить путем скручивания проводов?
   а. Электромагнитные помехи.
   б. Затухание
   в. Искажение.
   г. Перекрестные помехи
8. Какой тип разъема используется с неэкранированной витой парой в сетях Ethernet?
   а. RJ-45
   б. RJ-11.
   в. Разъем BNC
   г. Разъем F
9. Какое из приведенных утверждений о волоконно-оптическом кабеле справедливо? (Выбрать все подходящие.)
   а. Из всех типов кабелей волоконно-оптический легче всего установить и работать с ним
   б. Волоконно-оптический кабель обеспечивает большую безопасность данных, чем медный
   в. Волоконно-оптический кабель более чувствителен к затуханию, чем медный
   г. Пропускная способность волоконно-оптического кабеля в одномодовом режиме выше, чем в многомодовом.
10. Какое устройство используется для соединения двух сегментов сетевых кабелей и регенерации передаваемого сигнала для устранения эффекта затухания?
   а. Цилиндрический разъем
   б. Коммутационная панель
   в. Повторитель
   г. Пассивный концентратор

Глава 8

Сетевые протоколы и службы

Если сравнивать сетевое оборудование с костями и тканями организма, а сигналы, проходящие по сети, с кровью, то сетевые протоколы и службы следует назвать мозгом сети. Протоколы указывают сетевым устройствам, что они должны делать. Другими словами, протоколы управляют сетью так же, как мозг управляет телом.

Сетевые протоколы представляют собой наборы логических правил, согласно которым работает сеть. Сетевые *службы*, например службы разрешения имен или размещения адресов, выполняют специфические функции. Это немного похоже на то, как различные области головного мозга управляют функциями дыхания, речи, зрения и т.д.

Существует множество типов сетевых протоколов, работающих на разных уровнях модели OSI. В источниках по сетям персональных компьютеров термином "протокол" часто обозначаются протоколы *сетевого* и *транспортного* уровней, т.е. уровней 3 и 4 модели OSI. Чтобы сетевые компьютеры могли сообщаться, они должны использовать общий протокол.

В этой главе рассматриваются следующие протоколы сетевого и транспортного уровней:

- NetBEUI;
- IPX/SPX;
- TCP/IP.

Эти три стандартных стека протоколов поддерживаются большинством операционных систем персональных компьютеров. Каждый из них имеет определенные достоинства и недостатки, зависящие от условий работы локальной сети.

В этой главе рассматриваются также сетевые службы DNS (Domain Name System), WINS (Windows Internet Name Service) и DHCP (Dynamic Host Configuration Protocol). Все они работают с протоколом TCP/IP, расширяя его функциональные возможности.

Протокол NetBIOS/NetBEUI

В некоторых источниках можно прочитать, что NetBIOS и NetBEUI — это одно и то же. В недалеком прошлом фактически так и было. Служба NetBIOS (Network Basic Input/Output System) была разработана компанией IBM и применялась компанией Microsoft в ранних реализациях локальных сетей. В то время термин NetBIOS означал как API (Application Programming Interface), так и стек протоколов транспортного и сетевого уровней.

Замечание

Стек протоколов — это группа из двух или более протоколов, которые работают совместно, причем каждый на своем уровне модели OSI.

В дальнейшем компоненты NetBIOS были разделены на собственно NetBIOS (API) и протокол NetBEUI (NetBIOS Extended User Interface), включающий протоколы сетевого и транспортного уровней. NetBIOS не определяет кадры или формат передаваемых по сети данных; это делает NetBEUI.

NetBIOS: API

NetBIOS работает с протоколами NetBEUI, IPX/SPX или TCP/IP. С помощью NetBIOS приложения могут взаимодействовать с распространенными интерфейсами программирования, разделяя информацию с приложениями, использующими другие протоколы более низких уровней.

Работая на более высоких уровнях (на уровне приложений модели DoD и на сеансовом уровне модели OSI), NetBIOS поддерживает два режима коммуникации: сеансовый и дейтаграммный.

В сеансовом режиме NetBIOS позволяет устанавливать *сеанс* соединения между компьютерами с обнаружением ошибок и восстановлением данных. В дейтаграммном режиме индивидуальные сообщения посылаются отдельно. Соединение при этом не устанавливается, поэтому обнаружение и исправление ошибок возлагается на приложение.

NetBIOS содержит также службу имен (т.е. имен NetBIOS), с помощью которых в сети можно идентифицировать компьютеры и приложения.

NetBEUI — самый простой из трех рассматриваемых в этой главе стеков протоколов. Простота делает его самым быстродействующим (в смысле скорости) из этой тройки, однако эта же простота существенно ограничивает его функциональные возможности. В протоколе NetBEUI нет средств логической адресации на сетевом уровне, поэтому его нельзя маршрутизировать из одной сети или подсети в другую. Однако внутри одной локальной сети он работает неплохо. Его легко конфигурировать. Кроме того, NetBEUI можно использовать с маршрутизируемым протоколом, например с TCP/IP. При этом сохраняется преимущество высокого быстродействия NetBEUI внутри локальной сети и появляется возможность коммуникации с компьютерами за пределами локальной сети с помощью TCP/IP.

Протокол IPX/SPX

Протоколы IPX и SPX, работая совместно, обеспечивают маршрутизацию сетевых сообщений. Компания Novell разработала протокол IPX/SPX для серверов и клиентов NetWare, однако его можно использовать и в других операционных системах, например в Windows. Протокол IPX/SPX разрабатывался на основе протоколов XNS (Xerox Network System).

Замечание

IPX/SPX, или NWLink, необходим для соединения клиентов Microsoft с серверами NetWare 4.x или более ранних версий. Некоторые серверы NetWare 5.x могут работать только с протоколом TCP/IP.

Производительность и легкость конфигурирования IPX/SPX лучше, чем у TCP/IP. Иногда IPX/SPX используют во внутренней локальной сети специально для повышения безопасности: внешние компьютеры, получающие доступ к локальной сети посредством Internet, работают только по протоколу TCP/IP, поэтому они не могут получить доступ к компьютерам локальной сети, работающим с IPX/SPX.

Компания Microsoft поставляет совместимый с IPX/SPX стек протоколов NWLink, реализованный во всех современных операционных системах Windows. Однако по умолчанию NWLink не устанавливается.

Протокол IPX работает на сетевом уровне модели OSI, он относится к протоколам, работающим в режиме без установки соединения. Протокол SPX работает на транспортном уровне модели OSI, он обеспечивает распознавание и сборку пакетов, а также другие службы режима с установкой соединения.

Замечание

Режим *с установкой соединения* напоминает разговор двух людей по телефону. Если вам нужно поговорить с Джонсом, вы набираете его телефонный номер и спрашиваете его по фамилии. Вы не передаете сообщение, пока не убедитесь, что Джонс держит в руке телефонную трубку (т.е. пока не установлен сеанс соединения).

Режим *без установки соединения* похож на обычную почтовую систему. Человек отправляет по почте письмо с написанным на нем адресом. У него нет возможности убедиться, что письмо дойдет до адресата, однако из предыдущего опыта он знает, что адресат получит письмо почти наверняка. Передать сообщение без установки соединения можно и мистеру Джонсу в нашем предыдущем примере. Допустим, во время вашего звонка Джонса в комнате не оказалось. В этом случае вы просите написать Джонсу записку и положить на его стол. В этом случае у вас тоже нет возможности проверить, получил ли Джонс вашу записку (вернее, возможность есть — можно позвонить еще раз, однако вы не делаете этого, так как знаете, что скорее всего Джонс успешно получил ваше сообщение). Таким образом, вы передали Джонсу сообщение, не устанавливая сеанс соединения.

Протокол сетевого уровня IPX

В главе 3, "Концепции, модели и стандарты компьютерных сетей", рассматривается, как сетевой уровень модели OSI осуществляет логическую адресацию и маршрутизацию сообщений, т.е. обеспечивает передачу сообщений по нужному адресу. Это и есть главная задача протокола IPX.

Маршрутизируемый протокол должен иметь возможность идентифицировать сеть, в которой расположен принимающий компьютер. Для идентификации сети (подсети) в IPX используется шестнадцатеричный *номер сети*. Типичный номер сети в IPX выглядит так: 805609a0. Этот номер присваивается сети администратором.

Адрес IPX состоит из двух частей: номера сети и *номера узла* (рис. 8.1). Номер узла идентифицирует конкретное устройство на основе MAC-адреса сетевого адаптера.

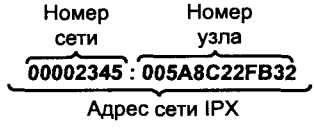


Рис. 8.1. Адрес IPX состоит из номера сети и номера узла

В сетях, использующих одновременно TCP/IP и IPX/SPX, номер сети часто получают из IP-адреса путем простого преобразования десятичного числа (IP-адреса) в шестнадцатеричное. Например, десятичный IP-адрес 214.12.1.42 преобразуется в шестнадцатеричный D6C12A.

Протокол извещения об услугах

Для извещения клиентов об услугах различных сетевых служб (например, файловых серверов) в IPX используется протокол SAP (Service Advertising Protocol). Каждой сетевой службе присваивается идентификатор SAP (число, которое называется SAP ID). Широковещательные сообщения SAP передаются каждые 60 с. Маршрутизаторы и серверы поддерживают таблицы, отображающие SAP ID на службы, и динамически обновляют эти таблицы с каждым широковещательным сообщением SAP. Постоянное обновление таблиц значительно загружает сети.

Протокол транспортного уровня SPX

Протокол SPX работает на один уровень выше, чем IPX, т.е. на транспортном уровне. В отличие от IPX, работающего в режиме без установки соединения, SPX работает в режиме с установкой соединения. Это делает SPX более надежным, что весьма уместно на транспортном уровне, ответственном за подтверждения, обнаружение ошибок и другие аспекты обеспечения надежности.

Протокол IPX доставляет пакеты по назначению, а SPX следит за тем, чтобы пакеты прибыли полностью и в целостном состоянии. Протокол SPX поддерживает нумерацию пакетов и отслеживает количество переданных пакетов. Он гарантирует доставку пакетов путем контроля принятых данных.

Протокол TCP/IP

Стек протоколов TCP/IP — фундамент Internet. Он неуклонно превращается в наиболее распространенный протокол сетевого и транспортного уровней для сетей всех размеров и конфигураций. Поэтому ему уделяется наибольшее внимание.

В следующих разделах этой главы рассматриваются основные понятия и теоретические основы различных компонентов пакета TCP/IP, что каждый из них делает и как они работают. В главе 12, "Клиентские операционные системы", речь пойдет о конфигурировании TCP/IP в различных операционных системах.

Пакет протоколов TCP/IP

Протокол TCP/IP — это не только стек протоколов сетевого и транспортного уровней, но и полный набор протоколов, работающих на многих уровнях сетевой модели. Пакет протоколов TCP/IP включает также дополнительные компоненты, необязательные в процессах сетевой коммуникации, например утилиты прикладного уровня, также входящие в состав пакета TCP/IP.

Многие протоколы, входящие в пакет, предназначены для сбора информации или для устранения неполадок. В следующих разделах все они будут рассмотрены, однако начнем с главного: протоколов транспортного и сетевого уровней.

Протокол сетевого уровня IP

Как упоминалось раньше, на сетевом уровне выполняются задачи маршрутизации. В протоколах TCP/IP маршрутизация поддерживается путем применения IP-адресов, иден-

тифицирующих сетевые устройства. Каждый компьютер, принтер (подключенный к сети), маршрутизатор или любое другое сетевое устройство имеет уникальный IP-адрес.

Замечание

Сетевое устройство фактически может иметь несколько IP-адресов, по одному для каждого *сетевого интерфейса*. Маршрутизаторы имеют, как минимум, два интерфейса, подключенных к разным подсетям. Каждый IP-адрес уникален. В компьютерах с несколькими сетевыми адаптерами каждому из них присвоен свой сетевой адрес.

IP-адресация

Каждый IP-адрес состоит из двух частей. Вместе они идентифицируют сеть, в которой расположено устройство, и само устройство. Один раздел IP-адреса представляет *сеть*, а другой — *хост* (отдельный компьютер). Это похоже на почтовый адрес, состоящий из двух частей, вместе идентифицирующих дом, в который направляется письмо.

- Название улицы сообщает почтовой службе о том, в каком районе расположен дом. Название этой улицы присутствует в адресах многих домов, расположенных на ней.
- Номер дома уникален для каждого отдельного дома, расположенного на этой улице. В городе есть много домов с таким номером, однако существует только один дом с указанными в адресе названием улицы и номером дома.

Аналогично этому, один и тот же адрес сети имеют многие компьютеры, однако сочетание адреса сети и адреса хоста для каждого компьютера уникально (вернее, для каждого сетевого адаптера, ведь есть компьютеры с несколькими сетевыми адаптерами).

Например, первые три раздела IP-адреса 201.32.0.4 идентифицируют сеть. Разделы называются *октетами*. Последний раздел идентифицирует сетевой интерфейс отдельного компьютера. Все компьютеры в этой подсети имеют один и тот же номер сети (идентификатор сети) — 201.32.0. Однако каждый компьютер имеет свой номер хоста — .4, единственный в этой подсети.

Если письмо отправлено из Далласа в Сан-Франциско, то почтовое отделение Далласа не интересует номер дома в Сан-Франциско. Сначала следует передать письмо в нужный город. Аналогично этому, если сообщение передается по Internet в другую локальную сеть, маршрутизаторам не нужна та часть IP-адреса, в которой записан номер хоста. Им требуется только адрес сети. Когда пакет поступает в нужную сеть (подсеть), адрес хоста используется для передачи пакета указанному компьютеру точно так же, как почтовое отделение в Сан-Франциско использует название улицы и номер дома для доставки письма в конкретный дом.

Если компьютер посылает сообщение по IP-адресу 201.32.0.4, в котором число 201.32.0 представляет сеть, а число 4 — хост, то первым шагом будет доставка пакета в сеть 201.32.0. После прибытия в сеть пакет маршрутизируется внутри сети на компьютер с номером хоста, равным 4.

В нашем примере сеть идентифицируется первыми тремя октетами. Однако так делается не всегда. В традиционной схеме IP части IP-адреса, представляющие сеть и хост, могут иметь разные размеры для различных *классов* IP-адреса, рассматриваемых в следующем разделе.

Классы IP-адресов

Подобно любой обрабатываемой компьютером информации, IP-адрес состоит из двоичных цифр, т.е. битов. Человеку трудно работать с длинными строками из нулей и еди-

ниц, поэтому обычно IP-адреса записываются в *десятичном* формате (двоичная и десятичная системы счисления рассматривались в главе 3, "Концепции, модели и стандарты компьютерных сетей"). Однако IP-адрес в десятичной записи — это не десятичное число. Десятичным числом является каждый раздел, или октет IP-адреса. Октеты отделяются друг от друга точкой, но это не десятичная точка, отделяющая целую часть от дробной, а всего лишь условный символ, отделяющий октеты друг от друга.

Длина октета равна восьми битам, т.е. октет — это последовательность из восьми нулей или единиц. Иногда четыре октета обозначаются как w.x.y.z. В такой записи первый октет (правый) называется z-октетом, следующий — y-октетом и т.д.

IP-адрес состоит из четырех октетов по восемь битов каждый, всего — 32 бита. Это значит, что максимальное количество различимых IP-адресов равно 2^{32}, или 4 294 967 296. Типичный IP-адрес выглядит так: 192.168.1.12.

Замечание

Здесь рассматривается протокол IP версии IPv4, которая используется в Internet в настоящее время. Однако сейчас разрабатывается новый стандарт — IPv6, или IPng (IP Next Generation). В новом стандарте IP-адрес будет 128-битовым, т.е. максимальное количество различимых адресов будет равно 2^{128}.

Итак, одна часть IP-адреса идентифицирует сеть, а другая — компьютер (хост). Но где же расположены эти части в IP-адресе? К сожалению, ответ на этот вопрос неоднозначен. Традиционно это зависит от класса сети, являющегося одновременно классом IP-адреса. (Далее в главе рассматривается новейший метод адресации, названный *бесклассовым*.)

IP-адреса предоставляет организация IANA (Internet Assigned Numbers Authority). Первое время после появления Internet казалось логичным выделять IP-адреса компаниям и организациям блоками, потому что для коммуникации в Internet каждому компьютеру локальной сети нужен уникальный адрес.

Замечание

С появлением NAT (см. главу 6, "Глобальные сети") каждому компьютеру локальной сети уже не обязательно иметь собственный публичный IP-адрес

Размер выделяемого блока адресов зависел от размера локальной сети. Большим компаниям нужны были большие блоки адресов, а маленьким — маленькие. *Классы адресов* назначались на основе размера локальной сети, т.е. количества хостов. В табл. 8.1 показаны традиционные классы IP-адресов.

Таблица 8.1. Классы IP-адресов

Класс адреса	Количество сетей	Количество хостов на сеть
A	126*	16 777 216
B	16 384	65 535
C	2 097 152	254
D (широковещательный)	–	–

** В классе A адреса 127.x.x.x зарезервированы для* обратных адресов, *используемых в проверочных и диагностических целях.*

Замечание

В блоке 127.x.x.x содержится 24 млн IP-адресов. В первые годы существования Internet это не было проблемой, потому что свободных IP-адресов было значительно больше, чем подключенных к Internet компьютеров. Тогда никто не мог предвидеть коммерциализацию и столь бурный рост Internet.

Как видно из табл. 8.1, доступны только 126 адресов класса A. К настоящему времени все они уже заняты. Они присвоены наиболее крупным корпорациям и учебным центрам, таким, как IBM, Hewlett Packard, Xerox, MIT (Massachusetts Institute of Technology), Columbia University, Digital Equipment Corporation, General Electric и Apple. В каждой из этих сетей индивидуальные номера можно присвоить 16 млн хостов.

В приведенной схеме адресации можно создать 2 млн сетей класса C, в каждой из которых может быть не более 254 адресов хостов. Адреса класса C выделяются провайдерам Internet.

Адреса класса B занимают промежуточное положение. Они присваивались главным образом большим компаниям, размер которых в то время был недостаточен для класса A. Компании Microsoft выделены адреса класса B.

Адреса класса D предназначены для *широковещательных сообщений*, т.е. для передачи одного сообщения одновременно многим получателям. Адрес класса D присваивается специальной группе компьютеров, в этом случае пакеты обрабатываются и распределяются широковещательными протоколами.

Деление IP-адресов на классы в зависимости от размера сети называется *классовой адресацией*. (*Бесклассовая адресация* рассматривается далее в главе.)

Широковещание и широковещательная магистраль

В Internet широковещательные сообщения выполняют те же функции, что и в локальных сетях. Однако в Internet они посылаются *не всем* компьютерам, а только входящим в предопределенную широковещательную группу.

Использование широковещательных сообщений имеет следующие преимущества:

- экономится пропускная способность сети, потому что по многим адресам передается один пакет, а не много одинаковых пакетов каждый по своему адресу;
- не нужно знать адрес каждого компьютера, которому передается пакет. Для отправки широковещательного сообщения необходимо знать только широковещательный адрес.

Традиционные сообщения, передаваемые одному адресату, называются *однонаправленными*. Традиционные маршрутизаторы Internet конфигурированы на передачу только однонаправленных сообщений, они не могут обрабатывать широковещательные пакеты. Для решения этой проблемы организация IETF (Internet Engineering Task Force) разработала виртуальную сеть, названную *широковещательной магистралью* (Multicast Backbone — MBONE), представляющую собой специальное программное обеспечение, работающее в Internet. Используя то же оборудование, что и Internet, программы широковещательной магистрали обеспечивают передачу широковещательных пакетов внутри обычных однонаправленных пакетов. Такая *инкапсуляция* скрывает широковещательные пакеты от маршрутизаторов, которые не могут их обрабатывать. В то же время инкапсулированные широковещательные пакеты могут проходить через традиционные нешироковещательные маршрутизаторы.

Классовая адресация

Для IP-адресов используется десятичное обозначение, однако фактически они представляют собой двоичные числа. В табл. 8.2 показано, как определить класс адреса, исходя из значения первого октета. Чтобы легче было понять табл. 8.2, будем рассматривать не десятичное представление IP-адреса, а двоичное.

Таблица 8.2. Определение класса адреса

Класс IP-адреса	Старшие биты	Диапазон адресов первого октета	Количество битов в адресе сети
Класс A	0	0-127*	7
Класс B	10	128-191	14
Класс C	110	192-223	21
Класс D	1110	224-239	28

** В классе A адреса 127.x.x.x зарезервированы для* обратных адресов, *используемых в проверочных и диагностических целях.*

Класс адреса идентифицируется *битами высших разрядов* или несколькими первыми битами самого левого октета (называемого w-октетом).

Как видно из табл. 8.2, адрес принадлежит классу A, если первый бит равен 0, классу B — если первые два бита равны 10, классу C — если первые три бита равны 110, классу D — если первые четыре бита равны 1110.

Рассмотрим такой IP-адрес: 11001111.00101100.010100001.11100111. Первые три бита равны 110, следовательно, адрес принадлежит классу C. Преобразуем двоичные числа этого адреса в десятичные (с помощью научного калькулятора или как описано в главе 3, "Концепции, модели и стандарты компьютерных сетей"). В десятичном формате адрес имеет вид 207.44.81.231.

Обратите внимание на то, что первый октет (207) попадает в диапазон 192–223, приведенный в табл. 8.2 для класса C. Первый октет адресов класса C попадает в диапазон 192–223 потому, что первые три бита равны 110. Это значит, что класс IP-адреса можно определить по значению первого октета.

В предыдущем примере октеты 207.44.81 определяют сеть (подсеть), в которой расположен компьютер. Для всех компьютеров этой подсети первые три октета их IP-адресов равны 207.44.81. Число 231 определяет конкретный хост. Ни для какого другого устройства этой подсети последний октет IP-адреса не может быть равным 231. На рис. 8.2 показано, как IP-адрес делится на номер сети и номер хоста.

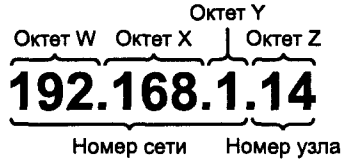


Рис. 8.2. В адресе класса C первые три октета определяют номер сети

Как определить максимальное количество сетей и компьютеров, которые можно реализовать в каждом классе? Традиционно в адресе класса A первый октет служит адресом сети, а три остальных — адресом хоста. Первый (старший) бит первого октета

в адресе класса A используется для идентификации класса, поэтому для идентификации сети остается только семь битов.

В адресе класса B для идентификации сети используются два первых октета, а для идентификации хоста — два вторых. Первые два октета содержат 16 бит, однако первые два из них используются для идентификации класса. Таким образом, для идентификации номера сети остается 14 бит.

В классе C первые три октета (24 бита) используются для идентификации сети, а последний — для идентификации хостов. Три первых бита идентифицируют класс, поэтому, чтобы получить количество битов, выделенных для идентификации сети, нужно из 24 вычесть 3. Другими словами для идентификации номера сети используется 21 бит.

Вернемся к сети класса A. В нем для идентификации номера сети выделено 7 бит. Если все 7 бит "включены" (равны единице), то получается самое большое число, которому может быть равен номер сети, — 1111111. В десятичном формате это число равно 127. Учитывая, что адрес 0.0.0.0 зарезервирован для представления всех IP-адресов и что номер 127 занят для обратных адресов, делаем вывод, что в классе A может существовать 126 различимых сетей.

Этот результат можно получить проще, если возвести число 2 в степень x, где x — количество битов, выделенных для номера сети. Так как $2^7 = 128$, значит, в семи битах можно записать 128 различимых чисел. Но, поскольку два адреса уже заняты (адрес 0.0.0.0 и обратный адрес), мы опять получаем, что максимальное количество сетей класса A равно 126.

Аналогично вычисляется максимальное количество сетей классов B и C.

- **Класс B** — 14 бит: $2^{14} = 16\,384$.
- **Класс C** — 21 бит: $2^{21} = 2\,097\,252$.

Замечание

В некоторых источниках используется формула $2^x - 2$. Двойка вычитается потому, что согласно старому правилу номера сети не могут состоять из одних нулей или единиц. Это правило появилось в связи с тем, что старые маршрутизаторы не могли обрабатывать такие номера сети. Однако многие современные маршрутизаторы лишены этого недостатка, поэтому вычитать двойку больше не нужно.

Современные маршрутизаторы могут обрабатывать *сетевые* номера, состоящие только из нулей или единиц. Однако на номера *хостов* это не распространяется, они по-прежнему не могут состоять только из нулей и единиц. Поэтому при подсчете максимального количества хостов нужно вычитать двойку.

Нетрудно заметить, что классовая адресация — не самый эффективный метод использования ограниченного количества IP-адресов, допустимых в 32-разрядной схеме адресации. Допустим, компания желает подключить к Internet 2 000 компьютеров. Адреса класса C не подойдут, потому что в этом классе сеть может содержать не более 254 хостов. Следующая ступень — адреса класса B. Если компании будет выделен номер сети этого класса, то она сможет разместить в ней 65 000 хостов. Однако ей нужно разместить только 2 000 хостов, остальные 63 000 IP-адресов окажутся занятыми ничем, т.е. утраченными. Эта проблема решается методом бесклассовой адресации.

Бесклассовая адресация

Бесполезная потеря IP-адресов в методе классовой адресации привела к нехватке публичных IP-адресов. Одно из возможных решений этой проблемы — реализация протокола IPv6, в котором используется большее адресное пространство — 128 бит. Однако переход к новой версии IP сложен и займет, видимо, еще немало времени. Между тем уже сейчас существует другое решение: бесклассовая адресация на основе метода CIDR (Classless Interdomain Routing).

В методе CIDR используются не классы адресов, а суффиксы, добавленные к каждому IP-адресу и определяющие количество битов, выделенное для сетевой части адреса. Сети CIDR иногда называются сетями "слэш *x*", потому что IP-адреса отделяются от суффикса символом слэша (/). Типичный адрес CIDR выглядит так: 192.168.1.0/24. Символы "/24" означают, что крайние левые 24 бита IP-адреса используются для хранения номера сети, а остальные восемь битов — номера хоста. Другими словами, первые три октета идентифицируют номер сети, а последний — номер хоста. В классовой схеме адресации это была бы сеть класса C.

В табл. 8 3 показано соответствие адресов CIDR и традиционных классовых адресов

Таблица 8.3. Адреса CIDR (бесклассовые) и традиционные классовые адреса

Адрес CIDR	Классовый адрес
/8	Класс A
/16	Класс B
/24	Класс C

В методе CIDR размещение IP-адресов происходит значительно эффективнее. Кроме суффиксов, приведенных в табл. 8.3, допускаются суффиксы /12, /20, /21, /28 и т.д. Другими словами, для номера сети можно выделить любое количество битов IP-адреса. Таким образом, размер сети может находиться в промежутке между максимальными размерами сетей традиционных классов.

В методе CIDR можно объединять небольшие непрерывные блоки адресов в один большой блок. Это называется созданием *суперсетей.*

Автоматическое выделение адресов

Для коммуникации с помощью протокола TCP/IP компьютер (или другое сетевое устройство) должен иметь уникальный IP-адрес, т.е. *логический* адрес, обрабатываемый на сетевом уровне.

Сетевая часть адреса для всех компьютеров данной подсети должна быть одной и той же. Например, если для сети класса C используется маска подсети по умолчанию, то адреса 192.168.1.12 и 192.168.1.34 принадлежат двум компьютерам одной и той же подсети, потому что в них номера сети, представленные первыми тремя октетами, совпадают.

В то же время части адресов, представляющие хосты, для двух компьютеров одной и той же подсети *должны отличаться.* Например, в одной подсети не может быть двух компьютеров с адресом хоста, равным 6.

Присвоить IP-адрес компьютеру можно двумя способами.

- Вручную. Для этого адрес необходимо ввести при конфигурировании параметров TCP/IP. Сетевой администратор, присваивающий адрес, должен понимать

принципы адресации TCP/IP и знать, как выбрать правильный адрес в конкретной сети.

- Автоматически. Для этого в сети должен быть компьютер, конфигурированный как сервер DHCP. Он присваивает другим компьютерам IP-адреса из списка допустимых адресов. Если компьютер не контактирует с сервером DHCP, то он может сам автоматически присвоить себе адрес с помощью процедуры автоматической IP-адресации APIPA (Automatic Private IP Addressing), входящей в состав операционной системы.

Служба DHCP

Протокол DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации хоста) выполняется на компьютере, конфигурированном как сервер DHCP. Сервер DHCP автоматически выделяет IP-адреса компьютерам, конфигурированным как клиенты DHCP (рис. 8.3).

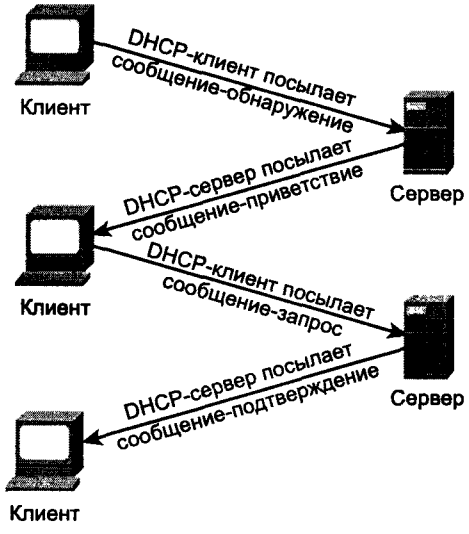


Рис. 8.3. Сервер DHCP выделяет адрес клиенту DHCP

Выделение IP-адреса сервером DHCP клиенту DHCP выполняется в несколько этапов.

1. Компьютер, у которого свойства TCP/IP конфигурированы на получение IP-адреса посредством DHCP, подключается к сети. При этом компьютер посылает в сеть (или подсеть) широковещательное сообщение, называемое *открытием DHCP*. (Широковещательные сообщения посылаются всем компьютерам с помощью специального широковещательного адреса.)
2. Если в сети присутствует сервер DHCP, то он получает широковещательное сообщение клиента и посылает в ответ сообщение, называемое *предложением DHCP*. В этом сообщении клиенту предлагается IP-адрес из хранящегося на сервере списка допустимых адресов. Предложенный адрес временно резервируется, пока сервер не получит ответ от клиента. Предложение DHCP также передается по широковещательному адресу, потому что не имеет своего IP-адреса, по которому можно было бы передать однонаправленное сообщение.

3. Если в сети есть несколько серверов DHCP, то клиент может получить несколько предложений. Когда поступает первое предложение, клиент посылает сообщение, называемое *запросом DHCP*. Это сообщение означает, что клиент одобрил первое полученное предложение. Запрос DHCP тоже является широковещательным сообщением, поэтому его получают все серверы DHCP. Те из них, чьи предложения DHCP не одобрены, узнают об этом из запроса DHCP и возвращают зарезервированные адреса обратно в список допустимых адресов.
4. Последний этап переговоров — *подтверждение DHCP* (или сообщение *ACK*, от *acknowledgment — подтверждение*). Сервер DHCP, предложение которого одобрено, получает посланный клиентом запрос DHCP. После этого сервер посылает клиенту подтверждение DHCP и присваивает ему IP-адрес, действительный в течение предопределенного периода времени — срока аренды адреса. Сервер может послать клиенту также дополнительную информацию по конфигурированию TCP/IP, например IP-адреса серверов DNS и WINS (рассматриваются далее в главе).

Когда эти этапы успешно завершены, клиент может использовать присвоенный ему IP-адрес для коммуникации с другими компьютерами в протоколе TCP/IP, пока не исчерпается срок аренды адреса. Обратите внимание: продолжительность срока аренды может быть установлена администратором на сервере DHCP.

Перед окончанием срока аренды клиент начинает переговоры об обновлении адреса, чтобы можно было продолжать использовать этот же адрес. Обычно сервер DHCP удовлетворяет этот запрос. Однако если сервер DHCP в этот момент отключен или посылает клиенту сообщение NACK (Negative Acknowledgment), то клиент должен начать процесс получения адреса сначала.

Замечание

Сервер DHCP может послать сообщение NACK, если, например, клиентский компьютер был перенесен в другую подсеть, в которой старый адрес недействителен.

По сравнению с ручным присвоением IP-адресов служба DHCP имеет существенные преимущества.

- Администратору не нужно тратить время на ручную конфигурацию свойств каждого компьютера.
- Работа сети становится более упорядоченной, потому что все необходимые адреса постоянно присвоены и администратору не нужно следить за тем, какие адреса заняты или свободны и не истекает ли у кого-нибудь из них срок аренды.

Услугами DHCP можно воспользоваться и в том случае, если компьютеры должны иметь один и тот же IP-адрес (часто это нужно для серверов). Такие компьютеры следует конфигурировать на использование *зарезервированного адреса*. Клиенту, заказавшему резервирование, сервер DHCP всегда присваивает один и тот же адрес. Резервирование осуществляется на основе MAC-адреса клиента (физического адреса).

Происхождение DHCP

Протокол DHCP создан на основе более раннего протокола Bootstrap Protocol (BOOTP). Протокол BOOTP был разработан для того, чтобы обеспечить возможность бездисковым рабочим станциям загрузиться, получить IP-адрес и подключить операционную систему к сети.

Протокол DHCP значительно совершеннее, чем BOOTP. С его помощью администратор может конфигурировать параметры TCP/IP и устанавливать сроки аренды адресов. В протоколе DHCP предусмотрено динамическое выделение адресов. Иногда серверы DHCP конфигурируют на поддержку клиентов BOOTP.

Протокол DHCP не ориентирован на определенную операционную систему. Его можно использовать с Windows, UNIX, NetWare и другими популярными операционными системами. Однако конкретные реализации поставщиков DHCP могут несколько отличаться друг от друга. Например, серверы DHCP для Windows 2000 интегрированы с Active Directory. Это позволяет администраторам предотвратить выделение IP-адресов несанкционированными (так называемыми шулерскими) серверами DHCP.

Процедура APIPA

Процедуры APIPA предоставляют еще один способ автоматического получения IP-адресов. Это средство включено в реализации TCP/IP последних операционных систем Microsoft, таких, как Windows 98 и Windows 2000.

Если компьютер, конфигурированный как клиент DHCP, при подключении к сети не может получить доступ к серверу DHCP, то традиционно он не может получить IP-адрес и сообщаться с сетью посредством TCP/IP. Для решения этой проблемы было создано средство APIPA.

Когда компьютер с установленной программой APIPA пытается получить адрес, но не может найти сервер DHCP, то он присваивает себе один из зарезервированных для этой цели адресов (набор номеров сети 169.254.0.0 класса B). Такой самоприсвоенный адрес можно использовать, пока не будет установлен контакт с сервером DHCP.

Создание подсетей и суперсетей

Создать в сети *подсеть* означает разделить ее на части. При создании подстети описанная выше двухуровневая иерархия адресов превращается в трехуровневую. Для создания подсети нужно "одолжить" часть битов IP-адреса, выделенных под адрес хоста, и записать в них второй уровень сетевого адреса, т.е. адрес подсети.

Маска подсети

Создание подсети предполагает заимствование битов одной части адреса для другой части адреса. Если создается подсеть, то процедуры протокола IP должны иметь возможность определить, какие биты идентифицируют сеть, а какие — номер хоста. Это делается с помощью *маски подсети* — 32-битового числа, введенного сетевым администратором при конфигурировании свойств TCP/IP. В маске подсети биты, определяющие номер сети, установлены в 1, а биты, определяющие номер хоста — в 0. Часть адреса, отведенная для номера сети, называется "замаскированной" битами, содержащими единицы.

По умолчанию в классе A для номера сети отведены биты первого октета, в классе B — биты двух первых октетов, а в классе C — биты трех первых октетов. В этом случае *маска подсети по умолчанию* выглядит как показано в табл. 8.4.

Таблица 8.4. Маски подсети по умолчанию

Класс адреса	Двоичная маска подсети	Десятичная маска подсети
Класс A	11111111.00000000 00000000.00000000	255.0.0.0
Класс B	11111111.11111111.00000000.00000000	255.255.0.0
Класс C	11111111.11111111.11111111.00000000	255 255.255.0

Маска подсети, приведенная в табл. 8.4, применима к сетям, *не имеющим подсетей*. Пока придерживаемся установок по умолчанию, все выглядит довольно просто.

Однако что получится, если разделить сеть на подсети? Допустим, сети присвоен адрес класса B, например 181.25.0.0. Как известно, сеть класса B может содержать до 65 535 хостов. Но в сети с таким огромным количеством компьютером управление широковещательными сообщениями станет невозможным.

Чтобы решить эту проблему, разделим сеть на шесть подсетей. Для этого придется позаимствовать несколько битов из адреса хоста для адреса подсети. Нужно также создать правильную маску подсети, с помощью которой процедуры IP смогут определить адрес подсети.

Вычисление маски подсети

Маска подсети, отличная от маски по умолчанию, называется маской *переменной длины* или *пользовательской* маской. Для вычисления маски подсети в нашем примере с шестью отдельными подсетями сначала нужно определить, сколько битов должно быть позаимствовано из числа битов, отведенных под номера хостов.

Двоичная система счисления имеет основание 2, поэтому максимальное количество создаваемых подсетей равно целой степени двойки. Мы должны найти, какая степень двойки (за вычетом 2, как будет сказано дальше) равна 6 или ближайшему большему числу.

Возведем двойку во вторую степень: $2^2 = 4$. Как видите, это меньше шести. Поэтому возведем двойку в следующую, третью степень: $2^3 = 8$. Теперь необходимо вычесть 2, чтобы удовлетворить старое правило, согласно которому номер сети не может состоять только из нулей или только из единиц. Вычтя 2, мы получили 6 оставшихся допустимых номеров сети. Следовательно, для номера сети нужно позаимствовать три бита из части адреса, отведенной под номера хостов. Для этого мы должны в маске подсети по умолчанию превратить три первых нуля в единицы. Теперь маска подсети выглядит следующим образом: 11111111.11111111.11100000.00000000. В десятичном формате она выглядит так: 255.255.224.0.

Сколько компьютеров можно разместить в каждой подсети? Посмотрим на оставшиеся нули в маске подсети. Осталось 13 нулей. Другими словами, в этих битах можно разместить $2^{13} = 8\ 192$ адресов. Однако номер хоста не может состоять из одних нулей или единиц, поэтому из полученного количества два номера недопустимы. Значит, в каждой из шести подсетей нашего примера можно разместить 8 190 компьютеров. (Как вы помните, запрет на номера, состоящие из одних нулей и единиц был снят только для номеров сети. Номера хостов по-прежнему подчиняются этому правилу.)

В табл. 8.5 приведено максимальное количество подсетей и хостов для каждой маски подсети.

Таблица 8.5. Допустимое количество подсетей и хостов

Десятичное значение первого изменяемого октета	Количество подсетей	Количество хостов класса A	Количество хостов класса B	Количество хостов класс C
.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

Окончание табл. 8.5

Десятичное значение первого изменяемого октета	Количество подсетей	Количество хостов класса A	Количество хостов класса B	Количество хостов класс C
252	62	262 142	1022	2
.254	126	131 070	510	—
.255	254	65 534	254	—

Использование логического И

Когда сообщение передается в сеть с помощью TCP/IP, процедуры протокола IP должны определить, расположены ли передающий и принимающий компьютеры в одной и той же подсети. Если да, то сообщение передается как широковещательное. Если нет, то сообщение передается по адресу *шлюза по умолчанию*, т.е. на интерфейс маршрутизатора (на выходе из сети функции шлюза выполняет маршрутизатор).

Для определения принадлежности передающего и принимающего компьютеров используется поразрядное применение логической операции И к IP-адресу и маске подсети каждого компьютера. Для каждого разряда операция И дает следующие результаты:

- 1 И 1 = 1;
- 1 И 0 = 0;
- 0 И 0 = 0.

Приведем пример. Допустим, передающий компьютер имеет IP-адрес 192.168.1.1 и маску подсети 255.255.255.0, а принимающий компьютер — IP-адрес 192.168.3.1 и маску подсети 255.255.255.0.

Сначала пересчитаем адрес и маску подсети передающего компьютера:

```
192.168.1.1     =  11000000.10101000.00000001.00000001
255.255.255.0   =  11111111.11111111.11111111.00000000
Результат       =  11000000.10101000.00000001.00000000
```

Затем выполним эти же вычисления для принимающего компьютера:

```
192.168.3.1     =  11000000.10101000.00000011.00000001
255.255.255.0   =  11111111.11111111.11111111.00000000
Результат       =  11000000.10101000.00000011.00000000
```

Результаты отличаются друг от друга, поэтому можно сделать вывод, что передающий и принимающий компьютеры находятся в разных подсетях. Следовательно, сообщение передается на маршрутизатор (шлюз по умолчанию) и направляется в нужную подсеть.

Если эти результаты совпадут, то принимающий компьютер находится в этой же подсети и сообщение будет передано с использованием широковещательного протокола ARP, который рассматривается далее в главе.

Преимущества создания подсетей

Разделение больших сетей на две или более подсетей предоставляет ряд преимуществ.

- Уменьшается загрузка сети. Подсети соединены друг с другом с помощью маршрутизаторов, которые по умолчанию не пропускают широковещательные сообщения. Это приводит к существенной экономии пропускной способности сетевых каналов.

- Компьютеры, расположенные в разных местах, организуются в подсети, поэтому ими легче управлять.
- Повышается безопасность, поскольку различные части сети изолируются друг от друга и передаваемые между ними сообщения можно фильтровать.
- Более эффективно используются выделенные адреса, так как уменьшается количество утраченных адресов.

Создание подсетей IP может составить предмет целой книги. Это сложная тема, большая часть которой выходит за рамки нашего обсуждения. В конце главы приведено несколько хороших учебников по созданию подсетей. А в этом разделе представлен неплохой базовый обзор основных понятий и принципов создания подсетей.

Протоколы транспортного уровня: TCP и UDP

Как отмечалось в главе 3, "Концепции, модели и стандарты компьютерных сетей", транспортный уровень отвечает за обеспечение надежной коммуникации одного компьютера с другим. Эта задача реализуется такими механизмами, как, например, подтверждение получения данных принимающим компьютером без потерь или повреждений.

Протоколы транспортного уровня предназначены также для идентификации сообщений, прибывающих на один и тот же компьютер. Различные приложения, установленные на одном компьютере, могут передавать и принимать сообщения одновременно. Чтобы разделять эти сообщения, в протоколах транспортного уровня используются *порты*. Подробнее порты и связанное с ними понятие *сокетов* рассматриваются несколько ниже.

Пакет TCP/IP содержит не один, а два протокола транспортного уровня.

- **TCP (Transmission Control Protocol — протокол управления передачей)**. Протокол, ориентированный на установку соединения.
- **UDP (User Datagram Protocol — протокол пользовательских дейтаграмм)**. Протокол, *не* ориентированный на установку соединения.

Какой из этих двух протоколов используется для передачи конкретного сообщения? Это зависит от назначения и характера передаваемых данных. Протокол TCP используется, когда более важна надежность передачи данных, а UDP — когда более важной характеристикой является производительность (скорость) коммуникации. Далее рассматриваются характеристики и функции каждого из этих протоколов.

Протокол транспортного уровня TCP

Прежде чем начать передавать данные, TCP устанавливает между двумя сообщающимися компьютерами сеанс соединения. Для этого используются сообщения уведомления и ответа. Затем выполняются процедуры обнаружения и исправления ошибок и данные разбиваются на пакеты.

В каждый пакет добавляется информация о нумерации пакетов, чтобы на принимающем конце их можно было собрать в правильной последовательности. Нумерация пакетов позволяет принимающему компьютеру обнаружить недостающие пакеты. Благодаря этим процедурам протокол TCP надежнее, чем UDP, однако выполнение дополнительных операций существенно снижает производительность.

Протокол транспортного уровня UDP

Протокол UDP не ориентирован на установление соединения. Не выполняется также нумерация пакетов данных, поэтому он более пригоден для передачи небольших сообщений, которые можно разместить в одном пакете. Протокол UDP не отслеживает также, что было передано и что получено. Однако в UDP выполняется проверка контрольной суммы, чем гарантируется правильность данных, поступивших на принимающий компьютер. Как и в TCP, в UDP, чтобы различить сообщения для или от разных приложений одного и того же компьютера, используются номера портов.

Протокол UDP не занимается нумерацией пакетов или обнаружением ошибок, поэтому его производительность высокая. Заголовок пакета UDP проще заголовка TCP. Протокол UDP используется в протоколах RIP (Routing Information Protocol), TFTP (Trivial File Transfer Protocol) и др.

Замечание

Что такое дейтаграмма? Спецификация RFC 1594 определяет этот термин как "самодостаточный независимый модуль данных, содержащий информацию, достаточную для маршрутизации этих данных от передающего к принимающему компьютеру без предварительного или текущего обмена между передающим и принимающим компьютерами и сетью".

В некоторых случаях термины "дейтаграмма" и "пакет" взаимозаменяемы. Пакет представляет собой модуль данных, являющийся частью группы нумерованных модулей, на которые разбито сообщение. Пакеты могут проходить по сети к адресату различными маршрутами. В принимающем компьютере сообщение собирается из поступивших пакетов. В то же время термин "дейтаграмма" означает более простые, ненумерованные модули данных, передаваемые с помощью UDP.

Порты и сокеты

Для идентификации передающего и принимающего компьютеров в TCP/IP используются логические адреса, состоящие из двух частей, т.е. IP-адреса. Но что получается, если два сетевых приложения, выполняющихся на одном компьютере, посылают или принимают сообщения одновременно? Например, если одно поступающее сообщение предназначено для программы электронной почты, а другое — для Web-броузера? Протоколы должны различать эти сообщения. Для этого используются порты TCP и UDP.

Номера портов

Как вы помните, IP-адрес принимающего компьютера состоит из двух частей: адреса сети (аналогичного названию улицы) и адреса хоста (аналогичного номеру дома). Номера портов можно представить себе как специфическую маршрутную информацию внутри адреса. Это своего рода дополнение к IP-адресу, как имя и фамилия получателя письма является дополнением к названию улицы и номеру дома. А разные приложения можно представить себе как разных людей, живущих в одном доме.

Порт — это *точка логического соединения*. В транспортных протоколах TCP и UDP порты используются для идентификации конкретного приложения, передающего или принимающего сообщение.

Наиболее распространенные приложения Internet используют предопределенные номера портов. Стандартизация облегчает процесс коммуникации. В табл. 8.6 приве-

ден список предопределенных номеров портов, используемых наиболее распространенными приложениями

Таблица 8.6. Предопределенные порты TCP и UDP

Предопределенный 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	Служба имен NetBIOS
161	TCP/UDP	SNMP
194	TCP/UDP	IRC
389	TCP/UDP	LDAP
396	TCP/UDP	NetWare в IP
458	TCP/UDP	QuickTime компании Apple
500	TCP/UDP	ISAKMP

Существует 65 536 допустимых номеров портов Порты от 0 до 1 024 зарезервированы для предопределенных служб, подобных приведенным в табл 8 6

Понятие сокета

Теперь, когда вы знакомы с портами, рассмотрим концепцию сокетов Сокет определяется как "конечная точка соединения" Чтобы коммуникация состоялась, должен быть создан сокет

Разные типы сокетов используют разные методы адресации Наибольшее распространение получила идентификация сокета по IP-адресу и номеру порта В терминологии UNIX это называется адресацией AF_INET В другом методе адресации — AF_UNIX — для идентификации сокетов используются пути

В TCP/IP стандартным интерфейсом являются сокеты BSD (Berkeley Sockets) Распространенный вариант сокетных интерфейсов — *Windows Sockets*, или *Winsock* Реализация Winsock предоставляет программный интерфейс для приложений Internet, выполняющихся в операционных системах Windows Программа Winsock загружается как динамически подключаемая библиотека DLL

Заголовок пакета: адрес на конверте

Сейчас вы уже знаете, что для передачи сообщения принимающему компьютеру протоколы TCP/IP используют адресную информацию Но где протоколы находят ее? На конверте письма, посылаемого по почте, должны быть написаны адреса отправителя и получателя, причем адрес должен быть написан *снаружи* конверта Точно так же сообщение, передаваемое с помощью TCP/IP, должно быть внутри "конверта", а адрес — снаружи

Когда сообщение помещается в пакет, к нему "снаружи" добавляется заголовок, содержащий адреса передающего и принимающего компьютеров Заголовки могут содержать также другую информацию и специальные инструкции, подобно тому как на конверте с письмом иногда пишут "Обращаться бережно" или "Заказное"

По умолчанию длина заголовка IP равна 20 байт. В состав заголовка входят поля, задающие ряд параметров. (Более подробное описание полей приведено на рис. 8.4.)

- Тип службы.
- Общая длина дейтаграммы.
- Уникальный идентификатор дейтаграммы.
- Флаги и смещения фрагментов, необходимые для сборки.
- Время жизни (Time to Live — TTL) — максимальное количество маршрутизаторов, через которые может пройти дейтаграмма.
- Протокол расположенного выше уровня, который должен принять данные (ICMP, TCP, UDP, IGRP или OSPF).
- Контрольная сумма для обнаружения ошибок.
- IP-адрес передающего компьютера.
- IP-адрес принимающего компьютера.

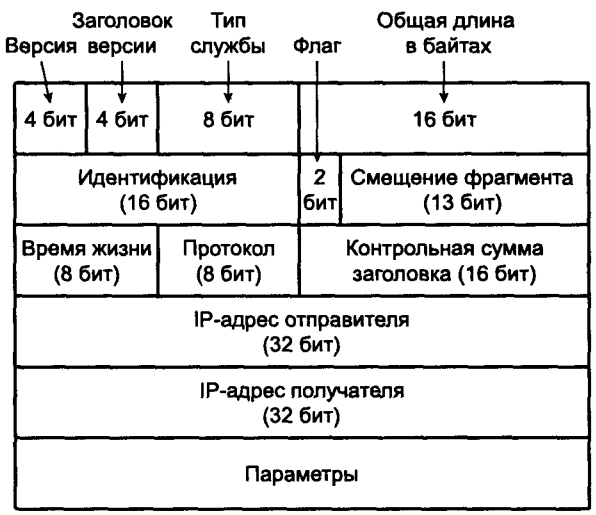


Рис 8 4. Заголовок IP состоит из 12 полей и параметров

В состав заголовка могут входить также некоторые параметры, такие, как ограничения безопасности, временная отметка и ограничения маршрутов. Заголовок *без параметров* имеет длину 20 байт.

Разрешение имен

Мы рассмотрели, как IP-адреса и номера портов используются в TCP/IP для идентификации сети, компьютеров и конкретных сетевых приложений, передающих или принимающих сообщения. Однако многие предпочитают использовать для идентификации не номера, а имена. Ведь мы значительно легче запоминаем имена и фамилии наших знакомых, чем номера их телефонов!

Однако, несмотря на то что имена нравятся нам больше, чем номера, компьютеры все же могут работать только с числами. Из-за этой несовместимости нужны

специальные службы, преобразующие имена в IP-адреса. С помощью таких служб можно, обращаясь, например, к Web-узлу компании Xerox, вводить в поле адреса броузера **www.xerox.com**, а не **208.134.240.50**. Адрес, состоящий из имен, значительно легче запомнить. Чтобы найти в Internet нужный Web-сервер и получить запрошенную страницу, броузер автоматически преобразует имя хоста в IP-адрес.

Что такое имя

В процессах сетевой коммуникации используются различные типы имен. В Internet имена хостов (компьютеров) организованы в иерархическую структуру внутри *доменов*. В США наиболее распространены следующие домены верхнего уровня:

- **com** — первоначально предназначался для коммерческих организаций;
- **net** — первоначально предназначался для сетей провайдеров услуг Internet;
- **org** — первоначально предназначался для бесприбыльных организаций;
- **edu** — для учебных организаций;
- **gov** — для правительственных организаций;
- **mil** — для военных организаций;
- **int** — для международных организаций.

За пределами США для идентификации доменов используются следующие коды стран:

- **uk** — Великобритания;
- **au** — Австралия;
- **ca** — Канада;
- **ru** — Россия;
- **ua** — Украина.

Коммерческие и некоммерческие организации, другие учреждения, а также отдельные лица регистрируют *имена доменов второго уровня* внутри доменов верхнего уровня (например, `ibm.com`, `whitehouse.gov` или `dallas.net`). Одно время присвоением имен доменов второго уровня занималась организация InterNIC, однако сейчас эта задача делегирована нескольким уполномоченным регистраторам имен.

Внутри домена второго уровня индивидуальные компьютеры идентифицируются именем хоста, именем домена второго уровня и именем домена верхнего уровня. В полном имени эти имена отделяются друг от друга точками. Таким образом, Web-сервер с именем `www` в домене `dallas.net` идентифицируется как `www.dallas.net`. Такое иерархическое имя с точками называется полностью определенным именем домена (Fully Qualified Domain Name — FQDN).

В сетях Microsoft каждому компьютеру присваивается также имя NetBIOS. Это 16-символьное имя, присвоенное администратором, используется для идентификации ресурсов локальной сети.

Чтобы коммуникация в протоколе TCP/IP стала возможной, имена обоих этих типов должны быть преобразованы в IP-адреса.

Преобразование имен в числа

Для преобразования имен в IP-адреса можно воспользоваться одним из следующих средств:

- файлы HOSTS и LMHOSTS;
- службы DNS или DDNS;
- серверы WINS.

В следующих разделах рассматриваются все три метода.

Файлы HOSTS и LMHOSTS

В первое время после появления Internet для сопоставления имен хостов (компьютеров) с IP-адресами с целью коммуникации в протоколе TCP/IP использовался файл HOSTS. Это текстовый файл, расположенный на локальном жестком диске. В нем содержится список всех имен хостов и соответствующих IP-адресов. В листинге 8.1 приведен пример файла HOSTS.

Листинг 8.1. Локальный файл HOSTS отображает IP-адреса на имена хостов

```
102.54.94.97   rhino.acme.com   # source server
38.25.63.10    x.acme.com       # x client host
127.0.0.1      localhost
```

Замечание

Символ # в файле HOSTS обозначает начало комментария. Любая информация после этого символа компьютером игнорируется.

Файлы HOSTS были удовлетворительным решением проблемы, пока количество компьютеров в Internet было небольшим. Их легко создавать. Модифицировать их можно в любом текстовом редакторе, например Windows Notepad либо Emacs в UNIX или Linux Когда пользователь запрашивал другой компьютер по имени хоста, операционная система находила в файле HOSTS соответствующий IP-адрес.

Однако при добавлении в сеть новых хостов файл HOSTS нужно было вручную модифицировать и копировать на все компьютеры сети. По мере роста Internet эта задача усложнялась.

В сетях Microsoft аналогичные функции выполняет файл LMHOSTS. Однако он отображает IP-адреса не на имена компьютеров, а на имена NetBIOS. Файл LMHOSTS страдает теми же недостатками, что и HOSTS: его нужно обновлять вручную. В листинге 8.2 приведен пример типичного файла LMHOSTS.

Листинг 8.2. Файл LMHOSTS отображает IP-адреса на имена NetBIOS

```
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
```

По мере роста Internet потребность в лучшем способе отображения имен на IP-адреса становилась все более острой.

Службы DNS и DDNS

Служба имен доменов (Domain Name System — DNS) разработана с целью устранения недостатков файлов HOSTS. На серверах DNS хранятся базы данных, в которых IP-адреса отображаются на имена хостов, а свойства TCP/IP клиентских компьютеров конфигурируются с адресом сервера DNS.

В системе Internet существует иерархия серверов DNS. Различные серверы поддерживают информацию DNS для своих зон, или областей ответственности. Если на сервере DNS нет запрошенного клиентским компьютером IP-адреса или имени хоста, он передает запрос на другой сервер DNS, пока запрошенная информация не будет найдена.

Для коммуникации в Internet служба DNS не является абсолютно необходимой, однако без нее вместо имен хостов пришлось бы использовать IP-адреса. Например, если в свойствах TCP/IP клиентского компьютера не сконфигурирован адрес сервера DNS, то обратиться к Web-узлу можно, набрав IP-адрес в поле ввода URL, однако если в поле URL ввести имя хоста, то броузер не отобразит запрошенную страницу. Адрес сервера DNS можно ввести вручную или получить от сервера DHCP (если компьютер конфигурирован как клиент DHCP).

По сравнению с локальными файлами HOSTS служба DNS обладает существенными преимуществами. База данных хранится на центральном сервере, поэтому обновлять ее нужно только в одном месте, а не на всех клиентских компьютерах. Однако база данных на сервере по-прежнему должна обновляться вручную. Эту проблему решает применение *динамической DNS* (*DDNS*), в которой базы данных DNS обновляются автоматически. С помощью этой расширенной версии DNS клиентские компьютеры могут регистрировать и обновлять на сервере DNS свои записи с информацией о ресурсах в момент внесения в них изменений.

Серверы DNS под управлением Windows 2000 и версия 8 службы BIND (Berkley Internet Name Domain) поддерживают расширение DDNS. Стандарты DDNS специфицируются документом RFC 2136.

Таблица базы данных DNS

В таблице базы данных DNS используются различные типы записей. Чаще всего используются следующие записи.

- **Записи адресов (A)**. Отображение имен хостов на IP-адреса.
- **Записи обмена почтовыми сообщениями (MX)**. Указатели на сервер обмена корреспонденцией для каждого хоста.
- **Записи канонических имен (CNAME)**. Отображение *псевдонимов* (дополнительных имен) на хосты.

Записи всех этих типов (и других, предусмотренных в специальных целях) хранятся в одной таблице DNS.

Серверы WINS

Еще один метод отображения имен хостов на IP-адреса состоит в применении серверов WINS. В базе данных на сервере WINS хранятся имена NetBIOS, используемые для идентификации компьютеров и служб в сетях Microsoft. Серверы Windows NT и Windows 2000 могут работать как серверы WINS.

В отличие от FQDN (имен хостов в DNS), имена NetBIOS не иерархические, а однородные. Если некоторый сервер имеет имя FQDN, например, `exeter.tacteam.net`, то

его имя NetBIOS можно записать просто как `Exeter`. Протокол TCP не понимает имена NetBIOS, для коммуникации с серверами ему нужны IP-адреса. Как и статический файл HOSTS, сервер WINS преобразует имя в IP-адрес.

В отличие от первоначального DNS, в сервере WINS применяется автоматическое обновление базы данных. Когда клиент WINS подключается к сети, он объявляет об этом серверу WINS и передает ему свое имя и IP-адрес. На основе этой информации сервер WINS поддерживает свою базу данных.

В одной и той же сети службы DHCP, DNS и WINS могут работать совместно и одновременно. В новых операционных системах, например в Windows 2000, эти три службы объединены и эффективно взаимодействуют.

Обзор методов разрешения имен

Различные методы разрешения имен не так уж сложно перепутать. Чтобы этого не случилось, в табл. 8.7 приведена краткая сводка характеристик этих методов.

Таблица 8.7. Методы разрешения имен

Метод разрешения имен	Типы отображаемых имен	Характеристики
Файл HOSTS	Имена хостов на IP-адреса	Текстовый файл: нуждается в ручном обновлении на каждом компьютере
Файл LMHOSTS	Имена NetBIOS на IP-адреса	Текстовый файл: нуждается в ручном обновлении на каждом компьютере
DNS	Имена хостов на IP-адреса	Централизованная база данных, управляемая сервером DNS; нуждается в ручном обновлении
DDNS	Имена хостов на IP-адреса	Централизованная база данных, управляемая сервером DNS; обновляется динамически
WINS	Имена NetBIOS на IP-адреса	Централизованная база данных, управляемая сервером WINS; обновляется динамически

Утилиты TCP/IP

Пакет TCP/IP представляет собой довольно сложный набор протоколов. Большинство поставщиков включают в пакет различные утилиты, предназначенные для просмотра параметров конфигурации TCP/IP и устранения неполадок. В следующих разделах рассматриваются наиболее распространенные утилиты TCP/IP:

- `ping`;
- `ARP` и `RARP`;
- `netstat` и `tpcon`;
- `nbstat`;
- утилиты конфигурирования IP: `ipconfig`, `winipcfg`, `config` и `ifconfig`;
- утилиты отслеживания маршрута: `traceroute`, `tracert` и `iptrace`.

Замечание

Разные поставщики могут давать разные имена утилитам, выполняющим одни и те же функции.

Утилита ping

Эта простая и очень полезная утилита, запускаемая в командной строке, включена в большинство реализаций TCP/IP. Утилита `ping` используется для проверки соединения IP. Ее можно запускать как с именем хоста, так и с IP-адресом.

Утилита `ping` посылает на принимающий компьютер эхо-запрос ICMP (Internet Control Message Protocol). Получив его, принимающий компьютер передает обратно эхо-ответ ICMP.

С помощью утилиты `ping` можно найти IP-адрес хоста по его имени. Если в командной строке ввести **ping apple.com** (листинг 8.3), то на экран будет выведен IP-адрес хоста, возвратившего ответ.

Листинг 8.3. Ответ, возвращенный утилите `ping` хостом `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
```

Другая утилита — `nslookup` — возвращает IP-адрес хоста с заданным именем по указанному IP-адресу.

Компания Novell поставляет утилиту `ping` в виде программы NLM (NetWare Loadable Module). В операционных системах Windows и UNIX/Linux утилита `ping` запускается из командной строки. Утилита `ping` поставляется также другими компаниями, причем некоторыми из них — с графическим интерфейсом.

Утилиты ARP и RARP

ARP (Address Resolution Protocol) может обозначать как протокол, так и утилиту, запускаемую из командной строки в целях просмотра и модификации кэша ARP. Чтобы правильно применять утилиту `ARP`, нужно понимать принцип работы протокола.

Протокол ARP

С помощью протокола ARP сетевые компьютеры отображают логические IP-адреса на физические MAC-адреса. В ARP создается и поддерживается таблица, называемая *кэшем ARP*, в которой хранятся адреса. С помощью протокола RARP компьютер, которому неизвестен его IP-адрес, может получить нужную информацию по MAC-адресу.

Утилита ARP

Утилита командной строки `ARP` поставляется в составе пакетов TCP/IP в операционных системах Windows и UNIX/Linux. С ее помощью в протоколе ARP можно просматривать и модифицировать отображение IP-адресов на MAC-адреса. Компания

Novell поставляет эту утилиту в виде модуля NLM под именем tpcon. С помощью утилиты ARP можно вывести на экран содержимое кэша ARP, а также добавить или удалить отдельные строки соответствия, как показано в листинге 8.4.

Листинг 8.4. Команда arp используется для просмотра кэша ARP

```
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 командой arp можно использовать три параметра.

- arp –a. Вывод кэша на экран.
- arp –s. Добавление постоянной строки соответствия IP-адреса MAC-адресу.
- arp –d. Удаление строки соответствия.

Утилиты netstat и tpcon

С помощью этих утилит можно получить статистику сети. Команда netstat используется в Windows и UNIX/Linux для вывода протокольной информации о соединении TCP/IP. Компания Novell для выполнения этой же задачи поставляет модуль NLM под именем tpcon.

Команда netstat выводит на экран список активных в данный момент соединений (листинг 8.5).

Листинг 8.5. Команда netstat используется для просмотра информации о соединениях

```
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 листинге 8.5 приведен протокол, имя локального компьютера и номер порта, используемые каждым соединением, внешний адрес (имя удаленного компьютера) и текущее состояние соединения.

В табл. 8.8 приведены параметры, которые можно использовать с командой netstat.

Таблица 8.8. Параметры команды netstat

Параметр	Назначение
-a	Просмотр всех соединений и активных портов
-e	Просмотр статистики Ethernet
-n	Просмотр адресов и портов

Окончание табл. 8 8

Параметр	Назначение
`-p` (используется в Windows)	Вывод информации о выбранном протоколе
`-t, -u, -w, -x` (используются в Linux)	Вывод информации о протоколах TCP, UDP, RAW и о сокетах
`-r`	Просмотр таблицы маршрутизации
`-s`	Обзорная статистика по каждому протоколу

Статистика, выведенная утилитой `netstat`, используется при устранении неполадок в соединении TCP/IP. В листинге 8.6 показано, какая информация выводится при активизации параметра `s`. Этот отчет об ошибках особенно полезен при диагностике проблем с оборудованием и маршрутизацией.

Листинг 8.6. Статистика TCP/IP, отображаемая с помощью команды `netstat -s`

```
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
Adress 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
```

Утилита nbtstat

Стек протоколов TCP/IP компании Microsoft, включенный в операционную систему Windows, содержит утилиту `nbtstat`, с помощью которой можно вывести на экран информацию NetBIOS. В листинге 8.7 приведены синтаксис и параметры утилиты `nbtstat`.

Листинг 8.7. Если в командной строке ввести `nbtstat`, то на экран будут выведены синтаксис и список параметров этой утилиты

```
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.
```

Утилиты ipconfig, winipcfg, config и ifconfig

В зависимости от используемой операционной системы, конфигурационную информацию TCP/IP можно вывести на экран с помощью одной из этих утилит:

- `ipconfig` — Windows NT и Windows 2000 (командная строка);
- `winipcfg` — Windows 95/98 (графический интерфейс);
- `ifconfig` — UNIX/Linux (командная строка);
- `config` — NetWare (серверная консоль).

Эти утилиты возвращают довольно много информации, включая текущий IP-адрес, MAC-адрес, маску подсети, шлюз по умолчанию, адреса серверов DNS и WINS, информацию DHCP и доступные серверы. В зависимости от поставщика и типа утилиты, в них используются различные параметры. В листинге 8.8 показан результат выполнения команды `ipconfig /all` в Windows 2000.

Листинг 8.8. Конфигурационная информация, отображаемая в результате выполнения команды `ipconfig /all` в системе 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
```

Утилиты tracert, Iptrace и traceroute

Эти утилиты часто используются для отслеживания маршрута, по которому пакеты проходят от передающего компьютера к принимающему. В стек TCP/IP входит утили-

та отслеживания маршрута, с помощью которой можно определить, через какие маршрутизаторы прошло сообщение. В разных операционных системах эта утилита называется по-разному:

- `tracert` (Windows);
- `lptrace` (загрузочный модуль NLM в NetWare);
- `traceout` (UNIX/Linux).

Команда `tracert` имеет следующий синтаксис:

```
tracert имя_адресата
```

Результат, возвращаемый командой `tracert`, приведен в листинге 8.9.

Листинг 8.9. Команда `tracert` отслеживает маршрут пакета

```
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  32 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.
```

Как видно из листинга, результат отслеживания содержит имена и IP-адреса компьютеров, или маршрутизаторов, через которые прошел пакет.

Обзор утилит TCP/IP

Пакет протоколов TCP/IP большой и сложный. В большинство его реализаций включено довольно много утилит, с помощью которых можно получать информацию, позволяющую устранять неполадки. В табл. 8.9 приведен обзор наиболее распространенных утилит.

Таблица 8.9. Утилиты TCP/IP

Утилита	Назначение
ARP/RARP	Просмотр строк соответствия IP- и MAC-адресов разрешаемых протоколом ARP, удаление строк из кэша ARP и добавление постоянных строк соответствия IP- и MAC-адресов
netstat (Windows, UNIX) tpcon (NetWare)	Просмотр статистики сетевых соединений и протоколов
nbtstat (Windows)	Просмотр соединений и статистика NetBIOS в TCP/IP (NetBT)
ipconfig (Windows NT/2000) winipcfg (Windows 95/98) config (NetWare), ifconfig (UNIX)	Просмотр конфигурационной информации TCP/IP, такой, как IP-адрес, маска подсети шлюз по умолчанию, MAC-адрес доступные службы и т д
tracert (Windows) iptrace (NetWare), traceout (UNIX)	Отслеживание маршрута пакета, определение маршрутизаторов, через которые прошел пакет
ping	Определение возможности установки соединения между двумя компьютерами

Протоколы прикладного уровня

Пакет TCP/IP содержит много протоколов прикладного уровня, предоставляющих такие услуги, как эмуляция терминала, копирование файлов и доступ к содержимому Word Wide Web Большинство реализаций содержат приложения, в которых используются следующие протоколы

- HTTP (Hypertext Transfer Protocol — протокол передачи гипертекста),
- SMTP (Simple Mail Transfer Protocol — простой протокол передачи почты),
- NNTP (Network News Transfer Protocol — протокол передачи сетевых новостей),
- FTP (File Transfer Protocol — протокол передачи файлов),
- Telnet

Протоколы прикладного уровня Internet и их программы подробно рассматриваются в главе 9, "Самая глобальная сеть — Internet"

Резюме

Для обеспечения коммуникации в локальных и глобальных сетях, кроме протоколов сетевого, транспортного и более высоких уровней, используется довольно много других протоколов, необходимых для установки и поддержания соединения В этой главе описаны три наиболее распространенных стека протоколов сетевого и транспортного уровней NetBEUI, IPX/SPX и TCP/IP

Компьютеры сообщаются друг с другом посредством двоичных чисел, однако люди предпочитают работать с удобоваримыми именами хостов и ресурсов В этой главе рассмотрены методы преобразования таких имен в двоичные IP-адреса, с которыми работают сетевые устройства

Основное внимание было сосредоточено на TCP/IP, потому что это протокол не только глобальной сети Internet, но и все большего количества локальных сетей Был рассмотрен стек протоколов, составляющих пакет TCP/IP

В этой главе обсуждались базовые понятия IP-адресации, традиционные классы IP-адресов и метод CIDR, в котором маршрутизация выполняется на основе бесклассового метода адресации. Рассмотрены две составные части IP-адреса, порты TCP и UDP, с помощью которых сообщения находят нужные приложения, создание подсетей IP и служба DHCP, автоматически присваивающая IP-адреса компьютерам, конфигурированным как клиенты DHCP.

Используемые в компьютерных сетях протоколы очень сложны. В этой главе приведен лишь их ограниченный обзор. Тема протоколов глубоко излагается в многочисленных книгах, на Web-узлах и в учебных курсах по Internet.

Теперь вы имеете базовые представления о работе сетевых протоколов. Это позволит нам приступить в следующей главе к рассмотрению самой большой и сложной компьютерной сети — Internet.

Рекомендуемые источники

Обзор протокола IPv6 — нового поколения протоколов Internet — приведен по адресу: `playground.sun.com/pub/ipng/html.ipng-main.html`.

Прекрасный источник информации по широковещанию и широковещательным магистралям можно найти по адресу: `www.savetz.com/mbone/ch3.html`.

Компания 3Com предоставляет хороший базовый обзор принципов IP-адресации, включая создание подсетей, по адресу: `www.3com.com/nsc/501302.html`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Какой из приведенных протоколов является немаршрутизируемым протоколом сетевого и транспортного уровней, который легко и просто конфигурировать?
   - **а.** NWLink.
   - **б.** NetBIOS.
   - **в.** NetBEUI.
   - **г.** IPX/SPX.
2. Какая часть адреса IPX основана на MAC-адресе устройства?
   - **а.** Номер узла.
   - **б.** Номер сети.
   - **в.** Номер подсети.
   - **г.** Номер хоста.
3. Какие из приведенных протоколов ориентированы на установку соединения? (Выбрать все подходящие.)
   - **а.** TCP
   - **б.** UDP.
   - **в.** IP.

г. IPX.

д. SPX.

4. Какое утверждение об IP-адресах справедливо? (Выбрать все подходящие.)

   а. IP-адрес состоит из двух октетов.

   б. Октет в IP-адресе состоит из восьми битов.

   в. IP-адрес представляет собой 32-разрядное двоичное число.

   г. IP-адреса обычно записываются в шестнадцатеричном формате.

5. Чему равно максимальное количество компьютеров в сети класса B?

   а. 16 384.

   б. 254.

   в. 65 535.

   г. 2 097 152.

   д. Более 16 миллионов.

6. Что из приведенного является маской подсети по умолчанию для сети класса C?

   а. 255.255.255.255.

   б. 255.255.255.0.

   в. 255.255.0.0.

   г. 255.0.0.0.

7. Адресу какого класса в методе классовой адресации принадлежит IP-адрес 190.23.201.6?

   а. Класс A.

   б. Класс B.

   в. Класс C.

   г. Класс D.

8. В каком методе маршрутизации применяется бесклассовая адресация?

   а. CIR.

   б. CD-R.

   в. CIDR.

   г. RIP.

9. Для чего предназначена служба DHCP?

   а. Для отображения имен NetBIOS на IP-адреса.

   б. Для преобразования частных IP-адресов в общедоступные адреса.

   в. Для отображения IP-адресов на MAC-адреса.

   г. Для автоматического присвоения IP-адресов клиентским компьютерам.

10. С помощью какой утилиты можно просматривать кэш IP-адресов, отображенных на MAC-адреса?

    а. ipconfig.

    б. iptrace.

    в. ARP.

    г. nbtstat.

Глава 9

Самая глобальная сеть — Internet

В главе 8, "Сетевые протоколы и службы", были рассмотрены протоколы, работающие как в небольших локальных, так и в глобальных сетях. Вы узнали, что стек протоколов TCP/IP служит основой коммуникации в самой большой и наиболее сложной из всех сетей — глобальной сети Internet.

В этой главе рассматриваются этапы развития Internet, наиболее популярные приложения Internet: World Wide Web, электронная почта, группы новостей, передача файлов, а также самые современные технологии коммуникации: телеконференции в реальном времени и воспроизведение звука и видео.

Затем обсуждаются методы маршрутизации пакетов в Internet, базовые понятия маршрутизации, статическая и динамическая маршрутизация и наиболее распространенные способы выбора маршрута. В конце главы представлены многочисленные организации, обеспечивающие правильное и эффективное функционирование Internet.

Развитие Internet

По определению *internet* — это сеть, состоящая из сетей. Internet состоит из тысяч больших и малых сетей, которые, в свою очередь, тоже разбросаны по всему миру. Как упоминалось в главе 1, "Введение в компьютерные сети", Internet появилась в 1960 году как сеть ARPAnet — совместный проект Министерства обороны США и наиболее крупных университетов.

В первые годы развития ARPAnet, пришедшиеся на пик холодной войны, доступ к сети имел лишь ограниченный элитный персонал правительственных учреждений и университетов. Главной целью военной части проекта была разработка сети, способной продолжить нормальное функционирование после разрушительных ядерных ударов по территории США. В то же время университеты были заинтересованы в создании сети, предоставляющей возможность исследователям легко и быстро получать информацию из удаленных источников.

Разработка магистрали

Национальный научный фонд США (National Science Foundation — NSF) начал разрабатывать магистраль Internet в середине 80-х годов и продолжает оказывать некоторые услуги Internet на территории США до настоящего времени. По мере роста Internet до размеров всемирной сети другие организации также разрабатывали различные средства Internet. В 1995 году финансирование магистрали было распределено по региональным сетям. В период с 1986-го по 1995-й год NSF потратила на разработку главной магистрали около 200 млн долларов.

Замечание

Магистраль Internet — это группа каналов связи, по которым сообщаются локальные сети, расположенные на больших расстояниях. Магистраль Internet содержит точки соединения, называемые *узлами*.

Как показано на рис. 9.1, в инфраструктуре Internet используется гибридная ячеистая топология. Благодаря избыточности такой топологии при выходе из строя одной из связей пакеты могут проходить в пункт назначения альтернативными маршрутами.

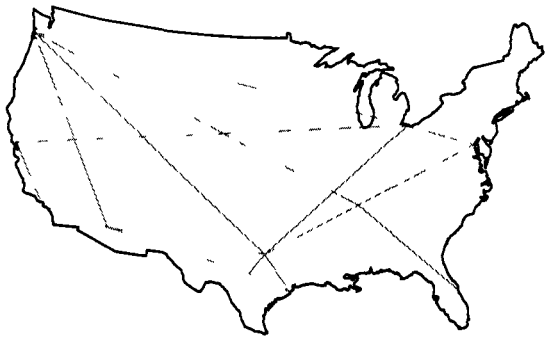


Рис. 9 1. Магистраль Internet выполнена в гибридной ячеистой топологии

В настоящее время инфраструктура Internet на территории США состоит из коммерческой магистрали и высокоскоростной службы vBNS (Very High-speed Backbone Network Service).

Коммерческая магистраль

Это комплекс коммерческих сетей таких крупных компаний, как AT&T, Sprint, UUNET (подразделение WorldComp), BBN Planet и Cable & Wireless USA. К этим коммерческим сетям подключены провайдеры услуг Internet.

Между магистральными провайдерами (другое название — главные провайдеры Internet) и провайдерами услуг Internet (чаще называются просто провайдерами) заключены *равноправные соглашения*, согласно которым они обслуживают информационные потоки друг друга. Эти соглашения обусловливают их взаимосвязь и обмен данными.

Большинство физических кабелей на территории США принадлежит компаниям RBOC (Regional Bell Operating Company), которые сдают их в аренду провайдерам. Сети провайдеров подключены к линиям T-1, T-3 или OC-3.

Служба vBNS и суперкомпьютерные центры

Служба vBNS используется в научно-исследовательских целях. Она соединяет пять "суперкомпьютерных" центров.

- NCSA (National Center for Supercomputing Applications), Урбана, шт. Иллинойс.
- NPACI (National Partnership for an Advanced Computational Infrastructure), Сан-Диего, шт. Калифорния.
- Cornell Theory Center, Итака, шт. Нью-Йорк.
- National Center for Atmospheric Research, Боулдер, шт. Колорадо.
- Pittsburgh Supercomputing Center, Питсбург, шт. Пенсильвания.

Служба vBNS финансируется организацией NSF по контрактам с MCI Основой службы vBNS являются линии OC-3 с пропускной способностью 155 Мбит/с и выше. Сеть vBNS соединена с точками доступа в сеть (Network Access Points — NAP), принадлежащими государству. Точки доступа NAP рассматриваются дальше в этой главе. Они используются также коммерческими магистралями.

Проект Internet2

Служба vBNS является частью совместного проекта американских университетов и правительства Internet2. Его цель — разработка высокоскоростной магистрали, которую можно использовать как полигон для проверки новых технологий. Например, в Internet2 испытываются новый протокол IPv6 и процедуры тестирования параметров QoS.

Internet2 не является отдельной физической сетью и не предназначена для замены "старой" Internet. Это консорциум организаций, собравшихся вместе для разработки и тестирования новых технологий, прежде чем они будут широко внедряться в коммерческую Internet.

Компоненты Internet

Современным пользователям Internet эта сеть кажется довольно простой. Когда модем компьютера подключен к телефонной линии, а программное обеспечение соответствующим образом сконфигурировано, пользователь всего лишь набирает телефонный номер провайдера, вводит имя учетной записи, пароль — и все готово! Если компьютер подключен к локальной сети с выделенным доступом, то получить доступ к Internet еще проще.

Многие не в состоянии постичь все тонкости технологии, делающей это возможным. Впрочем, включая телевизор и выбирая любимую программу, зритель тоже редко понимает, что *в действительности* происходит внутри телевизора. Он воспринимает чудеса современной техники как должное.

Однако вы взялись изучить эту технологию, а потому, конечно, захотите узнать больше о том, что происходит при получении доступа к Web-странице либо при отправке электронного письма на соседнюю улицу или на другой материк. Поэтому рассмотрим взаимодействие следующих элементов, составляющих Internet:

- компьютер или локальная сеть, подключенные к Internet;
- провайдер услуг Internet;

- региональная сеть;
- точка доступа в сеть (NAP);
- региональный пункт обмена (Metropolitan Area Exchange — MAE).

Компьютер или локальная сеть

Первый элемент, необходимый для установки соединения с Internet, — локальный компьютер, на котором выполняются соответствующие протоколы и программное обеспечение. Компьютер должен иметь телефонный модем или соединение с локальной сетью, предоставляющей услуги прокси или NAT.

Стеком протоколов Internet служит TCP/IP, поэтому он должен быть установлен и конфигурирован на локальном компьютере или на компьютере прокси/NAT. Для коммутируемого соединения необходимо соответствующее устройство и ПО.

Провайдер услуг Internet

Если соединение устанавливается с помощью провайдера услуг Internet (часто его называют просто провайдером), то компьютер становится удаленным клиентом его локальной сети.

В начале эры Internet локальный компьютер или локальная сеть должны были иметь непосредственное соединение с магистралью Internet. Для индивидуальных пользователей и небольших компаний это было слишком дорого и не всегда доступно.

Дорогое и сложное оборудование, необходимое для установки *точки присутствия*, т.е. точки доступа в Internet, находится в собственности провайдеров услуг Internet (иногда они арендуют это оборудование). Провайдеры арендуют у телефонных компаний выделенные скоростные линии. Крупные провайдеры имеют собственные линии. Небольшие локальные провайдеры могут не иметь непосредственного соединения с магистралью Internet, вместо этого они подключаются к большим региональным провайдерам, имеющим соединение с магистралью.

Региональная сеть

Провайдеры, не имеющие непосредственного соединения с национальной магистралью, платят *региональным провайдерам* за соединение с региональной сетью, подключенной к национальной магистрали. Ниже приведен список наиболее крупных региональных сетей США.

- **BARRNet**. Расположена на севере центральной части Калифорнии.
- **Westnet**. Покрывает западную часть США.
- **NEARNET и NYSERNet**. Покрывают северо-восточную часть США.
- **MIDnet**. Покрывает центральную часть США.
- **SURAnet**. Покрывает юго-восточную часть США.
- **CICnet**. Покрывает средний запад США.

Пункты NAP

Пункт NAP представляет собой точку, в которой взаимодействуют провайдеры доступа к магистрали (не путать с провайдерами услуг Internet, т.е. обычными провайдерами!). На территории США организация NSF разработала и профинансировала установку четырех базовых пунктов NAP. Ниже приведен список городов, в которых они расположены, и управляющих ими компаний.

- **Нью-Йорк** — компания Sprint.
- **Вашингтон, округ Колумбия** — компания WorldCom.
- **Чикаго** — компания Ameritech.
- **Сан-Франциско** — компания Pacific Bell.

Пункты NAP представляют собой точки коммутации передаваемых пакетов, однако через них проходит не весь поток информации Internet. Провайдеры услуг Internet могут взаимодействовать между собой внутри географических регионов и устанавливать равноправные отношения друг с другом.

Пункты MAE

Пункт MAE представляет собой точку, в которой провайдеры услуг Internet соединены друг с другом. В пунктах MAE коммутируются потоки информации между ними. Указанный пункт в Вашингтоне, округ Колумбия, называется MAE EAST. Компания WorldCom управляет пунктом MAE WEST, расположенным в Кремниевой Долине, Калифорния. Пункты MAE EAST и MAE WEST относятся к MAE первого уровня.

Существует пять MAE второго уровня: MAE CHICAGO, MAE DALLAS, MAE HOUSTON, MAE LOS ANGELES и MAE NEW YORK. В самих пунктах MAE данные не маршрутизируются, это делают провайдеры услуг Internet, подключенные к MAE. Однако в MAE *размещены* маршрутизаторы, принадлежащие провайдерам.

Маршрутизаторы, соединенные с MAE, содержат огромные таблицы маршрутизации. Поэтому здесь используются только самые высокопроизводительные маршрутизаторы, например серии Cisco 7000. Компании WorldCom принадлежат коммутирующие платформы, объединенные в сеть FDDI (Fiber Distributed Data Interface). Устройства MAE управляются рабочими станциями Sun с помощью протокола SNMP (Simple Network Management Protocol) и настраиваемых приложений мониторинга.

Самые большие национальные провайдеры услуг Internet, такие, как Sprint и Netcom, подключены к MAE первых двух уровней. Региональные и меньшие провайдеры подключены к MAE второго уровня, где используются менее производительные маршрутизаторы, например Cisco 4500-M.

Взаимодействие компонентов Internet

Как типичный пользователь взаимодействует с компонентами Internet? Когда пользователь, нажав клавишу, отправляет сообщение электронной почты, клиентское приложение форматирует данные, после чего они подвергаются преобразованиям, описанным в главе 3, "Концепции, модели и стандарты компьютерных сетей". На рис 9.2 показана упрощенная версия последовательности этих событий.



Рис. 9.2. Передача сообщения посредством Internet

1. Данные разбиваются на небольшие порции, которые называются пакетами.
2. Сетевые протоколы добавляют к пакетам заголовки и трейлеры.
3. Двоичные нули и единицы преобразуются в электрические или световые сигналы, передаваемые на носитель.
4. Если компьютер входит в состав локальной сети, данные проходят по ней к серверу или к маршрутизатору, соединенному с телефонной или выделенной арендованной линией.
5. Если используется модемное соединение, то пакеты инкапсулируются протоколами канального уровня PPP (Point-to Point Protocol) или SLIP (Serial Line Internet Protocol) и *модулированные* электрические сигналы передаются по аналоговой телефонной линии.
6. Сигналы поступают на принадлежащий провайдеру *сервер удаленного доступа* (*Remote Access Server — RAS*), настроенный для установки коммутируемого соединения. Другой вариант — использование прямой выделенной линии с провайдером. Если необходимо, пользователь регистрируется на сервере, набрав имя пользователя и пароль.
7. Компьютер становится удаленным узлом локальной сети провайдера.
8. Данные передаются из сервера провайдера в региональную сеть, к которой подключен провайдер (если провайдер входит в категорию крупнейших национальных провайдеров, то этот шаг отсутствует).
9. Данные проходят через один из главных пунктов NAP (если это необходимо) и передаются в коммерческую магистраль Internet.
10. На другом конце данные проходят через другой NAP, через другую региональную сеть и через провайдера на принимающем конце (или через почтовый сервер провайдера), который передает данные на принимающий компьютер.
11. И наконец, данные передаются клиентской почтовой программе пользователя, подключенного к провайдеру. Другой вариант — почтовый сервер провайдера

на некоторое время сохраняет, а затем выгружает содержимое почтового ящика. В конфигурации почтового ящика должна быть заложена учетная запись принимающего пользователя.

Как видите, процесс довольно сложный. На пути к адресату пакет должен пройти через многочисленные серверы и маршрутизаторы и по различным физическим носителям. Тем не менее типичное сообщение электронной почты проходит через всю страну в течение нескольких минут. Неудивительно, что это кажется своего рода чудом.

Теперь, когда вы знаете, как пакеты проходят по различным сетям из одних городов или стран в другие, можно приступить к выяснению того, что позволяет сделать эта технология. Что делает Internet и *что* может сделать пользователь с помощью Internet? И — что важнее всего — *как* это сделать с помощью Internet?

Что делает Internet

Если попытаться выразить назначение Internet одним словом, то это, вероятно, будет *коммуникация*. Коммуникация может быть односторонней и двусторонней, для дела или для развлечения, в реальном времени или нет. Существует много различных форм коммуникации.

Перечислим лишь несколько задач, которые пользователь может решать с помощью Internet.

- Просматривать ресурсы World Wide Web (в поиске полезной информации или для развлечения) и создавать свои Web-страницы, которые могут просматривать другие пользователи.
- Передавать и принимать электронные письма, которые доходят до адресата гораздо быстрее чем обычные.
- Присоединиться к тематическому списку рассылки и обмениваться сообщениями с людьми, имеющими общие интересы или занятия.
- Участвовать в группе новостей (или учредить такую группу), представляющей собой нечто вроде виртуальной доски объявлений, на которой заинтересованные лица могут помещать свою информацию.
- Передавать файлы (например, документы, рисунки, аудио- или видеофайлы) с одного компьютера на другой с помощью протокола FTP (File Transfer Protocol).
- С помощью средств терминальной эмуляции (например, Telnet) подключаться к удаленному компьютеру и выполнять на нем приложения или считывать данные, хранящиеся на его жестком диске.
- Слушать широковещательные аудиопрограммы или просматривать видеофильмы.
- Разговаривать в реальном времени с одним или несколькими людьми, удаленными на большое расстояние.
- Участвовать в телеконференциях, в которых можно совместно просматривать документы, рисунки, а также обмениваться текстовой, аудио- и видеоинформацией.
- С помощью телефонных и компьютерных технологий звонить на другой континент, не оплачивая при этом большие счета телефонным компаниям.
- Устанавливать надежную виртуальную частную сеть, в которой Internet служит связующим звеном между частными серверами или локальными сетями.

Теперь рассмотрим каждую из возможностей подробнее и обсудим используемые при этом приложения и протоколы.

World Wide Web

Для многих Internet и World Wide Web — синонимы. Под термином *адрес Internet* часто подразумевается URL (Uniform Resource Locator — унифицированный локатор ресурса) Web-страницы, например `www.yahoo.com`. Несмотря на то что в Internet работает много различных типов приложений, для многих пользователей Web — это и есть Internet.

Далее рассматриваются такие компоненты Web:

- HTTP (Hypertext Transfer Protocol — протокол передачи гипертекста);
- HTML (Hypertext Markup Language — язык разметки гипертекста);
- Web-серверы;
- DNS (Domain Name Service);
- Web-броузеры.

Кроме того, вы узнаете, что можно найти в Web, кто пользуется услугами Web и как вообще можно что-либо найти в неспокойном море из миллионов Web-страниц.

Протокол HTTP

Протоколом Web служит HTTP. Как вы знаете, протокол — это набор правил. Протокол HTTP определяет, как обмениваются файлы Web (текстовые, графические, аудио-, видеоданные и т.д.). HTTP — это протокол прикладного уровня. Стандарты HTTP разработаны организацией IETF (Internet Engineering Task Force); текущая версия протокола — HTTP 1.1.

Как следует из названия, HTTP используется для обмена файлами *гипертекста*. Гипертекстовые файлы могут содержать связи с другими файлами или с другими фрагментами текста в том же файле. На Web-сервере выполняется служебная программа HTTP, или *демон*, которая обслуживает запросы HTTP. Эти запросы передаются на сервер клиентскими программами HTTP, т.е. Web-броузерами.

Когда пользователь набирает в поле адреса броузера Web-адрес (т.е. URL), или щелкает кнопкой мыши на гиперссылке, броузер передает по этому адресу запрос на Web-сервер. Сервер обрабатывает запрос и возвращает броузеру запрошенный ресурс. Ресурс может быть HTML-страницей, графическим, звуковым или любым другим файлом.

Если запрошенного ресурса на Web-сервере нет или пользователь не имеет к нему права доступа, то Web-сервер возвращает сообщение об ошибке. Наиболее распространены следующие сообщения HTTP об ошибке.

- **401/Unauthorized**. В доступе отказано вследствие неправильного заголовка авторизации.
- **403/Forbidden**. В доступе отказано по неизвестной причине.
- **404/File not found**. Запрошенного ресурса на сервере нет.
- **500/Internal error**. По какой-то причине сервер не смог обработать запрос.

Язык HTML

Web-страницы создаются *Web-дизайнерами*, которые используют HTML для указания Web-броузера, как должна выглядеть Web-страница В языке HTML используются специальные метки, называемые *дескрипторами*, с помощью которых можно установить шрифт текста (полужирный, курсив и т д), окончания строк, окончания абзацев, гиперссылки, места вставки рисунков и др В листинге 9 1 приведен пример HTML-кода Web-страницы, показанной на рис 9 3 Эта Web-страница выводится на экран Web-броузером Internet Explorer компании Microsoft

Листинг 9.1. Пример кода HTML, определяющего вид Web-страницы

```
<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>
```

Код HTML можно создавать с помощью специальной программы, которая называется *редактором HTML*. Существует довольно много редакторов HTML, из которых наибольшее распространение получили Adobe Pagemill, Macromedia Dreamweaver, Microsoft FrontPage, SoftQuad HoTNetaL Pro и Sausage Software HotDog. Некоторые Web-дизайнеры предпочитают писать код HTML вручную с помощью какого-либо текстового редактора, например Notepad в Windows или vi в UNIX/Linux.

Web-серверы

Когда страница HTML создана, ее загружают на Web-сервер, т.е. компьютер, подключенный к Internet или локальной сети, на котором установлено программное обеспечение Web-сервера, например Apache (для Linux/UNIX), Internet Information Server (для Windows), Domino (для Lotus) или Suitespot (для Netscape). Web-сервер управляет размещенными документами. Все графические, звуковые и встроенные файлы, появляющиеся в документе при его просмотре, также хранятся на Web-сервере (возможно, на других Web-серверах).



Рис 9 3. Страница, HTML-код которой приведен в листинге 9 1

Web-сервер должен быть подключен к Internet. У него есть свой публичный IP-адрес, по которому его можно идентифицировать. Как вы помните, каждый сервер в Internet имеет имя хоста (например, `www`), имя домена второго уровня (например, `tacteam`) и имя домена верхнего уровня (например, `net`). Вместе эти имена составляют полностью определенное имя домена (Fully Qualified Domain Name — FQDN): `www.tacteam.net`. Это имя, фактически являющееся адресом Web-узла, входит в состав URL (Uniform Resource Locator).

Служба DNS

Когда пользователь хочет получить документ Web, он набирает в своем броузере URL `http://www.tacteam.net`. Поле `http://` задает протокол, используемый документом Web, в нашем примере это протокол HTTP. Запрос пользователя передается на сервер DNS (Domain Name System), который транслирует (преобразует) имя FQDN в IP-адрес Web-сервера. Пользуясь этим IP-адресом, хранящимся в пакете, маршрутизаторы передают его на Web-сервер. Получив запрос, Web-сервер отвечает на него, т е. возвращает нужную HTML-страницу пользователю.

Web-броузеры

Web-броузеры представляют собой клиентское программное обеспечение. Наибольшее распространение получили Web-броузеры Internet Explorer компании Microsoft и Communicator компании Netscape. Ниже перечислены некоторые другие доступные Web-броузеры разных компаний

- **Lynx**. Текстовый броузер. Его можно использовать на самых разных платформах, включая DOS, Macintosh, Windows, OS/2, AIX, SCO и Linux.
- **Amaya**. Распространяется консорциумом W3C (World Wide Web).
- **Emac/W3**. Web-броузер для UNIX, Windows, AmigaDOS, OS/2 и VMS.
- **QNX Voyager**. Web-броузер для операционной системы QNX

- **Opera**. Небольшой, но производительный Web-броузер, работающий в Windows, Linux и BeOS (рис. 9.4).

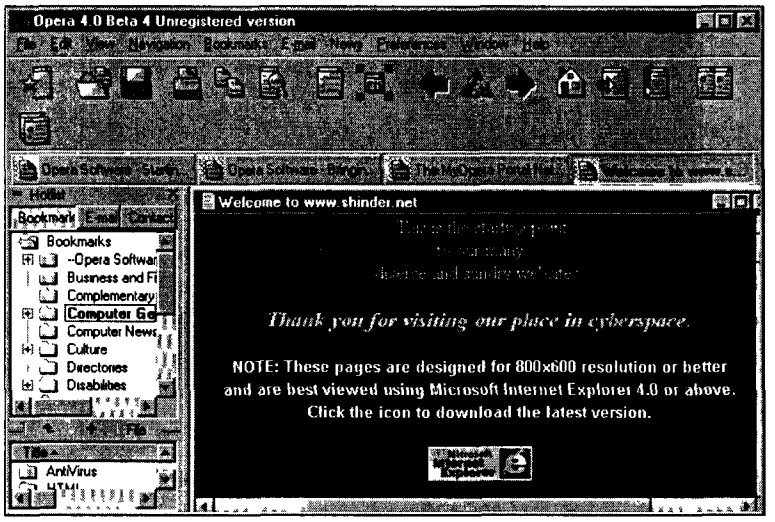


Рис. 9.4. Небольшой быстрый Web-броузер Opera работает на разных платформах

Некоторые Web-броузеры распространяются бесплатно, некоторые — как пробная версия (броузер работает непродолжительное время — несколько месяцев; после этого срабатывает защита и, чтобы продолжить работу с ним, нужно заплатить разработчику). Многие провайдеры работают со своими собственными версиями броузеров или же модифицируют версии Internet Explorer либо Netscape, которые они распространяют среди своих пользователей.

Что можно найти в Web

Все, что угодно: от простых текстовых документов до сложнейших мультимедийных приложений с применением технологий Java и ActiveX. Сказать, что Web расширил наши возможности легко и быстро получать доступ к информации, значит, не сказать ничего. Иметь доступ в Web — это все равно, что иметь на своем столе всю библиотеку Конгресса США, и даже больше того.

Со времени своих первых скромных шагов Web прошел длинный путь развития. Термин "гипертекст" впервые применил Тед Нельсон (Ted Nelson), включивший его в свой проект программного обеспечения Xanadu. Общепризнанный ясновидец Тим Бернерз-Ли (Tim Berners-Lee), которого называют отцом Internet, впервые применил при создании World Wide Web интерактивную технологию. В настоящее время Бернерз-Ли продолжает активно работать в консорциуме World Wide Web — международной организации, разрабатывающей и утверждающей стандарты Web.

Кто использует Web

Постепенно и неуклонно пользователем Web становится каждый житель Земли. В настоящее время доступ к Web почти обязателен для любого бизнеса. Личные и се-

мейные Web-страницы теперь уже никого не удивляют. Даже те, у кого их нет, интенсивно роются по чужим страницам в поиске выгодных предложений.

Организация NSFNET (National Science Foundation Network) собирала и обрабатывала статистические данные о потоках информации по магистрали Internet до 1995 года, т.е. до того момента, когда NSF (National Science Foundation) перестал курировать магистраль и передал ее коммерческим организациям. Согласно данным NSFNET по состоянию на июнь 1993 года на Web приходилось только 0,5% потоков информации Internet. К марту 1995 года эта величина выросла до 23,9%. Согласно обзору NUA — *общепризнанной консультационной компании* Internet — в апреле 2000 года в США около 52% частных домов имели доступ к Web. По сведениям многих источников количество страниц, передаваемых серверами Web, удваивается приблизительно за год. На январь 2000 года серверы Web содержали 2 млрд страниц и около 450 млн изображений. Естественно, эти оценки не остаются постоянными — ежедневно добавляются сотни и тысячи новых страниц, а старые постоянно модифицируются или удаляются.

Цены на персональные компьютеры постоянно снижаются, и подключение к Internet сейчас может позволить себе почти каждый. Некоторые компании даже предлагают бесплатное подключение, для них оно окупается за счет рекламы. К Internet подключается все больше "простых" людей. Школы устанавливают подключенные к Internet компьютеры в классах, а в курс обучения вводят уроки компьютерной грамотности. Получают все большее распространение Internet-кафе, в которых пользователи могут получить доступ к Internet за определенную плату.

Те, кто имеет доступ к Internet, пользуются услугами Web в самых разных целях и часто даже ежедневно. Потребители с помощью Web знакомятся с предлагаемыми товарами и делают покупки. Научные работники и студенты ищут в Web нужные им публикации. Учителя с помощью Web распространяют списки рекомендуемой литературы и учебные материалы. Туристы заказывают билеты и бронируют места в гостиницах. Пациенты ищут сведения о своих болезнях и методах лечения. Представители бизнеса изучают с помощью Web конъюнктуру рынка, ищут сведения о конкурентах, рекламируют и продают свои товары и услуги.

Web неуклонно превращается в технологию, меняющую общество и жизнь каждого из нас не менее радикально, чем в свое время это сделали электричество или телефон. Теперь уже легче ответить на вопрос, кто *не* использует Web, чем на вопрос, кто использует Web.

Поиск информации в Web

Невероятное количество самой разнообразной информации стало не только главным достоинством Web, но и породило серьезные проблемы. Найти все данные по нужной тематике, причем только самые необходимые, совсем непросто. Рассмотрим, как для этого можно использовать поисковые службы, метапоисковые службы и порталы.

Поисковые службы

В попытках облегчить поиск в Web нужной информации разработаны сотни различных поисковых служб. *Поисковая служба* представляет собой Web-узел с интерактивной индексированной базой данных, в которой Web-узлы классифицированы, как правило, с помощью метадескрипторов. *Метадескрипторы* — это ключевые слова, добавленные Web-дизайнером. Согласно `www.wwwmwtric.com` (на этом узле приводится статистическая информация по Web) к услугам поисковых служб прибегают 85%

пользователей, однако индексированы поисковыми службами лишь 20% общедоступных Web-узлов.

Первой солидной поисковой службой была Yahoo (`www.yahoo.com`), которая и сейчас пользуется большой популярностью. Ниже приведен список наиболее часто посещаемых поисковых служб.

- **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`).

Принцип действия большинства поисковых служб основан на анализе ключевых слов, или метадескрипторов, добавленных к HTML-страницам их разработчиками. Эти ключевые слова представляют собой технические или научные термины, по которым пользователь вручную искал бы материалы с нужной ему тематикой в реферативных журналах. Допустим, что пользователь хочет найти что-нибудь о разведении сиамских котов. В этом случае его заинтересуют страницы HTML с ключевыми словами "кот", "сиамский", "разведение" или "сиамский кот".

В поисковых службах применяются приведенные ниже компоненты.

- **Паук (spider)**. Программа, "путешествующая" по различным Web-узлам и собирающая индексную информацию.
- **Индексная база данных**. База данных, в которой хранится индексная информация, собранная пауком.
- **Механизм поиска и выдачи результатов**. Программы интерфейса между пользователями и поисковой службой, с помощью которых пользователи задают свои вопросы и получают ответы.

Некоторые поисковые службы могут в поиске ключевых слов перебирать не только метадескрипторы HTML-страниц, но и весь текст страниц. Это значительно увеличивает количество найденных страниц, но среди них будет намного больше ненужных. Пусть, например, пользователь ищет рецепт торта и поисковая служба нашла ему все страницы HTML, в тексте которых встречается слово "торт". Очевидно, что подавляющее большинство страниц будут содержать не кулинарные рецепты, интересующие пользователя, а все, что угодно, включая детективы и последние новости. Такой поиск может оказаться бесполезным, потому что в предложенных пользователю страницах HTML найти интересующие его кулинарные рецепты будет практически невозможно.

Повысить эффективность поиска можно путем правильного использования алгоритмов поисковой службы. Чаще всего в алгоритмах поиска используются логические функции И, ИЛИ и НЕТ. Вернемся к нашему примеру с тортом. Круг поиска значительно сужается, если в строке запроса ввести "торт И рецепт". В этом случае поисковая служба отбросит страницы, в которых есть торты, но нет рецептов, и страницы, в которых есть рецепты, но нет тортов.

Замечание

Большинство поисковых служб не могут индексировать содержимое Web-узлов, защищенных паролем. Еще нужно учитывать, что после загрузки документа на Web-сервер пройдет некоторое время, прежде чем его индексирует какая-либо поисковая служба. Поэтому в базах данных поисковых служб обычно нет документов, загруженных недавно.

Метапоисковые службы

Эти службы обобщают информацию, собранную поисковыми службами. Перечислим наиболее популярные метапоисковые службы.

- **MetaCrawler** (`www.metacrawler.com`).
- **SavvySearch** (`www.savvysearch.com`).
- **Ask Jeeves** (`www.askjeeves.com`).

Метапоисковые службы не поддерживают собственные индексные базы данных. Они пользуются базами данных других поисковых служб, анализируют накопленную в них информацию и обобщают ее в одном всеобъемлющем списке. Изощренные программы метапоисковых служб способны обнаруживать и устранять повторяющиеся результаты.

Web-порталы

Многие поисковые службы работают как *Web-порталы*. Портал — это Web-узел, который может служить для пользователей "стартовой страницей", т.е. точкой, с которой пользователь часто начинает просмотр интересующих его материалов. Пользователи могут настраивать свои стартовые страницы соответственно своим интересам. Например, можно задать вывод в такой странице местных новостей или прогноза погоды в своем регионе. Можно выбрать также специфические темы, например спортивные новости, коммерческая информация или местные развлекательные мероприятия. Текущее состояние порталов постоянно обновляется, так что их пользователи всегда имеют самую свежую информацию.

Провайдеры услуг Internet предлагают своим пользователям собственные порталы.

Другие службы Web

Кроме текстовых и графических страниц, ссылающихся на другие страницы, Web предоставляет пользователям немало других услуг:

- анимация;
- интерактивная переписка (беседы);
- воспроизведение видео в реальном времени (с помощью Web-камер или служб RealVideo);
- прослушивание радиовещательных каналов (с помощью служб RealAudio);
- трехмерные "прогулки" и панорамы;
- коммерческие Web-узлы, на которых можно совершать покупки;
- электронная почта на основе Web.

Многие службы (например, электронная почта, группы новостей, комнаты для бесед, передача файлов), для которых раньше требовались специальные клиентские приложения, теперь используют встроенные средства Web-броузеров.

Электронная почта и списки рассылки

Электронная почта — одна из наиболее популярных служб Internet. Согласно некоторым источникам через Internet и другие оперативные службы ежегодно передается более 6 млрд электронных сообщений.

В следующих разделах мы рассмотрим преимущества и недостатки электронной почты по сравнению с другими методами коммуникации, принципы работы клиентских и серверных программ электронной почты и списки рассылки Internet, используемые для массового распространения электронных сообщений.

Преимущества электронной почты

По сравнению с другими методами коммуникации электронная почта имеет многочисленные преимущества. Она объединяет достоинства "традиционной почты" и новейших средств телекоммуникации, нивелируя при этом их недостатки.

Электронная почта такая же быстрая и удобная, как телефонная связь. Как и обычные письма, электронные сообщения можно читать не спеша, возвращаясь к интересным местам. Кроме того, электронные письма легко распечатывать, размножать или хранить в любой удобной форме. Другими словами, электронная почта унаследовала все мыслимые достоинства обоих традиционных методов.

Электронное письмо может быть не только текстовым. Современные клиентские программы позволяют подключать к письму любые файлы (такие, как документы Word, рисунки, а также аудио- и видеофайлы). Переданные сообщения можно форматировать, ретушировать или преобразовывать в любую желаемую форму.

Электронная почта значительно дешевле обычной, особенно для документов большого объема. Она дешевле, чем телефонная связь на больших расстояниях. Электронная почта позволяет друзьям и родственникам поддерживать постоянный контакт, с ее помощью коммерческие компании ведут деловую переписку наиболее удобным и эффективным способом, а рекламным и торговым компаниям она позволяет распространять деловые предложения по огромному количеству адресов с минимальными затратами (впрочем, это достоинство электронной почты породило серьезную проблему, которую мы сейчас рассмотрим).

Недостатки электронной почты

Для пользователей и провайдеров серьезной проблемой стало массовое распространение коммерческими организациями своих рекламных материалов (*спам*). Они не только загружают каналы связи, но и значительно затрудняют пользователям поиск нужных сообщений среди огромного количества ненужных. Для противодействия этому многие современные программы электронной почты содержат специальные фильтры, которые отмечают подозрительные сообщения, помещают их в отдельный каталог, а иногда даже автоматически удаляют сразу после получения.

Электронная почта унаследовала от традиционных средств и такую проблему, как возможность неверного толкования. Исследования показывают, что на восприятие человеком информации очень влияют сопутствующие факторы. При обычном разговоре большое значение имеют жесты, выражение лица, интонация собеседника. По ним человек узнает, насколько искренен собеседник, оценивает характер сообщения, которое может быть серьезным, шутливым, саркастическим, сердитым, радостным и т.д. Письменные сообщения (включая сообщения электронной почты) лишены всего

этого. Для решения проблемы можно использовать так называемые *эмотиконы* (emotion+icon, эмоция+пиктограмма) и *смайлики* (smile, улыбка) — специальные пиктограммы, изображающие различные выражения лица. Если вставить их в электронное письмо, они в некоторой степени компенсируют отсутствие живого контакта, хотя это, конечно, явно неадекватная замена.

Отправить электронное письмо очень легко. Как ни странно, это тоже породило специфическую проблему. Многие стали относиться к отправляемым письмам крайне безответственно, позволять себе грубости и непристойности, которые никогда не допустили бы в обычном разговоре. В результате целые области электронной корреспонденции имеют плохую репутацию. Становятся все более распространенными даже электронные войны в Internet — грубые личные нападки, в которых оппоненты не ограничивают себя никакими рамками приличия.

Еще одна проблема — конфиденциальность передаваемой информации. Законодательные системы большинства стран уделяют этому явно недостаточное внимание. Электронное сообщение может быть перехвачено в любой точке на пути от передающего к принимающему компьютеру. Существуют различные методы шифрования (они рассматриваются в главе 14, "Защита сети"). Однако отправить зашифрованное письмо можно только человеку, знающему ключ шифра. Поэтому большинство электронных писем напоминают, скорее, не письма в конвертах, а открытки, которые по дороге к получателю может прочитать каждый желающий.

Программное обеспечение электронной почты

Существует два вида программного обеспечения электронной почты: программы сервера и программы клиента. Рассмотрим каждый из этих видов программного обеспечения в отдельности.

Серверы и протоколы электронной почты

В серверах электронной почты используются стандартизированные протоколы SMTP (Simple Mail Transfer Protocol — простой протокол передачи писем), POP3 (Post Office Protocol — протокол почтовой службы, версия 3) и IMAP (Internet Message Access Protocol — протокол доступа к сообщениям Internet), последняя версия которого — IMAP4.

Замечание

Протокол SMTP используется для передачи сообщений из одной точки в другую посредством Internet, а протоколы POP и IMAP — для чтения и обработки сообщений, поступающих на почтовый сервер.

Сервер SMTP обычно используется для отправки электронных писем. После того как пользователь набрал и подготовил письмо в своей клиентской программе электронной почты, оно передается на сервер SMTP провайдера, который передает его в Internet, используя TCP/IP.

В операционной системе UNIX в качестве сервера SMTP популярна программа Sendmail. Многие компании устанавливают в своих локальных сетях внутренние почтовые серверы (например, Exchange Server), которые маршрутизируют внутреннюю корреспонденцию на локальные принимающие компьютеры или направляют письма провайдеру, если заданный адрес находится вне локальной сети.

Серверы POP принимают электронные письма, адресованные на конкретную учетную запись (например, на `deb@shinder.net`), и хранят их в специальном каталоге, который называется *почтовым ящиком*. Когда клиент POP3 устанавливает с сервером соединение, корреспонденция выгружается на жесткий диск его компьютера. Обычно на сервере она при этом одновременно удаляется, хотя можно конфигурировать сервер на сохранение копии письма.

Серверы IMAP тоже принимают электронные письма, однако это более изощренные серверы, чем POP. На сервере IMAP клиент может просмотреть заголовки пришедших по его адресу писем и решить, какие из них нужно выгрузить. Остальные письма он может удалить, не выгружая на свой компьютер.

Наибольшее распространение получили почтовые серверы Microsoft Exchange, Netscape Messaging Server, Post Office, Sendmail, SLmail, IMail и MDaemon.

Клиентские почтовые программы

Клиентская почтовая программа — это приложение, с помощью которого можно создавать и читать электронные письма. Она должна быть конфигурирована на соединение с почтовым сервером. Наиболее распространены следующие клиентские почтовые программы:

- Eudora;
- Pegasus;
- Microsoft Outlook Express;
- Netscape Mail.

Существуют также клиентские почтовые программы (например, Microsoft Outlook или Lotus Notes), в которых функции обслуживания электронной корреспонденции совмещены с другими задачами — с календарем, службой расписаний, списками задач, записной книжкой и т.д. На рис. 9.5 приведен пример популярной клиентской почтовой программы Eudora.

Замечание

Для передачи и приема электронных писем на компьютере не обязательно должна быть установлена клиентская почтовая программа. В настоящее время общедоступны многие почтовые Web-узлы. С их помощью можно создавать, передавать и принимать электронные письма, пользуясь обычным Web-броузером. Во многих случаях провайдеры предоставляют почтовые учетные записи на основе Web бесплатно. Естественно, чтобы воспользоваться ими, нужно иметь доступ к Web.

С помощью современных клиентских почтовых программ можно организовать сортировку принятых почтовых сообщений и размещение их по разным каталогам. В программе можно задавать правила автоматической фильтрации поступающих электронных писем. Существуют программы, позволяющие передавать и принимать письма в формате HTML, в этом случае письмо может содержать все элементы полноценной Web-страницы — графические изображения, звук, видео и даже программные сценарии, выполняющие какие-либо действия.

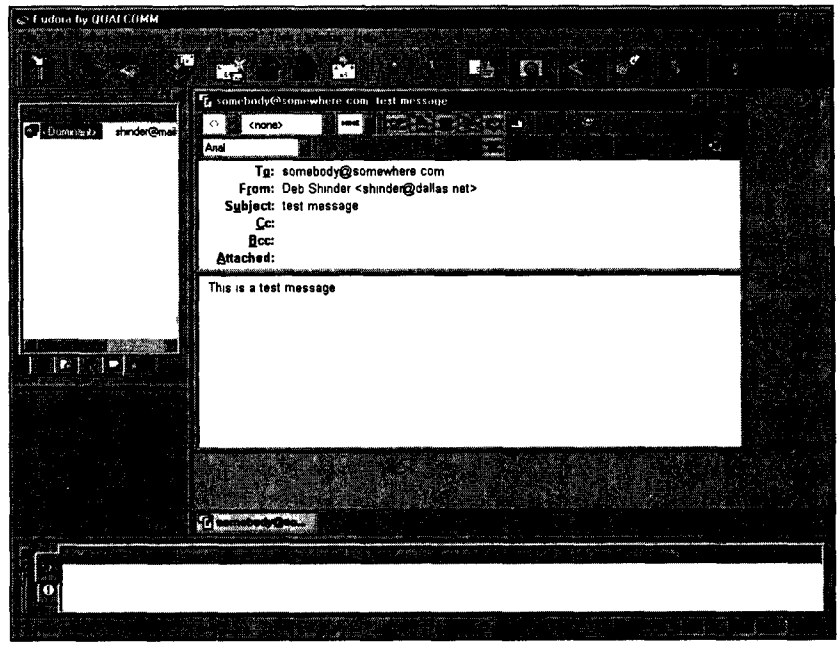


Рис. 9.5. Eudora — популярная клиентская почтовая программа, которую можно загрузить по адресу: `www.qualcomm.com`

Списки рассылки

Все большее распространение в Internet получают дискуссионные группы по интересам на основе списков рассылки. Их не следует путать с массовой рассылкой спама: списки рассылки распространяются по многим адресам, однако, чтобы получать письма группы, нужно войти в состав списка рассылки. В некоторых случаях владелец списка или координатор должен одобрить запрос на членство в группе. Многие списки определяют строгие критерии приема новых членов.

Списками рассылки охвачены разнообразнейшие области интересов. Есть списки рассылки для групп врачей, адвокатов, офицеров полиции, художников, писателей, специалистов по компьютерным технологиям и т.д. Существуют также списки рассылки, посвященные различным хобби, — для нумизматов, шахматистов, любителей электронных игр, фотографов и владельцев домашних животных. Есть даже списки, посвященные книгам, спортивным состязаниям, развлечениям, телевизионным шоу и компьютерным программам. Этот список списков можно продолжать до бесконечности.

Замечание

Каталог списков рассылки поддерживается по адресу: `www.liszt.com`. В нем можно найти инструкции относительно того, как стать членом какого-либо списка или учредить свой собственный.

Список рассылки может быть маленьким и неформальным. В такой группе электронные письма распространяются по адресам списка вручную. Если список большой, то письма распространяются автоматически с помощью специальной программы — сервера списка. Ниже перечислены некоторые наиболее популярные серверы списка.

- **Majordomo**. Обычно используется в операционной системе UNIX.
- **ListServ**. Разработан компанией L-Soft для операционной системы Windows NT.
- **Egroups** (`www.egroups.com`) и **Topica** (`www.topica.com`). Серверы списка на основе Web.

Группы новостей

Группы новостей похожи на списки рассылки тем, что они тоже обычно составляются на основе определенной тематики. Их главное отличие состоит в способе получения сообщений: пользователь, включенный в список рассылки (обычно путем передачи запроса по специальному адресу), получает по своему адресу все сообщения списка. Чтобы остановить поток сообщений, нужно аннулировать подписку.

В отличие от этого, для участия в группе новостей нет необходимости оформлять подписку. Достаточно установить и конфигурировать на своем компьютере специальную программу (например, Outlook Express, Netscape News или Free Agent) и подключиться к определенному серверу новостей. После этого можно просматривать все сообщения данной группы новостей, читать их и отправлять собственные сообщения. Однако существуют и группы новостей с ограниченным доступом, для входа в которые нужно указывать имя пользователя и пароль

Если пользователь больше не хочет читать сообщения группы новостей, ему достаточно лишь прервать соединение с сервером и его почтовый ящик больше не будет переполняться потоком сообщений, как это нередко происходит при подписке на объемный список рассылки.

Сетевые протоколы групп новостей

Серверы и клиенты групп новостей сообщаются друг с другом и управляют потоками новостей чаще всего с помощью протокола NNTP (Network News Protocol). Первоначально NNTP назывался *Usenet* и был построен на основе протокола UUCP (UNIX-to-UNIX Copy Protocol). Со временем NNTP заменил UUCP и стал главным стандартом распространения новостей. NNTP является протоколом прикладного уровня.

Программное обеспечение групп новостей

Как и в случае электронной почты, программное обеспечение групп новостей состоит из двух компонентов — программы *сервера новостей*, установленной на компьютере, распространяющем новости, и программы *клиента новостей* (рис. 9.6).

Программа сервера новостей чаще всего входит в состав Web-сервера, например Microsoft IIS. Многие программы электронной почты и Web-броузеры (например, Netscape Communicator, Microsoft Internet Explorer/Outlook Express и Opera) поставляются с встроенным клиентом новостей.

Сервер новостей (см. рис. 9.6) называется `msnews.microsoft.com` (его имя можно найти на левой панели). Под именем сервера приведен список групп новостей, доступных на данном сервере. В правой верхней панели приведен список сообщений выбранной группы новостей `microsoft.public.cert.mct`. Выбранное сообщение выводится в правой нижней панели.

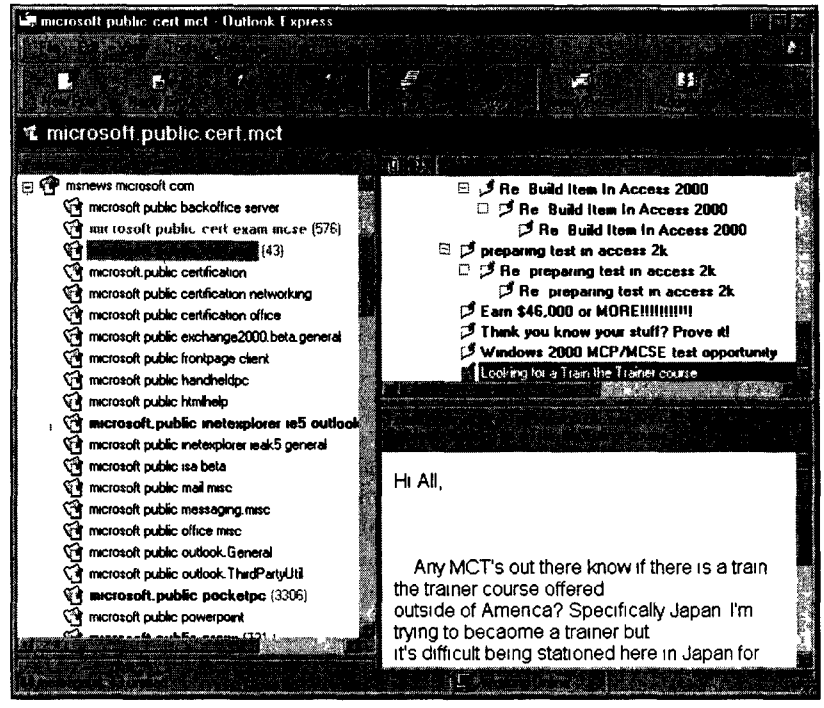


Рис. 9.6 С помощью программы Microsoft Outlook Express можно читать сообщения сервера группы новостей

Передача файлов

С помощью протокола FTP можно передавать файлы на удаленный компьютер. Протокол FTP используется во многих целях, например для выгрузки Web-страниц с локального компьютера на удаленный Web-сервер или для загрузки драйверов с FTP-сервера поставщика на компьютер пользователя.

В большинстве операционных систем, на которых установлен стек TCP/IP, есть встроенные клиентские программы FTP, запускаемые из командной строки. Многие компании поставляют удобные клиентские программы FTP с графическим интерфейсом. Встроенные средства FTP содержат почти все последние версии популярных Web-броузеров, такие, как Internet Explorer, Netscape и Opera.

В листинге 9.2 приведен пример запуска интерфейса FTP из командной строки. Соединение устанавливается с сервером Xerox FTP с помощью протокола FTP. Синтаксис команды имеет следующий вид:

```
ftp
open имя_сервера_FTP
```

Листинг 9.2. Установка соединения клиента FTP с сервером FTP из командной строки

```
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>
```

Первая строка в листинге 9.2 запускает клиентскую программу FTP. Вторая устанавливает соединение с указанным сервером FTP (в нашем случае — `ftp.xerox.com`).

Многие серверы FTP допускают анонимную регистрацию, но требуют применения адреса электронной почты клиента в качестве регистрационного пароля. Когда регистрация завершена, с помощью команды `dir` можно вывести на экран список доступных каталогов. Используя команду `get`, можно загрузить файл с сервера, а с помощью `put` — выгрузить файл на сервер.

Существуют также отдельные клиентские программы FTP с графическим интерфейсом, такие, как WSFTP, CuteFTP и FTP Voyager. Эти и другие приложения FTP можно найти из Web. Некоторые из них бесплатны (например, облегченная версия WSFTP), однако большинство являются пробными версиями.

Программа Telnet

С помощью программы терминальной эмуляции (Telnet) персональный компьютер может работать как простой терминал другого компьютера (обычно мэйнфрейма). Таким образом, пользователи могут запускать программы на мэйнфрейме. Программа Telnet — это клиентская программа эмуляции терминала, использующая протокол Telnet. Она входит в состав большинства реализаций TCP/IP.

Протокол Telnet позволяет компьютеру с клиентским программным обеспечением Telnet устанавливать соединение с сервером Telnet и взаимодействовать с удаленным сервером посредством терминального окна. С помощью протокола Telnet нельзя передавать файлы с одного компьютера на другой, можно только выполнять программы и просматривать файлы на удаленном сервере.

На рис. 9.7 показан сеанс клиентской программы Telnet, встроенной в Windows 2000. В приведенном примере сеанс установлен с удаленным сервером Fedworld, принадлежащим Национальной технической информационной службе правительства США.

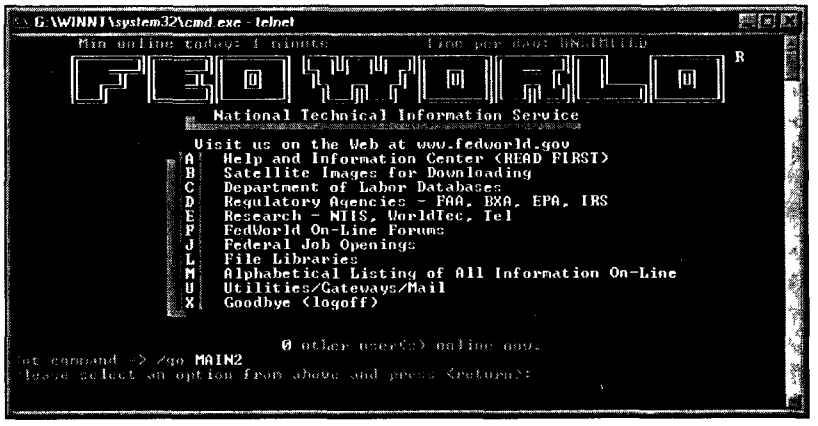


Рис. 9.7. Протокол прикладного уровня Telnet, входящий в состав стека TCP/IP, используется для эмуляции терминала удаленного сервера

Воспроизведение аудио- и видеопотока данных

Высокоскоростные соединения Internet и современные средства связи, такие, как ISDN, T-1, кабельные модемы и DSL, позволяют передавать аудио- и видеоданные в виде непрерывного потока. Это означает, что для прослушивания или просмотра аудио- или видеофайла не нужно дожидаться окончания его выгрузки. Просмотр можно начать как только будет установлено непрерывное соединение и начнется передача данных в потоковом режиме.

Программы аудио и видео в потоковом режиме должны воспроизводиться без неприятных пауз в звуке или изображении. Для этого должно быть обеспечено не только надежное скоростное соединение с сервером, но и достаточные объем памяти и быстродействие клиентского процессора, необходимые для того, чтобы справиться с непрерывным потоком данных. Воспроизведение потока аудио- и видеопрограмм становится все более популярным благодаря постоянному снижению цен на мощные персональные компьютеры, особенно на системы Macintosh.

Для воспроизведения музыкальных и видеоклипов используются приложения QickTime и Real Audio/Real Video компании Apple и Media Player компании Microsoft.

Беседы

Беседой (в периодике часто используется термин "чат", от англ. chat — разговор) называется текстовая коммуникация посредством Internet в реальном времени Она осуществляется с помощью различных программ мгновенной передачи сообщений, таких, как IRC (Internet Relay Chat) или беседы в Web.

Комнаты для бесед на основе IRC и на основе Web

Система IRC представляет собой среду, в которой клиенты IRC, соединенные с сервером IRC, могут участвовать в текстовом "разговоре" друг с другом, причем бесе-

довать могут одновременно несколько пользователей. Серверы IRC предоставляют отдельные "каналы" бесед, предназначенные для определенных тем или групп клиентов. К популярным клиентским приложениям IRC относятся mIRC (одна из наиболее популярных условно-бесплатных программ IRC), Visual IRC и PIRCH (также содержит средства видеокоммуникации в реальном времени).

Комнаты для бесед на основе Web представляют собой Web-узлы со специальным программным обеспечением на основе Java или других языков. Web-путешественники могут "входить" в комнату для бесед и обмениваться друг с другом текстовыми сообщениями в реальном времени.

Мгновенная передача сообщений

Программы мгновенной передачи сообщений позволяют мгновенно передать сообщение пользователю, с которым в данный момент установлено соединение. У обоих пользователей должно быть установлено специальное программное обеспечение. В большинстве случаев на экране принимающего компьютера появляется диалоговое окно, в котором сообщение появляется буква за буквой, по мере того как отправитель набирает его на своей клавиатуре. Некоторые службы предоставляют при этом также средства голосовой связи и двустороннего видео, аналогичные средствам аудио- и видеоконференций, которые рассматриваются в следующих разделах.

Среди популярных приложений мгновенной передачи сообщений можно назвать Mirabilis ICQ, AOL/Netscape Instant Messenger, Microsoft MSN Messenger, Yahoo Messenger, Tribal Voice PowWow и Eld Communications WinTalk.

Аудио- и видеоконференции

С помощью средств аудио- и видеоконференций можно проводить встречи людей, удаленных друг от друга на большие расстояния. Эта технология становится все более популярной в коммерческих кругах и в учебных организациях, которые могут создавать с ее помощью "виртуальные классные комнаты" для обучения в реальном времени.

В зависимости от используемого программного обеспечения, пользователь в процессе сеанса может показывать документы, которые увидят на своих экранах остальные участники конференции. Можно также писать условным "мелом" на виртуальной классной доске, отображаемой на экранах остальных участников.

На персональном компьютере каждого участника конференции должно быть установлено специальное программное обеспечение. Необходимо также установить на компьютере некоторое дополнительное оборудование — звуковой адаптер, микрофон и видеокамеру. Наиболее распространенные программы видеоконференций — CUseeMe (раньше она называлась White Pine Software) и Microsoft NetMeeting.

Для приложений конференций разрабатываются специальные стандарты. В частности, стандарт H.323, разработанный ITU (International Telecommunications Union), определяет различные параметры телекоммуникации в протоколах IP и IPX, в которых не поддерживаются стандарты QoS. Приложения видеоконференций различных поставщиков, удовлетворяющие стандарту H.323, должны обеспечивать взаимодействие друг с другом.

Программное обеспечение видеоконференций можно разделить на две категории.

- **Двухточечное**. Обеспечивает соединение между двумя компьютерами аналогично видеотелефону.
- **Многоточечное**. Предполагает наличие более двух участников видеоконференции.

Организация IMTC (International Multimedia Teleconferencing Consortium) разрабатывает и внедряет стандарты, финансирует различные мероприятия и распространяет информацию о мультимедийных технологиях телеконференций. Консорциум IMTC бесприбыльный, его членом может стать любая заинтересованная организация. Адрес Web-узла IMTC — `www.imtc.org`.

Internet-телефония

С помощью приложений Internet-телефонии пользователи могут устанавливать голосовую связь на больших расстояниях. Эта технология называется *Voice over IP*. При этом расходы оказываются меньше, чем при использовании обычного телефона, потому что стоимость дальней телефонной связи довольно высока.

Первоначально средства телефонии Internet обеспечивали довольно низкое качество связи; кроме того, значительным неудобством было то, что оба абонента должны были иметь одно и то же программное обеспечение. Современные средства позволяют с помощью шлюзовых серверов Internet звонить по обычному телефонному номеру. Абоненту на принимающем конце необязательно даже иметь компьютер или соединение с Internet.

При вызове посредством Internet-телефонии выполняется следующее.

- Абонент передает сообщение с вызовом по IP-адресу шлюзового сервера Internet.
- Вызов маршрутизируется по Internet на шлюзовый сервер.
- Шлюзовой сервер маршрутизирует вызов на сервер, подключенный к телефонной станции в городе, где расположен вызываемый абонент.
- Вызов преобразуется в сигнал традиционного телефонного вызова.
- Сигнал вызова распознается местной телефонной станцией как обычный местный звонок, потому что сервер расположен в том же городе, что и вызываемый абонент.

Замечание

С помощью Internet-телефонии можно передавать также факс-сообщения.

Наиболее популярные клиентские приложения телефонии Internet — NetPhone (для Macintosh), Internet Phone (для Windows), CyberPhone (для UNIX и Windows), PGPhone (для Windows и Macintosh) и Speak Freely (для UNIX и Windows).

К сожалению, в большинстве приложений телефонии до сих пор используются нестандартные технологии, поэтому пользователь может установить соединение только с абонентом, у которого установлено приложение того же поставщика. Однако приложения, разработанные для разных платформ, позволяют устанавливать соединение компьютеров на разных платформах. Например, пользователь PGPhone с компьютером Macintosh может установить соединение с пользователем PGPhone, на компьютере которого установлена операционная система Windows.

Виртуальные частные сети

Интересный способ применения Internet — виртуальная частная сеть (Virtual Private Networking — VPN). Популярность сетей VPN неуклонно растет, потому что их установка требует от компаний минимальных затрат. В технологии VPN Internet ис-

пользуется как промежуточный носитель, с помощью которого устанавливаются надежные и безопасные соединения с удаленными клиентами частной локальной сети. Другими словами, глобальная сеть Internet как бы становится встроенным компонентом частной локальной сети, которая таким образом превращается в глобальную. Аналогичного результата можно достичь, устанавливая соединения с удаленными компьютерами по телефонным каналам, однако телефонная связь на больших расстояниях обходится намного дороже, к тому же надежность и пропускная способность телефонных каналов значительно ниже, чем каналов Internet.

Сети VPN более подробно рассматриваются в главе 16, "Виртуальные частные сети".

Internet и маршрутизация TCP/IP

Во всех рассмотренных в этой главе приложениях Internet для установки соединения между различными операционными системами и платформами используются протоколы TCP/IP. В главе 8, "Сетевые протоколы и службы", рассматривалась работа компонентов протокола TCP/IP на различных участках локальных сетей. В данном разделе сосредоточимся на использовании протоколов TCP/IP в глобальных сетях.

Особенно важное свойство протоколов TCP/IP при работе в межсетевых соединениях и в Internet — пригодность для маршрутизации. Термин *маршрутизация* означает передачу пакетов из одной сети (или подсети) в другую. Звучит это довольно просто, однако маршрутизация в протоколе IP — весьма сложная задача. Конфигурированию маршрутизаторов и протоколам маршрутизации посвящено немалое количество толстых книг. Поэтому в данной главе приводятся лишь базовые понятия маршрутизации. В конце главы представлен список источников, содержащих более подробную информацию по данной теме.

Как выполняется маршрутизация IP

В главе 8, "Сетевые протоколы и службы", приведены преимущества разделения сети TCP/IP на подсети. Одно из преимуществ состоит в том, что при разделении на подсети уменьшается загрузка линий широковещательными сообщениями: для большинства широковещательных сообщений передающий и принимающий компьютеры находятся недалеко друг от друга, поэтому при разделении сети на подсети такие сообщения загружают только каналы подсети. Эффективность работы остальной части сети, естественно, увеличивается.

Процесс передачи сообщений, адресованных компьютеру в другой подсети, называется *продвижением IP*.

Замечание

Как вы уже знаете, IPX/SPX и TCP/IP представляют собой стеки маршрутизируемых протоколов. Большинство маршрутизаторов поддерживают продвижение как IP, так и IPX.

В протоколе IP выполняется логическая адресация и маршрутизация пакетов, т.е. анализируется адрес источника, адрес получателя, маска подсети и выполняется над ними логическая операция И, рассмотренная в главе 8, "Сетевые протоколы и службы". Таким образом определяется, находятся ли передающий и принимающий компьютеры в одной и той же подсети. Если да, то пакет направляется на принимающий компьютер. В противном случае процедура IP передает пакет на *шлюз по умолчанию*.

Шлюз по умолчанию — это IP-адрес маршрутизатора, соединенного с данной локальной сетью и, как минимум, с одной из других сетей. Затем маршрутизатор определяет оптимальный путь передачи пакета адресату с помощью таблицы маршрутизации. На пути к сети, в которой находится принимающий компьютер, пакет может пройти через множество маршрутизаторов. Когда пакет в конце концов достигает этой сети, анализируется та часть IP-адреса, в которой записан адрес принимающего компьютера, и пакет передается ему.

Пример простой маршрутизированной сети

Рассмотрим простую маршрутизированную сеть. Сеть А имеет номер 198.1.1.0. Сеть В — номер 203.13.4.0. Обе сети принадлежат классу С и не содержат подсетей. Сети А и В соединяет компьютер с двумя сетевыми адаптерами, на котором установлена операционная система Windows NT. Свойства TCP/IP этого компьютера сконфигурированы на выполнение продвижения IP, т.е. компьютер работает как маршрутизатор (рис. 9.8).

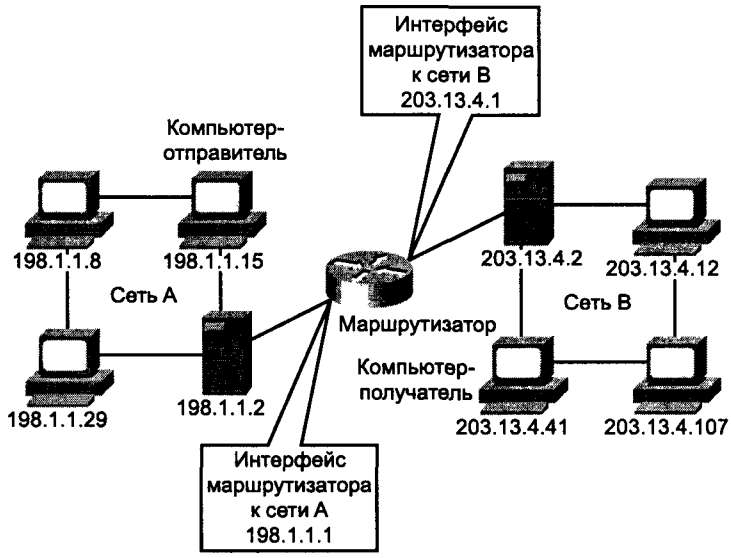


Рис. 9.8. Пакет передается от компьютера в сети А на компьютер в сети В

Маршрутизатор (выделенное устройство или компьютер, выполняющий функции маршрутизации) должен принадлежать, как минимум, двум сетям. Другими словами, IP-адреса его сетевых адаптеров принадлежат разным сетям или подсетям. В нашем примере один сетевой адаптер сконфигурирован с номером сети 198.1.1.1, а другой — с номером 203.13.4.1.

Замечание

Первые по счету адреса сети принято присваивать маршрутизаторам. Это не обязательно, однако так маршрутизаторы легче идентифицировать.

Когда компьютер первой сети с IP-адресом 198.1.1.15 передает пакет по адресу 203.13.4.41, в заголовке пакета рассматривается IP-адрес и маска подсети. Для обоих адресов маска подсети равна 255.255.255.0, потому что они оба принадлежат классу C.

Затем над адресом и маской выполняется логическая операция И:

```
198.1.1.15      = 11000110 00000001 00000001 00001111
255.255.255.0   = 11111111 11111111 11111111 00000000
Результат       = 11000110 00000001 00000001 00000000

203.13.4.41     = 11001011 00001101 00000100 00101001
255.255.255.0   = 11111111 11111111 11111111 00000000
Результат       = 11001011 00001101 00000100 00101001
```

Как видите, результаты отличаются. Следовательно, источник и адресат находятся в разных подсетях. Таким образом, пакет передается по адресу 198.1.1.1 — на шлюз по умолчанию первой подсети.

Затем пакет передается через шлюз во вторую подсеть. После этого адресом источника считается IP-адрес другой стороны маршрутизатора — 203.13.4.1.

Выполним еще раз операцию И:

```
203.13.4.1      = 11001011 00001101 00000100 00000001
255.255.255.0   = 11111111 11111111 11111111 00000000
Результат       = 11001011 00001101 00000100 00000000

203.13.4.1      = 11001011 00001101 00000100 00000001
255.255.255.0   = 11111111 11111111 11111111 00000000
Результат       = 11001011 00001101 00000100 00000000
```

На этот раз результаты совпадают. Следовательно, передающий и принимающий компьютеры находятся в одной и той же подсети и пакет передается непосредственно на принимающий компьютер. Путь прохождения пакета показан на рис. 9.8.

Типы интерфейсов маршрутизации

Маршрутизатор должен иметь более одного интерфейса более чем с одной сетью. Сеть может быть локальной или глобальной. Интерфейс с глобальной сетью представляет собой сетевой адаптер, модем, адаптер ISDN или какое-либо другое устройство глобальной сети.

Например, если локальная сеть подключена к Internet посредством коммутируемого соединения, то маршрутизатор (или компьютер, выполняющий его функции) имеет сетевой адаптер, подключенный к локальной сети, и модем, подключенный к глобальной сети. Каждый из этих интерфейсов конфигурируется отдельно и каждому присвоен свой IP-адрес.

Статическая и динамическая маршрутизация

В маршрутизаторах используются *таблицы маршрутизации*, которые представляют собой базы данных, содержащие пути к различным сетям. На рис. 9.9 показана таблица маршрутизации в Windows 2000 Server. Обратите внимание на адрес назначения 0.0.0.0. Это *маршрут по умолчанию*, т.е. IP-адрес шлюза по умолчанию. Пакеты, адресованные хостам вне сети 192.168.1.0, передаются на шлюз по умолчанию по адресу 192.168.1.16 для дальнейшего продвижения.

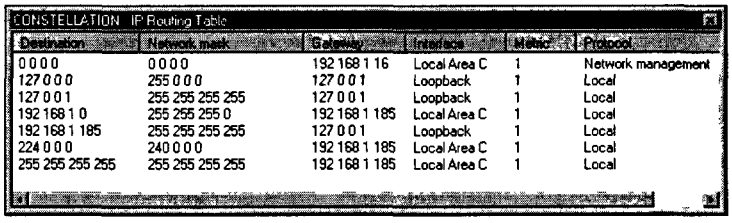


Рис 9 9 Таблица маршрутизации в Windows 2000 Server содержит маршруты к другим сетям

Как маршрутизатор находит в таблице маршрутизации нужный маршрут? Это зависит от того, какая маршрутизация используется — статическая или динамическая Рассмотрим оба типа маршрутизации.

Статическая маршрутизация

При статической маршрутизации администратор вручную вводит в таблицу маршрутизации IP-адреса, определяющие маршруты к разным сетям Это можно сделать с помощью команды `route`, поставляемой в пакетах TCP/IP Утилита командной строки `route` позволяет добавлять или удалять записи в таблице маршрутизации.

Попробуйте применить эту утилиту для просмотра таблицы маршрутизации Для этого введите в командной строке **route print**, как показано в листинге 9.3.

Листинг 9.3. Просмотр статической таблицы маршрутизации с помощью команды `route print`

```
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  192.158.1.201  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
```

В методе статической маршрутизации администратор полностью контролирует используемые маршруты Однако при этом приходится вводить вручную слишком много данных и обновлять таблицу при каждом изменении маршрутов Для больших сетей эта задача становится практически невыполнимой.

Динамическая маршрутизация

В методе динамической маршрутизации для автоматического создания и обновления таблиц маршрутизации используются специальные протоколы, которые рассматриваются в следующем разделе. С помощью этих протоколов сетевые маршрутизаторы сообщаются друг с другом и обмениваются маршрутной информацией. Динамическая маршрутизация имеет ряд преимуществ.

- Уменьшается нагрузка на сетевых администраторов.
- Обеспечивается большая отказоустойчивость (если маршрутизатор выходит из строя, другие маршрутизаторы узнают об этом и выбирают обходные маршруты).
- Уменьшается вероятность ошибок в записях таблицы маршрутизации.

Динамическая маршрутизация предпочтительна для любых сетей, кроме самых маленьких.

Дистанционно-векторные протоколы и протоколы на основе состояния каналов

Протоколы маршрутизации делятся на две категории: *дистанционно-векторные* и *на основе состояния каналов*. Дистанционно-векторные протоколы фактически являются стандартом динамической маршрутизации. Они основаны на алгоритмах, разработанных в 1960-х годах для маршрутизации в сетях ARPAnet. В основе дистанционно-векторных протоколов лежит уравнение Беллмана (Bellman), а их алгоритмы часто называют алгоритмами Беллмана–Форда (Bellman-Ford).

В дистанционно-векторных протоколах предполагается, что каждый маршрутизатор, или хост сети имеет доступ к информации обо всех целевых сетях (таких, куда передаются сообщения). Таблицы маршрутизации содержат адреса шлюзов и *метрику* каждого из них. Метрика — это общее расстояние до целевой сети, выраженное в количестве транзитных передач (промежуточных маршрутизаторов). С помощью метрик и алгоритма Беллмана–Форда маршрутизаторы находят оптимальный маршрут к целевой сети.

"Динамика" метода проявляется в том, что с помощью протокола *маршрутизации* маршрутизаторы передают обновленные таблицы маршрутизации своим ближайшим соседям. Когда обновление передано, новая маршрутная информация сравнивается с хранящейся в таблице маршрутизатора. Если обновленный маршрут, переданный соседним маршрутизатором, имеет лучшую метрику, чем хранящийся в таблице, то маршрутизатор обновляет свою таблицу на основе маршрутной информации с лучшей метрикой.

Дистанционно-векторные протоколы имеют ряд недостатков.

- В них может произойти зацикливание маршрутов.
- Максимальное расстояние маршрута не может превышать 15 транзитных передач.
- В больших сетях эти протоколы обладают плохой расширяемостью.

Протокол на основе состояния каналов — более современный тип протоколов динамической маршрутизации. В нем используются алгоритмы на основе создания "карты" сетей и поддержания базы данных с информацией о состоянии каналов. Когда происходят какие-либо изменения, база данных обновляется.

При использовании протоколов на основе состояния каналов маршрутизаторы передают широковещательные сообщения с маршрутной информацией, распространяя

ее таким образом по всей сети. Такой метод маршрутизации более эффективен, чем дистанционно-векторный, он устраняет многие недостатки последнего. Однако метод на основе состояния каналов порождает собственные проблемы. Одна из них состоит в том, что база данных с информацией о состоянии каналов может вырасти до огромных размеров, в результате чего возрастает нагрузка на процессор маршрутизатора и увеличиваются требования к объему памяти.

Конвергенция, т.е. распространение обновленной маршрутной информации на другие маршрутизаторы в методе на основе состояния каналов выполняется быстрее и чаще, чем в дистанционно-векторном методе.

Распространенные протоколы маршрутизации

Выделенные устройства маршрутизации, такие, как маршрутизаторы Cisco, поддерживают динамические протоколы маршрутизации. В некоторых операционных системах (например, в Windows 2000) протоколы динамической маршрутизации можно использовать на компьютере, выполняющем функции маршрутизатора. Наибольшее распространение в IP получили протоколы динамической маршрутизации RIP (Routing Information Protocol) версий 1 или 2 и OSPF (Open Shortest Path First). Оба протокола подробно рассматриваются ниже.

Замечание

В IPX используется протокол динамической маршрутизации NLSP (NetWare Link Service Protocol). Он работает аналогично протоколу OSPF. Сокращение NLSP иногда означает Network Layer Security Protocol.

Протокол RIP

Дистанционно-векторный RIP — один из первых протоколов динамической маршрутизации — подробно описан в документе RFC 1058. Происхождение RIP можно проследить от программы Routed, которая была частью BSD UNIX 4.3. Одно из основных достоинств RIP — его статус общепризнанного стандарта.

Маршрутизаторы RIP периодически "объявляют" свою маршрутную информацию другим маршрутизаторам. В протоколе RIPv1 объявления передаются в широковещательных пакетах, а в RIPv2 дополнительно используется многоадресная рассылка.

Для устранения некоторых недостатков дистанционно-векторного алгоритма RIP в процедурах протокола используются следующие методы:

- расщепление горизонта;
- обратное обновление с устранением ошибки;
- триггерные обновления.

Рассмотрим каждый из этих методов подробнее.

Расщепление горизонта

С помощью метода расщепления горизонта устраняется следующий недостаток. Маршрутизатор, получивший от соседнего маршрутизатора обновление с неправильной информацией, передает эту информацию обратно на тот же соседний маршрутизатор. В результате неправильный маршрут может передаваться бесконечно. Рассмотрим один из возможных примеров такого процесса (рис. 9.10).

1. Маршрутизатор B получает информацию о том, что маршрутизатор C вышел из строя, и передает эту информацию маршрутизатору A.
2. Маршрутизатор A обновляет свою таблицу маршрутизации с учетом неисправности маршрутизатора C.
3. Маршрутизатор B получает информацию о том, что маршрутизатор C восстановлен. Однако, прежде чем маршрутизатор B передает обновление маршрутизатору A, последний передает маршрутизатору B собственное обновление с информацией о неработающем маршрутизаторе C.
4. Маршрутизатор B обновляет свою таблицу маршрутизации на основе неправильной информации маршрутизатора A.

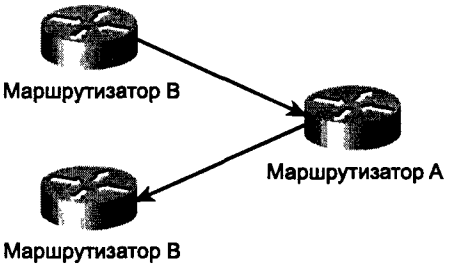


Рис. 9.10. Метод расщепления горизонта решает проблему бесконечного продвижения неправильной информации туда и обратно между маршрутизаторами

В методе расщепления горизонта указанная проблема решается следующим образом. Когда маршрутизатор A передает свои обновления маршрутизатору B, он *не включает* в них маршруты, полученные от него же. Поскольку обновления не передаются обратно, они распространяются по маршрутизаторам не хаотично, а направленно, как круги от брошенного в воду камня.

Обратное обновление с устранением ошибки

Метод обратного обновления с устранением ошибки работает аналогично методу расщепления горизонта. Однако вместо исключения маршрутов, полученных от маршрутизатора B, маршрутизатор A присваивает им метрику 16. В протоколе RIP максимально допустимое расстояние ограничено 15 транзитными передачами, поэтому маршруты с метрикой 16 рассматриваются маршрутизатором B как недопустимые.

Триггерные обновления

Метод триггерных обновлений состоит в том, что маршрутизаторы передают информацию об изменении метрики маршрутов немедленно, не дожидаясь окончания интервала задержки обновлений. В результате маршрутизаторы быстрее получают новую, правильную информацию, а неправильные обновления быстро устраняются.

Протокол OSPF

Протокол RIP неплохо работает в сетях средних размеров, однако для больших сетей нужен более совершенный протокол. Для этого в маршрутизаторах Cisco и в некоторых операционных системах, поддерживающих протокол IP, используется OSPF.

Это протокол на основе состояния каналов. В больших сетях, состоящих из многих подсетей, OSPF работает значительно эффективнее, чем RIP. Стандарты OSPF определяются документами RFC 1247 и 1583. Используемый в OSPF алгоритм на основе состояния каналов не подвержен зацикливанию маршрутов и гораздо более эффективен, чем RIP.

В методе OSPF высокая эффективность (несмотря на проблему разрастания баз данных) достигается благодаря разделению сети на *области*. Поэтому в OSPF таблицы маршрутизации имеют иерархическую структуру, в отличие от однородных баз данных в RIP.

Каждый маршрутизатор OSPF принадлежит определенной области и поддерживает в своей базе данных информацию только о шлюзах этой области. Специальный маршрутизатор, называемый *пограничным* (*Area Border Router — ABR*), соединяет каждую область с *магистралью области*. Когда пакет должен перейти из одной области в другую, он проходит через магистраль области. Применение этого метода снижает как размер таблиц маршрутизации, так и время, затраченное на повторное вычисление маршрутов при каждом изменении.

Кому принадлежит Internet

Глобальная сеть Internet была создана Министерством обороны США, затем перешла под управление Национального научного фонда США (National Science Foundation — NSF). Однако все это было в далеком прошлом. В настоящее время Internet — коммерческое предприятие, хоть и довольно необычное. Internet не принадлежит никому, тем не менее сотни тысяч различных правительственных и коммерческих организаций, учреждений и физических лиц владеют отдельными частями сети. Например, инфраструктурой сети на территории США, состоящей из кабелей и оборудования, владеют телефонные компании, коммерческие организации и общественные органы.

Несмотря на то что Internet никому не принадлежит, разработкой стандартов для нее и общим надзором за деятельностью в сети заняты многие организации, включая следующие:

- ISOC (Internet Society);
- IAB (Internet Architecture Board);
- IETF (Internet Engineering Task Force);
- IESG (Internet Engineering Steering Group);
- IANA (Internet Assigned Numbers Authority) и ICANN (Internet Corporation for Assigned Names and Numbers);
- W3C (World Wide Web Consortium).

Представим каждую из них подробнее.

ISOC

Состоит из организаций и лиц, занимающихся разработкой и внедрением стандартов Internet и обеспечивающих эффективное функционирование сети по всему миру. ISOC координирует деятельность других организаций в области Internet, финансирует редакторскую группу RFC и руководит деятельностью таких организаций, как IAB и IETF.

IAB

В состав комитета IAB (первоначально он назывался Internet Activities Board) входят 13 членов с правом голоса, один из которых является председателем IETF. Другие члены IAB назначаются организацией IETF. Комитет IAB публикует проекты Internet и документы RFC, формирует исследовательские группы и организует публичное обсуждение вопросов, связанных с организацией, инфраструктурой и работой Internet.

IETF

Состоит из рабочих групп, занимающихся техническими вопросами функционирования Internet. В настоящее время одна из рабочих групп IETF занята разработкой стандартов и способов перехода на более совершенный протокол IPv6. В работе IETF может принимать участие любой желающий. Большинство дискуссий, организуемых проблемной группой IETF, открыто ведутся в Internet. Каждая рабочая группа поддерживает один, или несколько списков рассылки, посредством которых члены группы сообщаются друг с другом.

IESG

Входит в состав ISOC и работает совместно с IAB. Комитет IESG руководит процессом подачи, рассмотрения и утверждения предложений, которые становятся стандартами Internet. Эта деятельность комитета регулируется положениями документа RFC 2026.

IANA/ICANN

Агентство IANA отвечает за присвоение IP-адресов и других уникальных идентификаторов Internet.

Агентство ICANN — это бесприбыльная организация, состоящая из государственных, коммерческих и технических подразделений. Агентство координирует управление службой имен доменов Internet и выделением IP-адресов.

W3C

Консорциум W3C разрабатывает протоколы и стандарты Web. Это международная организация, занимающая ведущие позиции в разработке и внедрении технических спецификаций, определяющих инфраструктуру и основы функционирования Web.

Резюме

В этой главе обсуждались вопросы развития Internet, начиная с ARPAnet и заканчивая сегодняшним днем. Рассмотрена инфраструктура и принцип действия магистрали Internet, с помощью которой устанавливаются соединения между локальными сетями, расположенными на больших расстояниях. Описаны коммерческая магистраль и магистраль vBNS, используемая в исследовательских проектах. Рассмотрены также проект Internet2 и консорциум университетов и государственных учреждений, занятых разработкой и тестированием новых технологий коммуникации.

Затем обсуждались способы установки соединений посредством Internet и участие в этом процессе провайдеров услуг Internet, региональных сетей и пунктов NAP и MAE. Рассмотрено прохождение пакетов по физической инфраструктуре с помощью различных протоколов и приложений Internet. Описаны World Wide Web, поисковые службы, электронная почта, передача файлов, система Telnet, современные технологии воспроизведения потока аудио- и видеоданных, аудио- и видеоконференции, беседы в реальном времени и система телефонии Internet.

Рассмотрены методы маршрутизации пакетов в Internet на основе протокола TCP/IP, основные концепции маршрутизации, статическая и динамическая маршрутизация, а также протоколы маршрутизации — дистанционно-векторные и на основе состояния каналов. Кратко описаны существующие реализации протоколов маршрутизации — RIP и OSPF.

В конце главы были представлены организации, занимающиеся анализом и регулированием различных аспектов функционирования Internet, включая ISOC, IAB, IETF, IESG, IANA, ICANN и W3C.

Теперь, когда вы больше знаете о протоколах и сетевом оборудовании самой большой из всех сетей — Internet, можно приступить в следующей главе к рассмотрению сетевых операционных систем, выполняющихся на серверах и предоставляющих доступ к их ресурсам всем локальным сетям Internet.

Рекомендуемые источники

Дополнительную информацию о системе пунктов MAE компании WorldCom можно найти по адресу: `http://208.234.102.97/MAE/doc/maedesc/maedescl.html`.

Набор карт с магистралями Internet на территории США и Европы, а также другие полезные карты и представленную графически информацию по Internet можно найти в *Атласе Киберпространства* (*Atlas of Cyberspace*) по адресу: `www.cybergeography.org/atlas/atlas.html`.

Дополнительная информация о World Wide Web и стандартах Web находится на Web-узле консорциума W3C: `www.w3.org`.

Дополнительная информация о стандартах электронной почты Internet находится на Web-узле консорциума IMC (Internet Mail Consortium) `www.imc.org`.

Гиперссылки на учебники и дополнительные источники по видеоконференциям есть по адресу: `http://netconference.about.com/internet/netconference/msubl.htm`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Магистраль Internet представляет собой набор каналов связи, используемых локальными сетями для установки соединений на больших расстояниях. Как называются точки соединения с магистралью?

   а. Хосты.

   б. Узлы.

в. Подсети.

г. Серверы.

2. В каких точках основные провайдеры Internet устанавливают соединение друг с другом?

   а. RIP.

   б. vBNS.

   в. Суперкомпьютеры.

   г. NAP.

3. Что из приведенного является определяющей, присущей только им, характеристикой гипертекстовых файлов?

   а. Они расположены на Web-сервере.

   б. Доступ к ним можно получить посредством адреса URL.

   в. Они содержат ссылки на другие файлы или на другие фрагменты в том же файле.

   г. В их состав не может входить встроенная графика.

4. Ниже приведены примеры вводимых в броузере адресов URL некоторых Web-узлов. Какие из них правильные?

   а. http:\www.acme\.

   б. html://www.acme.com.

   в. http://bigserver.acme.com/.

   г. html:\acme.com.

5. Как называется Web-узел, который служит для пользователей "стартовой точкой", предоставляемой им поставщиками услуг Internet, оперативными службами и основными поисковыми службами?

   а. Метапоисковая служба.

   б. Портал.

   в. Шлюз по умолчанию.

   г. Гиперссылка.

6. Какой протокол электронной почты Internet поддерживается на сервере, который получает электронные письма и предоставляет пользователям возможность просматривать заголовки и решать, какие из этих писем следует выгрузить на свой компьютер?

   а. SMTP.

   б. SNMP.

   в. POP.

   г. IMAP.

7. В каких целях используется NNTP?

   а. Для управления списками рассылки Internet.

   б. Для выполнения процедур Novell NetWare в протоколе TCP/IP.

   в. Для доступа к группам новостей.

   г. Для установки соединения с удаленным компьютером, просмотра на нем файлов и выполнения приложений.

8. Что используется для входа в комнату для бесед?
   а. IRC.
   б. Telnet.
   в. IGMP.
   г. FTP.
9. Что описывает стандарт H.323, учрежденный организацией ITU?
   а. Формат Web-страниц.
   б. Видеоконференции.
   в. Передачу файлов посредством Internet.
   г. Работу поисковых служб.
10. Какие из приведенных утверждений о протоколе RIP справедливы? (Выбрать все подходящие.)
   а. RIP — это протокол динамической маршрутизации.
   б. В протоколе RIP сеть делится на области, включая область магистрали, к которой подключены все остальные области.
   в. Эффективность и расширяемость протокола RIP лучше, чем OSPF.
   г. RIP — это дистанционно-векторный протокол.

Глава 10

Сетевые операционные системы

Операционная система компьютера — это программное обеспечение, управляющее работой всех остальных приложений и служебных программ. Аналогично этому, *сетевая операционная система* управляет процессами коммуникации между разными устройствами сети и совместным использованием (разделением) сетевых ресурсов.

Иногда сетевой операционной системой называют любую *не изолированную* операционную систему, содержащую встроенные сетевые компоненты. В противовес этому *изолированная операционная система* предназначена для работы на изолированном компьютере, т.е. не подключенном к сети.

Однако чаще всего термин "сетевая операционная система" означает операционную систему, специально созданную для работы на сетевом сервере, например NetWare или NT Server. В данной главе используется именно это определение.

Здесь рассматриваются перечисленные ниже популярные сетевые (как только что указано, серверные) операционные системы.

- Microsoft Windows NT 4.0.
- Microsoft Windows 2000.
- Novell NetWare.
- UNIX.
- Linux.
- Banyan Vines.
- OS/2 Warp Server.
- Apple.
- LANtastic.

Прежде чем приступить к обсуждению характеристик каждой из этих сетевых операционных систем и сетей, в которых они работают, рассмотрим некоторые общие принципы администрирования сетей в среде клиент/сервер.

Администрирование сетей

Сеть на основе серверов содержит один или более выделенный сервер. Обычно сервером служит компьютер с быстродействующим процессором, большим объемом оперативной памяти и вместительным диском или дисками. По этим показателям сервер чаще всего намного превышает клиентские компьютеры сети.

Серверная операционная система способна обеспечить централизованное администрирование и размещение хранимых данных. Тем не менее серверная система существенно отличается от *централизованной* системы, последний термин обычно применяется к сетям на основе мэйнфреймов. В сетях с мэйнфреймами почти все вычислительные процессы выполняются этими машинами, а клиентские компьютеры играют роль простых пользовательских терминалов. В отличие от этого, клиентские компьютеры серверной сети достаточно мощные, с большими собственными вычислительными возможностями. В зависимости от типа приложения, на клиентском компьютере могут выполняться или почти все вычислительные процессы, или значительная их часть.

Замечание

Как упоминалось в главе 2, "Классификация компьютерных сетей", между изолированными компьютерами и сетями на основе серверных операционных систем существует "промежуточная область" — одноранговые сети. Операционные системы Windows 9*x*, Windows NT и Windows 2000 содержат встроенные средства, с помощью которых компьютер можно подключить не к серверному домену, а к одноранговой рабочей группе, в которой все компьютеры равноправны.

Замечание

Компания NetWare тоже поставляет программное обеспечение для одноранговых сетей — NetWare Lite. Кроме того, компьютеры с операционными системами UNIX и Linux, разработанными главным образом как сетевые, можно легко объединять в одноранговой конфигурации. Одноранговые сети поддерживают также компьютеры Apple Macintosh; сети AppleTalk первоначально разрабатывались для небольших одноранговых рабочих групп.

Как показано в главе 2, "Классификация компьютерных сетей", среда клиент/сервер существенно отличается от одноранговой (рис. 10.1).

Далее рассматриваются основные характеристики среды клиент/сервер, а также способы разделения сетевых ресурсов и управления ими.

Среда клиент/сервер

Сеть на основе серверов предоставляет среду, в которой задачи администрирования, резервного копирования и обеспечения безопасности выполняются довольно просто. В этой среде клиентские компьютеры запрашивают данные и ресурсы у сервера. Сервер может предоставлять клиентам только файлы, однако чаще всего он, кроме этого, предоставляет и другие разделяемые ресурсы: принтеры, приложения, модемы, соединения с Internet и т.д.



Рис. 10.1. Различные типы среды: одноранговая, клиент/сервер и на основе мэйнфрейма

Приложения типа клиент/сервер

В *приложениях типа клиент/сервер* вычислительные возможности сервера (например, сервера базы данных SQL Server) используются для выполнения различных задач, таких, как обслуживание запросов к базе данных. Во многих приложениях больших баз данных применяется язык SQL (Structured Query Language — структурированный язык запросов). Рассмотрим, как выполняется запрос SQL.

1. Пользовательский компьютер, на котором выполняется клиентское приложение базы данных, называемое иногда *внешним интерфейсом* (это может быть, например, Microsoft Access), запрашивает данные у сервера SQL, называемого *внутренним интерфейсом*. Однако, прежде чем передать запрос, в клиентском приложении он транслируется в язык SQL.
2. Запрос SQL передается на сервер. Приняв запрос, сервер ищет запрошенную информацию в компьютере, на котором хранится база данных. Чаще всего это тот же компьютер, на котором установлен сервер.
3. Сервер возвращает результат запроса клиентскому приложению. Затем клиентское приложение предоставляет результат запроса пользователю.

Замечание

На некоторых сетевых серверах может выполняться программное обеспечение *терминальных служб*. С их помощью клиентский сетевой компьютер, на котором выполняется терминальная клиентская программа, может подключиться к серверу и выполнять программы обработки данных на сервере. Это немного похоже на централизованную вычислительную среду с мэйнфреймом и пользовательскими терминалами

Главный недостаток приложений клиент/сервер — высокая первоначальная цена. Программы баз данных клиент/сервер, такие, как SQL Server или Oracle, относительно дороги. В небольших сетях, в которых запросы к базам данных простые и передаются довольно редко, затраты на приложения клиент/сервер могут не окупиться.

Конфигурация сети с архитектурой клиент/сервер

Сеть клиент/сервер может иметь одну из двух следующих конфигураций:

- данные расположены на одном сервере баз данных;
- данные *распределены* на нескольких серверах баз данных.

На рис. 10.2 показаны обе конфигурации.

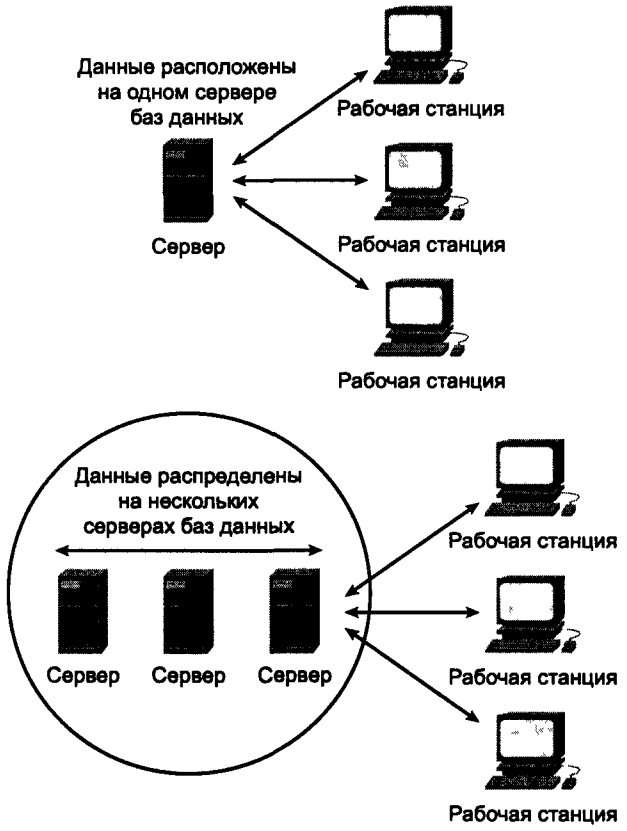


Рис. 10.2. Данные могут быть размещены на одном сервере или распределены по нескольким серверам

Хранилище данных — это вычислительная система, в которой хранится большой объем данных. Традиционно хранилища данных создавались на базе мэйнфреймов. В последнее время появились специально разработанные для этого сетевые операционные системы персональных компьютеров, например Windows 2000 Datacenter Server. В хранилище данные могут находиться на нескольких дисках одного сервера или на дисках нескольких серверов (так называемый *комплекс серверов*).

Разделение сетевых ресурсов

Способ разделения сетевых ресурсов зависит от типа операционной системы В некоторых сетевых операционных системах, например в семействе Windows, по умолчанию не разделяются никакие ресурсы (кроме административных). Чтобы ресурсы были доступны другим компьютерам сети, система должна быть определенным образом сконфигурирована. В других сетевых операционных системах, например в NetWare, принято противоположное правило: все ресурсы являются разделяемыми по умолчанию.

Чтобы компьютер с Windows 9*x* мог совместно использовать свои ресурсы, нужно в диалоговом окне File and Print Sharing (Доступ к файлам и принтерам) установить соответствующие флажки. На компьютере Windows NT или Windows 2000 для этого должна быть установлена и запущена специальная *служба сервера.*

Компьютеры объединяют в сеть для разделения ресурсов, однако это не означает, что каждый ресурс должен разделятся каждым пользователем. Следовательно, сетевая операционная система должна предоставлять возможность управления доступом к файлам, каталогам, принтерам и другим ресурсам. Существует два способа управления доступом, которые называются обеспечением безопасности на уровне ресурсов и на уровне пользователей.

Средства *безопасности на уровне ресурсов* обычно применяются в одноранговых сетях с операционными системами Windows 95/98. В этом способе для разделения, например, такого ресурса, как папка, ему присваивается пароль. Для получения доступа к защищенной совместно используемой папке пользователь должен знать этот пароль и при запросе системы правильно ввести его.

Несмотря на свою простоту, система безопасности на уровне ресурсов превращается в кошмар, когда в сети увеличивается число пользователей и ресурсов. Каждый разделяемый ресурс должен иметь свой пароль. Эти пароли нужно сообщить всем сотрудникам, имеющим право работать с соответствующими ресурсами, причем каждый сотрудник должен запомнить все нужные ему пароли и "забыть" ставшие ненужными (рис. 10.3).

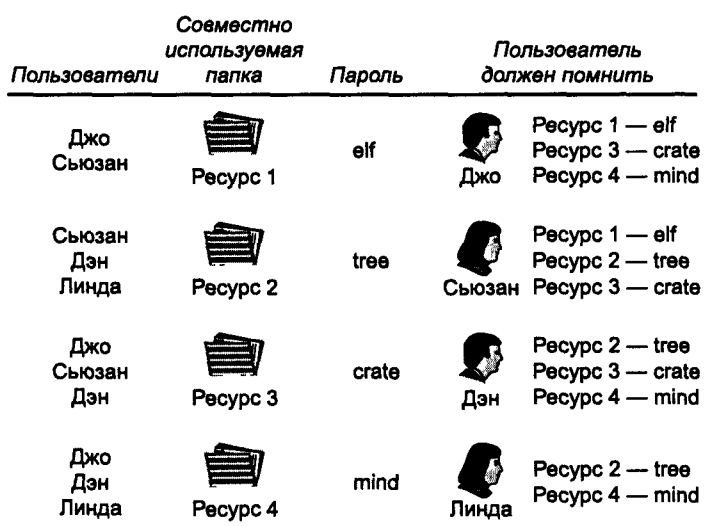


Рис 10.3 В системе безопасности на уровне ресурсов пароль присваивается каждому разделяемому ресурсу

В больших сетях управлять безопасностью *на уровне пользователей* значительно легче, чем на уровне ресурсов. В системе безопасности на уровне пользователей каждому пользователю присвоена защищенная паролем *учетная запись*. С ее помощью пользователь регистрируется на компьютере. Каждый разделяемый ресурс конфигурируется на доступ только тех пользователей, которым разрешено с ним работать. Когда пользователь пытается получить доступ к ресурсу, сервер проверяет ассоциированный с ресурсом *список контроля доступа*, который содержит зарегистрированные учетные записи, имеющие право доступа к этому ресурсу. Если в списке контроля доступа есть учетная запись пользователя, то он получает доступ к ресурсу, в противном случае сервер сообщает об отказе в доступе.

При использовании системы безопасности на уровне пользователей каждый из них, запомнив только один пароль, может получить доступ ко всем нужным ресурсам (рис. 10.4).

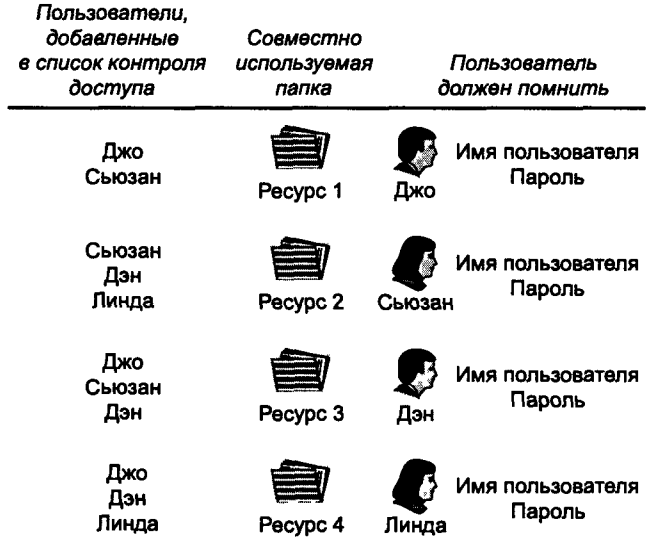


Рис. 10.4. В системе безопасности на уровне пользователей для каждого разделяемого ресурса создается список контроля доступа

Система безопасности на уровне пользователей обеспечивает большую безопасность, чем на уровне ресурсов, потому что для получения доступа к ресурсу пользователь должен зарегистрироваться с правильной учетной записью. В системе безопасности на уровне ресурсов доступ к ресурсу может получить каждый, кто знает пароль к нему. К тому же система безопасности на уровне пользователей позволяет сетевому администратору выполнять *аудит* пользователей, т.е. отслеживать, кто из них запрашивал и получал доступ к сетевым ресурсам.

Управление сетевыми учетными записями

В системе безопасности на уровне пользователей должны быть созданы учетные записи пользователей. В большинстве сетевых операционных систем для облегчения управления учетными записями пользователей их можно разделить на *группы*. В некоторых сетевых операционных системах каждый зарегистрированный в сети компьютер

должен иметь *учетную запись компьютера*. Это обеспечивает дополнительный уровень защиты и повышает безопасность сети. Рассмотрим все три типа учетных записей — пользователя, группы и компьютера.

Учетные записи пользователей

Система безопасности на уровне пользователей основана на создании отдельных учетных записей пользователей для каждого, кто получает доступ к ресурсам. Безопасность на уровне пользователей поддерживается такими операционными системами, как Windows NT/2000, на *локальном уровне*. Однако чаще всего безопасность на уровне пользователей поддерживается на *уровне сети*. В сетях на основе Windows это называется *безопасностью на уровне доменов*.

В общем случае реализация системы безопасности зависит от типа сетевой операционной системы, однако все они построены на основе применения учетных записей пользователей и списков контроля доступа. Безопасность на уровне сети реализуется следующим образом.

1. В процессе установки сетевой операционной системы создается специальная учетная запись пользователя, называемая *учетной записью администратора* (в старых версиях NetWare она называется *supervisor*, а в сетях UNIX/Linux — *root*).
2. С помощью учетной записи администратора сетевой администратор может создавать учетные записи пользователей, которым нужен доступ к сетевым ресурсам.
3. Когда пользователь регистрируется в сети, он вводит имя учетной записи пользователя и пароль, которые сверяются с регистрационной информацией, хранящейся в *регистрационной базе данных*. Эта база данных расположена на *сервере аутентификации* (в сетях Microsoft она называется *контроллером доменов*).
4. Если введенная регистрационная информация признается правильной, пользователь получает *маркер доступа*, с помощью которого его можно идентифицировать в группе.
5. Каждый совместно используемый ресурс имеет список контроля доступа, содержащий пользователей и группы пользователей, которым разрешен доступ к этому ресурсу, а также уровень доступа к ресурсу (разрешение на чтение, изменение или удаление ресурса). Когда пользователь пытается получить доступ к ресурсу (например, распечатать документ на принтере), маркер доступа проверяется по списку контроля доступа (рис. 10.5).
6. Если учетная запись пользователя или группы, к которой он принадлежит, присутствует в списке контроля доступа, пользователь получает доступ к ресурсу. Если пользователь не имеет соответствующего права доступа, сервер отказывает ему в доступе.

Это упрощенное описание работы системы безопасности. В главе 14, "Защита сети", система безопасности и методы аутентификации пользователей рассматриваются более подробно.

Учетная запись пользователя состоит из нескольких компонентов.

- Имя пользователя.
- Пароль (иногда может быть пустым).

- Условия и ограничения пользователя (компьютер, с которого пользователь может зарегистрироваться; разрешенные время и дата регистрации; разрешена ли удаленная регистрация и т.д.).
- Информация о пользователе (группы, к которым принадлежит пользователь, и его права доступа к данному ресурсу, т.е. разрешение на запись, чтение или удаление).
- Необязательная информация (полное имя, должность, служебный телефон и адрес электронной почты пользователя).

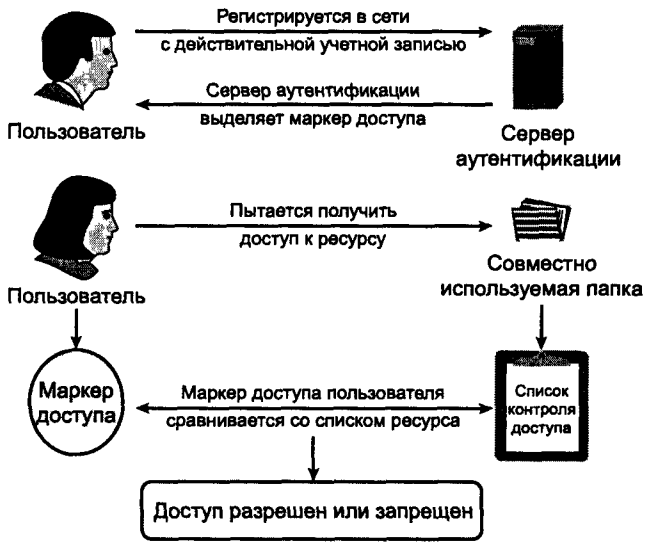


Рис 10.5. Пользовательский маркер доступа проверяется по списку контроля доступа к ресурсу

Конкретный способ создания учетных записей пользователей зависит от типа сетевой операционной системы. Общим для них является наличие утилит, или *инструментов администрирования*, с помощью которых в регистрационную базу данных можно добавлять новых пользователей. Для разных типов сетевых операционных систем общими являются также приведенные ниже правила создания имени пользователя.

- Имя пользователя должно быть уникальным.
- Допускается использование цифр и алфавитных символов верхнего и нижнего регистров.
- Следует избегать (в большинстве случаев запрещено) использования символов ", \, /, :, |, =, ,, +, *, ?, < и >.
- Максимальное число символов имени зависит от типа операционной системы.
- Следует избегать включения в имя пользователя пробелов.

Учетные записи групп

Правами доступа можно управлять путем их назначения отдельным пользователям, однако в большинстве сетевых операционных систем для облегчения администрирования учетных записей предусмотрено использование групп.

Сети многих компаний содержат сотни или даже тысячи пользователей. Предположим, в сети хранится десять совместно используемых каталогов, в которых содержится вся документация отдела продаж. Предположим также, что в отделе продаж работает 200 служащих, которым необходим доступ к этой документации.

В таком сценарии, конечно, можно сконфигурировать все десять каталогов на доступ к ним каждой из 200 учетных записей, однако представьте, сколько это займет времени и сколько при этом будет допущено ошибок! Кроме того, каждый раз при создании нового каталога потребуется опять добавлять эти же 200 учетных записей в список контроля доступа нового каталога. Нельзя ли придумать что-нибудь получше?

Да, лучший способ существует. Можно поместить учетные записи всех служащих отдела продаж в группу с именем `Sales`, тогда права доступа к каждому каталогу можно присваивать *одной* группе, а не *двумстам* учетным записям пользователей. Если создается новый каталог, то добавление в его список контроля доступа группы `Sales` станет делом одной минуты!

Группы можно использовать также для передачи многих копий одного и того же сообщения большому количеству пользователей.

Группы, которым присваиваются права доступа, называются *группами безопасности*. Если группа создана только для использования приложений (например, программы электронной почты) и права доступа ей не присваиваются, то она называется *группой распространения*.

В некоторых операционных системах группы делятся на категории в зависимости от области действия группы. Например, группа может быть локальной, если она применима на одном сервере, и глобальной, если применима во всем домене. В системе Windows 2000 поддерживается также категория *универсальной* группы, область действия которой распространяется на все дерево или лес доменов (рис. 10.6). В сетях NetWare и UNIX локальные и глобальные группы не различаются.

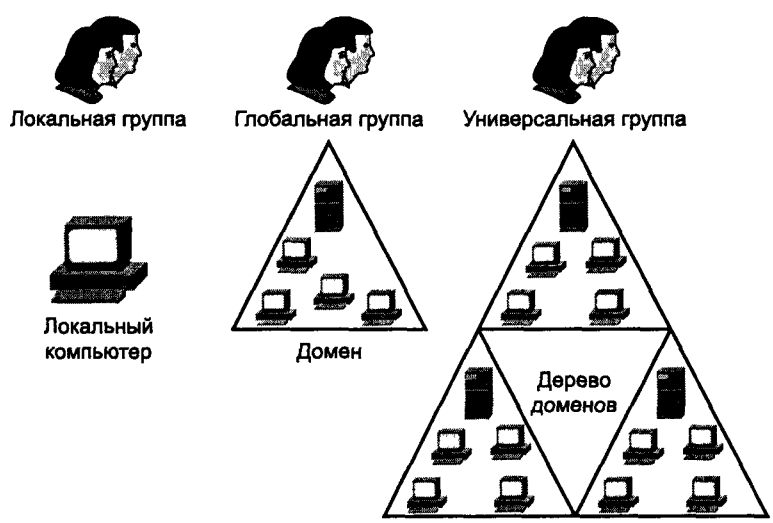


Рис. 10.6. В сетевой операционной системе Windows 2000 поддерживаются три категории групп

В большинстве сетевых операционных систем при установке создается одна или несколько *групп по умолчанию*. Обычно одна из этих групп включает учетные записи всех

пользователей. В системах Windows NT, Windows 2000 и NetWare 3*x* эта группа называется *Everyone* (в последних версиях NetWare такой группы нет). В UNIX она называется *World*. Другие группы по умолчанию — *Users*, *Administrators*, *Backup Operators* и т.д.

Все пользователи, принадлежащие группе, имеют присвоенные ей права доступа. В большинстве сетевых операционных систем пользователь может принадлежать нескольким группам одновременно (в некоторых операционных системах допускается *вложение* одних групп в другие). В связи с этим возникает вопрос о конфликтах прав доступа пользователя, принадлежащего разным группам. Анализ и разрешение этих конфликтов являются важной частью администрирования сетевых операционных систем.

Учетные записи компьютеров

Сетевые операционные системы должны обеспечивать высокий уровень безопасности. Поэтому для регистрации в сети учетные записи должны иметь не только пользователи, но и подключенные к сети компьютеры. Например, в домене Windows администратор должен создать учетную запись для каждого компьютера с операционной системой Windows NT или Windows 2000, прежде чем он войдет в состав домена.

Операционные системы Windows 9*x* создавались для домашних компьютеров и для небольших организаций с низкими требованиями к безопасности, поэтому компьютеры Windows 9*x* не могут войти в состав домена. Тем не менее пользователь с правильной учетной записью *может* зарегистрироваться в домене Windows, используя операционную систему Windows 9*x*.

Учетная запись компьютера используется сетевой операционной системой для проверки идентичности компьютера и для аудита (отслеживания) использования его учетной записи.

Управление совместно используемыми ресурсами

В таких сетевых операционных системах, как Windows, при создании совместно используемого (или разделяемого) ресурса он по умолчанию становится разделяемым группой Everyone, содержащей *всех* пользователей. Если это нежелательно, то при создании разделяемого ресурса нужно изменить права доступа.

Разделяемым ресурсам присваиваются *имена ресурсов*. Чаще всего (хотя и не обязательно) имя совместно используемого ресурса совпадает с фактическим именем ресурса. Например, если разделяемым ресурсом является каталог `salesdocs`, то именем совместно используемого ресурса может быть как `salesdocs`, так и `Sales Documents`, это отнюдь не влияет на имя самого каталога.

Разделяемыми ресурсами нужно управлять. Управление ресурсами предполагает следующее:

- обеспечение простого доступа к ресурсам тем пользователям, которым эти ресурсы необходимы;
- предотвращение несанкционированного доступа к ресурсам.

В некоторой степени эти цели противоречивы, однако обе они могут быть достигнуты путем использования *службы каталогов*, такой, как NDS (Novell Directory Services) или Active Directory компании Microsoft. Эта тема более подробно рассматривается в главе 11, "Службы каталогов".

Разделять можно любые типы устройств, включая сканеры, факсы, внешние накопители и т.д. Если кто-либо сумеет подключиться к сетевому компьютеру, то весьма вероятно, что рано или поздно он найдет способ получить доступ к ресурсам сети.

Теперь рассмотрим типы разделяемых ресурсов, которыми должен управлять сетевой администратор, включая следующие:

- файлы и каталоги;
- принтеры;
- приложения;
- подключения.

Разделяемые файлы и каталоги

Какие преимущества предоставляет разделение файлов и каталогов между пользователями сети? Есть много преимуществ разделения. Например, разделяемыми должны быть документы, которые просматривают и редактируют несколько пользователей. Если каждый пользователь будет хранить такой документ на своем диске, то избежать путаницы, вызванной наличием нескольких похожих копий, будет довольно трудно.

Пользователь *может* создать документ, сохранить его на своем диске и объявить совместно используемым. Однако намного лучше хранить все документы в одном месте — на *файловом сервере*. Это удобнее и эффективнее, чем хранить разделяемые документы на разных компьютерах, и вот почему.

- Администратор может обеспечить регулярное резервное копирование всех документов.
- Если компьютер одного из пользователей выходит из строя, то это не повлияет на работу с документами других пользователей.
- Если все документы хранятся на одном сервере, то каждому будет легче найти нужный ему документ.

Еще одно преимущество сетевого разделения каталогов состоит в том, что каждому пользователю предоставляется безопасное место хранения документов. Иногда это называется *домашним каталогом*. Все данные, созданные пользователем, поступают в его домашний каталог, расположенный на сетевом сервере. Никто, кроме хозяина каталога, не может вносить в него изменения, тем не менее резервные копии домашних каталогов регулярно создаются сервером автоматически.

Для облегчения доступа разделяемый каталог можно создать как сетевой логический диск. Тогда для пользователя удаленный каталог появляется в диалоговом окне программы управления локальными файлами (такой, как Windows Explorer) как логический диск. Например, если для Джона часто нужен доступ к файлам каталога `Marketing`, расположенного на файловом сервере, он может объявить его как логический диск, тогда в окне Windows Explorer этот каталог появится как диск `K:\`. Если теперь Джон дважды щелкнет кнопкой мыши на `K:\`, на экране появится содержимое каталога `Marketing`. Это намного проще, чем, перемещаясь по ресурсам сети, находить каталог `Marketing` и получать к нему доступ каждый раз, когда в нем возникнет необходимость.

Замечание

Дальше в этой главе мы рассмотрим создание сетевых логических дисков для всех операционных систем.

Разделяемые принтеры

В свое время необходимость разделения принтеров и другого периферийного оборудования послужила движущей силой развития коммерческих компьютерных сетей. Разделение принтеров означает, что каждый пользователь сети может распечатывать свои документы на принтере, подключенном к любому другому компьютеру сети (или на принтере, подключенном непосредственно к сети, как часто делают для лазерных принтеров).

В зависимости от операционной системы существует несколько способов подключения к удаленному разделяемому принтеру. В одном из них — *захвате порта принтера* — задачи принтера перенаправляются с порта локального принтера на сетевой принтер. Дальше в этой главе описано, как это делается в разных операционных системах.

Разделяемые приложения

На *сервере приложений* пользователи сети могут выполнять хранящиеся на нем программы (т.е. приложения). В этом случае приложения установлены и выполняются только на сервере, а не занимают место на жестких дисках локальных компьютеров. Производительность серверных приложений обычно немного ниже, чем приложений, выполняемых на локальных компьютерах, однако такой метод все же имеет некоторые преимущества:

- снижаются требования к объему памяти жестких дисков на локальных компьютерах;
- администратор может централизованно конфигурировать приложения;
- администратор может обеспечить, чтобы все служащие организации пользовались одной и той же версией приложения;
- приложение можно модернизировать один раз на сервере, нет необходимости модернизировать его на каждом локальном компьютере.

Разделение приложений можно также реализовать с помощью *терминальных служб*, которые описываются в главе 17, "Сети с тонкими клиентами".

Разделяемые подключения

Еще одно преимущество объединения компьютеров в сеть — возможность разделения подключений к Internet. Компьютеры, объединенные в сеть, могут подключаться к Internet с помощью одной линии и единственной учетной записи. В этом случае нет необходимости покупать модем и платить за телефонную линию и за учетную запись провайдера услуг Internet для каждого компьютера отдельно. Существуют следующие способы разделения подключений к Internet.

- С помощью маршрутизатора, подключающего к Internet все компьютеры локальной сети. При этом каждый компьютер может иметь свой публичный IP-адрес.
- С помощью программного обеспечения NAT (Network Address Translation), позволяющего подключить к Internet все компьютеры локальной сети посредством одного хоста NAT. В этом варианте все компьютеры имеют один публичный IP-адрес.
- С помощью прокси-сервера, который транслирует адреса и обеспечивает безопасность входящих и выходящих пакетов.

Соединения локальных сетей с глобальными посредством маршрутизатора или системы NAT подробно рассматривались в главе 6, "Глобальные сети".

Обзор сетевых операционных систем

Выбор сетевой операционной системы — довольно сложная задача. Каждая популярная операционная система имеет свои достоинства и недостатки. Сетевые операционные системы намного дороже клиентских. В зависимости от количества подключенных к серверу клиентов, стоимость операционной системы может достигать нескольких тысяч долларов. Поэтому к выбору сетевой операционной системы нужно отнестись весьма серьезно.

Сетевые администраторы должны знать, как минимум, основные характеристики трех наиболее распространенных семейств сетевых операционных систем — Windows, NetWare и UNIX/Linux. В настоящее время многие сети имеют в своем составе несколько типов серверов, следовательно, сетевые администраторы должны суметь обеспечить взаимодействие различных систем. Поэтому гибридным сетям и взаимодействию различающихся операционных систем посвящена глава 13, "Гибридные сети".

Для сетевого администратора важно научиться "говорить на языке" сетевой операционной системы. Поставщики операционных систем вкладывают в одни и те же термины разное значение. Например, в среде UNIX термин "корневая" означает главную административную учетную запись, а в сетях NetWare — объект NDS (Novell Directory Services). В то же время в мире Windows термин "корневой" обозначает верхний домен дерева доменов Windows 2000 или базовый элемент распределенной файловой системы.

Далее рассматриваются наиболее распространенные сетевые операционные системы:

- Windows NT и Windows 2000;
- NetWare;
- UNIX/Linux.

Сети Windows NT и Windows 2000

В сетях на основе Windows NT Server и Windows 2000 Server понятие домена является базовым. *Домен* — это группа компьютеров и пользователей, образующих базовую границу администрирования, т.е. управляемых как одно целое. Домены Windows NT и Windows 2000 выполняют одинаковые функции, однако реализация и взаимодействие у них существенно отличаются.

Терминология Windows

Компания Microsoft обозначает термином "домен" группу компьютеров, пользователей и ресурсов, образующих область администрирования, а термином "контроллер домена" — сервер аутентификации, на котором хранится копия регистрационной базы данных. Еще одна специфика терминологии Windows — различение понятий *принтер*, определяющего логическую конструкцию программного обеспечения, и *принтерное устройство*, обозначающего компонент оборудования, на котором распечатываются документы.

Для тех, кто работал с Windows NT 4.0, сетевая терминология Windows 2000 хорошо знакома, однако некоторые новые понятия, такие, как *дерево* или *лес доменов*, могут оказаться незнакомыми даже опытным администраторам NT. К тому же администраторы, пришедшие в Windows из среды NetWare, могут встретить знакомые термины (например, "дерево"), имеющие совершенно другое значение.

Рассмотрим некоторые специфические особенности систем Windows NT 4.0 и Windows 2000, а также выполнение типичных задач администрирования, включая создание в сетях Windows сетевых логических дисков и разделяемых принтеров.

Сети Windows NT 4.0

Графический интерфейс Windows NT 4.0 похож на Windows 95, поэтому он покажется хорошо знакомым каждому, кто работал с операционными системами Windows. Каждый домен NT должен иметь один (и только один) *первичный контроллер домена* (*Primary Domain Controller — PDC*). Контроллер PDC представляет собой "главный" сервер домена, на нем хранится база данных SAM (Security Accounts Management). В домене может быть один или несколько *резервных контроллеров домена* (*Backup Domain Controller — BDC*), каждый из которых хранит копию SAM с атрибутом "только для чтения".

Создание учетных записей пользователей и управление ими в Windows NT 4.0

Для облегчения задач администрирования компания Microsoft разработала программу UMD (User Manager for Domains). Запустив UMD на контроллере домена, можно создавать, изменять и удалять учетные записи пользователей домена. Чтобы запустить программу UMD, нужно выбрать команду Start⇨Programs⇨Administrative Tools⇨User Manager for Domains (Пуск⇨Программы⇨Администрирование⇨Диспетчер пользователей).

С помощью программы UMD администратор может создать новую учетную запись пользователя или группу учетных записей, изменить или удалить учетную запись, присвоить пароль, задать параметры учетной записи или установить ограничения пользователя. Ограничения пользователя определяют, в какое время и с какого компьютера данный пользователь может зарегистрироваться в системе. Диалоговое окно UMD показано на рис. 10.7.

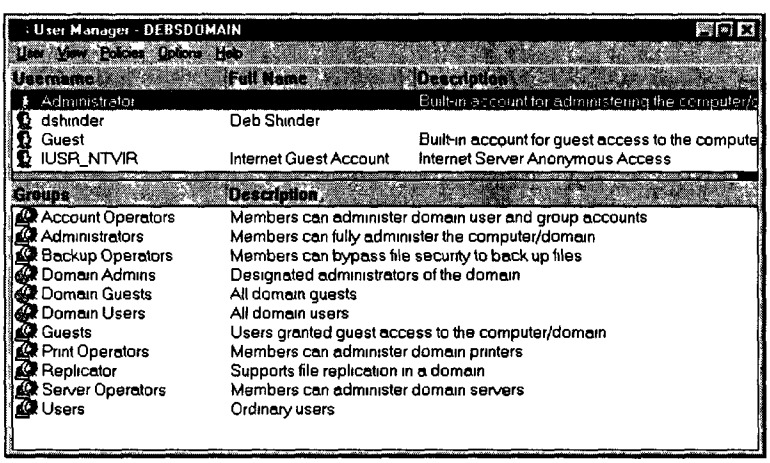


Рис. 10.7. С помощью программы UMD можно создавать учетные записи и управлять ими

Обратите внимание на группы, показанные на рис. 10.7. Все они представляют собой встроенные по умолчанию группы доменов Windows NT. На рис. 10.7 видны также две встроенные по умолчанию учетные записи пользователей — *Administrator* и *Guest*.

Сети Windows 2000

В сетях Windows 2000 для хранения регистрационной информации используется служба каталогов Active Directory, аналогичная службе NDS в сетях NetWare. (Многочисленные функции Active Directory подробно рассматриваются в главе 11, "Службы каталогов".) В отличие от "плоской" регистрационной базы данных NT, служба Active Directory имеет иерархическую структуру.

Домены Windows 2000 можно объединять в дерево доменов, т.е. в группу доменов, имеющих общее непрерывное пространство имен. В свою очередь, деревья можно объединить в лес. Такая структура позволяет наращивать сеть практически неограниченно.

В доменах Windows 2000 нет контроллеров PDC или BDC. Все контроллеры доменов хранят копию раздела Active Directory, а изменения можно вносить из любого контроллера. Выполненные таким образом изменения реплицируются на другие контроллеры домена.

Управление учетными записями в Windows 2000

В сетях Windows 2000 задачи администрирования выполняются с помощью общей консоли управления Microsoft (*Microsoft Management Console — MMC*). В состав MMC входят *интегрированные модули*, содержащие средства выполнения отдельных функций администрирования. Пользователи и группы создаются и управляются с помощью *Active Directory Users and Computers*. Чтобы получить к нему доступ, нужно выбрать команду Start⇨Programs⇨Administrative Tools⇨Active Directory Users and Computers (Пуск⇨Программы⇨Администрирование⇨Пользователи и компьютеры службы Active Directory). Диалоговое окно этого модуля показано на рис. 10.8.

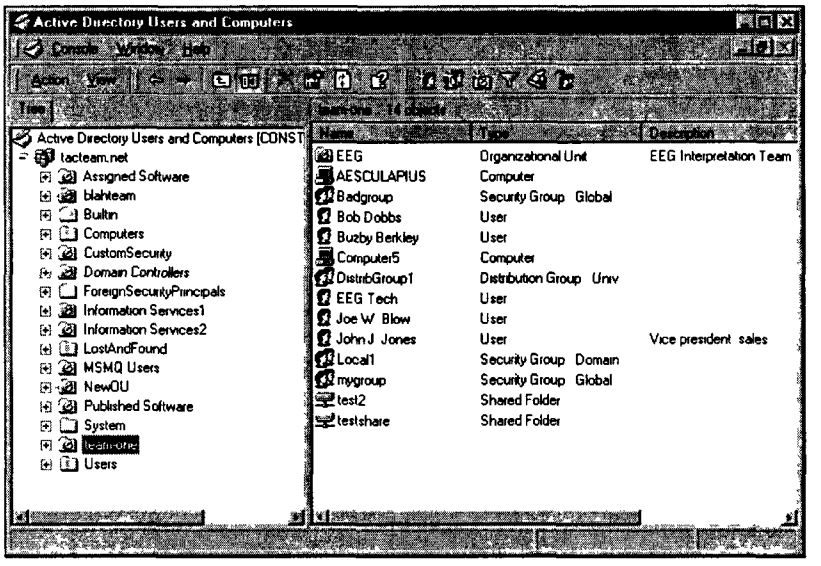


Рис. 10.8. В Windows 2000 пользователи и группы учетных записей управляются с помощью интегрированного модуля Active Directory Users and Computers

В отличие от Windows NT 4.0, в сети Windows 2000 такие объекты, как пользователи или ресурсы, можно помещать в контейнер объектов, который называется *OU* (*Organizational Unit — организационная единица*). Право администрирования каждого

OU можно передать пользователю или группе. Это позволяет детализировать средства администрирования значительно глубже, чем в Windows NT 4.0.

Создание логических дисков в сетях Windows

Создать логический диск в сетях Windows несложно. Это можно сделать двумя способами:

- с помощью Windows Explorer;
- с помощью команды `net use`.

Создание логического диска с помощью Windows Explorer

Для создания логического диска в диалоговом окне Windows Explorer нужно открыть каталог на удаленной системе. Для этого нужно дважды щелкнуть на пиктограмме Network Neighborhood и найти необходимый каталог на нужном сервере, а затем выбрать команду Tools⇨Map Network Drive (Сервис⇨Подключить сетевой диск), как показано на рис. 10.9. Обратите внимание: если установлен Internet Explorer 4.0 или более поздняя версия, то это можно сделать значительно проще — в диалоговом окне Windows Explorer щелкнуть правой кнопкой мыши на имени совместно используемого каталога и из появившегося контекстного меню выбрать команду Map Network Drive (Подключить сетевой диск).

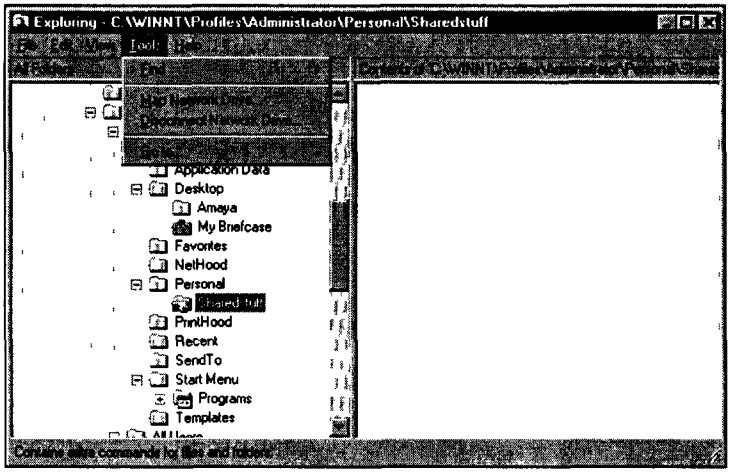


Рис. 10.9. Создание сетевого логического диска в Windows NT 4.0 с помощью Windows Explorer

Созданный диск отображается в левой панели Windows Explorer наряду с дисководом, накопителем CD-ROM и всеми жесткими дисками. К нему можно получить доступ из Windows Explorer или из окна My Computer. Можно также создать для него комбинацию клавиш.

Создание логического диска с помощью команды net use

Еще один способ создания логического диска в операционных системах Windows — использование *универсального соглашения об именах* (*Universal Naming Convention — UNC*). Синтаксис разделяемого ресурса имеет следующий вид:

```
\\имя_компьютера\имя_разделяемого_ресурса
```

Для создания сетевого логического диска разделяемого ресурса введите команду

```
net use <буква_логического_диска>:
\\имя_компьютера\имя_разделяемого_ресурса
```

Если вы предпочитаете выполнять задачи администрирования из командной строки, то вам, скорее всего, больше понравится создавать логические диски с помощью команды `net use`, чем из Windows Explorer.

Разделение принтеров в сетях Windows

Создать разделяемый принтер и установить с ним соединение в сети Windows несложно. Рассмотрим, как сделать локальный (подключенный к вашему компьютеру) принтер разделяемым и как установить соединение с другим сетевым разделяемым принтером.

Разделение локального принтера

Для установки разделения принтера, подключенного к локальному компьютеру, используя окно Control Panel (Панель управления), перейдите в каталог Printers (Принтеры) и щелкните правой кнопкой мыши на имени принтера. Выберите команду Sharing (Доступ), установите переключатель Shared (Общий ресурс), а затем или введите имя разделяемого ресурса, или оставьте имя, предложенное по умолчанию. На рис. 10.10 показана реализация этого процесс в Windows 2000.

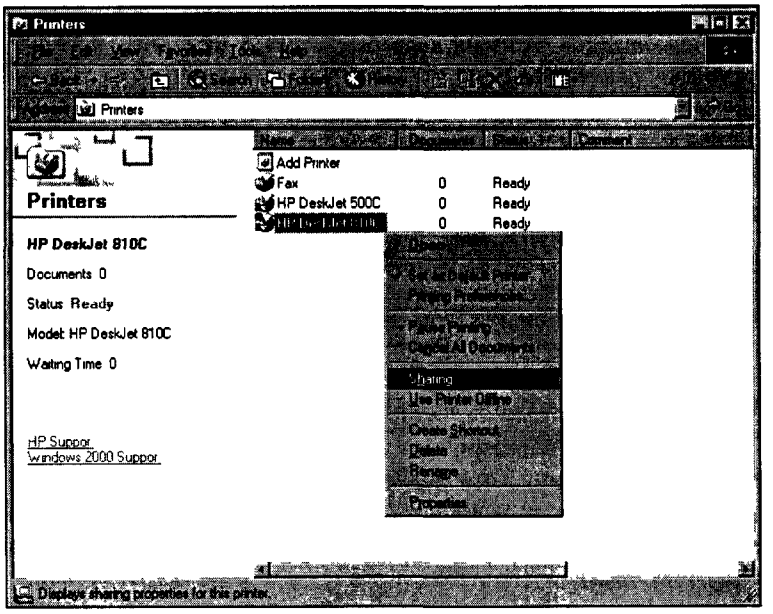


Рис 10 10 Объявление доступа к локальному принтеру в Windows 2000

Установка соединения с совместно используемым принтером

Как и при создании сетевого логического диска, существует два способа установки соединения с сетевым разделяемым принтером: с помощью мастера или с помощью команды `net use`, вводимой из командной строки. Рассмотрим каждый из этих методов подробнее.

Использование мастера Add Printer Wizard. Использовать удаленный принтер проще всего, если добавить его с помощью мастера Add Printer Wizard. Чтобы сделать это, дважды щелкните кнопкой мыши на пиктограмме Add Printer в каталоге Printers и выполняйте указания мастера.

Замечание

В программных продуктах Microsoft довольно часто используются *мастера*, представляющие собой упорядоченные последовательности диалоговых окон. Следуя указаниям мастера, приведенным в диалоговых окнах, пользователь последовательно переходит от одного окна к другому и выполняет таким образом задачу администрирования.

Когда работа мастера завершена, удаленный сетевой принтер появляется в каталоге Printers и пользователь может распечатывать на нем свои документы так, будто это его локальный принтер.

Задачи принтера выстраиваются в очередь печати. Список задач принтера, ожидающих в очереди, называется *спулом принтера*.

Применение команды net use для использования порта принтера. С помощью команды `net use` можно перенаправить задачи принтера с локального порта LPT1 на удаленный сетевой принтер. Синтаксис команды, вводимой из командной строки, имеет следующий вид:

```
net use LPT1: \\имя_компьютера\\имя_принтера
```

Здесь *имя_компьютера* — это имя сервера печати, к которому физически подключено устройство *имя_принтера*.

Совет

В источниках Microsoft принтер как компонент оборудования называется устройством печати. Термин *принтер* означает программную конструкцию, представляющую одно или несколько устройств печати. Другое название такой программной конструкции — *логический принтер*. Одно и то же устройство печати могут представлять несколько логических принтеров, аналогично этому один логический принтер может представлять несколько устройств печати (в этом случае он называется *пулом принтеров*).

Сети NetWare

Как и в разных версиях Windows, способы администрирования в версиях NetWare имеют существенные отличия. Хотя во многих сетях все еще используются серверы NetWare 3.*x*, в настоящее время наиболее распространена версия NetWare 5.1.

Замечание

Серверы версий, предшествовавших NetWare 5, работали только со стеком протоколов IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange). NetWare 5 — первая версия, способная работать с "чистым IP", входящим в состав стека TCP/IP.

Терминология NetWare

Компания Novell использует много терминов, малопонятных начинающим пользователям NetWare. Например, звучащий загадочно термин *bindery* означает всего лишь базу данных, аналогичную базам данных SAM в контроллерах доменов Windows NT.

Сети NetWare 3.*x* и база данных *bindery*

В сетях NetWare 3.*x* база данных *bindery* используется каждым сервером. В каждой *bindery* хранится регистрационная информация только данного сервера. Если в сети есть несколько серверов NetWare, то для доступа к их ресурсам пользователь должен иметь учетные записи, созданные на каждом сервере. Регистрационная информация не реплицируется на другие серверы. Это существенно усложняет задачи администрирования при добавлении в сеть новых серверов.

В версии NetWare 3.11 появилась поддержка добавляемых программных компонентов NLM (NetWare Loadable Modules), представляющих собой утилиты и драйверы, которые устанавливаются на сервере для расширения его функциональных возможностей.

Сети NetWare 4.*x* и служба NDS

В версии NetWare 4 появилась весьма совершенная служба каталогов под названием NDS (Novell Directory Services), которая в значительной степени устранила проблемы администрирования, вызванные существованием отдельных баз данных *bindery* на каждом сервере. NDS представляет собой распределенную базу данных, с помощью которой пользователь может с одной учетной записью регистрироваться на любом сервере и получать доступ ко всем сетевым ресурсам. База данных *bindery* была "плоской". В то же время NDS — иерархическая база данных, имеющая древовидную структуру. Компания Novell называет фактически все сетевые ресурсы, такие, как пользователи, группы, принтеры, каталоги и т.п., *листовыми объектами*.

Служба NDS появилась раньше, чем Active Directory компании Microsoft. Они имеют много общего, включая концепцию OU и возможность размещения объектов в древовидной структуре каталогов независимо от того, где объект находится в сети физически. Обе эти службы — как NDS, так и Active Directory — совместимы с протоколом LDAP (Lightweight Directory Access Protocol — упрощенный протокол доступа к службе каталогов), который рассматривается в главе 11, "Службы каталогов".

Замечание

В сетях NetWare значения терминов "дерево" и "корневой" отличаются от их значений в Windows 2000 и UNIX.

Управление учетными записями в NetWare 4.*x*

При установке NetWare 3.*x* создаются две учетные записи по умолчанию: *Guest* и *Supervisor*. Учетная запись *Guest* имеет ограниченные права доступа, а *Supervisor* — это учетная запись администратора с неограниченными правами. В версиях NetWare 4 и 5 при установке создается только одна учетная запись по умолчанию — *Admin*.

Учетные записи NetWare 4.*x* создаются и управляются с помощью одной из следующих утилит.

- **NetWare Administrator**. Выполняется на клиентском компьютере Windows, на котором установлено клиентское программное обеспечение Novell NDS.
- **NETADMIN**. Утилита командной строки.

Сети NetWare 5.*x*

В состав сетевой операционной системы NetWare 5.*x* входит графическая консоль администрирования на основе языка Java, которая называется ConsoleOne. С ее помощью можно выполнять удаленное администрирование. Она во многом напоминает интерфейс X Window операционной системы UNIX. Разрабатывалась ConsoleOne как графическая оболочка инструментов администрирования NetWare аналогично консоли MMC в системах Windows. Сети NetWare 5 можно администрировать также из командной строки или с помощью утилиты Monitor, основанной на системе меню.

В версии NetWare 5.1 впервые представлена программа NetWare Management Portal — Web-инструмент администрирования, с помощью которого можно управлять серверами NetWare 5.1 с клиентского компьютера посредством Web-броузера.

Клиенты NetWare

NetWare — это серверная операционная система. На клиентских компьютерах сети NetWare должна выполняться настольная операционная система, для которой разработано специальное клиентское программное обеспечение NetWare. Компания Novell поставляет клиентское программное обеспечение для DOS и всех версий Windows, компания Microsoft встраивает клиентские программы NetWare в свои операционные системы Windows. Есть компании, поставляющие клиентские программы NetWare для Macintosh и Linux.

Для некоторых операционных систем, например BeOS, клиентских программ NetWare не существует. Однако из этих операционных систем все же можно получить доступ к серверам NetWare с помощью средства SMB (Server Message Block). SMB позволяет подключиться к серверу NetWare посредством компьютера Linux, на котором выполняется программа Samba и клиентское программное обеспечение NetWare компании Linux. Samba более подробно описывается в главе 13, "Гибридные сети".

Замечание

В качестве клиентского программного обеспечения можно использовать одну из двух программ: Microsoft Client for NetWare (в Windows NT и 2000 она называется Client Services for NetWare) или клиентскую программу Novell, однако на одном компьютере нельзя установить обе эти программы. Клиентская программа Novell предоставляет более широкие функциональные возможности, чем встроенные клиентские программы Microsoft.

При установке и конфигурировании клиентской программы NetWare ей нужно предоставить следующую информацию.

- **Для NetWare 3.x**. Предпочтительный сервер, который нужно выбрать из раскрывшегося списка доступных серверов.
- **Для NetWare 4/5.x**. Предпочтительные дерево и контекст.

Создание логических дисков в сетях NetWare

На сервере NetWare логический диск можно создать с помощью Windows Explorer. Если на клиентском компьютере NetWare установлена операционная система Windows 95, 98, NT или 2000, то процесс создания логического диска ничем не отличается от аналогичного процесса в сетях Microsoft.

Логический диск можно также создать из командной строки с помощью команды map, синтаксис которой имеет вид:

```
map буква_диска:=сервер\том:каталог\подкаталог
```

Разделение принтеров в сетях NetWare

Чтобы распечатать документ на сетевом принтере, нужно с помощью команды capture перенаправить на него принтерную задачу из порта локального принтера. Синтаксис команды capture имеет вид:

```
capture L=<номер_порта> Q=<номер_очереди> P=<имя_принтера>
```

В сетях NetWare *очередь принтера* представляет собой хранящиеся задачи печати и напоминает аналогичную очередь в сетях Windows.

Сети UNIX и Linux

Сетевая операционная система UNIX весьма популярна уже продолжительное время. Она была разработана в 1969 году и с тех пор получила развитие в многочисленных вариантах. Исходный код системы открытый (т.е. доступен бесплатно для каждого, кто хочет использовать или модифицировать его) и написан на распространенном языке программирования C. Это послужило причиной того, что многие коммерческие организации, учебные учреждения и даже отдельные лица разрабатывают собственные версии UNIX.

Операционные системы UNIX используются на высокопроизводительных рабочих станциях, таких, как Silicon Graphics и Sun. Команды UNIX могут выполняться как из командной строки, так и с помощью удобного графического пользовательского интерфейса, например X Window.

Открытый исходный код

Организация Open Source Initiative предоставляет торговые марки тем разработчикам программного обеспечения, которые не возражают против свободного распространения и модификации разработанных ими программных продуктов. Чтобы получить такую торговую марку, программное обеспечение должно удовлетворять определенным критериям: оно должно свободно распространяться без ограничений, а исходный код должен быть доступен для каждого желающего получить его. Примерами программного обеспечения, удовлетворяющего этим требованиям, являются Linux, BSD (версия UNIX), система X Window и приложения, разработанные в рамках проекта GNU Организация Open Source Initiative имеет свой Web-узел по адресу: www.opensource.org.

Операционная система Linux создавалась на основе UNIX для компьютеров с процессорами Intel. Она была разработана Линусом Торвальдсом (Linus Torvalds) в начале 1990-х годов. Как и UNIX, Linux представляет собой операционную систему с открытым исходным кодом, вследствие чего появилось много ее различных вариантов. Опять же, подобно UNIX, в Linux можно использовать такие графические интерфейсы, как X Window, Gnome и KDE.

Теперь рассмотрим терминологию UNIX, некоторые доступные реализации UNIX и Linux, а также способы управления учетными записями и другие задачи администрирования в UNIX и Linux.

Терминология UNIX

В реализациях UNIX и Linux административные учетные записи, используемые для задач управления системой, называются *root*. Учетные записи *Bin* и *sys* владеют программами и запускают их.

Служебные программы сервера называются *демонами*. Примерами являются демон печати и демон FTP. Есть и другие специфичные для среды UNIX термины, мы определим их в следующих разделах этой главы.

Операционные системы UNIX

Существуют сотни различных версий UNIX. Из них наибольшее распространение получили следующие:

- Berkeley Software Design, Inc. (BSD UNIX, от которой происходят другие варианты, например FreeBSD);
- Santa Cruz Operation (SCO) UNIX;
- Sun Solaris;
- AIX (UNIX компании IBM);
- HP-UX (UNIX компании Hewlett Packard).

Открытость исходного кода служит источником как силы, так и слабости операционных систем UNIX. Разработчики могут улучшать и настраивать операционную систему как им заблагорассудится, однако это стало причиной недостаточной стандартизации, часто приводящей в уныние пользователей, администраторов и разработчиков приложений. Тем не менее не все так уж плохо: подавляющее большинство приложений могут выполняться почти на всех платформах UNIX и Linux.

Несмотря на популярность Windows и NetWare в корпоративных локальных сетях, значительная часть приложений Internet все еще выполняется в мощных системах UNIX. Обычно UNIX ассоциируется с дорогостоящим оборудованием и считается операционной системой, не дружественной к пользователю, однако последние разработки способны существенно изменить эту репутацию UNIX. Особенно появление в 1990-х годах операционной системы Linux, сделавшей UNIX популярной также для персональных компьютеров.

Операционные системы Linux

Linux иногда называют "облегченной UNIX". Она разработана для компьютеров с процессорами Intel, однако может работать и на компьютерах RISC. Операционная система Linux позволила воспользоваться преимуществами UNIX дома и в небольших организациях.

Как и в случае с UNIX, существуют многочисленные версии Linux. Некоторые из них можно выгрузить из Web бесплатно, другие распространяются в виде коммерческих продуктов. Наиболее популярны следующие версии Linux:

- RedHat Linux;
- OpenLinux;
- Corel Linux;
- Slackware;

- Debian GNU/Linux;
- SuSE Linux.

В последнее время наблюдается тенденция создания операционных систем Linux, способных поместиться на одной или двух дискетах. Одна из таких "уплотненных версий" — LOAF (Linux On A Floppy) — умещается на одной дискете. Другая версия — DOS Linux — представляет собой небольшую сетевую операционную систему Linux, которую можно установить в существующей системе DOS. Еще один пример: Coyote Linux — небольшая специализированная операционная система, разработанная для совместного использования подключений к Internet.

Список текущих реализаций Linux можно найти на Web-узле по адресу: `www.linux.org`.

Управление учетными записями UNIX и Linux

Для управления серверами UNIX можно использовать систему NIS (Network Information System), разработанную компанией Sun Microsystems. С помощью NIS можно получить доступ к сетевым ресурсам путем однократной регистрации, т.е. зарегистрировавшись единственный раз (с одной учетной записью и паролем), можно получить доступ к ресурсам компьютеров всей сети.

Замечание

Необходимо помнить, что, в отличие от Windows, имена и команды UNIX *чувствительны к регистру*. Другими словами, операционная система различает имена файлов `MyDoc` и `mydoc`. Фактически оба эти файла могут существовать одновременно в одном каталоге.

Возможно, вы уже встречались с этим, набирая URL в своем Web-броузере. Если Web-сервер, с которым броузер устанавливает соединение, работает на основе UNIX, то нужно вводить адрес *точно как написано*. Если Web-страница называется `WebSite.html`, а пользователь введет `Website.html`, то сервер возвратит сообщение об ошибке, например "файл не найден".

Создание учетных записей пользователей и управление ими

В системах UNIX и Linux для добавления новой учетной записи пользователя применяется команда `adduser` (рис. 10.11). Для добавления новой учетной записи нужно зарегистрироваться в качестве суперпользователя. Синтаксис команды `adduser` имеет вид:

имя_пользователя`:/#` **`adduser`**

Управление учетными записями пользователей выполняется путем редактирования файла `/etc/passwd`. Некоторые версии UNIX/Linux содержат *сценарии* для автоматизации этого процесса, однако файл `/etc/passwd` можно также редактировать в любом текстовом редакторе UNIX, например vi, Scripts или Emacs.

Замечание

Сценарии UNIX представляют собой небольшие программы, с помощью которых можно устанавливать какие-либо параметры системы. Сценарий управления учетными записями пользователей выводит на экран последовательность вопросов, отвечая на которые пользователь вносит изменения в файл `passwd`. Сценарии UNIX/Linux в некоторой степени аналогичны мастерам Windows.

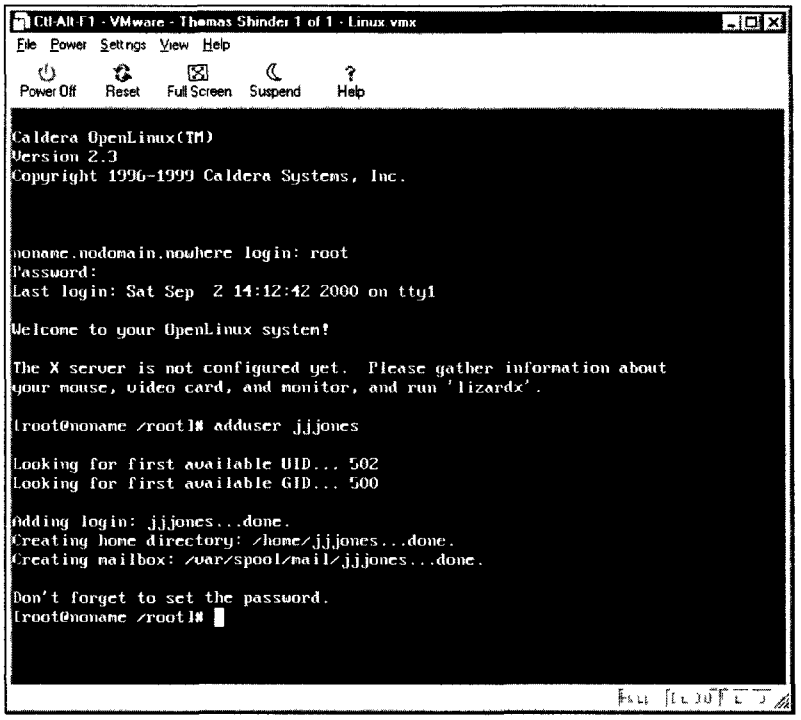


Рис 10 11 Для добавления новой учетной записи пользователя на сервер UNIX или Linux используется команда ***adduser***

Ручное редактирование файла `passwd` может оказаться довольно сложной задачей Пользователь должен ввести данные примерно такого вида

```
deb://BimowSOF9Ev:503:100:Deb Shinder:/home/deb./bin/bash
```

Назначение отдельных полей файла `passwd` разъясняется в табл 10 1

Таблица 10.1. Поля одной записи файла `passwd`

Поле	Назначение
deb	Имя пользователя
BimowSOF9Ev	Пароль (в файле он представлен в зашифрованном виде, поэтому другой пользователь, открывший файл, не сможет получить к нему доступ)
503	Идентификатор пользователя
100	Идентификатор группы
Deb Shinder	Полное имя пользователя
/home/deb	Домашний каталог пользователя
/bin/bash	Оболочка пользователя по умолчанию

Внимание!

Кроме информации о пользователях, файл `passwd` содержит конфигурационную информацию системы, поэтому редактировать его нужно осторожно К счастью, это можно делать с помощью удобных графических утилит, поставляемых многими компаниями

Группы UNIX

Аналогично Windows и NetWare, в системе UNIX для управления доступом пользователей к ресурсам поддерживаются группы. Группы UNIX похожи на локальные группы Windows NT и Windows 2000.

Группы UNIX добавляются с помощью команды `addgroup`, а управление ими осуществляется путем редактирования файла `/etc/groups`. Многие реализации UNIX содержат графические утилиты, предназначенные для выполнения этой задачи. Управлять группами с их помощью значительно легче и безопаснее, чем из командной строки.

Клиенты UNIX

Компания Sun Microsystems разработала файловую систему типа клиент/сервер — NFS (Network File System), которая используется в большинстве версий файловых серверов UNIX. Ее можно установить в системах на базе Windows с помощью средства Solstice Network Client компании Sun. Передача файлов в NFS выполняется с использованием протокола TCP/IP. Операционные системы Windows не содержат клиентских программ NFS.

Если на сервере UNIX выполняется программа Samba (использующая протокол прикладного уровня SMB), то клиенты Windows могут получать доступ к нему без специального клиентского программного обеспечения. В компьютерах Windows протокол SMB используется для доступа к файлам всей сети. Программа Samba делает файловую систему UNIX видимой для клиентов Windows.

Создание в сетях UNIX логических дисков

Логический диск разделяемого ресурса UNIX создается с помощью команды `mount`, синтаксис которой имеет вид:

`mount` *`имя_сервера:/каталог/подкаталог /локальный_каталог`*

Имя локального каталога называется *точкой монтирования (или подключения)*. Путь к точке монтирования должен фактически существовать *до* использования команды `mount`.

Разделение принтеров в сетях UNIX

Распечатать свой документ на принтере, физически подключенном к принтерному серверу UNIX, можно с помощью команды `lpr`. Для печати необходимо установить серверное программное обеспечение LPD (Line Printer Daemon). Синтаксис команды, с помощью которой документ можно распечатать на принтере UNIX, имеет вид:

`lpr -P` *`имя_принтера имя_файла`*

Если ввести команду без имени принтера, то задача будет передана принтеру по умолчанию. В UNIX используются также следующие команды печати:

- `lpq` (просмотр очереди принтера, т.е. списка задач);
- `lprm` (удаление файла из очереди принтера).

Для обеспечения взаимодействия средств печати в Windows NT и Windows 2000 включены службы печати для UNIX.

Другие сетевые операционные системы

Подавляющее большинство компьютерных сетей работают под управлением одной из трех рассмотренных сетевых операционных систем. Однако иногда используются и другие системы, например сетевые операционные системы Banyan VINES, OS/2 Warp Server, Apple и LANtastic, в которых управление сетью выполняется централизованно. Рассмотрим кратко каждую из этих систем.

Banyan VINES

Компания Banyan поставляет сетевую операционную систему VINES (Virtual Networking System), представляющую собой версию UNIX со своей собственной файловой системой VINES вместо NFS. Популярность этой системы невелика, в настоящее время она используется главным образом в академических кругах. Однако VINES все еще сохраняет свое значение благодаря тому, что в ней впервые появилась реальная служба каталогов — StreetTalk, которая более подробно описывается в главе 11, "Службы каталогов".

OS/2 Warp Server

Операционная система OS/2 известна как "настольная операционная система IBM, проигравшая гонку с Windows". С тех пор как в 1996 году компания IBM прекратила выпуск новых версий OS/2, она практически вышла из употребления. Несмотря на прекращение поддержки своей операционной системы, IBM продолжила разработку сервера OS/2. В наше время большое внимание уделяется электронной коммерции, поэтому IBM называет эту операционную систему OS/2 Warp Server for E-business. Традиционная OS/2 первоначально использовалась в банковских и финансовых кругах.

Система Warp Server содержит средства поддержки файловых серверов и серверов приложений. Ее файловая система JFS (Journaled File System) разрабатывалась для больших приложений с повышенной надежностью.

AppleShareIP

Компьютеры Apple Macintosh поставляются с встроенными средствами поддержки одноранговых сетей. Компания Apple выпустила сервер AppleShareIP, который, однако, так и не получил распространения за пределами небольшой ниши рынка. В состав AppleShareIP входят средства сервера FTP, почтового сервера POP3/SMTP, Web-сервера, а также файлового и сервера печати.

LANtastic

Сетевая операционная система LANtastic не является серверной, однако многие небольшие организации обращаются к ней для соединения с компьютерами DOS и Windows в целях совместного использования файлов, модемов и подключений к Internet. В системе LANtastic представлены средства управления одноранговыми сетями, позволяющие объединять до 500 компьютеров — намного больше, чем в традиционных рабочих группах других систем.

Резюме

В этой главе рассмотрены основные понятия сетевого администрирования и характеристики наиболее распространенных сетевых операционных систем. Вначале обсуждались отличия между централизованными системами на основе мэйнфреймов и сис-

темами клиент/сервер на основе персональных компьютеров. Затем были рассмотрены характеристики типичной среды клиент/сервер и оптимизация распределения сетевой вычислительной нагрузки в SQL Server и других серверных системах управления базами данных.

Отмечена необходимость правильного управления разделяемыми ресурсами для облегчения и упрощения санкционированного доступа к ним и предотвращения несанкционированного. Описаны особенности разделения файлов, каталогов, принтеров, приложений и подключений к Internet.

Затем подробно рассматривалась каждая из "большой тройки" сетевых операционных систем и обсуждалась их терминология и средства администрирования. Приведены способы создания учетных записей пользователей и сетевых логических дисков, а также описано использование средств печати в системах Windows NT, Windows 2000, NetWare и UNIX/Linux.

Глава заканчивается рассмотрением менее распространенных сетевых операционных систем, включая Banyan VINES, OS/2 Warp Server, AppleShareIP и LANtastic.

Теперь, когда вы знакомы с наиболее распространенными сетевыми операционными системами, можно приступить к рассмотрению важного компонента современных серверов — службы каталогов.

Рекомендуемые источники

Дополнительную информацию и описание продуктов компании Microsoft Windows NT и Windows 2000 Server можно найти по адресу: `www.microsoft.com`.

Техническую информацию и дополнительные источники по сетям NetWare можно найти на Web-узле компании Novell по адресу: `www.novell.com`.

Дополнительная информация о реализациях Linux размещена в Linux Online! по адресу: `www.linux.org`.

Выгрузить операционную систему FreeBSD вместе с учебниками, справочниками и ответами на часто задаваемые вопросы можно по адресу: `www.freebsd.org`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. В каких сетевых приложениях вычислительные мощности сервера используются для оптимизации запросов к базе данных?
   - **а.** Централизованные приложения.
   - **б.** Интерфейсы пользователя.
   - **в.** Приложения типа клиент/сервер.
   - **г.** Разделяемые приложения.
2. Какой ресурс доступен для других пользователей сети?
   - **а.** Сервер.
   - **б.** Разделяемый.

в. Клиент.

г. Распределенный ресурс.

3. Как называется тип системы безопасности, в котором каждый пользователь имеет учетную запись, пароль и маркер доступа, причем право доступа пользователя к конкретному сетевому ресурсу определяется с помощью списка контроля доступа?

   а. Безопасность на уровне пользователей.

   б. Безопасность на уровне паролей.

   в. Безопасность на уровне ресурсов.

   г. Безопасность на уровне рабочих групп.

4. Чем характеризуется административная учетная запись, которая, в зависимости от операционной системы, может называться *Administrator*, *Admin*, *Supervisor* или *root*? (Выбрать все подходящее.)

   а. Она создается в процессе установки операционной системы.

   б. Права доступа этой учетной записи к сетевым ресурсам ограничены.

   в. Ей нужно устанавливать криптографически сильный пароль.

   г. С ее помощью можно создавать учетные записи других пользователей.

5. Какой из приведенных идентификаторов можно использовать в качестве имени пользователя в любой из трех главных операционных систем, не опасаясь нарушения правил составления имени? (Выбрать все подходящие.)

   а. joesmith.

   б. Joe Smith.

   в. J+Smith.

   г. SMITH007.

6. Как называется группа компьютеров, пользователей и ресурсов, образующих базовую границу администрирования в серверных сетях Windows?

   а. Корень.

   б. Дерево.

   в. Домен.

   г. Лес.

7. Как называется инструмент, с помощью которого в контроллере доменов Windows NT 4.0 можно управлять учетными записями пользователей доменов и паролями?

   а. User Administrator.

   б. User Manager for Domains.

   в. User Manager.

   г. Account Administrator Tool for Domains.

8. Как называется служба каталогов сети Windows 2000, в которой хранится регистрационная информация?

   а. NDS.

   б. LDAP Directory Service.

в. Active Directory.

г. Directory Access Service.

9. Как называется база данных, в которой хранится регистрационная информация на сервере NetWare 3.*x*?

а. Корневая.

б. NDS.

в. Организационный модуль.

г. Bindery.

10. Какое из приведенных утверждений об операционной системе UNIX справедливо? (Выбрать все подходящие.)

а. Операции с файлами чувствительны к регистру символов.

б. Административная учетная запись называется Supervisor.

в. Службы сервера называются демонами.

г. Группы системы UNIX работают во многом аналогично глобальным группам Windows NT 4.0.

Глава 11

Службы каталогов

Важной частью современных сетевых операционных систем является *служба каталогов*, предназначенная для хранения информации о сетевых ресурсах, службах и учетных записях и для получения доступа к этой информации.

В этой главе рассматриваются каталоги, службы каталогов, их назначение и использование в современных сетях. Приводится описание стандартов и спецификаций, определяющих реализацию служб каталогов: спецификации OSI X.500 (Open System Interconnection — взаимодействие открытых систем) и стандартов DAP (Directory Access Protocol — протокол доступа к каталогу) и LDAP (Lightweight Directory Access Protocol — упрощенный протокол доступа к каталогу).

Затем вы познакомитесь с бесприбыльной организацией DEN (Directory-Enabled Networking), поддерживаемой компаниями Microsoft и Cisco Systems. Организация DEN занимается анализом практического использования служб каталогов в целях повышения эффективности управления сетевыми устройствами, ресурсами и службами.

Кроме того, рассматриваются наиболее распространенные службы каталогов, работающие в сетевых операционных системах для персональных компьютеров — NDS (Novell Directory Service) и Active Directory компании Microsoft. Описываются также службы каталогов, работающие на других платформах: SDS (Sun Microsystems' Directory Services) и AS/400 Directory Services компании IBM. Помимо этого, рассматривается межоперационное взаимодействие различных служб каталогов и перспективы создания службы каталогов глобальной сети Internet.

Что такое каталоги и службы каталогов

В сетях с каталогами обязательны два компонента: сами каталоги и службы, с помощью которых ими можно управлять. Рассмотрим эти компоненты.

Что такое каталог

Каталог — это средство упорядочения информации. В повседневной жизни люди пользуются каталогами на каждом шагу, например каталогом телефонного справочника, в котором названия различных организаций расположены в алфавитном порядке.

3. В каких службах каталогов используется однородное (плоское) пространство имен? (Выбрать все подходящие.)
   а. NDS.
   б. NTDS.
   в. Bindery компании Novell.
   г. Active Directory.
4. Как называется пространство имен, в котором в состав имени дочернего объекта входит имя родительского объекта?
   а. Однородное (плоское).
   б. Одного поколения.
   в. Транзитивное.
   г. Непрерывное.
5. Где используются агенты DSA (Directory System Agent), DUA (Directory User Agent) и DIB (Directory Information Base)?
   а. Windows 2000 Active Directory.
   б. DAP.
   в. Спецификация OSI X.500.
   г. Клиентская программа LDAP.
6. Как называется имя пути вида *DC=net DC=tacteam OU=traintng CN=Users CN=John Doe*, обозначающее объект в каталоге?
   а. Атрибут.
   б. Относительное DN.
   в. DN.
   г. Общее имя.
7. Как называется объект в дереве NDS, представляющий ресурс или конец ветви, но не объект, содержащий другие объекты?
   а. Листовой объект.
   б. Корневой объект.
   в. Стеблевой объект.
   г. Родительский объект.
8. В каком файле Active Directory хранятся сценарии и стратегии группирования объектов?
   а. В файле журнала Active Directory.
   б. В файле сценариев.
   в. В административном файле стратегии групп.
   г. В файле SysVol.
9. Какое из приведенных утверждений о доменах Windows 2000, расположенных в одном и том же дереве доменов, справедливо?
   а. Между ними нет доверительного отношения.
   б. Между ними существует двустороннее транзитивное доверительное отношение.

В мире компьютеров понятие каталога может означать разные вещи. Вы, конечно же, хорошо знакомы с файловой системой компьютера, в котором каталог представляет собой набор файлов и других каталогов, сгруппированных для более удобного применения. Однако каталоги и службы каталогов, используемые в сетевых операционных системах, — это несколько иные понятия, хотя и похожие на каталоги файловой системы. В сетевых операционных системах каталог представляет собой базу данных специального вида, содержащую информацию о различных объектах.

В объектно-ориентированной операционной системе каталог содержит *объекты*, имеющие *атрибуты*. Например, учетная запись пользователя — это объект, который может храниться в каталоге. Атрибуты этого объекта включают имя пользователя, его данные, пароль и другую информацию, имеющую отношение к учетной записи (рис. 11.1).

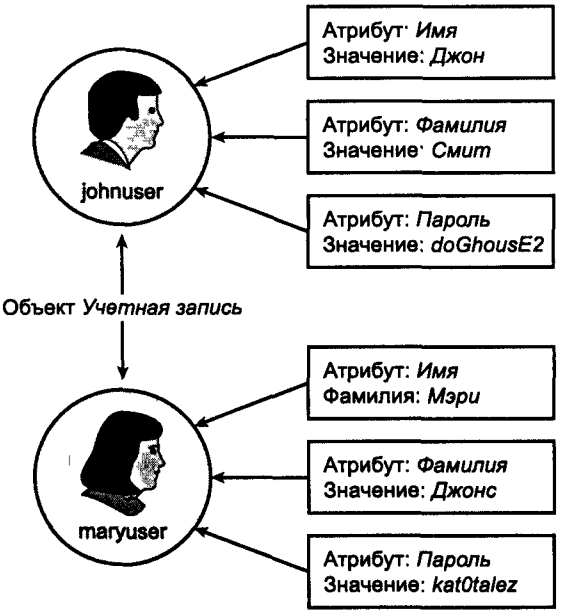


Рис 11.1 В каталоге хранятся объекты, имеющие атрибуты

Чтобы лучше понять концепцию каталогов и атрибутов, вернемся к примеру с каталогом телефонного справочника. В этом случае объектом является абонент или организация, а атрибутами — название, адрес, номер телефона и другая информация. Иными словами, атрибуты некоторым образом описывают объект.

Совет

Объекты каталога могут иметь много атрибутов. Одни из них обязательны (например, у каждой учетной записи должно быть имя пользователя), другие необязательны (например, некоторые учетные записи содержат поле для должности пользователя, однако оно может оставаться пустым)

Классы объектов определяют атрибуты, допустимые в классе, а также их место в структуре или иерархии каталога. Определение класса объектов с требуемыми и допустимыми атрибутами называется *схемой*. В некоторых сетевых операционных сис-

темах администратор может модифицировать или расширять схему для добавления новых классов объектов и атрибутов.

Что такое службы каталогов

Службы каталогов предоставляют средства хранения, обновления и поиска информации в каталогах, а также обеспечения их безопасности. Службы каталогов бывают *локальными* (ограниченными одним компьютером) или *глобальными* (обслуживающими многие компьютеры). Если информация службы каталогов распространяется на многие компьютеры, то такая служба каталогов называется *распределенной*.

Использование служб каталогов

Использование в сети служб каталогов предоставляет ряд преимуществ.

- Данные легко упорядочить.
- Легче обеспечить безопасность данных.
- Данные легко найти и получить к ним доступ.

Чтобы лучше понять преимущества использования служб каталогов, рассмотрим сначала традиционный способ получения доступа к сетевым ресурсам. В нем разделяемые файлы и каталоги хранятся на жестких дисках отдельных компьютеров или файловых серверов. Для подключения к разделяемому ресурсу пользователь должен знать, где он расположен.

Использование службы каталогов делает это требование необязательным. Разделяемые ресурсы публикуются в каталоге, поэтому для получения доступа к ресурсу пользователю не обязательно знать, на каком компьютере этот ресурс размещен физически. На рис. 11.2 показано диалоговое окно сетевого окружения Windows 2000. Как видно из рис. 11.2, существуют две возможности.

- **Просмотреть ресурсы сети Windows традиционным способом**. Так можно просмотреть разделяемые ресурсы каждого компьютера.
- **Просмотреть каталог**. Таким образом можно просмотреть все ресурсы, опубликованные в Active Directory.

Пространство имен каталога

Тип *пространства имен* каталога означает способ идентификации его объектов. В службах каталогов используются два разных типа пространств имен:

- однородный (плоский);
- иерархический.

В службе каталогов Windows NT (NTDS) и в базе данных *bindery* сетей NetWare 3.*x* используется однородное пространство имен. В более современных службах каталогов используется иерархическая структура, которую часто называют *деревом*. Иногда ее называют также *обращенным деревом*, потому что его корень находится сверху. Такой тип структуры используется в большинстве файловых систем компьютеров.

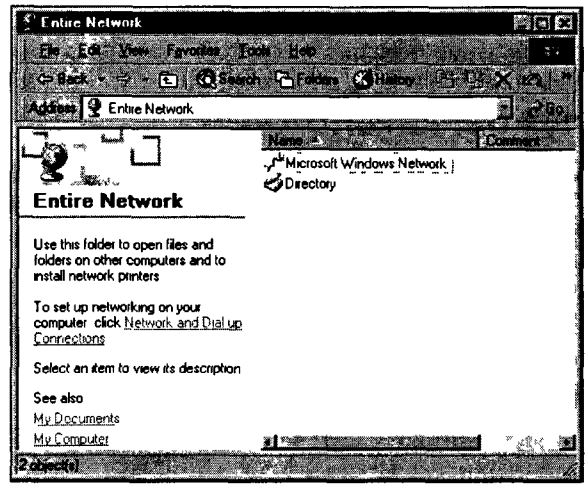


Рис. 11.2. С помощью сетевого окружения Windows 2000 можно просмотреть ресурсы сети как традиционным способом, так и с помощью службы каталогов

Древовидная структура каталога

В древовидной структуре объект может иметь один родительский объект и произвольное количество дочерних объектов. *Родительский объект* расположен в дереве непосредственно над данным объектом, а *объект-потомок (дочерний)* — под ним (рис. 11.3).

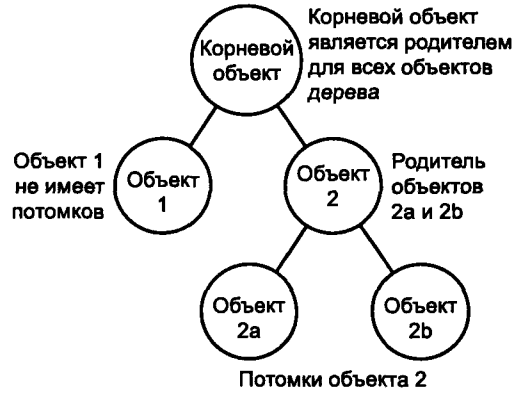


Рис. 11.3. Иерархическое дерево с родительскими и дочерними объектами

Соглашение об именах каталогов

На рис. 11.3 видно, что имена потомков объекта 2 содержат имя родителя. Это правило обязательно для *непрерывного пространства имен*. Как упоминалось в главе 8, "Сетевые протоколы и службы", таким способом структурированы имена DNS (Domain Name System). Иерархическая структура имен DNS обусловлена тем, что в этой службе каталогов используется иерархическое пространство имен. Пространство имен DNS показано на рис. 11.4.

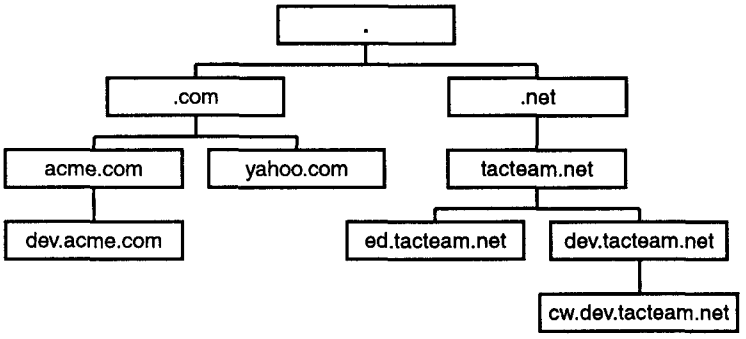


Рис. 11.4. В службе каталогов DNS используется иерархическое пространство имен

На рис. 11.4 корень DNS представлен точкой. Под корнем расположены два потомка — домены `.com` и `.net`. Каждый из этих доменов имеет потомков, каждый из которых тоже имеет потомков и т.д. Обратите внимание: в состав имен каждого следующего поколения входят полные имена родителей.

Замечание

Домен DNS, используемый в Internet, имеет почти ту же структуру, что и домен Active Directory в системе Windows 2000. Отличие состоит лишь в том, что в домене DNS в Internet нет точки в качестве корневого домена. Active Directory рассматривается далее в главе.

Аналогия с деревом может быть продолжена. Например, в терминологии NDS компании Novell последний объект ветви называется *листовым объектом*. NDS рассматривается несколько ниже в главе.

Стандарты служб каталогов

Для обеспечения межоперационного взаимодействия методы именования и получения доступа к объектам различных служб каталогов должны совпадать. Если бы не было стандартов, каждое приложение имело бы свои каталоги. Это привело бы к нерациональному использованию дискового пространства и невозможности применения базы данных одного поставщика в приложениях других поставщиков.

Соблюдение стандартов позволяет поставщикам служб каталогов обеспечить их совместимость в широком диапазоне других платформ и типов служб каталогов.

В этом разделе рассматриваются следующие стандарты служб каталогов:

- спецификации OSI X.500;
- DAP;
- LDAP.

X.500

Спецификации X.500 определяют стандарты EDS (Electronic Directory Service) в ISO 9594. Службы каталогов, описанные в X.500, разработаны для совместной работы со службами сообщений X.400.

Каталог, удовлетворяющий требованиям X.500, имеет три первичных компонента.

- **DSA (Directory System Agent — агент системы каталогов).** Программа, управляющая данными каталога.
- **DUA (Directory User Agent — агент пользователей каталога).** Программа, предоставляющая пользователям доступ к службам каталогов.
- **DIB (Directory Information Base — информационная база каталога).** Служит центральным *хранилищем данных*, или базой данных, в которой хранится информация каталога.

Стандарты X.500 определяют, как информация хранится в каталоге и как пользователи и операционные системы компьютеров получают к ней доступ. Система обеспечения безопасности данных, способы именования объектов, репликация данных каталогов между серверами — все это определяется стандартом X.500.

Спецификации X.500 определяют структуру каталога как обращенное дерево и задают иерархическую структуру базы данных. В службе каталогов, удовлетворяющей требованиям X.500, используется протокол DAP, рассматриваемый в следующем разделе.

Протоколы DAP и LDAP

С помощью протокола DAP (Directory Access Protocol) агент DUA взаимодействует с агентом DSA. Протокол DAP определяет способы поиска данных в каталоге и способы считывания, изменения, добавления и удаления записей каталога.

DAP — мощный протокол, однако он приводит к повышенной загрузке линий служебными (протокольными) сигналами. Для упрощения доступа к каталогам, определяемым стандартами X.500, было разработано его подмножество — протокол LDAP (Lightweight Directory Access Protocol). Со временем LDAP стал наиболее распространенным стандартом каталогов различных поставщиков. LDAP потребляет меньше системных ресурсов, чем DAP, кроме того его легче реализовать. Его текущая версия — LDAPv3.

Спецификации LDAPv3

В документе RFC 2251 описаны следующие спецификации LDAPv3:

- модель протокола LDAP;
- модель данных LDAP;
- общие элементы протокола, такие, как соглашение об именах, типы атрибутов, описания и операции связывания, поиска, добавления, изменения и удаления.

Что нового появилось в LDAPv3

По сравнению с предыдущими версиями LDAP в протокол LDAPv3 внесено несколько важных изменений. Главное внимание было уделено повышению безопасности новой версии. В протоколе LDAPv3 при передаче данных между клиентом и сервером поддерживается система шифрования SSL (Secure Socket Layer) и аутентификация сертификатов согласно X.509. Протокол LDAPv3 поддерживает передачу сервером запроса клиента LDAPv3 другому серверу, если первый не может ответить на запрос сам.

Еще одна новинка — поддержка Unicode. Это позволяет применять в атрибутах каталогов символы практически любого языка, что значительно облегчает работу с каталогами в разных странах.

Соглашение об именах объектов LDAP

В каталогах, удовлетворяющих LDAP, применяется соглашение об именовании объектов, определяемое стандартом X.500. В соглашении используется понятие *уникального имени* (*Distinguished Name — DN*). С помощью DN задается путь к объекту в структуре каталога. Имя DN выглядит примерно так:

```
DC=net DC=tacteam UO=training CN=Users CN=John Doe
```

Атрибуты имени в этом примере объясняются в табл. 11.1.

Таблица 11.1. Атрибуты DN и их описание

Атрибут DN	Описание
DC	Имя компонента домена
OU	Организационный модуль
CN	Общее имя

В таких службах каталогов, как Active Directory, может использоваться также *относительно уникальное имя* (*Relative Distinguished Name — RDN*), которое является атрибутом объекта. В предыдущем примере общее имя John Doe, являющееся атрибутом объекта, — это RDN.

Одно и то же RDN могут иметь несколько объектов каталога. Например, в каталоге могут быть два пользователя с RDN John Doe, но только если у них разные OU или домены. Однако два объекта никогда не могут иметь одинаковые DN.

Службы каталогов, удовлетворяющие LDAP и совместимые с ним

Первая реализация LDAP, выполненная в университете штата Мичиган, приобрела широкую популярность во всем мире. Благодаря тому что LDAP (в отличие от DAP) был разработан для TCP, он стал стандартом служб каталогов Internet.

Среди распространенных реализаций LDAP можно назвать Banyan StreetTalk, Netscape Directory Server, Alta Vista Directory и Lucent Internet Directory Server. Удовлетворяющие LDAP каталоги могут быть согласованы друг с другом, даже если они созданы разными компаниями-производителями.

Как NDS компании Novell, так и Active Directory компании Microsoft поддерживают клиентские программы LDAP. В них используется соглашение об именах стандарта X 500, однако ни одна из них не удовлетворяет этому стандарту полностью. Службы каталогов, поддерживающие клиентские программы LDAP, называются *совместимыми с LDAP*.

Межоперационное взаимодействие LDAP

Популярность каталогов LDAP объясняется не только возможностью межоперационного взаимодействия со всеми совместимыми с LDAP каталогами, но и возможностью их использования как интерфейса с каталогами, полностью удовлетворяющими требованиям стандарта X.500.

В настоящее время существуют клиентские программы LDAP для DOS, Windows, Macintosh, UNIX и для системы X Window. Это делает каталоги LDAP и X.500 применимыми в коммерческих сетях, составленных из компьютеров с разными операционными системами.

Сети с каталогами

Службы каталогов становятся все более распространенной составной частью средств управления ресурсами в коммерческих сетях. Их значение все более возрастает благодаря распространению стандартов QoS, групповой обработки информации и средств автоматизации технологических процессов, требующих централизованного хранения данных и управления приложениями, разделяющими данные.

В прошлом коммерческие сети с большим количеством узлов нуждались в многочисленных отдельных каталогах. Различные приложения использовали собственные базы данных, в результате чего одну и ту же информацию приходилось вводить многократно в разных местах. По мере роста сетей и количества приложений такой метод становился все менее эффективным.

Службы каталогов, доступ к которым могут получать как приложения, так и пользователи, экономят не только время, но и дисковое пространство сетевых компьютеров. Еще один движущий мотив стандартизации служб каталогов — развитие электронной коммерции. Каталоги используются также в средствах обеспечения безопасности, основанных на шифровании данных и применении электронной подписи. Такие методы обеспечения безопасности называются *PKI* (*Public Key Infrastructure*).

Распространенные службы каталогов

Теперь, когда вы знакомы с некоторыми концепциями каталогов и служб каталогов, можно приступить к рассмотрению их конкретных реализаций. В сетях персональных компьютеров наиболее популярны две службы каталогов: NDS компании Novell и Active Directory компании Microsoft.

Служба каталогов NDS

В версиях NetWare вплоть до 3.*x* в качестве каталога использовалась база данных *bindery*. Основным недостатком этой службы каталогов был ее локальный характер. Каждый сетевой сервер NetWare должен был поддерживать собственную базу данных, а пользователь для доступа к ресурсам серверов должен был иметь учетную запись на каждом сервере.

Рассмотрим структуру базы данных NDS подробнее и обсудим вопросы, связанные с безопасностью и совместимостью NDS с различными операционными системами и типами оборудования.

Структура базы данных NDS

Начиная с версии 4, сети NetWare содержат NDS — глобальную базу данных, реплицируемую между серверами сети. С ее помощью пользователи могут зарегистрироваться на любом сервере и получать доступ к ресурсам любого сервера.

База данных NDS имеет иерархическую структуру в форме обращенного дерева. В ней могут храниться два базовых типа объектов: *контейнерные* и *листовые*. Контейнерный объект может содержать другие объекты. Листовой объект представляет собой конец ветви, т.е. разделяемый ресурс. Примерами листовых объектов являются разделяемые файлы и принтеры. Пример контейнерного объекта — модуль OU.

Безопасность NDS

Хранящиеся в NDS права доступа к объектам присвоены модулям OU, в которых размещены пользователи и группы. Права доступа пользователя можно изменить путем перемещения его учетной записи из одного модуля OU в другой. Например, если переместить учетную запись пользователя `johndoe` из OU `Trainting` в OU `Sales`, то данный пользователь больше не будет иметь прав доступа, присвоенных OU `Training`, однако получит права доступа `Sales`. Такой способ присвоения прав доступа существенно отличается от принятого в сетях Microsoft Windows NT и Windows 2000. (Далее в главе рассматриваются права доступа в Windows.)

Совместимость NDS с разными платформами

Служба NDS обычно ассоциируется с сетевыми операционными системами NetWare, однако она может выполняться на разных платформах. Компания Novell предоставляет NDS для следующих платформ:

- NetWare 4 и 5;
- Windows NT и Windows 2000 компании Microsoft;
- AIX и OS/390 компании IBM;
- Caldera OpenLinux;
- SCO UNIX;
- Sun Solaris.

Разработанная компанией Novell реализация NDS eDirectory предназначена для межоперационного взаимодействия интегрированных коммерческих приложений, использующих службы каталогов.

Для получения доступа к информации, хранящейся в каталогах, в NDS могут использоваться различные протоколы, включая следующие:

- NDAP (Novell Directory Access Protocol);
- LDAP;
- HTTP (при использовании Web-сервера);
- программный интерфейс ODBC (Open Database Connectivity);
- ADSI (Active Directory Services Interface).

Службы Active Directory компании Microsoft

С выпуском Windows 2000 Server компания Microsoft внесла в свои сетевые компоненты фундаментальные изменения. Эти изменения даже более радикальны, чем сделанные компанией Novell при переходе с NetWare 4 на NetWare 5. Главное новшество — появление службы каталогов Active Directory. Служба каталогов NDS компании Novell представляет собой службу, работающую совместно с сетевой операционной системой, а служба Active Directory работает как приложение, глубоко интегрированное в операционную систему.

Рассмотрим подробнее структуру базы данных Active Directory, интеграцию Active Directory с DNS (Domain Name System) и серверами Active Directory, а также процессы репликации информации Active Directory с одного контроллера домена на другой.

Структура базы данных Active Directory

Информация Active Directory хранится в трех файлах.

- База данных Active Directory.
- Файл журнала Active Directory.
- Совместно используемый раздел.

База данных — это каталог. В файле журнала записываются изменения, внесенные в базу данных. Совместно используемый раздел (иногда его называют Sysvol) содержит сценарии и *объекты стратегии групп* контроллеров доменов Windows 2000. *Стратегия групп* представляет собой набор средств, с помощью которых администраторы Windows 2000 управляют компьютерами пользователей, автоматически развертывают приложения и устанавливают права пользователей.

Домены Windows 2000

В основу логической структуры Active Directory положены модули, называемые *доменами*. Несмотря на совпадение терминов, домены Windows 2000 существенно отличаются от доменов Windows NT. Как в Windows NT, так и в Windows 2000 домен представляет область (или границу) обеспечения безопасности, администрирования и репликации. Однако в Windows NT используется плоская структура домена, а в Windows 2000 домены организованы в иерархическое *дерево доменов*.

Понятия иерархического дерева в Active Directory и NDS значительно отличаются. В NDS сеть не разделена на домены. В то же время сеть Windows 2000 может состоять из многих доменов, организованных в дерево. Кроме того, эти деревья, объединяясь с другими деревьями, могут образовывать *лес*. На рис. 11.5 показана структура доменов Windows 2000, содержащая два дерева доменов (с корневыми доменами `shinder.net` и `tacteam.net`), объединенных в лес.

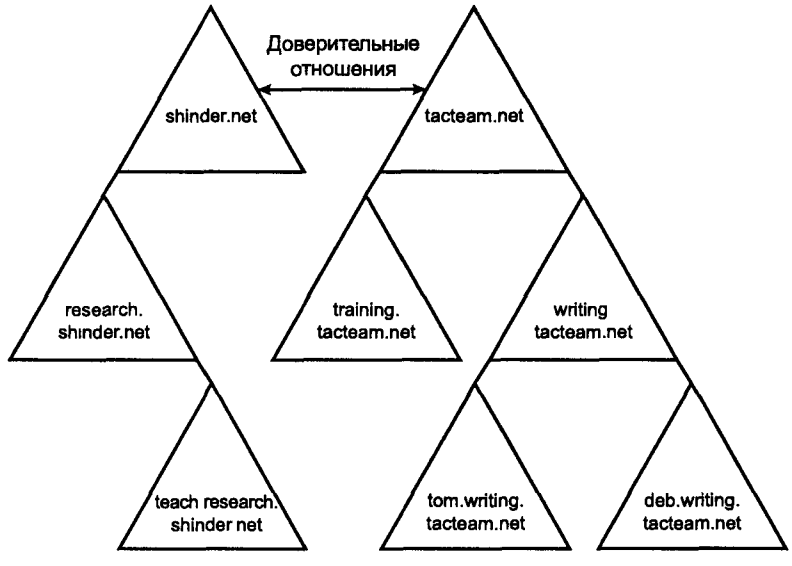


Рис. 11.5. Структура доменов Windows 2000 представляет собой иерархическое дерево

Преимуществом связывания деревьев доменов, имеющих отдельные непересекающиеся пространства имен, является возможность образования *доверительного отношения.* Рассмотрим доверительные отношения Windows 2000 и работу модулей OU в структуре доменов.

Доверительные отношения в Windows 2000

Между всеми доменами одного дерева и всеми деревьями одного леса автоматически установлено неявное *транзитивное доверительное отношение.* Это значит, что пользователи, принадлежащие одному домену, могут получать доступ к ресурсам другого домена (конечно, если их учетным записям присвоены соответствующие права доступа к этим ресурсам). Транзитивные доверительные отношения являются большим преимуществом сетей Windows 2000 по сравнению с Windows NT, в которых для достижения того же результата администратору приходилось вручную устанавливать односторонние доверительные отношения между каждой парой доменов.

Модули OU в сетях Windows 2000

Как и в NDS, в Active Directory для организации ресурсов в пределах домена используются модули OU. Административные права могут быть переданы отдельным OU. В противоположность этому в сетях Windows NT административные права можно присвоить только на уровне домена.

Службы Active Directory и DNS

В Active Directory используется соглашение об именах DNS (Domain Name System), причем работа Active Directory зависит от DNS. В каждой сети Windows 2000 должен быть сервер DNS. Кроме того, обновления зоны информации DNS могут совпадать с зонами репликации Active Directory, что значительно повышает эффективность традиционных методов обновления DNS.

Операционная система Windows 2000 поддерживает DDNS (Dynamic Domain Name System), в которой обновления базы данных DNS выполняются автоматически.

Серверы Active Directory

Чтобы можно было использовать Active Directory, как минимум один сервер должен быть конфигурирован как контролер домена. Для повышения отказоустойчивости рекомендуется устанавливать в домене более одного контроллера домена. Придать серверу Windows 2000 статус контроллера домена можно с помощью команды `dcpromo.exe`. Конфигурирование первого контроллера домена автоматически создает каталог этого домена.

В отличие от Windows NT, в Windows 2000 нет "первичного" контроллера домена. Все контроллеры домена содержат копии раздела Active Directory с атрибутами чтения и записи. С помощью процедур репликации информация, содержащаяся в этих копиях, постоянно обновляется и согласуется с другими копиями. Процесс репликации рассматривается далее в главе.

Мастера операций

В системе Windows 2000 не различаются первичные и вторичные контроллеры доменов. Однако во избежание коллизий в Windows 2000 все же оставлены некоторые функции, выполняемые только одним контроллером домена. Эти функции называются *операциями одного мастера.*

Например, должен быть только один контроллер домена, принимающий окончательное решение о пароле в случае конфликта. Такой конфликт может случиться, если на одном контроллере домена пароль изменился, но информация об этом еще не реплицирована на остальные контроллеры. Если в сети Windows 2000 есть контроллеры домена Windows NT, то должен быть единственный контроллер домена, служащий источником репликации. Контроллер домена, выполняющий эту функцию в сети Windows 2000 называется эмулятором PDC (Primary Domain Controller).

В сети Windows 2000 эмулятор PDC — это один из пяти *мастеров операций*. Каждый мастер операций является ролью контроллера домена, выполняемой только одним из контроллеров домена (или леса). Роли в пределах домена — это эмулятор PDC, мастер RID (Relative ID) и мастер инфраструктуры. Роли в пределах леса — мастер схемы и мастер именования домена.

Репликация в Active Directory

Репликацией называется процесс копирования данных с одного компьютера на другой (или другие) и согласование этих данных таким образом, чтобы они были идентичны во всех системах.

В Active Directory для копирования информации каталога между контроллерами домена в пределах домена используется *многомастерная репликация*. Изменения могут быть сделаны в любом контроллере домена. Затем изменения реплицируются на другие контроллеры доменов, но только не во время выполнения операции одного мастера.

Администраторы Windows 2000 могут выбирать стратегию репликации, определяющую, когда и как часто выполняется репликация каталогов. Это позволяет оптимизировать загрузку сетевых каналов. Управление расписанием репликации особенно важно, если контроллеры домена расположены на разных концах медленного канала, например в соединении глобальной сети с пропускной способностью 56 Кбит/с.

Безопасность Active Directory

У каждого объекта Active Directory есть список контроля доступа, содержащий все права доступа, ассоциированные с этим объектом. Право доступа может быть или явно предоставлено, или отменено отдельно для каждого пользователя либо группы.

Существует два типа прав доступа.

- **Присвоенные права доступа**. Явно предоставленное пользователю право сделать что-либо.
- **Наследованные права доступа**. Права доступа к дочерним объектам, унаследованные от родительского объекта.

Права доступа могут быть присвоены как отдельному пользователю, так и группе пользователей. В операционной системе Windows 2000 администратор может управлять процессом наследования и при необходимости отменять наследование. Это выполняется с помощью флажка Allow Inheritance... (Разрешить наследование...) в нижней части вкладки Security (Безопасность) диалогового окна свойств объекта (рис. 11.6).

Совместимость Active Directory

Служба Active Directory неразрывно связана с операционной системой и во всем зависит от нее, поэтому Active Directory может выполняться только на сервере Windows 2000. Однако вследствие совместимости Active Directory с LDAP клиенты LDAP

могут получать доступ к службе каталогов Active Directory, кроме того, Active Directory может обмениваться информацией с другими каталогами LDAP. Компания Microsoft предоставляет также инструменты переноса информации в Active Directory из других каталогов, например NDS.

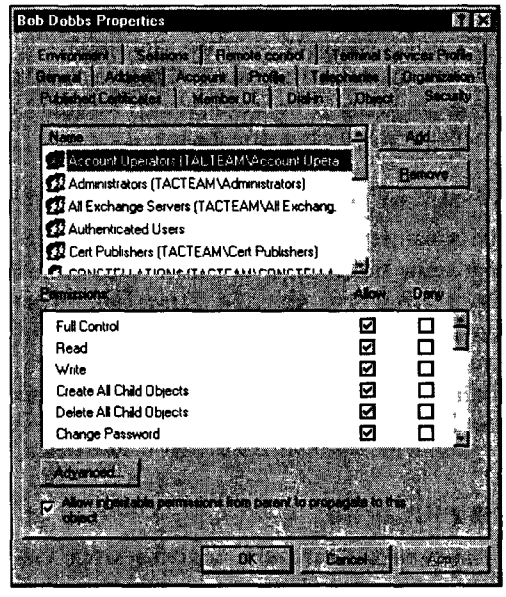


Рис. 11.6. Управление правами доступа к объекту Active Directory

Другие службы каталогов

Службы каталогов NDS и Active Directory хорошо знакомы пользователям и администраторам сетей. Однако стоит уделить внимание и другим службам каталогов, используемым на различных платформах. Далее рассматриваются такие службы каталогов:

- OS/400 компании IBM;
- компании Sun;
- VINES StreetTalk компании Banyan;
- в Internet.

Служба каталогов OS/400 компании IBM

Компания IBM предоставляет для своих мэйнфреймов совместимую с LDAP службу каталогов, входящую составной частью в SecureWay Directory, которая называется также службой каталогов OS/400. Это позволяет выполнять на машинах OS/400 совместимые с LDAP приложения (например, программы электронной почты), в которых службы LDAP используются для поиска адресов.

Клиентские программы LDAP OS/400 поддерживают взаимодействие с операционными системами компании Microsoft, а служба каталогов SecureWay Directory может выполняться в системах OS/300, OS/400, AIX, Solaris и Windows NT.

Службы каталогов компании Sun

Компания Sun предоставляет для операционной системы Solaris службу каталогов SDS в составе сервера Solaris Easy Access Server. Глобальная служба каталогов SDS поддерживает глобальную передачу сообщений и удаленную аутентификацию и предоставляет распределенный корпоративный каталог, управляющий сетевыми ресурсами.

Служба каталогов SDS поддерживает многие протоколы и псевдонимы имен. Ее каталог можно расширять до миллиона записей. Служба каталогов SDS совместима с LDAPv3 и доступна с Web-броузера и персонального компьютера Windows. Управление SDS выполняется посредством Java-интерфейса.

Служба каталогов StreetTalk компании Banyan

Одна из первых реализованных служб каталогов — VINES StreenTalk. В ее более поздние реализации добавлены поддержка LDAP и средства взаимодействия с приложениями, использующими каталоги. Служба StreetTalk переносима на платформы NetWare, UNIX и Windows NT. Перенос позволяет разделять общие каталоги сетей на этих платформах с каталогами сетей VINES.

1 мая 2000 года компания Banyan прекратила поддержку своего программного продукта и сосредоточила внимание на консультационной деятельности в области электронной коммерции.

Службы каталогов в Internet

В узлах электронной коммерции каталоги используются для хранения информации о товарах и отслеживания их продаж. В настоящее время существует огромное количество служб каталогов, работающих на индивидуальных узлах Internet. Например, узел `www.switchboard.com` предоставляет каталог с разнообразной информацией о коммерческих организациях, товарных запасах и т.д.

Однако глобальной службы каталогов, охватывающей всю Internet не существует. Разработкой такой глобальной службы каталогов на основе стандартов LDAP в настоящее время занимается организация IETF (Internet Engineering Task Force).

Резюме

В этой главе представлен обзор используемых в компьютерных сетях служб каталогов. Вы узнали, что каталоги — это базы данных, организующие информацию о ресурсах в логические структуры. Описаны способы хранения, поиска и обеспечения безопасности информации с помощью служб каталогов.

Рассмотрены также пространства имен каталогов, определяющие способ идентификации имен объектов, хранящихся в каталогах. Вы узнали, что пространство имен может быть плоским (как в Windows NT или в базе данных *bindery* сетей NetWare) или иерархическим (как в Active Directory или NDS).

Представлены распространенные структуры обращенного дерева, используемые в иерархических каталогах. В них обозначение объекта как "родительского" или "дочернего" зависит от его положения в дереве и положения, с которого рассматривается объект. Если в состав имен дочерних объектов входят имена родительских объектов, то пространство имен называется непрерывным.

Кроме того, описаны распространенные стандарты служб каталогов — OSI X.500, DAP и LDAP. Рассмотрены наиболее популярные службы каталогов, причем основное внимание уделено службам каталогов NDS компании Novell и Active Directory компании Microsoft.

Рассмотрены также другие службы каталогов: OS/400 Directory Services компании IBM, SDS и теперь уже устаревшая StreetTalk компании Banyan. Описано межоперационное взаимодействие служб каталогов на основе протоколов LDAP и приведены перспективы создания глобальной службы каталогов, охватывающей всю Internet.

Теперь вы лучше понимаете, как в сетевых операционных системах для облегчения доступа клиентов к сетевым ресурсам используются службы каталогов. В следующей главе рассматривается клиентская сторона сетей клиент/сервер и некоторые базовые понятия конфигурирования и работы с наиболее популярными клиентскими операционными системами.

Рекомендуемые источники

Дополнительная информация о стандартах OSI X.500 есть в учебнике X.500 по адресу: `www.opendirectory.com/Whitepapers/x500tut.html`.

Дополнительная информация о протоколе LDAP представлена на Web-узле LDAP по адресу: `www.innosoft.com/ldapworld`.

Дополнительную информацию о службе NDSv8 можно найти по адресу: `www.nwconnection.com/may.99/nds859/index.html`.

Дополнительная информация о службе каталогов Active Directory есть в руководстве по Active Directory по адресу: `www.worldowindows.com/w2000/active_directory.htm`.

Дополнительную информацию о глобальной службе каталогов Internet можно найти по адресу: `www.isoc.org/HMP/PAPER/173/html/paper.html`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Каталог (службы каталогов) — это ... (выбрать определяющее понятие).
   - **а.** Файл.
   - **б.** Папка.
   - **в.** База данных.
   - **г.** Способ хранения.
2. К какому типу принадлежит база данных, информация которой распространяется службой каталогов на многие компьютеры?
   - **а.** Организованная база данных.
   - **б.** Распределенная база данных.
   - **в.** Безопасная база данных.
   - **в.** Опубликованная база данных.

в. Между ними существует одностороннее нетранзитивное доверительное отношение.

г. Между ними может существовать доверительное отношение, только если оно явно создано администратором.

10. Где хранятся все права доступа, ассоциированные с объектом Active Directory?

а. В дочернем объекте.

б. В стратегии репликации.

в. В списке контроля доступа.

г. В модуле OU.

Глава 12

Клиентские операционные системы

В серверных сетях *клиентские* компьютеры устанавливают соединение и получают доступ к ресурсам, расположенным на сервере. На клиентских компьютерах выполняются различные, отличающиеся от серверных операционные системы (обычно они называются *настольными операционными системами* или *клиентскими операционными системами*).

В этой главе рассматриваются следующие наиболее популярные клиентские операционные системы:

- MS DOS;
- Windows 3.*x*;
- Windows 95 и Windows 98;
- Windows NT Workstation;
- Windows 2000 Professional;
- Linux и UNIX;
- Macintosh;
- OS/2.

Необходимо понимать, что на клиентском компьютере не обязательно должна быть установлена клиентская операционная система того же поставщика, что и серверная операционная система, установленная на сервере, с которым соединен клиентский компьютер. Например, клиенты Windows 98 могут устанавливать соединение с серверами UNIX или Linux. Некоторые поставщики сетевых операционных систем, например NetWare, даже не разрабатывают собственные клиентские операционные системы.

Основы операционных систем

Операционная система — это базовая программа, первоначально загруженная в компьютер. Операционная система управляет всеми другими программами (*приложениями*), выполняющимися на компьютере, включая следующие:

- рабочие программы, такие, как текстовые редакторы или электронные таблицы;
- сетевые приложения, такие, как программы электронной почты или Web-броузеры;
- мультимедийные программы, воспроизводящие аудио- и видеофайлы;
- утилиты, с помощью которых можно управлять операционной системой, файлами и приложениями;
- справочные программы, такие, как словари или энциклопедии;
- игры.

Операционная система выполняет *служебные программы* (или *службы*), которые приложения запрашивают посредством соответствующего программного интерфейса API (Application Programming Interface). В многозадачной среде операционная система выделяет одновременно выполняющимся приложениям необходимые им ресурсы памяти и процессорного времени. Фактически операционная система работает как посредник между приложениями и физическими устройствами компьютера.

Довольно часто приложения представляют собой добавляемые программы, которые покупаются отдельно и устанавливаются в операционную систему. Примерами таких приложений могут служить программы текстовых редакторов, электронных таблиц и баз данных, программное обеспечение просмотра и обработки графической информации и т.д. В поставку операционных систем входит довольно много встроенных приложений, таких, как системные инструменты (например, утилиты копирования и управления дисками), средства конфигурирования и базовые рабочие программы, например текстовые редакторы, калькуляторы, простые редакторы изображений и т.д.

Интерфейсы операционных систем

Пользователь взаимодействует с операционной системой и программами посредством *интерфейса пользователя*. Интерфейсы пользователя делятся на две категории: текстовые и графические. Графические интерфейсы пользователя часто называют GUI (Graphical User Interface). Рассмотрим характеристики обоих типов интерфейса.

Текстовые интерфейсы

В первых операционных системах персональных компьютеров использовались текстовые интерфейсы (иногда их называют *символьными*). В них пользователь вводил команды в командной строке с помощью клавиатуры. Примерами операционных систем с текстовыми интерфейсами являются MS DOS и UNIX/Linux. На рис. 12.1 приведен пример текстового интерфейса пользователя.

В большинстве текстовых операционных систем могут выполняться графические *оболочки*, предоставляющие пользователю интерфейс GUI. Например, для операционной системы Linux разработаны графические оболочки X Window и KDE. В системе MS DOS использовалась графическая оболочка DOSSHELL.

Графические оболочки существенно отличаются от истинно графических операционных систем, так как оболочка — это отдельная программа, выполняющаяся *в* операционной системе. Операционная система может работать без оболочки, однако оболочка не может работать без операционной системы.



Рис. 12.1 В операционной системе Linux можно зарегистрироваться с помощью текстового интерфейса пользователя

Замечание

Иногда Windows 3.*x* называют операционной системой, но фактически это оболочка, выполняющаяся в MS DOS.

Текстовые операционные системы, как правило, более быстродействующие и требуют меньше системных ресурсов, чем графические.

Графические интерфейсы

Такие операционные системы, как Windows 9*x* и выше, Macintosh и OS/2, основаны на GUI. Интерфейс GUI выводит на экран как изображения, так и текст. В GUI пользователь выполняет большинство команд и функций, манипулируя *пиктограммами*, которые служат графическим представлением программ, файлов и других элементов. Пример GUI приведен на рис. 12.2.

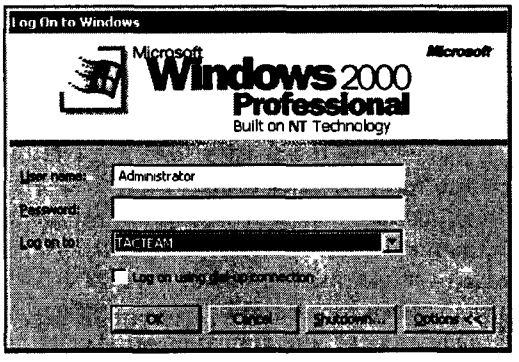


Рис. 12.2. Регистрация в Windows 2000 выполняется с помощью GUI

Интерфейсы GUI более дружественны к пользователю, чем текстовые, потому что люди воспринимают визуальную информацию значительно легче, чем текстовую. С помощью GUI пользователь может, например, переносить, или копировать файлы путем *перетаскивания* изображения файла с одного места в другое.

Однако GUI все же присущи определенные недостатки. Например, GUI замедляют формирование ответа системы, а вывод на экран сложных изображений увеличивает требования к системным ресурсам (памяти, производительности процессора и др.). В некоторых случаях взаимодействие с графическими элементами оказывается менее удобным, чем с текстовыми командами. Кроме того, в GUI трудно перемещаться, если к компьютеру не подключено специальное устройство — мышь или трекбол.

Для устранения этих недостатков операционные системы на основе GUI обычно дополнительно предоставляют командную строку в качестве альтернативы GUI. В ней можно набирать команды выполнения каких-либо административных задач. Например, в Windows NT встроенную программу резервного копирования можно запускать двумя способами: выбрать ее пиктограмму в меню или ввести команду `ntbackup.exe` в командной строке.

Использование команд

С помощью *команды* пользователь сообщает операционной системе, что она должна выполнить определенную программу. В текстовом интерфейсе команда вводится в командной строке как последовательность символов, а в интерфейсе GUI для выполнения команды нужно щелкнуть (или дважды щелкнуть) кнопкой мыши на пиктограмме или команде меню. В каждом из этих случаев поданная команда интерпретируется или обрабатывается по правилам какого-либо *языка программирования* (например, ассемблер, C или Java), на котором написана операционная система. Затем команда преобразуется в последовательность команд *машинного языка*, состоящую из нулей и единиц. И наконец, эти команды машинного языка выполняет процессор.

Чувствительность команд к регистру

Используемые в некоторых операционных системах (например, в UNIX) файловые системы *чувствительны к регистру символов*. Однако даже в операционных системах (например, в Windows), файловые системы которых нечувствительны к регистру, некоторые команды и аргументы команд все же зависят от регистра. Например, команда Windows `nbstat` с флагом `-r` и `-R`.

Важность соблюдения синтаксиса

Чтобы команда была выполнена правильно, она должна быть введена с точным соблюдением правил *синтаксиса*, определяющих структуру команды. Синтаксис команды определяет порядок слов, правила использования пробелов, расстановку служебных символов, а иногда использование символов верхнего регистра.

Синтаксис — это раздел грамматики, который изучает строение предложения. Например, в типичном предложении английского языка сначала записывается подлежащее, затем сказуемое и только после них дополнение. Имена прилагательные и наречия обычно записываются перед существительным или глаголом.

Допустим, человеку, не знакомому с английским языком, понадобилось составить какую-либо фразу по-английски. Сначала он составит эту фразу на родном языке, за-

тем возьмет словарь и заменит слова своего языка английскими словами При этом принятый в английском языке порядок слов, естественно, будет нарушен Тем не менее люди, знающие английский язык, скорее всего поймут, что хотел сообщить человек, составивший эту фразу

Однако в мире компьютеров дела обстоят значительно хуже Например, команда копирования файла с гибкого диска

```
copy имя_файла a: c:
```

ошибочно записана как

```
имя_файла copy a: c:
```

В таком случае компьютер не поймет и не выполнит эту команду

Различие результатов объясняется тем, что люди думают, а компьютеры только вычисляют Следовательно, команда должна точно соответствовать синтаксическим правилам, вплоть до пробелов между словами Например, если в командной строке Windows 2000 ввести `netview`, то компьютер возвратит только сообщение об ошибке, а если ввести `net view` (с пробелом), то на экран будет выведен список серверов в сети

Использование аргументов

Большинство команд операционной системы могут иметь дополнительные параметры — *аргументы*, или *флаги* Например, если команду `net view` ввести без аргументов, то на экран будет выведен список компьютеров под управлением операционной системы Microsoft (листинг 12 1)

Листинг 12.1. Команда `net view` без аргументов выводит на экран список серверов под управлением ОС Microsoft

```
C:\>net view
Server Name            Remark
------------------------------------------------------------------------
\\CONSTELLATION
\\CONSTITUTION
\\DELTA-FLYER
\\DS2000
\\EXETER
The command completed successfully.
```

Если в конец команды добавить аргумент (после чего она примет вид `net view /network:nw`), то на экран будет выведен список серверов под управлением операционной системы NetWare, как показано в листинге 12 2

Листинг 12.2. Команда `net view` с аргументом выводит на экран список серверов под управлением ОС NetWare

```
C:\>net view /network:nw
Resources on NetWare or Compatible Network
------------------------------------------------------------------------
-
\\DALTAC
\\NETGUY
The command completed successfully.
```

Чтобы увидеть синтаксис и параметры команды, нужно в командной строке ввести данную команду, подставив вместо параметров знак вопроса, как показано в листинге 12.3. Чтобы вывести на экран список всех команд операционной системы, нужно ввести в командной строке команду `help`. В UNIX можно получить доступ к справочной системе в реальном времени, для этого достаточно ввести в командной строке команду `man`.

Листинг 12.3. Если в командной строке ввести команду со знаком вопроса, то на экране появятся синтаксис и параметры команды

```
C:\>net view ?
The syntax of this command is:
NET VIEW [\\computername [/CACHE] : /DOMAIN[:domainname]]
NET VIEW /NETWORK:NW [\\computername]
```

Команды на разных языках

В некоторых случаях команда имеет один и тот же вид в разных операционных системах. Например, команда `arp` выводит на экран кэшированную информацию о протоколе ARP (Address Resolution Protocol) на компьютерах с установленным TCP/IP, независимо от типа операционной системы — Windows NT/2000, Windows 95/98, UNIX или Linux.

В то же время некоторые команды в разных операционных системах записываются по-разному. В табл. 12.1 приведены команды просмотра конфигурационной информации TCP/IP. Как видно из таблицы, написание команды зависит от типа операционной системы.

Таблица 12.1. Команды просмотра конфигурационной информации TCP/IP

Операционная система	Команда
Windows NT и Windows 2000	`ipconfig`
Windows 95 и Windows 98	`winipcfg`
Linux и UNIX	`ifconfig`
NetWare	`config`

Общие команды DOS

Все операционные системы Windows поддерживают командную строку, в которой можно вводить команды MS DOS. В Windows 9*x* для открытия окна командной строки нужно выбрать команду Start⇨Run (Пуск⇨Выполнить) и в появившемся окне ввести **command**.

В системах Windows NT/2000 для этого нужно ввести **cmd**. При этом открывается "диалоговое окно DOS", содержащее командную строку, в которой можно вводить команды. (Диалоговое окно DOS иногда называется "приглашением `C:`", хотя в разных конфигурациях компьютера текущий каталог может отличаться от `C:.`)

В табл. 12.2 приведены наиболее часто используемые команды DOS.

Таблица 12.2. Наиболее часто используемые команды DOS

Команда	Выполняемое действие
`dir`	Вывод списка файлов текущего каталога
`cd` *имя_каталога*	Изменение текущего каталога
`time`	Вывод на экран или установка системного времени
`date`	Вывод на экран или установка даты
`copy`	Копирование файлов
`diskcopy`	Копирование содержимого одного гибкого диска на другой
`attrib`	Вывод на экран или изменение атрибутов файла
`find` *текстовая_строка*	Поиск текстовой строки в файле
`help`	Вывод на экран списка доступных команд и их функций

Команды и файлы подсказки

В состав операционных систем на основе графического интерфейса обычно входят так называемые *справочные файлы*. Они могут поставляться в формате `.pdf`, разработанном для облегчения просмотра и печати, в формате HTML, допускающем использование перекрестных ссылок, или в формате `.hlp`. В справочную систему входят поисковые механизмы. Например, в состав операционной системы Windows 2000 входит расширенная справочная система с перекрестными ссылками (рис. 12.3), в которой справку по необходимому вопросу можно найти с помощью ключевых слов, индексированных списков или подробного содержания всей справочной системы. Поисковые механизмы значительно облегчают поиск и печать необходимых сведений

Файлы и файловые системы

Компьютерная информация содержится в единицах хранения, называемых *файлами*. Файл представляет собой совокупность данных, которыми можно управлять одной командой, например командой просмотра, копирования, удаления или перемещения. Каждый файл должен иметь имя, уникальное в том месте, где он расположен

Существует довольно много различных типов файлов, каждый из которых ассоциируется с определенным типом приложений, работающих с данным типом файла. Например, бухгалтерская информация хранится в файлах электронных таблиц. Письма и другая корреспонденция хранятся в файлах текстовых редакторов Картины художников хранятся в файлах `.bmp`, `.jpeg` и в других файлах графического типа.

Файлы различных типов создаются, открываются и обрабатываются с помощью разных типов приложений Например, файлы электронных таблиц обрабатываются с помощью таких приложений, как Excel или Lotus 1-2-3. Письма обрабатываются с помощью приложений WordPad, Notepad, Word или WordPerfect Файлы изображений можно обрабатывать с помощью приложения Paint, поставляемого в составе операционных систем Microsoft. Другими словами, тип файла *соответствует* программе или программам, предназначенным для обработки файлов этого типа

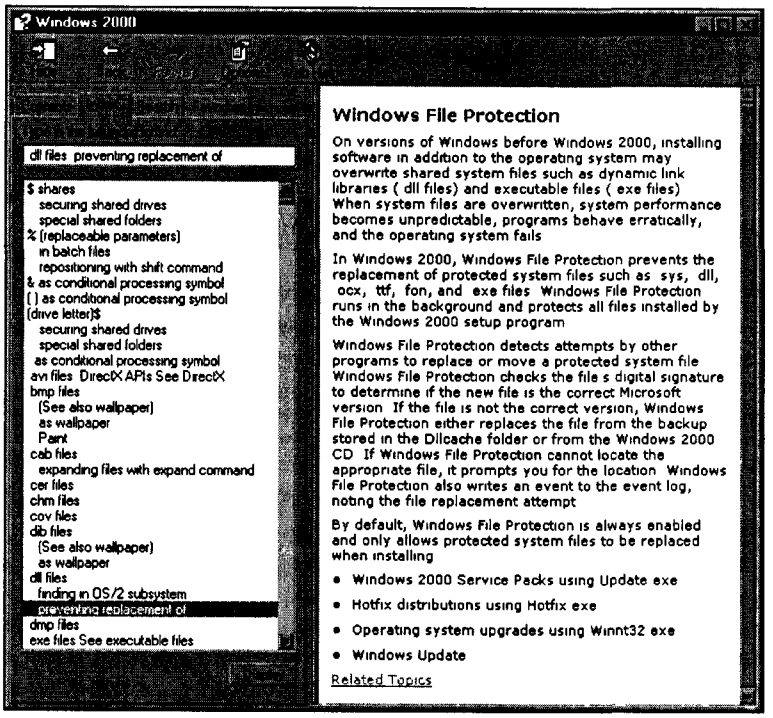


Рис 12 3 Каждая современная операционная система содержит подробную справочную систему с файлами подсказки

Расширения и типы файлов

Во многих операционных системах для определения типа файла и приложения, с помощью которого его можно обрабатывать, используется *расширение файла*, которое представляет собой суффикс из нескольких символов, следующих после точки. Например, расширение `.exe` в конце файла чаще всего обозначает выполняемый файл (т е. файл, содержащий программу) Расширение `.gif` обозначает графический файл, а `.htm` (или `.html`) — файл, созданный на языке HTML (HyperText Markup Language). В табл. 12 3 приведены наиболее часто используемые расширения файлов

Таблица 12.3. Общепринятые расширения файлов

Расширение файла	Тип файла	Описание	Ассоциированные приложения
`.avi`	Аудио и видео	Файл содержит видеофильм	Мультимедийные программы
`.bmp`	Растровое изображение	Графические файлы	Программы просмотра изображений
`.doc`	Документ	Документы Word	Программы Word
`.jpg`, или `jpeg`	Рисунок JPEG	Сжатые (уменьшенного размера) графические файлы	Программы просмотра изображений и Web-броузеры

Окончание табл. 12.3

Расширение файла	Тип файла	Описание	Ассоциированные приложения
`.gif`	Рисунки GIF (Graphics Interchange Format)	Графические файлы, могут совмещаться с анимацией	Программы просмотра изображений и Web-броузеры
`.hlp`	Help (Помощь)	Справочные файлы	Текстовые редакторы
`.htm`, или `.html`	HTML	Документы, содержащие гипертекстовые ссылки	Web-броузеры
`.ini`	Инициализации	Конфигурационные файлы	Используются операционной системой для установки параметров конфигурации, их можно просматривать текстовыми редакторами
`.mid`, или `.midi`	Звук MIDI (Musical Instrument Digital Interface)	Звуковые файлы, синтез музыки	Программы воспроизведения
`.pdf`	Формат переносимых документов	Текстовые и графические документы, которые можно распечатать	Adobe Acrobat
`.ra`	RealAudio	Файлы высококачественного аудио	RealPlayer
`.rtf`	Текстовый	Форматируемые текстовые файлы	Текстовые процессоры Word, или WordPad
`.tar`	Ленточные архивы	Архивные файлы UNIX	Команды UNIX
`.tif`, или `tiff`	Формат изображений	Графические файлы высокого качества	Программы просмотра изображений
`.wav`	Файлы звуковых сигналов	Звук (голос или музыка)	Программы воспроизведения

Файловые системы

Файлы, хранящиеся на жестком диске компьютера, должны быть организованы таким образом, чтобы при необходимости они могли быть найдены операционной системой или приложением. Способ размещения и поиска файлов называется *файловой системой.*

В разных операционных системах используются различные файловые системы. Некоторые операционные системы поддерживают несколько файловых систем. Например, в Windows 3.*x* используется только файловая система FAT16, а в Windows 2000 могут использоваться FAT16, FAT32 или NTFS. Эти и другие файловые системы рассматриваются позже в этой главе.

Файловая система определяет соглашения об именовании файлов и формат задания *пути*, или *маршрута* местоположения файла.

Соглашения об именовании файлов

Соглашения, или правила именования файлов, зависят от файловой системы и включают ряд ограничений.

- Максимально допустимое количество символов в имени файла.
- Максимальная длина расширения, или суффикса файла.
- Допустимость пробелов между словами в имени файла.
- Зависимость имени файла от регистра символов.
- Набор символов, которые можно использовать в имени файла.
- Формат задания пути.

Путь

Существует два вида путей.

- **Полный путь**. Содержит полную последовательность имен каталогов от корневого раздела до имени файла. Например, `c:\mydirectory\subdirectory1\myfile.ext`.
- **Относительный путь**. Содержит последовательность имен каталогов, начиная с текущего каталога операционной системы. Например, если текущим является каталог `mydirectory`, то относительный маршрут записывается как `subdirectory1\myfile.ext`.

В операционных системах Microsoft (MS DOS и Windows) и в OS/2 используется формат задания пути, показанный в предыдущих примерах. Символы обратной косой черты разделяют уровни структуры каталогов, или *дерева каталогов*. В то же время в операционной системе UNIX для этого используется *прямая* косая черта, например `/mydirectory/subdirectory/myfile`.

Замечание

В операционных системах Microsoft буква логического диска входит в состав пути, а в UNIX — нет.

В большинстве популярных операционных систем в файловой системе используется *древовидная* структура каталогов. В этой структуре корень дерева, расположенный в его вершине, представляет собой каталог верхнего уровня, в котором расположены все остальные файлы и каталоги. Иногда такую структуру называют *обращенным деревом*. Древовидная структура каталогов используется в операционных системах MS DOS, Windows (все версии), Macintosh, OS/2, UNIX и Linux.

В операционных системах Windows и Macintosh каталоги иногда называют *папками* (*folders*). Такое название помогает пользователям лучше усвоить структуру файловой системы благодаря аналогии с папками, используемыми в офисах для хранения документов. В продолжение этой аналогии файлы тоже часто называют *документами*.

Каталоги могут содержать подкаталоги, которые, в свою очередь, тоже могут содержать подкаталоги и т.д. Имена каталогов и файлов должны быть уникальными в пределах каталога, в котором они расположены. За пределами каталога уникальность имен не обязательна. Поясним это на таком примере. Допустим, в системе каталогов есть два каталога с именами `Dir1` и `Dir2`. Тогда в каждом из них одновременно может находиться подкаталог с именем `Sub1`. Однако в одном каталоге (например, в `Dir1`) не может находиться два подкаталога с одним и тем же именем (например, `Sub1`), иначе пути этих подкаталогов полностью совпадут и отличить их будет невозможно. В то же время в первом примере

маршруты разные: `C:\Dir1\Sub1` и `C:\Dir2\Sub1`. Заметим, что каталог может содержать подкаталог с тем же именем — `C:\Dir1\Dir1`.

Распространенные файловые системы

Рассмотрим некоторые наиболее распространенные файловые системы, используемые в современных операционных системах, включая такие:

- FAT (File Allocation Table);
- NTFS (NT File System);
- HPFS (High Performance File System);
- Macintosh HFS (Hierarchical File System);
- NFS (Network File System).

FAT. Существует несколько вариантов файловой системы FAT, включая FAT12, FAT16, FAT32 и VFAT. Название этих файловых систем обусловлено тем, что в них используется таблица размещения файлов (File Allocation Table), хранящаяся на жестком диске. В ней содержится информация о местах хранения файлов. Каждый файл хранится в виде отдельных *кластеров* — единиц хранения на диске. Кластер может содержать данные только одного файла, однако один файл может быть разбит на произвольное количество кластеров.

В настоящее время файловая система FAT12 почти не встречается, потому что она используется только при разбивке диска на очень маленькие разделы (об этом речь пойдет несколько позже). Версия FAT16 была создана для разделов большего размера, вплоть до 4 Гбайт.

В системе FAT16 можно форматировать довольно большие диски, однако дисковое пространство в ней используется неэффективно, потому что при больших разделах диска увеличиваются также размеры кластеров. Например, если раздел диска имеет объем 512 Мбайт, то размер кластеров (т.е. базовых единиц хранения) равен 8 Кбайт. Это значит, что, даже если объем файла равен 1 Кбайт, на диске он все равно займет 8 Кбайт, потому что в кластере могут храниться данные только одного файла. При этом 7 Кбайт дискового пространства окажутся утраченными. Для преодоления этого недостатка была разработана система FAT32. В этой 32-разрядной файловой системе используются кластеры меньшего размера при большем объеме дисков. В ней поддерживается разбивка дисков на разделы с размером вплоть до 2 Тбайт.

Преимуществом FAT16 является широкий набор поддерживающих ее операционных систем. Файлы системы FAT16 можно обрабатывать в MS DOS, OS/2, во всех версиях Windows и во многих других операционных системах. FAT32 поддерживается в Windows 95b (рассмотрим ее несколько ниже в главе), Windows 98, Windows ME и Windows 2000. Операционные системы MS DOS, Windows 3.*x* и Windows NT не поддерживают FAT32. Это ограничивает возможности применения FAT32 в системах с альтернативной загрузкой.

Компьютер с альтернативной загрузкой

Это такой компьютер, на котором установлено более одной операционной системы. Программа управления загрузкой предоставляет пользователю меню, в котором он может выбрать тип загружаемой операционной системы. В некоторых операционных системах программа управления загрузкой включена в дистрибутив установки операционной системы. Например, Windows NT и Windows 2000 содержат программу управления

загрузкой NT Boot Manager (параметры загрузки операционной системы задаются в файле `boot.ini`), а в Linux есть программа управления загрузкой LILO. Утилиты управления загрузкой других компаний (например, утилита System Commander) позволяют устанавливать на одном компьютере до 100 операционных систем.

Первоначально системы FAT были разработаны для MS DOS, в которой длина имени файла ограничена восемью символами с тремя символами расширения. *Виртуальная FAT (VFAT)* — это версия FAT, разработанная для Windows 95 для поддержки длинных имен файлов. Система VFAT реализована как *драйвер файловой системы*, расширяющий возможности FAT. В частности, VFAT поддерживает имена файлов длиной до 256 символов. Это позволяет создавать более осмысленные имена файлов, которые впоследствии будет легче узнать. Драйвер VFAT поддерживает также кэширование диска, которое улучшает производительность системы и уменьшает время чтения и записи на жесткий диск.

NTFS. Компания Microsoft разработала для Windows NT файловую систему NTFS, которая поддерживается только в операционных системах Windows NT и Windows 2000. Система NTFS была разработана для устранения некоторых присущих системам FAT недостатков, таких, например, как недостаточная поддержка безопасности на уровне файлов.

Перечислим некоторые новые возможности NTFS, устраняющие ограничения и недостатки FAT.

- **Обеспечение безопасности на уровне файлов посредством NTFS**. В системе NTFS для проверки прав доступа к файлам используется список контроля доступа независимо от того, откуда пользователь запрашивает данный файл — из сети или с этого же компьютера. Для сравнения: безопасность файлов FAT обеспечивается путем проверки прав доступа к *разделяемому ресурсу*, т.е. файл защищается от несанкционированного доступа из сети, но не с локального компьютера. В то же время файлы NTFS можно защитить одновременно и как разделяемый ресурс и на уровне файлов путем проверки системой NTFS права доступа к файлу.
- **Сжатие на уровне файлов**. Для сжатия данных в FAT должен быть сжат весь раздел диска, причем раздел превращается в один большой файл. Если этот файл испортится, то все данные на логическом диске могут оказаться утерянными. В то же время файлы NTFS можно сжимать отдельно. Если при этом один файл оказывается испорченным, это никак не затрагивает остальные файлы.
- **"Горячая" маркировка секторов**. С помощью этого метода система NTFS находит плохие секторы диска, переносит данные в хорошие секторы и помечает плохие как непригодные к использованию. Эти операции выполняются в процессе записи и чтения, пользователь их не замечает.
- **Поддержка формата Unicode**. В системе NTFS имена файлов могут содержать символы Unicode. Это значительно облегчает работу с компьютером на многих языках.
- **Поддержка огромных разделов**. NTFS поддерживает разделы объемом до 16 Эбайт (эксабайт).
- **Поддержка длинных имен файлов**. NTFS поддерживает длинные имена файлов и соответствующие им имена вида "восемь точка три", в которых под имя отводится до восьми символов и три символа под расширение (например, `file.doc`). Это обеспечивает обратную совместимость с MS DOS и Windows 3.*x*.

Замечание

Обратная совместимость означает способность файловой системы, операционной системы или приложений работать с файлами, созданными в более ранних версиях программного обеспечения. Для поставщиков программных продуктов очень важно обеспечить обратную совместимость, потому что в противном случае пользователи, переходящие на новую версию программы, потеряют все данные, созданные до этого.

Файловая система NTFS отслеживает кластеры файлов с помощью схемы *бинарного дерева каталогов*. Индексация бинарного дерева позволяет просматривать данные в упорядоченном виде. Отметим, что в FAT используется другая структура файлов — на основе *связанных списков*. Структура бинарного дерева обеспечивает более быстрый доступ к файлам в больших каталогах.

В системе FAT информация о кластерах файлов хранится только в таблице размещения файлов, в то же время в NTFS эта информация хранится в каждом отдельном кластере. По сравнению с FAT система NTFS меньше подвержена неблагоприятным последствиям *фрагментации файлов*, которая может существенно замедлить выполнение операций доступа к файлам на жестком диске.

Фрагментация файлов

На пустом, чистом, диске кластеры данных во время записи располагаются последовательно. Если файл не помещается в одном кластере, система размещает оставшиеся неразмещенными данные в следующем кластере. Если все данные каждого файла размещены в непрерывной последовательности кластеров, то говорят, что диск *нефрагментирован*.

Однако при копировании или перемещении данных неизбежно происходит фрагментация диска, потому что после каждого переноса обязательно остаются пустые кластеры посреди заполненных. Когда на диск записываются новые данные, они размещаются в первом доступном кластере. Если новый файл больше удаленного, то на месте удаленного размещается только часть нового файла, оставшаяся часть размещается в следующих доступных кластерах, которые могут оказаться отделенными от первой части другими заполненными кластерами.

Операционная система или приложение выполняют операции доступа к файлу значительно быстрее, если он размещен в кластерах, расположенных последовательно. Значит, фрагментация ухудшает производительность. Для предотвращения этого существуют специальные утилиты *дефрагментации* (например, Diskeeper компании Executive Software), которые, переставляя кластеры местами, располагают их последовательно. Такая операция уменьшает фрагментацию файлов и повышает производительность системы. В состав Windows 9x и Windows 2000 входят встроенные инструменты дефрагментации.

В состав Windows 2000 входит новая версия NTFS, называемая NTFS 5. Операционная система Windows NT может читать файлы NTFS 5, *только если* установлен пакет обновления Service Pack 4 или более поздний. Однако даже в этом случае Windows NT не может использовать расширенные средства NTFS 5 (например, шифрование файлов), поддерживаемые только в Windows 2000. По сравнению с NTFS 4 система NTFS 5 содержит много дополнительных средств и усовершенствований, включая приведенные ниже.

- Возможность шифрования файлов на жестком диске с помощью EFS (Encrypting File System).
- Поддержка средств хранения разреженных файлов. Под этим подразумевается способность хранить большие файлы, потребляя только необходимое дисковое пространство.
- Поддержка дисковых квот. Это означает, что администратор может выделять каждому пользователю определенный объем дискового пространства.
- Распределенное отслеживание связей — приложения сохраняют связи со своими файлами-источниками, когда последние по какой-либо причине перемещаются в другое место.
- Точки монтировки тома, позволяющие устанавливать том диска в каталоге NTFS. Таким образом можно обойти ограничение, вызванное тем, что количество томов не может превышать количество букв алфавита.
- Поддержка удаленного хранения, облегчающая хранение данных на непостоянных носителях (например, на ленточном накопителе).

Файловая система UNIX. Эта система организована как иерархия каталогов и подкаталогов, в которых размещаются файлы.

В системе UNIX корневой каталог представлен символом косой черты (/). Таким образом, путь каталога выглядит как `/dir2/subdir1`, т.е. каталог `subdir1` размещен в каталоге `dir2`, который размещен в корневом каталоге.

Система каталогов UNIX расположена непосредственно под корневым каталогом. Каталоги содержат файлы, используемые операционной системой. Ниже перечислены каталоги, входящие в стандартный набор.

- `/bin`. Содержит *выполняемые двоичные* файлы, т.е. команды и утилиты, используемые ежедневно.
- `/dev`. Содержит специальные файлы, представляющие физические *устройства*, такие, как принтеры.
- `/etc`. Содержит команды и файлы системного администрирования.
- `/lib`. Содержит *библиотеки*, используемые программами.
- `/tmp`. Содержит *временные* файлы, удаляемые при перезагрузке системы.
- `/usr`. Содержит *домашние каталоги* пользователей и другие файлы, например справочные.

Ядро операционной системы загружается вместе с операционной системой. Корневой каталог UNIX содержит файл ядра и *программу самозагрузки* — небольшую программу, которая начинает загружать операционную систему.

В именах системных файлов UNIX пробелы между символами не допускаются. В системах Windows можно записать имя файла, например `Joe Brown Memos`, однако в UNIX его придется переименовать в `JoeBrownMemos`, `Joe_Brown_Memos` или `Joe-Brown-Memos`.

В системе UNIX внутри имени файла можно использовать точки. Например, файл может называться `Joe.Brown.Memos`. То же самое можно делать и в 32-разрядных версиях Windows, однако в MS DOS и в Windows 3.*x* допускается использование только одной точки, все символы (до трех символов) после точки интерпретируются как расширение файла.

Имена файлов UNIX могут содержать до 255 символов. Использование некоторых символов (включая #, /, ?, ", ', [и]) не допускается, так как для операционной системы они имеют специальное значение.

Замечание

Символ подчеркивания (_) можно использовать в именах файлов, однако делать это не рекомендуется. Если символ подчеркивания встретится в имени компьютера, каталога, файла или другого ресурса, разделяемого посредством Internet, то сервер DNS не сможет преобразовать такое имя в IP-адрес.

Для пользователей главное отличие между файловыми системами UNIX и Microsoft состоит в *чувствительности к регистру символов*. В DOS и Windows имя файла `mydocuments` — это то же, что и `MyDocuments` или `MYDOCUMENTS`. В то же время файловая система UNIX интерпретирует эти имена как различающиеся — в каталоге могут одновременно находиться три разных файла с этими именами.

Путешествуя по Web, вы, наверное, заметили, что ошибочный регистр символа в URL иногда не приводит к ошибке, а иногда броузер попадает в другой Web-узел. Это объясняется тем, что на некоторых Web-серверах установлена операционная система Windows NT, файловая система которой не чувствительна к регистру, в то время как на других Web-серверах установлена UNIX, имена файлов которой чувствительны к регистру.

Для файловой системы UNIX характерны также и другие особенности.

- **Схема i-узлов**. В UNIX для идентификации всех файлов и каталогов используется их внутренняя нумерация. Эти внутренние номера называются *i-узлами*. Операционная система связывает внутренние номера с местами хранения данных на физическом диске. Для поддержки соответствия i-узлов и полных путей файлов в операционной системе используется специальная таблица.
- **Жесткие связи**. Метод жесткой связи позволяет присвоить одному файлу более одного имени. С помощью команды `ln` можно связать имя файла с i-узлом, т.е. с файлом. Таким образом, можно связать два разных имени файла, например `Myfile` и `Yourfile`, с одним i-узлом. При этом изменения, сделанные в файле `Myfile`, будут немедленно отражены в файле `Yourfile`.
- **Однородные файлы**. В UNIX нет жестких правил, определяющих заголовки различных типов файлов. Файлы представляют собой потоки данных без определенной структуры. За определение структуры и формата файлов отвечают приложения.

HPFS. Файловая система HPFS разработана компанией IBM для OS/2. Версия 1.0 операционной системы OS/2 поддерживает только файловую систему FAT, однако в версию 1 2 уже включена HPFS. Перечислим некоторые характерные особенности файловой системы HPFS.

- Поддержка длинных имен файлов (до 255 символов).
- Более высокая производительность, чем у FAT.
- Высокая надежность и восстанавливаемость.
- Меньшая подверженность фрагментации файлов, чем в FAT.

Замечание

В описании файловой системы *надежность* означает низкую вероятность ошибки или порчи файлов. *Восстанавливаемость* — это способность файловой системы поддерживать целостность данных путем создания, например, избыточных копий данных, по которым можно восстановить исходные данные после их искажения или утраты.

В системе HPFS поддерживается расширенный набор символов. HPFS сохраняет регистр символов, однако она *не чувствительна* к регистру. Если пользователь забыл регистр какого-либо символа в имени файла и ввел, например, `mydocuments` вместо `MyDocuments`, то система все равно предоставляет ему этот файл.

В системе HPFS используется структура каталогов, в которой диск делится на *полосы*, каждая из которых имеет объем 16 Мбайт. Информация о структуре каталогов и размещении файлов расположена в середине каждой полосы. Поэтому расстояние между содержимым файла и его управляющими элементами не может превышать 8 Мбайт, отсчитываемых по поверхности диска. Такая структура хранения является основой высокой производительности HPFS.

В системе HPFS поддерживаются разделы диска объемом до 64 Гбайт. Дисковое пространство разбивается не на кластеры, а на секторы. Это позволяет использовать дисковое пространство более экономно и уменьшает влияние дефрагментации. Для идентификации каждого сектора диска в HPFS используются *сигнатуры секторов*, поэтому данные могут быть восстановлены даже после значительного повреждения диска.

Macintosh HFS. В операционных системах Macintosh используется файловая система HFS. В ней диски разделены на *тома*, которые могут содержать следующие компоненты:

- файлы;
- каталоги;
- потоки файлов;
- потоки каталогов.

Замечание

Поток каталога содержит имя каталога и определение его родителя. *Поток файла* содержит имя файла и имя каталога, в котором этот файл расположен.

В системе HFS для организации содержимого каталогов и поиска в них данных используется алгоритм индексирования бинарного дерева. Кроме того, в HFS поддерживается *ветвление файлов*, т.е. файл состоит из нескольких частей, или *ветвей*, которые могут храниться как отдельные файлы. Это могут быть следующие файлы.

- **Ветвь источника**. В этом файле хранятся команды меню, диалоговые окна и т.д.
- **Ветвь данных**. В этом файле хранится поток данных.

В системе HFS каждому файлу и каталогу сопоставлены *записи каталогов* с идентификационными номерами, аналогичными i-узлам в UNIX. Потоки каталогов и потоки файлов представляют собой записи каталогов, включающие имя каталога или файла с идентификационными параметрами родительского каталога. Использование потоков обеспечивает избыточность данных и возможность их восстановления после краха диска.

Существуют утилиты (такие, как Global File System компании Charismac и MacOpener компании DataViz), позволяющие получать доступ к файлам Macintosh из операционных систем Linux, OS/2, Windows и MS DOS.

NFS. Разработанная компанией Sun Microsystems файловая система NFS стала стандартом для файловых серверов. Коммуникация в ней выполняется с помощью протокола RPC (Remote Procedure Call). Для работы в NFS на запрашивающем компьютере должна быть установлена клиентская программа NFS, кроме того, как клиент, так и сервер должны использовать TCP/IP. Существует расширение NFS — файловая система WebNFS, разработанная для использования в Internet. Она заменяет протоколы HTTP и FTP.

Выбор оптимальной файловой системы. Выбор файловой системы зависит от установленной на компьютере операционной системы, требований к безопасности данных и требований к параметрам доступа Файловые системы, как правило, разрабатывались вместе с операционной системой, однако ряд операционных систем поддерживает больше одной файловой системы. При работе в некоторых операционных системах можно даже использовать несколько файловых систем одновременно, однако они должны быть расположены в разных *разделах диска.*

Диски и разделы дисков

Базовый носитель памяти персональных компьютеров — жесткий диск. Объемы памяти разных жестких дисков значительно отличаются. Первые диски могли хранить лишь до 5 Мбайт данных. В настоящее время практически каждому пользователю доступны диски, способные хранить 50 Гбайт данных и больше.

Жесткий диск состоит из набора дисков, каждый из которых похож на грампластинку. Однако, в отличие от грампластинки, у которой одна непрерывная спираль тянется от начала до конца записи, на жестком диске данные записаны на концентрических кругах, называемых *дорожками.*

На приводе диска укреплены две *магнитные головки*, читающие и записывающие данные. Головки передвигаются с помощью привода по линии радиуса, а диски вращаются. Головки таким образом пробегают над всей поверхностью дисков. Скорость вращения дисков измеряется количеством оборотов в минуту. Время, прошедшее с момента подачи команды на чтение до начала чтения, называется *временем доступа.* Оно измеряется в миллисекундах, например 9 мс.

Скорость чтения данных с диска значительно меньше скорости чтения из оперативной памяти. Это объясняется тем, что доступ к информации на диске выполняется путем механического перемещения головок. Как известно, механическое перемещение любого физического объекта требует значительно большего времени, чем электронный процесс в какой-либо цепи. Доступ к оперативной памяти требует времени на протекание тока по электрической цепи. Скорость этого процесса хотя и меньше скорости света, однако довольно близка к ней. Она, естественно, значительно превышает скорость механического передвижения компонентов дисковода.

Хранящиеся на жестком диске данные размещены на *секторах, дорожках* и *цилиндрах* диска. Как уже упоминалось, дорожка — это концентрический круг на поверхности диска. Цилиндр — это совокупность дорожек, расположенных одна над другой в пакете дисков. Сектор — это часть дорожки. Чтобы данные при необходимости можно было найти, процедуры файловой системы должны вычислять точное физическое положение головок над поверхностью дисков.

Многие современные диски способны хранить огромное количество данных, объем которых измеряется многими сотнями гигабайт. Для лучшей организации хранения файлов на диске его можно разбить на *разделы*, которые пользователь видит как отдельные *логические диски*. Каждому разделу присваивается определенная буква таким образом, будто это отдельный физический диск. Можно, например, хранить все системные файлы в одном разделе, приложения — в другом, а данные пользователей — в третьем. Если общий объем диска равен 15 Гбайт, то его можно разбить на три раздела по 5 Гбайт каждый.

Замечание

Разделы не обязательно должны иметь одинаковый объем. Диск объемом 15 Гбайт можно разбить, например, на разделы по 2, 5, 7 и 1 Гбайт.

Разделы дисков создаются с помощью специальных утилит. Часто такие утилиты поставляются встроенными в операционную систему, например команда FDISK в системах DOS, Windows 9*x* и Linux или графическая программа управления дисками в системах Windows NT/2000. Используются также утилиты других поставщиков, например Partition Magic.

В DOS диск может иметь до четырех *первичных* разделов. Вместо одного из первичных разделов можно создать *расширенный* раздел и много логических дисков внутри этого раздела. Один из первичных разделов должен быть помечен как *активный*. С этого раздела начинается загрузка компьютера.

Если у вас много бумажных документов (например, финансовые записи за несколько лет), то вы можете счесть удобным поместить их в один большой ящик. Для облегчения поиска нужных документов вы можете также поместить их в несколько ящиков, рассортировав, например, по годам: в одном ящике документы за 70-е годы, в другом — за 80-е и т.д. Аналогично этому, разбивка диска на разделы помогает лучше организовать хранение электронных данных.

Можно назвать еще два преимущества разбивки диска на разделы.

- Разные разделы можно форматировать в разных файловых системах. Например, отформатировать раздел C: в системе FAT16, D: — в FAT32, а E: — в NTFS.
- В разные разделы можно установить разные операционные системы, реализуя таким образом альтернативную загрузку компьютера. Разные операционные системы можно установить и в один раздел (если в них используется одна и та же файловая система), однако делать так не рекомендуется, потому что операционные системы могут ошибочно переписать файлы друг друга.

В системе Windows 2000 представлена новая концепция операционных систем Microsoft — *динамические диски*. Когда диску присваивается статус динамического, на нем вместо разделов создаются тома. Объем томов можно динамически изменять без удаления и перезаписи данных. Можно также объединять фрагменты дискового пространства разных физических дисков в один том. Это делается для увеличения области хранения или для повышения *отказоустойчивости* системы. Более подробно отказоустойчивость дисков рассматривается в главе 14, "Защита сети".

Том функционирует как одно целое, даже если он составлен из нескольких физических дисков. Для пользователя том выглядит как один логический диск, идентифицируемый одной буквой, например C:\.

Распространенные клиентские операционные системы

В этом разделе рассматриваются распространенные клиентские операционные системы, выполняющие функции клиентов в сетевой среде клиент/сервер:

- MS DOS и Windows 3.*x*;
- Windows 9*x*;
- Windows NT Workstation;
- Windows 2000 Professional;
- Linux/UNIX;
- Macintosh;
- OS/2.

В оставшихся разделах этой главы приведены подробные процедуры и копии экрана, иллюстрирующие конфигурирование сетевых компонентов некоторых клиентских операционных систем. Обратите внимание: приведенные материалы не являются инструкцией того, "как это сделать", ссылки на подробные инструкции и руководства можно найти в конце главы. Цель данного раздела — ознакомить читателя с общими понятиями конфигурирования сетевых компонентов различных операционных систем и с наиболее популярными интерфейсами, с помощью которых это обычно делается.

MS DOS и Windows 3.*x*

Специалисты в области информационных технологий считают эти операционные системы устаревшими. Тем не менее одна из них — MS DOS — до сих пор довольно популярна во многих рабочих сетях. (Термин *рабочая сеть* означает сеть, в которой ежедневно выполняются коммерческие или технологические операции, в отличие от сетей, используемых в научных, образовательных или развлекательных целях.)

Старая добрая MS DOS обладает рядом существенных преимуществ.

- **Это простая система с низкими требованиями к оборудованию**. Требования к объему памяти и параметрам процессора очень низкие. MS DOS способна работать почти на любом устаревшем оборудовании.
- **Низкая стоимость**. Дешевая не только сама операционная система, но и, как упоминалось выше, совместимое с ней оборудование.
- **Стабильность и надежность**. MS DOS не является многозадачной операционной системой (т.е. в ней одновременно выполняется только одно приложение), поэтому нет необходимости беспокоиться о конфликтах и авариях, порожденных неправильным разделением внутренних ресурсов компьютера.
- **MS DOS легко освоить и использовать**. Хотя эта система и не настолько интуитивна, однако, усвоив синтаксис команд, работать в ней довольно легко.
- **Существует много программ, работающих в MS DOS**. На протяжении многих лет MS DOS была стандартной операционной системой. За это время создано огромное количество работающих в ней программ. Многие компании продолжа-

ют использовать MS DOS только потому, что созданные для нее программы в более новых операционных системах не работают должным образом.

Конечно, использование этой устаревшей операционной системы порождает ряд неудобств. MS DOS — это 16-разрядная операционная система, поэтому в ней не могут выполняться совершенные графические программы, написанные для 32-разрядных операционных систем Windows. Отсутствие средств многозадачности также является большим недостатком. Файловая система FAT — единственная, которую можно использовать в DOS — почти не содержит средств обеспечения безопасности, весьма актуальных в настоящее время. Кроме того, в сетевой среде клиентским программам MS DOS трудно получить доступ к разделяемым ресурсам, в которых используются длинные имена файлов. И наконец, многим пользователям очень не нравится интерфейс на основе командной строки.

Запуск Windows 3.*x* в среде MS DOS может смягчить некоторые из этих недостатков. Оболочка Windows 3.*x* предоставляет пользователю графический интерфейс и поддерживает *кооперативную многозадачность*, что позволяет пользователю выполнять несколько задач одновременно.

Кооперативная и вытесняющая многозадачность

В среде с кооперативной многозадачностью программы разделяют (совместно используют) адреса памяти и обмениваются информацией. В этой среде приложения совместно используют процессор с помощью метода *квантования времени*. Программы приложений написаны таким образом, что они освобождают процессор после определенного промежутка времени. Это дает возможность другим программам выполняться "одновременно". Однако, если программа плохо написана, она может захватить процессор на долгое время. Кроме того, если программа терпит крах, то это может остановить выполнение всех остальных программ.

В операционных системах Windows 9x, Windows NT и Windows 2000 используется более эффективная форма многозадачности — *вытесняющая многозадачность*. В этом случае операционная система управляет выделением процессорного времени, а 32-разрядные программы выполняются в своих отдельных пространствах адресов. В системе с вытесняющей многозадачностью плохая программа не может "захватить власть" в системе. Если одна программа терпит крах, это никак не влияет на остальные программы.

В системах MS DOS и Windows 3.1 для подключения к сети должно быть установлено дополнительное программное обеспечение *клиента сети*. Windows for Workgroups 3.11 — первая операционная система Microsoft с встроенными сетевыми компонентами. Операционные системы Windows 3.*x* и MS DOS разрабатывались для одноранговых сетей (рабочих групп), однако при соответствующем конфигурировании их можно использовать для подключения к домену Windows NT/2000. Обратите внимание: компьютеры Windows 3.*x* и MS DOS не имеют учетной записи компьютера в домене. С их помощью можно зарегистрироваться в домене (при наличии соответствующей учетной записи пользователя) и получать доступ к ресурсам, однако они не могут войти в состав домена.

Windows 9*x*

Операционная система Windows 95 была разработана для облегчения работы в сети. Эта же традиция была продолжена и расширена в Windows 98. Ниже перечислены операционные системы этого семейства, обобщенно называемые Windows 9*x*.

- **Windows 95a**. Первоначальная реализация первой 32-разрядной пользовательской операционной системы компании Microsoft.
- **Windows 95b**. Называется также OSR2. Дополнительно поддерживает FAT32. Первоначально эта операционная система предназначалась для установки производителями на готовые компьютеры.
- **Windows 98**. Усовершенствованная Windows 95. Добавлены средства Active Desktop (активный рабочий стол) и Advanced Configuration and Power Interface (расширенная конфигурация и управление электропитанием). Добавлена также поддержка USB (Universal Serial Bus) и адаптеров TV-тюнера. Расширены процедуры установки и управления системой.
- **Windows 98 SE (Second Edition)**. Добавлен Web-броузер Internet Explorer 5.0, усилена система шифрования коммутируемых соединений и добавлена поддержка совместного использования подключения к Internet.
- **Windows ME (Millennium Edition)**. Следующая пользовательская операционная система Microsoft, основательно реорганизованная в рамках членства в семействе Windows 9*x*. В систему Windows ME включен ряд дополнительных средств.
  - Расширенная поддержка мультимедийных приложений, облегчающая работу с цифровыми видео- и фотоматериалами.
  - Встроенные средства восстановления после краха системы, позволяющие восстанавливать систему в предопределенное состояние.
  - Упрощение конфигурирования соединений с простыми одноранговыми сетями.
  - Более быстрые загрузка и завершение системы (при использовании нового оборудования, поддерживающего технологию FastBoot).

Операционные системы Windows 9*x* содержат клиентские программы сетей Microsoft и NetWare. В них поддерживаются протоколы сетевого и транспортного уровней NetBEUI, TCP/IP и NWLink. Системы Windows 9*x* содержат также встроенные средства установки коммутируемых соединений с Internet и удаленными локальными сетями.

Благодаря богатым встроенным средствам установки соединений Windows 9*x* — один из наиболее популярных типов клиентских операционных систем в мире бизнеса. На протяжении нескольких лет они остаются лучшим типом клиентских операционных систем как для больших, так и для малых компаний, для одноранговых сетей и для клиентов, обслуживаемых серверами Windows NT/2000, NetWare и UNIX.

В системах Windows 9*x* поддерживаются 32-разрядные приложения, однако для обеспечения обратной совместимости с MS DOS и Windows 3.*x* включена также поддержка 16-разрядных приложений. Для поддержки длинных имен файлов в них используется файловая система VFAT, а в системах Windows 95b, 98 и ME для более эффективного использования дискового пространства поддерживается также FAT32.

Перечислим преимущества клиентских операционных систем Windows 9*x* в качестве сетевых клиентов.

- Они дешевле, чем Windows NT и Windows 2000.
- Под управлением этих систем могут выполняться приложения MS DOS, а также 16- и 32-разрядные приложения Windows.
- Интерфейсы этих систем хорошо знакомы для большинства пользователей персональных компьютеров.

- Для Windows 9*x* существует клиентское программное обеспечение, позволяющее устанавливать соединение почти с любой сетевой операционной системой, включая Windows, NetWare, UNIX и Linux.

Замечание

Компания Novell не разрабатывает клиентские операционные системы. В сетях NetWare на большинстве клиентских компьютеров установлены клиентские операционные системы Windows, содержащие встроенные клиентские программы Novell или клиентские компоненты NetWare. Компания Novell поставляет также клиентские программы DOS. Компания Prosoft Engineering поставляет программное обеспечение Macintosh Connectivity Solutions for NetWare.

Теперь рассмотрим базовые концепции установки соединений клиентов Windows 9*x* с сетями Microsoft, NetWare и с удаленными серверами.

Установка соединений клиентов Windows 9*x* с сетями Microsoft

Сетевые компоненты Windows 9*x* встроены в операционную систему. Компьютер можно сконфигурировать как часть одноранговой сети или просто зарегистрироваться в домене Windows NT/2000, если, конечно, в нем создана соответствующая учетная запись пользователя домена.

Параметры сети конфигурируются в диалоговом окне Network (Сеть), как показано на рис. 12.4. Чтобы открыть это окно, нужно выбрать команду Start⇨Settings⇨Control Panel⇨Network (Пуск⇨Настройка⇨Панель управления⇨Сеть) или щелкнуть правой кнопкой мыши на пиктограмме Network Neighborhood (Сетевое окружение), расположенной на рабочем столе (если она там установлена), и выбрать в контекстном меню команду Properties (Свойства).

Для установки компьютера Windows 95/98 как однорангового в рабочей группе Microsoft выполните ряд действий.

1. Убедитесь в том, что сетевой адаптер установлен и подключен к кабелю или другому сетевому носителю.
2. Согласно инструкциям поставщика установите необходимые драйверы сетевого адаптера (необходимо, чтобы эти драйверы были разработаны специально для используемой в данном случае версии Windows).
3. Откройте вкладку Configuration диалогового окна Network. Убедитесь, что установлена клиентская программа Client for Microsoft Networks (Клиент для сетей Microsoft). Если она не установлена, то установите ее. Для этого щелкните на кнопке Add (Добавить) и выберите ее в списке. При этом система может попросить вас поместить в накопитель инсталляционный компакт-диск Windows 9*x*.
4. Если вы хотите использовать компьютер для регистрации в домене Windows NT/2000, то нужно сконфигурировать регистрационные параметры домена. Для этого выделите компонент Client for Microsoft Network и щелкните на кнопке Properties (Свойства). При этом появляется диалоговое окно, показанное на рис. 12.5. Установите флажок Log on to Windows NT domain (Входить в домен Windows NT) и в поле Windows NT domain (Домен Windows NT) введите имя домена. В этом диалоговом окне можно также установить переключатель Quick logon (Быстрый вход), тогда созданные сетевые логические диски не бу-

дут восстановлены, пока вы к ним не обратитесь. Если установить переключатель Logon and restore network connection (Вход с восстановлением сетевых подключений), то при регистрации система проверит и подготовит все сетевые логические диски.

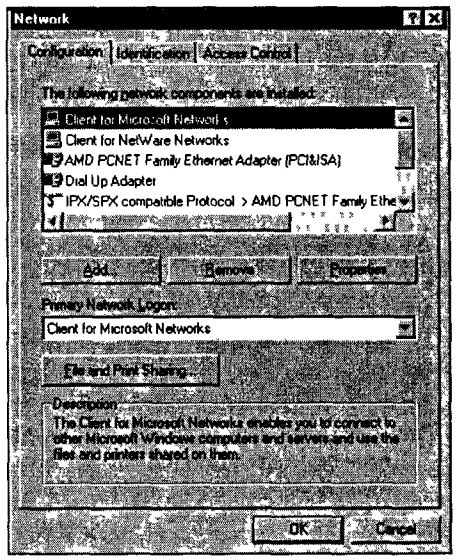


Рис. 12.4. В Windows 9x сетевые параметры конфигурируются в диалоговом окне Network

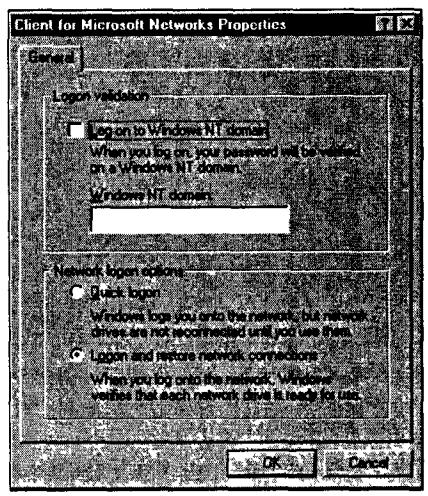


Рис. 12.5. Чтобы с компьютера можно было зарегистрироваться в домене Windows, необходимо соответственно сконфигурировать свойства клиентской программы

5. Откройте вкладку Identification (Идентификация), как показано на рис. 12.6. В поле Computer name (Имя компьютера) введите уникальное в пределах сети имя компьютера. Оно может содержать до 15 цифр или букв алфавита. Если компьютер будет членом рабочей группы, введите в поле Workgroup (Рабочая группа) имя рабочей группы. В текстовом поле Computer Description (Описание компьютера) можно ввести какие-либо необязательные сведения о компьютере.
6. Должен быть установлен и связан с сетевым адаптером, как минимум, один сетевой или транспортный протокол. Этот же протокол должен быть установлен и на других компьютерах сети, с которыми вы собираетесь сообщаться. Протоколы добавляются, удаляются и конфигурируются во вкладке Configuration с помощью кнопок Add (Добавить), Remove (Удалить) и Properties (Свойства). Для просмотра всех установленных компонентов нужно прокрутить список компонентов The following network components are installed (В системе установлены следующие компоненты).
7. Чтобы другие пользователи сети могли получить доступ к вашим принтерам и файлам, нужно объявить эти ресурсы разделяемыми. Для этого во вкладке Configuration щелкните на кнопке File and Print Sharing (Доступ к файлам и принтерам) и в открывшемся диалоговом окне установите соответствующие флажки (рис. 12.7). В этом окне представлены два флажка — установка режима разделения для файлов и для принтеров.

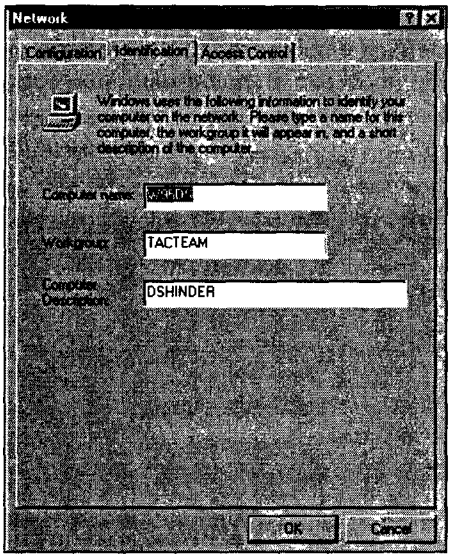


Рис. 12.6. Во вкладке Identification устанавливаются имена компьютера и рабочей группы

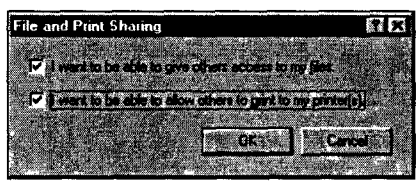


Рис. 12.7. Чтобы сделать свои файлы и принтеры доступными для других пользователей сети, нужно объявить их разделяемыми

Сконфигурировав таким образом компоненты сети, перезагрузите систему, чтобы изменения вступили в силу. Если вы перезагружаетесь опять в Windows, то на экране появится диалоговое окно регистрации, в котором нужно ввести имя пользователя и пароль (рис. 12.8).

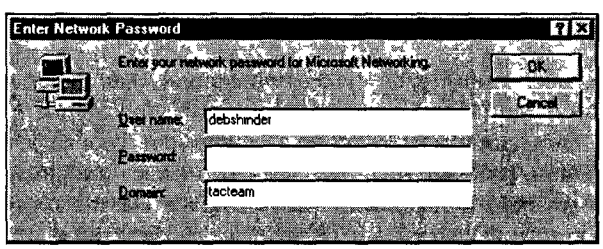


Рис. 12.8. Диалоговое окно регистрации, появляющееся после конфигурирования сетевых свойств и перезагрузки системы

Замечание

Если соединение с сетью устанавливается с помощью протокола TCP/IP, то должны быть сконфигурированы свойства TCP/IP — соответствующий IP-адрес и маска подсети (при необходимости также шлюз по умолчанию). Другой вариант — сконфигурировать компьютер как клиент DHCP (Dynamic Host Configuration Protocol). Клиент DHCP запрашивает свой IP-адрес у сервера DHCP во время первого подключения к сети.

Теперь дважды щелкните кнопкой мыши на пиктограмме Network Neighborhood и просмотрите список сетевых компьютеров, существующих в вашей рабочей группе или домене. В списке видны также компьютеры с разделяемыми файлами и принте-

рами и компьютеры Windows NT и Windows 2000 с выполняющимися серверными служебными программами. Этот список называется *списком просмотра* (рис. 12.9). Если компьютер зарегистрирован в домене, то для просмотра списка, возможно, потребуется выбрать имя домена.

Если ваша учетная запись пользователя имеет соответствующие права доступа, то доступ к разделяемым ресурсам другого компьютера выполняется двойным щелчком кнопкой мыши на имени этого компьютера. Более подробно права доступа рассматриваются в главе 14, "Защита сети".

Установка соединений клиентов Windows 9x с сетями NetWare

Компьютер Windows 9*x* может работать как клиент сервера NetWare с помощью одного из двух методов.

- Используя компонент Microsoft Client for NetWare Networks (Клиент Microsoft для сетей NetWare), входящий в поставку Windows 9*x* (по умолчанию не устанавливается).
- Используя клиентскую программу Novell для Windows 95/98.

На одном компьютере нельзя установить обе эти клиентские программы.

Установить соединение с любым сервером NetWare более ранней версии, чем 5.0, можно только с использованием протокола TCP/IP. При установке компонента Microsoft Client for NetWare Networks автоматически устанавливается NWLink — реализация стека IPX/SPX компании Microsoft. Клиентская программа Microsoft устанавливается как сетевой компонент во вкладке Configuration диалогового окна свойств Network.

Один из серверов NetWare можно объявить как предпочтительный. Для этого нужно выделить компонент Client for NetWare Network и щелкнуть на кнопке Properties, при этом появляется диалоговое окно, показанное на рис. 12.10. Если оставить поле Preferred server (Предпочтительный сервер) пустым, то компьютер будет пытаться зарегистрироваться на ближайшем сервере NetWare.

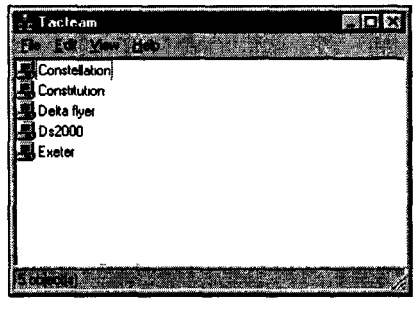


Рис. 12.9. Когда сетевые компоненты сконфигурированы, в диалоговом окне Network Neighborhood виден список компьютеров сети

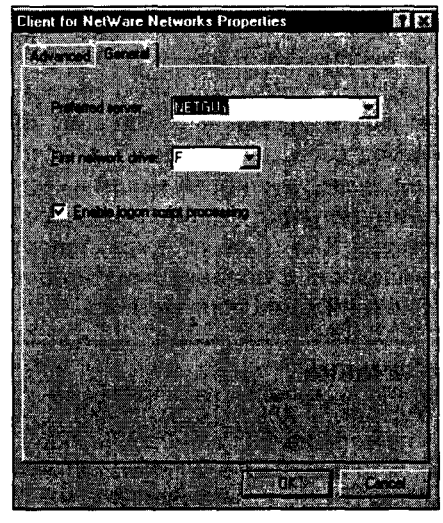


Рис. 12.10. Для компьютера Windows 9x можно установить предпочтительный сервер NetWare

Установив и конфигурировав таким образом клиентскую программу NetWare, перезагрузите компьютер.

После установки и конфигурирования клиента NetWare и программы NWLink в диалоговом окне Network Neighborhood появляется дерево NetWare. На рис. 12.11 оно показано под именем Daltac.

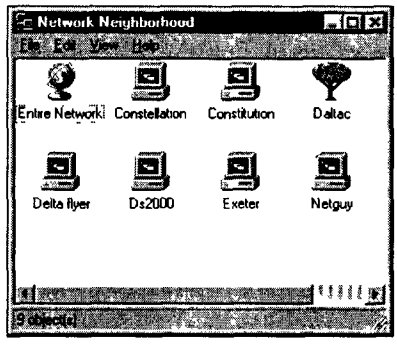


Рис. 12.11. После установки клиентской программы NetWare в диалоговом окне Network Neighborhood появляется дерево NetWare

В системе Windows 9*x* доступ к ресурсам NetWare выполняется путем перемещения по дереву и двойного щелчка на выбранном ресурсе. Естественно, для этого нужно иметь соответствующее право доступа к ресурсу сервера NetWare. Для пользователя ресурсы NetWare видны так же, как и ресурсы сервера Microsoft.

Установка соединений клиентов Windows 9*x* с удаленным сервером

Установить соединение компьютера Windows 9*x* с удаленным сервером с помощью телефонной линии довольно просто. Для этого Microsoft включила в состав операционной системы компонент Dialup Networking (Коммутируемое соединение с сетью). Для создания коммутируемого соединения нужно сначала установить и сконфигурировать модем. Наборное соединение конфигурируется с помощью пиктограммы Dialup Networking (Сеть и удаленный доступ к сети), доступ к которому можно получить, дважды щелкнув кнопкой мыши на пиктограмме My Computer на рабочем столе.

Коммутируемое соединение можно устанавливать с провайдером услуг Internet или с сервером RAS (Remote Access Service). Операционная система Windows 9*x* сама может выполнять функции коммутируемого сервера. Для этого нужно установить соответствующий компонент системы.

Замечание

В Windows 95 для использования коммутируемого соединения должен быть установлен пакет Microsoft Plus! Pack (набор добавляемых компонентов операционной системы). В то же время в Windows 98 компоненты коммутируемого соединения включены в состав операционной системы.

Службы удаленного доступа подробно рассматриваются в главе 15, "Удаленный доступ".

Операционная система Windows NT Workstation

Это первая операционная система компании Microsoft, разработанная для рынка корпоративных сетей. Ее более поздняя версия NT 4.0 содержит интерфейс пользователя, аналогичный интерфейсу системы Windows 95. Однако некоторые компании все еще используют версию NT 3.*x*, интерфейс которой аналогичен интерфейсу Windows 3.*x*. Операционная система Windows NT разрабатывалась для предоставления корпоративным пользователям более стабильной среды решения ответственных задач, чем это могли обеспечить пользовательские операционные системы Microsoft.

Замечание

Когда была выпущена первая версия Windows NT, компания Microsoft объявила, что это сокращение означает *New Technology* (новая технология). Однако в последнее время Microsoft утверждает, что NT никак не расшифровывается.

В качестве настольной операционной системы и сетевого клиента Windows NT Workstation обладает определенными преимуществами.

- Является по-настоящему 32-разрядной операционной системой с вытесняющей многозадачностью.
- Обеспечивает безопасность на уровне файлов и сжатие отдельных файлов.
- Обладает обратной совместимостью с большинством 16-разрядных программ, причем не жертвуя надежностью. Программы DOS и Windows 3.*x* в ней выполняются специальной виртуальной машиной. Если при использовании этого метода одна программа терпит крах, это никак не затрагивает другие программы и не требует перезагрузки операционной системы.

При разработке Windows NT главной целью компании Microsoft была ее интеграция в сеть. Операционная система Windows NT поддерживает все распространенные сетевые адаптеры и программное обеспечение, необходимое для подключения к сетям Microsoft и NetWare. В нее встроены также средства клиентов и серверов удаленного доступа.

Установка соединений Windows NT Workstation с сетями Microsoft

Операционная система Windows NT Workstation может работать как одноранговая в рабочей группе Microsoft или как клиент домена на основе серверов NT. Для установки соединения компьютера под управлением Windows NT Workstation с сетью Windows выполните ряд действий.

1. Убедитесь, что сетевой адаптер правильно установлен и подключен к кабелю или другому сетевому носителю.
2. Установите драйверы сетевого адаптера согласно инструкциям поставщика. Убедитесь, что эти драйверы написаны специально для Windows NT.
3. Сконфигурируйте сетевые свойства с помощью пиктограммы Network. Доступ к ней можно получить во вкладке свойств диалогового окна конфигурирования. Для этого выберите команду Start⇨Settings⇨Control Panel⇨Network или щелкните правой кнопкой мыши на пиктограмме Network Neighborhood на рабочем столе и в контекстном меню выберите команду Properties.

4. Как показано на рис. 12.12, во вкладке Identification дайте компьютеру уникальное в пределах сети имя. Это имя может содержать до 15 цифр и букв алфавита.
5. Введите имя домена (или рабочей группы), которому принадлежит компьютер, как показано на рис. 12.12.

Установка соединений Windows NT Workstation с сетями NetWare

Как и в Windows 9x, установить соединение компьютера Windows NT Workstation с сетью NetWare довольно легко. Microsoft поставляет с этой системой компонент CSNW (Client Services for NetWare). Можно также загрузить клиентскую программу для NT компании Novell по адресу: `www.novell.com`. При установке CSNW автоматически устанавливается NWLink. На рис. 12.13 показано диалоговое окно конфигурирования компонента CSNW.

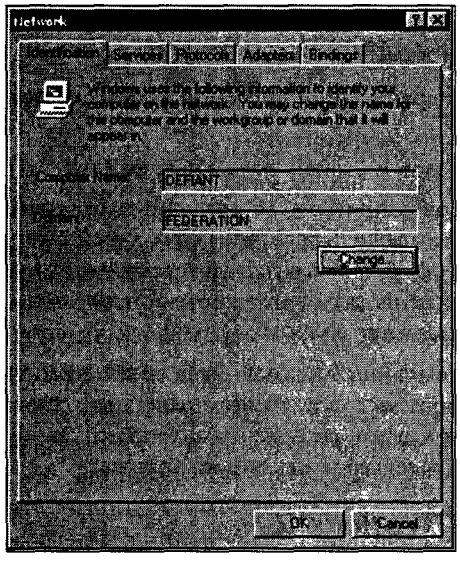


Рис. 12.12. Во вкладке Identification диалогового окна свойств Network необходимо ввести уникальное имя компьютера и имя домена

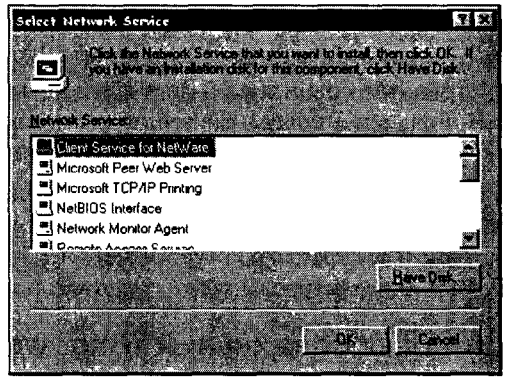


Рис. 12.13. Компонент CSNW используется для установки соединения компьютера Windows NT 4.0 с сервером NetWare

После установки на клиентском компьютере компонента CSNW в диалоговом окне Control Panel системы NT появляется соответствующая пиктограмма. Теперь можно получать доступ к ресурсам серверов NetWare (рис. 12.14). Конечно, как и в сетях Microsoft, для этого нужно иметь соответствующие права доступа.

Установка соединения Windows NT Workstation с удаленным сервером

Конфигурирование клиентского компьютера NT на установку соединения с удаленным сервером несколько сложнее, чем в Windows 9x. Сначала в диалоговом окне конфигурирования свойств сети необходимо установить компонент RAS (Remote Ac-

cess Service), как показано на рис. 12.15. Последующие операции подключения не отличаются от аналогичных действий в Windows 9x.

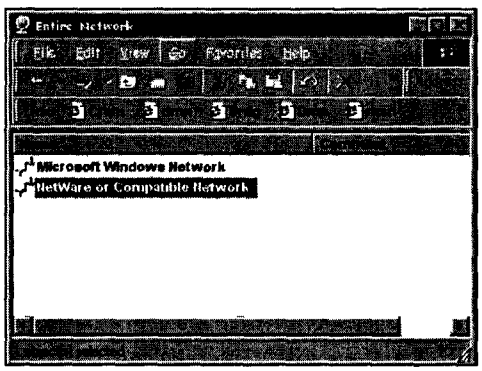


Рис. 12.14. После установки компонента CSNW доступ к сети NetWare можно получать из диалогового окна Network Neighborhood

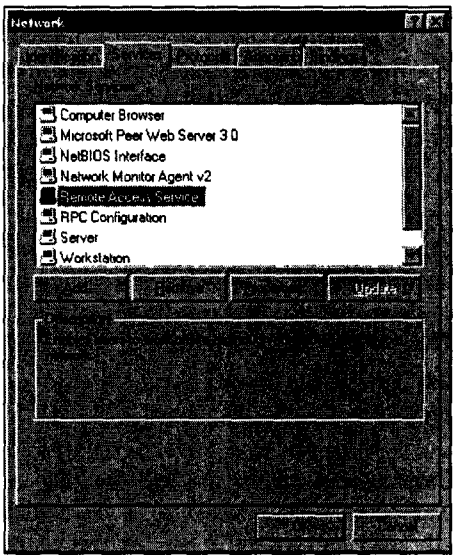


Рис. 12.15. Установка компонента RAS в диалоговом окне Network

Операционная система Windows 2000 Professional

Windows 2000 — операционная система компании Microsoft, предназначенная для корпоративных настольных компьютеров. Как и серверы Windows 2000, она построена на основе ядра NT, однако в ее состав дополнительно включены многие расширенные средства. В отличие от Windows NT Workstation, система Windows 2000 Professional поддерживает технологию Plug and Play. Она может быть установлена на жестком диске с файловой системой FAT32. В ее состав входят средства шифрования данных на жестких дисках. В отличие от Windows 9x, операционная система Windows 2000 Professional предоставляет более высокий уровень безопасности и надежности для решения ответственных задач.

В качестве настольной операционной системы и сетевого клиента Windows 2000 Professional обладает рядом преимуществ.

- Улучшенная поддержка мобильных пользователей с помощью средств APM (Advanced Power Management) и ACPI (Advanced System Configuration and Power Interface). Система Windows NT не поддерживает ACPI.
- Более безопасные средства поддержки виртуальных частных сетей (Virtual Private Networking — VPN) с помощью протоколов L2TP (Layer 2 Tunneling Protocol) и IPSec (IP Security). В предыдущих версиях Windows для VPN поддерживались только протоколы PPTP (Point-to-Point Protocol).

- Средства работы с каталогами в автономном режиме позволяют копировать и согласовывать сетевые документы, хранящиеся на локальном компьютере, таким образом, что к ним можно получать доступ, когда компьютер не подключен к сети.
- С помощью протокола IPP (Internet Printing Protocol) можно печатать с использованием адресов URL и управлять принтерами посредством интерфейса Web-броузера.
- Встроенные инструменты дефрагментации и другие утилиты значительно облегчают управление операционной системой. Для Windows NT их приходилось покупать отдельно у других поставщиков.
- Поддержка системы безопасности Kerberos.

Теперь рассмотрим установку соединения компьютера Windows 2000 Professional с сетями Microsoft и NetWare и с удаленным сервером.

Установка соединения компьютера Windows 2000 Professional с сетью Microsoft

Операционная система Windows 2000 Professional была разработана для использования в коммерческих сетях, поэтому поддержка сетевых приложений встроена в систему. Сетевой адаптер обнаруживается службой Plug and Play при загрузке компьютера. Для каждого найденного сетевого адаптера автоматически создается локальное соединение.

В этой операционной системе для портативных компьютеров можно создавать *профили оборудования*, которые в определенное время будут работать с сетевым соединением, причем в другое заданное время они будут отключаться. Это устраняет проблему возникновения сообщений об ошибках, когда компьютер не может найти сети.

Конфигурирование локальных соединений состоит из тех же базовых задач, которые были рассмотрены в предыдущем разделе. По умолчанию в качестве протокола сетевого и транспортного уровней устанавливается TCP/IP. Адресную информацию протокола IP можно установить вручную. Другой вариант — сконфигурировать компьютер в качестве клиента DHCP.

В отличие от Windows NT, в Windows 2000 поддерживается метод автоматической обработки частных IP-адресов (Automatic Private IP Addressing — APIPA). Это позволяет клиенту DHCP, который не может найти сервер DHCP, присвоить себе IP-адрес. После этого компьютер сможет устанавливать соединение с любыми компьютерами в том же сегменте сети, которые тоже присвоили себе адреса с помощью APIPA. Для сравнения: клиенты NT, не нашедшие сервер DHCP, не могут использовать TCP/IP.

Получить доступ к параметрам сетевой конфигурации можно с помощью пиктограммы Network and Dial-up Connections в диалоговом окне Control Panel или выбора соответствующей команды в главном меню. На рис. 12.16 показано диалоговое окно Local Area Connection Properties, в котором можно удалять, добавлять и конфигурировать сетевых клиентов, службы и протоколы.

В диалоговом окне статуса соединения, показанном на рис. 12.17, можно найти полезную информацию о сконфигурированном локальном соединении, включая такие сведения:

- активно ли сетевое соединение (Status) и как долго компьютер подключен к сети (Duration);
- какова пропускная способность соединения в мегабитах в секунду (Speed); для соединений Ethernet эта величина обычно составляет 10 или 100 Мбит/с;
- каково количество переданных (Sent) и принятых (Received) пакетов.

В этом диалоговом окне можно отключить соединение или, щелкнув на кнопке Properties, изменить конфигурацию

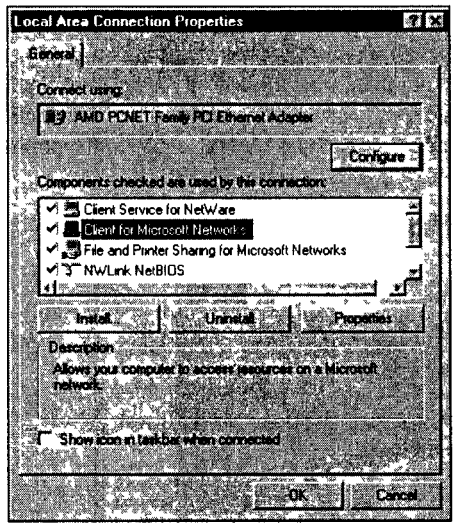


Рис 12 16 Настраивать сетевые компоненты Windows 2000 можно с помощью этого диалогового окна

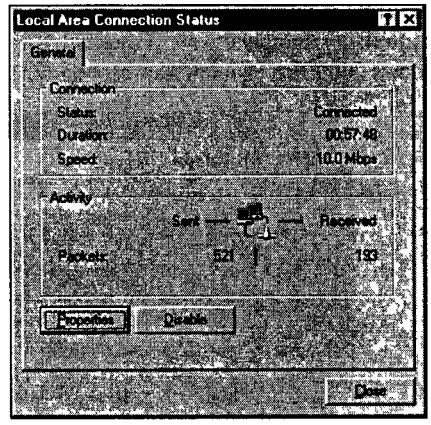


Рис 12 17 В диалоговом окне состояния локального соединения приводится информация об указанном сетевом соединении

В Windows 2000 поддерживаются локальные и глобальные соединения многих типов, включая соединения Ethernet, Token Ring, соединения посредством кабельных модемов, DSL, FDDI, соединения ATM и беспроводные соединения Поддерживается также эмуляция локальной сети LANE ATM

Установка соединения компьютера Windows 2000 Professional с сетью NetWare

Компания Microsoft включила в операционную систему Windows 2000 Professional средства поддержки клиентского программного обеспечения сетей NetWare. Как и в Windows NT, в Windows 2000 используется средство CSNW

Замечание

Обратите внимание CSNW используется для установки соединения компьютера Windows 2000 с сетями NetWare 4 *x* и более ранними Если на сервере NetWare выполняется версия 5 *x*, в которой используются собственные процедуры IP, то установить с ним соединение с помощью CSNW нельзя Это можно сделать с помощью клиентской программы NetWare (редиректора), совместимой с протоколами NCP (NetWare Core Protocol) и IP Соответствующее программное обеспечение можно загрузить по адресу `www.novell.com` То же можно сделать, установив в операционной системе NetWare 5 *x* шлюз IP/IPX

Как показано в диалоговом окне на рис 12 15, в системе Windows 2000 компонент CSNW установлен как сетевая клиентская служебная программа

Установка соединения компьютера Windows 2000 Professional с удаленной сетью

В состав Windows 2000 входит мастер установки удаленного подключения, который проводит пользователя по этапам установки соединения с сервером удаленного доступа. С помощью мастера пользователь может быстро установить соединение с удаленной частной сетью или с Internet, создать VPN (Virtual Private Network) для "туннелирования" своего соединения посредством Internet в удаленную частную сеть, сконфигурировать Windows 2000 Professional как сервер коммутируемого доступа (рис. 12.18).

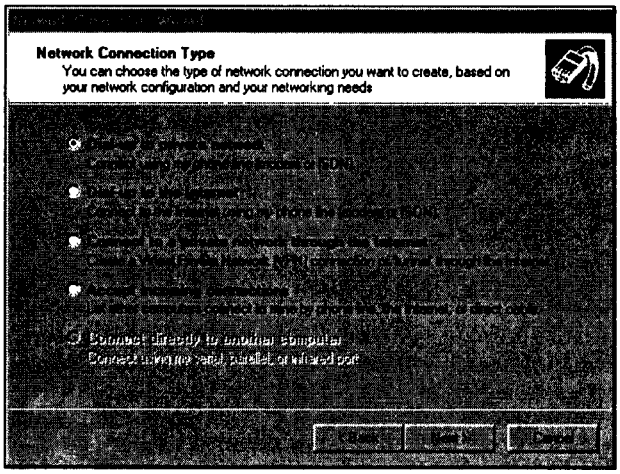


Рис. 12.18. С помощью мастера установки сетевого соединения можно сконфигурировать коммутируемое соединение, создать сеть VPN или сконфигурировать компьютер как сервер удаленного доступа

Систему Windows 2000 можно сконфигурировать на соединение непосредственно с другим компьютером с помощью последовательного или параллельного порта, а также инфракрасного порта. Указанные способы подключения можно использовать для установки соединения карманного компьютера с компьютером Windows 2000 в целях обмена файлами.

Linux/UNIX

UNIX — мощная операционная система. Чаще всего она используется в сетевых серверах, а в клиентских компьютерах применяется достаточно редко. Однако компьютеры UNIX могут получать доступ к файлам сетей Microsoft и NetWare с помощью дополнительного программного обеспечения.

В коммерческих сетях Linux завоевала весьма прочные позиции как сетевая операционная система. Довольно часто она встречается как корпоративная клиентская операционная система. В настоящее время для Linux разработаны графические интерфейсы (рис. 12.19), значительно облегчающие ее использование. Однако она все же требует от пользователя большей квалификации, чем большинство других клиентских операционных систем. Тем не менее многие компании (например, RedHat, SuSE,

Corel, Caldera и TurboLinux) прилагают значительные усилия, чтобы сделать Linux более конкурентоспособной в качестве клиентской операционной системы.

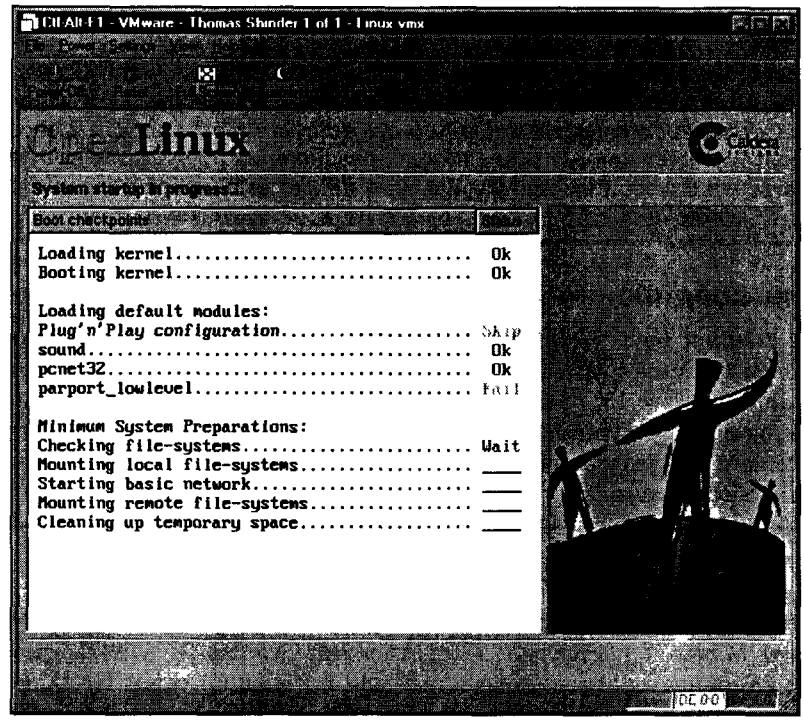


Рис. 12.19. Современные реализации Linux содержат графические интерфейсы, делающие среду более дружественной к пользователю

Последние реализации Linux содержат встроенные сетевые компоненты, с помощью которых можно устанавливать соединение с локальной сетью, коммутируемое соединение с Internet или соединение с удаленной сетью. Протокол TCP/IP фактически интегрирован в ядро операционной системы, а не реализуется как отдельная подсистема.

При использовании Linux в качестве клиентской операционной системы следует учитывать, что в Linux поддерживаются не все приложения. По сравнению с Windows количество коммерческих рабочих приложений в Linux весьма ограниченно. Однако некоторые поставщики предлагают программы эмуляции Windows, позволяющие выполнять в Linux многие приложения Windows. Это такие программы, как WABI или WINE. Кроме того, некоторые компании (например, Corel) создают для Linux версии своих офисных пакетов и других популярных программ.

Можно назвать ряд преимуществ Linux, используемой в качестве сетевой операционной системы или сетевого клиента.

- Это по-настоящему 32-разрядная операционная система.
- В Linux поддерживается вытесняющая многозадачность и виртуальная организация памяти.
- Компьютеры Linux могут разделять файлы с компьютерами UNIX, NetWare, Windows и Macintosh.

Рассмотрим установку соединения клиента Linux/UNIX с сетями Microsoft, NetWare и с Internet посредством сервера коммутируемого доступа.

Замечание

Система UNIX чаще всего используется как серверная операционная система, однако компьютеры UNIX могут работать и как клиенты сети. Конфигурация и набор команд UNIX и Linux во многом совпадают. Однако существует много различных версий Linux и UNIX, поэтому приведенные в следующих разделах инструкции нельзя применить непосредственно к любой их реализации. Тем не менее в любой версии с помощью команды `man` можно просмотреть справочные материалы по конкретной реализации.

Установка соединения клиента Linux/UNIX с сетью Microsoft

Рабочие станции Linux могут получать доступ к файлам сервера Microsoft с помощью файловой системы SMB, построенной на основе кода Samba. (Протокол Samba рассматривается в главе 13, "Гибридные сети".) Для установки соединения с удаленными разделяемыми ресурсами SMB (такими, как на сервере Microsoft), передачи файлов и печати на удаленном принтере в UNIX можно использовать клиентское программное обеспечение SMB — составную часть набора Samba.

Замечание

Протокол SMB (Server Message Block) используется на серверах Microsoft.

Компания Microsoft поставляет пакет Microsoft Services for UNIX, состоящий из нескольких компонентов, предназначенных для интеграции сетей UNIX и Microsoft. В качестве протокола в этом пакете используется NFS (Network File System), позволяющая разделять ресурсы между сетевыми операционными системами с помощью удаленного вызова процедур (Remote Procedure Call — RPC).

В состав пакета Microsoft Services for UNIX входят: клиентская программа, сервер и шлюз NFS. Эти компоненты предоставляют пользователю ряд возможностей.

- Разделение файлов и принтеров между компьютерами UNIX и Windows.
- Установка удаленных соединений между компьютерами UNIX и Windows с помощью командной строки.
- Согласование паролей между компьютерами Windows и UNIX.

Для получения доступа к файлам компьютера UNIX на компьютере Windows 2000 Professional должна быть установлена клиентская часть NFS. Сервер NFS устанавливается на компьютере Windows 2000 Professional или Windows 2000 Server для того, чтобы компьютер UNIX мог получить доступ к файлам компьютера Windows. Шлюз NFS устанавливается на сервере Windows 2000 для того, чтобы этот сервер мог работать в качестве шлюза между протоколом GIFS, используемым в сетях Windows 2000, и протоколом NFS, используемым в сетях UNIX (рис. 12.20). Служебные программы для UNIX обычно могут работать с несколькими версиями UNIX и RedHat Linux.

Установка соединения клиента Linux/UNIX с сервером NetWare

Для получения доступа к файлам и принтерам сетей NetWare операционную систему Linux или UNIX можно конфигурировать как клиента NCP (NetWare Core Proto-

col). Модуль ядра файловой системы Linux позволяет использовать в ней том NetWare с помощью программного обеспечения файловой системы NCP. Если он установлен, то компьютер Linux, эмулируя клиент NetWare, может получать доступ к файловому серверу NetWare или распечатывать свои документы на сервере печати NetWare. Дистрибутив файловой системы NCP можно найти по адресу: `ftp.gwdg.de` или `sunsite.unc.edu`. Более устаревшие версии работали только с NetWare 3 *x* и NetWare 4 *x* в режиме эмуляции базы данных bindery. В последних версиях поддерживается NDS (Novell Directory Services).

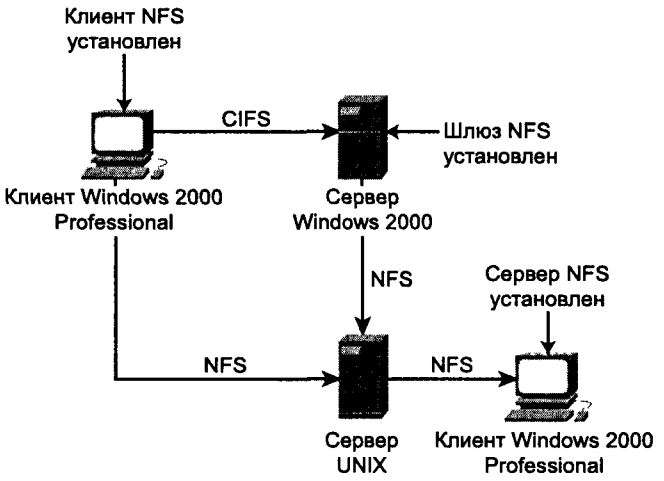


Рис 12 20 С помощью служебных программ Microsoft для UNIX реализуется межоперационное взаимодействие сетей Windows и UNIX

Получить доступ с компьютеров Linux к ресурсам NetWare можно также, установив на сервере NetWare программу-сервер NFS компании Novell.

Установка соединения клиента Linux с сервером Linux/UNIX

Большинство популярных реализаций Linux поставляются с инструментами, необходимыми для конфигурирования сетевых устройств Эти инструменты можно также загрузить по адресу: `ftp.uk.linux.org`. С этого же узла можно загрузить и сетевые приложения Linux — Telnet и FTP.

Для конфигурирования сетевого интерфейса используется команда `ifconfig` В листинге 12 4 с помощью команды `ifconfig` конфигурируется сетевой адаптер Ethernet с именем `eth0` на использование сетевого адреса 192 168 1.16 с маской подсети 255 255 255 0 (маска класса С по умолчанию) Параметр `up` в конце команды активизирует интерфейс

Листинг 12.4. Команда `ifconfig` используется для конфигурирования сетевого интерфейса

```
# ifconfig eth0 192.168.1.16 netmask 255.255.255.0 up
```

Протокол NFS (Network File System) обычно используется в серверной среде UNIX. Этот протокол может также компилироваться с ядром операционной системы Linux. Он включен во многие популярные дистрибутивы Linux, например, в RedHat. Чтобы компьютер Linux можно было использовать в качестве клиента NFS, нужно установить файловую систему NFS с помощью команды `mount`. Сделав это, можно получать доступ к удаленным файлам таким образом, будто они локальные; однако операции доступа выполняются обычно медленнее.

Установка соединения клиента Linux/UNIX с Internet

Для установки коммутируемого соединения компьютера Linux или UNIX с Internet нужно установить соответствующие модули и сконфигурировать последовательный порт на использование модема.

Если провайдер предоставляет доступ с помощью оболочки, то установить соединение непосредственно с ней можно с помощью программы minicom. Такая учетная запись представляет собой командный интерфейс сервера UNIX, к которому можно получить доступ посредством Telnet. При этом компьютер Linux должен быть сконфигурирован с приведенными ниже параметрами.

- Адрес DNS (определяется в файле `/etc/revolv.conf`).
- Фиксированный IP-адрес (определяется в файле `etc/hosts`).
- Внешний почтовый домен (определяется в файле `/etc/mailname`).
- Имя учетной записи и пароль, присвоенные пользователю провайдером. Если используется протокол PAP (Password Authentication Protocol), то эти параметры определяются в файле `etc/ppp/pap-secrets`, а если CHAP (Challenge Handshake Authentication Protocol), то в `/etc/ppp/chap-secrets`.

Сценарий соединения, определяющий процедуру установки соединения, находится в файле `/etc/ppp/chatscript`. Сценарий содержит строку инициализации модема, телефонный номер сервера провайдера и другую информацию, зависящую от регистрационных процедур сервера провайдера.

Протокол PPP (Point-to-Point Protocol) часто используется для установки соединения по телефонной линии. В некоторых случаях вместо него используют протоколы SLIP (Serial Line Internet Protocol) или UUCP (UNIX-to-UNIX Copy Protocol).

После установки соединения можно войти в сеть посредством текстового броузера Lynx. Если установлена система X Window или другая графическая оболочка, то работать в сети можно с помощью Netscape или другого графического броузера. Для отправки электронного письма используется программа Sendmail, а для его приема — протокол POP (Post Office Protocol) версии 3.

Существуют и другие почтовые программы UNIX/Linux, включая Pine, Elm, Fetchmail, Smail и Procmail. В частности, программа Procmail может сортировать входящие письма, генерировать автоответы и выполнять другие подобные задачи.

Macintosh

В этой системе сетевые интерфейсы часто включены в состав сетевых компонентов, встроенных в операционную систему Macintosh. Для компьютеров Macintosh разработаны также сетевые адаптеры для сетей Ethernet и TokenRing.

Операционная система Macintosh, или Mac, популярна во многих образовательных и корпоративных организациях. Компьютеры Mac можно объединять в рабочие группы и получать из них доступ к файловым серверам Applshare Их можно также подключать к локальным сетям персональных компьютеров, содержащим серверы Microsoft, NetWare и UNIX

Рассмотрим установку соединений компьютеров Macintosh со своей рабочей группой, с серверами Windows, NetWare и UNIX/Linux и с Internet посредством сервера удаленного доступа.

Объединение компьютеров Macintosh в рабочую группу

С помощью сетевых компонентов и протоколов AppleTalk компьютеры Macintosh легко и быстро объединяются в рабочую группу. В ранних реализациях использовались более медленные последовательные сетевые соединения LocalTalk. Современные системы все еще поддерживают LocalTalk, однако новые версии AppleTalk обладают более высокой производительностью, кроме того, они обеспечивают межоперационное взаимодействие с другими операционными системами. В системе LocalTalk для физического подключения к сети разработана специальная соединительная коробка, к которой подключается последовательный порт и телефонный кабель.

В системе AppleTalk используется концепция *зоны*, которая в данном случае означает логически сгруппированные ресурсы. Зоне аналогична рабочая группа в сетях персональных компьютеров. При установке соединения с сетью AppleTalk из меню можно получить список зон. Для просмотра списка зон система AppleTalk должна быть установлена как "активная" в окне Chooser. Иногда может понадобиться задание типа сети (LocalTalk или EtherTalk) Это делается в диалоговом окне Network Control Panel (Панель управления сетью), которое открывается из каталога Control Panel, расположенного в каталоге System.

Установка соединения компьютера Macintosh с сетями Microsoft, NetWare и UNIX

Всего несколько лет назад было трудно или даже невозможно установить соединение компьютеров Apple с сетями персональных компьютеров Однако сейчас уже существует самое разнообразное программное обеспечение, позволяющее пользователям Macintosh работать в сетях Microsoft, NetWare и UNIX

Для установки соединений с сетями Macintosh компания Microsoft предоставляет в составе Windows NT/2000 следующие компоненты:

- файловые серверы для Macintosh;
- серверы печати для Macintosh;
- протокол AppleTalk.

Когда эти компоненты установлены на сервере Windows, клиенты Macintosh могут получать доступ к файлам и принтерам сети Microsoft. Сервер Windows может также работать как маршрутизатор AppleTalk, для этого на компьютерах Macintosh не требуется устанавливать дополнительное программное обеспечение.

Для серверов NetWare разработан добавляемый модуль, делающий их видимыми для клиентов Macintosh так, будто это серверы Applshare. Добавляемый модуль называется модулем NetWare для Macintosh NLM (NetWare Loadable Module). Модуль принимает и обрабатывает пакеты данных AppleTalk, передаваемые компью-

тером Macintosh. В протоколе IPX компьютеры Macintosh могут также работать в сети NetWare 4.0.

С помощью программного обеспечения Syntax клиенты Macintosh (как и клиенты DOS, Windows и OS/2) могут получать доступ к файлам, принтерам и приложениям сервера UNIX.

Существующие сети AppleTalk можно подключить к корпоративным локальным сетям с помощью шлюзов и маршрутизаторов. Разработанные специально для этого устройства поставляются многими компаниями, например Shiva.

Установка соединений компьютеров Macintosh с Internet

Чтобы подключить компьютер Macintosh к Internet, на нем, как и на любом другом компьютере, должен быть настроен протокол TCP/IP. Компания Apple поставляет реализацию TCP/IP под названием AppleIP. Этой же цели служат и другие коммерческие продукты, например MacTCP. Если на компьютере Macintosh установлены эти протоколы, то он может сообщаться с локальными и глобальными сетями на основе TCP/IP.

Как и в других операционных системах, должны быть сконфигурированы следующие параметры TCP/IP: IP-адрес, маска подсети и шлюз по умолчанию (если это необходимо). Для отображения имен хостов на IP-адреса необходимо выбрать также адрес сервера DNS. Вид диалогового окна конфигурирования зависит от конкретной реализации используемого программного обеспечения.

Если для установки соединения с Internet используется модем, то на компьютере Macintosh должен быть конфигурирован протокол PPP (Point-to-Point Protocol). Программное обеспечение PPP для Macintosh можно найти в Web. Одна из таких программ называется ConfigPPP. При конфигурировании этих программ пользователь вводит порт модема, скорость порта, время существования соединения, параметры соединения и телефонный номер удаленного сервера.

В компьютерах iMac пользователю предоставляется программа Internet Setup Assistant (рис. 12.21). Аналогично мастерам Windows, эта программа проводит пользователя по этапам процесса конфигурирования соединения.

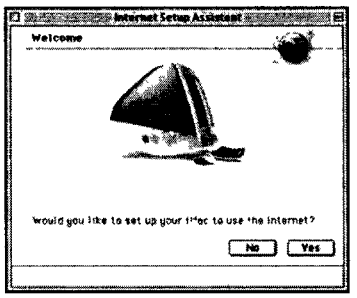


Рис. 12.21. В компьютере iMac пользователю предоставлен интерфейс конфигурирования соединений с Internet

OS/2

Компания IBM прекратила поддержку и развитие настольной операционной системы OS/2 в середине 1990-х годов, однако все еще остается довольно много стойких приверженцев этой системы. В настоящее время OS/2 можно встретить в некоторых коммерческих сетях, особенно в банковской сфере.

В свое время разработка OS/2 началась как совместный проект IBM и Macintosh. Когда эти компании прекратили сотрудничество, Microsoft разработала Windows NT (частично на основе OS/2), а IBM выпустила на рынок OS/2, позже переименовав ее в OS/2 Warp.

Замечание

Компания IBM все еще поставляет и поддерживает OS/2 Wrap Server. Текущая версия Warp Server разработана как сервер электронной коммерции и поставляется большим компаниям, выполняющим коммерческие операции посредством Internet.

Установить соединение операционной системы OS/2 с серверами NetWare можно с помощью пакета NetWare Client Kit for OS/2 компании Novell. Для сообщения OS/2 с сетями TCP/IP используется программное обеспечение TCP/IP компании IBM. Для поддержки NFS, NetBIOS и IPX/SPX компания IBM разработала дополнительно устанавливаемый пакет программ.

В OS/2 Warp версии 4 включены поддержка коммутируемых соединений и средства установки соединений с Internet.

Резюме

В этой главе рассмотрены наиболее распространенные клиентские операционные системы и их использование в качестве клиентов различных типов сетей.

Глава начинается с обзора основ операционных систем. Рассматриваются два типа пользовательских интерфейсов: текстовые и графические. Затем описывается синтаксис команд и их параметры.

Далее представлены файлы и файловые системы, соглашения об именах файлов, расширения различных типов файлов и использование расширений операционной системой и приложениями. Рассмотрены наиболее популярные файловые системы: FAT/FAT32, NTFS, файловая система UNIX, HPFS, Macintosh HFS и NFS. Описано использование дисков и создание разделов дисков.

Затем каждая операционная система рассматривалась отдельно: клиентские операционные системы MS DOS и Windows компании Microsoft, Linux/UNIX, Apple Macintosh и OS/2 компании IBM.

В главах 7–11 изложены основные сведения о базовых компонентах сетевых технологий, включая протоколы, популярные сетевые операционные системы (серверы), службы каталогов и клиентские операционные системы. В следующей главе все эти вопросы будут вновь затронуты при рассмотрении гибридных сетей, в которых одновременно используются многие протоколы, платформы и операционные системы.

Рекомендуемые источники

Обзор файловых систем FAT, VFAT, FAT32 и NTFS приведен на Web-узле компании Microsoft по адресу: `www.microsoft.com/technet/winnt/filesyst.asp`.

Обсуждение и документацию файловой системы NTFS можно найти на Web-узле по адресу: `www.via.ecp.fr/~regis/ntfs/new`.

Хороший учебник по файловой системе UNIX можно найти по адресу: `www.anet-stl.com/tech/unix/Pages/concepts_fsystem.html`.

Программу разделения дисков Partition Magic можно загрузить по адресу: `www.powerquest.com`.

Изучение операционных систем и сетевых компонентов Microsoft лучше всего начать с материалов Web-узла TechNet: `www.microsoft.com/technet/default.asp`.

Списки источников, советы и руководства по операционной системе и сетям Linux можно найти по адресу: `www.linuxhq.com`.

Хороший источник информации по межоперационному взаимодействию и установке соединений компьютеров Macintosh с сетями персональных компьютеров представлен по адресу: `www.macwindows.com/Network.html`.

Дополнительную информацию об OS/2 Warp можно найти, пользуясь предметным указателем, приведенным по адресу: `www.nfwa.com/os2/news/e-zines.html`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Что из приведенного является преимуществом текстовых операционных систем? (Выберите все, что подходит.)
   - **а.** По сравнению с системами с графическим интерфейсом их быстродействие выше.
   - **б.** Они требуют меньше ресурсов, чем графические системы.
   - **в.** Их легче использовать, чем графические системы.
   - **г.** В отличие от графических операционных систем они поддерживают многозадачность.
2. Какая из приведенных команд используется для вывода конфигурационной информации TCP/IP в операционной системе Windows 95?
   - **а.** ifconfig.
   - **б.** ipconfug.
   - **в.** winipcfg.
   - **г.** config.
3. Как называется суффикс из двух или трех символов, расположенный после точки в конце имени файла?
   - **а.** Ветвь файла.
   - **б.** Файловая таблица.
   - **в.** Тип файла.
   - **г.** Расширение файла.
4. Что из приведенного является преимуществом файловой системы FAT16 в операционной системе Microsoft?
   - **а.** Количество операционных систем, с которыми она совместима, больше, чем у любой другой файловой системы.
   - **б.** Она обеспечивает большую безопасность, чем другие популярные файловые системы.

в. Она более надежна (менее подвержена потерям данных), чем любая другая популярная файловая система.

г. Она обеспечивает лучшую производительность, чем любая другая файловая система.

5. Какой максимальный размер раздела поддерживается файловой системой NTFS?

   а. 2 Гбайт.

   б. 4 Гбайт.

   в. 4 Тбайт.

   г. 16 Эбайт.

6. Какая из приведенных строк является маршрутом в файловой системе UNIX?

   а. c:/dir01/subdir02/myfile.ext.

   б. \dir01\subdir02\myfile.ext.

   в. /dir01/subdir02/myfile.ext.

   г. /dir01/subdir02\myfile.ext.

7. В какой из приведенных файловых систем используется нумерация i-узлов?

   а. FAT32.

   б. Файловая система UNIX.

   в. Macintosh HFS.

   г. NTFS.

8. Какой компонент установить, чтобы пользователь клиентского компьютера Windows NT мог зарегистрироваться непосредственно на сервере NetWare?

   а. File and Print Services for NetWare.

   б. Gateway Services for NetWare.

   в. Client Services for NetWare.

   г. IPX/SPX.

9. С помощью чего клиентский компьютер Linux может получить доступ к файлам сервера Microsoft?

   а. SMBFS.

   б. NCP.

   в. TCP/IP.

   г. PPP.

10. В какой из приведенных операционных систем используется файловая система HPFS?

    а. MS DOS.

    б. Windows 2000.

    в. OS/2.

    г. Windows NT 4.0.

Глава 13

Гибридные сети

В части II, "Сетевое оборудование и программное обеспечение", рассмотрены различные сетевые протоколы, используемые для установки соединений между компьютерами, популярные сетевые операционные системы, выполняемые на серверах, и клиентские операционные системы, выполняемые на клиентских компьютерах. Описаны также службы каталогов, предназначенные для организации хранения и поиска сетевых ресурсов, и глобальная сеть, объединяющая многие локальные и глобальные сети, — Internet.

Гибридная сеть — это сеть, в которой сосуществуют разные операционные системы, типы оборудования, протоколы и службы. Наибольшей гибридной сетью является, естественно, Internet. Гибридные сети довольно распространены, в сегодняшнем корпоративном мире даже небольшие локальные сети работают как гибридные.

В этой главе рассматриваются основные принципы работы в гибридных сетях, состоящих из компонентов оборудования и программного обеспечения различных типов. Главное внимание уделено трем категориям гибридных сетей.

- Сети с разными протоколами.
- Сети с разными операционными системами (как серверными, так и клиентскими).
- Сети на основе разнотипного оборудования.

Естественно, конкретная сеть может одновременно принадлежать к нескольким категориям.

Прежде чем подробно рассмотреть каждую из этих категорий, остановимся на общих характеристиках гибридных сетей и на причинах их реализации как гибридных.

Характеристики гибридных сетей

Существуют определенные преимущества построения сети в "чистом" виде, т.е. на однотипном оборудовании, на основе одной операционной системы и с одним стеком протоколов. Однако существуют также многочисленные причины, побуждающие включать в сеть компоненты разных поставщиков:

- невозможность реализации всех необходимых средств и характеристик сети с помощью компонентов одного поставщика;
- личные предпочтения пользователей;

- финансовые соображения;
- непредсказуемый рост сети.

Рассмотрим каждую из причин создания гибридных сетей.

Невозможность реализации требуемых характеристик на основе компонентов одного поставщика

Одна из главных причин объединения различных платформ и операционных систем в одной сети — неспособность одного поставщика предоставить все необходимые компоненты с нужными характеристиками.

Например, первоначально сеть была построена на основе серверов UINX. Однако со временем, скорее всего, окажется, что в сети должны выполняться также приложения, предоставляемые только серверами Windows NT/2000. Другой пример: допустим, на клиентских компьютерах выполняется операционная система Windows 9*x*, причем понадобилось, чтобы они сообщались друг с другом с помощью имен NetBIOS. Решить эту задачу можно, установив сервер Windows NT/2000 как сервер WINS, предоставляющий имена NetBIOS для разрешения IP-адресов.

Еще один пример: допустим, в сети Windows NT установлены клиенты Windows 9*x*, а какому-то отделу понадобились графические приложения, выполняющиеся только на платформе Macintosh. В этом случае можно установить системы Macintosh в этом единственном отделе, а на серверах NT дополнительно установить служебные программы для Macintosh, тогда клиенты Macintosh смогут получать доступ к сетевым файлам.

Личные предпочтения пользователей

В некоторых компаниях служащим разрешено выбирать операционную систему. Для пользователей управленческого уровня это практикуется довольно часто. Если в сети Windows 2000 установлены клиенты Windows 2000 Professional, а вице-президент компании предпочитает Linux, то можно интегрировать клиентский компьютер Linux в сеть Microsoft.

Финансовые соображения

Часто реализации чистой сети препятствует ограниченное финансирование. Например, компания запланировала переход с NetWare на Windows 2000, однако денег на приобретение лицензий на программное обеспечение Windows одновременно для всех серверов выделено недостаточно. В этом случае компания может переходить на Windows постепенно, временно оставив на части серверов программное обеспечение NetWare. При этом сеть некоторое время будет гибридной.

Аналогичная ситуация возникает, когда организация решает перевести клиентские компьютеры своих пользователей на Windows 2000 Professional, но не может оплатить замену оборудования на всех рабочих станциях. В таком случае клиентские компьютеры, не удовлетворяющие требованиям Windows 2000, могут продолжать работать на основе более старых версий Windows или других операционных систем, предъявляющих менее жесткие требования к оборудованию, например Linux.

Непредсказуемый рост сети

Во многих случаях реального плана реализации гибридной сети не существует. Оборудование и программное обеспечение покупаются и устанавливаются постепенно, в зависимости от конъюнктуры рынка и результатов торговых переговоров.

Рассмотрим такую ситуацию. Компания решила установить серверы NetWare, возможно, потому что сетевой администратор имел соответствующую квалификацию и сертификат NetWare. Позже решено было добавить серверы NT, так как программные продукты Microsoft становятся все более популярными. Затем компания решила установить собственный Web-узел и наняла Web-дизайнера, который предпочитает программное обеспечение Apache, выполняющееся на компьютерах UNIX/Linux. В результате в сети появился Web-сервер на платформе Linux. И наконец, чтобы окончательно запутать ситуацию, руководство компании решило, что к сети персональных компьютеров необходимо подключить мэйнфрейм IBM, работающий в бухгалтерии компании. Теперь представьте себя в роли сетевого администратора, которому нужно объединить все эти системы в гибридную сеть.

Сети на основе многих протоколов

В компьютерных сетях используются многие типы протоколов, работающих на разных уровнях сетевой модели.

Собственно говоря, в *любой* сети используются многие протоколы. Однако, когда речь идет о множественности протоколов при обсуждении гибридных сетей, подразумеваются главным образом два случая.

- В сети используется более одного протокола сетевого/транспортного уровня.
- В сети используется более одного протокола разделения файлов (которые иногда называются *протоколами ядра*).

Протоколы сетевого/транспортного уровня

Чтобы компьютеры могли сообщаться друг с другом посредством сети, на них должен быть установлен один и тот же стек протоколов сетевого/транспортного уровня, например TCP/IP, IPX/SPX или NetBEUI. Во многих случаях в сети необходимо более одного стека протоколов сетевого/транспортного уровня. Можно назвать следующие причины использования в сети многих протоколов:

- наличие нескольких сетевых операционных систем;
- необходимость установки соединений с Internet;
- соображения безопасности.

Рассмотрим каждую из этих причин отдельно.

Множество сетевых операционных систем

Чаще всего необходимость в нескольких протоколах возникает в связи с использованием гибридных сетей Microsoft/NetWare.

Сети NetWare 5.*x* могут работать с чистым IP, однако в корпоративных сетях все еще применяется много серверов NetWare 3.*x* и 4.*x*, требующих использования в сетевой коммуникации стека протоколов IPX/SPX.

Обычно в сетях средних или больших размеров клиенты сообщаются с серверами Microsoft с помощью TCP/IP. Если этим же клиентам нужен доступ к файлам серверов NetWare 3.*x* или 4.*x*, то для этого у них должно быть установлено не только клиентское программное обеспечение Novell или Microsoft, но и реализации стека протоколов IPX/SPX, например NWLink.

Соединения с Internet

Если в компании эксплуатируется небольшая сеть Microsoft, состоящая только из одной немаршрутизируемой подсети, то для установки локальных соединений в этой сети может использоваться протокол NetBEUI, так как он более быстродействующий, его легче конфигурировать и в нем проще устранять неполадки, чем в NWLink или в TCP/IP.

Однако для установки соединений компьютеров такой локальной сети с Internet все же должен использоваться стек протоколов глобальных сетей TCP/IP. В целях повышения производительности компьютеры могут использовать для сообщения друг с другом протокол NetBEUI, а для сообщения с Internet — TCP/IP.

Замечание

Если небольшая сеть подключается к Internet с помощью NAT (Network Address Translation), то на каждом компьютере, получающем доступ к Internet, должен быть установлен TCP/IP. Это справедливо, даже если непосредственно к Internet подключен только один хост NAT, потому что в методе NAT для идентификации локальных компьютеров им должны быть присвоены IP-адреса из набора частных адресов.

Возможен также случай, когда клиентам, получающим доступ к серверам NetWare, нужно сообщаться с операционными системами Microsoft и устанавливать соединение с Internet посредством хоста NAT. Для этого придется использовать три протокола — IPX/SPX, NetBEUI и TCP/IP, причем все они должны быть установлены на одном компьютере и связаны с одним сетевым адаптером.

Использование многих протоколов из соображений безопасности

Некоторые сетевые администраторы устанавливают во внутренней сети (или в ее части) отличный от TCP/IP стек сетевых/транспортных протоколов для того, чтобы повысить безопасность сети при подключении ее к Internet.

Допустим, некоторая группа сетевых компьютеров содержит особо ценные данные. Для повышения их безопасности можно установить на них не TCP/IP, а IPX/SPX. Тогда эти компьютеры не смогут сообщаться с Internet. Другие компьютеры внутренней сети могут сообщаться с ними посредством IPX/SPX, а с внешним миром — посредством TCP/IP. Компьютеры, установленные за пределами внутренней сети и не использующие IPX/SPX (это типичный профиль сконфигурированных для Internet компьютеров), не смогут получить доступ к компьютерам IPX/SPX, потому что у них нет общего протокола. Такая конфигурация сети показана на рис. 13.1.

Замечание

Обычно стек IPX/SPX ассоциируется с сетями NetWare, однако его можно использовать также в соединениях локальных сетей, содержащих только операционные системы Microsoft. Если установка соединений с Internet не требуется, то такое решение

вполне приемлемо, поскольку маршрутизируемый стек IPX/SPX обладает более высоким быстродействием, чем TCP/IP; кроме того, его легче конфигурировать.

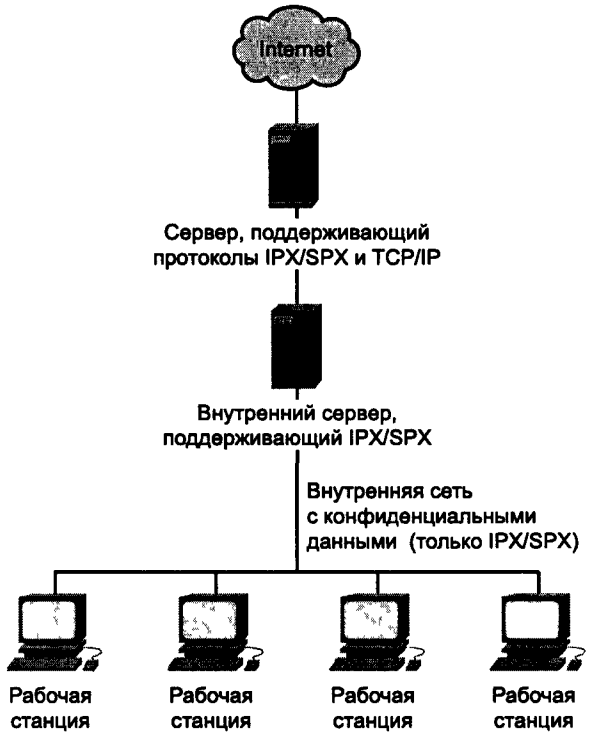


Рис. 13.1. Одновременно несколько протоколов можно использовать для защиты части сети от внешнего вторжения

Порядок связывания протоколов

Если с одним сетевым адаптером связано несколько стеков протоколов сетевого/транспортного уровня, то большое значение имеет порядок их связывания. *Порядок связывания* протоколов на клиентском компьютере определяет, какой протокол будет использован для сообщения с сервером, когда на этих двух компьютерах установлено более одного общего протокола.

Замечание

Спецификации NDIS (Network Driver Interface Specification) компании Microsoft и ODI (Open Datalink Interface) компании Novell допускают связывание многих протоколов с одним сетевым адаптером и наоборот — многих сетевых адаптеров с одним протоколом.

Допустим, что на клиентском компьютере установлены и связаны в перечисленном здесь порядке протоколы TCP/IP, NetBEUI и IPX/SPX, а на сервере — NetBEUI, IPX/SPX и TCP/IP. Тогда клиентский компьютер сначала пытается установить соединение на основе протокола TCP/IP, расположенного первым в его последовательно-

сти связывания. Если на сервере протокол TCP/IP оказывается установленным, то он используется в сеансе связи, несмотря на то что в последовательности связывания сервера он расположен последним. Отсюда следует, что для оптимизации производительности сети нужно располагать на клиентских компьютерах наиболее часто используемые протоколы в начале последовательности связывания.

На рис. 13.2 показано, как в системе Windows 2000 можно сконфигурировать несколько протоколов конкретного сетевого адаптера или изменить порядок их связывания. Пользователь может выбрать и перемещать установленный протокол вверх или вниз в последовательности связывания с помощью кнопок "вверх" и "вниз".

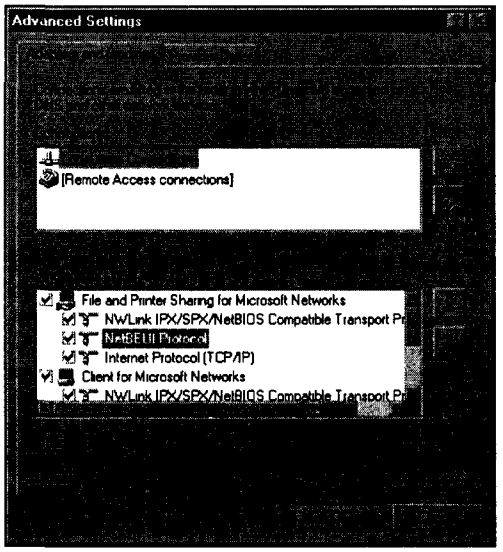


Рис. 13.2. Если используется несколько протоколов, то для оптимизации производительности можно изменить порядок их связывания

В других операционных системах способы конфигурирования порядка связывания аналогичны приведенному.

Протоколы разделения файлов

Второй тип протоколов, используемых для сообщения в гибридной сети, — *протоколы разделения файлов*, которые иногда называют протоколами ядра. В сетях Microsoft для разделения файлов используется протокол SMB (Server Message Block), в сетях NetWare — NCP (NetWare Core Protocol), а в системе UNIX — NFS (Network File System).

Для получения доступа к файлам сервера на компьютере должно быть установлено соответствующее клиентское программное обеспечение. Например, установить на компьютере с Windows клиентское программное обеспечение NCP можно путем установки на нем программы Client Service for NetWare компании Microsoft или какой-либо клиентской программы компании Novell. В состав Samba входит клиентское программное обеспечение SMB для компьютеров UNIX, что позволяет им получать доступ к серверам Microsoft с помощью протокола разделения файлов SMB.

Сети с несколькими операционными системами

В сетях с несколькими операционными системами может использоваться несколько протоколов сетевого/транспортного уровня, однако они могут работать и на основе одного протокола. Протокол TCP/IP поддерживается почти всеми системами (системы NetWare версий 5.0 и выше могут работать только с TCP/IP), поэтому в сети с несколькими операционными системами компьютеры могут сообщаться с помощью одного и того же стека протоколов.

Гибридные сети с несколькими операционными системами можно разделить на три типа.

- Сети, в которых установлено несколько сетевых операционных систем.
- Сети, в которых используется одна серверная и несколько клиентских операционных систем.
- Сети, в которых используется несколько серверных и несколько клиентских операционных систем.

Сети с несколькими серверными операционными системами

В сети может быть несколько серверов, на которых работают разные операционные системы. Например, сеть может содержать несколько контроллеров доменов на основе как Windows 2000, так и Windows NT, файловые серверы и серверы печати NetWare, FTP- и Web-серверы на основе UNIX или Linux (рис. 13.3). Подобная конфигурация гибридной сети довольно распространена.

Задача сетевого администратора — создать среду, в которой пользователи могут получать доступ к файлам и другим нужным им ресурсам независимо от операционной системы.

К счастью, существуют пакеты, с помощью которых клиентам можно предоставить доступ к разным серверам. Некоторые из этих пакетов включены в состав клиентских операционных систем. Есть и пакеты, разработанные другими компаниями. Ниже перечислены наиболее распространенные пакеты программ, используемые для интеграции разных операционных систем.

- **Client Services for NetWare (CSNW)**. Включены в состав Windows NT Workstation и Windows 2000 Professional. Позволяют клиентам Windows NT/2000 получать доступ к серверам NetWare.
- **Microsoft Client for NetWare Networks**. Включена в состав операционных систем Windows 9*x*. Выполняет те же функции, что и CSNW, однако для клиентов Windows 95/98.
- **Gateway Service for NetWare (GSNW)**. Включена в состав операционных систем Windows NT Server и Windows 2000 Server. Позволяет клиентам зарегистрироваться на сервере Windows и получать доступ к ресурсам сервера NetWare через шлюз на сервере Windows NT/2000.

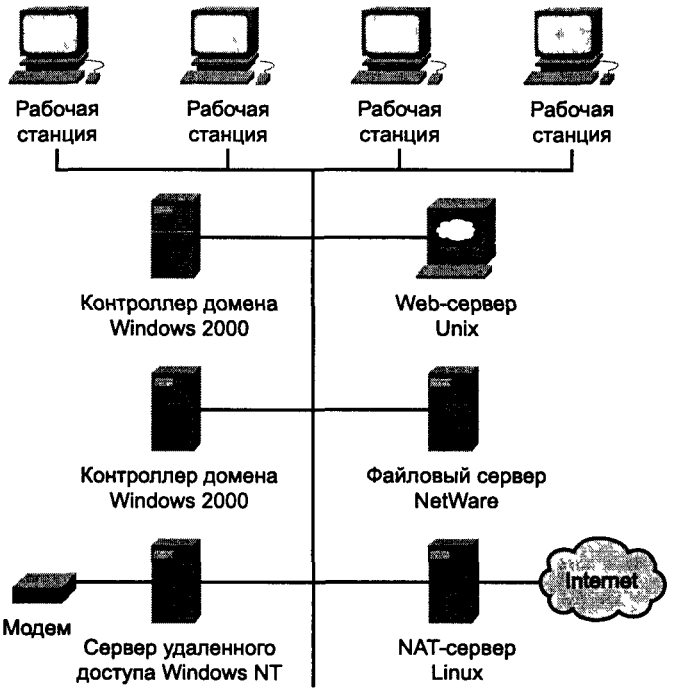


Рис. 13.3. В гибридной сети на серверах может быть установлено несколько разных сетевых операционных систем

- **Novell Client for Windows 9x/NT/2000**. Распространяется бесплатно. Можно загрузить с Web-узла компании Novell. Позволяет компьютерам Windows получать доступ к файлам сервера NetWare.
- **Samba**. Распространяется бесплатно как программный продукт независимой компании. Позволяет клиентам SMB (например, клиентам Windows) получать доступ к файлам сервера UNIX, на котором выполняется программное обеспечение Samba.
- **SMBFS (SMB File System)**. Распространяется в составе Samba. Позволяет компьютерам UNIX отображать сетевые логические диски на разделяемые ресурсы SMB.
- **Microsoft Services for Macintosh**. Входит в поставку Windows NT/2000 Server. Позволяет клиентам Macintosh получать доступ к ресурсам сетей Microsoft.
- **Linux Service for Macintosh**. Реализованы в программных продуктах независимых компаний, например CAP (Columbia AppleTalk Package), или в Netatalk. Позволяет компьютерам Macintosh получать доступ к ресурсам компьютеров Linux путем добавления протокола DDP (AppleTalk Datagram Delivery Protocol) в ядро Linux.

Несколько клиентских операционных систем

Конфигурировать сетевые клиентские компьютеры, на которых функционируют разные операционные системы, значительно проще, чем серверы с разными системами. В главе 12, "Клиентские операционные системы", подробно рассмотрен процесс конфигурирования клиентских систем для установки соединения с разными сетевыми операционными системами.

Несколько серверных и клиентских операционных систем

Часто встречаются гибридные сети, содержащие много серверных операционных систем и много клиентских операционных систем. Это несколько усложняет задачи администрирования, потому что нужно знать, как управлять разными операционными системами. Работая в такой сложной среде, особенно важно получать новейшую информацию о служебных пакетах и последних исправлениях всех операционных систем, работающих в сети. В противном случае администратор неизбежно обрекает сеть на низкую эффективность или подвергает ее риску взлома.

Сети на основе нескольких платформ

Термин *платформа* иногда используется для обозначения операционных систем, например платформа UNIX или платформа Windows. В этой книге термин *платформа* обозначает тип сетевой архитектуры или оборудования. Необходимо, однако, отметить, что на разных платформах часто (хотя и не всегда) выполняются разные операционные системы.

Например, *платформа персональных компьютеров* предполагает архитектуру и оборудование, отличающиеся от *платформы Macintosh* или *платформы мэйнфреймов IBM*. Новая и набирающая все большую популярность вычислительная платформа используется в карманных персональных компьютерах (КПК) Конфигурация оборудования этой платформы существенно отличается от платформы персональных компьютеров

Далее рассмотрим сетевую коммуникацию между следующими платформами.

- персональных компьютеров и компьютеров Macintosh;
- персональных компьютеров и мэйнфреймов;
- персональных компьютеров и КПК.

Коммуникация персональных компьютеров с компьютерами Macintosh

Сетевая коммуникация между IBM-совместимыми персональными компьютерами (так называемыми IBM, потому что эта компания первой начала производство и распространение персональных компьютеров) и компьютерами Macintosh реализуется относительно просто. Это объясняется тем, что названные платформы близки по производительности и масштабам использования. Обычно взаимодействие между этими платформами рассматривается как взаимодействие между операционными системами, подробно рассмотренное выше в главе.

Коммуникация персональных компьютеров с мэйнфреймами

Концепции и техническая реализация мэйнфреймов (например, IBM AS/400) и различных моделей персональных компьютеров существенно отличаются друг от друга. Однако во многих случаях мэйнфреймы используются для обработки больших объемов данных и взаимодействуют с сетями персональных компьютеров.

Например, в городском совете мэйнфрейм используется для обработки счетов за коммунальные услуги и налогов на недвижимость. В районных отделах служащие, скорее всего, общаются с этой машиной с помощью терминалов ввода данных. Служащие других отделов используют персональные компьютеры для обработки текстов, передачи и приема электронных писем, работы с электронными таблицами и базами данных и т.д. Однако этим служащим время от времени нужен доступ к данным на мэйнфрейме. Один из способов предоставить им такой доступ — размещение на рабочих местах (дополнительно к персональным компьютерам) терминалов мэйнфрейма. Такое решение имеет ряд недостатков.

- Дополнительные расходы на избыточное оборудование. (У персональных компьютеров уже есть дисплей и клавиатура, зачем же тратить деньги на еще один дисплей и еще одну клавиатуру?)
- Загромождение рабочего места техникой, которая будет мешать служащему.
- Дополнительные проблемы с обменом данными между терминалом и персональным компьютером.

Более оптимальное решение — подключить к мэйнфрейму персональные компьютеры служащих. Тогда персональные компьютеры будут работать как терминалы мэйнфрейма, сохранив при этом все функциональные возможности настольных компьютеров. В мэйнфреймах и персональных компьютерах для сетевой коммуникации используются разные протоколы, поэтому для установки соединения между ними нужен *протокольный шлюз*.

Для коммуникации сетей персональных компьютеров с мэйнфреймами IBM чаще всего используется архитектура SNA (Systems Network Architecture), которая описывается далее в главе.

Коммуникация персональных компьютеров с карманными компьютерами

В нашем все более мобильном мире популярность портативных устройств неуклонно растет. Устройства КПК — это простые карманные компьютеры, функции которых ограничены поддержкой адресных книг, календарей, расписаний, записных книжек, а также отправкой и получением электронных писем. Более сложные КПК содержат дополнительные программы, загружаемые в программный модуль, который обычно представляет собой карту памяти. По мере наращивания функциональных возможностей грань между КПК и полнофункциональными портативными компьютерами постепенно стирается. Примером последних служат устройства Palm и Pocket PC.

Карманные устройства должны иметь возможность сообщаться с настольными компьютерами таким образом, чтобы пользователь мог вводить новые данные в одно из этих устройств и согласовывать введенные данные с информацией, хранящейся в другом устройстве. Допустим, пользователь карманного устройства встречает на улице своего делового партнера, получает от него какие-либо полезные сведения (адрес, номер телефона, коммерческие предложения) и записывает их в память устройства. После этого пользователь должен иметь возможность автоматически перенести введенные данные в свой настольный компьютер.

В большинстве карманных устройств предусмотрены средства установки соединения с настольным компьютером посредством последовательного порта или порта

USB. Существуют программы согласования данных карманного и настольного компьютеров, позволяющие автоматически находить изменения и обновлять информацию, например программа ActiveSynch компании Microsoft, обслуживающая коммуникацию между настольными компьютерами Windows и устройствами Windows CE. Между устройствами можно переносить файлы данных и программ. Программное обеспечение для карманных компьютеров можно загрузить из Internet в настольный компьютер, а затем установить его в карманном устройстве посредством последовательного порта или какого-либо другого соединения.

Шлюз как еще один способ гибридного соединения

В области компьютерных сетей термин *шлюз*, или *служба шлюза*, в зависимости от контекста имеет несколько значений. В общем случае шлюз — это точка в сети, выполняющая функции входа в другую сеть. Этому определению может удовлетворять также маршрутизатор, поскольку он служит точкой выхода из подсети либо точкой соединения двух разных подсетей или сетей.

Программное обеспечение шлюзов (например, Gateway Service for NetWare) позволяет двум сетям разного типа сообщаться друг с другом. Иными словами, оно служит связующим звеном между компьютерами, в которых используются разные протоколы, операционные системы и платформы.

Далее рассматриваются разные типы программного обеспечения шлюзов, включая следующие:

- редиректоры Windows–NetWare;
- соединения Macintosh и персональных компьютеров;
- соединения SNA между мэйнфреймами и персональными компьютерами.

Редиректоры Windows–NetWare

Пакет FPNW (File and Print Service for NetWare) позволяет клиентам NetWare получать доступ к ресурсам серверов Windows. Пакеты такого типа иногда называют *редиректорами*, потому что они перехватывают запрос к ресурсу, преобразуют его в соответствующем протоколе разделения файлов и перенаправляют на сервер, на котором хранятся нужные данные. Поскольку программа преобразует запрос в другой протокол, она относится к категории программного обеспечения шлюза.

Редиректоры NetWare, включенные в операционные системы Windows, содержат программу NWLink, представляющую собой совместимую с NDIS (Network Driver Interface Specification) 32-разрядную реализацию стека протоколов IPX/SPX компании Novell. В NWLink коммуникация выполняется с помощью одного из двух интерфейсов прикладного программирования — Winsock или NetBIOS.

Замечание

Для установки соединения с приложением типа клиент/сервер (например, с базой данных SQL) не требуется клиентское программное обеспечение разделения файлов и принтеров. Например, клиент NetWare может получать доступ к приложениям кли-

ент/сервер на Windows NT Server без установки FPNW, а клиент Windows — к приложениям клиент/сервер на сервере NetWare без CSNW, GSNW или любой другой клиентской программы Novell. Однако для этого *требуется* общий протокол, например IPX/SPX для компьютера NetWare с установленной версией до 5.*x*.

Компонент GSNW предоставляет клиентам Windows доступ к ресурсам NetWare без установки какого-либо дополнительного программного обеспечения на клиентском компьютере. Он работает как шлюз (транслятор протоколов) между протоколом SMB, используемым в сетях Windows, и NCP, используемым в сетях NetWare.

После установки необходимого программного обеспечения пользователь компьютера Windows может запускать утилиты NetWare из командной строки.

Соединения между разными платформами

Устанавливать соединение между разными платформами, например компьютерами Macintosh и сетями Windows, можно с помощью шлюзов. Для интеграции компьютеров Macintosh и Windows нужен общий протокол (обычно для этого используется AppleTalk) и служебные программы разделения файлов и принтеров. При этом для коммуникации в системе Macintosh можно не устанавливать дополнительное программное обеспечение, однако оно необходимо для аутентификации клиентов Macintosh в целях повышения безопасности.

Клиенты Macintosh могут также получать удаленный доступ к серверу Windows с помощью AppleTalk и протокола PPP (Point-to-Point Protocol).

Архитектура SNA

В 1970-х годах IBM разработала для соединения несовместимых систем архитектуру SNA (System Network Architecture). Архитектура разрабатывалась для того, чтобы различные системы IBM (такие, как персональные компьютеры IBM и ее же мэйнфреймы) могли совместно использовать данные.

Архитектура SNA состоит из нескольких компонентов.

- **Узел**. Набор компьютеров в сети SNA.
- **NAU (Network Addressable Unit)**. Точка отправки или приема данных. Объект NAU может быть логическим устройством, физическим устройством или точкой SSCP (System Service Control Point).
- **LU (Logical Unit)**. Порт, с помощью которого сетевые пользователи получают доступ к сети SNA.
- **PU (Physical Unit)**. Устройство, управляющее ресурсами узла.
- **SSCP (System Services Control Point)**. Точка в сети, используемая для управления программами, обслуживающими пользователей.

На рис. 13.4 показана работа системы SNA в качестве шлюза между сетью персональных компьютеров и мэйнфреймами.

Первоначально сети SNA работали на основе центрального мэйнфрейма, который управлял выделенными мини-компьютерами с помощью программного обеспечения NCP (Network Control Protocol). В свою очередь, мини-компьютеры управляли группой терминалов, рабочих станций и телефонных линий.

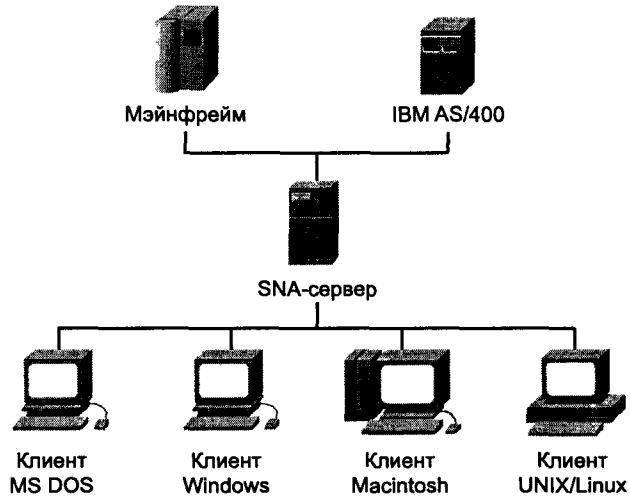


Рис. 13.4. SNA-сервер работает как шлюз между сетью персональных компьютеров и мэйнфреймами

Соединения SNA

Современная реализация SNA называется APPN (Advanced Peer-to-Peer Networking). В ней поддерживается два типа узлов.

- **Сетевые узлы**. К ним относятся маршрутизаторы, системы управления, а также клиентские и серверные программы.
- **Концевые узлы**. К ним относятся только клиентские и серверные программы.

В архитектуре SNA для передачи данных между клиентом и сервером должен быть установлен сеанс связи. Для сравнения: в протоколе IP фиксированный сеанс не обязателен.

Набор протоколов SNA более сложен, чем TCP/IP. Система SNA входит составной частью в систему AS/400, однако она реализована также компанией IBM в виде компонента Communication Manager для OS/2 и компанией Microsoft как SNA Server for Windows NT.

Замечание

В момент написания этой книги система Linux-SNA находилась в стадии разработки. Текущую информацию о бета-тестировании и выпуске системы можно найти по адресу: `www.linux-sna.org`.

Microsoft SNA Server

Программа SNA Server компании Microsoft разработана как шлюз для связи сетей клиент/сервер с системами AS/400 и мэйнфреймами, в которых используется архитектура SNA. Программа выполняется на компьютере с установленными Windows NT/2000 Server. Она может быть сконфигурирована как сервер удаленного доступа, предоставляющий коммутируемое соединение, или соединение VPN (Virtual Private Network) с хостом SNA. Последняя версия SNA Server переименована компанией Microsoft в Host Integration Server.

Samba

Пакет программ Samba описывался в этой и в предыдущих главах книги. С его помощью компьютеры Windows и UNIX могут сообщаться друг с другом. Рассмотрим работу пакета Samba подробнее.

Пакет создан путем переработки процедур протокола SMB (Server Message Block) компании Microsoft, который представляет собой так называемый протокол ядра (или протокол разделения файлов), используемый в операционных системах Microsoft для разделения сетевых ресурсов. При разработке ставилась задача сделать компьютер UNIX "видимым" для сервера Windows. Последние версии Samba решают не только эту, но и многие другие задачи.

Пакет Samba позволяет операционным системам Microsoft и UNIX сообщаться друг с другом с помощью файловой системы CIFS (Common Internet File System), основанной на протоколе разделения файлов SMB. Протокол CIFS предоставляет пользователю следующие виды услуг:

- аутентификация и авторизация (определение прав доступа);
- разрешение имен;
- службы разделения файлов и принтеров;
- службы просмотра сети.

В системе Samba разделяемые ресурсы могут быть защищены паролями, а разрешение имен NetBIOS может выполняться с помощью как широковещательных сообщений, так и какой-либо службы именования NetBIOS, например WINS (Windows Internet Name Service), если она, конечно, присутствует в данной сети. Служба просмотра предоставляет пользователю список разделяемых сетевых ресурсов в диалоговом окне Network Neighborhood (Сетевое окружение) компьютеров Windows 9*x* или Windows NT (рис. 13.5).

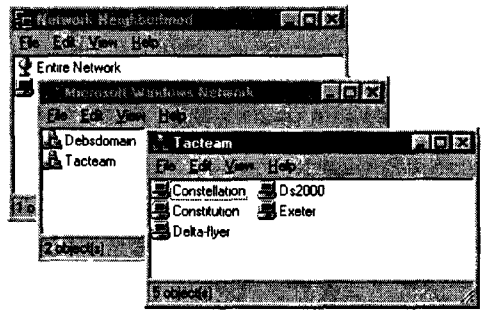


Рис. 13.5. В диалоговом окне Network Neighborhood (или My Network Places в Windows 2000) отображается список разделяемых сетевых ресурсов

Как работает пакет Samba

Пакет Samba состоит из нескольких программ. Только две из них предоставляют перечисленные выше базовые услуги.

- Демон SMB (называется SMBd).
- Демон NMB (называется NMBd).

Если вы знакомы с UNIX, то вы узнаете букву "d" в названии программ, обозначающую *daemon*, т.е. службу. Программа SMBd обеспечивает разделение файлов и принтеров Samba, аутентификацию и авторизацию, а NMBd — разрешение имен и просмотр служб.

Замечание

В Linux для получения доступа к удаленным разделяемым ресурсам SMB, например расположенным на компьютерах Windows, можно использовать файловую систему SMBFS (SMB File System). Фактически SMBFS не входит в Samba, однако она распространяется вместе с Samba. Она работает только в операционных системах Linux. Сама же Samba может быть перенесена на NetWare, VMS и другие операционные системы.

Резюме

В этой главе рассмотрены различные типы гибридных, или интегрированных сетей, объединяющих компоненты разных поставщиков. К ним относятся сети на основе разных протоколов, операционных систем и платформ оборудования.

Рассмотрены некоторые трудности, с которыми сталкивается сетевой администратор, объединяющий компоненты разных поставщиков для создания среды, в которой пользователи персональных компьютеров смогли бы получать доступ к данным на мэйнфреймах или пользователи Apple Macintosh смогли бы сообщаться с серверами UNIX.

Приведены причины создания гибридных сетей и технические решения (такие, как редиректоры и программные шлюзы), облегчающие интеграцию компонентов разных поставщиков.

Описаны клиентские и шлюзовые программы для NetWare, включенные в операционные системы Windows, программы Microsoft Services for Macintosh и программы, позволяющие клиентам Macintosh получать доступ к ресурсам Linux.

Вы узнали об архитектуре SNA и программе SNA Server компании Microsoft, позволяющей устанавливать соединения персональных компьютеров с мэйнфреймами IBM. Глава заканчивается описанием процесса коммуникации между компьютерами Windows и UNIX с помощью пакета Samba, представляющего собой серверное и клиентское программное обеспечения SMB для UNIX.

Независимо от используемых протоколов, операционных систем и платформ оборудования, в каждой сети существуют общие задачи администрирования, которым следует уделять постоянное внимание. В части III, "Специальные вопросы", рассматриваются наиболее важные из этих задач, включая весьма актуальные вопросы обеспечения безопасности сети и восстановления сети после аварии.

Рекомендуемые источники

Полезное руководство по интеграции компонентов NetWare и Windows NT можно найти по адресу: `www.microsoft.com/TechNet/network/int-netw.asp`.

Информацию о клиентском программном обеспечении NFS для Windows компании Intergraph можно получить по адресу: `www.intergraph.com/nfs/da-br.asp`.

Хороший конспект по работе пакета SNA есть по адресу: `www.protocols.com/pbook/sna.htm`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Как по-другому называется протокол, используемый для разделения сетевых файлов и ресурсов?
   - **а.** Протокол сетевого/транспортного уровня.
   - **б.** Протокол канального уровня.
   - **в.** Протокол ядра.
   - **г.** Протокол уровня 2.
2. Какие из приведенных утверждений о протоколе IPX/SPX справедливы?
   - **а.** Протокол IPX/SPX может использоваться только в сетях NetWare.
   - **б.** Протокол IPX/SPX является маршрутизируемым.
   - **в.** Протокол IPX/SPX не поддерживается в NetWare 5.*x*.
   - **г.** Протокол IPX/SPX работает медленнее и более сложен в конфигурировании, чем TCP/IP.
3. С помощью чего несколько протоколов связываются с одним сетевым адаптером или один протокол связывается с несколькими сетевыми адаптерами? (Выбрать все, что подходит.)
   - **а.** NDIS.
   - **б.** Winsock.
   - **в.** TDI.
   - **г.** ODI.
4. Что из приведенного используется для разделения файлов в сетях Microsoft?
   - **а.** NCP.
   - **б.** SMB.
   - **в.** NFS.
   - **г.** DLC.
5. Какие из приведенных утверждений о GSNW (Gateway Service for NetWare) справедливы?
   - **а.** Служба GSNW устанавливается на сервере NetWare для того, чтобы предоставить клиентам Windows доступ к ресурсам этого сервера.
   - **б.** Служба GSNW входит в состав операционных систем Windows NT Server и Windows 2000 Server.
   - **в.** Служба GSNW позволяет клиентам сервера Windows подключаться к серверу NetWare без установки у клиента дополнительного программного обеспечения и без дополнительного конфигурирования сервера NetWare.
   - **г.** Служба GSNW устанавливается на сервере Windows для того, чтобы клиенты этого сервера могли получать доступ к ресурсам сервера NetWare.

6. Что из приведенного является бесплатно распространяемым программным продуктом независимой организации, позволяющим пользователям систем Windows и UNIX обмениваться данными посредством сети?
   а. CDFS.
   б. Samba.
   в. Client Services for UNIX (Клиентские служебные программы для UNIX).
   г. SNA.
7. Как называются программы, транслирующие данные между разными протоколами и позволяющие сообщаться компьютерам, расположенным в сетях разных типов?
   а. Программное обеспечение моста.
   б. Программное обеспечение сервера.
   в. Программное обеспечение шлюза.
   г. Программное обеспечение маршрутизатора.
8. Как называется программный компонент, перехватывающий запросы к ресурсам?
   а. Платформа.
   б. Клиент.
   в. Директор.
   г. Редиректор.
9. Какую услугу предоставляет CIFS (Common Internet File System)?
   а. Разрешение имен.
   б. Коммутируемый доступ.
   в. Разделение файлов и принтеров.
   г. Обеспечение безопасности на уровне файлов.
10. Какой из приведенных компонентов Samba выполняет аутентификацию и авторизацию пользователей?
    а. SMBd.
    б. MBXd.
    в. NMBd.
    г. smbfs.

Часть III

Специальные вопросы

В этой части...

14. Защита сети
15. Удаленный доступ
16. Виртуальные частные сети
17. Сети с тонкими клиентами
18. Инструменты мониторинга, управления и устранения неполадок

Глава 14

Защита сети

В части I, "Основные концепции компьютерных сетей", были рассмотрены технические концепции разделения данных в компьютерных сетях; в части II, "Сетевое оборудование и программное обеспечение", — взаимодействие сетевых компонентов (оборудования, серверных и клиентских операционных систем и сетевых протоколов), с помощью которых пользователи получают доступ к разделяемым данным.

В этой главе обсуждается весьма важный аспект разделения сетевых компьютерных ресурсов — поддержание целостности разделяемых данных. Проблемы защиты данных от потерь и неправильного (злонамеренного) использования делятся на две категории:

- безопасность данных;
- защита от аварий и восстановление данных.

Чем больше деловой мир становится зависимым от компьютерных сетей и циркулирующей в них информации, тем более он уязвим для различных неполадок. Знаменитый закон Мэрфи гласит: неприятное случится рано или поздно. Это может быть умышленное или случайное разрушение безопасности сети в целях промышленного шпионажа либо какая-нибудь авария (крах диска, наводнение, пожар), приводящая к потере хранящихся на сервере данных.

В этой главе рассматривается, как защитить данные и уменьшить риск потери данных, не отказываясь от преимуществ объединения компьютеров в сеть и подключения сети к внешнему миру. Вы узнаете, что во многих случаях объединение в сеть даже облегчает защиту и восстановление данных по сравнению с изолированными системами.

Безопасность сети

В настоящее время безопасность сетей — весьма актуальная тема информационных технологий. Средства массовой информации постоянно рассказывают о случаях вторжения в правительственные или корпоративные сети, о массовом распространении компьютерных вирусов и об изощренных кознях компьютерных хакеров. Опасностью несанкционированного доступа к своим данным в разной степени озабочены практически все "подключенные" — от администраторов огромных коммерческих сетей до пользователей домашних компьютеров с коммутируемым подключением к Internet.

Применительно к сетевым технологиям безопасность никогда не бывает абсолютно гарантированной. Абсолютно безопасной может быть только система, к которой *никто* не имеет доступа. Однако подобная система также и абсолютно бесполезна. Обеспечение безопасности компьютера предполагает комплекс мер, направленных на защиту компьютера и хранящейся в нем информации. Обратите внимание: о гарантированной защите ничего не говорится.

Вопросы безопасности могут стать причиной обострения отношений между администратором и пользователями сети. Обычно пользователи предпочитают иметь больше прав доступа, в то время как сетевые администраторы больше склонны к ограничению доступа в целях повышения безопасности.

Рассмотрим, как оценить требования к безопасности в конкретной сети, как предусмотреть существующие и потенциальные угрозы безопасности данных и как практически реализовать оптимальные меры безопасности. Также рассмотрим сетевые компоненты, предназначенные для обеспечения безопасности, и самые современные методы идентификации и аутентификации.

Оценка требований к безопасности

Какой уровень безопасности компьютерной сети является достаточным? Ответ на этот вопрос зависит от характера деятельности организации. Первым этапом разработки жизнеспособного плана защиты сетевых данных должна быть оценка требований к безопасности этих данных. При этом необходимо рассмотреть следующие факторы:

- характер коммерческой деятельности компании;
- характер хранящихся в сети данных;
- принятая в организации стратегия управления.

Характер деятельности

В некоторых областях, например в юриспруденции или медицине, все данные по своей природе являются строго конфиденциальными. Конфиденциальность медицинской карточки пациента или переговоров адвоката со своим клиентом защищается законом. Если в сети хранится документация, доступ к которой нежелательных лиц может привести к неприятным последствиям, то обязательно должен поддерживаться высокий уровень безопасности данных. В противном случае организация подвергается риску финансовых потерь или использования данных конкурентами во вред этой организации.

Перечислим другие типы организаций, данные которых могут быть конфиденциальными.

- Правоохранительные органы, суды или другие государственные учреждения.
- Образовательные организации, хранящие в сети информацию об успеваемости студентов.
- Медицинские учреждения и психиатрические клиники.
- Компании, имеющие контракты с оборонными ведомствами или выполняющие другие работы, связанные с обеспечением национальной безопасности.
- Любые организации, собирающие конфиденциальную информацию и гарантирующие ее неразглашение.

- Любые организации, производящие товары либо предоставляющие услуги в коммерческих или исследовательских областях, где уровень конкуренции достаточно высок.
- Любые организации, сети которых подключены к Internet.

Характер данных

Некоторые виды данных рассматриваются как конфиденциальные и должны быть защищены, независимо от характера деятельности организации. К ним относятся следующие виды данных.

- Платежные ведомости на зарплату и другая информация о наемных работниках.
- Бухгалтерская и налоговая информация.
- Промышленные секреты, такие, как тексты программ, планы и диаграммы организаций, рецепты, технология изготовления, коммерческие планы и т.д.

Если такая информация хранится в сети, то для ее защиты следует планировать высокий уровень безопасности.

Стратегия управления организацией

Если конфиденциальность хранящихся в сети данных не является предметом законодательной защиты, то требования к уровню сетевой безопасности могут зависеть от личных взглядов владельца бизнеса или управляющего персонала на то, какой должна быть сеть

В некоторых организациях каждый служащий считается членом одной большой и счастливой семьи. Доступность и легкость использования информации ценятся выше, чем конфиденциальность и безопасность. В других организациях исповедуется принцип "необходимой информации", т.е. каждому служащему предоставляется только та информации, которая ему необходима для выполнения служебных обязанностей. Ни одну из этих стратегий нельзя назвать верной (неверной). Сетевой администратор должен знать принятый в организации стиль управления и реализовать его в подведомственной ему сети.

Замечание

Как показано в следующем разделе, в распределенных атаках DoS используются промежуточные компьютеры, на которые тайно устанавливаются программы, предназначенные для атаки на выбранную цель. Таким образом, компьютеры компании могут быть вовлечены в чужие игры, а сама компания подвергается риску судебных преследований. Поэтому система безопасности необходима для любой сети, подключенной к Internet, независимо от конфиденциальности хранящихся в ней данных.

Оценка угроз безопасности

Итак, на основе характера деятельности организации, характера сетевых данных и выбранной стратегии безопасности принимается решение о реализации необходимых мер безопасности. Однако нужно оценить также источники, из которых может исходить угроза безопасности данных.

Организация может легко недооценить, переоценить или даже полностью упустить из виду возможные источники неприятностей. Всегда легче увидеть то, что есть, чем

то, что только может быть. Существует много видов угроз безопасности сети, однако все они могут быть отнесены к одной из двух обширных категорий:

- внешние угрозы;
- внутренние угрозы.

Рассмотрим эти типы угроз подробнее.

Внешние угрозы

Было время, когда для локальных сетей большинства компаний внешние угрозы не представляли серьезной опасности. Сети были самодостаточными. Для вторжения извне нужно было каким-либо образом обратиться к модему изнутри сети или физически подключиться к сетевому кабелю. Сейчас большинство локальных сетей подключены к Internet, и это радикально изменяет ситуацию. Если к сети есть доступ из внешнего мира, значит, вторжения оттуда можно ожидать в любой момент.

Существует множество мотивов внешнего вторжения. Наиболее распространенные мотивы — месть (раздосадованных клиентов, обиженных бывших служащих, конкурентов), самовыражение (одни занимаются этим просто для развлечения, другие — чтобы показать свою квалификацию) и вознаграждение. В последнем случае злоумышленник вторгается в сеть из соображений личной выгоды: кто-то ему за это платит или он сам рассчитывает поживиться на этом, как, например, хакер, пытающийся перевести деньги на свой личный банковский счет или удалить записи о своем долге.

Нарушение внешней безопасности может проявляться в разных формах.

- Несанкционированное использование паролей и ключей.
- Атаки DoS (Denial of Service).
- Подмена IP-адреса.
- Компьютерные вирусы и черви.
- Программы вида "троянский конь".

Несанкционированное использование паролей и ключей

Пароль — это последовательность букв, цифр и других символов, с помощью которой система проверяет, действительно ли это тот самый пользователь, который имеет данную учетную запись и право доступа к ресурсам. *Ключ* — это число, или код, используемый системой для проверки целостности канала коммуникации.

Пароли и ключи — это меры безопасности, разработанные для предотвращения несанкционированного доступа пользователей к ресурсам сети. Естественно, они действенны, только если держать их в секрете. Если кто-либо узнает имя учетной записи и пароль пользователя и сумеет каким-нибудь образом физически подключиться к компьютеру или к сети, то он получит доступ к любым ресурсам, к которым имеет право доступа данный пользователь. Получение пароля часто становится первым шагом проникновения в систему.

В зависимости от контекста, термин *хакер* может иметь разное значение. В былые времена так называли квалифицированного программиста, однако современные средства массовой информации придали этому "герою" негативный оттенок. Сейчас под "хакером" подразумевается некто, проникающий в компьютерную систему, причем чаще всего для того, чтобы украсть или разрушить хранящиеся в ней данные.

Хакеров часто представляют как злых гениев, использующих для проникновения в сеть изощренные, эзотерические методы. Человек, научившийся подделывать документы, почему-то не считается талантливым художником. В то же время хакерам журналисты придали (видимо, непроизвольно) некий ореол романтичности. Однако в действительности все происходит гораздо прозаичнее. Зачастую вторжение вообще не основано на мастерском владении техникой программирования. Порой хакеры проникают в сеть так же, как и санкционированные пользователи: путем ввода правильного имени учетной записи и пароля. Тех, кто проникает в сеть таким образом, иногда называют *крэкерами* (от англ. *crack*, взлом), потому что они получают пароль и входят в сеть аналогично тому, как взломщик открывает сейф.

Замечание

Получение доступа с помощью чужой учетной записи — это одна из форм *имперсонификации*. Этот тип нарушения безопасности включает также подмену IP и другие методы, основанные на представлении себя как кого-то другого (иного человека или другое устройство).

Существует много способов получения хакерами нужных паролей. Довольно часто они используют для этого не технические средства, а наблюдательность и искусство убеждения — ведь именно это нужно, чтобы выманить у пользователя имя учетной записи и пароль.

Многие пользователи создают пароли, которые можно попросту угадать, например год рождения или имя супруги (или супруга). Другие создают (или получают от администратора) менее наглядные пароли. Однако, поскольку такие пароли труднее запомнить, пользователи записывают их на клочках бумаги, иногда оставляя такие записи в ящике незапертого стола. Бывает даже, что пользователи записывают их карандашом на корпусе компьютера.

Хакер может также получить пароль, попросту спросив его у пользователя, предварительно представившись как технический работник или служащий административного отдела, находящийся по отношению к пользователю на более высокой ступени иерархической лестницы. Уж ему-то пользователь не решится отказать. Такие способы иногда называются *атакой на основе социальной инженерии*.

Еще одним способом получения пароля является метод грубой силы или автоматический перебор паролей — испытание всех возможных комбинаций символов, пока не встретится сработавший пароль. Для этого хакеры пишут специальные программы, которые называются взломщиками паролей. Такая программа автоматически перебирает списки различных слов и комбинации букв и цифр, так что хакеру не нужно сидеть возле компьютера и вводить вручную все возможные пароли.

Если и этот метод получения пароля потерпит неудачу, хакер может попытаться перехватить пакет данных, содержащий искомый пароль, с помощью специальной программы сетевого анализатора пакетов. Именно поэтому все руководители настоятельно рекомендуют передавать пароли по сети только в зашифрованном виде, ни в коем случае как открытый текст. Программы анализаторов пакетов подробно рассматриваются в главе 18, "Инструменты мониторинга, управления и устранения неполадок".

Безопасность паролей — важнейшая часть всей стратегии сетевой безопасности. Этот вопрос более подробно рассматривается далее в главе.

Атаки DoS

Атаки DoS (Denial of Service — отказ в обслуживании) могут выполняться несколькими разными способами, но все имеют целью нарушить нормальную работу компьютера, подвергнутого атаке. В феврале 2000 года по этой причине были временно закрыты несколько крупных Web-узлов, включая Amazon.com и Yahoo.

В атаках DoS, направленных на компьютер, используются малозаметные недочеты в операционной системе компьютера или в приложениях. Другие атаки направлены непосредственно на сеть. Поставщики программного обеспечения часто разрабатывают и предоставляют своим пользователям так называемые "заплатки" — исправления, добавляемые в операционную систему или приложение для того, чтобы закрыть обнаружившуюся прореху в системе защиты, через которую становится возможной атака.

Атаки DoS не влекут за собой крах компьютера, они предназначены лишь для разрыва сетевого соединения или приведения его в неработоспособное состояние. Эти атаки наводняют сеть бесполезными пакетами или имитируют сетевые проблемы, вызывающие разрыв соединений.

Известны следующие наиболее распространенные формы атак DoS:

- на основе протокола ICMP;
- атаки Smurf;
- Ping of Death;
- атаки SYN.

Кратко рассмотрим каждую из них.

Протокол ICMP. Это умышленное переполнение системы пакетами ICMP, в нормальном режиме предназначенными для проверки правильности сообщений и обнаружения ошибок в передаваемой по Internet информации. Команда `ping` обычно используется для передачи пакетов ICMP с целью определения, подключен ли к сети данный компьютер (идентифицируемый IP-адресом или именем хоста, преобразуемым в IP-адрес).

Команда `ping` посылает сообщение ICMP Echo Request и ожидает от проверяемого компьютера сообщение ICMP Echo Reply. Если пакеты посылать по IP-адресу непрерывно, то сервер не может справиться с их потоком, его производительность уменьшается, и в конце концов он отключается из-за превышения времени ожидания ответа.

Атаки Smurf. Представляет собой поток пакетов ICMP, затрагивающий все службы провайдера или весь сегмент сети. Сообщения ICMP посылаются по широковещательному адресу и генерируют ответы всех компьютеров подсети. Когда провайдер атакован указанным методом, снижается производительность всех соединений, в результате чего все пользователи отключаются.

Атаки Smurf — это разновидность атак DoS. Когда атакующий получает доступ в сеть, он посылает в нее широковещательное сообщение, в котором на место адреса источника подставлен один из адресов атакуемой сети. В результате этого все устройства атакованной сети посылают сообщения ICMP по адресу подставленного источника. Таким образом, сотни хостов посылают в сеть тысячи битов ответов отклика ICMP. Генерируемый таким процессом поток сообщений легко переполняет низкоскоростные глобальные каналы между провайдером и сетью. При этом затрагивается не только атакуемая сеть, но и промежуточные сети, по которым проходит поток сгенерированных сообщений.

Ping Of Death. В этой более изощренной разновидности атаки DoS используется ограничение на длину MTU (Maximum Transmission Unit). Конкретная величина MTU зависит от типа среды и сетевой архитектуры. Если длина передаваемого пакета превышает MTU, то он должен быть разбит на несколько меньших пакетов, которые затем будут собраны в принимающем компьютере.

Длина пакета IP, в котором инкапсулирован ответ отклика ICMP, ограничена 65 535 октетами (*октет* — это 8 бит данных). Атакующий, естественно, знает это. Он посылает пакет, в котором длина поля данных ответа отклика ICMP превышает допустимое количество октетов. Пытаясь собрать такой пакет, принимающий компьютер терпит крах.

Атаки SYN. Для разрыва соединения атакующий может использовать последовательность согласования TCP. Процесс установки сеанса TCP показан на рис. 14.1.

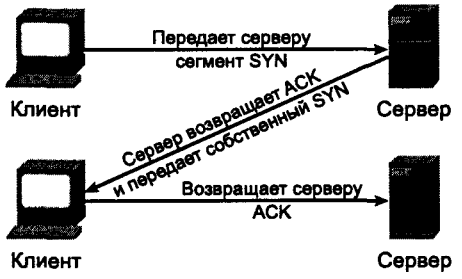


Рис. 14.1. Для установки сеанса связи в TCP используется трехэтапный процесс

Процесс установки соединения состоит из трех этапов.

1. Клиент передает запрос согласования SYN, представляющий собой последовательность цифр, т.е. число, сгенерированное клиентом.
2. Сервер передает подтверждение ACK, представляющее собой принятое сервером число клиента плюс единица. Одновременно с этим сервер передает клиенту свое число SYN, сгенерированное независимо от клиента.
3. Клиент добавляет единицу к числу SYN сервера и передает его серверу как подтверждение ACK. После того как оба компьютера получают подтверждения, устанавливается соединение.

Атакующий запускает достаточно большое количество запросов сеанса (обычно используя для этого поддельный IP-адрес). Принимающий компьютер ставит эти запросы в очередь. Переполняя таким образом очередь и поддерживая ее постоянно заполненной, атакующий может полностью блокировать обработку запросов и установку сеансов. В результате законные пользователи не могут установить соединение с сервером.

Подмена IP-адреса

Подмена IP-адреса выполняется путем изменения заголовка передаваемого пакета, после чего пакет выглядит так, будто его передал компьютер, имеющий подставленный адрес. Сама по себе подмена адреса не является формой атаки, это лишь метод, используемый для получения доступа к сетевым компьютерам с целью кражи или разрушения данных.

Компьютерные вирусы и черви

Компьютерный вирус — это программа (либо фрагмент программы), способная без ведома или согласия пользователя размножаться и распространяться на другие программы и компьютеры путем копирования своего кода в хранящиеся в системе файлы. Подобно биологическим вирусам, компьютерные вирусы могут быть "смертельны" или служить всего лишь досадной помехой. Например, безвредный вирус может выводить на экран какое-либо сообщение, в то время как более зловредные вирусы разрушают данные или удаляют файлы операционной системы, после чего пользователь не может загрузить свой компьютер.

В недалеком прошлом вирусы пользовались повышенным вниманием средств массовой информации, охотно рассказывавших о том, как вирусы Melissa, CIH (Chernobyl), Michelangelo и Iloveyou заразили тысячи компьютерных систем по всему миру.

Червь — это одна из разновидностей зловредного вируса, размножающегося и повреждающего файлы, хранящиеся в компьютере. Черви часто распространяются во вложениях к электронным сообщениям или в HTML-страницах, содержащих сценарии.

Троянский конь

Троянский конь — это программа, внедряемая в компьютер под видом другой программы для получения информации. Например, троянский конь может эмулировать диалоговое окно регистрации в системе. Когда пользователь вводит в нем имя своей учетной записи и пароль, они запоминаются или передаются владельцу троянского коня. Затем полученные таким образом регистрационные данные могут быть использованы для доступа в систему.

Внутренние угрозы

Довольно часто, разрабатывая стратегию обеспечения сетевой безопасности, администратор сосредоточивает внимание почти исключительно на Internet и внешних угрозах. Это серьезная ошибка. Компании, занимающиеся розничной продажей, иногда обнаруживают, что их собственные служащие повинны в кражах чаще, чем "внешние" воришки. То же самое может происходить и в корпоративной сети. Поэтому сетевой администратор должен уделять внутренним угрозам самое пристальное внимание. В практике корпоративных сетей известно множество случаев кражи данных, их злонамеренного использования или разрушения не без помощи служащих самой компании.

Перечислим некоторые мотивы, являющиеся причинами внутренних угроз безопасности сети.

- Промышленный шпионаж.
- Внутренние интриги.
- Недовольные служащие (или бывшие служащие).
- Случайные нарушения.

Рассмотрим каждый из этих мотивов и способы защиты от них.

Промышленный шпионаж

Это наиболее изощренный тип внутренней угрозы безопасности. Кража промышленных секретов — весьма прибыльный бизнес. В результате кражи компания может мгновенно достичь крупного успеха или потерпеть крах.

Конкуренты могут тайно обратиться к любому из служащих вашей компании с очень заманчивым предложением и получить таким образом доступ к секретным данным. Возможен и такой вариант: служащие других компаний устраиваются к вам на работу, входят в доверие, после чего собирают секретные данные и передают их конкуренту, получая при этом зарплату в обеих компаниях одновременно.

И наконец, существуют люди, занимающиеся промышленным шпионажем профессионально, на основе контрактов с различными компаниями. В областях с жесткой конкуренцией они иногда воруют секретные данные по собственной инициативе, чтобы затем продать их тому, кто больше заплатит. "Похитители данных" могут даже шантажировать обворованную компанию, обещая не передавать украденные данные конкурентам, если компания сама заплатит за них приличную сумму.

Довольно часто промышленные шпионы — интеллигентные, образованные, далеко не бедные люди с хорошей технической подготовкой. Обычно им удается ускользать от обнаружения так долго, пока они не выведают все, что нужно. Если коммерческая компания занята в той области, где промышленный шпионаж широко распространен, то сеть компании подвержена серьезным угрозам. Таких областей, к сожалению, довольно много. К ним относятся промышленные технологии, нефтепереработка, энергетика, фармацевтика, конструирование технических устройств и любые другие области, в которых успех зависит от того, кто первым представит рынку новый, более совершенный товар или услугу.

Меры безопасности, призванные противодействовать промышленным шпионам, должны разрабатываться как можно тщательнее. Компания не должна полагаться в этом на собственные силы. Очень полезны консультации привлеченных специалистов, занимающихся этим профессионально.

Внутренние интриги

Еще одна внутренняя угроза безопасности сети — не в меру амбициозные служащие, готовые на все, чтобы подавить своих коллег и добиться повышения. Такой человек может попытаться получить доступ к сети и нарушить нормальную работу тех, кого он считает своими личными конкурентами. Другой попытается повредить репутации своих коллег путем просмотра их файлов или электронной корреспонденции в поисках компрометирующих сведений или личностной информации. Особенно неразборчивые в средствах могут даже внедрить фальшивые компрометирующие данные в компьютер своего недруга или посылать от его имени электронные письма, подрывающие его репутацию.

Естественно, угроза сетевой безопасности, исходящая от подобных личностей, значительно менее серьезна, чем со стороны промышленных шпионов. Однако она все же может породить множество проблем внутри организации. Большинство нарушителей такого типа не обладают хорошей технической подготовкой, поэтому правильно спланированная стратегия сетевой безопасности (криптографически сильные пароли, периодический аудит сетевых событий и т.д.) способна легко предотвратить или быстро выявить подобную деятельность.

Недовольные служащие

Особенно разрушительные угрозы безопасности сети исходят от служащих или бывших служащих, озлобленных на компанию и стремящихся отомстить ей. Такие люди могут разрушить ценные данные или прервать жизненно важное сетевое соединение просто из злорадства либо во имя ложно понимаемой ими "справедливости".

Компания особенно подвергается этой угрозе, когда увольняет кого-либо из технически осведомленных служащих. Нередки случаи, когда разозленный служащий пе-

ред уходом удаляет данные с жесткого диска, портит компьютерное оборудование или запускает в сеть компании вирус.

Стратегия сетевой безопасности должна учитывать угрозу этого типа. Здравый смысл подсказывает, что учетные записи увольняемых служащих должны быть немедленно удалены, а в некоторых случаях даже должен быть ограничен физический доступ увольняемого служащего к компьютерам компании. Последняя мера реализуется путем назначения сопровождающего, постоянно находящегося рядом с увольняемым служащим, пока он собирает свои вещи или зачем-либо входит в офис компании.

Случайные нарушения

Во многих случаях нарушения внутренней безопасности происходят неумышленно вследствие небрежности или недостаточной технической подготовки части служащих. Каждому сетевому администратору приходилось встречаться с пользователями, которые удаляют необходимые файлы операционной системы при попытке решить небольшую проблему или решают освободить побольше дискового пространства путем удаления файлов приложений.

Именно вследствие угрозы случайных нарушений безопасности для ответственных коммерческих задач настоятельно рекомендуются операционные системы с усиленными средствами безопасности. Системный администратор может предотвратить удаление или перемещение пользователями необходимых системных файлов путем реализации прав доступа на уровне файлов с помощью системных или групповых политик операционной системы Windows NT/2000.

Мятежные пользователи

Нарушение внутренней безопасности может произойти также вследствие деструктивных действий тех пользователей, которые считают, что навязанные им меры безопасности слишком строгие. Хотя такие нарушения и не относятся к категории случайных, тем не менее их целью не является нанесение ущерба компании, напротив — пользователем движет желание сделать нечто такое, что ему мешают сделать жесткие правила безопасности. Иногда бывает так, что правила безопасности не запрещают пользователю устанавливать на своем компьютере дополнительные приложения или драйверы устройств, однако пользователь недоволен политикой компании относительно доступа в Internet. В таком случае он может подключить к компьютеру внешний модем, подключить его к телефонной линии, установить драйверы и установить соединение со своим собственным провайдером. Другой пользователь установит на своем компьютере приложение удаленного контроля (например, PCAnywhere) и откроет этим свой компьютер — вместе со всей внутренней сетью — для любого внешнего пользователя, на компьютере которого установлено PCAnywhere.

Меры против мятежных пользователей зависят от политики компании и требований к уровню безопасности сети. В некоторых случаях адекватной мерой является более жесткий контроль за действиями пользователей. В других ситуациях следует оценить, действительно ли стратегия безопасности должна быть столь жесткой и не следует ли предоставить пользователям больше свободы и прав доступа.

Реализация мер безопасности

Защита сетевых данных нередко обеспечивается путем сочетания разных методов поддержания безопасности. В этом разделе описано, как учетные записи пользовате-

лей и групп вместе с их правами доступа могут быть задействованы в качестве первой линии обороны. Кроме того, рассматриваются методы шифрования секретных данных как в файлах на диске, так и в пакетах, передаваемых в сеть.

Электронная почта — одно из наиболее популярных сетевых приложений — довольно часто становится средством передачи конфиденциальной информации, поэтому мы сосредоточим внимание на доступных пользователям средствах обеспечения безопасности электронных писем. В этом разделе рассматриваются способы практической реализации мер безопасности, а в следующем — обсуждается, как эти меры фактически работают.

Уровни безопасности операционных систем

Существуют операционные системы, которым присуща большая степень безопасность, чем другим. В более старых операционных системах, например MS DOS, при доступе к ресурсам аутентификация учетных записей пользователей не поддерживается (хотя при доступе к сетевым ресурсам аутентификация в них все же выполняется). Любой желающий может сесть за компьютер под управлением MS DOS, загрузить операционную систему и выполнять приложения или получать доступ к файлам на жестком диске.

Более современные операционные системы, например Windows 95, позволяют создавать учетные записи пользователей компьютера. Однако пароль в них хранится в ненадежном текстовом файле. К нему можно получить доступ, загрузив компьютер в MS DOS с помощью дискеты. Если при загрузке в ответ на запрос имени пользователя и пароля щелкнуть на кнопке Cancel (Отмена), то операционная система все же загружается и в ней можно нормально работать, так как по умолчанию пароли не присвоены ни одному ресурсу.

В операционных системах с высоким уровнем безопасности, таких, как Windows NT, Windows 2000 или Linux, для загрузки системы и работы в ней нужно ввести правильное имя пользователя и пароль. Пароль в них хранится в зашифрованном виде и получить к нему доступ непросто.

Правительством США разработаны и поддерживаются спецификации, определяющие уровни компьютерной безопасности. Они более подробно описываются далее в главе.

Пользователи, группы и права доступа

В современных операционных системах несколько пользователей одного компьютера могут получать доступ к нему и к сетевым ресурсам с помощью отдельных учетных записей, которым присвоены разные пароли. После правильного ввода регистрационной информации пользователь может:

- получить доступ к операционной системе и сети;
- читать и изменять те разделяемые ресурсы, к которым его учетная запись имеет соответствующие права доступа;
- выполнять любые действия (завершать операционную систему и выключать компьютер, устанавливать программы и т.д.), право на выполнение которых присвоено его учетной записи;
- загружать систему персональной конфигурации, т.е. на рабочем столе появляются нужные пиктограммы, устанавливается заданный цвет фона и т.д.

Если хранящиеся в компьютере данные не представляют ценности для взломщиков и требования к безопасности данных невысокие, то в некоторых случаях можно вообще не создавать отдельные учетные записи пользователей. При этом все пользо-

ватели получают одинаковые права доступа к ресурсам. Однако при этом не только создается полностью открытая ненадежная среда, но и сами пользователи испытывают определенные неудобства, так как при загрузке операционная система не конфигурируется автоматически применительно к предпочтениям каждого пользователя.

Создание отдельных учетных записей для разных пользователей практикуется в подавляющем большинстве организаций. Если требования к безопасности невелики, то пароли при этом можно оставить пустыми.

Пароли

Стратегия обеспечения сетевой безопасности обязательно должна содержать меры, предотвращающие использование слабых паролей. Если пользователям разрешается выбирать пароли на свой вкус, то все же должны быть установлены правила, ограничивающие этот выбор соответственно нуждам сетевой безопасности.

Перечислим некоторые полезные правила создания паролей.

- Пароль ни в коем случае не должен быть словом или числом, которое можно угадать, зная пользователя (например, номером его паспорта или именем его собаки).
- Во многих программах взлома паролей методом автоматического перебора используются списки обычных слов, поэтому пароль не должен быть словом из словаря. Рекомендуется сочетать в пароле буквы и цифры, например *рыбка28*.
- В большинстве операционных систем пароли чувствительны к регистру, поэтому рекомендуется переводить часть букв пароля в верхний регистр, например *берЕЗА*.
- Пароль *должен* быть легко запоминаемым. Иначе пользователь будет забывать его и рано или поздно станет записывать на клочках бумаги.
- Чем длиннее пароль, тем труднее его взломать. Например, пароль "черноеморе" лучше, чем "море". Однако, чем длиннее пароль, тем труднее его запомнить. К счастью, при увеличении числа символов количество вариантов пароля (а значит, его криптографическая сила) возрастает в геометрической прогрессии. Обычно достаточно 7–8 символов. Пароль из 9–10 символов можно считать чрезвычайно сильным, дальнейшее удлинение не имеет никакого смысла.
- В системах с высокими требованиями к безопасности пользователи должны периодически менять свои пароли. Новый пароль не должен быть похож на старый. Например, нельзя менять пароль "автобус2" на "автобус5". Не следует также менять пароли слишком часто, потому что пользователям будет труднее их запомнить и придется записывать на клочках бумаги.
- Многие сетевые операционные системы позволяют администратору задавать такие критерии выбора паролей, как длина пароля, история паролей (т.е. система хранит список предыдущих паролей и следит, чтобы они не повторялись) и время жизни пароля (по истечении заданного промежутка времени система напоминает пользователю, что пора сменить пароль). Существуют также программы, позволяющие администратору устанавливать параметры паролей. Например, программа проверяет, есть ли такое слово в словаре и, если есть, предотвращает использование пароля.

Замечание

В некоторых операционных системах с высоким уровнем безопасности (таких, как Windows NT и Windows 2000) по умолчанию нельзя оставить пароль пустым. Чтобы позволить это, администратор должен изменить параметры установки паролей.

Стратегия управления доступом

Современные сетевые операционные системы позволяют администраторам контролировать доступ к ресурсам довольно подробно. Например, учетной записи `marysmith` можно разрешить просматривать содержимое файла `file1.doc`, но запретить вносить в него изменения. Одновременно этой же учетной записи можно предоставить право читать, изменять, удалять файл `file2.doc` и даже устанавливать права доступа к нему других пользователей, а к файлу `file3.doc` отменить все права доступа.

Каждому пользователю следует предоставлять только те права доступа, которые нужны ему для выполнения своих служебных обязанностей. В файловых системах с высоким уровнем безопасности права доступа можно устанавливать не только на разделение ресурсов по сети, но и на использование этих ресурсов на этом же локальном компьютере. Локальные и сетевые права доступа не обязательно должны совпадать. Например, Мэри можно предоставить право полного контроля над файлом `file4.doc`, когда она регистрируется на компьютере, в котором этот файл хранится, но ограничить ее право доступа к `file4.doc`, когда она получает к нему доступ с другого компьютера сети.

Администратор должен учитывать, какие права доступа предоставляются в данной операционной системе по умолчанию. Например, в серверах Windows NT/2000 разделяемый ресурс по умолчанию полностью доступен для любого пользователя сети. Чтобы ограничить права доступа к нему, нужно изменить их явно. В серверах NetWare действует противоположное правило: по умолчанию разделяемый ресурс недоступен ни для одного пользователя, пока параметры доступа к этому ресурсу не изменены явно.

Ни один из этих методов нельзя назвать правильным или неправильным, но если не знать, какие правила приняты в конкретной операционной системе, то секретные данные могут оказаться "рассекреченными", а данные, необходимые пользователям для работы, — "засекреченными".

В организациях с высокими требованиями к безопасности стратегия обеспечения безопасности должна определять, к каким ресурсам и какое право доступа должен иметь каждый пользователь. В общем случае право доступа должно быть предоставлено только тем пользователям и только к тем ресурсам, которые нужны для выполнения служебных обязанностей. Если пользователю для выполнения своих обязанностей нужен доступ к данному ресурсу, то ему должно быть предоставлено соответствующее право доступа, в противном случае оно должно быть отменено.

Группы безопасности

Концепция групп безопасности поддерживается многими сетевыми операционными системами. Их использование значительно облегчает задачу управления правами доступа в большой сети. Сетевой администратор создает группу, присваивает ей определенные права доступа к ресурсам, а затем включает в группу необходимые учетные записи пользователей. В результате все пользователи, включенные в группу, получают права доступа, присвоенные данной группе. Это значительно легче, чем присваивать права доступа каждому пользователю отдельно.

Пусть, например, каждому служащему отдела продаж нужен доступ к нескольким каталогам (назовем их `salestat`, `salesbudget` и `salesmemos`). Можно предоставить права доступа к этим каталогам отдельно каждому из 20 пользователей отдела продаж. Однако значительно легче будет создать группу безопасности (назовем ее `sales`), предоставить ей право доступа ко всем трем каталогам и включить в нее 20 учетных записей пользователей. Если создается новый каталог `salescalendars`, доступ к которому должны иметь все служащие отдела продаж, то нужно будет всего лишь присвоить право доступа к нему группе `sales`. В противном случае пришлось бы присваивать права доступа к новому каталогу отдельно 20 различным учетным записям.

Если нужно отменить право доступа пользователя к определенному ресурсу, то отмена права доступа к нему только в учетной записи пользователя может оказаться недостаточной. Следует убедиться, что пользователь не является членом какой-либо группы, имеющей право доступа к данному ресурсу. Кроме того, если операционная система (например, Windows NT/2000) позволяет отменять доступ конкретного пользователя к отдельному ресурсу, то необходимо делать это явно.

Шифрование файлов

Шифрование — это преобразование данных к такому виду, в котором их не смогут понять другие. Технические вопросы шифрования подробно рассматриваются далее в главе.

Шифрование файлов означает преобразование хранящихся на диске компьютера данных таким образом, чтобы их не смог прочитать никто, кроме обладателя ключа. Некоторые операционные системы (например, Windows 2000) содержат встроенные средства шифрования файлов. При работе с системами, не содержащими встроенных средств шифрования (например, Windows 9*x* или Windows NT), можно использовать программы шифрования других поставщиков.

Если хранящийся на диске документ зашифрован, то его может просматривать только пользователь, которому известен правильный ключ. Если к файлу попытается обратиться пользователь, не знающий ключа, то файл или не откроется, или будет выглядеть как бессмысленная последовательность символов. Особенно ценные данные должны быть защищены как с помощью прав доступа, так и шифрованием.

Протокол IP Security

Шифрование файлов защищает данные, хранящиеся на диске, однако в некоторых случаях оно не обеспечивает достаточную безопасность данных, передаваемых по сети. Для преодоления этого недостатка был разработан протокол IPSec (IPSecurity). В нем безопасность данных обеспечивается на уровне пакетов. Протокол IPSec работает на сетевом уровне модели OSI, поэтому приложения его не видят. Поддержка IPSec включена в маршрутизаторы компании Cisco Systems и операционную систему Windows 2000. Кроме того, IPSec включен в стек протоколов TCP/IP.

В протоколе IPSec используются два протокола.

- **AH (Authentication Header)**. Позволяет проверять идентичность отправителя.
- **ESP (Encapsulating Security Payloads)**. Обеспечивает конфиденциальность самих данных.

Эти два протокола могут использоваться вместе или отдельно.

Протокол IPSec может работать в двух режимах: транспортном и туннелирования (рис. 14.2). В транспортном режиме обеспечивается безопасность *от точки к точке*,

т.е. данные зашифрованы на всем пути от передающего компьютера к принимающему. В режиме туннелирования данные зашифрованы от точки выхода из одной сети до точки входа в другую сеть.

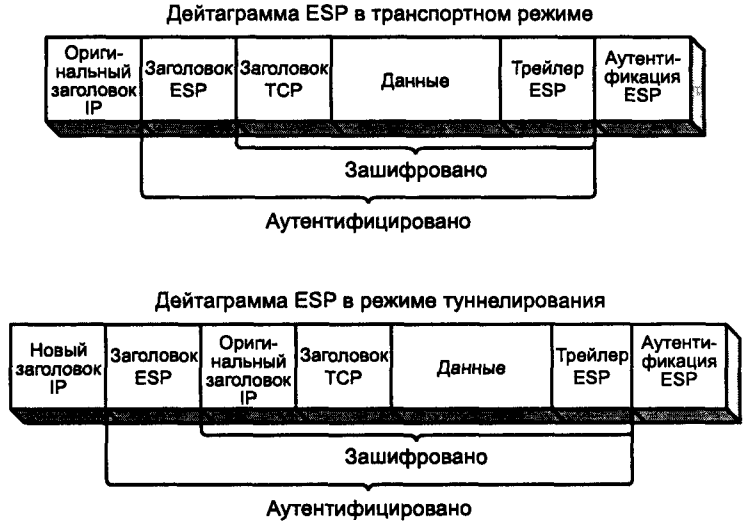


Рис. 14 2. В транспортном режиме и режиме туннелирования протокола IPSec используются разные форматы заголовков пакетов

SSL

Еще одно средство повышения безопасности сетевых соединений — протокол SSL (Secure Sockets Layer), в котором криптографическая система с открытым ключом комбинируется с блочным шифрованием данных. Недостатком SSL является то, что он работает на прикладном уровне, т.е. должен поддерживаться пользовательскими приложениями.

Протокол SSL был разработан компанией Netscape для защиты своих Web-броузеров. В нем используются *шифры с открытыми/закрытыми ключами*, которые описываются далее в главе.

Безопасность электронной почты

Многим пользователям присуще ложное чувство безопасности сетевой коммуникации, в том числе систем электронной почты. Они думают, что сообщения, которые они составили и передали посредством локальной сети, или Internet, будут прочитаны только теми, кому они адресованы. Пользователи электронной почты часто считают, что передаваемое ими электронное письмо аналогично письму обычной почты, отправляемому в закрытом конверте. Однако в действительности оно больше похоже на открытку, которую может прочитать каждый, кому она попадет в руки на пути между отправителем и получателем.

Как показано на рис. 14.3, электронное письмо довольно легко перехватить На своем пути от передающего к принимающему компьютеру оно часто проходит через десятки узлов (серверов) Даже если письмо передается в пределах локальной сети, его копии хранятся, как минимум, на трех компьютерах: передающем, принимающем и на внутреннем почтовом сервере. Письмо, передаваемое через Internet, может пройти через десятки серве-

ров. Если оно не зашифровано или не представлено в какой-либо другой нечитаемой форме (например, как нетекстовый файл), то его легко можно прочитать, скопировать или изменить в любой точке между отправителем и получателем.

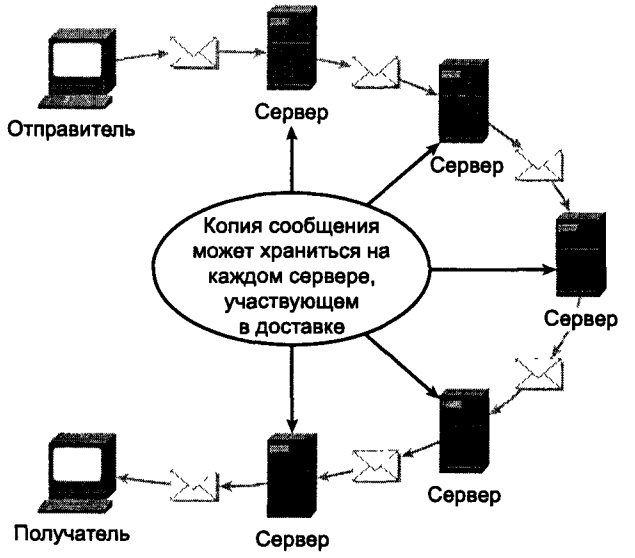


Рис. 14.3. Электронное письмо может быть легко перехвачено в любом пункте его путешествия по Internet

Замечание

Удаление электронного письма на пользовательском компьютере *не гарантирует*, что не осталось его копий на одном или нескольких серверах.

Для решения этой проблемы разработано много различных программ, использование которых преследует определенные цели.

- Сообщение не должно быть прочитано несанкционированным пользователем.
- Сообщение не должно быть изменено в промежуток времени между его отправкой передающим компьютером и получением на принимающем конце.
- Пользователь, идентифицируемый как отправитель сообщения, действительно им является.

Важная характеристика средств защиты электронной почты — простота их использования. Если для передачи или приема электронных писем пользователи должны выполнять сложные действия, занимающие много времени, то, скорее всего, они попросту отключат систему безопасности.

В настоящее время популярны следующие программы защиты электронной почты:

- PGP (Pretty Good Privacy);
- Kerberos;
- Baltimore Mail Secure;
- MailMarshal компании Softek.

В большинстве этих программ для обеспечения конфиденциальности данных и аутентификации сторон используются открытые/закрытые ключи шифрования (рассматриваются далее в главе) и цифровые подписи.

Принцип действия компонентов безопасности

Основой средств компьютерной безопасности служит *криптография* — наука о "секретном письме", или *шифре*. Шифрование представляет собой преобразование данных к такому виду, в котором они не могут быть прочитаны или использованы посторонними лицами. Обратно к исходному виду данные преобразуются в процессе *дешифрования*. Чтобы расшифровать данные, пользователю должен быть известен *ключ*, который был использован при шифровании. Процедура анализа и расшифровки зашифрованных данных называется *криптоанализом*.

Основные понятия криптографии

В компьютерах данные шифруются автоматически с помощью определенного *алгоритма шифрования*. Зашифрованные данные иногда называются *шифротекстом*. Алгоритмы шифрования и дешифования, а также ключ называются *шифром*. Чтобы лучше понять принципы шифрования, рассмотрим простой "секретный код", используемый детьми (а иногда и взрослыми). Присвоим каждой букве алфавита определенное число. Пусть, например, букву "a" представляет число "1", букву "b" число "2" и т.д.. Пользуясь таким шифром, мы можем передать сообщение

```
4-9-14-14-5-18 9-19 18-5-1-4-25
```

Непосвященный, естественно, не поймет, о чем в нем говорится, а мы можем расшифровать его, пользуясь тем же шифром:

```
dinner is ready (обед готов)
```

К сожалению, этот шифр очень легко взломать, его безопасность невелика. В компьютерах используются более сложные алгоритмы шифрования. Обычно в процессе шифрования и последующего дешифрования используется *ключ*, представляющий собой некоторую последовательность символов, сочетаемую с данными. Метод сочетания ключа с шифруемыми данными называется *алгоритмом шифрования*. Компьютеры обрабатывают двоичную информацию, поэтому алгоритм шифрования применяется к каждому биту данных или к группе битов (рис. 14.4).



Рис. 14.4. В компьютерных программах шифрования используются ключи и алгоритмы

Чем длиннее ключ шифра, тем труднее взломать зашифрованный текст. В криптографии шифры с ключами длиной 40 и 56 бит называются *стандартными*, а с ключами длиной 128 бит — *сильными*.

Законодательная поддержка технологий шифрования

Во многих странах законодательство ограничивает экспорт и импорт технологий шифрования. В законодательстве США программы шифрования классифицируются как "военное снаряжение" и экспорт сильных программ шифрования запрещен. Лишь недавно разрешен экспорт шифров с ключами 128 бит. Импорт шифров и их компонентов не ограничивается.

В других странах законодательное регулирование вопросов шифрования может быть самым разнообразным. Например, в законах Аргентины вообще нет никаких статей о шифровании, а в России законодательно регулируется как импорт, так и экспорт шифров, причем использование несанкционированных шифров внутри страны запрещено.

Наиболее распространены два типа шифров: на основе секретных и на основе открытых/закрытых ключей. Рассмотрим их подробнее.

Шифры с секретными ключами

Их часто называют *симметричными шифрами*, потому что они используют один и тот же ключ как для шифрования, так и для дешифрования данных. При обмене сообщениями отправитель и получатель договариваются о конкретном значении секретного ключа. Например, если Тэд и Кэрол хотят обмениваться конфиденциальными сообщениями, они договариваются использовать следующий алгоритм шифрования.

1. Каждая буква преобразуется в число по определенной схеме, например a=6, b=7, c=8 и т.д.
2. Каждое число умножается на 4.

Секретным ключом здесь, очевидно, является схема преобразования букв в числа. Такой шифр довольно легко взломать, он лишь немного сильнее, чем шифр нашего предыдущего примера. Чтобы зашифровать сообщение "dinner is ready", Кэрол выполняет следующие арифметические действия:

```
d=9
9*4=36
i=14
14*4=56
...
```

В результате зашифрованное сообщение выглядит так:

```
36-56-76-76-40-92 56-96 92-40-24-36-120
```

У Тэда есть этот же ключ, поэтому он может расшифровать сообщение. Для этого ему нужно поделить каждое число на 4 и, согласно ключу, заменить его соответствующей буквой.

В США популярны шифры с секретными ключами DES (Data Encryption Standard) и 3DES ("тройной DES"), утвержденные Министерством обороны в качестве стандартных. Распространен также шифр RC-4 (Rivest Cipher-4), разработанный Роном Ривестом (Ron Rivest). Совместно с Ади Шамиром (Adi Shamir) и Леонардом Адлманом (Leonard Adleman) он разработал популярный шифр с открытыми/закрытыми ключами RSA. Этот тип шифров рассматривается несколько ниже.

При работе с секретными ключами возникает три главные проблемы.

- Создание секретных ключей.
- Обмен ключами между санкционированными пользователями таким образом, чтобы они не попали к посторонним лицам.
- Сложности, связанные с безопасностью коммуникации большого количества пользователей.

Весьма благоразумной мерой является периодическое изменение ключа. Однако это означает, что должна быть выработана какая-то стратегия или правила создания новых ключей. Должны быть также разработаны способы безопасной передачи новых ключей партнерам. Вернемся к предыдущему примеру. Если Кэрол передаст Тэду ключ по электронной почте в незашифрованном виде, то его могут перехватить и само шифрование станет бесполезным С другой стороны, если она передаст ключ в зашифрованном письме, то Тэд не сможет расшифровать его, потому что не знает нового ключа. Нельзя также сообщать новый ключ в последнем письме, зашифрованном старым ключом, потому что если у взломщика есть старый ключ, то он легко получит и новый.

Для решения этой проблемы разработаны специальные способы создания и безопасного обмена ключами. Один из них — алгоритм Диффи–Хеллмана (Diffie–Hellman) — позволяет партнерам создать новый ключ и обменяться им с помощью сетевого соединения с низким уровнем безопасности.

Третья проблема из нашего списка намного сложнее. Тэд и Кэрол, используя один и тот же ключ, могут успешно обмениваться секретными (до определенной степени) сообщениями на протяжении многих лет. Но что делать, если Кэрол понадобится передать секретное сообщение Бобу? Если она использует тот же ключ, то сообщение сможет расшифровать Тэд. Кроме того, получив ключ, Боб сможет расшифровывать переписку между Кэрол и Тэдом.

Конечно, Кэрол и Боб могут договориться о новом ключе. Пусть, например, сообщения Кэрол, предназначенные Бобу, шифруются по схеме a=12, b=13 и т д., а затем к результату добавляется 15. Однако теперь Кэрол должна помнить два ключа. Если же ей нужно обмениваться секретными сообщениями с большим количеством людей, то ситуация становится неуправляемой. Существует более эффективное решение: использовать шифр с открытыми/закрытыми ключами.

Шифры с открытыми/закрытыми ключами

Для краткости эти ключи иногда называют публичными, однако более точный термин — *шифры с открытыми/закрытыми ключами*, потому что в них используется два ключа: один из них, открытый, известен многим, а другой, закрытый, — только одному пользователю. В процессе коммуникации используются оба ключа. Шифры такого типа иногда называют *асимметричными*, а ключи — *парой ключей*. Работает шифр следующим образом.

- Кэрол и Тэд обмениваются своими открытыми ключами. Это можно делать даже в незашифрованном письме, потому что расшифровать сообщение с помощью открытого ключа невозможно.
- Когда Кэрол хочет передать секретное сообщение Тэду, она шифрует его с помощью открытого ключа Тэда, закрытый ключ для этого не нужен. Каждый открытый ключ ассоциирован с единственным закрытым ключом. Расшифровать сообщение, зашифрованное с помощью открытого ключа, можно только имея закрытый ключ. (Верно также обратное: сообщение, зашифрованное закрытым ключом, можно расшифровать только с помощью открытого ключа.)

- Тэд, используя свой закрытый ключ, успешно дешифрует сообщение Кэрол, потому что оно зашифровано с помощью его открытого ключа. Обратите внимание: во всем этом процессе использовались только ключи Тэда (открытый и закрытый).

Если Кэрол зашифрует сообщение с помощью своего закрытого ключа, то его сможет расшифровать каждый, потому что открытый ключ известен всем. Однако при этом закрытый ключ Кэрол все же останется засекреченным, открыть его невозможно.

В процессах шифрования и дешифрования используются оба ключа пары, принадлежащей Тэду, причем ни одному из партнеров нет необходимости знать закрытый ключ другого партнера.

Аутентификация

До сих пор рассматривалось только обеспечение *конфиденциальности* данных. *Аутентификация* пользователя — это совершенно другая задача.

С помощью шифра с открытым/закрытым ключом можно легко защитить сами данные. Однако открытый ключ известен всем, поэтому Тэд не может определить, действительно ли сообщение с его открытым ключом пришло от Кэрол. Чтобы Тэд мог определить (аутентифицировать) личность отправителя, Кэрол должна зашифровать сообщение с помощью своего закрытого ключа. Тогда Тэд сможет расшифровать это сообщение, используя открытый ключ Кэрол, и убедиться, что сообщение передала действительно Кэрол, потому что она единственный человек, знающий этот закрытый ключ.

Рассмотрим еще один способ аутентификации отправителя — использование *цифровой подписи.*

Цифровые подписи

Цифровая подпись представляет собой порцию информации, зашифрованную закрытым ключом отправителя и добавленную к документу. Получатель расшифровывает подпись открытым ключом отправителя и этим убеждается в ее аутентичности.

Аутентичность подписи гарантируется тем, что ее закрытый ключ известен только отправителю, благодаря этому создать ее может только он. Злоумышленник не может вырезать подпись и присоединить ее к другому документу, потому что подпись содержит элементы исходного документа. Если он сделает так, то при расшифровке подписи открытым ключом отправителя будет ясно видно, что она относится не к этому документу.

Подпись может подтверждать как личность отправителя, так и целостность самого документа. Подпись не шифрует данные, она лишь предотвращает несанкционированное изменение данных и подтверждает личность отправителя.

Алгоритмы хэширования

Хэш — это результат одностороннего математического преобразования (алгоритма хэширования), создающего *дайджест сообщения.* Преобразование называется односторонним потому, что обратное преобразование, т.е. получение сообщения из его профиля, невозможно.

Аутентичность сообщения проверяется с помощью хэша следующим образом.

1. Отправитель хэширует сообщение с помощью ключа, известного только ему и получателю. Результат хэширования представляет собой некоторое длинное число, например 0010110010100001.
2. Сообщение и дайджест (результат хэширования) передаются получателю.

3. Для проверки аутентичности сообщения получатель применяет к сообщению тот же ключ. В результате он должен получить тот же дайджест — 0010110010100001. Если содержимое сообщения при передаче изменилось, то результаты хэширования не совпадут.

В настоящее время наиболее распространены следующие алгоритмы хэширования.

- **SHA (Secure Hash Algorithm)**. Разработан институтом NIST (National Institute of Standards and Technology) и Управлением национальной безопасности США (National Security Agency — NSA).
- **MD5 (Message Digest 5)**. Разработан Роном Ривестом в Массачусетском технологическом институте (Massachussets Institute of Technologies — MIT).

Цифровые сертификаты

Цифровые сертификаты — это сообщения, содержащие цифровую подпись третьего доверительного лица, или *полномочного источника сертификата*. Третье лицо гарантирует, что данный открытый ключ действительно принадлежит указанной личности Сертификаты используются для обеспечения аутентичности сообщений, передающихся по публичным сетям с низким уровнем безопасности, таким, как Internet.

Пользователь, закрытый ключ которого ассоциирован с данным открытым ключом, запрашивает сертификат у полномочного источника сертификата. На полномочный источник возлагается обязанность проверки, действительно ли данный открытый ключ принадлежит данному пользователю. Сертификат действителен только на протяжении определенного промежутка времени. Полномочный источник может аннулировать сертификат.

Организации могут создавать собственные полномочные источники сертификатов как часть *инфраструктуры открытых ключей* (*Public Key Infrastructure — PKI*). Инфраструктура PKI представляет собой систему проверки и аутентификации идентичности лиц (физических и юридических), участвующих в процессах электронной коммуникации.

Цифровые сертификаты распространяются следующими публичными полномочными источниками сертификатов:

- Verisign;
- GTE Cybertrust;
- Keywitness;
- TradeWave.

Цифровые сертификаты можно рассматривать как электронные удостоверения личности. Водительская лицензия, паспорт и другие документы, выдаваемые государственными учреждениями, удостоверяют личность человека в физическом мире. Аналогично этому в мире сетевых коммуникаций цифровой сертификат удостоверяет идентичность пользователя или организации.

Kerberos

Kerberos — это стандартный в Internet протокол аутентификации, с помощью которого проверяется идентичность пользователей или компьютерных систем. Он был разработан в Массачусетском технологическом институте и назван по имени свирепого трехголового пса из древнегреческих мифов, охранявшего ворота в подземное

царство Аида. Надежность системы Kerberos обеспечивается тремя компонентами: клиентскими программами, серверными программами и доверительным авторитетным органом, который называется *центром распределения ключей* (*Key Distribution Center — KDC*). В системе KDC поддерживается база данных, с помощью которой отслеживаются действия участников протокола Kerberos.

Принцип действия Kerberos основан на концепции билетов, которые представляют собой зашифрованные сообщения, используемые для передачи на сервер запросов на услуги. Аутентификация выполняется с помощью симметричного алгоритма шифрования (шифра с секретным ключом), как показано на рис. 14.5.

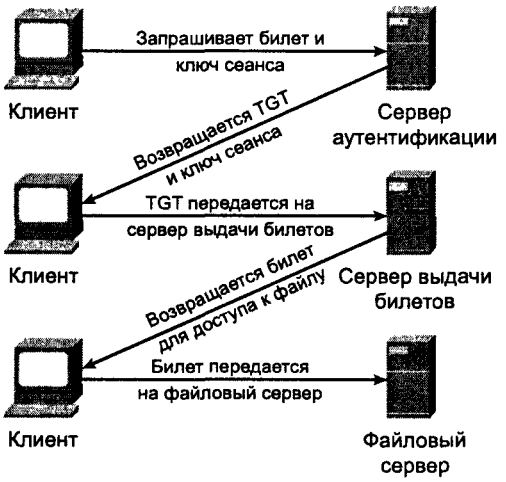


Рис. 14.5. Для проверки идентичности и предоставления доступа к серверу в процедуре аутентификации Kerberos используются билеты

Система Kerberos работает следующим образом.

1. Клиент передает на сервер аутентификации запрос на билет и *ключ сеанса*. Этот ключ зашифрован на основе пароля пользователя, передавшего запрос. К нему добавляется случайное число, представляющее запрашиваемую услугу. Возвращаемый пользователю билет, удостоверяющий идентичность клиента, называется TGT (*Ticket-Granting Ticket — билет на получение билета*).
2. Билет TGT передается клиентом на сервер, предоставляющий билеты (физически это может быть на том же компьютере, что и сервер аутентификации). На основе TGT сервер, предоставляющий билеты, передает клиенту билет. Клиент передает билет для доступа к файловому серверу, на котором хранятся нужные клиенту ресурсы.
3. Билет действителен только определенный промежуток времени, в течение которого клиент может передавать на сервер запросы, не выполняя процедуру получения билета повторно.

В сетях UNIX система Kerberos используется уже много лет. Компания Microsoft включила поддержку Kerberos в Windows 2000. Доверительные отношения доменов Active Directory основаны на аутентификации Kerberos.

Современные средства идентификации и аутентификации

По мере того как растут размеры корпоративных сетей, поддерживающих уже тысячи пользователей, идентификация и аутентификация пользователей становятся все более важной частью систем обеспечения безопасности. Определение идентичности пользователя, пытающегося зарегистрироваться в сети или получить доступ к ресурсам, служит фундаментом хорошего плана обеспечения безопасности.

Несмотря на всю изощренность средств шифрования паролей, слабым местом метода аутентификации на основе имени пользователя и пароля остается возможность их обнаружения и применения потенциальным злоумышленником. Для решения этой проблемы разрабатываются методы идентификации и аутентификации, которые невозможно подделать:

- интеллектуальные карты;
- биометрические методы, включая идентификацию отпечатков пальцев, радужной оболочки глаза и "отпечатков" голоса.

Пока что эти методы можно встретить лишь в некоторых правительственных учреждениях. Однако в ближайшее десятилетие следует ожидать их весьма широкого распространения, поэтому сетевым администраторам важно уже сейчас знать основные принципы их работы. Рассмотрим каждый биометрический метод подробнее.

Интеллектуальные карты

Это устройство аутентификации внешне напоминает кредитную карточку. В интеллектуальной карте хранится необходимая регистрационная информация, например открытые/закрытые ключи и пароли. Технология хранения может варьировать от самой простой (на основе магнитной полоски на поверхности карты) до такой сложной, как встроенная в карту интегральная микросхема.

Замечание

Применительно к технологиям сетевой безопасности термин "интеллектуальная карта" означает устройство идентификации и аутентификации, в котором хранится регистрационная информация, позволяющая пользователю получить доступ к системе. В других областях используется более широкое значение термина "интеллектуальная карта". В самом общем случае этот термин обозначает пластиковую карточку с встроенной микросхемой, выполняющей самые разнообразные функции — кредитной карточки, медицинской карты пациента и т.д.

В некоторые операционные системы, например Windows 2000, включены встроенные средства поддержки интеллектуальных карточек. Если в операционной системе нет встроенных средств их поддержки, то для этого можно использовать дополнительное программное обеспечение.

Информация интеллектуальной карточки поступает в компьютер с помощью специального устройства, которое называется *считывателем интеллектуальных карт*. Благодаря тому что пользователь должен физически держать в руках интеллектуальную карту, она является более сильным средством обеспечения безопасности, чем па-

роль. Карта может использоваться вместо ввода пользователем регистрационной информации или совместно с этим методом.

В системах с высокими требованиями к безопасности получить доступ только с помощью карты нельзя. Пользователь должен вставить карту в считыватель и ввести правильную регистрационную информацию с клавиатуры. Поэтому потенциальный злоумышленник, обнаруживший каким-либо образом пароль, не сможет зарегистрироваться и получить доступ, не имея в руках карты. И наоборот: если злоумышленник похитит карту, то он не сможет получить доступ, не зная правильного пароля.

Одной из разновидностей интеллектуальной карты можно считать *I-ключ*, разработанный компанией Rainbow Technologies. Он представляет собой небольшое устройство, сообщающееся с компьютером через порт USB.

Биометрические устройства

Однако все еще сохраняется возможность того, что злоумышленник выведает пароль и завладеет интеллектуальной картой. Чтобы исключить и эту возможность, разрабатываются такие средства, как идентификация отпечатков пальцев, радужной оболочки глаза и индивидуальных характеристик голоса пользователя. Научная дисциплина, на основе которой разрабатываются такие технологии, называется *биометрией*.

Работа биометрических методов основана на анализе индивидуальных характеристик человеческого организма, вероятность совпадения которых у двух разных людей настолько мала, что в судебном законодательстве допускается использование результатов биометрического анализа в качестве вещественного доказательства. На основе индивидуальных биологических параметров биометрические средства идентификации способны обеспечить вполне надежную позитивную идентификацию пользователя.

Рассмотрим, как работают различные биометрические методы.

Идентификация отпечатков пальцев

Система идентификации отпечатков пальцев часто используется совместно с интеллектуальной картой. Отпечатки пальцев пользователей предварительно считываются и вводятся в базу данных. Когда пользователь хочет получить доступ к компьютеру, он должен поместить палец (или несколько пальцев) на экран считывателя. Данные считывателя сравниваются с отпечатками, хранящимися в базе данных. В зависимости от результата сравнения, пользователь получает или не получает доступ.

Для технической реализации метода аутентификации на основе отпечатков пальцев разработано специальное оборудование и программное обеспечение. Это такие системы, как VeriPrint и U.are.U, поставляемые корпорацией FingerSec.

Идентификация сетчатки и радужной оболочки глаза

Еще один способ идентификации личности основан на уникальности биологических характеристик сетчатки глаза (внутренней поверхности глазного яблока, на которой располагаются нервные окончания, служащие рецепторами световых сигналов). Для сканирования участка поверхности сетчатки используется световой луч низкой интенсивности.

На уникальности характеристик человеческого глаза основан также метод *идентификации радужной оболочки*. В этом методе компьютер анализирует рисунок радужной оболочки, представляющей собой пигментированную округлую мембрану, благодаря которой глаза имеют определенный цвет. По некоторым данным рисунок радужной оболочки даже более индивидуален, чем отпечатки пальцев или ДНК. Рисунки радужной оболочки отличаются даже у полных близнецов.

Отпечатки голоса

Этот метод идентификации личности основан на уникальности некоторых характеристик голоса.

Замечание

Метод идентификации на основе отпечатков голоса иногда путают с задачей *распознавания голоса*. Решение последней задачи означает не идентификацию личности говорящего, а распознавание произнесенных слов и, применительно к программам распознавания голоса, преобразование распознанных слов в текстовый файл.

В данном методе пользователь должен сначала произнести пароль, т.е. некоторую фразу, которая сохраняется в базе данных. После этого для регистрации пользователь произносит эту же фразу и образцы сравниваются. При сравнении учитываются такие характеристики, как высота основного тона, интонация и модуляция голоса. Методы на основе отпечатков голоса считаются менее надежными, чем на основе рисунков сетчатки, радужной оболочки или отпечатков пальцев. Чаще всего методы идентификации по отпечаткам голоса используются, когда нужно аутентифицировать личность по телефонной линии.

Будущее биометрических методов

Во всем мире популярность биометрических методов аутентификации быстро растет. Особенно после трагических событий 11 сентября 2001 года.

Биометрические методы становятся все более надежными. Постепенно решаются проблемы, связанные с возможностями подделки. Эти факторы определенно указывают на то, что в недалеком будущем биометрические методы будут использоваться почти на каждом рабочем месте, оборудованном выходом в сеть.

Замечание

Специалисты в области биометрии строго различают понятия распознавания и аутентификации. Аутентификация рассматривается как добровольный акт предоставления пользователем своей регистрационной информации (имени, пароля, биометрических данных) для получения доступа в систему. Вводимые биометрические данные сравниваются с хранящимися в базе данных. Сравнение используется для проверки личности пользователя. Если проверка выполнена успешно, пользователь получает доступ. В то же время при распознавании в компьютер вводятся *только* биометрические данные (образцы голоса, сетчатки или отпечатков пальцев), после чего в базе данных ищутся образцы, совпадающие с введенными. Например, распознавание выполняется, когда судебный эксперт пытается идентифицировать отпечатки пальцев, найденные на месте преступления. Чтобы идентифицировать найденные отпечатки пальцев, эксперт должен найти совпадающие с ними в какой-либо базе данных, например в принадлежащей ФБР базе данных AFIS (Automated Fingerprint Identification System).

Разработка правил безопасности

Новые средства обеспечения безопасности появляются на рынке постоянно. Чтобы разработать эффективный план обеспечения безопасности сети, нужно хорошо знать все доступные для этого средства. Следует также определить уровень безопасности, необходимый или желательный в данной ситуации.

Разработанные правила безопасности должны быть результатом коллективных усилий технического и управленческого персонала, а также части пользователей. Кроме того, они должны поддерживаться руководством компании и пользователями. Финансовые и общие соображения должны быть сопоставлены с необходимым уровнем безопасности и найдены приемлемые компромиссные решения.

Правила безопасности должны быть изложены письменно, чтобы их можно было проанализировать и со временем вносить изменения соответственно изменяющимся обстоятельствам. Первым шагом создания правил является подробный анализ различных аспектов безопасности. Следует определить, какие меры безопасности применяются сейчас, достигают ли они своей цели и какие из них нуждаются в пересмотре.

Рассмотрим наиболее важные факторы, которые должны быть учтены при разработке правил безопасности, включая следующие:

- правила предоставления доступа;
- порядок прекращения доступа;
- нормы безопасности, учреждаемые правительством;
- выполнение аудита и обнаружение вторжений;
- брандмауэры и прокси;
- обеспечение безопасности с помощью нескольких протоколов;
- физическая безопасность.

Правила предоставления доступа

В состав правил сетевой безопасности должны входить правила предоставления доступа, определяющие, как санкционированные пользователи могут получать доступ и использовать сетевые ресурсы. Сюда входят такие вопросы, как шифрование сообщений и файлов, доступ к Web-узлам, загрузка файлов из Internet, использование имеющейся пропускной способности каналов, установка программ и игр, правила использования электронной почты и других пользовательских интерфейсов.

Порядок прекращения доступа

В правилах обеспечения безопасности должна быть предусмотрена ситуация, когда по собственному желанию или принудительно увольняется кто-либо из служащих. Это не должно нарушить нормальную работу сети или целостность сетевых данных.

Необходимо особенно позаботиться о сохранности собственности компании. Служащий должен немедленно сдать интеллектуальную карту и другие устройства доступа. Учетную запись увольняемого служащего следует аннулировать. Если служащий имел доступ к ценным данным, ему нельзя позволить унести свои личные дискеты, zip-дисководы или другие носители без их проверки, в процессе которой необходимо удостовериться, что он не скопировал на них конфиденциальные данные компании.

Нормы безопасности, учреждаемые правительством

Правительством США установлены критерии определения норм сетевой безопасности. Эти критерии устанавливаются спецификациями *Department of Defense Trusted Computer System Evaluation Criteria (Критерии оценки безопасности компьютерных систем Министерства обороны)*, сокращенно — TCSEC. Иногда этот документ называют "оранжевой книгой". Спецификации TCSEC опубликованы Национальным центром

компьютерной безопасности (National Computer Security Center — NCSC). Они используются вместе со спецификациями TNI (Trusted Network Interpretation of TCSEC — Интерпретация TCSEC для безопасных сетей), которые иногда называют "красной книгой".

Спецификации TNI определяют критерии оценки безопасности для сетей. Шкала рейтингов сетей начинается с рейтинга A — самого высокого уровня безопасности — и продолжается до самого низкого рейтинга D. Рейтинг C разделен на два подуровня — C1 и C2, однако подуровень C1 в настоящее время больше не используется. Рейтинг C2 — более высокий, чем рейтинг C1 — является обязательным для коммерческих организаций, желающих получать государственные заказы. Нормами рейтинга C2 обусловлено, что в операционной системе должны быть средства отслеживания получения доступа к данным. В операционной системе, претендующей на рейтинг C2, администратор должен иметь возможность контролировать доступ пользователей к объектам и должны поддерживаться средства уникальной идентификации пользователей и аудита событий, связанных с безопасностью.

Если организации нужно, чтобы ее компьютерные системы имели рейтинг C2, то сетевой администратор должен обеспечить выполнение всех соответствующих этом уровню условий TCSEC и TNI. После этого для выполнения государственных контрактов необходимо получить сертификат рейтинга C2, официально утвержденный полномочными органами.

Замечание

В других странах используются иные рейтинги безопасности, во многом аналогичные рассмотренным В Канаде они называются CTCPEC (Canadian Trusted Computer Product Evaluation Criteria), в Австралии — AISEP (Australian Information Security Evaluation Programme), а в Западной Европе — ITSEC (Information Technology Security Evaluation Criteria)

В табл. 14.1 приведены различные операционные системы и присвоенные им рейтинги безопасности.

Таблица 14.1. Рейтинги безопасности различных операционных систем, присвоенные Агентством национальной безопасности

Операционная система	Поставщик	Сертификат NSA
UNIX XTS-200 и 300	Wang Government Svcs	Оранжевая книга, B3
UNIX Trusted Xenix 3 и 4	Trusted Information Systems	Оранжевая книга, B2
UNIX HP-UX 8 04 и 9 0 9	Hewlett Packard	Оранжевая книга, B1
UNIX UNICOS 8 0 2	Cray Research	Красная книга, B1
UNIX RS/6000	IBM	Оранжевая книга, C2
Windows NT 3 5/SP3 и Windows NT 4 0	Microsoft	Оранжевая книга, C2
NetWare 4 и 4 11	Novell	Красная книга, C2

Только установка сертифицированной операционной системы не гарантирует выполнения всех требований критериев безопасности. Необходимо удовлетворить и другие спецификации, а именно на сетевые соединения и конфигурацию средств операционной системы. Фактически рейтинг безопасности присваивается не самой операционной системе, а всей архитектуре оборудования и программного обеспечения.

Аудит безопасности и обнаружение вторжения

Одно из требований рейтинга безопасности C2 — возможность аудита событий безопасности и действий пользователей. *Аудит* — это отслеживание действий пользователей и системы. Например, в процессе аудита администратор определяет, к каким файлам, кем и когда был запрошен доступ. В результат аудита может входить информация о том, кто регистрировался в системе или завершал зарегистрированный сеанс, кто получал доступ к объектам и какие права доступа были использованы.

Операционные системы Windows NT/2000 содержат встроенные средства аудита, которые можно сконфигурировать довольно подробно. События безопасности (действия пользователей и операции системы, которые могут повлиять на безопасность) не только отслеживаются, но и записываются в файл журнала, где их можно легко просмотреть. Доступ к журналам безопасности должны иметь только администраторы.

Пассивное обнаружение

Аудит безопасности является *пассивной* формой обнаружения вторжения. В процессе работы системы события безопасности автоматически записываются в файл журнала. Администратор проверяет файл и находит возможные нарушения безопасности. Для облегчения этой задачи существуют программы пассивного обнаружения, такие, как Tripwire для UNIX и встроенные средства аудита безопасности в Windows NT/2000.

Активное обнаружение

Если требования к безопасности сетевых данных особенно высоки, то не следует полагаться лишь на пассивное обнаружение вторжения. План поддержания безопасности должен содержать один или несколько методов активного обнаружения. В этих методах специальная программа непрерывно просматривает сеть в поисках признаков возможного вторжения. Обнаружив что-либо подозрительное, программа оповещает администратора или автоматически отключает сетевое соединение. Примерами таких программ являются NetRanger и SATAN (зловещая аббревиатура означает всего лишь Security Administrator's Tool for Analyzing Networks).

В последнее время выпущена обновленная версия программы SATAN, носящая более приятное имя SAINT (святой) — Security Administrator's Integrated Tool — и предназначенная для обеспечения безопасности. Программа SAINT способна обнаруживать большее число признаков вторжения, чем SATAN. В настоящее время доступна ее версия WebSaint, более легкая в использовании и, кроме того, позволяющая администратору проверять систему через Internet.

Брандмауэры и прокси-серверы

Для обеспечения большей безопасности иногда бывает необходимо организовать защиту по всему периметру локальной сети. Это можно сделать с помощью *брандмауэров* и *прокси-серверов*, использовав их для создания барьера между внутренней локальной сетью и соединениями с внешним миром. Такая защищенная область может быть установлена также в подсети. Иногда ее называют *демилитаризованной зоной (DMZ)* или *экранированной сетью* (рис. 14.6).

Брандмауэр может быть реализован как аппаратным, так и программным образом. Фактически он является средством фильтрации входящих и исходящих пакетов. На основе правил безопасности, установленных сетевым администратором, брандмауэр определяет, следует ли пропустить поступивший пакет. Обычно брандмауэры располагают на *шлюзах* сети, являющихся точками ее соединения с другой сетью.

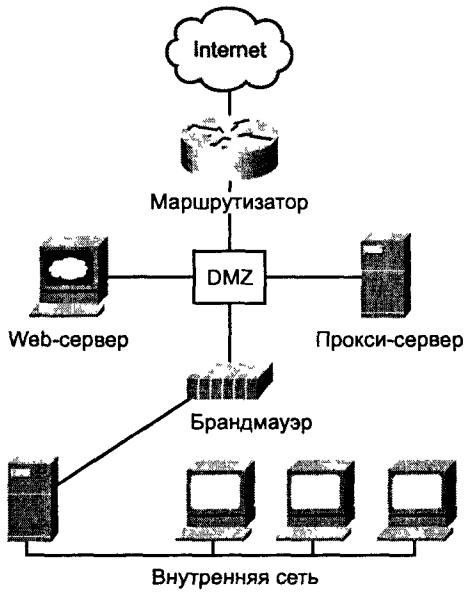


Рис 14.6 Брандмауэры и прокси-серверы образуют барьер между демилитаризованной зоной и внешней сетью

Различают следующие базовые типы фильтрации с помощью брандмауэров:

- фильтрация пакетов;
- фильтрация каналов;
- фильтрация приложений.

При *фильтрации пакетов* анализируется информация заголовков IP, TCP/IP и ICMP. В этом способе фильтрации администратор может разрешить либо заблокировать определенные IP-адреса или номера портов. *Фильтрация канала* выполняется для текущего соединения. Если пакет не является частью установленного соединения, то брандмауэр не пропустит его. И наконец, *фильтрация приложений* выполняется на основе протоколов, используемых конкретным приложением. Например, могут быть заблокированы аплеты Java или сценарии Visual Basic.

Аппаратно реализованные брандмауэры иногда называют "черными ящиками". Они представляют собой выделенные компьютеры, на которых установлена особая операционная система (или в некоторых случаях UNIX) Такой компьютер работает *только* как брандмауэр, поэтому он выполняет процедуры фильтрации быстрее и надежнее, чем это делал бы компьютер, совмещающий функции брундмауэра с выполнением других задач.

Прокси-серверы работают как "посредники" сетевых соединений. Их функции аналогичны функциям брандмауэров. Компьютеры внутренней сети сообщаются с прокси, которые, в свою очередь, сообщаются с компьютерами внешних сетей (рис 14 7)

Прокси-серверы предоставляют такие услуги, как *обращение прокси* и *обращение хостирования*. В методе обращения прокси внешний запрос HTTP перенаправляется прокси-сервером на единственный предназначенный для него компьютер. Это повышает безопасность внутреннего Web-сервера, потому что в этом случае к нему нет доступа непосредственно из внешней сети. В методе обращения хостирования прокси-сервер может перена-

правлять запросы HTTP более чем на один Web-сервер путем отображения нескольких серверов на один логический адрес (рис. 14.8). Прокси-серверы выполняют также кэширование Web-страниц, повышая этим производительность Web-серверов.

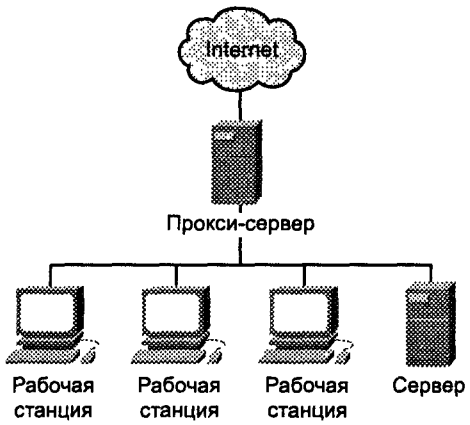


Рис. 14.7. Прокси-сервер работает как посредник между внутренними и внешними компьютерами



Рис. 14.8. В методе обращенного хостирования прокси-сервер перенаправляет запросы HTTP на несколько Web-серверов

Маршрутизаторы и коммутаторы уровня 3 могут быть сконфигурированы со *списком контроля доступа*, ограничивающим использование маршрутизатора определенными компьютерами или разрешающим коммуникацию только в одном направлении. В этом случае маршрутизатор выполняет функции брандмауэра.

Маршрутизаторы, сконфигурированные со списком контроля доступа, фактически являются "первой линией обороны" сети. Они часто используются для защиты программных брандмауэров от постороннего вмешательства.

Замечание

Используемые в маршрутизаторах списки контроля доступа предоставляют или блокируют доступ на основе таких параметров, как, например, IP-адреса. Это значит, что пакет с поддельным IP-адресом пройдет через брандмауэр маршрутизатора беспрепятственно.

Повышение безопасности с помощью нескольких протоколов

Стратегия сетевой безопасности должна также учитывать используемые протоколы. Повысить безопасность внутренней сети можно путем использования в локальной сети или в демилитаризованной зоне, отделяющей подсеть от внешнего мира, стека протоколов, отличного от TCP/IP.

Если в локальной сети в качестве сетевого/транспортного протокола вместо TCP/IP использовать IPX/SPX, то атаки из Internet на основе IP-адресов не смогут проникнуть в локальную сеть. Для создания такой защиты необходимо сконфигурировать маршрутизаторы на использование TCP/IP со стороны Internet и IPX/SPX со стороны локальной сети. Если внутренние компьютеры сети должны сообщаться между собой с помощью TCP/IP, то следует установить демилитаризованную зону, в которой для сообщения локальной сети с Internet используется IPX/SPX.

Физическая безопасность

Хорошая стратегия сетевой безопасности должна регулировать *физический доступ* к сетевым компонентам. При разработке плана безопасности этому важному фактору часто не уделяют должного внимания. Сетевой администратор должен оценить необходимые уровни доступа, предоставляемого служащим, партнерам, клиентам и широкой публике к рабочим компьютерам, серверам, кабелям, иным носителям, маршрутизаторам, коммутаторам и к другим физическим компонентам.

В сетях с высокими требованиями к безопасности серверы и соединительные устройства должны находиться в комнатах, запираемых на замок. Если рабочий компьютер находится в общей комнате, то следует программно контролировать его доступ к ценным данным. Кабели должны быть защищены прочными кожухами, причем на потолках и стенах не должно быть оставлено незащищенных участков. Злоумышленнику легче всего подключиться к витым парам и коаксиальным кабелям, однако перехват данных, передаваемых по оптическому кабелю физически тоже возможен. Для этого используют оптические разветвители. Поскольку незаконное подключение выполняется на физическом уровне, администратор может обнаружить его с помощью рефлектометра OTDR (Optical Time Domain Reflectometer). Однако квалифицированный взломщик может подключиться таким образом, что обнаружить подключение с помощью OTDR будет довольно сложно.

Во многих организациях прилагаются значительные усилия для ограничения доступа к компьютерному оборудованию служащих и других пользователей в рабочее время, а затем двери остаются открытыми для обслуживающего персонала, например уборщиков. Если требования к сетевой безопасности высоки, то уборка помещений должна выполняться под надзором кого-либо из надежных служащих.

Защита от краха и восстановление

Вторжение извне — не единственная угроза безопасности сетевых данных. К потере ценных файлов могут привести также отказы оборудования, стихийные бедствия и технические ошибки. Поэтому стратегия защиты от краха и восстановления потерянных данных важна для любой рабочей сети.

Стратегия защиты от краха и восстановления включает следующие элементы:

- резервирование электропитания;
- резервное копирование данных;
- обеспечение отказоустойчивости дисков;
- обеспечение отказоустойчивости серверов (кластеризация).

Рассмотрим базовые принципы и способы реализации этих мер.

Резервирование электропитания

Известны многочисленные случаи потери компаниями ценных данных, когда во время летней грозы внезапно пропадало электропитание или в электросети возникал скачок напряжения. Особенно огорчительны такие потери тем, что их можно было легко предотвратить.

Тем не менее компании продолжают терять данные вследствие скачков или перебоев в электропитании. Здесь рассматривается, как защитить сеть от сбоев электропитания с помощью фильтров, источников бесперебойного электропитания и автономных генераторов.

Фильтры питания

Пик, или скачок, напряжения питания может вывести из строя оборудование компьютера или разрушить хранящиеся данные. Хороший фильтр питания, или подавитель скачков — это абсолютный минимум, который необходимо обеспечить для каждого критичного сетевого компьютера, включая серверы и ответственные клиентские компьютеры.

Замечание

Подавитель скачков — это более дешевое устройство защиты электропитания, однако его функции ограничиваются предотвращением последствий *повышения* напряжения. Они не защищают компьютер от понижения напряжения или отключения электропитания.

Источники бесперебойного питания

Более совершенный, но и более дорогой способ защиты — использование источника бесперебойного питания, представляющего собой устройство с аккумулятором, в котором накоплен достаточный запас энергии, чтобы компьютер смог нормально работать некоторое время после отключения напряжения электросети.

Источник бесперебойного питания *не предназначен* для длительной работы. Его назначение — поддержать питание несколько минут, в течение которых пользователь может закрыть файлы и приложения и правильно завершить работу операционной системы. Типичные источники бесперебойного питания продолжают работать от 5 до 20 минут, после чего аккумулятор разряжается и напряжение пропадает.

Вилка источника бесперебойного питания вставляется в розетку электросети, а вилка компьютера — в розетку на источнике. На многих источниках установлено несколько розеток, поэтому к ним можно подключить несколько компьютеров. В нормальном режиме аккумулятор источника непрерывно подзаряжается. Когда электропитание отключается, источник бесперебойного питания обнаруживает это и переключает компьютер на аккумулятор. Многие источники можно сконфигурировать таким образом, чтобы пользователь извещался о переключении. Извещение может быть в форме звукового сигнала или передачи специального сообщения по заданному сетевому адресу. Это же программное обеспечение может быть сконфигурировано на автоматическое завершение работы операционной системы и приложений.

К таким источникам должны быть подключены все критичные системы сети. Цена хорошего источника бесперебойного питания намного меньше стоимости нового компьютера или стоимости потери ценных данных.

Замечание

В литературе по источникам бесперебойного питания часто используется термин "режим аккумулятора", однако в действительности оборудование компьютера практически всегда питается не от аккумулятора, а от электросети. Название режима означает, что аккумулятор постоянно подзаряжается. Поэтому аккумулятор находится в постоянной готовности.

Автономные генераторы

Следующий шаг защиты электропитания — использование автономных генераторов электроэнергии. Генератор производит электрическую энергию с помощью двигателя внутреннего сгорания. Если установлен генератор, то при исчезновении напряжения в электросети работа электрооборудования (включая компьютеры) может продолжаться как угодно долго.

Автономные генераторы дороги. Их покупка редко окупается, за исключением случаев, когда электропитание отключается часто и на долгое время или когда прекращение работы компьютерной системы ведет к тяжелым последствиям.

Резервное копирование данных

Несмотря на все попытки предотвратить потерю данных, время от времени это все же происходит. Жесткий диск может выйти из строя, сервер может оказаться поврежденным в результате наводнения, пожара или даже простого падения со стола на пол, компьютерный вирус может отформатировать диск и т д. В результате данные окажутся утерянными. Но если с помощью специальной программы регулярно выполнялось резервное копирование, то восстановить утерянные данные не так уж сложно.

Разработка плана резервного копирования предполагает ответы на следующие вопросы.

- Какие файлы следует копировать?
- Когда нужно выполнять копирование?
- Как выполнять копирование?
- Зачем выполняется копирование?

Ответ на последний вопрос очевиден. План резервного копирования предотвращает катастрофическую потерю данных, времени и денег ценой всего лишь небольших неудобств и некоторого труда на восстановление файлов в исходное состояние. Рассмотрим ответы на три остальных вопроса.

Что следует копировать

При составлении плана резервного копирования в первую очередь необходимо определить, какие файлы следует копировать, и присвоить файлам приоритеты соответственно их значимости. Конечно, в идеале следовало бы копировать все. Однако это редко выполнимо из-за ограниченности времени и объема носителей.

Резервное копирование операционной системы и файлов приложений не обязательно, потому что их всегда можно установить заново с дистрибутивов. Намного важнее выполнять резервное копирование рабочих данных, включая текстовые документы, базы данных, электронные таблицы и другие данные, созданные различными пользовательскими приложениями. Высокий приоритет должно иметь копирование результатов творческой работы, например картин художников или литературных произведений, потому что их невозможно восстановить точно. Высокий приоритет имеют также данные, утрата которых может привести к большим финансовым потерям или к нарушению нормальной работы компании.

Необходимо составить список подлежащих копированию объектов. Резервные копии данных следует хранить в одном месте, например на специально выделенном для этого диске сервера. Если резервные копии данных разбросаны в сети по отдельным жестким дискам, то нетрудно упустить какие-либо важные данные.

Когда выполнять резервное копирование

Необходимо создать расписание периодического, *регулярного* резервного копирования важных данных. Оптимальный интервал времени между созданием копий зависит от того, как много данных может позволить себе потерять компания, например созданные за день или за неделю.

Расписание резервного копирования рекомендуется составить таким образом, чтобы копии создавались в нерабочее время, тогда процессы копирования не повлияют на производительность сети. Как показано в следующем подразделе, большинство хороших программ резервного копирования позволяют создавать расписание автоматического копирования, выполняющееся без личного присутствия сетевого администратора или других служащих.

В расписание обычно включаются различные типы резервного копирования. Различают три базовых типа копирования (хотя некоторые утилиты резервного копированию предоставляют дополнительные возможности).

- **Полное резервное копирование**. Копируются все данные заданных дисков независимо от того, когда их копирование выполнялось последний раз и вносились ли с тех пор изменения.
- **Дифференциальное резервное копирование**. Копируются все файлы, которые изменялись со времени последнего полного копирования.
- **Инкрементное копирование**. Копируются все файлы, которые изменялись со времени любого последнего копирования (а не последнего полного копирования).

Полное копирование требует больше всего времени и занимает больше всего места на носителях резервных копий, следовательно, это самый дорогостоящий метод копирования. Но это и самый простой метод: если выполнять полное резервное копирование каждую ночь, то можно быть уверенным, что сохранятся все обновления данных, выполненные до сегодняшнего дня. В этом методе также легче всего восстанавливать данные.

Дифференциальное копирование экономит время. Оно выполняется наряду с полным копированием. Например, можно выполнять полное копирование раз в неделю или раз в месяц, а в промежутках каждую ночь выполнять дифференциальное копирование. Для восстановления данных нужно восстанавливать две копии — последнюю полную и последнюю дифференциальную, тогда во всех данных будут учтены последние обновления. Такой метод оптимален при копировании большого объема данных, причем по ночам для этого выделяется недостаточно времени. Дифференциальное копирование требует намного меньше времени, чем полное. К тому же полные копии могут создаваться в выходные дни, когда для этого можно выделить больше времени.

Инкрементное резервное копирование выполняется быстрее, чем другие методы, однако в нем намного сложнее восстановить данные, причем это занимает гораздо больше времени. При использовании этого метода необходимо восстанавливать последнюю полную копию и *все* инкрементные копии, созданные со времени последнего полного копирования.

Замечание

Откуда программа копирования "знает", какие данные изменялись со времени последнего копирования? Для этого каждому файлу присвоен *архивный бит*, представляющий собой атрибут файла, аналогичный атрибутам, указывающим на то, что файл

является скрытым или предназначен только для чтения. При полном или инкрементном копировании файла этот бит обнуляется. При дифференциальном копировании бит *не* обнуляется

Как следует выполнять резервное копирование

Перед выполнением резервного копирования необходимо ответить на ряд вопросов.

- На каких носителях сохранять резервные копии?
- Какие программы резервного копирования использовать?
- Кто отвечает за резервное копирование?
- Выполнять резервное копирование вручную или автоматически?

На протяжении многих лет наиболее популярным носителем для резервных копий были магнитные ленты Поэтому некоторые программы резервного копирования (например, утилиты резервного копирования, встроенные в Windows NT) не поддерживают других носителей. Однако сейчас уже существует множество программ, позволяющих выбирать из нескольких типов носителей, включая сменные диски Zip, Jaz, CD-R, CD-RW, DVD и магнитооптические.

Многие операционные системы содержат встроенные утилиты резервного копирования. В состав Windows 9*x* и Windows NT/2000 входит утилита резервного копирования Windows Backup, в состав NetWare — SBackup, а в состав UNIX — встроенная программа архивирования *tar*. Другие поставщики также предоставляют программы резервного копирования, причем некоторые из них имеют более широкий набор средств, чем встроенные в операционные системы В среде Windows популярны следующие программы резервного копирования· ARCserve компании Cheyenne, Backup Exec компании Seagate и Norton Backup компании Symantec.

Необходимо назначить ответственного за выполнение операций резервного копирования. Учетная запись такого сотрудника должна иметь соответствующие права доступа на копирование данных всех других пользователей. При этом ему можно не предоставлять права чтения файлов. Для выполнения операций резервного копирования и даже восстановления эти права не обязательны. Необходимо также назначить сотрудника, способного в любой момент подменить ответственного за резервное копирование. Естественно, он должен обладать соответствующей квалификацией и знать используемый организацией план резервного копирования.

Независимо от того, вручную или автоматически выполняется резервное копирование, очень важно периодически проверять правильность процедуры копирования. Для проверки целостности восстановленных данных не следует ожидать аварии оборудования. После аварии может оказаться, что из-за какой-либо мелкой ошибки на носитель вообще ничего не записывалось. Для проверки следует периодически выполнять процедуру восстановления данных из резервных копий, даже если в этом нет необходимости.

И наконец, следует предусмотреть многократное резервное копирование особенно ценных данных Как минимум одну из таких копий необходимо хранить за пределами здания. Если хранить ленту или диск с резервной копией в ящике стола рядом с сервером, то в результате пожара или стихийного бедствия могут оказаться уничтоженными как данные, так и резервные копии. Одна из резервных копий может храниться дома у служащего, пользующегося доверием, в банковском сейфе, в филиале компании либо на удаленном сервере, с которым есть связь по телефонной линии или по Internet.

Отказоустойчивость дисков

Еще один способ защиты данных на диске от аварии — реализация отказоустойчивой конфигурации дисков. (*Отказоустойчивость* означает способность системы к восстановлению после аварии.) Отказоустойчивая конфигурация представляет собой объединение нескольких физических жестких дисков в *отказоустойчивый набор*, который может быть реализован в нескольких различных формах.

Отказоустойчивая конфигурация дисков называется также системой *RAID* (*Redundant Array of Independent (Inexpensive) Disks — избыточный набор независимых (недорогих) дисков*). В сетевых технологиях используется несколько типов отказоустойчивой конфигурации.

- **Зеркальное отображение дисков (RAID уровня 1)**. Для реализации этого метода нужны два физических жестких диска, предпочтительно одного и того же объема. Все данные одного диска зеркально отображаются на другой. На втором диске хранится точный дубликат всех файлов и структур первого диска. Если один из дисков выходит из строя, вместо него подключается другой диск. Переключение может выполняться автоматически. Можно также сконфигурировать операционную систему таким образом, чтобы она знала, где найти резервный диск. Например, в Windows NT это выполняется путем редактирования файла `boot.ini`.
- **Дуплексирование дисков (RAID уровня 1)**. Метод дуплексирования дисков отличается от зеркального отображения лишь тем, что в нем два физических диска подключаются к отдельным контроллерам дисководов. Это повышает отказоустойчивость, потому что в случае выхода из строя одного из контроллеров другой диск может продолжать нормально работать.
- **Распределение дисковой памяти с контролем четности (RAID уровня 3)**. В этом методе данные записываются на двух дисках полосами (слоями), а на третьем диске, специально выделенном для этого, записывается информация контроля четности. Поэтому для реализации метода необходимы, как минимум, три физических диска. Если диск данных терпит крах, то данные могут быть восстановлены с помощью информации контроля четности.
- **Распределение дисковой памяти со слоями контроля четности (RAID уровня 5)**. Этот метод работает аналогично RAID 3, за исключением того, что информация контроля четности (как и данные) записывается полосами, перемежающимися по дискам. Для данных контроля четности отдельный диск не выделяется. Как и в RAID 3, для реализации метода необходимы, как минимум, три диска. Если один из дисков терпит крах, данные могут быть восстановлены.

Используются также два менее распространенных уровня метода RAID.

- **RAID 2**. Аналогичен RAID 3 в том, что данные записываются полосами на многих дисках и один диск выделен для информации контроля четности. Отличие состоит в том, что данные расслоены по битам, в то время как в RAID 3 — по байтам.
- **RAID 4**. Также аналогичен RAID 2 и 3 за исключением того, что данные расслоены по блокам, а не по битам или байтам.

Для повышения скорости чтения и записи данных часто используется метод RAID 0, однако он *не* является отказоустойчивым. В методе RAID 0 данные расслаиваются по многим дискам поблочно, информация контроля четности не за-

писывается. Следовательно, если один из дисков терпит крах, то данные не могут быть восстановлены.

Метод RAID может быть реализован как программно, так и аппаратно. Аппаратный метод RAID более быстродействующий и надежный, однако его реализация обходится дороже. Некоторые операционные системы, такие, как Windows NT Server и Windows 2000 Server содержат встроенные средства поддержки программного RAID.

Методы кластеризации

Основой всех методов защиты данных от аварий является *избыточность*. При резервировании электропитания используются избыточные источники электроэнергии — устройство бесперебойного питания наряду с электросетью. Резервное копирование данных предполагает создание избыточных копий ценных файлов на дополнительных носителях. В системах отказоустойчивых дисков данные записываются на избыточных дисках. Крайней степенью избыточности является кластеризация.

В общем случае *кластеризация* означает группирование серверов в *кластеры*. В сети кластер серверов виден пользователям как один сервер. Если один сервер выходит из строя, его обязанности выполняет другой сервер кластера. Пользователи не замечают этот переход. Кластер серверов показан на рис. 14.9.

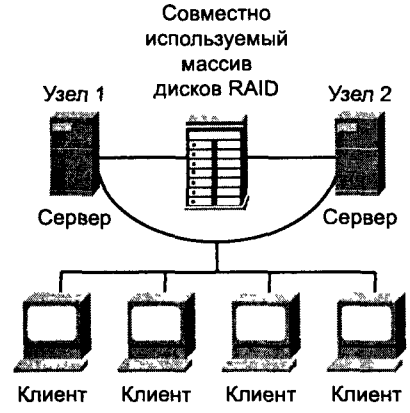


Рис 14 9. Объединение серверов в кластеры — дорогой, но эффективный способ обеспечения отказоустойчивости

Средства поддержки кластеризации встроены в такие операционные системы, как, например, Windows 2000 Advanced Server. Существует также программное обеспечение кластеризации, предназначенное для конфигурирования серверов в других операционных системах. Кроме повышенной отказоустойчивости, применение кластеризации имеет и другие преимущества, например выравнивание загрузки серверов.

Резюме

Для обеспечения безопасности сети должны быть одновременно задействованы многие меры. Высокая безопасность достигается путем использования плана, предусматривающего применение многих средств и мер обеспечения безопасности

В этой главе рассмотрены различные способы защиты сети и сетевых данных, хранящихся в сети или передаваемых по ней. Сначала была затронута обширная тема защиты сетей от злоумышленников, а затем — защита данных от аварий и методы восстановления.

Описаны способы обеспечения безопасности сети и внешние угрозы, способные нарушить ее, такие, как несанкционированное использование паролей и ключей, атаки DoS, подмена IP-адресов, компьютерные вирусы, черви и другие зловредные участки выполняемого кода, например троянские кони.

Затем были рассмотрены внутренние угрозы — промышленный шпионаж, внутренние интриги, недовольство служащих, бывших служащих и случайные нарушения безопасности.

Приведен обзор основных концепций криптографии и методов шифрования и дешифрования файлов, имеющих целью предотвратить использование конфиденциальной информации нежелательными лицами. Вы узнали, чем отличаются симметричные шифры с секретными ключами от несимметричных шифров с открытыми/закрытыми ключами. Рассмотрена аутентификация — процесс определения, действительно ли сообщение было отправлено указанным лицом или компьютером.

Представлены нормы и рейтинги безопасности, утвержденные правительством США, рейтинги наиболее популярных операционных систем, аудит безопасности и способы обнаружения вторжений. Затем были рассмотрены брандмауэры и прокси-серверы, а также создание демилитаризованной зоны между внутренней сетью и Internet (или другой внешней сетью) для защиты ресурсов локальной сети.

Описано использование разных протоколов для внутренней и внешней сетей в целях уменьшения риска вторжения извне. Первая половина главы заканчивается кратким обзором средств обеспечения физической безопасности сетевых компонентов.

Вторая половина главы посвящена защите от потери сетевых данных в результате аварий и методам восстановления данных: резервированию электропитания, резервному копированию данных, отказоустойчивым наборам дисков и кластеризации серверов.

Теперь вы знаете, как защитить сеть от вторжения из внешнего мира. В следующей главе рассматривается, как подключиться к внешнему миру с помощью телефонной линии.

Средства удаленного доступа становятся все более популярными. Все больше служащих используют доступ к сети компании из своего дома или находясь в дороге. В главе 15, "Удаленный доступ", рассматриваются устройства удаленного доступа и способы установки и конфигурирования клиентов и серверов удаленного доступа. Обсуждаются также специальные вопросы безопасности, возникающие при установке коммутируемых соединений с сетью.

Рекомендуемые источники

Дополнительная информация о законах США, регулирующих экспорт технологий шифрования, приведена по адресу: `www.bxa.doc.gov/Encryption`.

Прекрасный обзор протокола IPSec приведен на Web-узле компании Cisco по адресу: `www.cisco.com/warp/public/cc/techno/protocol/ipsecur/prodlit/ipsec_ov.htm`.

Полезная книга издательства Cisco Press, раскрывающая многие аспекты создания безопасных сетей — *Designing Network Security*.

Хороший источник информации о безопасности средств электронной почты находится по адресу www.emailtoday.com/emailtoday/dir/email_security.htm

Полезные ссылки на Web-узлы, в которых рассматриваются службы сертификации и технологии шифрования, можно найти по адресу www.security-online.com/info/certificates.html

Упрощенное изложение системы Kerberos можно найти по адресу www.homex.s-one.net.sg/member/itsecurity/netsec1.htm

Сертификаты безопасности NCSC/NSA Security приведены по адресу www.radium.ncsc.mil/tpep/epl.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы

1. Как называется число или код, используемые системой для проверки целостности сетевого соединения?
   - **а.** Пароль
   - **б.** Криптография
   - **в.** Ключ
   - **г.** Аутентификация
2. Как называется процесс перебора всех возможных комбинаций букв и цифр с целью взлома пароля?
   - **а.** Дешифрование
   - **б.** Атака методом грубой силы
   - **в.** Атака троянского коня
   - **г.** Атомная атака
3. Как называется передача сообщений ICMP с целью переполнить и вывести из строя сервер или сеть?
   - **а.** Атака SYN
   - **б.** Червь
   - **в.** Ping of Death
   - **г.** Наводнение Ping
4. Что из приведенного является распространенной внутренней угрозой сетевой безопасности? (Выбрать все подходящее)
   - **а.** Промышленный шпионаж
   - **б.** Случайные нарушения
   - **в.** Подмена IP-адресов
   - **г.** Прокси
5. Какие из приведенных требований правильной стратегии парольной защиты в сетях с высокими требованиями к безопасности справедливы?

а. Пользователям разрешается создавать и использовать пароли, которые легко запомнить.

б. Пароли должны иметь большую длину, например шесть символов.

в. В паролях нельзя использовать символы или цифры.

г. Пользователям запрещено изменять свои пароли.

6. Что из приведенного правильно описывает права доступа по умолчанию к вновь созданному разделяемому ресурсу на сервере Windows 2000?

а. Права доступа к ресурсу не имеет никто.

б. Каждый имеет к ресурсу право доступа "только чтение".

в. Каждый имеет право полного контроля над ресурсом.

г. Члены группы администраторов имеют к ресурсу право доступа "только чтение".

7. Что из приведенного лучше всего характеризует шифрование файлов?

а. Шифрование файлов защищает данные, хранящиеся на жестком диске.

б. Шифрование файлов защищает данные, передаваемые по сети.

в. Шифрование файлов защищает данные как при хранении на диске, так и при передаче по сети.

г. Программы шифрования предоставляются не в составе операционных систем, а поставляются независимыми компаниями.

8. Что такое ESP (применительно к вопросам сетевой безопасности)?

а. Extra-Sensitive Packets.

б. Extended Security Protocol.

в. Encapsulating Security Payload.

г. External Security Properties.

9. В каком из приведенных методов шифрования для шифрования и дешифрования данных используется один и тот же ключ?

а. Асимметричный шифр.

б. Шифр с открытым ключом.

в. Шифр с открытым/закрытым ключами.

г. Шифр с секретным ключом.

10. Как называется одностороннее математическое преобразование, создающее дайджест сообщения, используемый для проверки его аутентичности?

а. Цифровой сертификат.

б. Алгоритм хэширования.

в. Билет на получение билета.

г. Сканирование сетчатки.

Глава 15

Удаленный доступ

В традиционных локальных сетях компьютеры подключены к сети посредством кабеля. Однако для каждого типа кабеля расстояние, которое может пройти сигнал без существенного ослабления, ограничено. В то же время методы удаленного доступа позволяют пользователям подключаться к сети, расположенной за тысячи километров, и работать в ней таким образом, будто они подключены посредством кабеля. В результате удаленный компьютер становится (хотя и временно) участником локальной сети.

В типичном коммутируемом соединении телефонная линия выполняет те же функции, что и кабель Ethernet в локальной сети, а модем — те же функции, что и сетевой адаптер. Единственная разница (правда, весьма существенная в практическом аспекте) состоит в том, что удаленное соединение значительно медленнее соединения посредством кабеля. Например, считающееся медленным соединение Ethernet 10BaseT имеет базовую пропускную способность 10 Мбит/с, а довольно быстрая (для телефонных каналов) линия DSL (Digital Subscribe Line) — 1,5 Мбит/с.

Удаленный доступ к сети может быть реализован также посредством беспроводных линий связи или сетей кабельного телевидения. В этой главе внимание акцентируется на коммутируемых соединениях — наиболее распространенной форме удаленного доступа.

Средства удаленного доступа позволяют расширить сеть далеко за физические границы кабельной локальной сети, практически на весь мир. Для этого необходимо лишь установить *сервер удаленного доступа*, принимающий и обслуживающий запросы, и *клиент удаленного доступа*, т.е. компьютер с программным обеспечением, поддерживающим коммутируемое соединение. Конечно, обе эти системы должны иметь в своем составе соответствующее оборудование (обычно модемы) и должны быть подключены к телефонной линии. Кроме того, на обоих компьютерах должен быть установлен один и тот же протокол.

Большинство современных операционных систем могут выполнять функции как удаленного сервера, так и удаленного клиента. Они могут даже делать это одновременно, как будто к ним подключены по два модема с двумя телефонными линиями.

Рассмотрим следующие важные аспекты реализации систем удаленного доступа:

- практическое значение удаленного доступа;
- принцип действия систем удаленного доступа;
- устройства удаленного доступа;
- конфигурирование серверов и клиентов удаленного доступа;
- безопасность соединений удаленного доступа.

Зачем нужен удаленный доступ

Технологии удаленного доступа становятся все более популярными по мере того, как возрастает мобильность пользователей, а компании увеличивают количество филиалов и предоставляют свои данные избранным заказчикам и клиентам, не публикуя их в Internet.

Перечислим некоторые наиболее распространенные области использования технологий удаленного доступа.

- Соединение филиалов компаний друг с другом и с центральным офисом.
- Предоставление сотрудникам средств связи с сетью компании в нерабочее время.
- Телекоммуникация со служащими, т.е. предоставление сотрудникам возможности частично или полностью выполнять работу дома.
- Предоставление сотрудникам, находящимся в дороге или в командировке, возможности устанавливать соединение с корпоративной сетью.
- Предоставление партнерам или клиентам компании доступа к корпоративным сетевым ресурсам.

Рассмотрим, какие преимущества предоставляют технологии удаленного доступа в каждой из этих ситуаций.

Филиалы компании

По мере нарастания в экономике процессов глобализации даже небольшим компаниям приходится открывать филиалы во многих местах. Если этим филиалам предоставить возможность сообщаться с локальной сетью в главном офисе компании, то все отделы смогут совместно пользоваться самой последней информацией и ресурсами друг друга.

Если необходимость в доступе к ресурсам друг друга возникает редко или количество сообщающихся компьютеров невелико, то оптимальным решением является коммутируемое соединение. Один из сетевых компьютеров, расположенных в главном офисе, может быть сконфигурирован как коммутируемый сервер. Посредством этого сервера пользователи, находящиеся в филиалах, смогут устанавливать с корпоративной сетью коммутируемое соединение.

Связь в нерабочее время

Для многих служащих компании рабочий день продолжается и после окончания рабочего времени. Управляющий персонал и другие служащие часто берут работу домой. Чтобы эта работа была эффективной, весьма полезно или даже необходимо получать доступ к сети компании из дома.

Используя коммутируемое соединение, служащий может установить соединение с сервером корпоративной сети и зарегистрироваться со своей обычной учетной записью. После этого он может получать доступ ко всем ресурсам, к которым имеет доступ на рабочем месте в офисе.

С помощью терминальных служб служащий может даже работать на том же персональном компьютере, на котором работал в офисе. Он может продолжить незаконченную работу с того места, где прервал ее в офисе. Для этого ему не придется носить с собой дискеты с файлами и переписывать их с одного компьютера на другой. Приложения, хранящиеся на терминальном сервере, тоже можно запускать дома, даже ес-

ли они не установлены на домашнем компьютере служащего. Более подробно терминальные службы рассматриваются в главе 17, "Сети с тонкими клиентами".

Телекоммуникация

Большое количество служащих, включая творческих и научных работников, разработчиков программного обеспечения, агентов по продажам и конторских служащих, частично или все время работают дома. Для них весьма полезными оказываются такие средства *телекоммуникации*, т.е. общения на расстоянии, как электронная почта, интерактивная беседа в реальном времени (чаты) и даже аудио- и видеоконференции.

Телекоммуникация привлекательна для служащих тем, что позволяет экономить время на дорогу до офиса и деньги, расходуемые на деловую одежду, питание в столовых и транспорт. Экономит средства и компания, так как не нужно оборудовать рабочее место, требуется меньше помещений, уменьшаются накладные расходы на освещение, отопление, уборку помещений и т.д.

Наиболее распространенный способ телекоммуникации служащих с локальной сетью компании — коммутируемый доступ, хотя в некоторых случаях используется также выделенное соединение. Если количество служащих, работающих вне офиса компании, велико, то для сервера удаленного доступа должно быть установлено несколько модемов (*модемный пул*). Тогда многочисленные соединения могут устанавливаться одновременно и служащим не придется тратить время на ожидание в очереди на соединение. Конечно, для каждого модема нужна отдельная телефонная линия, как показано на рис. 15.1.

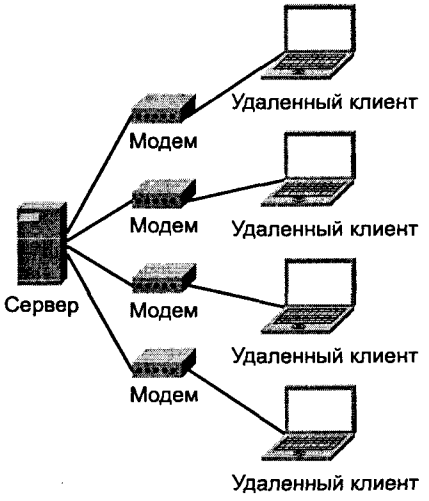


Рис. 15.1. Коммутируемый доступ многих клиентов реализуется с помощью модемного пула

Замечание

При использовании модемного пула на сервере удаленного доступа должен быть установлен адаптер COM-портов. Адаптер позволяет операционной системе распознавать многочисленные порты модемов. Многопортовые карты позволяют подключать к одному ISA- или PCI-разъему до 128 портов.

Альтернативный, более дорогой способ организации удаленного доступа — использование *виртуальных частных сетей*, которые рассматриваются в главе 16, "Виртуальные частные сети".

Мобильные пользователи

Компании стремятся продвигать свои товары на возможно более широкий рынок как внутри, так и за пределами страны, поэтому становятся все более частыми деловые поездки. Коммивояжеры, агенты по найму кадров, преподаватели, руководители предприятий все больше времени проводят в дороге. Подобно служащим, работающим на дому, им также необходима постоянная связь с сетью компании.

Было бы очень трудно или даже невозможно хранить все файлы в портативном компьютере, который можно взять с собой в дорогу. Такой способ также поставил бы под угрозу безопасность корпоративных данных, потому что портативный компьютер вместе со всем его содержимым могут украсть. Более оптимальное решение — предоставить мобильным пользователям коммутируемый доступ к локальной сети компании. Тогда вместо хранения данных на своем жестком диске мобильные пользователи смогут регистрироваться на сервере локальной сети, проходить процедуру аутентификации и получать доступ ко всем необходимым им данным (рис 15.2).

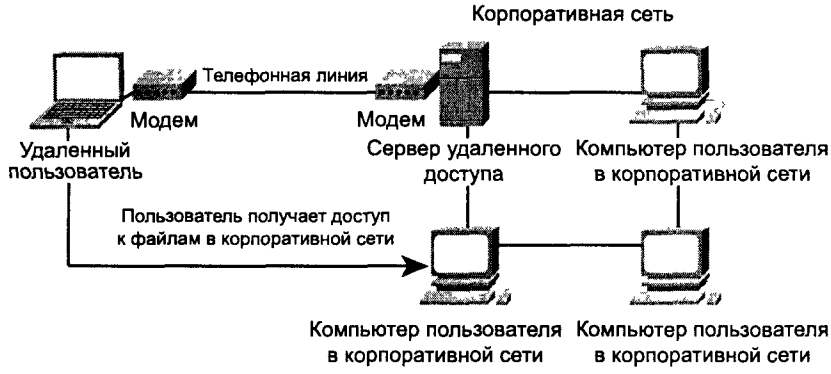


Рис. 15 2. Установив коммутируемое соединение, мобильный пользователь может получить доступ ко всем данным, к которым получает его на рабочем месте

Предоставление доступа партнерам и клиентам

Поставщики компьютерного оборудования уже давно практикуют предоставление клиентам коммутируемого доступа к своим серверам, откуда они могут выгружать последние версии драйверов. Поставщики программного обеспечения распространяют "заплатки" и обновления своих продуктов таким же образом.

Традиция предоставления клиентам (или *партнерам*, т.е. другим компаниям, с которыми заключены взаимовыгодные соглашения) коммутируемого доступа к отдельным данным корпоративной сети становится все более распространенной. Однако в целях безопасности следует продумать вопрос, предоставить ли этим "гостевым пользователям" доступ к сети с помощью общей для них учетной записи (которую обычно называют *гостевой учетной записью*) или с помощью уникальных имен пользователей и паролей. Последнее решение значительно увеличивает объем административной ра-

боты, но позволяет отслеживать, кто и когда получал доступ к сетевым ресурсам и к каким именно Анонимный доступ предпочтителен в сетях с низкими требованиями к безопасности или в том случае, когда сервер удаленного доступа отделен от остальной части внутренней сети с помощью брандмауэра

Принцип действия систем удаленного доступа

Существует несколько типов соединений удаленного доступа

- Коммутируемое соединение посредством аналоговой или цифровой телефонной линии — наиболее распространенный тип соединений удаленного доступа
- *Выделенное соединение*, представляющее собой соединение двух точек с помощью, например, линии T1 Здесь используется постоянный канал между двумя физическими точками

Замечание

Коммутируемое соединение может быть установлено посредством сети X 25 В этом типе сети клиент устанавливает коммутируемое соединение с PAD (Packet Assembler/Disassembler) Технология X 25 рассматривалась более подробно в главе 6 'Глобальные сети"

Виртуальная частная сеть представляет собой форму удаленного доступа, в которой Internet используется в качестве канала связи с удаленной частной сетью Естественно, как клиент VPN (Virtual Private Network), так и частная сеть, с которой он устанавливает соединение, должны быть подключены к Internet

Рассмотрим следующие вопросы администрирования удаленного доступа

- протоколы, используемые при удаленном доступе,
- методы аутентификации при удаленном доступе,
- как присваиваются IP-адреса для удаленных соединений TCP/IP,
- как группировать пропускные способности каналов в целях повышения производительности соединений,
- как управлять использованием пропускной способности для предотвращения чрезмерной загрузки каналов

Протоколы удаленного доступа

Удаленный клиент и удаленный сервер должны использовать, как минимум, один общий сетевой/транспортный протокол (иногда в данном случае называемый локальным протоколом), например TCP/IP, IPX/SPX, AppleTalk или NetBEUI Кроме того, для установки соединения клиентского компьютера с сервером посредством телефонной линии или Internet необходим канальный протокол (который иногда называют глобальным протоколом)

Для установки соединения удаленного доступа используются следующие канальные протоколы

- SLIP (Serial Line Internet Protocol);
- PPP (Point-to-Point Protocol).

Если соединение удаленного доступа устанавливается посредством VPN, то используются такие канальные протоколы:

- PPTP (Point-to-Point Tunneling Protocol);
- L2TP (Layer 2 Tunneling Protocol).

Канальные протоколы рассматриваются в главе 8, "Сетевые протоколы и службы".

Аутентификация удаленного доступа

Сервер удаленного доступа аутентифицирует удаленного клиента с помощью метода аутентификации, определенного администратором при конфигурировании соединения удаленного доступа (рис. 15.3).

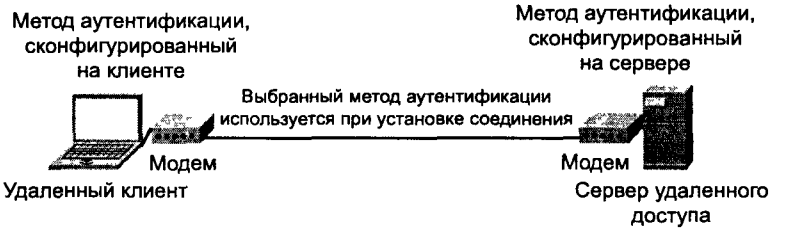


Рис. 15.3. Сервер удаленного доступа аутентифицирует удаленного клиента

Применяются следующие методы аутентификации:

- PAP (Password Authentication Protocol) — по сети передаются незашифрованные пароли;
- SPAP (Shiva PAP);
- CHAP (Challenge Handshake Authentication Protocol) — по сети передаются зашифрованные пароли;
- EAP (Extensible Authentication Protocol) — используются MD5, интеллектуальные карты или сертификаты.

Наиболее безопасен метод EAP с интеллектуальными картами. Более подробно интеллектуальные карты рассматриваются в главе 14, "Защита сети".

Замечание

Удаленные клиенты и серверы операционных систем Windows могут использовать версию CHAP, называемую MS-CHAP (Microsoft CHAP). В ней для шифрования данных используется протокол MPPE (Microsoft Point-to-Point Encryption). В версии 2 этого метода может выполняться *взаимная аутентификация*, в которой сервер передает клиенту подтверждение, что он может аутентифицировать пароль пользователя.

Служба RADIUS (Remote Authentication Dial-In User Service) обеспечивает аутентификацию удаленных пользователей и предоставляет пользователям учетные записи распределенных коммутируемых сетей. Более подробно служба RADIUS рассматривается далее в главе.

Сервер можно конфигурировать на предоставление неаутентифицированного доступа В этом случае клиенту не нужно вводить имя пользователя и пароль Если некоторым клиентам необходим доступ из операционных систем или с платформ, в которых нет средств удаленной аутентификации, то им нужно предоставлять неаутентифицированый доступ, иначе они не смогут установить соединение

Присвоение IP-адресов

Если в локальной сети используется протокол TCP/IP, то все компьютеры сети должны иметь правильные IP-адреса Это требование должно быть удовлетворено как для удаленных клиентов, так и для клиентских компьютеров, подключенных к сети посредством кабеля

Серверы удаленного доступа, например RAS (Remote Access Server) под управлением Windows 2000, можно сконфигурировать на обслуживание сервером DHCP (Dynamic Host Configuration Protocol) данной сети Тогда они будут получать IP-адреса удаленных клиентов от сервера DHCP Если в локальной сети нет сервера DHCP, то сервер RAS можно сконфигурировать со статическим пулом (набором) адресов, содержащим правильные адреса данной сети Альтернативное решение — сконфигурировать клиентские компьютеры с правильными статическими IP-адресами для удаленной сети

Если удаленный клиент и сервер используют в качестве локального протокола NetBEUI, AppleTalk или IPX/SPX, то IP-адреса им не нужны

Группировка пропускных способностей в коммутируемых соединениях

Если операционные системы клиента и сервера поддерживают *группировку пропускных способностей*, то путем объединения нескольких физических каналов (например, двух телефонных линий) можно установить соединение с повышенной пропускной способностью Обычно такой метод применяется при использовании каналов BRI (Basic Rate ISDN) с помощью двух B-каналов (каналы данных) с пропускной способностью 64 Кбит/с можно создать соединение 128 Кбит/с

Замечание

Два канала ISDN можно группировать также на аппаратном уровне

Указанный метод используется также для группировки двух модемов с пропускной способностью 56 Кбит/с (каждый из них со своей телефонной линией) Тогда пропускная способность коммутируемого соединения с провайдером услуг Internet посредством аналоговых телефонных линий может достигать 100 Кбит/с или выше (в зависимости от качества телефонных линий) Однако это возможно только при наличии у провайдера соответствующего оборудования и программного обеспечения

Управление использованием пропускной способности

При группировке пропускных способностей для управления использованием дополнительных линий применяется протокол BAP (Bandwidth Allocation Protocol) В этом случае дополнительные линии будут задействованы, только когда они нужны

Если объем передаваемых данных в единицу времени уменьшается, то одна или несколько дополнительных линий отключаются, а если объем данных увеличивается, то дополнительные линии автоматически добавляются.

Устройства соединений удаленного доступа

По сравнению с традиционными кабельными сетями производительность соединений удаленного доступа невелика. Все более популярными становятся каналы с повышенной производительностью, такие, как линии DSL (Digital Subscriber Line), однако их пропускная способность тоже относительно невелика — от 1 до 5 Мбит/с. Для сравнения: пропускная способность стандартных каналов Ethernet равна 10 или 100 Мбит/с. В главе 6, "Глобальные сети", подробно описывается применение в глобальных соединениях высокоскоростных линий DSL и кабелей.

Чаще всего удаленные соединения устанавливаются с помощью модемов по аналоговым телефонным линиям. Рассмотрим характеристики модемов и других устройств удаленного доступа.

Модемы

Модем представляет собой устройство, преобразующее цифровые сигналы компьютера в аналоговые, которые можно передавать по телефонной линии. На другом конце соединения другой модем преобразует аналоговый сигнал обратно в цифровой, чтобы он мог быть обработан принимающим компьютером (рис. 15.4). В главе 4, "Методы сетевой коммуникации", приведено описание отличий аналоговых сигналов от цифровых.

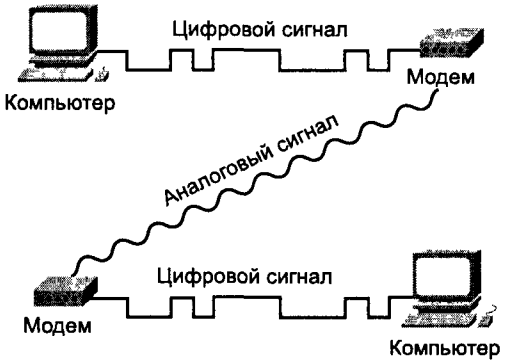


Рис. 15.4. Модемы преобразуют цифровые сигналы в аналоговые, а аналоговые — обратно в цифровые

Принцип действия модемов

Процесс преобразования аналогового сигнала в цифровой и обратно называется *модуляцией/демодуляцией* (отсюда название устройства — *модем*). Как вы помните, цифровая коммуникация основана на *двоичном* представлении данных, т.е. двоичный сигнал является или нулем, или единицей. Для передачи по телефонной линии эти сигналы должны быть преобразованы в аналоговую форму определенной частоты и амплитуды.

Когда модем пытается установить соединение с другим модемом, он передает ему по телефонной линии тональный сигнал, состоящий из быстро чередующихся тонов с низкой и высокой частотой. Каждый звуковой тон представляет 0 или 1 исходного цифрового сигнала. Если модем на принимающем конце может принять и обработать такой сигнал, то соединение устанавливается. В противном случае передающий модем пытается использовать более низкие тона. Затем еще более низкие. Этот процесс продолжается до тех пор, пока принимающий модем не сообщит передающему, что установлено надежное соединение. Таким образом модемы используют наиболее высокие частоты, обеспечивая этим максимально возможную пропускную способность.

Опытные пользователи могут определить скорость установленного соединения по высоте тонов, издаваемых модемом. Когда модем устанавливает соединение пользователь слышит характерный сигнал "приветствия модемов", завершающий процесс переговоров.

Асинхронные коммуникационные порты

В аналоговых модемах используется метод *асинхронной коммуникации*, который описывался в главе 4, "Методы сетевой коммуникации". В системные платы современных компьютеров встроены COM-порты, поддерживающие асинхронную коммуникацию. Обычно в компьютере есть два COM-разъема — 9- и 25-контактный. Если в компьютере есть только один из них, а модем рассчитан на другой, то можно использовать специальный переходник. Внешний модем подключается к одному из этих последовательных портов с помощью последовательного кабеля.

Портами COM управляют микросхемы UART (Universal Asynchronous Receiver/Transmitter). Пропускная способность порта определяется типом микросхемы UART. Более старые микросхемы UART 8259 имеют пропускную способность 9 600 бит/с, UART 16450 — 115 200 бит/с, а UART 16550 — 230 400 бит/с.

Во внутренние модемы встроены свои микросхемы UART, поэтому их пропускная способность не ограничивается микросхемами UART COM-портов.

В старых модемах для связи с телефонной линией использовался *акустический соединитель*, представлявший собой устройство, в которое вставлялась телефонная трубка. Эти модемы не могли набирать номер, его приходилось набирать вручную на телефонном аппарате. Их пропускная способность крайне низкой — модем на 2 400 бит/с считался очень быстрым. Первые совершенные модемы, способные набирать номер вместо пользователя, выпустила на рынок компания Hayes.

Еще одним недостатком старых модемов была сложность их конфигурирования. Для этого нужно было написать специальный сценарий — *строку инициализации модема*. Эта строка, представлявшая собой последовательность символов, устанавливала параметры метода, с помощью которого связывались два модема.

Современные модемы обладают большей пропускной способностью — от 14,4 до 56 Кбит/с. Акустические соединители все еще существуют, они применяются когда телефонный провод заделан в стену таким образом, что подключить к нему модем невозможно.

Типы модемов

Большинство современных модемов принадлежат к одному из трех типов.

- Внутренние.
- Внешние.

- PC Card (PCMCIA).

Модемы каждого типа подключаются к телефонной линии с помощью стандартного телефонного гнезда RJ-11. Каждый из этих типов имеет свои преимущества и недостатки. Рассмотрим их подробнее.

Внутренние модемы

Как видно из названия, внутренние модемы находятся внутри компьютера. Конструктивно внутренний модем — это плата, вставляемая в разъем на системной плате компьютера. Модемы могут подключаться к разъему шины ISA или PCI. Кроме того, для портативных компьютеров разработаны внутренние модемы в виде плат PCMCIA/PC Card.

Внутренние модемы не загромождают рабочее место, однако для их установки нужно открывать компьютер. В общем случае внутренние модемы немного дешевле, чем внешние с такими же характеристиками.

Для конфигурирования внутреннего модема нужно с помощью перемычек установить IRQ и адреса ввода-вывода. Этот процесс напоминает конфигурирование сетевого адаптера, которое описано в главе 7, "Физические компоненты сетей". Модем должен быть сконфигурирован на использование одного из свободных COM-портов. Необходимо учитывать, что, кроме модемов, COM-порты используются многими устройствами: сканерами, устройствами указания, гнездами для портативных компьютеров и др. При использовании модема на компьютере должны быть также установлены его программные драйверы.

Если модем, система BIOS и операционная система поддерживают метод PnP (Plug and Play), то конфигурировать модем вручную не нужно.

Внешние модемы

Обычно внешние модемы стоят немного дороже, чем внутренние, однако они обладают некоторыми преимуществами.

- Для установки внутреннего модема не нужно открывать компьютер. Разъем модема подключается к COM-порту с помощью последовательного кабеля. Новейшая разработка — модемы USB — подключаются к порту или концентратору USB.
- Для внешнего модема используются IRQ и адрес ввода-вывода, присвоенные тому последовательному порту, к которому подключен модем, т.е. эти параметры уже сконфигурированы. Поэтому конфигурировать внешний модем проще, чем внутренний. Однако, если для внутреннего модема используется технология PnP, это преимущество внешнего модема сводится к нулю.
- На передней панели внешних модемов обычно есть световые индикаторы, или *индикаторы состояния*. С их помощью можно увидеть, подключен ли модем, принимает ли (или передает) данные и т.д. У некоторых внешних модемов тоже есть световые индикаторы, но они обычно не видны, так как расположены на задней стенке компьютера.

Как и для внутреннего модема, для внешнего должны быть установлены программные драйверы, позволяющие ему сообщаться с операционной системой. Драйверы наиболее популярных моделей модемов, например компаний Motorola и U.S. Robotics обычно входят в поставку операционных систем.

Модемы PC Card

Модемы PC Card (другое их название — модемы PCMCIA) представляют собой карточки, вставляемые в щель на корпусе портативного компьютера Иногда они используются и в настольных компьютерах Модемы PC Card конфигурируются аналогично модемам других типов Большим преимуществом модемов PC Card является их малый размер, вследствие чего их легко перенести с одного компьютера на другой

Установка параметров модема

В зависимости от типа модема и операционной системы, пользователь может также настраивать следующие свойства

- возможность регулировки громкости (или набор номера вообще беззвучно),
- установка кода города, что понадобится модему при наборе номера абонента, расположенного в другом городе,
- возможность установки режима автоматического разрыва соединения, если в течение определенного времени оно не используется,
- установка количества повторных автоматических вызовов (оно может быть также равным нулю), если номер вызываемого абонента занят,
- установка пропускной способности COM-порта, к которому подключен модем

В дружественных к пользователю операционных системах, таких, как Windows 2000, сконфигурировать свойства коммутируемого соединения несложно (рис 15 5)

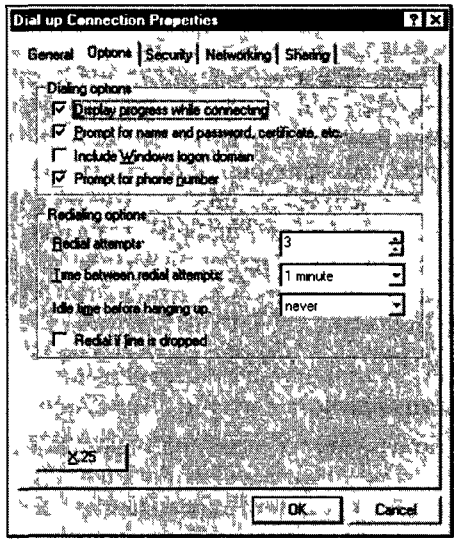


Рис 15 5 В Windows 2000 режим работы модема конфигурируется в диалоговом окне Dial-up Connection Properties (Своиства коммутируемого соединения)

Устранение неполадок при работе с модемами

При работе с модемами могут возникать самые разные проблемы. Например, модем не набирает номер, или скорость передачи чрезвычайно низка, или модем часто отключается. В состав программного обеспечения, поставляемого с модемами, обычно включены утилиты диагностики, с помощью которых модем можно тестировать. Кроме того, утилиты диагностики модемов и устранения неполадок включены в состав некоторых операционных систем, таких, как Windows 2000.

Теперь рассмотрим возможные проблемы с модемами:

- модем не набирает номер;
- модем набирает номер, однако соединение не устанавливается;
- модем устанавливает соединение, но затем оно разрывается;
- устанавливается соединение с низкой скоростью передачи;
- некоторые проблемы с COM-портом, влияющие на работу модема.

Модем не набирает номер

Если модем не набирает номер, то, скорее всего, программное обеспечение компьютера не сообщается с модемом. Одной из причин может быть то, что операционная система не распознает COM-порт, к которому подключен модем. Еще одна возможная причина — конфликт между COM-портом внутреннего модема и другим устройством последовательного доступа, использующим тот же IRQ, что и COM-порт. Неполадку устраняет изменение параметров COM-порта в BIOS или присвоение COM-порту другого номера IRQ.

Отсутствие связи между операционной системой и модемом может быть вызвано также тем, что не установлены драйверы модема, установлены неправильные (чужие) драйверы или испорчены файлы драйверов. Устранить эту неполадку можно путем повторной установки правильных драйверов.

Если и после этого модем, сконфигурированный на ожидание тонального сигнала перед набором, не набирает номер, то, возможно, проблема в телефонной линии.

И наконец, возможна такая забавная причина неполадки: разъем модема не вставлен в гнездо телефонной линии. Обратите внимание: во многих модемах используются *два* разъема RJ-11, причем выглядят они одинаково. Один из них должен быть вставлен в гнездо телефонной линии, а другой — в гнездо телефонного аппарата. Поэтому нужно убедиться, что разъемы модема подключены правильно.

Не устанавливается соединение

Если модем набирает номер, значит, причина неполадки не в телефонной линии и не в кабелях от линии к модему. Наиболее частая причина — набор модемом неправильного номера. Необходимо проверить, правильный ли номер набирает модем и включен ли в номер код города, в котором расположен вызываемый абонент.

Еще одна возможная причина — вызываемый номер занят. Если динамик модема включен, то можно услышать короткие сигналы, указывающие на занятость линии. Модем можно сконфигурировать на многократное автоматическое повторение набора в случае получения сигналов о занятости линии.

Если другой модем ответил, однако соединение не устанавливается, то, возможно, несовместимы типы модемов. Еще одна причина — скорость передачи данных вызы-

вающего модема установилась выше, чем может принять вызываемый модем. В этом случае нужно установить более низкую скорость порта модема.

Соединение разрывается

Если соединение с модемом на другом конце установилось, но тут же разорвалось, то, возможно, сервер удаленного доступа не смог аутентифицировать учетную запись. Необходимо проверить, правильно ли в свойствах коммутируемого соединения установлены имя пользователя и пароль.

Возможно также, что на удаленном сервере для данной учетной записи установлен режим безопасности с обратным вызовом. В этом случае сервер после ввода имени пользователя и пароля разрывает соединение, однако после этого немедленно передает обратный вызов и восстанавливает соединение. Необходимо проверить, сконфигурирован ли модем на прием сообщений. Более подробно режим с обратным вызовом рассматривается далее в главе.

Если соединение установилось, модем некоторое время поработал, а затем соединение разорвалось, то, возможно, телефонная линия зашумлена Если это повторяется, нужно обратиться в телефонную компанию, которая должна соответствующим образом наладить линию.

Если модем работает в режиме ожидания звонков, то при поступлении вызова от другого абонента соединение разрывается. Режим ожидания звонков можно отключить в диалоговом окне свойств коммутируемого соединения

Если используется спаренный телефон и кто-либо поднимает трубку телефона, подключенного к этой же линии, то соединение может разорваться. Чтобы предотвратить такие разрывы, нужно приобрести и подключить к телефонной линии специальное устройство.

Если разрыв соединения с провайдером услуг Internet происходит через регулярные интервалы времени, то, возможно, программное обеспечение провайдера сконфигурировано на ограничение максимального времени соединения. В этом случае по истечении определенного промежутка времени, например шести часов, пользователь автоматически отключается. Этот вопрос должен быть согласован с провайдером. Однако во многих случаях разрешен повторный набор и установка соединения с Internet немедленно после разрыва.

Устанавливается низкая скорость передачи

Низкая скорость передачи может быть обусловлена помехами в телефонной линии. В некоторых регионах модем с максимальной пропускной способностью 56 Кбит/с может обеспечить скорость передачи не более 30—50 Кбит/с.

Еще одна возможная причина низкой скорости передачи может состоять в том, что модем на другом конце соединения не поддерживает высокую скорость. Если на другом конце модем имеет максимальную скорость 28,8 Кбит/с, то на этом конце модем с пропускной способностью 56 Кбит/с сможет обеспечить лишь 28,8 Кбит/с.

Иногда возникают проблемы совместимости модемов. Первые модемы на 56 Кбит/с выпускались двух видов· 56Kflex, поддерживаемые такими поставщиками, как Motorola, и X2 компании U.S Robotics. Современные модемы поддерживают общий стандарт, но если у вас установлен более старый модем, то для решения проблемы несовместимости необходимо обновить BIOS модема

Еще одной причиной низкой скорости соединения могут быть неправильные или устаревшие драйверы модема. Последние версии драйверов обычно можно загрузить с Web-узла производителя модема.

Для внешнего модема причиной низкой скорости или даже невозможности установить соединение может быть некачественный кабель модема Возможно также, что сам модем неисправен и его нужно заменить

Неполадки в COM-порте

В некоторых случаях проблема заключена не в самом модеме, а в COM-порте, к которому он подключен Если скоростной модем устанавливает соединение с низкой скоростью (например, 9 600 бит/с), то следует проверить микросхему UART порта

Иногда, даже если COM-порт использует высокоскоростную микросхему UART, в операционной системе может оказаться низкой скорость порта, установленная по умолчанию На рис 15 6 показана установка скорости порта в диалоговом окне Windows 2000

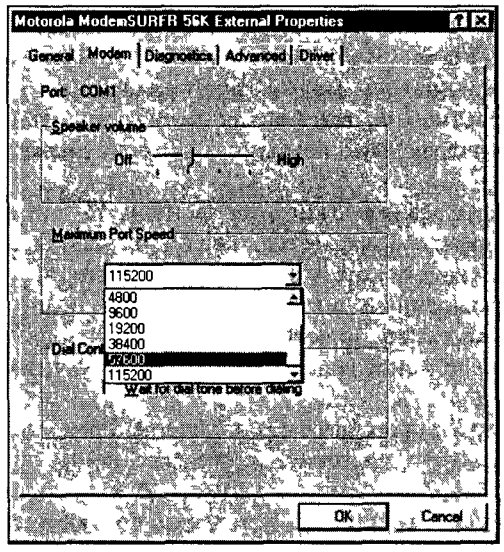


Рис 15 6 В Windows 2000 скорость порта можно изменить в диалоговом окне свойств модема

Терминальные адаптеры ISDN

Терминальные адаптеры ISDN (Integrated Services Digital Network) иногда называют модемами ISDN, однако такой термин не совсем точен, потому что они не модулируют и не демодулируют сигнал — линия ISDN сама является цифровой

Адаптеры ISDN выпускаются главным образом теми же компаниями, что и модемы Аналогично модемам, они также поставляются во внутреннем и внешнем исполнении Большинство из них используют один или два B-канала с пропускной способностью 64 Кбит/с Обычно двум линиям присвоены разные телефонные номера, даже если их провода объединены в один кабель

Адаптер ISDN устанавливается аналогично модему Для него должен быть установлен и сконфигурирован программный драйвер Для некоторых адаптеров нужно ввести номера *SPID* (*Service Profile Identifier — идентификатор услуги и линии*) для обеих линий В зависимости от модели адаптера, может понадобиться установка и других параметров

Замечание

Номер SPID представляет собой 10-значный телефонный номер, к которому может быть присоединен префикс или суффикс, идентифицирующий параметры линии. Номера SPID присваиваются телефонной компанией.

Для обеспечения доступа к Internet из всей локальной сети можно использовать маршрутизаторы ISDN. В этом случае провайдер услуг Internet может присвоить всем компьютерам сети блок IP-адресов. Альтернативное решение — отображать частные внутренние адреса на один зарегистрированный публичный адрес с помощью программы трансляции адресов (Network Address Translation — NAT). В этом случае маршрутизатор не нужен. Реализация системы NAT рассматривалась в главе 6, "Глобальные сети".

При использовании ISDN наиболее распространенная неполадка — подключение только одной линии из двух. В этом случае нужно проверить, правильно ли сконфигурировано программное обеспечение на поддержку многоканального соединения.

К большинству адаптеров ISDN можно подключать аналоговый телефонный аппарат и устанавливать голосовую связь. Адаптер можно сконфигурировать на подключение к Internet с пропускной способностью 128 Кбит/с таким образом, что при поступлении по одной из линий запроса на голосовую связь скорость соединения с Internet снижается до 64 Кбит/с и остается такой на протяжении разговора. По окончании разговора вторая линия автоматически подключается и скорость связи с Internet вновь повышается до 128 Кбит/с.

Кабельные модемы

Это устройство фактически является интерфейсом локальной сети. Посредством этого модема компьютер сообщается с сетью кабельной компании по тому же коаксиальному кабелю, по которому на телевизор передаются сигналы кабельного телевидения.

В отличие от аналоговых модемов и адаптеров ISDN кабельные модемы обеспечивают доступ только к Internet. Если установлен аналоговый модем или адаптер ISDN, то пользователь может установить соединение с любым провайдером или сервером удаленного доступа любой частной сети. В то же время кабельный модем непосредственно подключен только к кабельной сети. Единственный провайдер, с которым можно установить соединение — провайдер кабельной компании.

Кабельный модем подключен к сети постоянно. Однако если инфраструктура кабельной компании обеспечивает только односторонний режим передачи, то для передачи запросов от пользователя необходимо дополнительно устанавливать коммутируемое соединение. Более подробно этот вопрос рассматривается в главе 6, "Глобальные сети".

Даже если сервер, с которым устанавливается соединение, расположен далеко, доступ с помощью кабельного модема все равно больше напоминает непосредственное соединение в локальной сети, чем удаленный доступ. Хорошо запомните это, потому что дальше в главе рассматриваются методы удаленного доступа, служащие той же цели.

Замечание

Некоторые кабельные компании предоставляют или планируют предоставить телефонные услуги посредством этой же сети кабельного телевидения.

Аналогично адаптерам ISDN и аналоговым модемам, кабельные модемы бывают внутренние и внешние. Обычно кабельная компания однозначно определяет, какой тип модема должен быть установлен. Часто компания даже заставляет пользователя устанавливать лишь тот модем, который она ему продает или сдает в аренду.

Внешний кабельный модем представляет собой небольшую коробочку, к которой подключается коаксиальный телевизионный кабель. Для подачи сигнала одновременно на модем и на телевизор используется разветвитель. С другой стороны внешний модем подключается к сетевому адаптеру Ethernet, установленному в компьютере, посредством стандартной витой пары. Некоторые типы внешних модемов могут подключаться к порту USB компьютера, адаптер Ethernet в этом случае не нужен.

Внутренние кабельные модемы представляют собой электронные платы, помещаемые в разъем на системной плате компьютера. Они дешевле внешних, однако работать могут не с любой сетью кабельного телевидения. Кроме того, внутренний модем нельзя установить в портативный компьютер или Macintosh.

В состав кабельного модема входит тюнер с встроенным дуплексером — устройством двусторонней передачи сигналов. Однако инфраструктура некоторых кабельных телевизионных компаний поддерживает только одностороннюю передачу — от провайдера к пользователю. В этом случае запросы от пользователя должны передаваться по телефонной линии. Для этого в некоторые типы кабельных модемов встроен телефонный разъем.

Кабельный модем принимает цифровые модулированные сигналы. Для их обработки в модем встроен демодулятор. Если модем работает в двустороннем режиме, то для передачи сигналов от компьютера используется пакетный модулятор. В состав внешнего модема входит процессор. В то же время внутренние модемы, как и аналоговые модемы типа Winmodem, передают сигналы на обработку процессору компьютера.

К сожалению, сложилось так, что за лидерство конкурируют несколько стандартов кабельного доступа. Пока один из них не станет несомненным лидером, от кабельной компании будет существенно зависеть как техническая реализация конкретной системы, так и ее конфигурация, производительность, надежность и набор предоставляемых услуг.

Хороший учебник по кабельным модемам со многими техническими подробностями можно найти на Web-узле по адресу: `www.cable-modems.org/tutorial/index.htm`.

Устройства CSU/DSU

Устройства CSU/DSU (Channel Service Unit/Data Service Unit — модуль обслуживания канала/модуль обслуживания данных) применяются при использовании арендуемых цифровых линий (T-носителей). Они преобразуют пакеты цифровых данных локальной сети в формат соединений глобальных сетей. Конструктивно устройство CSU/DSU похоже на внешний модем или терминальный адаптер ISDN.

Устройства CSU/DSU должны быть установлены на обоих концах соединения. Устройство CSU защищает линию T-1 от электрических помех. Оно используется также для обратной передачи тестовых сигналов в процедуре *петлевого контроля*, проводимой телефонными компаниями. Устройство DSU предназначено для контроля ошибок синхронизации и регенерации сигналов. Оно преобразует сигналы данных компьютера к виду, пригодному для передачи по линии. Устройство CSU/DSU подключается к компьютеру посредством интерфейса DTE (Data Terminal Equipment).

Конфигурирование клиентов и серверов удаленного доступа

Чтобы компьютер мог работать в кабельной сети, его нужно соответствующим образом сконфигурировать. Аналогично этому, должны быть сконфигурированы и системы, сообщающиеся друг с другом с помощью средств удаленного доступа. Рассмотрим, как сконфигурировать удаленного клиента на установку соединения и как сконфигурировать сервер удаленного доступа на обработку запроса на соединение.

Конфигурирование клиента удаленного доступа

Прежде чем набрать телефонный номер и установить соединение с сервером удаленного доступа (например, с коммутируемым сервером провайдера или с сервером RAS частной компании), необходимо сконфигурировать компьютер как клиентский компьютер (клиент) удаленного доступа. Для этого выполните ряд действий.

1. Установите соответствующее устройство (обычно аналоговый модем).
2. Установите и сконфигурируйте программные драйверы этого устройства.
3. Подключите устройство к телефонной линии.
4. Сконфигурируйте свойства коммутируемого соединения — набираемый телефонный номер, имя пользователя и пароль для доступа к удаленному серверу, тип протокола (PPP или SLIP) и другие параметры.

В состав некоторых операционных систем (например, Windows 9*x* и Windows 2000) включены мастера, облегчающие процесс установки свойств коммутируемого соединения (рис. 15.7).

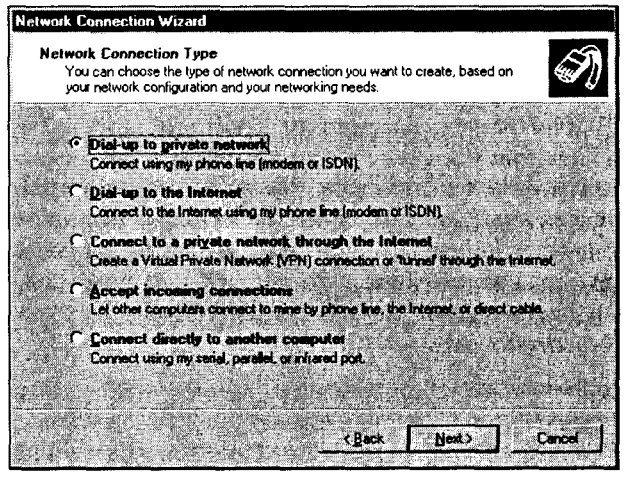


Рис. 15.7. Мастер сетевых соединений проводит пользователя по этапам установки свойств нового коммутируемого соединения

Конфигурирование сервера удаленного доступа

Удаленный сервер должен быть оборудован модемом или модемами и сконфигурирован на прием и обработку входных звонков. Процесс конфигурирования зависит от типа операционной системы.

При использовании сервера удаленного доступа необходимо ответить на ряд вопросов, в зависимости от которых могут изменятся конфигурационные параметры сервера.

- Должен ли сервер устанавливать многоканальные соединения PPP?
- Должен ли сервер динамически управлять использованием пропускной способности с помощью протокола BAP (Bandwidth Allocation Protocol — протокол распределения пропускной способности)? Этот параметр доступен, только если включен режим многоканальных соединений.
- Должна ли быть включена маршрутизация IP? Если используется локальный протокол, отличный от TCP/IP, то к чему следует предоставить доступ — только к серверу или ко всей сети?
- Если используется TCP/IP, то откуда сервер будет брать IP-адреса — из статического пула (набора) адресов или от сервера DHCP?
- Какой метод аутентификации будет использоваться для установки удаленных соединений?

Для управления доступом на основе групп пользователей должны быть разработаны определенные правила предоставления удаленного доступа.

Безопасность удаленного доступа

Независимо от того, устанавливаете ли вы соединение с Internet к качестве коммутируемого клиента или открываете свой сервер удаленного доступа, вы подключаетесь к внешнему миру, а это всегда связано с некоторым риском для безопасности вашей информации.

В главе 14, "Защита сети", были рассмотрены общие аспекты безопасности соединений с Internet. В этом разделе рассмотрим некоторые специальные вопросы безопасности, возникающие при установке в сети коммутируемого сервера

Предоставляя удаленным пользователям доступ к сети, необходимо позаботиться о повышении ее безопасности. Существует несколько способов достижения этой цели. Сочетая меры безопасности с управлением правами доступа к разделяемым файлам и ресурсам, можно поддерживать безопасность сети на должном уровне, не лишая пользователей удобств и преимуществ удаленного доступа. Рассмотрим наиболее распространенные меры безопасности:

- метод обратного вызова;
- служба RADIUS;
- правила удаленного доступа;
- блокировка учетных записей;
- хосты безопасности.

Метод обратного вызова

При использовании этой меры безопасности сервер удаленного доступа устанавливает соединения только с теми абонентами, чей телефонный номер входит в ограниченный список. Если включен режим обратного вызова, то сервер не верит регистрационной информации (имени пользователя и паролю), введенной пользователем. Рассмотрим это на следующем примере. Допустим, вам позвонили из полиции по какому-либо вопросу, однако у вас возникло сомнение, действительно ли с вами говорят из полицейского участка. Чтобы проверить это, вы можете попросить вашего собеседника сообщить номер его телефона и номер полицейского участка. Проверив номер по телефонному справочнику, вы можете через минуту перезвонить ему и продолжить разговор. Аналогично этому, сервер проверяет аутентичность пользователя, запрашивающего удаленный доступ (рис. 15.8).

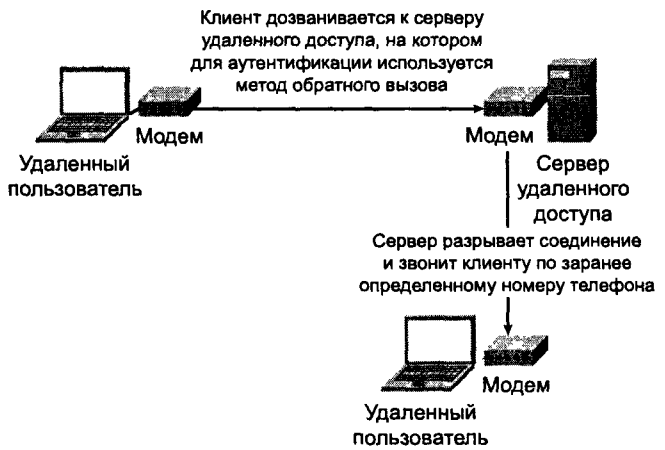


Рис. 15.8. При использовании метода обратного вызова список телефонных номеров, с которых удаленный пользователь может установить соединение, ограничен

Метод обратного вызова работает следующим образом.

1. При конфигурировании сервера удаленного доступа в качестве параметров вводится предопределенный список телефонных номеров с учетными записями пользователей.
2. Когда пользователь набирает номер сервера, он вводит имя пользователя и пароль. По ним сервер идентифицирует пользователя и проверяет его учетную запись.
3. Сервер разрывает соединение и немедленно после этого набирает телефонный номер пользователя, взятый из предопределенного списка. Получив ответ пользователя по этому номеру, сервер предоставляет ему доступ к сети.

Благодаря такой процедуре злоумышленник, даже если выведает имя пользователя и пароль, не сможет получить удаленный доступ. Конечно, если он не звонит из дома или с рабочего места пользователя либо не подключился к телефонной линии пользователя.

Служба RADIUS

Протокол RADIUS стал фактическим промышленным стандартом аутентификации коммутируемых пользователей. Он используется коммутируемыми серверами провайдеров услуг Internet для обслуживания учетных записей пользователей. Коммутируемый сервер конфигурируется как клиент службы RADIUS, регистрационная информация (имя пользователя и пароль) передаются коммутируемым сервером на сервер RADIUS. На основе этой информации сервер RADIUS выполняет аутентификацию пользователей.

Сервер RADIUS выполняет централизованную аутентификацию с помощью одного из следующих протоколов:

- PAP (Password Authentication Protocol);
- CHAP (Challenge Handshake Authentication Protocol) и MS-CHAP;
- EAP (Extensible Authentication Protocol);
- DNIS (Dialed Number Identification Service — служба идентификации набранного номера);
- Служба ANI (Automatic Number Identification — автоматическая идентификация номера).

Первые три из этих методов рассмотрены выше в главе. Работа DNIS основана на номере, набранном пользователем, а ANI — на номере, с которого звонит пользователь.

Служба RADIUS обеспечивает запись аудитной информации в журнал, использование этой информации и управление доступом ко всем серверам сети из одного центра. Работа службы RADIUS специфицирована документами RFC 2138 и RFC 2139.

Стратегия удаленного доступа

Управление доступом осуществляется путем создания и применения *стратегии удаленного доступа*, зависящей от типа операционной системы. Стратегия определяет правила предоставления доступа или отказа в доступе на основе следующих критериев:

- время дня (например, удаленный доступ может предоставляться только с 8.00 до 18.00);
- день недели (например, доступ может предоставляться только с понедельника по субботу, но не в воскресенье);
- членство в группе (например, можно установить отказ в доступе всем членам группы `Newbies`);
- тип удаленного соединения (например, можно разрешить соединения VPN и запретить коммутируемые соединения и наоборот).

Стратегия может также ограничивать время жизни соединения или используемые методы аутентификации.

Блокировка учетных записей

В соединениях удаленного доступа блокировка учетных записей может применяться для предотвращения взлома пароля несанкционированным пользователем путем последовательного перебора разных паролей вручную или программно методом грубой силы.

Если включен режим блокировки учетных записей, то после определенного количества неудачных попыток зарегистрироваться сервер отказывается обрабатывать дальнейшие попытки Метод блокировки учетных записей конфигурируется одним из приведенных ниже способов

- Можно установить допустимое количество неудачных попыток Пользователь может ошибиться при вводе пароля один или даже два раза, однако вряд ли он будет непрерывно и многократно вводить неправильные пароли Поэтому рекомендуется установить допустимое количество попыток равным 3
- Можно задать, будет ли учетная запись автоматически разблокирована по истечении определенного промежутка времени или останется заблокированной, пока ее не разблокирует администратор Промежуток времени должен быть небольшим, например 2 часа, чтобы после блокировки действий злоумышленника смогли зарегистрироваться законные пользователи

Хосты безопасности

Хост безопасности представляет собой устройство, используемое для аутентификации коммутируемых пользователей Он применяется дополнительно к собственным мерам безопасности сервера удаленного доступа Устройство хоста устанавливается между клиентом удаленного доступа и сервером

Существует несколько типов хостов безопасности Для некоторых хостов пользователь должен вводить имя и пароль, отличающиеся и не зависящие от имени пользователя и пароля, используемых для регистрации на сервере удаленного доступа Компания Security Dynamics поставляет модемы SecurID, представляющие собой модемы PC Card, с помощью которых выполняется автоматическая аутентификация мобильных пользователей Пользователь вводит номер PIN (Personal Identification Number) Если номер PIN введен правильно, то модем автоматически передает регистрационную информацию на хост безопасности для проверки

Резюме

В этой главе рассмотрены средства и методы удаленного доступа, приобретающие все большую популярность в современном деловом мире Приведен обзор ситуаций, в которых применение удаленного доступа оказывается весьма полезным К таким ситуациям относятся соединение филиалов компании с центральным офисом и друг с другом, предоставление работникам компании доступа к сети в нерабочее время, телекоммуникация, предоставление доступа к сети мобильным пользователям и предоставление сетевых данных компании ее партнерам и клиентам

Рассмотрены принцип действия средств удаленного доступа и используемые при этом протоколы Вы узнали, что удаленный клиент и сервер должны использовать, как минимум, один общий сетевой/транспортный протокол и что для установки соединения по телефонной линии используется канальный протокол PPP или SLIP

Были описаны различные методы аутентификации удаленных клиентов, включая PAP, SPAP, CHAP, MS-CHAP и EAP Вы узнали, что сервер DHCP присваивает IP-адреса коммутируемым клиентам и что сервер удаленного доступа можно сконфигурировать со статическим пулом адресов, из которого клиенты получают адреса

Рассмотрено группирование пропускных способностей каналов с помощью многоканального протокола PPP и на уровне оборудования. При использовании любого из этих методов пропускные способности двух или большего количества линий объединяются, образуя высокоскоростное соединение. Описан также протокол BAP, применяемый для динамического управления пропускной способностью такого соединения.

Затем был приведен обзор устройств удаленных соединений, включая модемы, терминальные адаптеры ISDN, кабельные модемы и устройства CSU/DSU. Вы узнали, что модемы осуществляют модуляцию и демодуляцию сигналов, т.е. преобразование цифровых сигналов в аналоговые и наоборот. Рассмотрены основные характеристики трех типов модемов: внутренних, внешних и PCMCIA. Описана настройка параметров модемов и устранение неполадок, возникающих при работе с ними.

Кроме того, рассмотрено конфигурирование клиентов и серверов удаленного доступа. В конце главы представлены некоторые вопросы безопасности соединений удаленного доступа. Вы узнали, что существует довольно много различных мер обеспечения безопасности, включая метод обратного вызова, службу RADIUS, стратегию удаленного доступа, блокировку учетных записей и хосты безопасности.

В этой главе были рассмотрены методы коммутируемого доступа. В следующей главе внимание акцентируется на другом типе удаленного доступа — виртуальных частных сетях.

Рекомендуемые источники

Основательное обсуждение модемов можно найти по адресу: `www.teleport.com/~curt/modems.html`.

Полезную информацию и ссылки на дополнительные источники по службе RADIUS можно найти на Web-узле RADIUS Resources по адресу: `www.funk.com/radius`.

Начальная страница рабочей группы IETF, посвященная службам RADIUS, находится по адресу: `www.ietf.org/html.charters/radius-charter.html`.

Документ RFC 2284, специфицирующий протокол EAP, приведен по адресу: `www.rfc-editor.org/rfc/rfc2284.txt`.

Организация 3Com предоставляет хороший источник информации о протоколах BAP и многоканальном PPP на Web-узле по адресу: `infodeli.3com.com/infodeli/tools/isdn/mlppp/mlppp.htm`.

Информация о программном обеспечении Shiva, предназначенном для управления безопасностью удаленного доступа, приведена по адресу: `www.shiva.com/images/t-products.gif`.

Обширная информация по вопросам безопасности удаленного доступа приведена по адресу: `www.list.gmu.edu/ras.htm`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Что из приведенного используется для обеспечения коммутируемого доступа многих клиентов одновременно?

а. Многоканальная связь.

б. Протокол BAP.

в. Пул модемов.

г. Устройства CSU/DSU.

2. Какой тип соединений удаленного доступа наиболее распространен?

а. Выделенное цифровое соединение.

б. Коммутируемое аналоговое соединение.

в. Коммутируемое цифровое соединение.

г. Беспроводное соединение

3. Что из приведенного является канальным протоколом, используемым для установки соединения посредством телефонных линий? (Выберите все, что подходит.)

а. SLIP.

б. IPX/SPX.

в. NetBEUI.

г. PPP.

4. В каком из приведенных методов аутентификации по сети передается незашифрованный пароль?

а. CHAP.

б. PAP.

в. EAP

г. SPAP.

5. Что используется для обеспечения соединения ISDN с пропускной способностью 128 Кбит/с?

а. Протокол BAP.

б. Протокол PPP.

в. Многоканальный протокол PPP.

г. Широковещание

6. Как называется процедура, выполняемая модемами в процессе переговоров об установке соединения?

а. Обратная настройка

б. Группирование на уровне оборудования.

в. Ремодуляция.

г. Обратный вызов

7. Как называется микросхема, на основе которой работает COM-порт?

а. USB.

б. UART.

в. UNC.

г. UDP

8. Что из приведенного является преимуществом внутреннего модема по сравнению с внешним?

а. Внутренний модем легче установить.

б. Проще узнать состояние внутреннего модема.

в. Внутренний модем дешевле.

г. У внутреннего модема нет преимуществ.

9. Что из приведенного является частой причиной низкой скорости модема? (Выбрать все, что подходит.)

а. Неправильный ввод имени пользователя и пароля.

б. Вызов поступил по телефонной линии, к которой подключена служба ожидания звонка.

в. Телефонная линия зашумлена.

г. Модем несовместим с модемом на другом конце соединения.

10. Что из приведенного является средством централизованной аутентификации, обслуживания учетных записей и управления доступом к серверам?

а. NAT.

б. RADIUS.

в. RAID.

г. RARP.

Глава 16

Виртуальные частные сети

В главе 15, "Удаленный доступ", рассматриваются методы установки коммутируемых соединений, однако это не единственная форма удаленного доступа. Еще одно интересное средство установления удаленного доступа — *виртуальные частные сети* (*Virtual Private Network — VPN*). По мере того как поставщики программного обеспечения упрощают их реализацию, а корпорации открывают для себя их преимущества, популярность виртуальных частных сетей быстро растет.

В данной главе подробно рассматривается эта полезная, высокорентабельная форма удаленного доступа. Вы узнаете, что такое виртуальная частная сеть и как она работает. Будут представлены протоколы, используемые для установки VPN и описаны важные аспекты безопасности VPN. Кроме того, рассматриваются типы VPN, способы их реализации и приводится практический пример конфигурирования соединения VPN.

Что такое VPN

Каждое из слов термина "виртуальная частная сеть" является основополагающим в концепции VPN. *Сеть* — это компьютеры, сообщающиеся друг с другом. Понятия *виртуальная* и *частная* определяют, чем виртуальная частная сеть отличается от других типов сетей.

Виртуальная сеть

До сих пор рассматривались локальные и глобальные компьютерные сети. Общим для них является то, что они используют некоторый *носитель* (кабель или беспроводный канал), непосредственно объединяющий компьютеры сети. В виртуальной сети нет такого непосредственного носителя. Для нее создается туннель в публичной сети (обычно в Internet), посредством которого сообщаются компьютеры VPN (рис. 16.1).

Данные передаются по публичной сети методом эмуляции соединения от точки к точке, реализуемым путем *инкапсуляции* данных. Далее в главе рассмотрим, как выполняется процесс инкапсуляции. Сейчас нужно знать лишь то, что VPN создает логическую сеть, независимую от географического расположения компьютеров и непосредственных физических соединений.

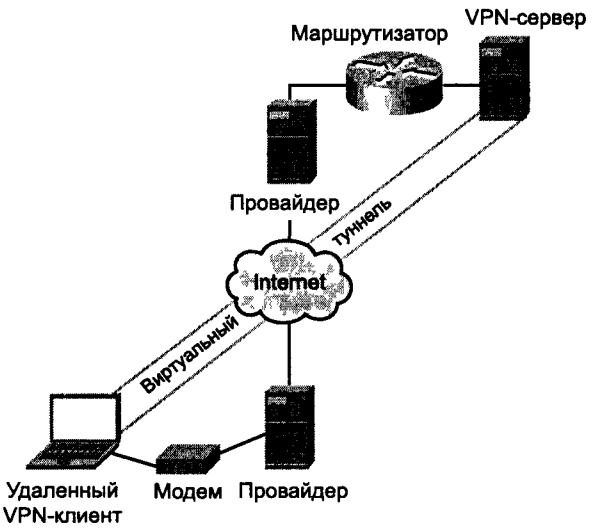


Рис. 16 1. Соединение VPN представляет собой туннель в какой-либо публичной сети, например в Internet

Частная сеть

Конфиденциальность передаваемой по VPN информации обеспечивается шифрованием данных, передаваемых по публичной сети. По туннелю (установленному с помощью одного из протоколов туннелирования, рассматриваемых далее в главе) можно передавать и незашифрованные данные, однако, строго говоря, таким образом создается только виртуальная сеть, но не виртуальная частная сеть.

Поскольку данные зашифрованы, их конфиденциальность сохраняется даже при передаче по публичной сети. Это очень важно, потому что пакеты, передаваемые по Internet, уязвимы для перехвата при их прохождении через каждый из узлов (серверов) на пути от передающего к принимающему компьютеру. Зашифрованные данные, даже если они перехвачены, бесполезны для злоумышленника (если, конечно, он не знает ключ шифра). Более подробно шифрование рассматривается далее в главе.

Принцип действия VPN

Виртуальная частная сеть может быть сконфигурирована для работы с помощью коммутируемых соединений или соединений типа "маршрутизатор–маршрутизатор". В последнем случае используются маршрутизаторы и выделенные подключения к Internet, такие, как линии T-1. Между маршрутизаторами можно создать соединение VPN "по требованию". В таком типе соединения отвечающему маршрутизатору выделено определенное соединение Internet, а вызывающий маршрутизатор использует коммутируемое соединение Internet.

Рассмотрим установку туннеля VPN и средства поддержки соединений VPN, встроенные в современные операционные системы.

Создание туннеля

Туннель, созданный для соединения VPN, фактически представляет собой лишь логическое соединение от точки к точке, поддерживающее аутентификацию пользователей и шифрование данных при их передаче с одного конца туннеля на другой.

Допустим, офисы компании размещены в двух зданиях, расположенных через дорогу. При выполнении своих ежедневных обязанностей служащим часто приходится переходить из одного здания в другое. Чтобы перейти в другое здание, служащий должен выйти на улицу, перейти дорогу и войти в него Это напоминает маршрутизацию данных по *публичной сети*, в которой корпоративные данные проходят по общим соединениям Internet. Файлы корпоративных данных могут передаваться посредством электронной почты Internet или с помощью публичного сервера FTP.

Теперь предположим, что нужно обезопасить служащих от всяких случайностей, подстерегающих их при переходе из одного здания в другое, и, кроме того, сделать эти переходы невидимыми для посторонних глаз. Для этого можно вырыть *частный туннель* между двумя зданиями. Таким образом создается конструкция, аналогичная виртуальной частной сети.

Посторонние лица не должны входить в туннель и проходить по нему между зданиями, поэтому нужно установить на каждом конце туннеля двери, которые можно открывать только с помощью ключей, выдаваемых уполномоченными служащими Это напоминает процесс аутентификации пользователя, желающего передать данные по соединению VPN.

К сожалению, если злоумышленник проникнет в туннель, он сможет общаться со служащими, проходящими по туннелю из одного здания в другое. Эту проблему можно решить (хотя это обойдется и дороговато) путем создания одноместных закрытых транспортных средств, которые будут перевозить служащих по туннелю Теперь это будет напоминать шифрование данных, защищающее их от перехвата и использования по пути следования (рис. 16.2).

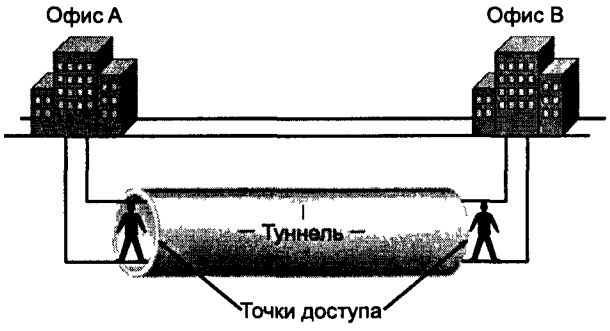


Рис 16 2 Туннель представляет собой частный путь, предназначенный для перехода сотрудников и данных из одной точки в другую

Теперь рассмотрим процесс инкапсуляции и характеристики двух типов туннелирования: уровня 2 и уровня 3.

Процесс инкапсуляции

Туннелирование скрывает исходный пакет данных внутри другого пакета. Для маршрутизации по туннелю в заголовке внешнего (нового) пакета, называемого *заголовком инкапсуляции*, размещается адрес *конца туннеля*. При этом конечный адрес принимающего компьютера расположен внутри, в заголовке исходного пакета. Когда пакет достигает конца туннеля, заголовок инкапсуляции удаляется. Теперь исходный пакет может быть передан на принимающий компьютер. Таким образом, процесс туннелирования представляет собой инкапсуляцию, маршрутизацию по туннелю и извлечение исходного пакета данных.

Туннели могут устанавливаться на разных уровнях сетевой модели OSI: на уровне 2 (канальный уровень модели OSI) и на уровне 3 (сетевой уровень модели OSI).

Туннелирование на уровне 2

Чаще всего в VPN используются протоколы туннелирования, работающие на канальном уровне (уровне 2). С помощью этих протоколов создаются виртуальные каналы между двумя точками. На канальном уровне работает протокол PPTP (Point-to-Point Tunneling Protocol).

Другой протокол канального уровня — L2F (Layer 2 Forwarding) — способен обеспечивать туннелирование по каналам ATM и Frame Relay, поскольку он не зависит от IP. В отличие от PPTP, туннель L2F может поддерживать более одного соединения. Технология L2F, разработанная компанией Cisco Systems, поддерживается операционной системой IOS (Internetwork Operating System), используемой в маршрутизаторах Cisco. Кроме того, L2F поддерживается программами Nortel и Shiva.

Новейший протокол туннелирования — L2TP (Layer 2 Tunneling Protocol) — объединяет элементы PPTP и L2F. Более подробно эти протоколы рассматриваются далее в главе.

Туннелирование на уровне 3

Туннели могут создаваться и на сетевом уровне. В таком случае устанавливается виртуальное соединение на основе IP. Эти соединения работают путем передачи пакетов IP, инкапсулированных в оболочки, определяемые спецификациями IETF (Internet Engineering Task Force). При обработке оболочек используются средства IPSec (IP Security), IKE (Internet Key Exchange) и методы шифрования и аутентификации: MD5 (Message Digest 5), DES (Data Encryption Standard) и SHA (Secure Hash Algorithm).

Протокол IPSec может использоваться совместно с L2TP: процедуры протокола L2TP создают туннель, а IPSec шифруют данные. В этом случае процедуры IPSec работают в *транспортном режиме*. Процедуры IPSec могут также работать в *режиме туннелирования*, в котором они создают туннель.

Туннелирование IPSec уровня 3 используется в ситуациях, когда применение L2TP по каким-либо причинам нежелательно. Далее в главе рассматривается шифрование в протоколе IPSec.

Туннелирование IPSec

Необходимо понимать отличие между виртуальными сетями, в которых протокол L2TP используется для туннелирования, а IPSec — для шифрования, и сетями, в которых IPSec используется в режиме туннелирования.

Одно из существенных отличий состоит в том, что IPSec может инкапсулировать только пакеты IP. В то же время L2TP может инкапсулировать пакеты как IPX, так и других протоколов для передачи их по сетям IP.

Некоторые шлюзы не поддерживают виртуальные сети на основе L2TP или PPTP В этом случае для создания туннеля можно использовать IPSec Обычно туннели IPSec работают от шлюза к шлюзу

Поддержка VPN операционными системами

Современные операционные системы содержат встроенные средства поддержки виртуальных частных сетей Это позволяет создавать соединения с сервером VPN так же просто, как и устанавливать коммутируемое соединение

С помощью своих встроенных компонентов операционные системы Windows 95/98 и Windows NT/2000 могут работать как клиенты VPN В Windows 9*x* и Windows NT поддерживается использование PPTP, а в Windows 2000 — PPTP или L2TP

В состав Windows 2000 включен мастер, который помогает пользователю пройти по этапам установки соединения VPN (рис 16 3)

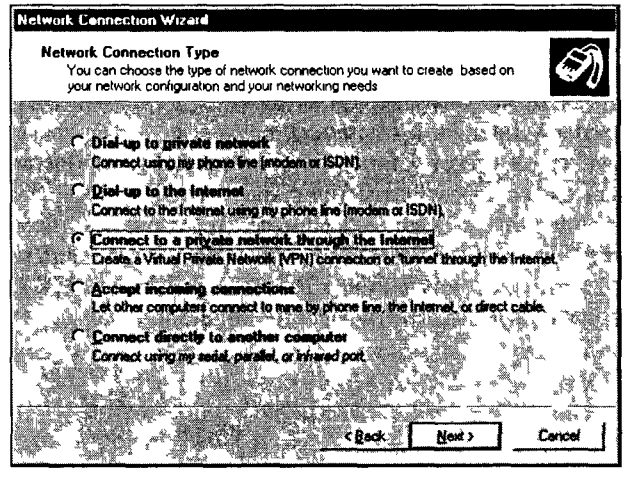


Рис 16 3 Входящий в состав Windows 2000 мастер сетевых подключении облегчает установку соединении VPN

В Linux поддерживается использование IPSec и PPTP Кроме того, можно создавать "псевдотуннели" с помощью PPP и SSH При этом для аутентификации и обеспечения безопасности соединения используется шифр с открытыми/закрытыми ключами RSA

Виртуальные частные сети могут применяться практически в любых операционных системах, при этом может использоваться программное обеспечение и оборудование других поставщиков Компьютеры, входящие в VPN, могут работать на разных платформах, как и компьютеры в системах удаленного доступа

Что дает использование VPN

В начале главы виртуальная частная сеть была определена как способ коммуникации между двумя компьютерами (или двумя сетями) посредством публичной сети Но ничего не было сказано о том, зачем это делать Ведь можно просто установить коммутируемый сервер удаленного доступа, с помощью которого пользователи смогут сообщаться с сетью Таким образом, они обойдут публичную сеть стороной и проблем с безопасностью прохождения данных по публичной сети вообще не будет

Иногда коммутируемый сервер действительно способен выполнять те же задачи, что и VPN. Однако во многих случаях виртуальная сеть имеет существенные преимущества по сравнению с коммутируемым сервером удаленного доступа.

Обсудим преимущества и недостатки VPN и коммутируемых сетей, а затем рассмотрим некоторые популярные способы реализации VPN.

VPN и коммутируемые сети: преимущества и недостатки

В главе 15, "Удаленный доступ", рассматривались ситуации, в которых обычно используются технологии удаленного доступа. Многим служащим необходим доступ к сети компании, когда они находятся за пределами офиса, например во время командировки или при выполнении работы на дому. Чтобы получить доступ к сети, пользователю достаточно позвонить на сервер удаленного доступа. Но что делать, если у служащего нет телефона или он находится в другом городе? Стоимость междугородных звонков довольно высока и часто делает использование коммутируемого удаленного доступа нерентабельным.

Использование VPN может значительно удешевить удаленный доступ. Если корпоративная сеть подключена к Internet, а служащий компании имеет доступ к местному провайдеру услуг Internet, то он может установить соединение, не прибегая к услугам междугородной телефонной связи. Провайдеры услуг Internet могут предоставить путешествующим пользователям доступ к своим местным телефонным номерам. Служащему достаточно лишь позвонить по местному номеру провайдера и создать посредством Internet туннель к локальной сети своей компании, как показано на рис. 16.4. Обычно для этого в корпоративной сети существует выделенное соединение с Internet.

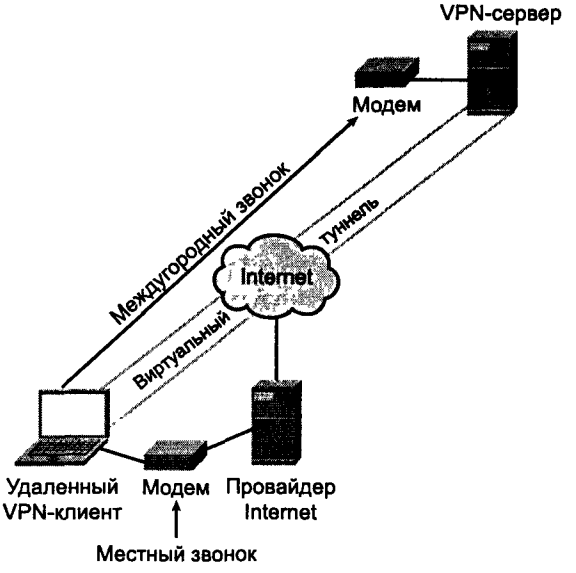


Рис. 16.4. Если используется VPN, то служащий может звонить не по междугородному номеру удаленного сервера, а по местному номеру провайдера

Использование VPN экономит деньги также благодаря уменьшению количества телефонных линий. Если многим пользователям нужен коммутируемый доступ к сети одновременно, то компания вынуждена арендовать отдельные телефонные линии и устанавливать модемы для каждого соединения. В то же время, если эти пользователи получают доступ посредством VPN, компании достаточно установить одно соединение с Internet Уменьшение количества телефонных линий приносит существенную ежемесячную экономию средств.

Многие провайдеры услуг Internet предоставляют соединения VPN Такие провайдеры сами управляют каналами. Это существенно уменьшает расходы компании на выполнение задач сетевого администрирования, потому что значительная их часть перекладывается на провайдера. Если провайдер работает в национальном масштабе, то посредством VPN провайдера данные могут передаваться по принадлежащей ему магистрали, а не по Internet, что также уменьшает затраты.

Итак, по сравнению с методами коммутируемого доступа сети VPN имеют ряд преимуществ.

- Если пользователь находится в другом городе, то, используя VPN, он экономит на междугородных звонках.
- Использование VPN уменьшает количество телефонных линий, необходимых для одновременного предоставления удаленного доступа многим пользователям.
- При использовании VPN нужно меньше модемов и другого оборудования, в частности не нужны пулы модемов.
- Использование VPN, принадлежащих провайдерам, уменьшает расходы на сетевое администрирование и обучение персонала.

Конечно, VPN имеют и недостатки. Для установки VPN необходимо, чтобы компьютеры (или сети) на обоих концах имели соединение с Internet. Если на одном из концов соединение с Internet ненадежно, то это становится существенным препятствием. Например, пользователь, получающий доступ к корпоративной сети, может обнаружить, что сервер его провайдера отключен для профилактических работ. В таком случае он не сможет установить соединение с локальной сетью своей компании посредством VPN. В то же время при использовании непосредственного коммутируемого доступа к локальной сети компании служащий не зависит от надежности оборудования провайдера.

Еще один недостаток VPN — снижение пропускной способности каналов вследствие дополнительного инкапсулирования пакетов. В зависимости от типа VPN и соединений Internet, величина такого уменьшения может изменяться в больших пределах. В любом случае добавление уровня VPN в некоторой степени влияет на производительность. Окупаются ли эти потери преимуществами VPN, должна решать сама компания

В табл. 16.1 приведен краткий обзор преимуществ и недостатков использования VPN.

Таблица 16.1. Преимущества и недостатки VPN по сравнению с коммутируемым доступом

Преимущества VPN	Недостатки VPN
Нет расходов на междугородную телефонную связь	Оба конца должны иметь надежное соединение с Internet
Требуется меньше телефонных линий	Снижается производительность вследствие дополнительной инкапсуляции пакетов
Требуется меньше модемов	
Если используется VPN провайдера, то уменьшаются расходы на администрирование и обучение персонала	

Сценарии VPN

В зависимости от потребностей компании, виртуальные частные сети используются поразному. Чаще всего VPN создаются для достижения одной из следующих целей:

- для предоставления удаленного доступа служащим, находящимся дома или в дороге;
- для создания *экстрасети*, данные которой доступны служащим, партнерам и клиентам;
- для коммуникации двух расположенных на большом расстоянии офисов без затрат на выделенные прямые каналы.

Теперь рассмотрим каждую из этих ситуаций, а также способы реализации виртуальных сетей и обеспечение безопасности передаваемых по ним данных.

VPN удаленного доступа

Концептуально наиболее простой сценарий реализации VPN — это использование VPN для предоставления удаленного доступа индивидуальным пользователям. Однако его реализация может быть усложнена такими факторами, как разные операционные системы и протоколы, установленные на клиентских компьютерах.

Клиентские компьютеры VPN должны поддерживать протоколы, используемые сервером VPN (протоколы туннелирования, сетевой и транспортный) и методы шифрования, принятые в данной VPN. Например, клиенты с установленными операционными системами, отличными от систем Microsoft, могут устанавливать соединение VPN с сервером удаленного доступа Windows 2000 с помощью PPTP, однако если соединение должно быть безопасным, то клиентская операционная система должна поддерживать протокол MPPE (Microsoft Point-to-Point Encryption Protocol).

Когда компоненты VPN установлены и сконфигурированы, для установки соединения VPN нужно подключиться к Internet (рис. 16.5).

1. Для установки соединения с Internet мобильный или домашний пользователь звонит местному провайдеру и регистрируется со своей учетной записью. (Если клиент использует выделенное или постоянное соединение с Internet, например DSL (Digital Subscriber Line — цифровая абонентская линия) либо кабельный модем, то этот шаг не нужен.)

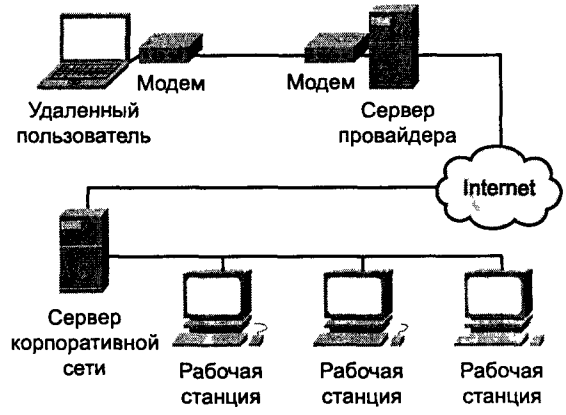


Рис 16 5 Для установки соединения с Internet, посредством которого можно создать туннель в частную сеть, мобильный или домашний пользователь набирает номер провайдера

2. После установки соединения с Internet клиент устанавливает соединение с сервером удаленного доступа, сконфигурированным на установку соединений VPN (на основе IP-адреса удаленного сервера) Этим действием создается туннель
3. Сервер аутентифицирует пользователя и предоставляет ему доступ к ресурсам частной сети

Этот сценарий может выполняться в обратном направлении следующим образом Если домашний компьютер пользователя имеет выделенное соединение с Internet, то пользователь может сконфигурировать его как сервер VPN, установить с ним соединение из офиса и получать доступ к файлам, хранящимся дома

Виртуальные частные экстрасети

В этом сценарии удаленные пользователи получают посредством соединения VPN доступ к части локальной сети компании, называемой экстрасетью В экстрасети могут храниться, например, технические материалы для заказчиков или совместно используемые документы для партнеров компании

Остальная часть внутренней сети должна быть защищена от внешнего доступа Создание отдельной подсети в качестве экстрасети и размещение остальной части локальной сети за брандмауэром повышает безопасность сети (рис 16 6)

Обычно пользователи экстрасети получают доступ к данным с помощью Web-броузера, а Web-сервер устанавливается в подсети, подключенной к соединению VPN Здесь же можно расположить и файловые серверы

Существующие и разрабатываемые стандарты облегчают компаниям разделение данных и приложений экстрасети, которые можно использовать в совместных проектах Применяется три стандарта форматирования данных

- **HTML (Hypertext Markup Language — язык разметки гипертекста)** Предназначен для чтения документов с помощью Web-броузера Для просмотра файлов HTML пользователю не нужно иметь специальный текстовый процессор или другую программу

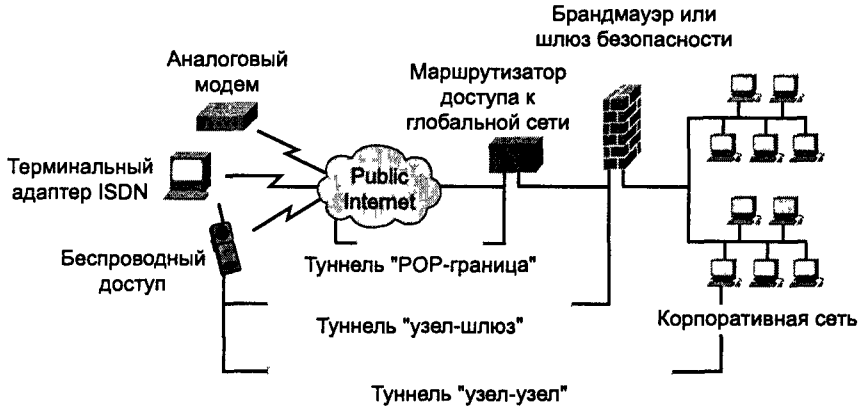


Рис 16 6 Внутреннюю сеть можно защитить от доступа извне с помощью брандмауэра

- **XML (Extensible Markup Language — расширенный язык разметки) и cXML (Commerce XML — коммерческий XML)** Как и HTML, этот язык обеспечивает совместимость разных платформ
- **OBI (Open Buying on the Internet — открытая торговля по Internet)** Является стандартом для сделок электронной коммерции

Соединения VPN между офисами

В этом сценарии соединение между двумя офисами филиалов компании устанавливается с использованием конфигурации VPN от маршрутизатора к маршрутизатору Такая конфигурация называется также *от шлюза к шлюзу* Сервер VPN работает как маршрутизатор, выполняющий передачу IP-пакетов (рис 16 7)

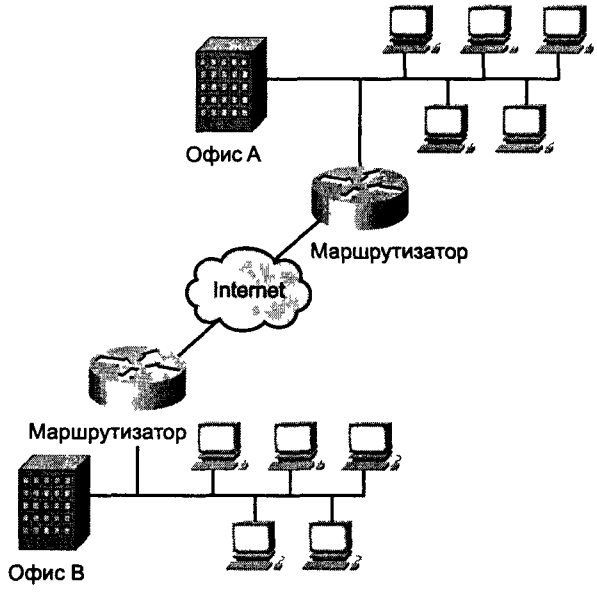


Рис 16 7 Объединение двух офисов при конфигурации VPN от маршрутизатора к маршрутизатору

Локальная сеть каждого из офисов имеет маршрутизируемое соединение с Internet. Это соединение может быть коммутируемым или постоянным. Если используется коммутируемое соединение, то маршрутизатор, инициирующий соединение, использует коммутируемое соединение с Internet. Вызываемый маршрутизатор должен иметь выделенное (постоянное) соединение с Internet. Он должен быть также сконфигурирован на обработку запросов на коммутируемые соединения по требованию. На вызывающем маршрутизаторе конфигурируются два коммутируемых соединения по требованию: одно для набора номера провайдера, а другое для установки соединения с VPN. Если оба маршрутизатора имеют выделенные соединения с Internet, то при желании соединение VPN может быть установлено постоянно.

Сеть VPN от маршрутизатора к маршрутизатору может быть сконфигурирована таким образом, что один маршрутизатор будет работать как клиент, инициирующий соединение, а другой — как сервер VPN. Такое одностороннее соединение предпочтительно, если оно должно быть постоянно открытым. Можно также создать двустороннее соединение, которое может быть инициировано каждым маршрутизатором. В этом случае оба маршрутизатора должны иметь постоянное соединение с Internet и должны быть сконфигурированы как маршрутизаторы локальной и глобальной сетей.

Замечание

В сценарии от маршрутизатора к маршрутизатору таблицы обоих маршрутизаторов должны быть сконфигурированы с необходимыми маршрутами передачи пакетов по соединению. Маршруты можно добавлять вручную или, если коммутируемый по требованию интерфейс имеет постоянное соединение, с помощью протокола динамической маршрутизации.

Для соединения двух локальных сетей на основе Linux или FreeBSD используется специальное программное обеспечение, например vpnd (VPNdaemon). В этом случае безопасность передаваемых по соединению данных обеспечивается применением алгоритма шифрования Blowfish.

Протоколы VPN

В этом разделе рассматриваются три типа протоколов, применяемых в VPN.

- **Протоколы туннелирования** Иногда их называют протоколами VPN. Используются для создания туннеля.
- **Протоколы шифрования**. Другое название — протоколы безопасности. Используются для обеспечения безопасности данных.
- **Сетевые/транспортные протоколы**. Иногда их называют локальными протоколами. Применяются для коммуникации в частной сети.

Протоколы туннелирования

Протоколы туннелирования инкапсулируют данные таким образом, что заголовки исходных протоколов оказываются внутри инкапсулирующих заголовков. Рассмотрим *следующие протоколы туннелирования:*

- PPTP (Point-to-Point Tunneling Protocol);
- L2F (Layer 2 Forwarding);

- L2TP (Layer 2 Tunneling Protocol);
- IPSec (IP Security);
- SSH (Secure Shell) и SSH2;
- CIPE (Crypto IP Encapsulation).

PPTP

Разработанный компанией Microsoft протокол PPTP стал стандартным протоколом туннелирования. Фактически он является расширением канального протокола PPP, используемым для создания каналов глобальных сетей посредством соединений удаленного доступа. Протокол PPTP работает следующим образом.

1. Пакеты PPP (это могут быть пакеты IP, IPX или NetBEUI) инкапсулируются в заголовок GRE (Generic Routing Encapsulation). Добавляется также заголовок IP, содержащий IP-адреса источника и получателя данных. Источник — это клиент VPN, получатель — сервер VPN.
2. Данные исходной дейтаграммы (пакета с адресной информацией) обычно зашифрованы, поэтому несанкционированные пользователи не смогут их прочитать. В сетях VPN компании Microsoft совместно с PPTP используется протокол MPPE, в котором для повышения безопасности данные дополнительно шифруются.

Программное обеспечение PPTP на компьютерах Linux или UNIX называется PPTP-linux. С его помощью компьютер Linux может устанавливать соединения с серверами PPTP. Разработано также программное обеспечение серверов PPTP (называемое PoPToP) для Linux, Sun Solaris, FreeBSD и других реализаций UNIX. Распространяется оно бесплатно. Серверы на его основе могут обслуживать клиентов как Windows, так и PPTP-linux.

Клиенты Macintosh могут устанавливать соединение с серверами Windows PPTP с помощью программ других поставщиков, например TunnelBuilder компании Network Telesystems.

L2F

В 1996 году компания Cisco разработала протокол L2F и включила его в свою систему IOS. Будучи альтернативой PPTP, протокол L2F способен создавать туннели в каналах ATM и Frame Relay. Для PPTP необходимо использование IP, в то же время для L2F протокол IP не обязателен. Кроме того, в L2F выполняется дополнительная аутентификация в концах туннеля.

L2TP

На основе объединения PPTP и L2P компании Microsoft и Cisco создали протокол L2TP. Подобно PPTP, он инкапсулирует данные, передаваемые посредством IP. Протокол L2TP может также инкапсулировать данные для передачи по каналам ATM, Frame Relay или X.25. Таким образом, L2TP можно использовать для туннелирования данных как по Internet, так и по специальным носителям глобальных сетей без применения IP.

Перечислим некоторые преимущества L2TP по сравнению с PPTP.

- Поддерживает множественное туннелирование между двумя точками. Это позволяет создавать отдельные туннели, например с разными уровнями QoS (Quality of Service).

- Поддерживает сжатие заголовков, что повышает производительность.
- В отличие от PPTP, может выполнять аутентификацию туннелей.
- Может работать в межсетевых соединениях на основе виртуальных каналов ATM или Frame Relay без использования IP.

IPSec

Протокол IPSec можно использовать для шифрования данных, передаваемых по туннелю, созданному другим протоколом, таким, как L2TP. Его можно также использовать в режиме туннелирования, т.е. для создания туннеля В режиме туннелирования IPSec используется для инкапсулирования пакетов IP. Туннель IPSec можно сконфигурировать на защиту данных как между двумя IP-адресами, так и между двумя подсетями IP.

В главе 14, "Защита сети", отмечалось, что в IPSec используются протоколы AH (Authentication Header) и ESP (Encapsulating Security Payload), причем может быть использован как один из них, так и оба.

Рассмотрим каждый из этих протоколов и взаимодействие IPSec с разными операционными системами

Режим туннелирования AH

В отдельно взятом режиме AH не выполняется шифрование данных, передаваемых по туннелю. Однако он гарантирует целостность данных, проверяя, не изменялись ли они кем-либо. Кроме того, в режиме AH аутентифицируется отправитель. При использовании AH в адрес передающего или принимающего компьютера не могут быть внесены никакие изменения на всем пути пакета по туннелю.

Режим туннелирования ESP

В этом режиме исходные адреса источника и приемника данных содержатся в исходном (инкапсулированном) заголовке IP. Внешний заголовок обычно содержит адреса шлюзов В режиме ESP данные шифруются с помощью алгоритмов DES или 3DES.

При использовании ESP внешний заголовок IP не защищен и его целостность не гарантируется Если необходимы шифрование, аутентификация и гарантия целостности всего пакета, то следует применять AH и ESP совместно.

Межоперационное взаимодействие IPSec

Операционная система Windows 2000 содержит встроенные средства поддержки IPSec. Протокол IPSec стандартизирован IETF. Он работает также в операционных системах UNIX, Macintosh и других, поддерживающих семейство протоколов IP В IPSec аутентификация может выполняться разными методами, включая предварительно согласованные секретные ключи, Kerberos и службы сертификации.

Для Linux протокол IPSec реализован в программе FreeS/WAN, которая распространяется бесплатно и может быть выгружена из Internet.

SSH/SSH2

Протокол SSH первоначально разрабатывался для предоставления безопасных альтернатив команды `r` системы UNIX, таких, как `rsh`, `rlogin` и `rcp`. В протоколе SSH используются сильные методы шифрования и аутентификации. Его развитие — версия SSH2 — представляет собой безопасный протокол туннелирования, используемый для создания VPN под управлением операционных систем UNIX или Linux. Сети

VPN, создаваемые в SSH2, называются *VPN на уровне каналов*. Существует также клиентское программное обеспечение SSH для Windows.

Замечание

Шлюзы на уровне каналов работают на сеансовом уровне модели OSI. Когда данные передаются на удаленный компьютер посредством шлюза на уровне каналов, они имеют такой вид, будто созданы самим шлюзом. Это позволяет скрывать информацию о структуре защищаемой сети.

Поддержку SSH можно установить на брандмауэре частной сети, тогда туннель создается от клиента SSH, имеющего коммутируемый доступ в Internet, до брандмауэра. Брандмауэр конфигурируется на передачу данных на сервер внутренней сети. Если высокая производительность не очень существенна, то такой простой способ во многих случаях является предпочтительным. Для SSH нужна своя регистрационная учетная запись, такая конфигурация будет оптимальной, когда, например, нескольким доверенным служащим нужно устанавливать из своего дома соединение с небольшой офисной сетью.

CIPE

Программа CIPE представляет собой драйвер ядра Linux, используемый для создания туннеля между двумя подсетями IP. Данные шифруются на сетевом уровне модели OSI. Это называется низкоуровневым шифрованием. По сравнению с высокоуровневым шифрованием оно обладает тем преимуществом, что при объединении двух сетей посредством VPN в приложения не нужно вносить никаких изменений. Программа CIPE проще и эффективнее, чем IPSec.

Протоколы шифрования

Когда туннель создан, необходимо зашифровать данные для обеспечения их безопасности. Чаще всего используются следующие способы шифрования данных:

- MPPE;
- IPSec;
- VPNd;
- SSH.

MPPE

Протокол MPPE используется в соединениях VPN на основе PPTP (или в коммутируемых соединениях PPP). В нем может использоваться алгоритм шифрования с 40-, 56- или 128-битовым ключом.

Шифрование IPSec

В протоколе IPSec для передачи по туннелю L2TP данные шифруются с помощью алгоритмов DES и 3DES. Эти алгоритмы обеспечивают высокую безопасность данных. Алгоритм Диффи–Хеллмана с открытыми/закрытыми ключами позволяет открыто обмениваться по сети открытыми ключами. При этом безопасность не нарушается, поскольку с помощью открытого ключа можно только шифровать данные, дешифрование без закрытого ключа невозможно.

Шифрование VPNd

В программе VPNd, работающей под управлением Linux, используется алгоритм шифрования Blowfish. В этом 64-битовом алгоритме используются ключи разной длины — от 32 до 448 бит. Алгоритм обладает высоким быстродействием. Программа VPNd распространяется бесплатно, и доступен ее исходный код. Существует несколько вариантов программы VPNd, включая GOLDFISH, DOSFISH и TWOFISH.

Шифрование SSH

В SSH для UNIX используются шифры с открытыми/закрытыми ключами, которые подробно рассматриваются в главе 14, "Защита сети".

Локальные протоколы

Для коммуникации клиента и сервера VPN необходимо установить общий стек сетевых/транспортных протоколов. Им может быть TCP/IP, однако это не обязательно. Даже при использовании PPTP, в котором для создания туннеля в публичной сети необходим IP, в частной сети можно использовать IPX/SPX или даже NetBEUI.

Безопасность VPN

Безопасность VPN обеспечивают следующие процедуры:

- аутентификация;
- авторизация;
- шифрование.

Такая многоуровневая система мер безопасности обеспечивает высокую конфиденциальность данных, передаваемых по VPN. Рассмотрим каждый из этих компонентов безопасности.

Аутентификация

Аутентификация клиента VPN предполагает проверку идентичности компьютера и пользователя, инициирующих соединение VPN. Аутентификация может выполнятся на уровне компьютеров. Например, если в сети VPN на основе Windows 2000 для создания соединения VPN L2TP используется IPSec, то выполняется обмен сертификатами компьютеров.

Как показано в главе 15, "Удаленный доступ", аутентификация пользователей может выполняться с помощью одного из нескольких методов, среди которых EAP (Extensible Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft CHAP), PAP (Password Authentication Protocol) или SPAP (Shiva PAP).

Авторизация

Этот термин означает ограничение числа пользователей, которым предоставляется доступ в VPN соответственно принятой стратегии безопасности. Стратегия безопасности определяет, кто из пользователей может получать доступ в VPN, а кому в доступе должно быть отказано.

Шифрование

Для защиты данных VPN используются различные технологии шифрования. Многие реализации VPN позволяют выбирать метод шифрования. Шифрование обеспечивает безопасность данных, передаваемых по VPN. Незашифрованные данные уязвимы для перехвата злоумышленниками в процессе их передачи по публичной сети.

Производительность VPN

Факторы, влияющие на производительность VPN, можно разбить на две категории: общие и специфические для конкретных реализаций VPN.

Более всего на производительность VPN влияет природа самой Internet. Известны многочисленные случаи выхода из строя региональных участков. Интенсивные потоки данных (как, например, при известных событиях 11 сентября 2001 года) могут вызвать существенное снижение производительности каналов. Кроме того, вследствие чрезмерной загрузки иногда закрываются серверы провайдеров, что затрагивает сотни или даже тысячи пользователей.

Использование VPN приводит к увеличению количества передаваемых служебных сигналов, что также уменьшает производительность сетей. Сети VPN на уровне каналов обладают значительно меньшей производительностью, чем на уровне сетей. Если для установки соединения VPN используется публичная сеть, то теряются многие элементы управления, доступные при использовании непосредственного коммутируемого соединения.

Типы VPN

Сеть VPN может быть реализована как программно, так и аппаратно. Рассмотрим кратко обе реализации, то, чем они отличаются и как их можно сочетать в целях повышения безопасности.

Программные реализации VPN

В программных VPN используются рассмотренные в предыдущих разделах этой главы протоколы туннелирования. Эту категорию сетей можно разбить на два типа: сети на основе программного обеспечения независимых поставщиков и на основе программных средств, встроенных в операционные системы. Очевидным преимуществом последних является меньшая стоимость. Ничего не нужно покупать дополнительно, а средства создания VPN, включенные в современные операционные системы, такие, как Windows 2000, оказываются достаточными для решения большинства задач.

В программное обеспечение VPN независимых поставщиков обычно включены дополнительные средства, расширяющие диапазон использования VPN. Многие программы VPN предоставляют более широкий выбор средств безопасности. В некоторых случаях их легче реализовать. Некоторые программы VPN позволяют создавать туннели на основе как протоколов, так и IP-адресов. Реализовать такой тип фильтрации в сетях VPN на основе оборудования обычно нельзя.

Примерами программ VPN независимых поставщиков служат Safeguard VPN, Checkpoint SVN (Secure Virtual Networking) и NetMAX VPN Suite для Linux.

Аппаратные реализации VPN

Оборудование VPN выпускается компаниями Shiva, 3Com и VPNet Technologies. Средства поддержки VPN встроены как в маршрутизаторы Cisco, так и в маршрутизаторы других компаний. Компания NTS поставляет программу TunnelBuilder, являющуюся средством безопасной коммуникации VPN для Windows, NetWare и Macintosh. Поставщики брандмауэров, такие, как Raptor Systems, предоставляют средства создания VPN на основе брандмауэров, оснащенных дополнительными средствами безопасности.

Сети VPN на основе оборудования можно разбить на две категории.

- **На основе маршрутизаторов**. Основой этих VPN являются маршрутизаторы с встроенными средствами шифрования. Они обладают самой высокой сетевой производительностью, к тому же их обычно легко устанавливать и использовать.
- **На основе брандмауэров**. Сети VPN этого типа обычно содержат дополнительные средства безопасности, такие, как усиленная аутентификация и детализированная регистрация. В этих VPN может выполняться трансляция адресов. Недостатком VPN на основе брандмауэров является пониженная производительность, однако применение в некоторых реализациях процессоров, разработанных специально для шифрования, решает эту проблему.

Конфигурирование соединения VPN

Процесс конфигурирования соединения VPN зависит от типа VPN и от того, реализована она программно или аппаратно.

В этом разделе рассматриваются этапы установки соединения VPN в Windows 2000.

1. В главном меню выберите команду Settings⇨Network and Dialup Connections, как показано на рис. 16.8.
2. Дважды щелкните на пиктограмме Make New Connection в диалоговом окне Network and Dial-up Connections (рис. 16.9).
3. При этом открывается мастер Network Connection Wizard. Выберите третий переключатель Connect to a private network through the Internet, как показано на рис. 16.3.
4. Щелкните на кнопке Next. В следующем окне мастера необходимо ввести такую информацию.
   - Whether to dial in to a server to establish an initial connection to the Internet. Если активизировать этот параметр, то мастер просит сконфигурировать или выбрать коммутируемое соединение. Если у вас есть выделенное соединение с Internet, то здесь вам необходимо выбрать do not dial.
   - The host name or IP address of the VPN server. Введите информацию о компьютере или маршрутизаторе, с которым необходимо установить соединение VPN. Помните, что лучше вводить IP-адрес, а не имя хоста. Это упрощает соединение.
   - Whether the connection should be available to all users who share the computer, or only to the user who is creating it. По умолчанию использовать соединение могут все пользователи.

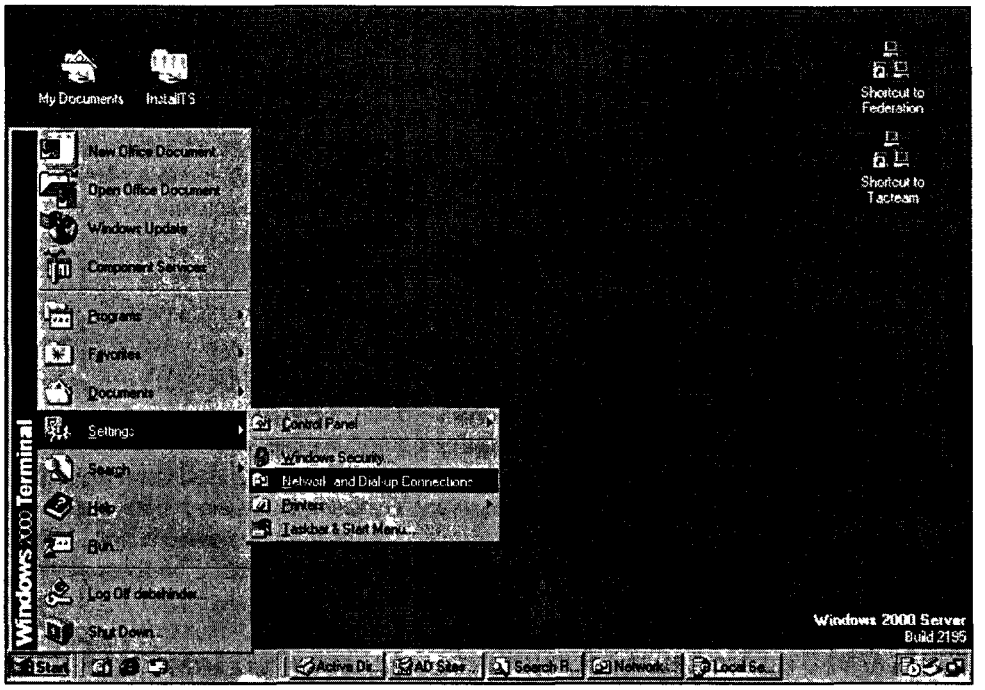


Рис. 16.8 Создание соединения VPN в Windows 2000 начинается с выбора команды главного меню Network and Dialup Connections

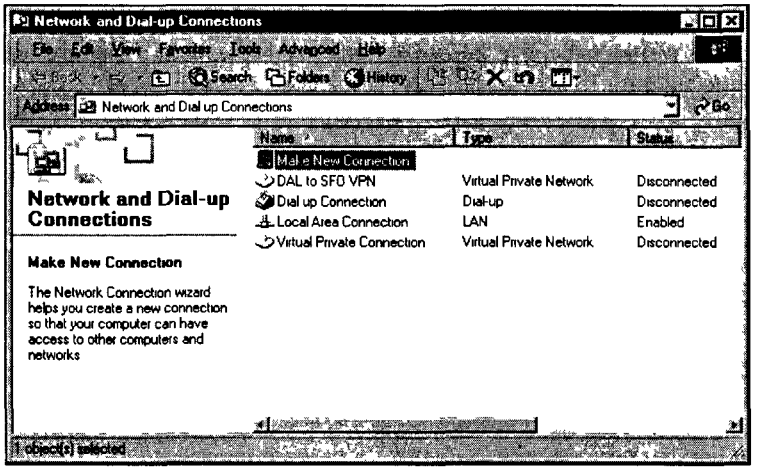


Рис. 16.9. Для создания соединения VPN дважды щелкните на пиктограмме Make New Connection

- Whether to enable Internet Connection Sharing (ICS) to share the VPN connection over the network. Если активизировать этот режим, то другие компьютеры локальной сети смогут пользоваться созданным соединением посредством NAT (Network Address Translation). Обратите внимание· протокол IPSec не работает с NAT.

5. Итак, вы прошли по этапам мастера и ответили на все его вопросы. Теперь на последней странице мастера необходимо ввести имя соединения (рис. 16.10).

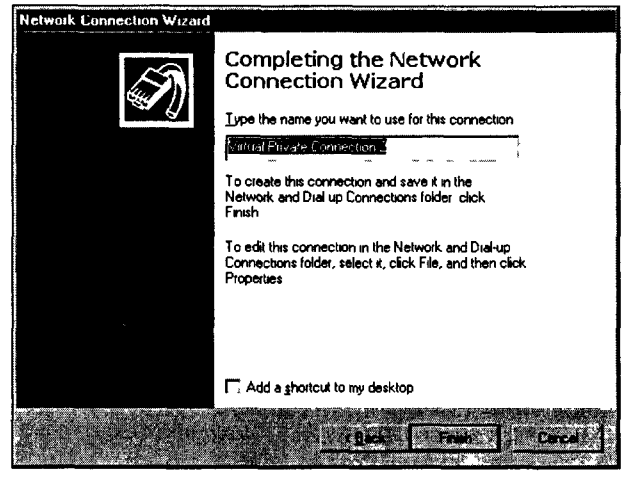


Рис. 16.10. На своей последней странице мастер приглашает ввести имя созданного соединения VPN

Когда соединение VPN на клиентском компьютере сконфигурировано, установить соединение с VPN несложно. Для этого достаточно дважды щелкнуть на пиктограмме соединения в диалоговом окне Network and Dialup Connections и ввести имя пользователя и пароль удаленного сервера VPN. После этого операционная система Windows 2000 автоматически выполнит все операции, необходимые для создания соединения.

Если используется конфигурация по умолчанию (тип VPN установлен в Automatic), то программа самостоятельно выясняет, какой протокол используется на сервере VPN (PPTP или L2TP), и применяет соответствующий протокол для создания туннеля.

Сконфигурировать соединение заново или изменить его свойства (например, используемый протокол аутентификации) можно в любое время.

Резюме

В этой главе рассмотрены основные понятия виртуальных частных сетей в их различных формах. Вы узнали, что VPN позволяют устанавливать безопасные соединения с удаленной частной сетью путем туннелирования, т.е. создания туннеля в Internet или другой публичной сети. Рассмотрены способы реализации VPN посредством коммутируемого соединения и методом "маршрутизатор–маршрутизатор".

Вы узнали, что туннелирование может выполнятся на разных уровнях модели OSI. Рассмотрено туннелирование на уровне 2 с помощью протоколов PPTP и L2TP и туннелирование на уровне 3 с помощью протокола IPSec. Все современные операционные системы содержат встроенные средства создания соединений VPN, однако для этого можно использовать также программные продукты сторонних поставщиков.

Показаны финансовые преимущества использования VPN, описаны протоколы создания VPN и распространенные локальные протоколы, используемые для коммуникации клиентов и серверов VPN.

Рассмотрены различные вопросы безопасности VPN и три главных компонента обеспечения безопасности — аутентификация, авторизация и шифрование, а также производительность VPN и два базовых типа VPN — аппаратный и программный. Глава заканчивается практическим примером создания соединения VPN для клиентского компьютера под управлением Windows 2000.

Сети VPN можно использовать совместно с другой технологией, популярность которой быстро растет: технологией сетей с тонкими клиентами. Концепция тонких клиентов рассматривается в главе 17, "Сети с тонкими клиентами". В этой главе вы узнаете, что с помощью таких средств, как терминальные службы компании Microsoft, программы Metaframe компании Citrix и NetPC, можно сэкономить деньги организации и вдохнуть новую жизнь в старое оборудование.

Рекомендуемые источники

Информация о списке рассылки по тематике VPN и ответы на часто задаваемые вопросы о VPN приведены по адресу: `http://kubarb.phsx.ukans.edu/~tbird/vpn/FAQ.html`.

Документация программы Linux mini-HOWTO, в которой приведено подробное описание установки VPN на основе SSH/PPP, находится по адресу: `http://sunsite.unc.edu/LDP/HOWTO/mini/VPN.html`.

Подробная информация о программах TunnelBuilder и TunnelMaster компании NTS приведена по адресу: `www.nts.com/products/index.html`.

Сжатый отчет по виртуальным частным сетям можно найти по адресу: `www.corecom.com/html/vpn.html`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Как называется процесс размещения заголовка одного протокола внутри другого?
   - **а.** Шифрование.
   - **б.** Инкапсуляция.
   - **в.** Аутентификация.
   - **г.** Авторизация.
2. Как называется логическое соединение от точки к точке, в котором выполняется аутентификация и шифрование данных от одного конца публичной сети до другого?
   - **а.** Туннель.
   - **б.** Протокол.
   - **в.** Шлюз.
   - **г.** Соединение удаленного доступа.
3. Какие из приведенных утверждений о PPTP справедливы? (Выбрать все, что подходят.)

а. Протокол PPTP используется совместно с IPSec для создания безопасной VPN.

б. Протокол PPTP основан на канальном протоколе PPP.

в. Протокол PPTP является протоколом туннелирования на уровне 3.

г. Протокол PPTP используется совместно с MPPE для создания безопасной VPN.

4. Что может работать как в транспортном режиме, так и в режиме туннелирования?

а. PPTP.

б. L2F.

в. IPSec.

г. SSH.

5. Что из приведенного является преимуществом VPN по сравнению с коммутируемым удаленным доступом? (Выбрать все подходящее.)

а. Производительность VPN выше, чем коммутируемого соединения.

б. Соединение VPN более надежное, чем прямое коммутируемое соединение.

в. Если соединение устанавливается между разными городами, то использование VPN экономит деньги на междугородные звонки.

г. При установке соединений VPN одновременно со многими удаленными пользователями серверу не нужна отдельная телефонная линия с модемом для каждого пользователя.

6. Как называется часть корпоративной локальной сети, доступная для таких "избранных" пользователей, как служащие, партнеры и клиенты?

а. Internet.

б. Intranet.

в. Экстрасеть.

г. Подсеть.

7. С какой целью часто используются VPN типа "маршрутизатор–маршрутизатор"?

а. Для предоставления заказчикам доступа к локальной сети компании.

б. Для предоставления служащим доступа к сети компании из их дома.

в. Для предоставления доступа к сети компании ее руководителям, находящимся в дороге.

г. Для создания соединения между двумя офисами, расположенными на большом расстоянии друг от друга.

8. Что из приведенного справедливо как для PPTP, так и для L2TP?

а. Оба могут быть использованы для создания туннеля VPN.

б. Оба могут использовать для туннелирования каналы ATM и Frame Relay.

в. Оба работают на канальном уровне модели OSI.

г. Оба поддерживают множественное туннелирование между двумя точками.

9. Как называется драйвер ядра UNIX, используемый для создания безопасного туннеля между двумя подсетями IP?

а. TunnelBuilder.

б. CIPE.

в. CIR.

г. Демон VPN.

10. Какое из приведенных утверждений аппаратных реализаций сетей VPN справедливо? (Выбрать все подходящие.)

   а. Аппаратные сети VPN на основе оборудования можно разделить на две категории: сети на основе маршрутизаторов и на основе брандмауэров.

   б. Аппаратные сети VPN обычно легче устанавливать и использовать, чем программные VPN.

   в. Аппаратные сети VPN обычно дешевле программных VPN.

   г. В аппаратных сетях VPN выполняется трансляция адресов.

Глава 17

Сети с тонкими клиентами

Если виртуальные частные сети занимают одну из первых строк в списке популярных технологий, то сети с тонкими клиентами расположены в этом списке уж точно не на последнем месте. Применение технологий тонких клиентов позволяет компаниям экономить тысячи долларов на покупке нового оборудования с помощью таких программных продуктов, как Microsoft Terminal Services и Citrix Meteframe, а также с помощью Java-вычислений.

Технология тонких клиентов позволяет использовать устаревшие или малопроизводительные компьютеры для выполнения многих популярных приложений, для которых нужен быстродействующий процессор и большой объем памяти. Эта задача решается путем установки на компьютере тонкого клиента такого программного обеспечения, которое дает возможность устанавливать соединение с сервером (обычно он называется *терминальным сервером*) и выполнять на нем необходимые программы. Пользователь работает за своим настольным компьютером, однако фактически программы выполняются на сервере, тонкому клиенту по сети передаются лишь копии экрана.

В этой главе рассматриваются преимущества и недостатки применения технологии тонких клиентов для уменьшения основных фондов как больших корпораций, так и небольших коммерческих организаций. Сначала приводится общая концепция сетей с тонкими клиентами, а затем способы их реализации.

Подробно описано оборудование тонкого клиента: терминалы WBT (Windows-based Terminal — терминал на основе Windows), сетевые компьютеры NC и NPC, обычные настольные компьютеры и портативные, или карманные компьютеры. Обсуждаются также вопросы выбора оборудования и программного обеспечения, необходимых при развертывании сети с тонкими клиентами.

Затем рассматриваются наиболее распространенные протоколы, используемые для коммуникации тонкого клиента с сервером, и следующие популярные технологии тонких клиентов:

- Microsoft Terminal Services, включая Windows NT Terminal Server Edition и Windows 2000 Terminal Service;
- Citrix Winframe и MetaFrame;
- терминалы X Window;
- технологии Web и виртуальные машины Java.

В конце главы представлена модель ASP (Application Service Provider — поставщик услуг выполнения приложений) и философия "Internet как операционная система", лежащая в основе стратегии Microsoft .NET — новой инициативы компании Microsoft.

Развитие сетей с тонкими клиентами

На протяжении двух последних десятилетий традиционные настольные операционные системы становились все более мощными и сложными, причем их требования к оборудованию постоянно возрастали. В табл. 17.1 приведено сравнение наиболее популярных операционных систем компании Microsoft. Как видите, с течением времени DOS была вытеснена системой Windows, которая постепенно развилась в Windows 9*x*, Windows ME, Windows NT и Windows 2000.

Таблица 17.1. Сравнение операционных систем компании Microsoft

Год выпуска	Операционная система	Типичный объем оперативной памяти	Типичное быстродействие процессора, МГц
1981	MS DOS	64 Кбайт	4,77
1985	Windows	1–2 Мбайт	12
1990	Windows 3 0	2–4 Мбайт	16–25
1994	Windows NT	16 Мбайт	33–66
1995	Windows 95	16 Мбайт	66–90
1996	Windows NT 4.0	32 Мбайт	100–133
1998	Windows 98	32 Мбайт	200–233
2000	Windows ME	32–64 Мбайт	333–450
2000	Windows 2000	64–128 Мбайт	333–450

Примечание. *В таблице приведены не минимальные требования операционной системы к оборудованию. Операционная система может работать и на менее производительном компьютере. Приведенные числа являются "типичными" характеристиками компьютера, обеспечивающими нормальную производительность. Обратите внимание, что эти характеристики приведены для настольных версий операционных систем, таких, как Windows NT Workstation или Windows 2000 Professional.*

Быстрый рост типичных требований операционных систем к оборудованию привел к нежелательному побочному эффекту: миллионы компьютеров, все еще находящихся в отличном состоянии, устаревают по мере того, как на рынок выходят новые, более "толстые" операционные системы. Другими словами, эти компьютеры должны быть или модернизированы, или заменены более мощными. Оба решения ведут к значительным расходам, особенно для компаний, эксплуатирующих сотни, а иногда и тысячи компьютеров. При этом старые компьютеры компания переносит на склад, где они лишь загромождают место, пускает на запчасти или дарит бесприбыльным организациям, которые счастливы иметь хотя бы такие системы.

Для компании существуют и другие возможности: продолжать работать в старых операционных системах или установить компактные операционные системы, например "крошечную" Linux, для которой требуется всего 4 Мбайт оперативной памяти, а дистрибутив умещается на стандартной дискете. Однако такое решение редко бывает удовлетворительным, потому что тогда компания не сможет работать с многими популярными приложениями, например Microsoft Word, или обмениваться программами и данными с партнерами, работающими с более современными операционными системами.

Технология тонких клиентов позволяет использовать устаревшие компьютеры, не отказываясь от преимуществ современных операционных систем и приложений. Основная концепция тонкого клиента проста: использовать маломощные компьютеры или терминалы в качестве настольных, а главную вычислительную нагрузку переложить на мощный сервер.

Это напоминает архитектуру универсальных вычислительных машин IBM, в которых мощные центральные процессоры выполняли приложения и обрабатывали данные многочисленных пользователей. Итак, круг замкнулся? Чем же технология тонких клиентов на основе персональных компьютеров отличается от мэйнфреймов? Ответы на эти вопросы вы найдете в следующих разделах.

Технология тонких клиентов

В чем суть технологии тонких клиентов? В типичной реализации этой технологии программы, выполняющиеся на сервере, передают тонкому клиенту посредством сети пользовательский интерфейс. Настольный компьютер, на котором выполняется клиентская программа, передает на сервер действия пользователя, такие, как нажатие клавиш и передвижение указателя или щелчки мышью. Все вычисления выполняются на сервере

Пользователь регистрируется на сервере с индивидуальной, предварительно сконфигурированной учетной записью, поэтому у каждого пользователя рабочий стол (экран компьютера) настроен соответственно его пожеланиям Многие пользователи могут зарегистрироваться одновременно, однако каждый пользователь никак не ощущает присутствия других (не считая, конечно, снижения производительности) Многопользовательские приложения устанавливаются таким образом, что каждый пользователь может работать с предпочтительной для него конфигурацией этих приложений. Пользователи могут получать доступ к своим локальным дискам, записывать данные на гибкие диски, передавать задачи печати на принтер и т.д. (рис. 17.1)

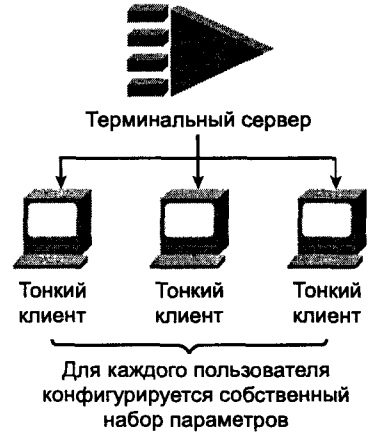


Рис 17 1 У каждого пользователя тонкого клиента может быть собственный уникальный рабочий стол и конфигурация приложений

Преимущества технологии тонких клиентов

Очевидным преимуществом модели тонких клиентов является экономия денежных средств Клиентское программное обеспечение может выполняться на самых разных платформах, поэтому такая технология очень гибкая. Например, пользователь компьютера X386 или Macintosh может работать с рабочим столом Windows 2000 и приложениями набора Office 2000 (рис. 17.2).

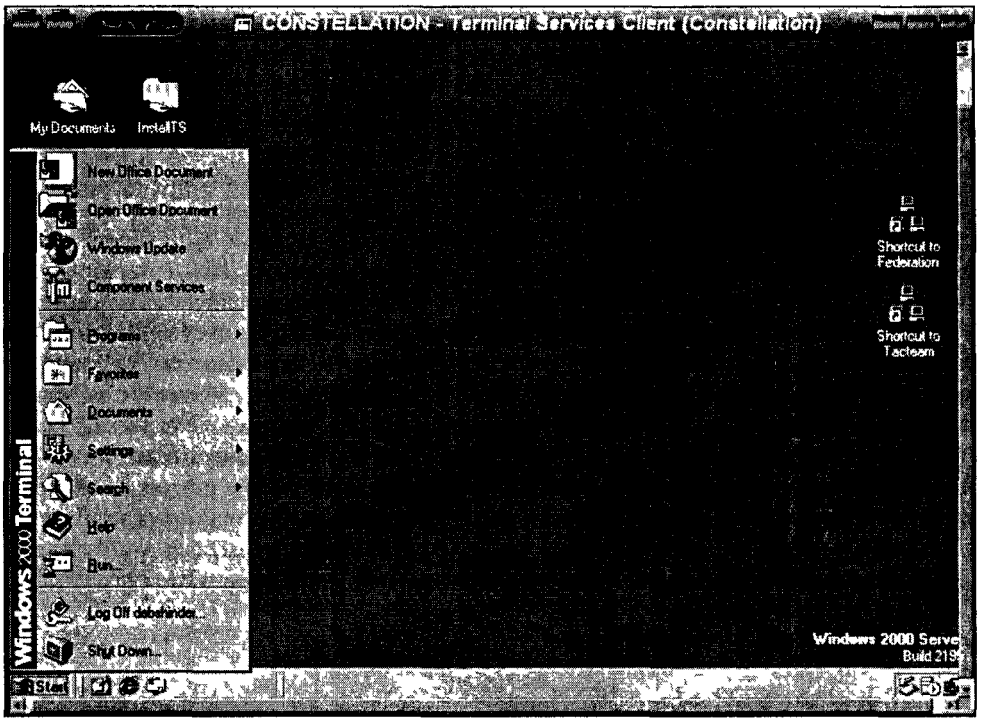


Рис 17 2 С помощью терминала на основе устаревшего или маломощного оборудования пользователь может работать в Windows 2000

Реализация такой технологии обходится дешевле, чем замена всех настольных компьютеров более производительными, поддерживающими Windows 2000. Сервер приложений должен быть реализован на основе относительно мощного персонального компьютера. Например, в качестве минимальной конфигурации для Windows 2000 Terminal Server компания Microsoft рекомендует применять процессор Pentium, имеющий по меньшей мере 128 Мбайт оперативной памяти с дополнительными 12–21 Мбайт на каждого пользователя. Тем не менее производительный сервер, достаточный для поддержки многих клиентов, стоит дешевле мэйнфрейма

Другим преимуществом является то, что в качестве терминала можно использовать полноценный персональный компьютер. Тогда можно одновременно выполнять приложения, хранящиеся на сервере, и, когда это удобнее, выполнять локальные приложения на своем компьютере. Обычно терминалы, используемые для получения доступа к мэйнфреймам, не обладают собственной вычислительной мощностью Для предоставления персональным компьютерам доступа к мэйнфреймам можно воспользоваться ка-

ким-либо шлюзом, например SNA (Systems Network Architecture), однако его реализация обходится довольно дорого.

Для сетевого администратора развертывание сети с тонкими клиентами предоставляет ряд преимуществ.

- Упрощается модернизация приложений, потому что при этом обновляется только одно многопользовательское приложение на сервере, а не сотни или даже тысячи приложений на отдельных компьютерах.
- В некоторых случаях деньги экономятся также на лицензиях программного обеспечения. Тщательно проанализируйте лицензионные соглашения: в них может оказаться требование покупки лицензии для каждого пользователя приложения, даже если все приложения выполняются на одном компьютере.
- Защита от вирусов выполняется на сервере. На рабочих столах пользователей можно заблокировать доступ к гибким дискам и установить использование системы WBT (Windows-based Terminal), не имеющей дисководов. Кроме того, администратору легко ограничить или проконтролировать установку пользователями своих программ.
- При использовании терминалов данные хранятся на сервере. Концентрация данных на одном сервере облегчает обеспечение безопасности и резервное копирование. Если в качестве терминалов пользователи применяют персональные компьютеры, то можно позволить им хранить часть данных локально.
- Легко контролировать сеансы терминалов. Администратор может контролировать открытие, закрытие сеансов и даже перемещение указателя мыши пользователя.
- Облегчается реализация правил безопасности. Стратегия доступа в технологии тонких клиентов существенно отличаться от стратегии при использовании локальных компьютеров, потому что в первом случае администратор может легко контролировать рабочие столы и действия пользователей.

Протоколы тонких клиентов

Реализация сети с тонкими клиентами основана на трех компонентах: оборудовании (сервера и клиента), программном обеспечении (тоже сервера и клиента) и протоколах, на основе которых сервер и клиент сообщаются друг с другом.

В этом разделе рассматриваются протоколы, используемые в двух наиболее популярных программах технологии тонких клиентов — Windows Terminal Services и Citrix MetaFrame. В них используются протоколы *RDP* (*Remote Desktop Protocol — протокол удаленного рабочего стола*) и *ICA* (*Independent Computing Architecture — архитектура независимых вычислений*).

Замечание

Компания Microsoft разработала RDP для работы с терминальными службами без добавления компонентов Citrix. Протокол ICA поставляется в составе Citrix MetaFrame

Кроме того, рассматриваются протоколы X и XDM, используемые терминалами X Window в среде Linux/UNIX, а также RFB (Remote Frame Buffer), BOOTP (Bootstrap Protocol), DHCP (Dynamic Host Configuration Protocol) и TFTP (Trivial File Transfer

Protocol), используемые для загрузки сетевых персональных компьютеров и бездисковых рабочих станций.

RDP

Протокол RDP (Remote Desktop Protocol) поддерживается Windows NT Terminal Server Edition и Windows 2000 Terminal Services из поставки Windows 2000 Server. Он может работать с WBT под управлением операционной системы Windows CE и с компьютерами под управлением Windows for Workgroups 3.11, Windows 95/98 и Windows NT/2000.

В RDP поддерживается сетевой транспортный протокол TCP/IP. Он может работать в соединениях локальных и глобальных сетей и в соединениях коммутируемого доступа. Он позволяет распечатывать документы посредством локального порта LPT и поддерживает перенаправление буфера обмена, т.е. позволяет переносить (вырезать и вставлять) участки кода между терминалами и приложениями локальных систем.

ICA

Компания Citrix поставляет ICA (Independent Computing Architecture) в составе Winframe и MetaFrame. Средства ICA существенно расширяют функциональные возможности Windows Terminal Services. Например, ICA может работать в DOS, Macintosh и в нескольких версиях Linux и UNIX, в то время как RDP работает только с клиентами Windows. Средством ICA поддерживается также использование броузеров Internet Explorer и Netscape в качестве терминальных клиентов. Это позволяет использовать терминальные службы практически в любой среде персональных компьютеров.

ICA может работать на самых разнообразных клиентских устройствах: персональных компьютерах, сетевых компьютерах, WBT, сетевых терминалах Wyse Technology, портативных и карманных компьютерах, телевизионных приставках и различных сетевых устройствах.

Еще одним преимуществом программ компании Citrix является поддержка протоколов IPX, SPX и NetBEUI дополнительно к TCP/IP. ICA может выполняться в соединениях локальных и глобальных сетей, в коммутируемых и других соединениях. В отличие от RDP, в ICA поддерживается использование 16-разрядных звуковых файлов, поэтому пользователи ICA могут воспроизводить на своих терминалах файлы `.wav`, `.mid` и `.avi`.

X и XDMCP

Протокол X позволяет устанавливать соединения между X-сервером и X-терминалами. В качестве протокола тонких клиентов он несколько ограничен, так как, в отличие от других протоколов, не содержит средств надежного обеспечения безопасности и сжатия данных. Использовать протокол X в соединениях глобальных сетей не рекомендуется, потому что в нем отсутствуют средства оптимизации, однако попытка решить эту проблему сделана в его варианте — протоколе LBX (Low-Bandwidth X — протокол X для каналов с низкой пропускной способностью).

Протокол XDMCP (XDM Communication Protocol — протокол коммуникации в XDM) используется в XDM для управления распределением ресурсов сервера пользователям терминалов X.

RFB

Протокол RFB (Remote Frame Buffer) предоставляет пользователю терминала удаленный доступ к графическим интерфейсам. Это межплатформенный протокол, он способен работать с X, Windows и Macintosh.

Протокол RFB определяют как протокол тонких клиентов, потому что его требования к клиенту минимальны. Вся обработка данных выполняется на сервере RFB. Когда клиент отключается, сервер запоминает состояние сеанса. Когда клиент вновь подключается к серверу, он получает от сервера свой интерфейс в том же состоянии, что и в момент отключения. Например, любое приложение, выполнявшееся в момент отключения, при подключении будет выполняться с той же точки, а любой открытый документ будет точно так же открыт и отображен на экране. Причем все это выполнение не зависит от того, с какого клиентского терминала пользователь подключился повторно — с того же или с другого.

BOOTP, DHCP и TFTP

Протоколы BOOTP, DHCP и TFTP не являются протоколами тонких клиентов, однако они используются для того, чтобы позволить "очень тонким" клиентам, например бездисковым рабочим станциям, подключаться к сети и загружать из нее операционную систему. Такой процесс показан на рис. 17.3.

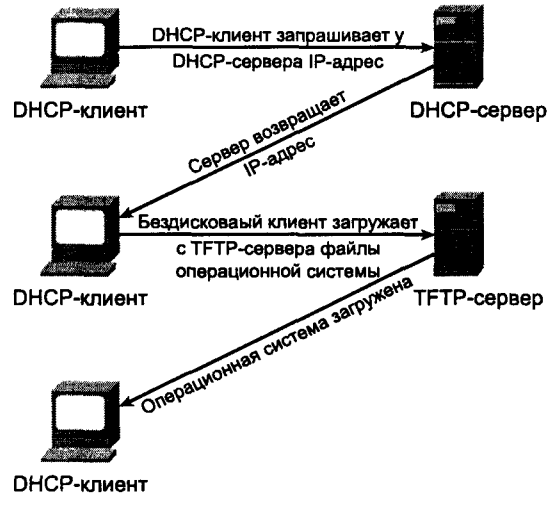


Рис. 17.3. Протоколы BOOTP, DHCP и TFTP используются для подключения к сети бездисковых рабочих станций и загрузки из нее операционной системы

Первоначально BOOTP был разработан как способ подключения к сети бездискового компьютера и присвоения ему IP-адреса. После этого бездисковый компьютер может подключиться к серверу посредством TFTP и загрузить в память файлы операционной системы. Сервер BOOTP присваивает IP-адреса компьютерам, сконфигурированным как клиенты BOOTP.

Протокол DHCP представляет собой новую и более совершенную версию BOOTP. Сервер DHCP присваивает адреса компьютерам, сконфигурированным как клиенты DHCP. Процесс присвоения адресов рассматривается в главе 8, "Сетевые протоколы и службы".

После присвоения IP-адреса клиент может посредством протокола TCP/IP сообщаться с сетью, в частности с сервером TFTP, на котором хранится загрузочный код. На сервере TFTP используется протокол UDP (User Datagram Protocol), производительность которого выше, чем TCP. Бездисковые компьютеры могут загружать с сервера загрузки самые разные операционные системы, включая Windows и Linux. Из-за отсутствия жесткого диска файлы загрузчика операционной системы находятся в оперативной памяти клиента. Программа начальной загрузки предварительно заносится в память сетевого адаптера согласно стандарту PXE (Preboot Execution Environment).

Стандарт PXE

Компания Intel и другие производители при разработке кодов начальной загрузки тонких клиентов и других компьютеров, загружающих операционные системы из сети, придерживаются стандарта PXE. Код PXE записывается в постоянную память сетевого адаптера или в устройство тонкого клиента.

Карта PXE передает на сервер сообщение о том, что она может выполнить начальную загрузку методом PXE. Сконфигурированный соответствующим образом сервер возвращает команду, разрешающую клиенту обратиться к серверу загрузки, на котором хранится образ операционной системы.

Оборудование тонкого клиента

Для реализации тонкого клиента могут использоваться самые разные типы устройств. Одно из главных преимуществ технологии тонких клиентов — легкая переносимость на разные платформы.

Обычно тонкие клиенты реализуются на основе следующих типов устройств:

- WBT;
- сетевые компьютеры NC;
- сетевые персональные компьютеры NPC;
- настольные компьютеры (как персональные, так и Macintosh с установленными разными операционными системами);
- портативные и карманные компьютеры.

Рассмотрим каждый из этих типов устройств и их место в корпоративной сети.

WBT

Терминалы WBT (Window-based Terminal — терминал на основе Windows) разрабатывались с целью предоставить рабочий стол и приложения Windows пользователям технологии тонких клиентов. На большинстве моделей WBT установлено программное обеспечение терминального сервера Microsoft и предварительно загружены клиентские программы RDP или Citrix ICA. Обычно они рассчитаны на использование операционных систем Windows CE или встраиваемых систем NT.

Устройства WBT дешевле, чем полнофункциональные персональные компьютеры, тем не менее пользователи могут выполнять на них большинство приложений, предназначенных для компьютеров Windows. На терминале WBT нет жесткого диска, это уменьшает риск заражения вирусами или несанкционированного копирования данных компании. Еще одно преимущество бездисковых машин — меньшая вероятность их кражи. Без сети бездисковые устройства бесполезны, поэтому для вора они вряд ли привлекательны.

Компания Wyse Technology (поставщик WBT, пользующийся заслуженной репутацией) первая выпустила WBT на рынок в 1995 году.

Сетевые компьютеры

Сетевые компьютеры (*Network Computers — NC*) были разработаны компанией Sun Microsystems в середине 1990-х годов. К этому проекту присоединились также IBM и Oracle. Архитектура NC построена на основе истинно тонких клиентов, содержащих лишь минимальное оборудование, необходимое для загрузки операционной системы и подключения к сети.

Компьютеры NC предоставляют пользователям Web-интерфейс и виртуальную машину Java (Java Virtual Machine — JVM), обеспечивающие большую гибкость. Спецификации NC со временем развились в открытый стандарт, охватывающий следующие базовые характеристики.

- Архитектура NC не является патентованной вычислительной платформой. Для нее не нужна особая операционная система.
- Система NC поддерживает Web-интерфейс (броузер) для формирования запросов и обработки документов по протоколам HTTP (Hypertext Transfer Protocol) и HTTPS (Secure HTTP).
- Система NC поддерживает средства электронной почты на основе SMTP (Simple Mail Transfer Protocol).
- Система NC поддерживает выполнение аплетов Java.
- Система NC поддерживает сетевой/транспортный стек протоколов TCP/IP.

Современной реализацией NC является Network Station компании IBM. Это устройство может работать как терминал мэйнфрейма IBM или, используя протокол Citrix ICA, как терминал для приложений Windows.

Многочисленные бездисковые сетевые компьютеры могут загружаться из сети и выполнять приложения Windows или Linux. Операционная система загружается из сети. Например, клиент Sun Ray может не только получать доступ к приложениям Java и Sun Solaris, но и выполнять приложения NT на сервере Sun Ray с помощью MetaFrame.

Сетевые персональные компьютеры

Вскоре после появления на рынке компьютеров NC совместными усилиями компаний Microsoft, Dell, Compaq и Hewlett Packard была разработана их альтернатива — *сетевой персональный компьютер* (*Network Personal Computer — NPC*). Это базовый персональный компьютер с малопроизводительным процессором и небольшим объемом оперативной памяти. Система NPC поддерживает такие средства локальных сетей, как Wakeup, позволяющее включать компьютер и управлять им с большого расстояния, даже если он был выключен.

Компьютер NPC является полнофункциональным. Когда сеть отключена, его можно использовать как отдельный компьютер и выполнять на нем локальные приложения. Это существенное преимущество по сравнению с терминальными устройствами, которые можно загрузить только из сети.

Спецификации NPC определяют следующие требования к характеристикам компьютера: минимальный объем оперативной памяти — 16 Мбайт, процессор Pentium с тактовой частотой не ниже 100 МГц (или эквивалентный) и поддержка технологии PnP. Корпус компьютера должен запираться на замок — пользователь не должен иметь доступа к его компонентам. Права пользователя на установку и конфигурирование устройств должны быть ограничены. Накопители CD-ROM, дисководы и гнезда расширения обычно отсутствуют. Однако, в отличие от WBT, компьютеры NPC имеют локальный жесткий диск.

Настольные компьютеры

На обычных настольных компьютерах, включая самые производительные модели, могут выполняться клиентские программы Microsoft Terminal Services или Citrix ICA, т.е. они могут работать как "толстые тонкие клиенты". Зачем может понадобиться такая конфигурация? Развертывание приложений на терминальном сервере предоставляет многие преимущества. Это позволяет контролировать конфигурацию и предпочтения пользователей, а также существенно облегчает модернизацию приложений. На настольном персональном компьютере терминальная клиентская программа выполняется точно так же, как и любое приложение. Одновременно с ней на компьютере могут выполнятся локальные приложения.

Клиентские программы могут работать под управлением DOS, Windows, Macintosh или UNIX/Linux. Такой метод особенно полезен, когда пользователям, у которых установлена операционная система, отличная от Windows, время от времени нужно выполнять приложения Windows.

Недостатком использования настольных компьютеров в качестве терминальных клиентов является снижение уровня безопасности. В состав компьютеров входят дисководы и накопители CD-ROM, поэтому пользователи могут устанавливать несанкционированные программы и копировать сетевые данные на свои носители. Однако некоторые из этих рисков могут быть устранены или уменьшены применением более жестких правил безопасности, например содержанием персональных компьютеров "под замком" и ограничение действий пользователей.

Тончайшие клиенты: портативные компьютеры

На основе портативного персонального компьютера можно создать мобильный терминал WBT путем установки на нем терминальных клиентских служебных программ под управлением Windows CE. С помощью беспроводных каналов связи эти портативные устройства используются для доступа к приложениям и данным, когда пользователь находится в дороге.

Портативные терминалы устанавливаются в госпиталях для обеспечения мгновенного доступа к записям пациента во время обхода. Более подробно беспроводные портативные сетевые устройства рассматриваются в главе 19, "Технологии завтрашнего дня".

Программное обеспечение тонких клиентов

В этом разделе представлены программы, используемые в технологиях тонких клиентов: Terminal Services компании Microsoft, включенные в поставку Windows 2000 Server, программу Citrix MetaFrame для Windows NT 4.0 и Windows 2000, Winframe для Windows 3.51 и программное обеспечение X Window для UNIX/Linux. Рассматриваются также технологии Web и виртуальные машины Java.

Microsoft Terminal Services

На основе интеграции с технологиями Citrix компания Microsoft разработала версию операционной системы Windows NT 4.0, которая называется Windows NT 4.0 Terminal Server Edition. С операционной системой Windows 2000 (Windows 2000 Server, Advanced Server и Datacenter Server) поставляются все необходимые терминальные службы, поэтому пользователям теперь нет необходимости покупать "специальные издания" операционных систем.

Операционная система Windows 2000 Terminal Services может быть установлена в одном из двух следующих режимов:

- режим сервера приложений;
- режим удаленного администрирования

Режим сервера приложений

Сконфигурированный на режим сервера приложений сервер Windows 2000 Terminal Server работает в традиционной модели тонкого клиента. В этом режиме он предоставляет рабочий стол Windows 2000 и приложения Windows клиентским компьютерам, на которых установлены терминальные клиентские служебные программы.

В этом же режиме можно создать группы пользователей, индивидуальные для терминальных служб, и профили пользователей, действительные только для терминального сеанса. Можно установить время жизни сеансов пользователей, т.е. промежуток времени, по истечении которого они будут отключены Для регистрации на сервере или в домене сети в качестве терминальных клиентов пользователи должны иметь соответствующие учетные записи. Это ограничение повышает безопасность системы

С помощью средства Terminal Services Manager, установленного на сервере Windows 2000, администратор может просматривать сеансы терминалов и управлять ими (рис. 17.4).

Средства удаленного контроля позволяют выполнять мониторинг сеансов пользователей. С их помощью можно наблюдать за действиями пользователей или управлять в сеансе клавиатурой и мышью пользователя. Это может быть полезным при устранении неполадок у пользователей или для демонстрации пользователям правильных действий, когда администратор находится далеко.

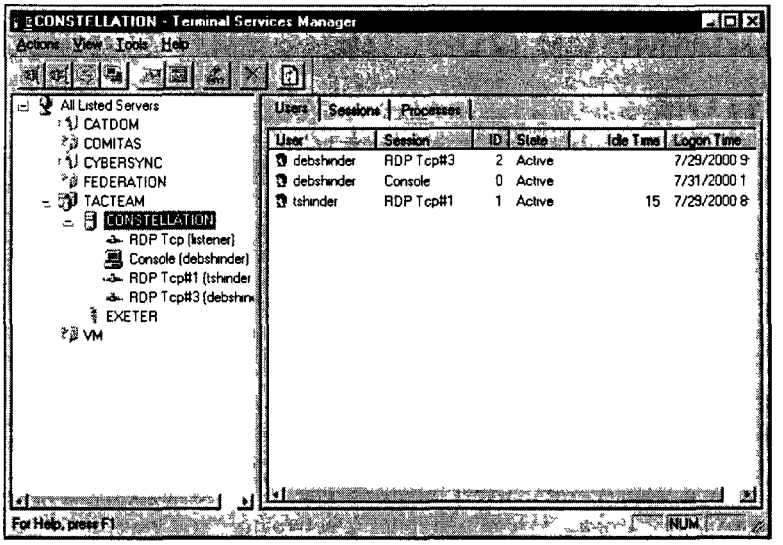


Рис. 17.4. Сеансами терминалов Windows 2000 можно управлять с помощью средства Terminal Services Manager

Режим удаленного администрирования

С помощью терминальных служб можно подключиться к серверу и управлять им с любого настольного компьютера. Это реальная альтернатива таким программам независимых поставщиков, как PCAnywhere.

В режиме удаленного администрирования на терминальный сервер накладываются следующие ограничения:

- зарегистрироваться на терминале удаленного администрирования могут только члены группы администраторов;
- допустимы только два соединения одновременно

С учетом этих ограничений в режиме удаленного администрирования можно запускать программы, управлять рабочими столами — словом, делать все, что допускается в режиме сервера приложений.

Программы Winframe и MetaFrame компании Citrix

Программа Winframe, созданная для работы под управлением Windows NT 3.51 Server, обеспечивает выполнение функций терминальных служб. Более новая версия этого продукта компании Citrix — программа MetaFrame — поддерживает расширенный набор средств и может работать под управлением Windows NT 4.0 Terminal Server Edition и Windows 2000. Компания Ctirix поставляет также версию программы MetaFrame для UNIX.

В программах компании Citrix используется протокол ICA, поэтому MetaFrame предоставляет дополнительные функциональные возможности, реализуемые с помощью ICA. В гибридной сети MetaFrame может подключаться к терминальному серверу с клиентами, отличными от Windows.

В программу MetaFrame 1 8 для Windows 2000 включена технология портала приложений компании Citrix, которая называется NFuse Она позволяет выполнять инте-

рактивные приложения с помощью стандартных Web-броузеров Microsoft Internet Explorer и Netscape. Эта концепция вычислений рассматривается далее в главе.

Технология NFuse позволяет также объединять несколько серверов в группу — *ферму серверов*. Внутри фермы существенно облегчается балансировка нагрузки, пул лицензий и публикация приложений. В программе MetaFrame есть диалоговое окно Program Neighborhood (Программное окружение), аналогичное окну Network Neighborhood (Сетевое окружение) в операционных системах Windows и предоставляющее более строгий контроль над приложениями (рис. 17.5).

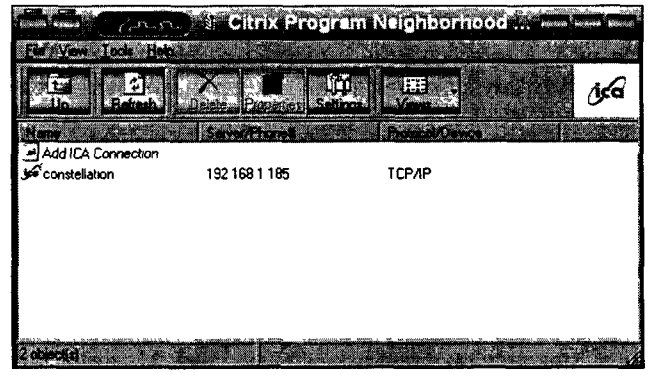


Рис 17 5 В программе Citrix MetaFrame управление приложениями и соединениями выполняется с помощью диалогового окна Program Neighborhood

Система X Window

Система X Window (иногда неправильно пишут X Windows) разработана в Массачусетском технологическом институте для предоставления удобного графического интерфейса пользователям UNIX и Linux.

На основе протокола X создается пользовательская среда, аналогичная среде Windows, OS/2, Macintosh OS и других графических операционных систем С его помощью можно выводить на экран диалоговые окна многих приложений одновременно. Однако X отличается от многих операционных систем с графическим интерфейсом тем, что это сетевой протокол, в других системах используются программные вызовы процедур.

Посредством сети сервер X принимает вводимые данные и передает рисунок экрана обратно клиенту. Клиентская программа X может выполняться на том же компьютере, что и программа сервера, или на другом компьютере. В последнем случае клиентский компьютер является терминалом X Window.

Некоторые поставщики, например компания Hummingbird, предоставляют программное обеспечение клиентов и серверов X для компьютеров под управлением операционных систем, отличных от UNIX. Это такие программы, как Exceed, клиентская программа X на основе Windows и Exceed Web, обеспечивающая соединения тонкого клиента на основе Web

Технологии Web

В технологиях Web для создания документов, их просмотра с помощью Web-броузеров и передачи посредством Internet или локальных сетей используются прото-

кол HTTP (Hypertext Transfer Protocol) и язык HTML (Hypertext Markup Language — язык разметки гипертекста). Доступ к приложениям Web можно получать из любых операционных систем, в которых выполняются стандартные программы броузеров.

Недостатком традиционных Web-технологий является высокая стоимость разработки или покупки Web-приложений. Однако программные продукты компании Citrix предоставляют возможность публикации приложений Windows на Web-сервере, где они доступны для любого пользователя с установленным броузером.

При публикации с помощью программы Citrix приложения помещаются на Web-сервер. Доступ к ним можно ограничить с помощью учетных записей пользователей или групп. Web-броузер — относительно небольшая программа, все вычисления выполняются на Web-сервере (который, в свою очередь, может получать доступ к базам данных или к серверам приложений), поэтому клиентский компьютер может быть "тонким".

Виртуальные машины Java

Java — это платформа разработки, в которой используется объектно-ориентированный язык программирования. Небольшие приложения Java — *аплеты* — могут быть написаны таким образом, чтобы они выполнялись на сервере.

В технологиях на основе Java можно использовать небольшие аплеты JavaScript, выполняемые на малопроизводительном клиентском компьютере или терминальном устройстве. Аплеты выполняет виртуальная машина Java. Машина Java может работать в различных операционных системах. Ею поддерживается многопоточность и компиляция по требованию программ Java, обеспечивающие высокое быстродействие.

В технологиях Java код приложения выгружается на клиентский компьютер по требованию. Там он хранится в кэше. Приложения могут выполнятся также броузером, оснащенным машиной Java, таким, как Netscape или Internet Explorer. На специализированных клиентских устройствах Java могут работать простые операционные системы Java и машины Java, хранящиеся в оперативной памяти или выгружаемые из сети.

Модель ASP

Концепция модели ASP (Application Service Provider — поставщик услуг выполнения приложений), в которой приложения предоставляются по требованию, тесно связана с технологиями тонких клиентов. Поставщик услуг управляет приложениями и делает их доступными для клиентов посредством скоростных сетевых соединений. В модели ASP выполняется также лицензионная поддержка программного обеспечения, модернизация и техническая поддержка приложений.

Модель ASP предоставляет существенные преимущества компаниям небольших и средних размеров, которые не могут содержать собственный отдел информационных технологий. Особенно она выгодна при использовании таких технологий Web, как, например, электронная коммерция. Вместо покупки программного обеспечения компания может арендовать его у ASP. Многие ASP используют технологию Web в качестве платформы распространения своих приложений.

Преимуществами предоставления приложений являются также возможность применения совершенных механизмов безопасности, реализуемых в центрах обработки данных, и повышенная отказоустойчивость системы благодаря избыточности оборудования у поставщика.

Инициатива Microsoft .NET

Компания Microsoft вложила немалые средства в разработку новой платформы программного обеспечения для Internet, получившей название Microsoft .NET и декларируемой как часть бизнес-плана компании на новое тысячелетие.

В технологии Microsoft .NET данные и приложения хранятся на серверах, доступных посредством Internet. Доступ к этим серверам можно будет получать из любой точки земного шара и с любого устройства. Широкое распространение Web-служб позволит унифицировать данные и развивать сотрудничество с любыми лицами и организациями, где бы они ни находились. Именно таким в Microsoft видят недалекое будущее сетей персональных компьютеров.

Основой модели Microsoft .NET служит язык XML (Extensible Markup Language). Этот язык способен обеспечивать коммуникацию между разными платформами и позволяет отделять представление данных от самих данных. Целью проекта является распространение данных на возможно более широкий диапазон устройств, таких, как беспроводные портативные устройства, объединяющие функции телефона, пейджера и персонального компьютера. Программы приложений будут распространяться как услуги и передаваться посредством Internet. Компания Microsoft уже объявила о планах разработки настольной платформы следующего поколения — Windows .NET (рабочее название "Whistler"), предназначенной специально для Internet.

Успех стратегии Microsoft .NET пока еще не очевиден, однако уже сейчас понятно, что в недалеком будущем сетевые технологии будут играть постоянно возрастающую роль в бизнесе, быту и повседневной жизни каждого человека.

Резюме

В этой главе концепция сетей с тонкими клиентами рассмотрена с нескольких точек зрения. Вы узнали, что тонкими клиентами могут быть малопроизводительные компьютеры и терминалы, оснащенные устройством ввода, экраном и соединением с сервером, на котором выполняются все вычисления.

Были рассмотрены преимущества сетей с тонкими клиентами и протоколы, используемые в коммуникации между тонкими клиентами и сервером приложений. Представлено оборудование тонких клиентов, включая устройства WBT, компьютеры NC и NPC, а также использование обычных настольных систем в качестве тонких клиентов Описано использование "очень тонких" клиентов — переносных и карманных персональных компьютеров, сообщающихся с сетью посредством беспроводных носителей и работающих под управлением компактных операционных систем, таких, как Windows CE.

Кроме того, представлено программное обеспечение тонких клиентов, включая такие продукты компании Microsoft, как Windows NT 4.0 Terminal Server Edition и Windows 2000 со встроенными терминальными службами. Рассмотрены программы Winframe и MetaFrame компании Citrix, интерфейс X Window, технологии Web и построение тонких клиентов на основе виртуальных машин Java.

В конце главы обсуждалась развивающаяся технология ASP и новейшая инициатива компании Microsoft — .NET, декларированная как стратегия компании в области Internet.

В последних главах рассматриваются многочисленные захватывающие новые технологии, но вы должны помнить, что все они основаны на высокой эффективности функционирования сети. В следующей главе акцентируется внимание на использовании инстру-

ментов мониторинга, управления и устранения неполадок в целях достижения максимально высокой производительности сетевых операций и реализации всех преимуществ, предоставляемых все более изощренными средствами сетевой коммуникации.

Рекомендуемые источники

Ссылки на информацию о многочисленных средствах реализации тонких клиентов можно найти на Web-узле Manchester Thin Client Computing по адресу: `www.mcc.ac.uk/thin/links.htm`.

Хороший источник новейшей информации о различных технологиях тонких клиентов — Web-узел Thin Planet по адресу: `www.thinplanet.com`.

Дополнительную информацию об операционной системе Windows 2000 Terminal Services можно найти по адресу: `www.microsoft.com/windows2000/guide/server/features/terminalsvcs.asp`.

Дополнительная информация о программе MetaFrame для Windows NT, Windows 2000 и UNIX есть на Web-узле компании Citrix по адресу: `www.citrix.com`.

Информация об интерфейсе X Window приведена по адресу: `www.x.org`.

Полезную статью о технологиях Java можно найти по адресу: `www.empowermentzone.com/javacomp.txt`.

Дополнительная информация о стратегии компании Microsoft в области Internet на двадцать первое столетие приведена по адресу: `www.microsoft.net/net`.

Прекрасный обзор терминальных служб — книга Теда Харвуда (Ted Harwood) *Windows NT Terminal Server and Citrix MetaFrame*, опубликованная издательством New Riders.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Что из приведенного является преимуществом тонких клиентов на основе персональных компьютеров по сравнению с мэйнфреймами? (Выберите все, что подходит.)
   - **а.** Сервер на основе персонального компьютера стоит дешевле, чем мэйнфрейм.
   - **б.** Персональный компьютер стоит дешевле, чем терминал мэйнфрейма.
   - **в.** Дополнительно к выполнению на сервере приложения могут выполняться на персональном компьютере локально.
   - **г.** Тонкие клиенты на основе персональных компьютеров не имеют преимуществ по сравнению с мэйнфреймами.
2. Какое из приведенных утверждений о технологии тонких клиентов справедливо?
   - **а.** Все пользователи должны иметь одинаковые параметры конфигурации и права доступа.
   - **б.** Использование терминалов затрудняет резервное копирование данных.
   - **в.** Администратор может контролировать или закрывать терминальный сеанс пользователя.

г. Модернизация приложений должна выполняться на каждом индивидуальном клиентском компьютере.

3. Какой из приведенных протоколов тонких клиентов используется для предоставления клиентам Macintosh или UNIX доступа к терминальному серверу Windows?
   а. RDP.
   б. ICA.
   в. X.
   г. DHCP.
4. Какое из приведенных утверждений о протоколе RDP справедливо? (Выберите все, что подходит.)
   а. Протокол RDP поддерживает печать через локальный порт LPT.
   б. Протокол RDP поддерживает сетевые/транспортные протоколы IPX/SPX, NetBEUI и TCP/IP.
   в. Протокол RDP поддерживает перенаправление порта COM.
   г. Протокол RDP поддерживает перенаправление буфера обмена.
5. Какой протокол используется для управления распределением ресурсов сервера X между пользователями терминалов X?
   а. X.
   б. LBX.
   в. XDMCP.
   г. RFB.
6. Что является целью стандарта PXE?
   а. Протокол PXE (Private X Exchange) используется для коммуникации между сервером X и клиентами Windows.
   б. Метод PXE (Preboot Execution Environment) используется для передачи кода начальной загрузки бездисковому терминалу.
   в. Протокол PXE (Protocol for Extended Encapsulation) используется для создания соединения VPN (Virtual Private Network) между тонким клиентом и сервером.
   г. Программа PXE (Private X Window Emulator) используется для предоставления интерфейса X пользователю системы Macintosh.
7. Какое из приведенных утверждений о технологии NC справедливо? (Выбрать все, что подходит.)
   а. Технология NC является патентованной и применяется только в операционной системе Sun Solaris.
   б. В технологии NC поддерживается выполнение аплетов Java.
   в. В технологии NC поддерживается стек протоколов TCP/IP
   г. На компьютерах NC установлены Web-броузеры, формирующие запросы HTTP и HTTPS.
8. В каком из приведенных режимов может работать система Windows 2000 Terminal Services? (Выбрать все, что подходит.)
   а. Режим удаленного администрирования.

б. Режим сервера приложений.

в. Режим локального доступа.

г. Режим виртуальной машины.

9. Какое из приведенных утверждений о программе MetaFrame компании Citrix справедливо? (Выбрать все, что подходит.)

   а. Программа MetaFrame предназначена для добавления в Windows 3.51.

   б. Программу MetaFrame можно использовать для переноса приложений на Web-сервер и предоставления к ним доступа из Web-броузеров.

   в. С помощью программы MetaFrame можно объединить много серверов в одну ферму серверов.

   г. В диалоговом окне Application Neighborhood программы MetaFrame можно управлять приложениями и создавать новые соединения ICA.

10. Какое из приведенных утверждений о технологиях Java справедливо?

   а. Аплеты Java выполняются на сервере, их не нужно выгружать на клиентский компьютер.

   б. Java — это стандартизированный язык программирования, реализации Java всех поставщиков идентичны.

   в. Виртуальная машина Java может выполняться только под управлением операционной системы UNIX.

   г. В технологии Java поддерживается многопоточность и компиляция по требованию, обеспечивающие высокое быстродействие.

Глава 18

Инструменты мониторинга, управления и устранения неполадок

На этом этапе изучения компьютерных сетей вы, видимо, уже поняли, что концепция сетей довольно проста, однако их реализация может быть очень сложной. Самые разнообразные неполадки могут возникать в любом месте сети. Вы, как сетевой администратор, должны быть постоянно готовы обнаружить, диагностировать и устранить любую угрозу нормальному функционированию сети.

Как известно, всегда лучше избежать неприятностей, чем потом устранять их последствия. Поэтому необходимо регулярно выполнять мониторинг сети для обнаружения и устранения потенциальных проблем. В корпоративной среде недостаточно лишь организовать коммуникацию компьютеров друг с другом. В современном деловом мире важным фактором является время, поэтому требуется достичь наиболее высокой производительности сети. Чтобы облегчить мониторинг, управление и устранение неполадок в локальных и глобальных сетях, разработано большое количество разнообразных инструментов — от простых утилит TCP/IP до изощренных программных пакетов независимых компаний и сетевых устройств.

Однако наиболее важен человеческий фактор. Часто сетевые администраторы смотрят на пользователей сети как на неприятеля: они ничего не умеют делать, а только вечно жалуются, плетут интриги и саботируют работу "идеальной" системы. Но следует помнить, что без пользователей само существование сети не имеет смысла. К тому же и сетевой администратор стал бы ненужным.

В этой главе рассматриваются основы анализа и оптимизации производительности, управления сетевыми службами и устранения наиболее распространенных проблем. Будут описаны сбор информации и утилиты устранения неполадок, включенные в пакет протоколов TCP/IP, а также программы и устройства, используемые для мониторинга и управления сетью.

В конце главы и этой части книги приведен список полезных советов, которые помогут правильно организовать процесс устранения неполадок.

Анализ и оптимизация производительности сети

Администрирование компьютерной сети — тяжелая и ответственная работа. Это справедливо независимо от того, работает ли сетевой администратор в отделе информационных технологий крупной компании или является единственным администратором небольшой локальной сети.

Обычно компания не допускает непроизводительных потерь времени персонала, обслуживающего сеть, поэтому администратору чаще всего приходится работать в *текущем* режиме, т.е. поддерживать эффективность работы сети и устранять проблемы по мере их возникновения. В таком режиме трудно найти время на углубленный анализ работы сети и прогнозирование возможных проблем.

И хотя вполне понятно, почему администратор вынужден работать в текущем режиме, в перспективе такой режим малоэффективен и чреват неприятными последствиями. Несмотря на загрузку текущими делами, администратор все же должен выделить время на разработку *активного* плана управления сетью. Такой план позволит обнаруживать небольшие проблемы, прежде чем они станут катастрофическими. Предвидя потенциальные угрозы эффективной работе сети и вовремя устраняя их, администратор сэкономит немало времени, предотвратит множество неприятностей, а порой даже сэкономит компании немалые деньги.

Рассмотрим ключевые понятия анализа и оптимизации сетевой производительности:

- узкие места;
- базовые уровни;
- положительный опыт.

Теперь рассмотрим каждое из этих понятий подробнее и обсудим другой важный фактор в оценке эффективности и оптимизации производительности сети — пропускную способность соединения с Internet. Также определим некоторые термины, необходимые для понимания способов мониторинга производительности.

Узкие места

Узкое место — это именно то, на что указывает название, т.е. точка в сети, ограничивающая пропускную способность или производительность всей сети. Узкое место ограничивает пропускную способность так же, как, например, горлышко бутылки ограничивает скорость вытекания из нее жидкости.

Узкое место может быть порождено неполадками в каком-либо компоненте или присущими ему ограничениями. Например, если в сети установлены концентраторы, коммутаторы и сетевые адаптеры, рассчитанные на 10/100 Мбит/с, но в качестве носителей используются витые пары категории 3, имеющие низкую пропускную способность, то узким местом становятся носители — именно они замедляют работу всей сети.

Подобрать все компоненты сети таким образом, чтобы каждый из них обеспечивал точно заданную пропускную способность, удается довольно редко. Поэтому возникает задача оптимизации производительности, состоящая в отыскании узких мест и их устранении путем модернизации, повторного конфигурирования или замены компонентов для повышения их производительности до уровня остальных компонентов сети. Однако если

этот процесс завершается успешно, то узкое место возникает на каком-либо другом участке. Поэтому устранить все узкие места не удается практически никогда

Базовые уровни

Первым шагом определения эффективности работы сети является сравнение различных показателей (таких, как количество битов, переданных в секунду, или количество пропущенных пакетов) с этими же показателями, полученными раньше. Улучшилась или ухудшилась производительность? Как повлияла на производительность реализация новой службы или применение новой программы? Единственный способ получить ответы на эти вопросы — сравнить новые показатели со старыми. Точкой отсчета для такого сравнения служит *базовый уровень*, представляющий собой допустимый уровень производительности системы при типичной рабочей нагрузке.

Измерение базовых показателей необходимо выполнять в процессе нормальной работы сети Не проводите измерения в самое напряженное время дня. Не ждите также, пока вечером все уйдут домой и сеть станет почти незагруженной Для установки базового уровня нужно определять производительность в типичном режиме работы Рекомендуется выполнить несколько отдельных измерений через определенные интервалы времени, а затем усреднить их

Кроме идентификации узких мест, заложенных в систему в процессе разработки, определение базовых уровней поможет·

- обнаружить активных пользователей;
- построить диаграмму использования сетевых ресурсов в течение дня, недели или месяца;
- определить загрузку отдельных участков сети;
- обосновать расходы на модернизацию сетевых компонентов

Рассмотрим, как это можно использовать для оптимизации производительности сети.

Обнаружение активных пользователей

Довольно часто оказывается, что всего несколько пользователей "потребляют" значительную часть общей пропускной способности Обнаружение таких активных пользователей позволит сделать следующее

- порекомендовать им способы экономного использования пропускной способности;
- ограничить загрузку каналов активными пользователями путем контроля их деятельности программными средствами;
- спланировать их пользование сетевыми каналами таким образом, чтобы уменьшить их влияние на других пользователей и общую производительность сети.

Естественно, характер принимаемых мер должен зависеть от характера задач, выполняемых активным пользователем, и его места в организации

Замечание

Некоторые сетевые приложения (например, программы резервного копирования или антивирусные сканеры сервера) тоже интенсивно загружают сеть Необходимо составлять их расписание таким образом, чтобы они выполнялись в периоды низкой загрузки сети

Диаграммы использования сетевых ресурсов

Мониторинг сети позволяет также создавать диаграммы использования пропускных способностей сетевых компонентов. Можно определить не только перегруженные компоненты, но и время их интенсивной загрузки. Это значительно облегчит распределение пропускных способностей в ожидаемые дни или часы пиковой загрузки и поможет более рационально составить расписание задач администрирования, установив их выполнение на время, когда они меньше всего влияют на работу пользователей.

Определение загрузки сети с помощью различных протоколов

Средства мониторинга сети (как программные, так и аппаратные) позволяют различать загрузку сети приложениями, использующими различные протоколы. Можно определить также, какие порты используются этими приложениями. Таким образом администратор может определить, как используются каналы — для поиска в Web или сетевыми играми.

Положительный опыт

Рекомендуемые, наиболее эффективные и экономные способы выполнения задач администрирования и других сетевых задач — это и есть *положительный опыт*. Например, поставщики средств мониторинга сети рекомендуют при определении базовых показателей сохранять перехваченные пакеты в отдельных файлах. Это позволяет подробно проанализировать их или передать профессиональному сетевому аналитику.

Средства мониторинга сети иногда называют *анализаторами протоколов*. Большинство анализаторов являются программными средствами, они позволяют перехватывать отдельные пакеты (кадры) в процессе их передачи по сети. Работа анализаторов более подробно описывается далее в главе. Объем статистических данных, собираемых для оценки производительности сети, не должен быть слишком большим, потому что используемые для этого программы мониторинга сами отрицательно влияют на работу сети. По этой же причине мониторинг следует выполнять в периоды низкой загрузки сети.

Определение пропускной способности соединения с Internet

Если сеть подключена к Internet, то часто оказывается полезным определение пропускной способности соединения. Если для соединения используется модем на 56 Кбит/с, это еще не означает, что пропускная способность соединения составляет 56 Кбит/с. В зависимости от состояния линии, реальная пропускная способность может оказаться, например, 50 Кбит/с или ниже. Некоторые провайдеры не позволяют устанавливать соединение ниже какой-то определенной пропускной способности, например 19,6 Кбит/с.

Скорость передачи данных может зависеть от применяемых средств сжатия данных, как программных, так и аппаратных. Сжатие делает возможным передачу со скоростью 112 Кбит/с посредством модема на 56 Кбит/с и аналоговой телефонной линии.

Пропускная скорость соединения ограничена пропускной способностью наиболее медленного компонента, т.е. узким местом. Если у абонента установлен модем на 33,6 Кбит/с, то вам не удастся превысить эту скорость, даже если ваше оборудование может поддерживать соединение на 50 Кбит/с.

Низкая пропускная способность соединения с Internet может быть вызвана следующими причинами:

- низкое качество соединения с сервером удаленного доступа провайдера, обусловленное проблемами с модемом на любом из концов, шумами в линии и т.д.;
- низкая производительность сервера FTP, Web или другого типа, которому передаются запросы;
- перегруженность магистральных каналов Internet вследствие событий национального или международного значения;
- уменьшение пропускной способности каналов вследствие их разделения с другими пользователями в локальной сети или в сети провайдера.

Довольно часто происходят кратковременные нерегулярные периоды пониженной производительности каналов Internet, и с этим ничего нельзя поделать. Если же пропускная способность соединения постоянно находится ниже допустимого уровня, следует подыскать другой тип подключения.

В операционных системах обычно есть компонент коммутированного соединения, с помощью которого можно посмотреть его пропускную способность, выраженную битами в секунду. Например, соединение с пропускной способностью 50 Кбит/с будет представлено как 50 000 бит/с. Однако это не всегда отражает фактическую скорость передачи данных, потому что измерение пропускной способности выполнено только в момент установки соединения с удаленным модемом. На протяжении сеанса соединения фактическая скорость передачи может существенно изменяться.

Замечание

Скорость передачи данных можно вывести как *скорость порта* (т.е. скорость соединения модем–компьютер, учитывая сжатие данных) или как *фактическую скорость соединения* (т е. соединения модем–модем). В операционной системе Windows можно вывести на экран любую из этих скоростей

Из Internet можно загрузить какой-либо файл и в процессе его передачи с помощью броузера или программы FTP наблюдать скорость его загрузки Величина скорости часто выводится на экран в килобайтах в секунду. В байте содержится 8 бит, поэтому скорость передачи 50 Кбит/с будет выглядеть как 6,25 Кбайт/с.

В Internet есть несколько Web-узлов, предназначенных специально для измерения скорости загрузки данных. Однако для разных узлов результаты измерения могут немного отличаться Необходимо также учитывать, что на скорость загрузки влияет наличие служебных сигналов протокола HTTP (Hypertext Transfer Protocol). Для практических целей точность измерения чаще всего вполне приемлема Перечислим некоторые Web-узлы, предназначенные для измерения пропускной способности соединений.

- **MSN Speedtest** (`http://computingcentral.msn.com/topics/bandwidth/speedtest50.asp`).
- **Telus.net High-Speed Internet** (`http://speedtest.mybc.com`).
- **Toast.net Internet Service** (`http://www.toast.net`).

Инструменты мониторинга и управления сетью

К настоящему времени разработано много программных пакетов, предназначенных для мониторинга и управления сетью. Некоторые из них включены в сетевые операционные системы, другие можно загрузить из Web бесплатно или практически бесплатно. Есть также весьма изощренные и дорогие пакеты.

Рассмотрим наиболее популярные программы мониторинга и управления сетями, а также поставщиков услуг управления сетями, с которыми можно заключить контракт на управление конкретной сетью.

Программы мониторинга сети

Программное обеспечение мониторинга сетей может быть простым или сложным, бесплатным или довольно дорогим. Инструменты мониторинга встроены во многие современные операционные системы, такие, как Windows NT и Windows 2000. Они проще и обладают меньшими функциональными возможностями, чем программы мониторинга независимых поставщиков, однако они вполне пригодны для определения базовых показателей производительности или диагностирования и устранения неполадок в сети.

Даже в Windows 95 есть встроенные простые инструменты мониторинга, например Net Watcher (рис. 18.1).

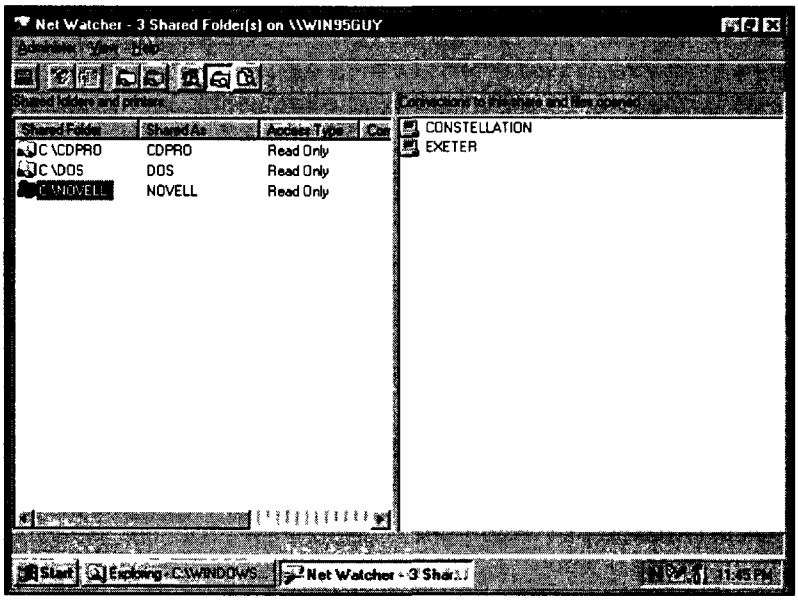


Рис. 18.1. Операционная система Windows 95 содержит дополнительный инструмент мониторинга Net Watcher

Более сложные инструменты мониторинга сетей называются анализаторами протоколов. Они перехватывают пакеты (кадры), передаваемые между компьютерами или сетевыми устройствами. Затем анализаторы декодируют (интерпретируют) перехва-

ченные пакеты, т.е. преобразуют их из двоичного формата к виду, пригодному для анализа человеком. Существуют анализаторы протоколов, предоставляющие статистическую информацию о перехваченных пакетах.

Программы, с помощью которых можно "подслушивать" передаваемую по сети информацию, называются *sniffer* ("сетевые нюхачи"). Компания Network Associates поставляет программу Sniffer и ее расширенную версию Sniffer Pro. Обе эти программы являются сетевыми анализаторами.

В некоторых кругах эти средства имеют плохую репутацию, потому что с их помощью хакеры извлекают имена пользователей и пароли, передаваемые по сети в незашифрованном виде. Перехваченная таким образом регистрационная информация затем используется для получения несанкционированного доступа к системе. Однако анализаторы могут быть полезными и для сетевых администраторов, например в следующих случаях:

- анализ неполадок в соединениях;
- анализ производительности;
- обнаружение вторжений.

Рассмотрим программы Microsoft Performance Monitor и Microsoft System Monitor подробнее, а затем обсудим некоторые программы независимых разработчиков, такие, как Sniffer Pro и LANalyzer компании Novell.

Программы Microsoft Performance Monitor и Microsoft System Monitor

С помощью встроенной в Windows NT 4.0 программы Performance Monitor (в Windows 2000 она называется System Monitor) можно измерять производительность многих системных компонентов, в частности выводить на экран показания счетчиков сетевых компонентов.

Эта программа позволяет выводить данные в графическом формате, сохранять их в журнале и составлять по ним отчеты. Измерения можно просматривать в реальном времени, обновлять их автоматически или по требованию.

На рис. 18.2 показано, как программа System Monitor в Windows 2000 используется для измерения количества пакетов в секунду, переданных или принятых в процессе копирования файла посредством сети.

В программах Performance Monitor и System Monitor можно конфигурировать оповещения, т.е. установить автоматическое уведомление администратора при наступлении некоторого события; например, если заданный параметр производительности достигнет определенного верхнего или нижнего уровня.

Для обнаружения узких мест следует выполнять мониторинг следующих счетчиков сетевых интерфейсов:

- общее количество байт в секунду;
- количество переданных байт в секунду;
- количество принятых байт в секунду.

Полезен также мониторинг следующих счетчиков:

- количество сегментов, принятых в секунду;
- количество сегментов, переданных в секунду;

- количество кадров, принятых в секунду;
- количество кадров, переданных в секунду.

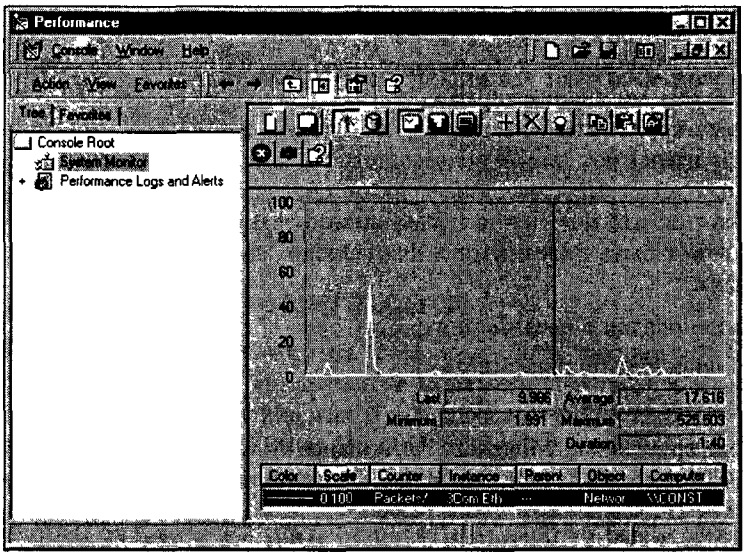


Рис. 18 2. Программа System Monitor, встроенная в Windows 2000, используется для измерения производительности сети

Мониторинг этих счетчиков помогает правильно спланировать распределение пропускной способности. Например, если общее количество переданных байт в секунду близко или равно пропускной способности сетевого носителя, то следует рассмотреть возможности его модернизации (например, замены кабелей Ethernet 10 на Ethernet 100) или уменьшения рабочей загрузки сети.

Программа Microsoft Network Monitor

С помощью программы System Monitor можно измерять сетевые показатели, имеющие отношение к производительности. Однако с ее помощью нельзя перехватить передаваемые по сети пакеты, а затем проанализировать их Для этого необходимо использовать другие инструменты. В состав Windows NT 4.0 и Windows 2000 включена облегченная версия Microsoft Network Monitor, являющаяся частью программы SMS (System Management Server) компании Microsoft. Программа SMS рассматривается далее в главе.

Программа Network Monitor, поставляемая в составе Windows NT и Windows 2000, — весьма полезный инструмент с богатыми функциональными возможностями. Она предназначена для анализа работы процедур протоколов. На рис. 18.3 показано, как Network Monitor применяется для мониторинга использования пропускной способности сети, измерения количества кадров в секунду и получения дополнительной статистической информации о работе сети.

На рис. 18.4 показано, как программу Network Monitor можно использовать для вывода отдельных кадров перехваченных данных. Обратите внимание: перехвачены пакеты нескольких различных протоколов, включая TCP, UDP и SMB.

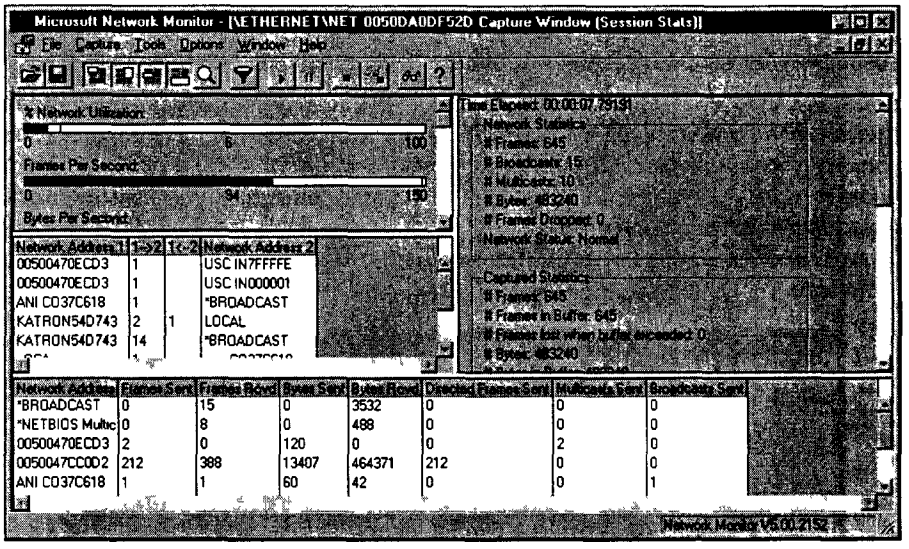


Рис 18 3 Компания Microsoft включила в состав операционных систем Windows NT/2000 облегченную версию Network Monitor

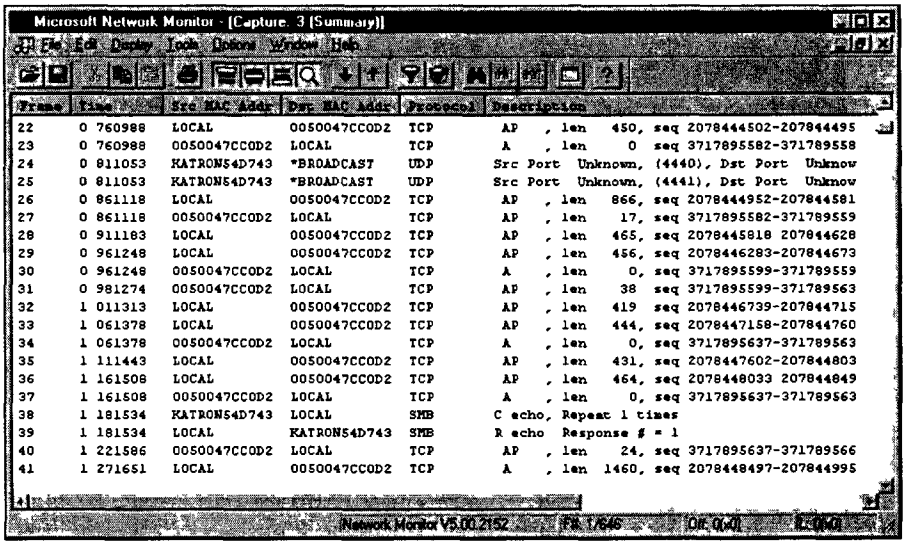


Рис 18 4 Перехваченные с помощью Network Monitor данные можно проанализировать на уровне отдельных кадров

Программы-анализаторы

Популярный сетевой анализатор Sniffer со временем вырос в сложный набор сетевых инструментов, в состав которого входят следующие средства

- Sniffer Pro LAN и Sniffer Pro WAN,
- Sniffer Pro High-Speed,

- Gigabit Sniffer Pro;
- набор Sniffer Distributed Analysis Suite.

С помощью этих средств можно выполнять утонченную фильтрацию на основе сопоставления образцов, адресов TCP/IP или DLC. В состав Sniffer Pro входит генератор загрузки сети, облегчающий тестирование новых устройств и приложений. Его можно использовать для моделирования сетевой нагрузки, определения времени ответа и подсчета количества ретрансляций.

Как показано на рис. 18.5, в Sniffer используется интерфейс, имеющий вид приборной панели.

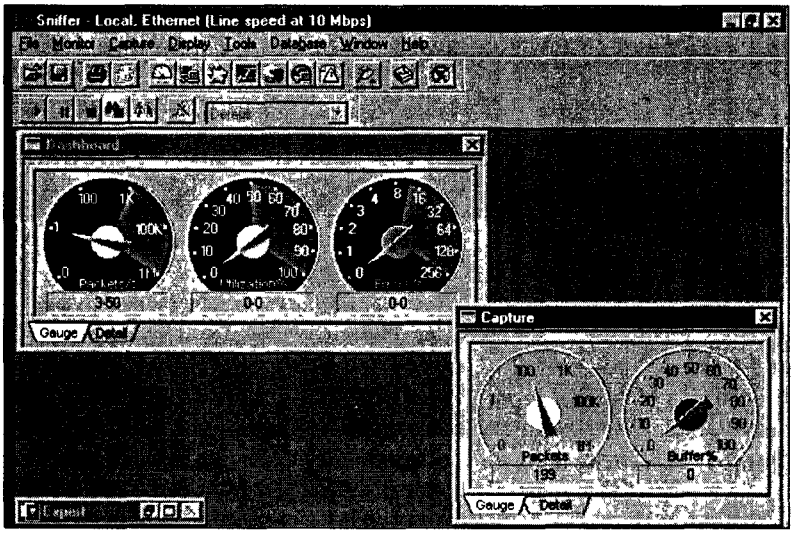


Рис. 18.5. В программе Sniffer Pro перехваченная информация отображается с помощью интерфейса, напоминающего приборную панель

В программы Sniffer встроены такие утилиты TCP/IP, как `ping`, `tracert`, просмотра DNS (Domain Name System) и др. Предусмотрено гибкое конфигурирование формата вывода программ Sniffer. Вывод информации о пакетах и распределении протоколов показан (в виде диаграмм) на рис. 18.6.

В состав Sniffer входит программа Expert Analyzer, облегчающая диагностирование сетевых неполадок. Можно запустить одновременно несколько экземпляров этой программы или использовать только ее отдельные инструменты.

Программа LANalyzer компании Novell

Программа LANalyzer, выполняющаяся под управлением Windows, содержит базовые инструменты мониторинга и устранения неполадок в сетях Ethernet и Token Ring. Кроме перехвата пакетов, программа может выдавать конкретные рекомендации по устранению неполадок и оптимизации производительности сети.

Программа LANalyzer поддерживает службы NDS (Novell Directory Services). Она может работать с NetWare, AppleTalk, NFS, SNA и TCP/IP. Графический интерфейс LANalyzer, как и в Sniffer Pro, похож на приборную панель. Сетевые компоненты идентифицируются в программе именами и MAC-адресами.

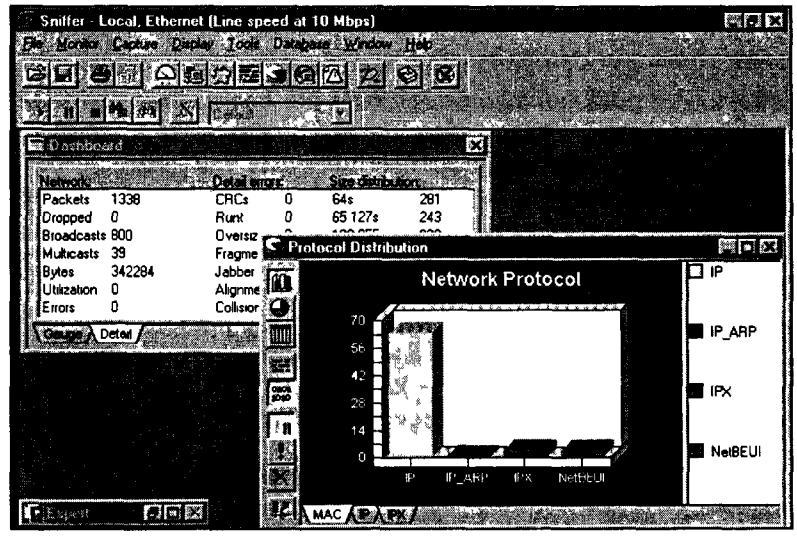


Рис 18 6 Формат вывода Sniffer Pro можно сконфигурировать так, как удобно пользователю

Программы управления сетями

Какая разница между программами мониторинга и программами управления сетями? Программы управления более полные, в них включены не только компоненты мониторинга, но и много других средств

Задачи управления сетью составляют значительную часть работы сетевого администратора. Это особенно справедливо для корпоративных сетей Сетевой администратор должен хорошо знать инструменты, упрощающие выполнение этих задач, включая средства, встроенные в современные сетевые операционные системы, и программные продукты, предоставляемые поставщиками операционных систем и другими производителями

Управление сетью предполагает выполнение ряда задач

- Документирование устройств сети и статуса каждого из них.
- Создание списка сетевых программ, что значительно облегчает их установку и модернизацию
- Измерение рабочих показателей программ, т е получение данных о том, какие приложения используются, как, когда и кем
- Решение вопросов, связанных с лицензированием программного обеспечения
- Удаленный контроль посредством сети клиентских компьютеров и серверов Управление удаленными рабочими столами.
- Оповещение администрации о существенных событиях, таких, как выход из строя сетевых компонентов или заполнение дисков до предельно допустимого уровня

Существует несколько программ управления сетями (точнее, наборов программ) Рассмотрим наиболее популярные из них, включая следующие·

- SMS компании Microsoft,
- ManageWise компании Novell;

- Tivoli Enterprise компании IBM;
- OpenView компании Hewlett Packard.

Эти программы разрабатывались для управления большими корпоративными сетями со многим узлами.

Рассмотрим также программы, предназначенные для управления небольшими или средними локальными сетями, включая LANErplorer и Network Monitoring Suite компании Lanware.

Программа SMS компании Microsoft

Пакет программ SMS (Systems Management Server) представляет собой мощное средство управления сетями, с помощью которого можно получать списки оборудования и программного обеспечения (рис. 18.7), выполнять удаленную диагностику, контролировать удаленные рабочие столы и установку программного обеспечения.

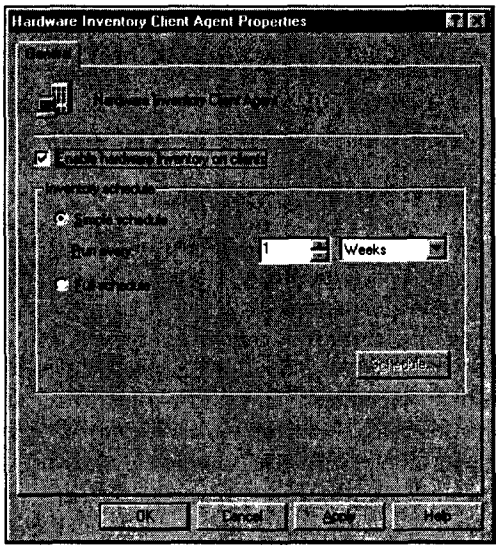


Рис. 18.7. Программа SMS позволяет собирать информацию об оборудовании путем установки на целевых компьютерах клиентских агентов

В состав SMS также включена более полная версия программы Network Monitor компании Microsoft, чем встроенная в операционные системы Windows NT/2000. Например, в Network Monitor программы SMS добавлены возможности поиска маршрутизаторов сети и разрешения имен.

Один из наиболее полезных инструментов программы SMS — встроенные в нее средства распространения программного обеспечения. С их помощью можно создать *пакет распространения*. Пакет содержит информацию, используемую SMS для координации распространения программного обеспечения (рис. 18.8).

Для хранения данных в SMS используется СУБД SQL Sever. Поэтому данные можно легко экспортировать в Microsoft Access. Программой SMS поддерживаются клиенты Macintosh. Кроме того, ее легко интегрировать в среду NDS (Novell Directory Services).

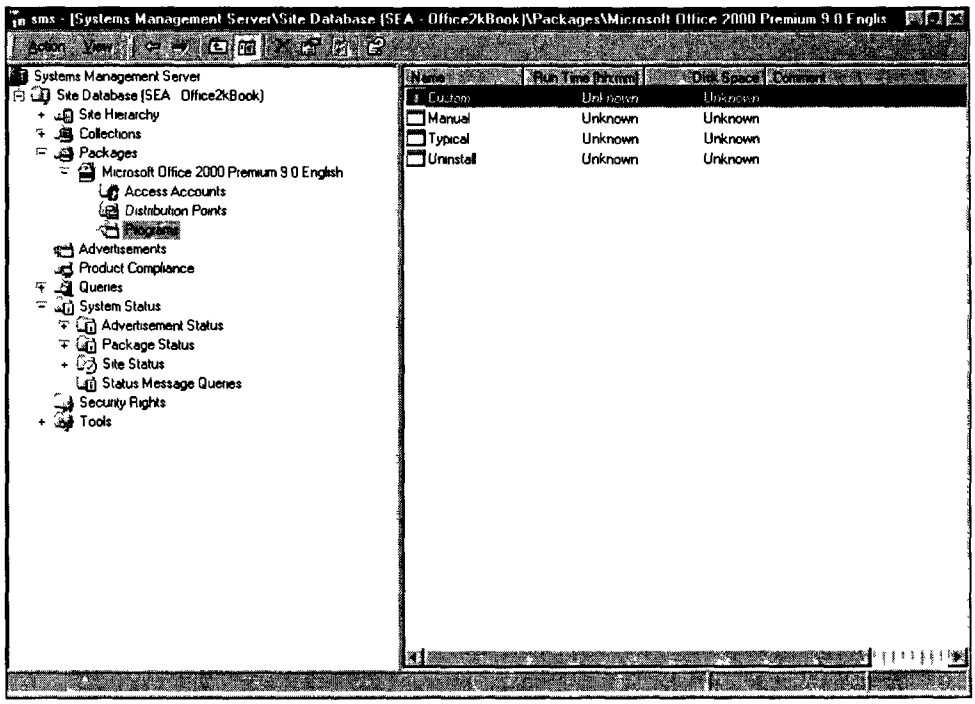


Рис 18 8 В программе SMS пакеты распространения используются для развертывания программного обеспечения коммерческой сети

Программа ManageWise компании Novell

Программа ManageWise представляет собой интегрированную группу служебных программ управления сетями. Ее можно использовать для управления серверами NetWare или, с добавлением дополнительных агентов, серверами Windows NT В ее состав входят компоненты контроля рабочих станций и серверов, анализа сетевой нагрузки и администрирования сетевых приложений. На рис. 18.9 показано рабочее окно программы ManageWise.

Как и SMS, программа ManageWise может создавать и выводить список сетевых устройств Кроме того, в нее дополнительно включены средства оповещения В программу ManageWise включены также агент LANalyzer для сетей NetWare, агент управления, программа LANDesk компании Intel, средства антивирусной защиты, входящие в состав программы LANDesk, и программа Desktop Manager (последняя показана на рис 18 10).

С помощью Desktop Manager можно просматривать списки оборудования и программного обеспечения компьютера пользователя, передавать файлы в обоих направлениях, выполнять удаленный контроль рабочего стола пользователя, "беседовать" с ним и перезагружать его компьютер

Программа Tivoli Enterprise компании IBM

Это популярный пакет программ управления сетями, в состав которого включены инструменты управления оборудованием, доступом к ресурсам, изменениями, приложениями, средствами безопасности, службами и конфигурацией хранения данных. В

программе предусмотрена несложная поэтапная реализация перечисленных компонентов управления.

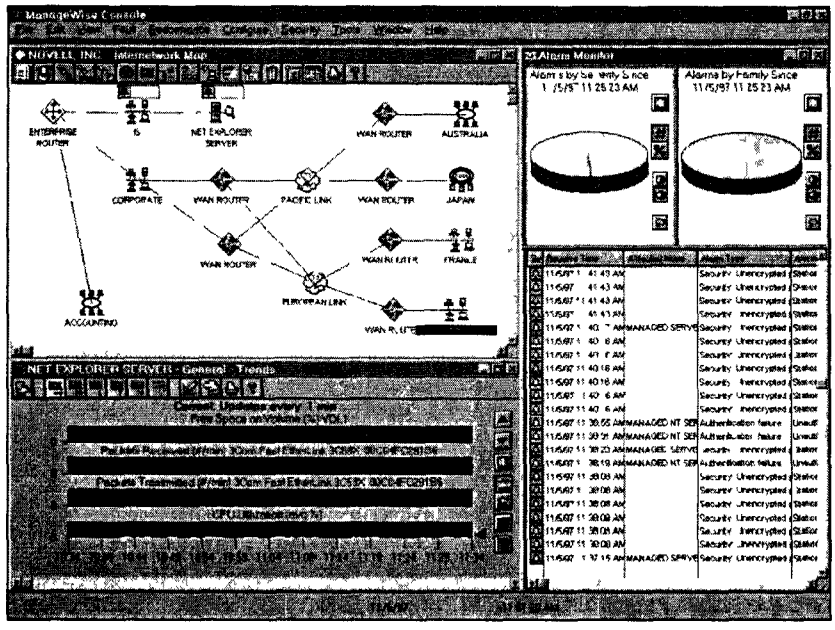


Рис. 18 9. В состав программы ManageWise включены средства отображения структуры сети

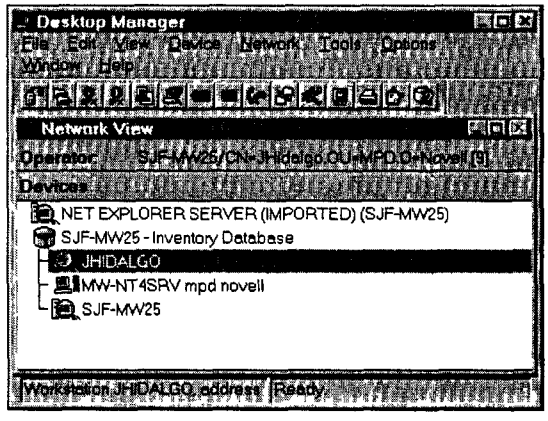


Рис 18 10 Программа Desktop Manager пакета ManageWise предоставляет графический интерфейс, облегчающий выполнение задач управления сетью

С помощью Tivoli Enterprise можно просматривать полную топологию сети. Средства создания отчетов позволяют настраивать вид представления данных. Программа позволяет создавать "интеллектуальные наборы", в которых данные сгруппированы логически. Это существенно облегчает анализ состояния сети (рис. 18.11).

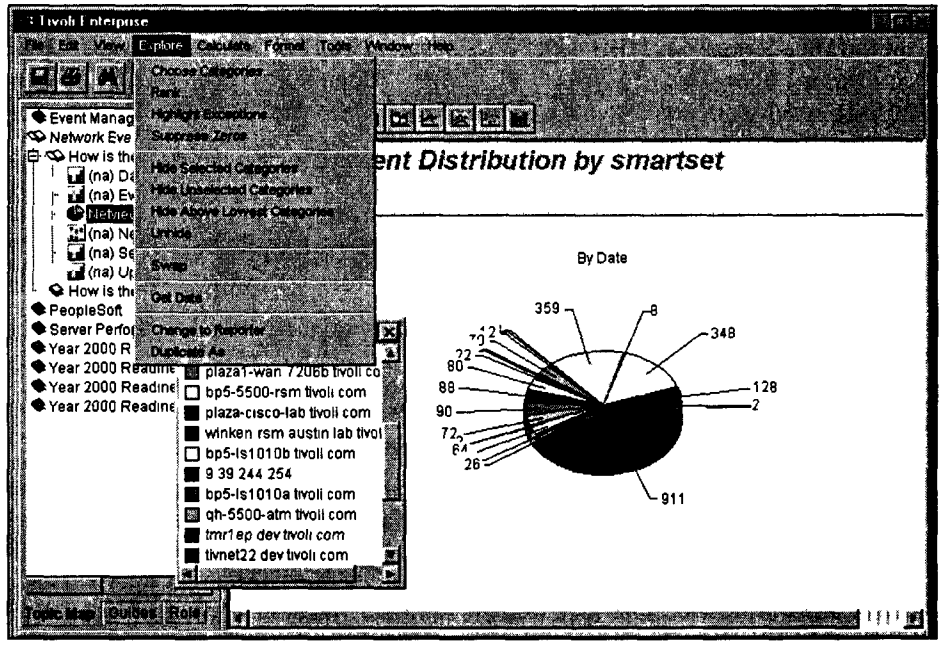


Рис 18.11. В программе Tivoli Enterprise можно настраивать способ представления собранной информации

Существуют версии Tivoli для небольших компаний и организаций средних размеров.

Программа OpenView компании Hewlett Packard

В программу OpenView включены инструменты управления большими сетями (OpenView Enterprise) и сетями средних размеров (OpenView Express). Программа OpenView Enterprise разработана для сетей, в состав которых входят тысячи серверов и более 5 000 рабочих станций под управлением сетевых операционных систем Windows NT/2000 или UNIX. Программа OpenView Express предоставляет средства управления Web-серверами, почтовыми серверами Exchange и гибридными сетями на основе Windows NT/2000.

В состав OpenView входит компонент ManageX, позволяющий управлять серверами и производительностью в среде NT и NetWare.

Программы управления небольшими сетями и сетями средних размеров

Кроме программ управления сетями, предоставляемых основными поставщиками программного обеспечения, такими, как Microsoft, Novell, IBM и Hewlett Packard, существуют программы, разработанные многочисленными небольшими компаниями и предназначенные для сетей небольших и средних размеров. К ним относится программа NMS (Network Monitoring Suite) компании Lanware, в которой используется протокол SNMP (Simple Network Management Protocol) Программа NMS предоставляет такие возможности, как повторный запуск служебных программ, составление расписаний и перезагрузка серверов. Программа ViewLAN ком-

пании NuLink — еще один пример относительно простой программы управления и мониторинга на основе SNMP.

Рассмотрим протоколы SNMP и CMIP (Common Management Information Protocol), на которых основаны эти простые программы управления.

SNMP

Утилита SNMP включена в большинство реализаций протокола TCP/IP. Ее использование в задачах сетевого управления предоставляет несколько преимуществ.

- Простота.
- Дешевизна.
- Простота реализации.
- Небольшое количество служебных сигналов, передаваемых по сети.
- Поддержка большинством сетевых устройств.

Для организации информации, собранной о сети, в протоколе SNMP используется иерархическая база данных MIB (Management Information Base). Диспетчер SNMP устанавливается на хостирующем компьютере, используемом для сбора данных. На сетевых компьютерах, о которых собираются данные, устанавливаются программы агентов SNMP. Существуют бесплатные версии как диспетчеров, так и агентов SNMP для различных операционных систем.

CMIP

Протокол CMIP разработан в целях улучшения SNMP и расширения его функциональных возможностей. Принципы его работы аналогичны SNMP, однако в CMIP заложены усиленные средства безопасности и средства извещения о наступлении определенных событий.

В протоколе CMIP используется значительно больше служебных сигналов, чем в SNMP, поэтому он менее распространен. Основой CMIP служит набор протоколов OSI, в то же время SNMP рассматривается как часть набора TCP/IP.

Провайдеры услуг управления

В главе 17, "Сети с тонкими клиентами", рассматривались провайдеры услуг приложений — компании, распространяющие и обслуживающие сетевое программное обеспечение. Провайдеров услуг управления можно рассматривать как развитие этой тенденции.

Компания может подписаться на обслуживание провайдером услуг управления, который в этом случае берет на себя мониторинг производительности и управление сетью. Это экономит компании деньги на покупку и установку программ мониторинга и управления и на обучение персонала.

Примером компании, предоставляющей услуги внешнего управления сетями, является Luminate.Net. Для коммуникации с заказчиками посредством Internet эта компания предоставляет Web-интерфейс.

Устройства мониторинга и устранения неполадок

Большинство устройств, используемых для сетевого мониторинга и управления, являются всего лишь выделенными компьютерами (часто портативными), на которых запускаются программы анализа протоколов и сетевого управления. Однако существуют и специальные устройства, полезные при устранении неполадок в сети. Перечислим некоторые из них.

- **Тональный генератор/локатор**. Иногда это устройство называют *fox and hound* (*лиса и собака*). Устройство, называемое "лисой" и подключаемое к одному из концов кабеля, генерирует тональный сигнал. На другом конце кабеля сигнал принимает локатор ("собака"). На основе параметров принятого сигнала диагностируется состояние кабеля.
- **Перекрученный кабель**. Представляет собой неэкранированную витую пару Ethernet, в которой пары проводников соединены "крест на крест". В нормальной паре контакт 1 на одном конце подключен к контакту 1 на другом конце, а контакт 2 — к контакту 2. В перекрученном кабеле контакты 1 и 2 подключены к контактам 3 и 6 на другом конце, а контакты 3 и 6 — к контактам 1 и 2. Перекрученный кабель используется для объединения двух компьютеров без концентратора или объединения двух концентраторов, не имеющих специальных выделенных портов связи.
- **Рефлектометр TDR (Time Domain Reflectometer)**. Это устройство передает в кабель зондирующий импульс и принимает его отражение. На основе параметров принятого импульса устройство обнаруживает и локализует короткие замыкания и разрывы кабеля.
- **Аппаратная петля**. Подключается к последовательному порту компьютера. Пройдя по петле, тестирующие сигналы возвращаются на этот же компьютер. Это позволяет диагностировать последовательный порт без подключения к нему модема или другого устройства.
- **Цифровой тестер (вольтметр/омметр)**. Используется для измерения сигналов, передаваемых по кабелю, и обнаружения коротких замыканий и разрывов в кабеле.
- **Осциллограф**. Используется для калибровки электронных схем и определения параметров импульсов (амплитуды, длительности и крутизны фронтов), передаваемых по кабелю. На экране осциллографа видна форма импульсов. С его помощью можно определять короткие замыкания и разрывы кабеля, скрутки проводов и затухание сигналов.
- **Измеритель параметров локальных сетей**. С помощью этого устройства можно проверять широковещательные сигналы и уровень загрузки каналов, обнаруживать коллизии и ошибки данных в локальных сетях Ethernet и Token Ring, измерять объем данных, передаваемых по глобальным каналам, а также идентифицировать устройства, подключенные к сети.

Устранение неполадок в сетях

Несмотря на все принятые меры, в качестве сетевого администратора вам неизбежно придется сталкиваться с различными неполадками. Они могут варьировать от постепенного понижения производительности, раздражающего пользователей, до полного разрыва соединений по всей сети, в результате чего тысячи служащих вынуждены прекратить свою работу.

Для устранения сетевых неполадок могут быть использованы любые рассмотренные в предыдущих разделах программы и устройства. Большинство современных сетей работают в протоколе TCP/IP, поэтому для устранения неполадок можно воспользоваться предоставленными этим протоколом утилитами. Чтобы воспользоваться ими, не нужно покупать, устанавливать и изучать сложные и дорогие программы управления сетями.

Рассмотрим основы устранения неполадок, а также использование файлов журналов и различных инструментов и утилит, включенных в большинство реализаций TCP/IP. Кроме того, рассмотрим, как их можно использовать для устранения неполадок в сетевых соединениях. В конце главы приводится подробный список рекомендаций по устранению сетевых неполадок, который поможет вам отслеживать и решать проблемы сетевых соединений и производительности каналов.

Основы устранения неполадок

Базовая сетевая проблема — отсутствие соединения одного компьютера с другим. Возможны многие причины потери соединения, однако любая из них состоит в неполадках оборудования и/или программного обеспечения.

Первый шаг устранения неполадки — проверка физического соединения. Не пренебрегайте этим простым правилом. Нередки случаи, когда специалист по сетям тратит много часов на реконфигурирование протоколов, повторную установку программ или даже операционных систем, обнаруживая в конце концов, что кто-то всего лишь вытащил кабель из разъема сетевого адаптера. Следовательно, начиная сложный процесс устранения неполадки, убедитесь прежде всего, что все кабели подключены на *обоих* концах, что сетевой адаптер работает (проверьте, горят ли индикаторы на нем) и что горят лампочки состояния концентратора. Другими словами, убедитесь, что причиной отсутствия соединения не является какая-либо простая неисправность оборудования.

Другую распространенную причину сетевой неполадки иногда вежливо называют "ошибкой оператора". Если на клиентском компьютере не удается увидеть остальную часть сети, то, возможно, пользователь зарегистрировался только на локальном компьютере, но не в сети. Необходимо убедиться, что пользователи применяют правильные имена пользователей и пароли, а их учетные записи не ограничены таким образом, что установка соединения с сетью невозможна. Например, допустимое время регистрации может быть ограничено рабочим временем дня или пользователь может зарегистрироваться только на определенном компьютере.

Замечание

Одна из распространенных причин "неисправности" пароля — его чувствительность к регистру символов в большинстве операционных систем. Случайное нажатие клавиши <Caps Lock> перед вводом пароля влечет отказ в регистрации. Пользовательские пароли чувствительны к регистру символов даже в операционных системах, в которых файловая система нечувствительна к регистру, например в Windows.

Неполадки оборудования относительно простые, обнаружить их можно довольно быстро. Обнаружив неисправность, необходимо выключить или отключить устройство, а затем отремонтировать его или заменить исправным.

Найти причину неполадок в программном обеспечении значительно труднее. Наиболее частой причиной является неправильная конфигурация программ. Параметры конфигурации могут оказаться измененными процедурами установки какой-то программы. Возможно, пользователи экспериментировали с конфигурацией. Отсутствующие или испорченные файлы могут вызвать самые разнообразные проблемы, включая нарушение сетевых соединений. Пользователи могут случайно или умышленно удалить файлы. В результате скачков напряжения или неправильного завершения сеанса работы компьютера файлы данных могут оказаться поврежденными. Нельзя также упускать из виду возможность повреждения файлов вирусом.

Независимо от предполагаемого источника неполадок, приведенные ниже этапы их диагностики и устранения покрывают практически все возможные причины Программа сертификации Network+ рекомендует такую последовательность этапов устранения неполадок.

1. Четко определите проблему, соберите о ней как можно больше информации.
2. Попытайтесь воссоздать ее. Определите, можно ли воссоздать проблему на другом компьютере или она возникает только на этом компьютере.
3. Попытайтесь изолировать причину проблемы. Сформулируйте возможные причины и устраните их одну за другой.
4. На основе предыдущего опыта и проведенного анализа сформулируйте способ исправления неполадки.
5. Составьте и реализуйте план исправления
6. Проверьте, работает ли план исправления.
7. Документируйте проблему и план ее исправления для использования в будущем В документацию следует включить журнал любых изменений конфигурации.
8. Обсудите решение проблемы с пользователями.

Первые шесть этапов вполне соответствуют здравому смыслу и не вызывают возражений ни у кого. В то же время этапы 7 и 8 опускают даже многие специалисты по сетям. Они считают, что когда проблема решена, ее можно оставить и забыть о ней Тем не менее в сетевой среде последние два этапа весьма существенны

Потратив несколько дней на решение проблемы и в конце концов решив ее, человек полагает, что он никогда не забудет этих мучительных поисков и гениальных догадок. Однако жизнь сетевого администратора заполнена весьма плотно. Если эта же проблема возникнет через год, то, скорее всего, он вспомнит лишь то, что *когда-то это уже происходило и как-то было решено* Сохранившаяся документация этапов решения сэкономит не только время и деньги компании, но и ваши нервы

Обсуждение проблемы с пользователями не менее существенно Не упускайте возможность повысить их квалификацию. Это ключевой элемент предотвращения проблем. Вам может показаться, что пользователям безразлично, в чем причина неполадок, лишь бы все работало нормально. Тем не менее многие высоко ценят полезную информацию, особенно если она помогает им скорректировать их приемы работы или

уловить признаки нависающих проблем, чтобы вовремя предотвратить их, пока они не выросли в крупные неприятности. Общаясь с пользователями, говорите на их языке, постарайтесь правильно учесть уровень их технической подготовки.

Замечание

Обсуждая с пользователями какую-либо проблему, постарайтесь, чтобы они поняли, что нужно делать, если проблема возникнет опять. Если проблема простая и, на ваш взгляд, пользователь может справиться с ней самостоятельно, дайте ему подробную инструкцию, что он должен сделать, лучше даже письменную. Или, по крайней мере, ясно дайте ему понять, что вы лишь предоставляете информацию и политика компании состоит в том, чтобы пользователи немедленно извещали вас при возникновении проблемы.

Использование файлов системного журнала

В большинстве операционных систем предусмотрены средства автоматической записи в журнал операционной системы таких событий, как отказы устройств, неудачные попытки установки соединения и другие ошибки. Эта информация весьма полезна в качестве начальной точки процесса устранения неполадки. Например, в Windows NT/2000 есть программа Event Viewer, с помощью которой можно просматривать список системных событий (рис. 18.12).

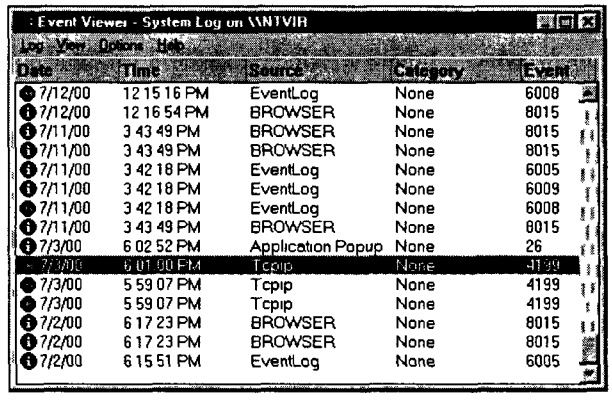


Рис. 18.12. Программа Event Viewer операционной системы Windows NT Server выводит список возникших ошибок

Выбрав конкретное событие (например, ошибку TCP/IP, как показано на рис. 18.12), можно получить о нем более подробную информацию (рис. 18.13). В данном примере система сообщает, что произошел конфликт IP-адреса, в результате чего компьютер не может сообщаться с сетью.

В других операционных системах тоже есть средства записи в журнал. В системе NetWare журналом ошибок сервера служит файл `SYS$LOG.ERR`. Файл `CONSOLE.LOG` содержит ошибки и сообщения, выводившиеся в процессе работы сервера. В системе NetWare есть также журнал `ABEND.LOG`, в котором записаны события Abnormal End, повлекшие завершение какой-либо программы или закрытие модуля NLM (NetWare Loadable Module).

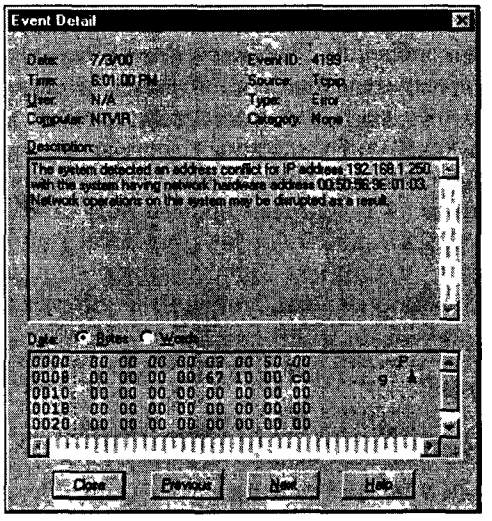


Рис 18 13 Выбрав конкретное событие, можно получить подробную информацию о нем

Использование утилит TCP/IP

В состав большинства реализаций TCP/IP включен набор утилит, которые можно использовать для сбора информации, проверки соединений и устранения сетевых неполадок. В разных реализациях TCP/IP они могут иметь разные имена и обладать разными функциональными возможностями.

Рассмотрим несколько категорий утилит TCP/IP: предназначенные для тестирования соединений, для конфигурирования и для устранения неполадок в сетях.

Утилиты тестирования соединений

При восстановлении прерванного соединения в первую очередь нужно определить, действительно ли оно разорвано. Когда в диалоговом окне Network Neighborhood (Сетевое окружение) неопытный пользователь не видит имя сервера, он немедленно приходит к выводу, что прервано соединение с сервером. Довольно часто это всего лишь ошибка процедуры просмотра: сервер не регистрирует себя на компьютере, отслеживающем сетевые ресурсы и выводящем их в список просмотра. Если при этом попытаться получить доступ к серверу путем ввода пути в формате UNC (Universal Naming Convention), то окажется, что соединение вполне работоспособно.

Проверить соединение с другим компьютером и определить маршрут, по которому прошел пакет данных, можно с помощью следующих инструментов TCP/IP:

- команды `ping` и `pathping`;
- утилиты отслеживания (трассировки).

Команды ping и pathping

Сокращение *ping* означает *packet internetwork groper*. Эта команда представляет собой простую утилиту, передающую на выбранный целевой компьютер сообщение Echo

Request с помощью протокола ICMP (Internet Control Message Protocol). Целевой компьютер передает обратно сообщение Echo Reply тоже с помощью протокола ICMP.

При тестировании подозрительного соединения в первую очередь нужно подать команду `ping` на какой-либо хост. Это делается для проверки соединения с Internet, поэтому нужно выбрать какой-либо надежный хост, например `www.yahoo.com`. Если ответ получен, значит, физическое соединение между двумя компьютерами вполне работоспособно. В листинге 18.1 приведен пример подачи команды `ping` и полученный на нее ответ.

Листинг 18.1. Команда `ping` используется для тестирования соединения между двумя компьютерами

```
G:\>ping www.yahoo.com

Pinging www.yahoo.akadns.net [216.32.74.52] with 32 bytes of data:

Reply form 216.32.74.52: bytes=32 time=110ms TTL=241
Reply form 216.32.74.52: bytes=32 time=141ms TTL=241
Reply form 216.32.74.52: bytes=32 time=100ms TTL=241
Reply form 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
```

Команду `ping` можно выполнять как с IP-адресом, так и с именем целевого компьютера. Для проверки соединения рекомендуется использовать IP-адрес. Если проверка `ping` по IP-адресу прошла успешно, а `ping` с именем не возвращает ответа, значит, причина неполадки в сервере разрешения имен или в неправильной конфигурации. Это может произойти, если компьютер не использует ни сервер DHCP (Dynamic Host Configuration Protocol), ни сервер DNS (Domain Name System), адрес которого должен быть определен в свойствах TCP/IP.

Замечание

Термин *ping time (время ping)* означает промежуток времени, прошедший с момента передачи сигнала Echo Request до получения ответа Echo Reply. Если промежуток времени небольшой, значит, быстродействие соединения высокое.

С помощью команды `ping` можно также проверить, правильно ли установлен на компьютере стек протоколов TCP/IP и правильно ли он работает. Для выполнения этой проверки дайте команду **ping** по адресу 127.0.0.1. (Обратные адреса рассматривались в главе 8, "Сетевые протоколы и службы".) Если вы получите ответ, значит, стек TCP/IP работает нормально.

Версия команды `ping`, выполняемая из командной строки, включена в стеки TCP/IP всех дистрибутив операционных систем Windows, UNIX и Linux. На сервере NetWare есть две версии этой команды: `ping` и `tping` (trivial ping, простой ping). Они загружаются как модули NLM.

В состав Windows 2000 (но не в Windows 9*x* или NT) включена команда `pathping` Она объединяет средства команд `ping` и `tracert` и, кроме того, предоставляет дополнительную информацию, не выводимую ни одной из этих утилит С помощью `pathping` можно обнаружить, какой маршрутизатор вызывает сетевые проблемы, или измерить количество пакетов, потерянных на конкретном маршрутизаторе

Утилиты трассирования

Утилиты трассирования (отслеживания) используются для определения маршрута, по которому пакет прошел на принимающий компьютер В табл 18 1 приведены команды трассирования, используемые в различных операционных системах

Таблица 18.1. Утилиты трассирования в разных операционных системах

Операционная система	Команда трассирования
Windows (9*x*, NT и 2000)	Ввести **tracert** из командной строки
Linux/UNIX	Ввести **traceroute** из командной строки
NetWare	Ввести **load iptrace** в консоли сервера

Помните для доступа к командной строке в Windows 9x необходимо выбрать команду Start⇨Run и в появившемся окне ввести ***command*** *В системах Windows NT/2000 для этого нужно ввести* ***cmd***

Утилита трассирования выводит на экран все маршрутизаторы, через которые прошел пакет на своем пути от передающего компьютера к принимающему (листинг 18 2) Эта утилита весьма полезна для обнаружения точки, в которой соединение разрывается или замедляется

Листинг 18.2. Команда `tracert` выводит маршрут пакета от одного компьютера к другому

```
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.stngo1.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]
```

Утилиты конфигурирования

Причиной неполадок в соединении часто оказывается его неправильное конфигурирование Возможно, присвоенный компьютеру IP-адрес находится в неправильном диапазоне адресов подсети или неправильно введены маска подсети, шлюз по умолчанию, адрес DNS и т д Если любой из этих параметров неверен или случайно удален, то компьютер не может правильно сообщаться с сетью TCP/IP

В каждой операционной системе есть утилита вывода конфигурационных параметров IP, используемых системой или сетевым адаптером В табл 18 2 перечислены команды вызова этих утилит в различных операционных системах

Таблица 18.2. Команды конфигурирования IP в разных операционных системах

Операционная система	Команда конфигурирования
NetWare	`config`
Windows NT/2000	`ipconfig`
Linux и UNIX	`ifconfig`
Windows 95/98	`winipcfg`

Формат ввода и точный вид выводимой информации для разных команд могут немного отличаться Каждая утилита выводит базовые конфигурационные параметры, такие, как используемый IP-адрес, маска сети (подсети) и шлюза, MAC-адрес (физический), используемый сервер DNS и др

Команда config системы NetWare

Команда `config` вводится в консоли сервера NetWare В листинге 18 3 приведен пример результата, возвращаемого командой `config`

Листинг 18.3. Команда `config` возвращает в консоль сервера NetWare конфигурационные параметры IP

```
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

<Press ESC to terminate or any other key to continue>
```

Команда ipconfig систем Windows NT/2000

Команда `ipconfig` используется в системах Windows NT/2000 для вывода IP-адреса, маски подсети и шлюза по умолчанию, для которых сконфигурирован сетевой адаптер Для вывода более подробной информации используется параметр `/all` В листинге 18 4 приведен результат, возвращаемый командой **ipconfig /all** на сервере Windows NT

Листинг 18.4. Команда `config` с параметром `/all` используется для вывода подробной конфигурационной информации в системах Windows NT/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
```

Если компьютер сконфигурирован как клиент DHCP, то в команде `ipconfig` можно применить два дополнительных параметра Первый из них — `/renew` — приводит к обновлению срока аренды IP-адреса Второй флажок — `/release` — освобождает IP-адрес, чтобы сервер DHCP мог присваивать его повторно

Команда ifconfig систем Linux/UNIX

Команда `ifconfig` используется на компьютерах Linux/UNIX для просмотра конфигурационной информации С помощью этой утилиты можно изменять конфигурацию соединений путем добавления аргументов команды

Замечание

В отличие от команд Windows и NetWare, команда `ifconfig` в UNIX и Linux чувствительна к регистру символов Если ввести `IFCONFIG`, то команда не будет распознана и выполнена

В листинге 18 5 приведен результат, возвращаемый командой `ifconfig` на компьютере Linux

Листинг 18.5. В системах Linux и UNIX команда `ifconfig` используется для вывода конфигурационной информации

```
[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
```

Команда winipcfg системы Windows 9*x*

В операционных системах Windows 95/98 есть утилита конфигурирования с графическим интерфейсом Если в командной строке ввести **winipcfg**, то на экране появится диалоговое окно, показанное на рис 18 14 Для вывода более подробной информации утилиту `winipcfg` нужно запускать с параметром `/all`

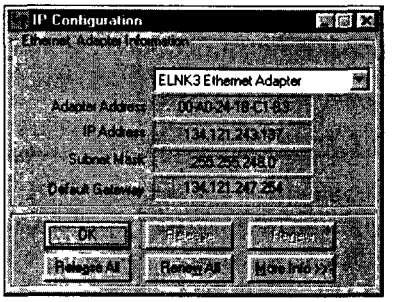


Рис 18 14 В операционных системах Windows 9x используется утилита `winipcfg` с графическим интерфейсом

Другие утилиты TCP/IP

При возникновении сетевых неполадок соединения и параметры конфигурирования проверяют чаще всего с помощью утилит TCP/IP. Однако для сбора информации можно использовать и другие инструменты.

- **Netstat и Nbtstat.** Выводят статистическую информацию TCP/IP и NetBIOS
- **ARP (или *arp* в Linux/UNIX)** Используется для вывода и обновления кэша ARP (Address Resolution Protocol).
- **ROUTE (или *route* в Linux/UNIX).** Используется для просмотра и обновления записей в таблицах маршрутизации.

Указания по устранению неполадок

Устранение сетевых неполадок требует немалого мастерства Шансы на успех существенно повышаются при использовании структурированного метода обнаружения, анализа и решения проблемы. Процесс устранения неполадки необходимо выполнять шаг за шагом.

Следует заметить, что мастерство требуется не только при решении проблем, возникающих в компьютерных сетях. Оно необходимо также врачу, столкнувшемуся со сложной медицинской проблемой, или инспектору полиции, расследующему преступление. Независимо от области деятельности, можно выделить пять этапов решения проблемы.

1. **Сбор информации.** Врач изучает медицинскую карточку пациента и расспрашивает его о симптомах болезни. Инспектор полиции задает вопросы жертвам и свидетелям преступления. Они полагаются не только на собственную наблюдательность, при исследовании относящихся к делу фактов они могут обратиться к книгам или к другим специалистам Чтобы успешно устранять сетевые неполадки, нужно научиться слушать пользователей, рассказывающих о своих проблемах, и правильно формулировать вопросы, ответы на которые помогут диагностировать проблему
2. **Анализ информации.** На этом этапе вам понадобится весь ваш опыт и все ваши знания В первую очередь устраните наиболее очевидные возможные причины Когда пациент жалуется на головную боль, врач не делает немедленно операцию на мозге, сначала он анализирует более простые факторы, способные вызвать наблюдаемые симптомы Как упоминалось раньше, если отсутствует соединение, то, прежде чем форматировать жесткий диск и устанавливать операционную систему заново, нужно проверить, подключен ли к компьютеру сетевой кабель Последовательное отбрасывание очевидных причин существенно сужает круг поиска
3. **Составление и реализация плана действий** На основе проведенного анализа составьте план решения проблемы. В план должны быть включены действия, выполняемые в случае неудачи первых этапов плана Выполняйте план организованно и "планомерно" *За один раз пробуйте только один вариант действия*
4. **Проверяйте результаты ваших действий.** Даже если вы абсолютно уверены, что знаете, в чем причина неполадки и что нужно сделать, все равно необходимо проверить результаты предпринимаемых действий Возможно, действия по устранению неполадки вызвали побочные эффекты, породившие дополнительные проблемы в других местах.

5. **Документирование**. Необходимо выделить определенное время для записи подробностей возникшей проблемы, плана ее устранения и предпринятых для этого действий. Рекомендуется создавать электронную копию этих записей. Помните, что, даже если у вас безупречная, фотографическая память, вы можете перейти на другую работу и весь опыт устранения проблемы будет утерян. Человек, пришедший на ваше место, будет вам очень благодарен, если ему не придется повторять ваши ошибки.

Устраняя сетевые неполадки или оптимизируя производительность сети, помните, что устанавливаемые цели и приоритеты должны быть реалистичны. Если вы не уверены, какой проблемой следует заняться в первую очередь, попытайтесь оценить их стоимость. Учитывайте, что стоимость оценивается не только деньгами. Финансовые соображения, несомненно, играют решающую роль, тем не менее весьма существенны также другие факторы: эффективность функционирования сети, затраты времени, предельные сроки исполнения и даже внутренняя политика компании.

Устранение неполадок — одна из наиболее трудных задач сетевого администрирования. В то же время это область, в которой хороший администратор может доказать, что он достоин своей зарплаты.

Резюме

В этой главе была обоснована важность превентивных мер по обеспечению работоспособности сети. Рассмотрены способы мониторинга и управления сетями и основные принципы устранения сетевых неполадок. Вы узнали, как обнаружить узкие места и установить базовые уровни сетевых показателей, относительно которых следует оценивать производительность сети.

Рассмотрены вопросы измерения пропускной способности соединения с Internet и применения программ мониторинга, таких, как Network Monitor компании Microsoft, LANalyzer компании Novell, и программ независимых компаний, например Sniffer Pro, для сбора информации о производительности сети.

Затем были представлены программы управления сетями и их применение для сбора информации о сетевом оборудовании, программном обеспечении и топологии сети. Рассмотрены развертывание программного обеспечения, управление лицензированием, удаленный контроль рабочих столов пользователей и средства извещения администратора о существенных сетевых событиях. Описаны наиболее популярные программные пакеты управления сетями, такие, как SMS компании Microsoft, ManageWise компании Novell, Tivoli компании IBM и OpenView компании Hewlett Packard, а также утилиты SNMP и CMIP.

Кроме того, рассмотрены сетевые устройства, используемые для мониторинга и устранения неполадок в соединениях. К этим устройствам относятся тональные генераторы/локаторы, перекрестные кабели, обратные петли, тестеры кабелей, рефлектометры и осциллографы. Приведены программные способы решения сетевых проблем — использование файлов журналов и утилит TCP/IP (`ping`, `pathping`, утилиты трассирования, конфигурирования и др.). В конце главы обсуждены основы устранения неполадок в сетях и приведены указания, призванные помочь вам правильно организовать процесс решения сетевых проблем.

Изучая материал книги, вы узнали, как строится сеть, начиная с самого нижнего, физического уровня. Подробно обсуждалось оборудование и программное обеспечение, со-

ставляющие основу современных компьютерных сетей. В заключительной главе рассматривается, как развиваются задачи сетевого администрирования по мере все большего охвата различных сторон нашей жизни коммуникационными технологиями завтрашнего дня.

Рекомендуемые источники

Обстоятельное обсуждение программ-анализаторов и способов работы с ними приведено на Web-узле по адресу: `http://secinf.net/info/misc/sniffingfaq.html`.

Дополнительную информацию о программах сетевого управления Tivoli можно найти по адресу: `http://www.tivoli.com`.

Демонстрационную версию программного обеспечения OpenView компании Hewlett Packard можно загрузить по адресу: `http://www.openview.hp.com`.

Учебник по утилите `ping` находится по адресу:
`http://www.hgmp.mrc.ac.uk/Embnetut/Universl/ping.html`.

Контрольные вопросы

С помощью этих вопросов вы можете проверить степень усвоения материала, изложенного в этой главе. Внимательно прочитайте каждый вопрос и выберите *наиболее правильный* ответ или ответы.

1. Как называется количество данных, которые фактически можно передать по сети в единицу времени?
   - **а.** Полоса пропускания.
   - **б.** Пропускная возможность.
   - **в.** Согласованная скорость передачи.
   - **г.** Базовый уровень.
2. Как называется программный инструмент, с помощью которого можно перехватывать отдельные кадры или пакеты, передаваемые по сети?
   - **а.** Анализатор протоколов.
   - **б.** Монитор производительности.
   - **в.** Рефлектометр временных интервалов.
   - **г.** Фильтр пакетов.
3. Что из приведенного является анализатором протоколов? (Выберите все, что подходит)
   - **а.** Network Monitor компании Microsoft.
   - **б.** SNMP (Simple Network Management Protocol).
   - **в.** Sniffer Pro.
   - **г.** TCPCON компании Novell.
4. В состав чего входит полнофункциональная версия программы Network Monitor компании Microsoft?
   - **а.** OpenView.
   - **б.** Tivoli

в. SMTP.

г. SMS.

5. В какой программе мониторинга используется интерфейс в виде приборной панели? (Выберите все подходящие.)

   а. Network Monitor.

   б. LANalyzer.

   в. Sniffer Pro.

   г. Performance Monitor.

6. Какое из приведенных утверждений о программе SMS справедливо? (Выбрать все подходящие.)

   а. Программу SMS можно использовать для развертывания программного обеспечения.

   б. Программа SMS включена в Windows NT/2000, но не в Windows 9*x*.

   в. Программа SMS используется в соединениях между сетями Windows и мэйнфреймами IBM.

   г. Программа SMS содержит полную версию программы Network Monitor компании Microsoft.

7. Где для организации собранной о сети информации используется база данных MIB?

   а. Network Monitor.

   б. SNMP

   в. Анализатор протоколов.

   г. ASP.

8. Какое устройство называют "лисой и собакой"?

   а. Рефлектометр временных интервалов.

   б. Осциллограф.

   в. Тональный генератор/локатор.

   г. Цифровой вольтметр/омметр.

9. Что необходимо проверить в первую очередь при возникновении неполадки в сетевом соединении?

   а. Конфигурацию протоколов.

   б. Файлы операционной системы.

   в. Правильность учетной записи пользователя на сервере.

   г. Физическое соединение.

10. Какая команда в операционной системе UNIX используется для определения маршрута, которым пакет проходит от передающего компьютера к принимающему?

    а. TRACERT.

    б. TRACEROUTE.

    в. tracert.

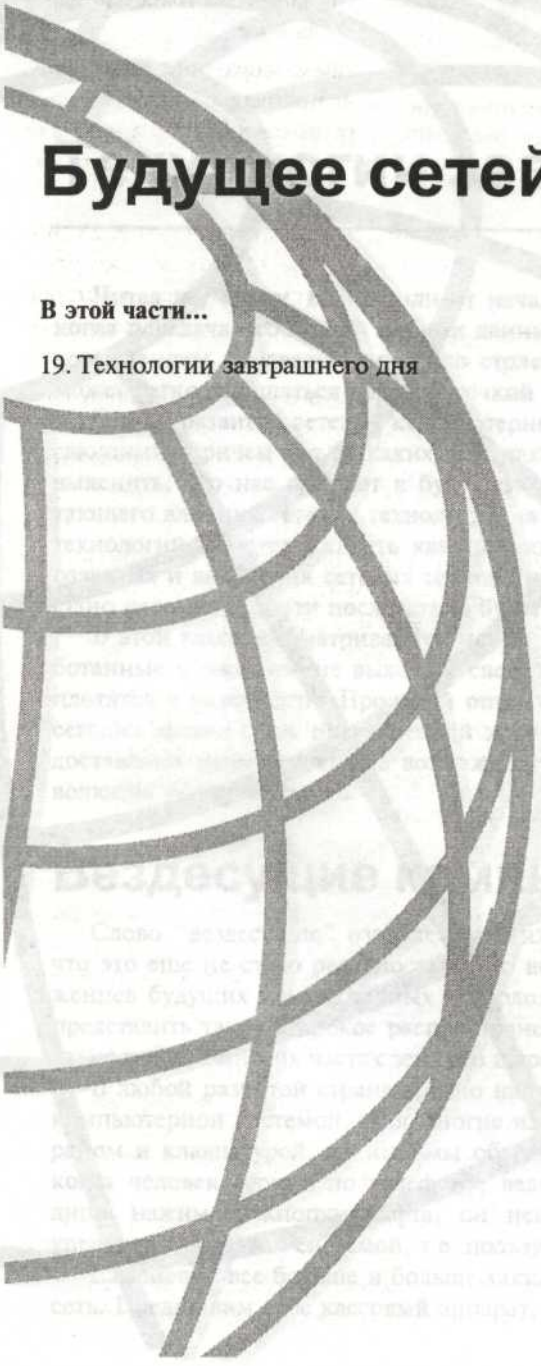
    г. traceroute.

Часть IV

Будущее сетей

В этой части...

19. Технологии завтрашнего дня



Глава 19

Технологии завтрашнего дня

Читая эту книгу, вы прошли от начальных стадий развития компьютерных сетей, когда передача небольшой порции данных из одной системы в другую была немалым достижением, до двадцать первого столетия, в котором практически каждый человек может легко сообщаться с любой точкой земного шара.

Темпы развития сетевых компьютерных технологий в последние годы были потрясающими, причем нет никаких признаков их замедления. В этой главе попытаемся выяснить, что нас ожидает в будущем и чего можно ожидать от постоянно возрастающего влияния сетевых технологий на все стороны жизни. Как и в развитии любых технологий, следует ожидать как положительных, так и отрицательных последствий развития и внедрения сетевых технологий в промышленность и повседневную жизнь. Одно несомненно: эти последствия будут весьма глубокими.

В этой главе рассматриваются новые и захватывающие технологии, как уже разработанные и ожидающие выхода в свет, так и те, которые, возможно, никогда не воплотятся в реальности. Прошлый опыт учит нас, что вчерашняя научная фантастика сегодня может стать повседневной жизнью. Сетевые технологии потенциально предоставляют неограниченные возможности, причем их развитие — точнее говоря, революция — уже началось.

Вездесущие компьютеры

Слово "вездесущие" означает, что их можно встретить практически везде. Пока что это еще не стало реальностью, это всего лишь амбициозные мечты ярых приверженцев будущих компьютерных технологий. Еще десять лет назад трудно было даже представить такое широкое распространение компьютеров, которое сегодня стало реальностью во многих частях земного шара.

В любой развитой стране трудно найти человека, не имеющего дела с какой-либо компьютерной системой, хотя многие из этих систем не являются устройствами с экраном и клавиатурой, какими мы обычно представляем себе компьютер. Например, когда человек звонит по телефону, ведет автомобиль последней модели или всего лишь нажимает кнопку лифта, он неизбежно подает команды микропроцессору, управляющему этой системой, т.е. пользуется компьютерными технологиями.

Ежедневно все больше и больше таких "невидимых компьютеров" объединяются в сеть. Представим себе кассовый аппарат, установленный в супермаркете. Посредством

огромной сети он автоматически сообщается с вашим банком и оформляет сделку (т.е. покупку) без вмешательства человека. В современные автомобили устанавливаются системы GPS (Global Positioning System — система глобального позиционирования), сообщающие водителю о местонахождении автомобиля. Сотни тысяч людей ежедневно пользуются беспроводной телефонной сетью. Продавцы овощных магазинов пользуются кассовыми аппаратами, считывающими штриховые коды товаров с помощью сканеров и передающими данные в сеть. Дети путешествуют по Internet в школе и, вернувшись домой, смотрят любимые телевизионные программы по локальной сети кабельного телевидения. Глобальные цели вездесущих сетей весьма близки к повседневной реальности.

В этой главе рассматриваются следующие аспекты развития сетевых технологий:

- сетевые технологии в нашем доме;
- преодоление ограничений протокола IP;
- новые направления сетевых технологий.

Домашние сети

Одно из наиболее перспективных направлений развития компьютерных технологий — использование компьютерных сетей у нас дома. Устройства и программы, разработанные для быстрого и простого объединения двух или более домашних компьютеров, сейчас рекламируются как нечто такое, что должен иметь каждый.

Во многих из этих домашних сетевых технологий используются традиционные кабели Ethernet. Многие строительные фирмы рассматривают кабели Ethernet как часть инфраструктуры дома, наряду с водопроводными трубами, электрической сетью и телефонными проводами.

Другие домашние сетевые технологии основаны на более новых идеях, таких, как использование уже проложенных в доме телефонных и электрических проводов для передачи компьютерных сигналов. Еще одна новая идея — беспроводные сетевые технологии. Эта альтернатива особенно привлекательна для тех, кто не хочет тратить свое время и деньги на прокладку в стенах новых кабелей.

В настоящее время наиболее распространенной формой реализации домашней сети является коммутируемое соединение с провайдером услуг Internet. Многие пользователи даже не знают, что при наборе номера провайдера их компьютер становится удаленным узлом локальной сети провайдера. Для большинства пользователей необходимо именно соединение с Internet, другие преимущества объединения компьютеров в сеть интересуют их незначительно. Поэтому глобальные соединения с Internet стали базой развития новых технологий.

Однако, чтобы всеобщее соединение с Internet стало возможным, должны быть преодолены некоторые реальные технические ограничения. Наиболее актуальное из них — нехватка допустимых IP-адресов. Сеть Internet работает на основе протокола TCP/IP, поэтому каждый компьютер, сообщающийся с Internet посредством TCP/IP, должен иметь уникальный IP-адрес.

Как показано в предыдущих главах, в текущей версии протокола IP, которая называется IPv4, используются 32-битовые адреса. Это значит, что существует "только" 4 294 967 296 допустимых адресов. На первый взгляд может показаться, что более 4 млрд адресов вполне достаточно; разработчики протокола IP в ранний период суще-

ствования ARPAnet не ожидали, что со временем потребность в адресах вырастет до огромных размеров.

Население земного шара сейчас составляет более 6 млрд человек, причем эта цифра быстро растет. Если сбудутся смелые мечты о всеобщей связи и каждый человек на земле будет иметь соединение с глобальной сетью (не говоря уже о каждой интеллектуальной микроволновой печи, холодильнике и т.д.), то уже сейчас нужно серьезно задуматься о преодолении ограничений протокола IPv4.

Преодоление ограничений IP

Планы реализации следующего поколения протоколов IP (называемого IPv6 или IPing, что означает IP next generation — IP следующего поколения) разрабатываются на протяжении уже многих лет. Организация IETF (Internet Engineering Task Force) работает над спецификациями нового протокола IP с 1994 года.

Как отмечается в главе 8, "Сетевые протоколы и службы", использование метода CIDR (Classless Interdomain Routing — бесклассовая междоменная маршрутизация) и методов разделения IP-адресов, например NAT (Network Address Translation) замедляет нехватку адресов. Однако это лишь временная мера. Несмотря на все трудности, связанные с изменениями в таких огромных масштабах, Internet со временем неизбежно перейдет на новую версию IP.

Чтобы сделать переход как можно более безболезненным, внимание разработчиков IPv6 сконцентрировано на совместимости с существующей системой. Ставится задача обеспечить системам IPv4 и IPv6 возможность сообщаться друг с другом на всем протяжении длительного периода полного развертывания новой версии IP. Это критическое условие успешного внедрения IPv6. Неудача, постигшая попытку замены TCP/IP набором OSI, вызвана главным образом отсутствием хорошего плана перехода

Чем протокол IPv6 лучше протокола IPv4

Наиболее существенное отличие между старой и новой версиями IP — объем адресного пространства. В протоколе IPv4 используются 32-битовые адреса, а в IPv6 — 128-битовые. Другими словами, новое адресное пространство содержит $3{,}4\times10^{38}$ допустимых IP-адресов. Трудно даже представить себе такое огромное число. Записанное на бумаге, оно выглядит так:

340 282 366 920 938 463 463 374 607 431 768 211 456.

Другими словами, на каждый квадратный метр земной поверхности приходится 3 911 873 538 269 506 102 допустимых адресов. Такой объем адресного пространства достаточен на любой обозримый период в будущем, даже если каждый человек на Земле будет обладать десятками устройств с отдельными IP-адресами.

Насколько безопасен IPv6

В протоколе IPv6 поддерживаются новые механизмы безопасности — IPing AH (Authentication Header) и IPing ESH (Encapsulation Security Header). Протокол на основе заголовков AH уже встречался в главе 14, "Защита сети", при обсуждении протокола IPSec. В протоколе IPv6 уменьшается объем широковещательных сообщений, что тоже повышает производительность и безопасность сети.

Реализация протокола IPv6

Как вы понимаете, для перехода на IPv6 невозможно закрыть Internet на несколько дней или недель, чтобы заменить все оборудование и программное обеспечение. В настоящее время предлагается и рассматривается несколько методов перехода с IPv4 на IPv6. Скорее всего, переход будет выполняться путем некоторого их сочетания. Перечислим предполагаемые методы перехода.

- **Двойной протокол**. В этом методе обе версии IP будут выполняться на одних и тех же устройствах в пределах одной и той же сети. Программное обеспечение IPv6 будет выполняться наряду с IPv4 приблизительно так же, как сейчас различные протоколы (например, TCP/IP и IPX) выполняются на одном и том же устройстве.
- **Трансляция**. В этом методе предполагается коммуникация устройств IPv6 с устройствами IPv4 путем трансляции (преобразования) сигналов протокола IPv6 в старый формат. Это немного похоже на трансляцию частных IP-адресов в публичные методом NAT.
- **Туннелирование**. При использовании этого метода предполагается туннелирование пакетов IPv6 по сетям IPv4. Таким образом устройства IPv6 смогут работать в сетях с устройствами IPv4, пока они не будут постепенно заменены новыми. Фактически создается виртуальная сеть IPv6 в Internet на основе IPv4.

Для тестирования процедур перехода разработана экспериментальная сеть 6bone, на начальном этапе представлявшая собой виртуальную сеть на основе IPv6, сигналы которой туннелируются в Internet. Проект 6bone реализован как часть проекта IPing организации IETF. Сеть 6bone развернута по всему земному шару, ее узлы расположены в большинстве промышленно развитых стран. В настоящее время с ее помощью выполняются эксперименты с процедурами адресации и маршрутизации на основе IPv6.

За разработку новой версии IP отвечает организация IPv6 Forum. На ее Web-узле `www.ipv6forum.com` приведена обширная информация о протоколе IP нового поколения.

Новые направления сетевых технологий

Новая версия IP, какой бы захватывающей она ни казалась, основана все еще на традиционных сетевых технологиях. Пытаясь заглянуть в более отдаленное будущее, не следует отбрасывать возможность того, что сети в нем будут построены на основе других, совершенно новых компьютерных и сетевых технологий. Многие идеи в области сетевых технологий звучат как научная фантастика. Тем не менее уже сейчас ведутся серьезные исследования в области нейронных компьютерных сетей, принцип действия которых аналогичен человеческому мозгу, сообщающемуся с "узлами", разбросанными по всему телу. Ведутся также исследования так называемых квантовых сетей. В них информация обрабатывается на основе теории квантовой физики на молекулярном и атомном уровнях. Рассмотрим некоторые из этих новых направлений подробнее.

Нейронные сети

В мире компьютерных технологий концепция *нейронных компьютерных сетей* стала довольно модной. Архитектура искусственной нейронной сети моделирует нейронную сеть человеческого мозга. Другими словами, большое количество относительно простых процессоров объединены аналогично нейронам мозга.

Модель нейронной сети основана на концепции параллельных вычислений (рис. 19.1). В ней используется огромное количество небольших процессоров, в то время как в традиционной компьютерной архитектуре вычисления выполняются одним или несколькими мощными процессорами.

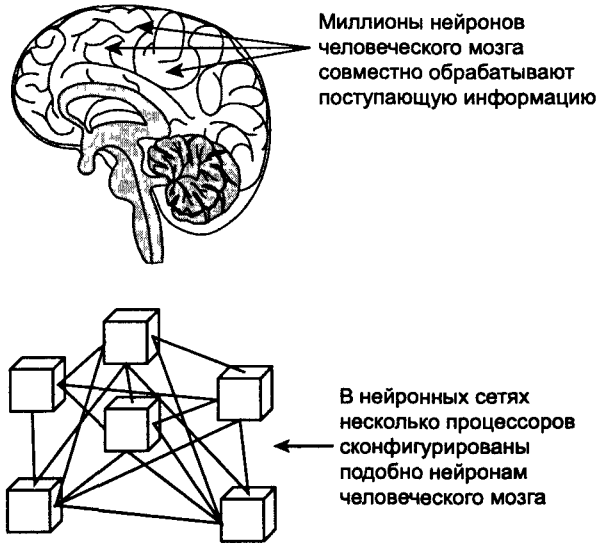


Рис. 19.1. В нейронной сети большое количество маломощных процессоров работают совместно аналогично нейронам головного мозга

Предполагается, что нейронная компьютерная сеть составит фундамент *искусственного интеллекта*, рассматриваемого как вершина развития компьютерных технологий. К концепции искусственного интеллекта мы еще вернемся в конце главы.

Квантовые сети

Основой квантовой теории является концепция неприменимости физических законов *макро*мира к явлениям *микро*мира, в котором элементарные частицы вещества составляют атомы и молекулы.

Согласно теориям квантовой механики, субатомные частицы, такие, как электроны или протоны, могут существовать во многих состояниях одновременно, т.е. параметры микрочастицы (скорость, координаты) не определены точно, они являются вероятностными величинами. Это положение может радикально изменить способы компьютерной обработки информации. Традиционные компьютеры работают с двоичным кодом. Их принцип действия основан на том, что каждый бит информации в конкретный момент времени может находиться только в одном из двух состояний — выключенном (нуль) или включенном (единица).

В то же время в физике микромира квантовый бит (так называемый *qubit, q-бит*) может в один и тот же момент времени находиться как во включенном, так и в выключенном состоянии. Кроме того, многочисленные q-биты можно некоторым образом связать друг с другом, что позволяет обрабатывать многие значения одновременно. На основе теории квантовой физики в современной промышленности работают многочисленные устройства — лазеры, приборы ядерного магнитного резонанса и т.д.

Квантовая теория охватывает представления о ветвящихся вселенных (*мультивселенных*). Парадоксальные идеи квантовой теории не укладываются в рамки обычного здравого смысла. Например, принцип *шредингерова кота*, сформулированный знаменитым физиком Эрвином Шредингером (Erwin Schrödinger), утверждает, что кот, находящийся в ящике, может быть живым и мертвым одновременно. В квантовую теорию внесли значительный вклад такие выдающиеся ученые, как Макс Планк (Max Planck), считающийся основателем квантовой теории, Вернер Гейзенберг (Werner Heisenberg) и Нильс Бор (Neils Bohr), теория строения атома которого получила всеобщее признание, хотя Альберт Эйнштейн (Albert Einstein) и не согласен с его взглядами.

В рамках данной книги, естественно, невозможно изложить принципы квантовой теории хоть сколько-нибудь полно или последовательно. Тем не менее мы все же попытались приоткрыть захватывающие перспективы, предлагаемые квантовой теорией для будущего компьютеров и компьютерных сетей. Ссылки на источники более подробной информации по этой теме приведены в конце главы.

Всеобщая связь

Если компьютеры станут действительно вездесущими, то мы достигнем состояния *всеобщей связи*, т.е. такого положения, когда каждый человек на Земле, желающий получить доступ к глобальной сети, сможет легко установить соединение с Internet. Достичь такого уровня развития довольно сложно, однако в последнее десятилетие мы двигались к этой цели быстрыми темпами.

Согласно последним исследованиям количество пользователей глобальной сети Internet начиная с 1995 года удваивалось каждый год (см. `www.e-land.com`). Если эта тенденция сохранится, то всеобщая (или почти всеобщая связь) станет реальностью довольно скоро. Следует ожидать, что в течение следующих двух десятилетий соединение с Internet в большинстве домов станет таким же обычным, как сегодня, например, телефон.

Оборудование, программное обеспечение и услуги Internet постепенно становятся все более дешевыми. В начале 1980-х годов персональный компьютер (гораздо менее производительный, чем современный компьютер стоимостью 500 долларов) стоил 10 000 долларов, а коммутируемое соединение со службой в реальном времени (например, CompuServe) с потрясающей для тех лет пропускной способностью 900–1 200 бит/с стоило более 20 долларов в час. Сегодня мощный мультимедийный персональный компьютер со всеми периферийными устройствами стоит не более 3 000 долларов, а базовые устройства и программы, обеспечивающие соединение с Internet, продаются не более чем за несколько сотен долларов. Провайдеры услуг Internet предоставляют учетные записи с неограниченным коммутируемым доступом всего лишь за 10 долларов в месяц, аренда скоростных линий DSL (Digital Subscribe Line) и учетных записей кабельных модемов, равноценных линии T-1, стоят менее 50 долларов в месяц. Во многих регионах провайдеры предоставляют даже бесплатные услуги Internet, окупаемые за счет рекламы.

В ближайшем будущем Internet будет интегрирована в нашу повседневную жизнь в значительно большей степени, чем сейчас. Чтобы войти в киберпространство, не нужно будет садиться за клавиатуру и загружать компьютер. Фактически устройства оперативного доступа в Internet существуют уже сегодня.

Беспроводные средства доступа в Internet посредством сотовых телефонов и портативных компьютеров пока еще не получили широкого распространения, однако их популяр-

ность быстро растет. Некоторые пейджеры фактически представляют собой небольшие компьютеры, способные принимать сообщения электронной почты. Недалек то час, когда Internet будет состоять из самых разнообразных устройств коммуникации, многие из которых будут лишь весьма отдаленно напоминать традиционный компьютер.

Теперь рассмотрим "интеллектуальные" устройства и те перемены, которые внесут в нашу повседневную жизнь сетевые технологии. Также обсудим вопросы конфиденциальности, возникающие в связи с глобальным охватом средствами коммуникации всех сторон жизни людей.

Интеллектуальные предметы

Термин *устройство Internet* означает портативную выделенную систему, в которой выполняется только специальное программное обеспечение (например, Web-броузер или клиентская программа электронной почты) и с помощью которого можно легко путешествовать по Internet или передавать и принимать сообщения. Конфигурирование такого устройства максимально упрощено. Главным приоритетом устройства Internet является не вычислительная мощность, а дружественность к пользователю.

Однако в контексте достижений компьютерной технологии термин "устройство Internet" получает новое значение. Компании, занятые разработкой программного обеспечения, такие, как Microsoft и Sun Microsystems, совместно с поставщиками оборудования (Maytag, Whirlpool и др.) разрабатывают интеллектуальные холодильники и микроволновые печи. Согласно их представлениям о будущем, обычные кухонные приборы будут оснащены микропроцессорами и объединены в сеть друг с другом и с Internet.

Зачем может понадобиться подключение, например, кофеварки к Internet? Рассмотрим такой сценарий. Допустим, холодным зимним вечером вы возвращаетесь домой из офиса и хотите выпить чашку горячего кофе. Разве не приятно было бы взять ее в руки сразу, как только вы войдете в дом? В нашем футуристическом видении будущего для этого нужно всего лишь установить соединение с вашей Internet-кофеваркой посредством беспроводного телефона, подключенного к Internet, и дать команду начать приготовление вашего любимого каппучино.

Интеллектуальные кофеварки — это только начало. Идея интеллектуальных устройств предполагает намного более амбициозную цель — интеллектуальный дом. Компания Emware, расположенная в штате Юта, разрабатывает программное обеспечение для устройств, содержащих встроенные микропроцессоры. Программное обеспечение позволяет этим устройствам подключаться к Internet и обмениваться информацией с другими устройствами. Это возможно даже для устройств на основе 8- или 16-разрядных микропроцессоров, таких, как термостаты, поливальные машины, торговые автоматы и др. Компания Emware объединилась с другими компаниями, такими как Hitachi, Phillips, SAP и Sybase в консорциум, имеющий целью "встраивание в Internet".

Возможности коммуникационных технологий ограничиваются только нашим воображением. Уже разработаны интеллектуальные холодильники, способные обнаружить нехватку определенных продуктов и автоматически заказать их в супермаркете.

Семейная сеть

Развитие коммуникационных технологий изменяет даже семейную жизнь людей, правда, не всегда в благоприятном направлении. Внимание средств массовой информации сосредоточено главным образом на отрицательных сторонах этих изменений,

например разводах, вызванных чрезмерной увлеченностью одного из супругов путешествиями по Internet, или супружеской неверности "в интерактивном режиме". Тем не менее Internet может немало способствовать созданию и укреплению семейных уз.

Электронная почта, видеоконференции, интерактивная переписка, телефония посредством Internet предоставляют членам семей и друзьям возможность находиться в постоянном контакте независимо от географического расстояния. Семейные локальные сети позволяют разделять файлы, принтеры и соединения с Internet. Общие интересы в области компьютерной коммуникации становятся постоянной темой разговоров и движущей силой многих семейных дел.

Десять лет назад никто даже представить себе не мог, что любой человек (кроме, конечно, очень богатых людей) сможет контролировать поведение своих детей или общаться со своим врачом в режиме реального времени непосредственно с рабочего места. Сегодня это не только экономически достижимо, но и реализовано во многих регионах. В недалеком будущем коммуникационные технологии проникнут в семейную жизнь в значительно большей степени и в таких направлениях, которые сейчас трудно даже представить.

Развлечения

Одна из областей, на которую Internet сейчас оказывает сильнейшее влияние, — это индустрия развлечений. В средствах массовой информации ведется бурная полемика относительно правовых аспектов обмена музыкальными файлами в формате MP3. Серьезные правовые проблемы возникают вокруг казино, в которых люди играют в азартные игры в интерактивном режиме. Эти и другие правовые вопросы слишком запутаны двусмысленностью законодательства, регулирующего существование и использование Web-узлов. Разрешение таких конфликтов законодательства — весьма актуальная задача сегодняшнего дня.

Становятся обычными загружаемые электронные книги. Посредством высокоскоростных соединений по сети могут передаваться даже кинофильмы. Компании, занятые арендой видеофильмов, вкладывают деньги в разработку и тестирование программ, позволяющих загружать фильмы посредством сети, что устранит необходимость покидать дом для покупки очередной видеокассеты.

Сама Web стала мощным источником развлечений. В интерактивном режиме сейчас доступны такие узлы, как ITEN (Internet Talk and Entertainment Network), а также десятки традиционных развлекательных изданий, например *Variety* или *Hollywood Reporter*. Фактически Internet является движущей силой роста популярности так называемого *infotainment (information entertainment — информационное развлечение)*. Этот термин означает представление информации и новостей в увлекательной форме.

Безопасность всеобщей связи

Реализация всеобщей связи порождает немало серьезных проблем, касающихся прав человека и конфиденциальности информации. Особенно это относится к государственным учреждениям, контролирующим и использующим информацию, передаваемую по Internet и другим сетям. Система надзора за электронной почтой Carnivore, принадлежащая ФБР, и контроль данных, передаваемых по Internet, со стороны английской разведывательной службы MI5 подняли бурю негодования среди защитников прав человека.

Другой широко дебатируемый вопрос — использование информации, собираемой в Internet крупными корпорациями в коммерческих целях. В настоящее время есть методы отслеживания посетителей Web-узлов и сбора информации о них без их ведома или согласия. Существуют также возможности получения доступа к жестким дискам пользователей и хранящимся на них данным. Контроль над системами пользователей может проводиться путем тайной установки на их дисках агентских программ, которые могут распространяться по электронной почте, или путем выполнения пользователем сценариев на Web-странице.

Компании часто отслеживают действия своих служащих в Internet. Во многих случаях суды выносят решения, подтверждающие их право делать это, когда затронуты собственность компании или оплаченное ею рабочее время.

Существуют многочисленные организации, занимающиеся вопросами защиты сетевой конфиденциальности. Законодательными органами принимаются специальные законы, посвященные этим вопросам, например *Children's Online Privacy Protection Act* (Акт о защите сетевой конфиденциальности детей), вступивший в силу в апреле 2000 года. Целью этих законов является регулирование сбора информации о потребителях. В некоторых штатах приняты законы, защищающие пользователей Internet от "кибersталкеров", использующих средства электронной коммуникации для оскорбления или запугивания других людей.

Вполне очевидно, что в двадцать первом столетии мы увидим немало новых законов, принятых с целью регулирования процессов перехвата, сбора или использования данных, передаваемых по сети как частными лицами, так и организациями.

Сетевые технологии на рабочем месте

Как уже указывалось выше, некоторые компании отслеживают действия своих служащих в Internet. Однако это далеко не единственное применение сетевых технологий на рабочем месте. Коммуникационные технологии радикально изменили многие рабочие места. Особенно это справедливо для профессий, связанных с обработкой большого объема информации, о чем пойдет речь далее в главе. Со временем влияние коммуникационных технологий будет распространяться на все больше областей человеческой деятельности.

Технологии электронной коммерции оказывают сильное влияние на розничную торговлю, а реклама в Web — на коммерцию любого типа. Потребители сейчас могут "ходить по магазинам" и приобретать любые товары в любых количествах, сидя за экранами своих компьютеров и даже не выходя из дома. Сетевые технологии кардинально меняют характер нашей работы везде — от небольших офисов с одним служащим до огромных государственных предприятий, выполняющих программы космических исследований.

Рассмотрим, как современные коммуникационные технологии влияют на работу государственных органов, на профессии врачей и юристов, а также на издательское дело.

Влияние сетевых технологий на государство

Учреждения федерального правительства и правительств штатов все больше используют Internet для информирования своих сограждан и для повышения производительности и эффективности работы своих служащих. Рассмотрим эти вопросы подробнее.

Повышение качества услуг, предоставляемых гражданам

В настоящее время власти многих городов размещают на своих Web-узлах формы документов (таких, как заявления, разрешение на строительство и т.д.) в виде, пригодном для непосредственной загрузки и печати. Это избавляет граждан от лишнего посещения учреждений и экономит время служащих, которые вынуждены были бы искать необходимые формы и выяснять, что нужно посетителю. Посредством Web учреждения предоставляют гражданам различную информацию.

- Справочники телефонных номеров разных отделов.
- Адреса электронной почты, по которым граждане могут направлять свои жалобы, вопросы и предложения.
- Сообщения об открывшихся вакансиях в учреждении.
- Карты и описания городских заведений, мест отдыха, предоставляемых услуг и т.д.
- Даты предстоящих важных событий города.
- Информацию налоговой службы (нормы налогового обложения недвижимости и т.д.).
- Базы данных с механизмами поиска, в которых хранятся постановления, даты собраний комитетов и другие публичные документы.

Облегчение работы государственных служащих

Развитие коммуникационных технологий существенно изменило характер работы государственных служб. Использование компьютерных сетей для сбора и обработки данных значительно упростило выполнение задач, требующих обработки большого объема информации, таких, как перепись населения, работа с налоговыми ведомостями и др. Депутаты законодательных органов, начиная с местных и кончая федеральными, с помощью частных и публичных сетей легко и быстро получают информацию, необходимую им в работе над законами.

Компьютерные войны и терроризм

На всем земном шаре стр*а*ны становятся все более зависимыми от компьютерных технологий. Может ли это таить в себе угрозу возникновения новых войн? Согласно некоторым предсказаниям, в будущем войны между странами будут вестись не на полях сражений, а в киберпространстве. На войну отправятся сетевые роботы, а не призывники.

Оптимисты видят в развитии коммуникационных технологий перспективу превращения войн в бескровные. Борьба будет вестись в сети между виртуальными солдатами, как это стало обычным в компьютерных играх. Однако переделать человеческую природу невозможно — радужные мечты о полностью бескровных войнах вряд ли когда-либо осуществятся. Тем не менее развитие компьютерных технологий способно значительно уменьшить человеческие потери на поле боя. В Центре космических и морских военных исследований (Space and Naval Warfare Center), расположенном в Сан-Диего, разрабатываются автоматические наземные, воздушные и подводные средства передвижения, а также автономные наземные роботы и управляемые дистанционно манипуляторы, которые можно использовать для ведения "рукопашного боя", находясь на безопасном расстоянии.

Так будущее представляется оптимистам. Пессимисты же видят в развитии компьютерных технологий угрозу появления "кибертеррористов", несущих реальные разрушения в наш реальный мир. По их мнению, доступ к изощренным технологиям все большего количества людей приведет к осуществлению сценария Судного дня. Хакеры проникнут в компьютеризированные системы управления термоядерными ракетами и сделают заложниками целые страны. Власти враждебных стран получат доступ к жизненно важным военным тайнам. Тоталитарные правительства получат средства контроля и управления всеми сторонами жизни своих граждан.

Коммуникационные технологии станут основой создания "интеллектуальных" ракет и бомб, получающих информацию в полете и корректирующих свою траекторию с целью максимально эффективного поражения выбранных объектов. Военные специалисты предсказывают, что в ближайшем будущем каждый солдат будет нести с собой GPS и другие устройства, подключенные к сети.

Компьютерные коммуникационные технологии — особенно беспроводные — предоставляют командованию средства сбора информации, ее оперативной обработки и передачи приказов подразделениям на поле боя. Полная и достоверная информация всегда была решающим фактором победы как в отдельном сражении, так и во всей войне. В ближайшем будущем победа в войне будет зависеть главным образом не от размера армии, а от стратегически эффективного применения новейших технологий.

Правительственная поддержка исследований в области коммуникации

Начиная с периода, когда Министерство обороны США финансировало разработку сети ARPAnet, правительство прилагает значительные усилия для развития и поддержки структуры Internet. В последние годы одним из главных приоритетов федерального правительства было создание информационной супермагистрали, предоставляющей высокоскоростной доступ в Internet по всей территории США.

Исходя из тенденций, наблюдавшихся в недалеком прошлом, следует ожидать, что правительства многих стран предпримут значительные усилия в направлении развития новых технологий и их реализации в промышленности.

Влияние коммуникационных технологий на законодательство

Простота доступа к информации посредством компьютерных сетей серьезно повлияла на работу практикующих адвокатов. Юридические исследования (работа весьма трудоемкая и нудная) с помощью компьютеров выполняются значительно быстрее, а их результаты становятся гораздо полнее и точнее. Компьютеры могут автоматически просматривать тысячи прецедентов, законодательных положений и подзаконных актов, затрачивая на это намного меньше времени, чем понадобилось бы человеку для листания фолиантов.

Рассмотрим, как новые технологии изменяют не только юридическую практику, но и процесс принятия законов.

Законодательство на основе информации

Информация является базисом законодательных и регулятивных решений. Лицам, принимающим решения, коммуникационные технологии значительно облегчают и ускоряют получение необходимой для этого информации. Например, члены Конгрес-

са США, законодательных органов штатов, муниципальных советов и других публичных организаций используют Internet и частные сети в следующих случаях:

- исследования вопросов, связанных с принятием конкретного законодательного акта;
- быстрой и эффективной коммуникации друг с другом;
- оперативной связи с избирателями.

Вполне возможно, что в недалеком будущем в интерактивном режиме будет выполняться не только регистрация избирателей, но и само голосование. Электронная избирательная система имеет огромное количество преимуществ по сравнению с обычной, включая сокращение организационных расходов, экономию времени избирателей, более глубокую детализацию вопросов, выносимых на голосование, и т.д. Естественно, сначала должны быть решены многочисленные вопросы, связанные с безопасностью и аутентификацией избирателей.

Коммуникационные технологии в правоохранительных органах

Составление и принятие новых законов — не единственная область права, адаптирующаяся к новым технологиям. Коммуникационные технологии (особенно беспроводные) существенно влияют также на работу правоохранительных органов.

В настоящее время многие полицейские участки оснащены устройствами MDT (Mobile Display Terminal — мобильный терминал вывода), а на патрульных машинах устанавливаются полнофункциональные портативные компьютеры. Они используются для коммуникации с другими MDT и с сетью полицейского участка посредством беспроводных носителей. Офицеры полиции, установив с помощью терминалов соединение с местными или федеральными базами данных, могут проверять регистрацию номерных знаков автомобилей и водительские права, просматривать досье преступников и т.д. В недалеком прошлом патрульный полицейский должен был для этого связаться с диспетчером в участке, который с помощью компьютера собирал необходимую информацию, а затем устно передавал ее полицейскому.

Все больше патрульных машин оборудуются устройствами GPS. С ее помощью диспетчер полицейского участка в любой момент времени имеет точную информацию о местонахождении каждой машины, что позволяет значительно повысить оперативность реагирования на экстренные вызовы. Другое интересное применение коммуникационных технологий, объединяющее правовую и коммерческую области, — система LoJack, в которой в автомобили встраиваются скрытые передатчики. Это позволяет полиции быстро выследить и задержать украденный автомобиль. В ближайшем будущем следует ожидать самого широкого использования таких технологий в работе правоохранительных органов.

Влияние сетевых технологий на медицину

Медицина — одна из первых областей, в которых начали широко использоваться переносные сетевые компьютеры. Врачи и медицинские сестры могут вносить записи в медицинские карточки пациентов, причем сделанные записи мгновенно реплицируются на другие сетевые системы, имеющие отношение к пациенту. Это значительно повышает эффективность и аккуратность медицинской документации. Используя эту систему, врачи могут легко и быстро получать доступ к новейшей медицинской информации.

Лечение на расстоянии

С помощью компьютерной сети и управляемых устройств хирурги уже сейчас могут выполнять хирургические операции дистанционно. Концепция *телемедицины*, предполагающая выполнение врачом предварительного обследования средствами видеоконференций, — еще одно захватывающее, хотя и противоречивое, новое направление.

Врачи в Internet

Такие издания, как *MD netguide* (Руководство по сетям для медиков), предоставляют медицинским работникам информацию о возможностях и способах получения доступа к специализированным сетевым источникам. Существуют также многочисленные частные службы предоставления медицинской информации. Врач может легко установить удаленное коммутируемое соединение с такой службой и оперативно получить нужную информацию или проконсультироваться с другим специалистом.

Многие врачи создают собственные Web-узлы, с которыми пациенты могут ознакомиться посредством электронной почты или в режиме интерактивной переписки. На Web-узле своего врача пациенты могут получить информацию об условиях и стоимости медицинских услуг, о госпитализации, о стандартных медицинских процедурах, условия сочетаемости лекарственных средств и различные медицинские советы. Целью всей системы является облегчение коммуникации между врачом и пациентами, что позволит повысить качество диагноза и лечения.

Пациенты в Internet

Существует довольно много групп поддержки, работающих в интерактивном режиме, для лиц страдающих хроническими заболеваниями, как физиологическими, так и психическими. Пациенты и члены их семей могут сообщаться с другими пациентами, страдающими этим же заболеванием, и обмениваться с ними своим опытом и полезной информацией о методиках лечения, врачах и лечебных учреждениях.

Например, популярная организация Alcoholics Anonymous (Анонимные алкоголики) финансирует Web-узлы, списки рассылки и группы новостей, которыми пользуются ее члены. Кроме того, существует огромное количество коммерческих и бесприбыльных Web-узлов, посвященных проблемам здоровья. В этих узлах пациенты могут найти для себя много полезной информации, к которой раньше не имели доступа.

Согласие на основе полной информированности

С помощью обширной медицинской информации, хранящейся в клиниках, библиотеках и образовательных учреждениях пациенты теперь могут не только исследовать свое заболевание, но и получать сведения о своем лечащем враче. Существуют многочисленные наблюдательные, или "сторожевые" Web-узлы, где можно получать информацию о врачах, клиниках и различных проблемах, с которыми сталкиваются пациенты.

Компьютерные сетевые технологии предоставят также немало других новых способов коммуникации пациентов с организациями и лицами, предоставляющими медицинские услуги.

Влияние сетевых технологий на издание книг

Новейшее модное словечко в издательском деле — *электронная книга*. Постоянно возрастающая доступность электронных книг, журналов и газет в интерактивном режиме медленно, но уверенно меняет индустрию издательства книг.

Такие программы, как Glassbook Reader for PC и Microsoft Reader (с версиями для портативных компьютеров), позволяют легко читать роман или справочник в электронном формате. По сравнению с обычной электронная книга имеет ряд преимуществ.

- В небольшом объеме можно хранить сотни или даже тысячи книг, которые в напечатанном виде заняли бы целую комнату.
- Много электронных книг легко переносить с одного места в другое.
- Для создания электронных книг не нужно рубить деревья, следовательно, не страдает окружающая среда.
- Электронные издания можно продавать по значительно меньшей цене, поскольку нет расходов на печать и намного меньше расходы на распространение.
- Ошибки в электронных версиях книг исправляются легко и быстро.
- Авторы могут сами издавать электронные книги.
- Посредством Web или FTP электронные книги можно легко и быстро распространять по всему миру.

Конечно, электронные книги имеют и недостатки. Например, возникают сложности с охраной авторских прав. К тому же многим не нравится читать с экрана.

Замечание

Многие вопросы, связанные с индустрией электронных книг, относятся и к электронному распространению музыкальных произведений. Прежде чем электронное издание получит широкое распространение, издатели и читатели должны договориться об условиях этой новой модели доступа. Потребитель, купивший книгу или компакт-диск, считает себя вправе распоряжаться ими как ему заблагорассудится, в том числе и продать их. Ведь заплатил же он за них! Ему трудно свыкнуться с мыслью, что он не имеет права продавать или передавать кому бы то ни было купленную им электронную копию книги либо музыкального произведения.

Существуют и другие недостатки. Например, с экрана некоторых портативных устройств трудно читать при ярком освещении. Когда в батареях кончается запас энергии, книга становится недоступной. Тем не менее многие предсказывают, что на протяжении следующего (уже текущего) столетия бумажные книги устареют и большая часть информации будет храниться и использоваться в электронном формате.

Новые способы обучения

Новые технологии изменяют не только способ чтения. Они предоставляют также новые возможности получения образования, как формального, так и неформального. Компьютерные сети и Internet значительно облегчают проведение учебных занятий и сдачу экзаменов. Теперь это можно делать даже не выходя из дома.

Существует много университетов, работающих в интерактивном режиме, как аккредитованных, так и неформальных. Многие традиционные образовательные учреждения предоставляют всем желающим курсы *дистанционного образования*.

Посредством Web могут проводиться виртуальные занятия, в которых преподаватели передают учебные материалы по сети и в интерактивном режиме руководят сеансами обсуждения. Студенты могут получать учебные задания по электронной почте, а

средства аудио- и видеоконференций сделают возможным их почти реальное присутствие в учебном классе.

В недалеком будущем станут обычными "учебные аудитории без стен". При таком способе обучения студенты смогут работать в удобном для них режиме, им не придется тратить время на дорогу в университет, кроме того, сами университеты сэкономят немалые средства, затрачиваемые на поддержание учебных корпусов (ремонт, уборка, освещение и т.д.).

Согласно некоторым исследованиям, дистанционное образование может быть таким же эффективным, как и традиционные методы обучения, однако лишь при условии использования достаточно совершенных коммуникационных технологий, обеспечивающих беспрепятственное взаимодействие учащихся друг с другом и преподавателя с учащимися.

Искусственный интеллект

Искусственный интеллект в энциклопедии информационных технологий определяется как "моделирование процессов человеческого мышления с помощью искусственного устройства, в частности компьютерной системы. Указанные процессы включают обучение, аргументацию и коррекцию своих ошибок".

Компьютерная программа, которая может эмулировать суждения и поведение человека, являющегося специалистом в какой-либо области знаний, называется *экспертной системой.* Основой экспертной системы обычно служит нереляционная база данных. Кроме базы данных, система содержит набор запрограммированных правил, определяющих применение хранящихся знаний в предопределенных ситуациях. Один из примеров экспертных систем — программа игры в шахматы Deep Blue, разработанная компанией IBM специально для того, чтобы нанести поражение чемпиону мира по шахматам Гарри Каспарову. В научной фантастике в качестве примера экспертной системы можно назвать голографического врача на борту звездолета *Voyager* в телевизионном сериале *Star Trek: Voyager.*

Думающие компьютеры

Настоящий искусственный интеллект должен уметь не только сортировать данные и выполнять запрограммированные операции, но и учиться на основе своего предыдущего опыта. Другими словами, машина должна уметь думать, выявлять отношения между предметами и понятиями, обобщать информацию. До сих пор ни один компьютер даже близко не подошел к этому.

В последнее десятилетие усилия по созданию интеллектуального компьютера значительно интенсифицированы. Многие крупные университеты, включая такие престижные, как Массачусетский технологический институт, выполняют программы, направленные на достижение этой цели. Разработкой проектов, связанных с искусственным интеллектом, заняты военные ведомства, например Центр прикладных исследований в области искусственного интеллекта, принадлежащий военно-морским силам США. На исследования тратятся миллиарды долларов. Тем не менее, несмотря на потрясающие возможности современных компьютеров, мыслительные способности человеческого мозга для них недоступны.

Компьютеры способны быстро и точно обрабатывать огромные объемы числовых данных. Однако в том виде, как мы знаем их сейчас, они остаются рабами программистов: они не могут принимать решения или выполнять действия, которые не были заранее запрограммированы. Думающий компьютер будет устройством совершенно другого типа.

Когда такие устройства будут созданы (если, конечно, будут), их объединение в сеть для разделения информации представляется неизбежным и вполне естественным. Многие исследователи считают, что в будущем (видимо, весьма отдаленном) в сеть будут объединены не только устройства искусственного интеллекта, но человек сумеет подключить непосредственно к такой сети и собственный мозг, образуя некое частично органическое, частично техническое существо.

Вершина развития сетевых технологий — кибернетические формы жизни

Распространенная тема многих современных научно-фантастических романов — кибернетические формы жизни, в которых человек, или *киборг*, с имплантированными электронными и механическими органами подключен к суперсети, делающей его частью некоего "коллективного сознания". Как известно, кибернетика является областью серьезных исследований во многих университетах различных стран мира. Некоторые исследователи считают, что путем объединения человеческого тела с компьютерными устройствами люди смогут достичь бессмертия.

Резюме

В этой главе рассмотрено будущее сетей и коммуникационных технологий, обещающих радикально изменить мир, в котором мы живем.

Сначала была представлена концепция всеобщей компьютеризации, которая быстро воплощается в реальность и меняет принципы работы Internet и других сетей. Вы узнали о предполагаемых путях преодоления ограничений протокола Internet, включая такие временные меры, как применение методов NAT и CIDR, широко реализуемых уже сегодня.

Затем было приведено радикальное решение проблемы нехватки IP-адресов: внедрение новой версии IP, называемой IPv6. Рассмотрены характеристики нового протокола и методы как можно более безболезненного перехода на него с IPv4.

Далее были кратко затронуты некоторые новые направления сетевых технологий, такие, как нейронные и квантовые сети.

Рассмотрена концепция всеобщего соединения с Internet и ее влияние на нашу жизнь как на работе, так и дома. Представлены разрабатываемые в настоящее время проекты "интеллектуальных устройств" и "интеллектуального дома" и некоторые социальные и правовые вопросы, возникающие вследствие все большего превращения нашего мира в одну "большую деревню".

Более подробно описано влияние современных сетевых технологий на работу государственных органов, на законодательство, медицину и издательское дело. Показано, как развитие коммуникационных технологий способно радикально изменить характер этих профессий. Приведены новые способы обучения, которые становятся возможными благодаря доступу в Internet, и пути приспособления традиционных моделей образования к новым коммуникационным технологиям.

И наконец, эта глава и вся книга завершилась кратким экскурсом в более отдаленное будущее; были рассмотрены перспективы реализации таких невероятных (на сегодняшний день) фантазий, как искусственный интеллект и кибернетические формы жизни.

Изучая материал этой книги, вы прошли от основ технологии компьютерных сетей до областей, имеющих сегодня лишь теоретическое значение. Мы завершаем курс обучения догматом, справедливым с самого начала развития персональных компьютеров и компьютерных сетей: сегодняшние технологии, какими бы изощренными и сложными они ни казались, неизбежно поблекнут в сравнении с технологиями завтрашнего дня.

Рекомендуемые источники

Прекрасная статья о протоколе IPv6 находится по адресу: `http://playground.sun/com/pub/ipng/html/INET-IPng-Paper.html#CH1`.

Подробное обсуждение сети IPv6 6bone можно найти по адресу: `http://www.6bone.net`.

Хорошее, краткое и простое объяснение теорий квантовой физики приведено по адресу: `http://www.jracademy.com/~jtucek/science/what.html`.

Дополнительную информацию о различных аспектах конфиденциальности в Internet можно найти на Web-узле организации Electronic Privacy Information Center по адресу: `http://www.epic/org`.

Web-узел, посвященный информационным технологиям, используемым правительством США, находится по адресу: `http://www.govtech.net`.

Подробный обзор взглядов и концепций китайского правительства на характер войн двадцать первого столетия приведен на Web-узле организации Institute for National Strategic Studies по адресу: `http://www.ndu.edu/inss.books.chinview/chinapt4.html`.

Дополнительная информация о портативных компьютерах для медиков приведена по адресу: `http://www.handheldmed.com`.

Хороший источник информации и ссылок по методам дистанционного образования расположен по адресу: `http://www.dlrn.org`.

Научное издание *Journal of Artificial Intelligence Research* находится по адресу: `http://www.cs.washington.edu/research/jair/home.html`.

Начальная страница организации American Society for Cybernetics: `http://gwis.circ.gwu.edu/~asc/asc-cyber.html`.

Заключительные вопросы

Завершая изучение материала книги и начиная свою карьеру в области компьютерных сетевых технологий, попытайтесь ответить на несколько провокационных вопросов, призванных подтолкнуть вашу мысль в определенном направлении.

- Каким образом вы будете использовать компьютеры на вашей работе через три года? Как это будет отличаться от способов их использования сейчас?
- Как повлияют компьютеры на ваши личные отношения? Будет ли вообще ощущаться это влияние?
- Какие изменение произойдут в вашей жизни — эмоциональной, физической, финансовой — благодаря развитию компьютерных технологий?

- Как много времени вы будете тратить на изучение компьютерных технологий в следующее десятилетие?
- Как много из того, что вы знаете о компьютерах сейчас, будет полезным для вас через три года? Через десять лет?
- Сможете ли вы с помощью Internet зарабатывать деньги в вашем собственном бизнесе через год? Какой бизнес на основе Internet вы можете основать? Будет ли он приносить доход, окупающий хотя бы затраченное время?
- На какой работе с хорошим доходом в компании, занимающейся информационными технологиями, вы сможете продержаться в течение года?
- Будете ли вы когда-нибудь голосовать за киборга на должность президента?
- Станете ли вы следующим Биллом Гейтсом или Стивом Джобсом и добьетесь ли славы и богатства как исключительно удачливый предприниматель в области информационных технологий?

Приложение

Ответы на контрольные вопросы

В этом приложении даются ответы на контрольные вопросы, приведенные в конце каждой главы.

Глава 1

1. **б.** Оптическая телеграфная сеть была разработана во Франции в начале девятнадцатого века. Ее пропускная способность составляла 20 символов в секунду. Приблизительно в то же время Самюэль Морзе впервые продемонстрировал работу электрического телеграфа в США. Телефонной сети не существовало вплоть до конца девятнадцатого века, а Ethernet впервые была реализована исследовательским центром в Пало-Альто в 60-х годах двадцатого века. Сеть ARPAnet тоже появилась лишь в 1960-х годах.
2. **г.** В телефонной сети сигналы передаются по коммутируемым каналам. Это означает, что канал устанавливается на время сеанса связи. После разрыва соединения и его повторной установки сигнал может проходить по совершенно другому каналу цепи. Более новая технология — коммутация пакетов — используется в компьютерных сетях. Коммутация на уровнях 2 и 3 используется в локальных сетях для повышения производительности соединения путем создания выделенных маршрутов от одного компьютера к другому.
3. **а.** Технология коммутации пакетов была разработана в Массачусетском технологическом институте, RAND Institute и Национальной физической лаборатории (Англия) специально для передачи данных, поступающих крупными порциями, т.е. во взрывообразном режиме. Технология коммутации каналов лучше подходит для передачи голосовых сигналов, являющихся более плавными. Термин "аналоговая передача" означает метод прохождения сигналов, а "коммутационные панели" — это устройства, предназначенные для соединения цепей вручную.
4. **а, в.** Оборудование для мэйнфреймов более дорогое, чем для персональных компьютеров. Традиционно мэйнфреймы менее отказоустойчивы, потому что полностью зависят от бесперебойной работы центрального процессора. Их терминалы не

имеют собственных вычислительных мощностей и при выходе из строя мэйнфрейма становятся бесполезными. Мэйнфреймы способны обрабатывать огромные объемы данных. Персональные компьютеры менее безопасны, чем мэйнфреймы, потому что в их состав входят жесткие и гибкие диски, с помощью которых пользователи могут устанавливать свои программы (потенциально содержащие вирусы) или копировать ценные данные и уносить их с собой.

5. **а, б, в, г.** Сетевые компьютеры способны разделять как аппаратные, так и программные ресурсы. Пользователи могут передавать по сети данные на принтер, разделять модемные соединения (если установлены соответствующие программы), получать доступ к данным, хранящимся в любом месте сети (если их учетные записи имеют соответствующие права доступа), и выполнять приложения, установленные на серверах приложений.

6. **б, в.** Факсы относятся к устройствам как ввода, так и вывода, потому что они могут и принимать и передавать данные. Цифровые видеокамеры являются устройствами ввода, они преобразуют изображение к цифровому виду и передают его в компьютер. Плоттеры и принтеры являются устройствами вывода: они принимают данные от компьютера и распечатывают их на бумаге.

7. **г.** Служба DNS (Domain Name System) была разработана в 1980-х годах в связи с тем, что количество главных компьютеров (хостов) сети ARPAnet слишком увеличилось и возникла необходимость в эффективном и удобном способе разрешения имен хостов. Министерство обороны США (Department of Defence — DoD) принимало участие в создании ARPAnet. Служба DHCP (Dynamic Host Configuration Protocol) предназначена для автоматического присвоения компьютерам IP-адресов. DSL (Digital Subscriber Line) — это высокоскоростной канал связи, предоставляемый телефонными компаниями во многих регионах для передачи данных и голоса.

8. **б.** Методы телефонии объединяют телекоммуникационные и компьютерные технологии, реализованные в соответствии со спецификациями TAPI (Telephony Applications Programmers Interface), разработанными компанией Microsoft. Консорциум ITC (Internet and Telecoms Convergence) разрабатывает и внедряет стандарты телефонии.

9. **в.** В сети клиент/сервер компьютер, запрашивающий данные другого компьютера, называется клиентским. Компьютер, разделяющий свои данные с клиентскими компьютерами, называется сервером. Рабочая станция может быть клиентским компьютером, однако это не обязательно — некоторые рабочие станции представляют собой изолированные системы, не имеющие доступа к сетевым ресурсам. Терминал не является собственно компьютером, это всего лишь устройство ввода и вывода, подключенное к компьютеру (чаще всего к мэйнфрейму).

10. **а.** Наборы правил, которых придерживаются сообщающиеся друг с другом компьютеры, называются протоколами. Эти правила определяют формат передаваемых данных и последовательность их обработки. Тип носителя означает физический тип среды передачи данных — кабель, радиоволны, световые лучи и т.д. Байт — это единица количества информации, равная восьми битам. В байтах принято выражать размер файлов, объем памяти или объем данных, передаваемых по сети. Топология — это физическая или логическая форма (конфигурация) сети.

Глава 2

1. **б.** В классификации по физической области, охваченной сетью, сети подразделяются на глобальные (Wide Area Network — WAN), локальные (Local Area Network — LAN) и городские (Metropolitan Area Network — MAN). Термин 10Base2 обозначает архитектуру сети. Термин "сеть IPX/SPX" означает, что в сети используется протокол IPX/SPX. Кольцо — это тип сети в классификации на основе топологии.
2. **в, г.** По физической области действия локальные сети самые маленькие. Географически они ограничены небольшой областью, компьютеры локальной сети расположены близко друг к другу. Городские и глобальные сети состоят из большого количества локальных сетей. Узлы в различных городах, штатах и странах имеют глобальные, а не локальные сети.
3. **а.** Термин "сеть internet" означает группу сетей, объединенных друг с другом. Наиболее характерный пример сети internet — глобальная сеть Internet. В интрасетях и экстрасетях используются такие средства Intetnet, как броузеры, однако они являются частными сетями, предназначенными для ограниченного круга пользователей. Рабочая группа — это несколько компьютеров, пользователи которых получают доступ к одним и тем же ресурсам.
4. **б, в, г.** Сети типа клиент/сервер обеспечивают централизованное хранение данных на серверах, что облегчает резервное копирование данных. Для их обслуживания необходим сетевой администратор, потому что на серверах выполняются довольно сложные сетевые операционные системы. Централизованное администрирование, применяемое в сетях клиент/сервер, обеспечивает более высокую безопасность данных. Однако реализация таких сетей более дорогая, потому что для их развертывания нужно покупать дорогое программное обеспечение сервера и нанимать одного или нескольких сетевых администраторов.
5. **в.** Сети клиент/сервер компании Microsoft состоят из групп компьютеров и ресурсов, которые называются *доменами*. Сервер, на котором пользователь регистрируется для получения доступа к домену, называется контроллером домена. Демон — это программа системы UNIX, выполняющаяся непрерывно и обрабатывающая передаваемые на нее запросы. Термин SAM (Security Accounts Manager) означает базу данных, в которой хранится регистрационная информация пользователей и групп пользователей в системе Windows NT. На кластерном сервере выполняется программное обеспечение, объединяющее несколько серверов в группу, работающую как один сервер. Метод кластеризации применяют для повышения отказоустойчивости и балансировки нагрузки серверов.
6. **в, г.** В рабочей группе каждый компьютер поддерживает отдельную регистрационную базу данных. Пользователь должен иметь учетную запись на каждом компьютере, к которому он хочет получать доступ. Если пароли присваиваются каждому разделяемому ресурсу, то это называется безопасностью на уровне разделяемых ресурсов. В отличие от среды клиент/сервер, в рабочей группе система безопасности не централизована и сетевой администратор не управляет ею. Управление регистрационной информацией выполняется локально пользователем каждого компьютера, на котором размещены разделяемые ресурсы. Поэтому в одноранговой сети уровень безопасности ниже, чем в сети клиент/сервер, и ее легче взломать.

7. **а, г.** В системе Windows NT база данных SAM (Security Account Manager) расположена на первичном контроллере доменов. В отличие от этого, домены Windows 2000 собраны в Active Directory. В сети Windows 2000 может быть много контроллеров доменов, причем каждый из них может как читать, так и записывать регистрационную информацию в базе данных службы каталогов. В то же время в Windows NT вносить записи в регистрационную базу данных может только первичный контроллер домена. Bindery — это регистрационная база данных, использовавшаяся серверами NetWare 3.*x*. *Домены Windows NT иногда называют доменами нижнего уровня.*

8. **а, б.** Протокол TCP/IP разрабатывался для сетей средних и больших размеров. Для сетей малых размеров лучше подходят протоколы NetBEUI или IPX/SPX, они проще и обладают более высоким быстродействием. Internet работает на основе протокола TCP/IP. Для администрирования, мониторинга и устранения неполадок в сетях TCP/IP разработано огромное количество различных инструментов и утилит. Несмотря на это, вследствие сложности схемы адресации, некоторых особенностей маршрутизации и большого размера сетей выполнять задачи администрирования в сетях TCP/IP труднее, чем в NetBEUI.

9. **в.** В шинной топологии компьютеры расположены по линии, кабель идет от одного компьютера к другому, затем к следующему и т.д. Для предотвращения отражения сигналов от концов кабеля, что нарушает нормальную работу сети, на каждом конце кабеля должно быть установлено устройство, называемое терминатором. В звездообразной сети каждый компьютер соединен с центральным концентратором. В смешанной ячеистой топологии между некоторыми компьютерами (но не между всеми) установлены дополнительные избыточные связи. Название сетей Token Ring означает архитектуру, а не топологию. Обычно сети Token Ring физически реализуются в звездообразной топологии, в которой все компьютеры подключены к центральному устройству, называемому MAU (Multistation Access Unit). Внутри MAU сигналы проходят по логическому кольцу.

10. **б.** Спецификации сетей 10BaseT обусловливают применение топологии звезды и неэкранированной витой пары, обычно категории 5. В сетях 10Base2 используется тонкий коаксиальный кабель и шинная топология. Сети 100BaseFL работают на волоконно-оптических кабелях. В сетях Token Ring обычно используются экранированные витые пары.

Глава 3

1. **б.** В шестнадцатеричной системе счисления для представления чисел используются цифры от 0 до 9 и буквы от A до F. В компьютерных технологиях эта система счисления используется довольно часто, потому что шестнадцатеричные числа значительно легче преобразуются в двоичные (с которыми работает процессор), чем десятичные в двоичные. Десятичная система счисления используется людьми в повседневных расчетах. Основанием десятичной системы является число 10. Машинным кодом называется последовательность битов (двоичных чисел), управляющая работой компьютера.

2. **а.** Двоичная цифра (и число) называется битом. Байт равен восьми битам. q-бит — это квантовый бит, представляющий собой не дискретное состояние ви-

да включено—выключено, а неопределенное состояние, зависящее от наблюдения. Гигабайт равен 1024 мегабайтам, или 1 073 741 824 байтам.

3. **в.** В двоичном числе 10010001 включены биты, представляющие десятичные значения 1, 16 и 128. Сумма этих значений равна 145. Выключенные биты (представленные нулями) имеют значения, равные нулю, следовательно, они не влияют на результат. Преобразование двоичных чисел в десятичные выполняется путем суммирования всех битов, представленных единицами. Десятичное число 256 представляется двоичным числом 100000000, 128 — 10000000, а 64 — 1000000.

4. **б.** Порция данных, передаваемая по сети отдельно, называется пакетом (иногда кадром или сегментом). Шестнадцатеричные числа — это числа в шестнадцатеричной системе счисления. Заголовком называется часть пакета, несущая служебную информацию (адреса, последовательность сборки и т.д.) и присоединенная сетевыми протоколами к началу пакета. Биты действительно передаются по сети, однако файлы данных разбиваются не на отдельные биты, а на группы битов (пакеты).

5. **г.** Компонент трейлера, предназначенный для обнаружения ошибок, называется кодом CRC (Cyclical Redundancy Check). Проверка выполняется следующим образом. В передающем компьютере над исходными данными выполняются двоичные вычисления по алгоритму CRC. Затем эти же вычисления выполняются над данными, поступившими на принимающий компьютер. Если результаты этих двух вычислений совпадают, значит, данные в процессе передачи не изменились. В трейлере нет проверочного бита. Кадр — синоним термина "пакет" — это порция данных, передаваемая по сети отдельно. Протокол UDP (Use Datagram Protocol) представляет собой протокол транспортного уровня, входящий в состав набора TCP/IP и работающий в режиме без установки соединения.

6. **б.** Модель определяется как "Схематическое описание системы, теории или явления, включающее его известные или изучаемые свойства и используемое для дальнейшего изучения его характеристик". Модель сети используется для графического представления протекающих в сети процессов. Протокол — это набор правил, которых придерживаются сообщающиеся друг с другом компьютеры. Процесс — это последовательность действий или изменений, приводящая к некоторому результату. Уровнем называется часть набора протоколов, в котором выполняются характерные для этого уровня операции. Популярные сетевые модели OSI и DoD называются уровневыми моделями, так как они разбиты на уровни.

7. **б.** Канальный уровень (уровень 2) разделен на подуровни MAC (Media Access Control — управление доступом к среде) и LLC (Logical Link Control — управление логическими связями). Физический, сетевой и транспортный уровни не делятся на подуровни.

8. **а.** Физический уровень не добавляет заголовочную информацию, потому что он работает с оборудованием и сигналами. Канальный, сеансовый и прикладной уровни (а также сетевой и представления) добавляют заголовочную информацию, которая обрабатывается принимающим компьютером на соответствующем уровне.

9. **в.** NetBIOS и Winsock — два распространенных протокола сеансового уровня. С помощью протокола NetBIOS выполняется установка соединения двух компьютеров, обнаружение ошибок и восстановление. Протокол TCP (Transmission Control Protocol), как и UDP (User Datagram Protocol), работает на транспорт-

ном уровне. Протокол IPX, как и IP, работает на сетевом уровне. Telnet — это протокол прикладного уровня.

10. **г.** Активный концентратор является повторителем. К его портам может быть подключено много станций. Прежде чем передать сигнал на другие компьютеры сети, активный концентратор регенерирует его. Мост — это устройство уровня 2, используемое для сегментации и уменьшения загрузки сети. Маршрутизатор — это устройство уровня 3, перемещающее пакеты из одной подсети в другую. Коммутатор, в зависимости от реализации, может принадлежать уровням 2, 3 или 4. Он передает сигнал только на порт, подключенный к компьютеру, которому адресован пакет.

Глава 4

1. **б.** Процесс преобразования данных, сгенерированных компьютером, в импульсы электрической или световой энергии называется кодированием. Шифрование означает преобразование данных к формату, в котором их не смогут прочитать посторонние лица. Обеспечение безопасности — это защита данных путем шифрования, установкой прав доступа и другими методами. Цикличность — это процесс периодического изменения аналоговых сигналов.
2. **г.** Цифровые сигналы называются сигналами с дискретными состояниями потому, что они переходят из одного состояния в другое почти мгновенно, не задерживаясь в промежуточных состояниях. Плавно и постоянно изменяющаяся электромагнитная волна является аналоговым сигналом. Периодический аналоговый сигнал характеризуется тремя параметрами — амплитудой, частотой и фазой.
3. **в, г.** Аналоговые сигналы легче мультиплексировать (т.е. передавать по одному каналу много сигналов одновременно), чем цифровые. Они также менее чувствительны к затуханию (ослаблению сигнала с увеличением расстояния). Однако аналоговые сигналы более чувствительны к помехам (электромагнитным, перекрестными и другим). Цифровые устройства дешевле, потому что цифровые сигналы проще аналоговых.
4. **а.** В технологиях на основе немодулированных сигналов, таких, как Ethernet, для передачи данных по одному каналу пропускная способность кабеля используется полностью. В технологиях с модулированными сигналами, таких, как DSL (Digital Subscribe Line), пропускная способность разделяется на много каналов. При мультиплексировании по одному каналу передается много сигналов одновременно, что увеличивает пропускную способность канала. Мультисоединения используются для повышения пропускной способности аналоговой телефонной линии или линии ISDN (Integrated Services Digital Network).
5. **а, г.** Немодулированные сигналы являются двунаправленными — они могут проходить в обоих направлениях, поэтому их можно передавать и принимать по одному и тому же каналу. Немодулированные сигналы обычно используются в цифровых технологиях передачи данных, хотя их можно применять и в аналоговых устройствах. В технологиях кабельного телевидения используются модулированные сигналы. В них сигналы распределяются по десяткам различных каналов. Модулированные сигналы являются однонаправленными, однако полоса пропускания канала

может быть разделена на несколько каналов, одни из которых могут работать в одном направлении, а другие — в противоположном.

6. **в.** Для передачи сигналов по волоконно-оптическим кабелям используется метод, называемый мультиплексированием по длине волны высокой плотности. В этом методе сигналы передаются в обоих направлениях, причем каждый сигнал передается на отдельной длине световой волны. В методе частотного разделения каналов линия делится на несколько каналов, каждый из которых располагается на своей частоте. В методе временного разделения сигналов они (сигналы) разбиваются на сегменты и передаются по линии в течение коротких промежутков времени, каждый из которых выделен отдельному сегменту.
7. **г.** В асинхронном методе для определения начала и конца передачи и синхронизации передающего и принимающего устройств используются стартовый и конечный биты. При синхронной передаче используется встроенный часовой механизм и различные методы синхронизации, включая гарантированное изменение состояния (наиболее распространенный метод) и стробирование.
8. **б.** В полудуплексном методе связи сигналы могут передаваться в обоих направлениях, но не одновременно. В настоящее время такой метод используется редко, так как он неудобен. В прошлом он широко использовался в различных радиотехнических устройствах связи, например в полицейских переносных радиостанциях. В традиционной системе телевидения используется симплексный метод, в нем сигналы передаются только в одном направлении. В телефонных линиях и линиях DSL (Digital Subscriber Line) используется дуплексный метод, в котором сигналы передаются в обоих направлениях одновременно.
9. **а.** Наиболее чувствительна к электромагнитным помехам неэкранированная витая пара, хотя скручивание пары проводов значительно уменьшает чувствительность к помехам. Коаксиальный кабель и экранированная витая пара защищены от электромагнитных помех внешним металлическим экраном, однако помехи в некоторой степени все же могут проникать внутрь экрана. В волоконно-оптическом кабеле используются световые, а не электрические импульсы, они совершенно нечувствительны к электромагнитным помехам, поэтому их рекомендуется использовать в зонах с повышенным уровнем помех.
10. **б.** В сетях Ethernet используется метод доступа CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением конфликтов). Метод CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance — множественный доступ с контролем несущей и предотвращением конфликтов) используется в сетях AppleTalk. Передача маркера используется в сетях Token Ring, а приоритеты запросов — в малораспространенных сетях 100VG-AnyLAN.

Глава 5

1. **б.** Спецификации 802.3 обусловливают использование в сетях Ethernet метода доступа CSMA/CD. Сети Token Ring и FDDI основаны на спецификациях 802.5, а сети ARCnet приблизительно соответствуют спецификациям 802.4. Комитет 802 организации IEEE (Institute of Electrical and Electronics Engineers) разработал стандарты IEEE 802 для протоколов физического и канального уровней.

2. **а.** В сетях Ethernet используется метод доступа CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением конфликтов). В этом методе компьютер, которому в текущий момент нужно передать данные, прослушивает кабель и передает данные, только если кабель не занят. Если два компьютера сделают это одновременно, происходит коллизия данных. Оба компьютера обнаруживают коллизию и после короткого случайного интервала времени опять прослушивают кабель и передают эти же данные. Метод CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance — множественный доступ с контролем несущей и *предотвращением* конфликтов) используется в сетях AppleTalk. В сетях Token Ring, ARCnet и FDDI используется передача маркера, а в 100VG-AnyLAN — приоритеты запросов.

3. **а.** Согласно спецификациям Ethernet 10Base2 при использовании тонкого коаксиального кабеля максимальное количество узлов на сегмент кабеля (отрезок кабеля между двумя повторителями) равно 30. Узел — это компьютер или другое сетевое устройство, передающее или принимающее данные посредством сети.

4. **в.** Разъем BNC используется с тонкими коаксиальными кабелями в сетях Ethernet 10Base2. С неэкранированными витыми парами в сетях 10BaseT используются разъемы RJ, чаще всего — RJ-45. С толстыми коаксиальными кабелями в сетях 10Base5 используются 15-контактные разъемы AUI. С помощью разъема AUI компьютер подключается к внешнему трансиверу, который подключается к кабелю посредством устройства, называемого "зубом вампира". С волоконно-оптическими кабелями используются разъемы SMA и FSMA.

5. **г.** Термин "стандартная Ethernet" означает сеть 10Base5. Другое ее название — толстая сеть. Архитектура 10Base5 менее популярна, чем другие архитектуры Ethernet. Наибольшее распространение получили сети Ethernet на основе витых пар. Сеть 10Base5 была "стандартной", когда в 1960-х годах началась разработка Ethernet, с тех пор ее так и продолжают называть.

6. **б.** Спецификации 10Base5 определяют максимальную длину сегмента толстого коаксиального кабеля равной 500 метрам. Для сравнения: в 10BaseT максимальная длина сегмента равна 100 метрам, а в 10Base2 — 185 метрам. Большая допустимая длина сегмента позволяет использовать фрагмент толстой сети в качестве "магистрали" для тонкой сети. Спецификации IEEE определяют длину кабеля в метрах. В США распространенной единицей длины все еще остается фут. Максимальная длина сегмента 10Base5 равна 1 640 футам.

7. **б, в.** В зависимости от используемых сетевых адаптеров и концентраторов, пропускная способность сетей Token Ring может составлять 4 или 16 Мбит/с. Концентратор Token Ring называется устройством MAU или MSAU (Multistation Access Unit — устройство многостанционного доступа). В сетях Token Ring используется активная топология, т.е. на каждой станции, прежде чем передать сигналы обратно в кольцо, они регенерируются. Как и в Ethernet, в Token Ring используются немодулированные сигналы, занимающие всю полосу пропускания кабеля.

8. **в.** Управляющий компьютер посылает кадр, называемый маяком. Каждый компьютер, готовый передавать данные, ожидает получения маяка. Если компьютер получает маяк, то он передает на управляющий компьютер свой адрес и адрес компьютера NAUN (Nearest Active Upstream Neighbor — ближайший

активный сосед сверху). После этого устройство MSAU реконфигурирует путь сигнала в целях исключения неработающей станции и восстановления нормальной коммуникации остальных компьютеров кольца. Маркер — это сигнал, передаваемый по кругу. Прежде чем начать передавать данные, станция должна дождаться маркера. Кадр данных содержит передаваемую информацию.

9. **б.** Для сети AppleTalk первоначально был разработан протокол канального уровня LocalTalk, предназначенный для быстрого и легкого объединения в сеть компьютеров Macintosh путем подключения кабелей к их принтерным портам. Пропускная способность LocalTalk составляет всего 230,4 Кбит/с. Со временем он был заменен архитектурой Ethernet в большинстве сетей Macintosh. Протокол EtherTalk позволяет компьютерам Macintosh, в которых выполняются протоколы верхних уровней AppleTalk, подключаться к коаксиальному кабелю сети Ethernet. Протокол TokenTalk позволяет компьютерам Macintosh подключаться к сетям Token Ring.

10. **а.** Стандартная сеть ARCnet относительно медленная, ее пропускная способность составляет всего 2,5 Мбит/с. Среди популярных сетевых архитектур медленнее ARCnet только LocalTalk. Для преодоления этого ограничения разработана расширенная версия ARCnet, которая называется ARCnet Plus. Ее пропускная способность равна 20 Мбит/с, что вдвое превышает пропускную способность стандартной Ethernet и выше пропускной способности "высокоскоростных" сетей Token Ring, составляющей 16 Мбит/с.

Глава 6

1. **а, в, г.** Для внутренних модемов, не поддерживающих технологию Plug and Play, обычно конфигурируются адрес ввода-вывода, IRQ и параметры виртуального коммуникационного порта. Перечисленные конфигурационные параметры устанавливаются с помощью перемычек, микропереключателей или программными средствами. IP-адрес присваивается модемному соединению (внешнему сетевому адаптеру), когда компьютер подключается к сети TCP/IP, однако IP-адрес не является конфигурационным параметром оборудования.

2. **б.** Устройства CSU/DSU (Channel Service Unit/Data Service Unit — модуль обслуживания канала/модуль обслуживания данных) или PAD (Packet Assembler/Disassembler — сборщик/разборщик пакетов) относятся к оборудованию пользователя. Устройства CSU/DSU используются в качестве интерфейса с Т-линиями. Устройство CSU принимает и передает сигналы. Устройство DSU предназначено для управления линией, обработки ошибок синхронизации и регенерации сигналов.

3. **а.** Все перечисленные технологии основаны на коммутации каналов. В сетях с коммутацией каналов устанавливается соединение (канал), по которому данные передаются на протяжении сеанса связи. В сетях с коммутацией пакетов отдельные пакеты одного и того же сообщения могут проходить на принимающий компьютер разными путями. В сетях Switched 56 используется коммутация пакетов. Все перечисленные технологии являются технологиями глобальных сетей.

4. **б, в, д.** Линии ISDN (Integrated Services Digital Network) устанавливаются телефонными компаниями. Они дороже, чем аналоговые телефонные линии PSTN (Public Switched Telephone Network). Для линий ISDN на телефонной станции, обслужи-

вающей данный регион, должно быть установлено специальное оборудование, обрабатывающее цифровые сигналы, а у пользователя должен быть установлен терминальный адаптер ISDN (который иногда называют модемом ISDN). По линиям ISDN могут передаваться как голос, так и данные. По линии BRI (Basic Rate ISDN), состоящей из двух B-каналов, могут передавать данные и голос одновременно: по одному из B-каналов — голос, а по другому — данные.

5. **в.** Легче всего наращивать сеть, построенную по звездообразной топологии, потому что в ней добавление дополнительных узлов не требует реконфигурирования сети. Кольцевую топологию наращивать труднее, так как в ней для добавления узла нужно прервать соединение между двумя существующими узлами. Точечная топология не наращивается.

6. **б.** Первой коммуникационной технологией с коммутацией пакетов была X.25. Более новая технология Frame Relay, разработанная на основе X.25, несколько улучшена. Еще более новая технология ATM (Asynchronous Transfer Mode), в которой используется коммутация пакетов, обеспечивает высокую скорость передачи. В технологии DSL (Digital Subscriber Line) используется коммутация каналов.

7. **а, в, г.** Технология Frame Relay обеспечивает более высокую производительность, чем X.25, вплоть до 45 Мбит/с. В отличие от X.25, в Frame Relay не выполняется обнаружение ошибок, потому что в ней используются надежные цифровые сигналы. В технологии X.25 используются аналоговые сигналы. Как Frame Relay, так и X.25 основаны на коммутации пакетов.

8. **в, г, д.** Особенностью ATM (Asynchronous Transfer Mode) является использование ячеек данных с фиксированной длиной 53 байт. Это высокоскоростная технология, предназначенная для одновременной передачи видео, голоса и данных. В технологии ATM используются предопределенные каналы.

9. **г.** Средства технологии OS-SONET уровня OC-48 обеспечивают скорость передачи 2,488 Гбит/с. Пропускная способность ADSL (Asymmetric DSL) находится в диапазоне от 384 Кбит/с до 6 Мбит/с. Максимальная пропускная способность линий T-1 составляет 1,544 Мбит/с. Линия ISDN BRI (два канала по 64 Кбит/с каждый) имеет пропускную способность 128 Кбит/с.

10. **в, г.** В методе NAT (Network Address Translation) используется таблица, отображающая много частных внутренних IP-адресов на один или несколько публичных адресов. Это избавляет от необходимости регистрировать публичный адрес отдельно для каждого компьютера внутренней сети. Однако метод NAT не может применяться совместно с протоколами шифрования. Кроме того, метод NAT несовместим с некоторыми приложениями.

Глава 7

1. **в.** К компьютеру подключается сетевой адаптер — основной компонент сетевого оборудования. Он играет роль интерфейса с сетью и необходим для каждого сетевого компьютера. Большинство сетевых адаптеров помещаются в разъем ISA/EISA, PCI или PCMCIA. Иногда сетевой адаптер интегрируется в системную плату компьютера. Маршрутизатор используется для передачи пакетов из одной сети в другую. Кабель является сетевым носителем, используе-

мым в традиционных сетях, однако в беспроводных сетях кабели не нужны. Концентратор используется для соединения компьютеров.

2. **б.** Внешний трансивер используется в сетях 10Base5. Он подключается к сетевому адаптеру посредством разъема AUI и к толстому коаксиальному кабелю с помощью "зуба вампира". В сетях 10Base2 (тонкие сети) и 10BaseT (сети на основе неэкранированных витых пар) используются внутренние трансиверы, т.е. встроенные в сетевые адаптеры.

3. **а.** Число IRQ, равное 5, часто используется для звуковой карты. Однако в данном примере для звуковой карты используется IRQ 10. По умолчанию для параллельного принтерного порта LPT1 (если он используется) установлено IRQ 7. Для контроллера IDE используется IRQ 14. Параллельный порт LPT2 в данном примере не упоминается. Следовательно, IRQ 5 свободно и его можно использовать для сетевого адаптера.

4. **г.** Пространство между полом и фальшь-полом называется пленумом. Строительные и пожарные правила требуют установки в пленуме специального пленум-кабеля, оболочка которого сделана из тефлона, или другого пожаробезопасного материала, а не из поливинилхлорида, которым покрывается обычный кабель.

5. **в.** Спецификации 10Base2 определяют использование тонкого коаксиального кабеля RG-58 A/U с многожильным сердечником. Внешне на него похож кабель RG-58 /U, однако его сердечник одножильный, поэтому он не удовлетворяет спецификациям 10Base2. Кабель RG-58 C/U представляет собой "военный" вариант кабеля RG-58 A/U, у него более толстая внешняя оболочка. Использовать кабель GR-58 C/U в сетях 10Base2 можно, но не рекомендуется. Кабель RG-59 используется в кабельном телевидении.

6. **в.** "Зуб вампира" используется в сетях 10Base5 для подключения толстого коаксиального кабеля к внешнему трансиверу. К сетевому адаптеру внешний трансивер подключается с помощью разъема AUI. Экранированные и неэкранированные витые пары и тонкий коаксиальный кабель используются в сетях, в которых трансивер встроен в сетевой адаптер.

7. **г.** Скручивание проводов уменьшает перекрестные помехи, представляющие собой нежелательный перенос сигналов с одного кабеля на другой, расположенный близко к первому. При увеличении количества витков на единицу длины перекрестные помехи уменьшаются. Скручивание проводов уменьшает также электромагнитные помехи, однако они порождаются не соседним кабелем, а другими радиотехническими устройствами. Затухание — это уменьшение интенсивности сигнала с увеличением расстояния. Искажения — это нежелательное изменение формы аналогового сигнала в процессе его передачи по линии.

8. **а.** В сетях Ethernet с неэкранированной витой парой категории 5 используются разъемы RJ-45. Вилка и розетка RJ-45 внешне похожи на вилку и розетку телефонного разъема RJ-11, однако у RJ-45 они немного больше. Разъем BNC используется с тонкими коаксиальными кабелями в сетях 10Base2. Разъем F используется для соединения двух отрезков телевизионного коаксиального кабеля.

9. **б, г.** Волоконно-оптический кабель обеспечивает большую безопасность данных, чем медный. К нему труднее подключиться и перехватить передаваемые по нему сигналы, потому что сигналами в нем являются не электрические, а световые импульсы. В одномодовом режиме пропускная способность волоконно-оптического

кабеля выше, чем в многомодовом, так как в многомодовом режиме импульсы света "размазываются" по длине кабеля, что вынуждает увеличивать длину импульсов. Волоконно-оптический кабель труднее установить, чем медный. С ним также труднее работать. Устанавливать волоконно-оптический кабель может только обученный этому специалист, потому что при установке нужно точно подогнать торцы тончайших стеклянных или пластмассовых нитей. Волоконно-оптический кабель менее чувствителен к затуханию, чем медный, поэтому по нему можно передавать сигналы на большее расстояние.

10. **в.** Для соединения двух сегментов кабеля и регенерации сигналов, передаваемых с одного сегмента на другой, используется повторитель. Применение этих устройств нивелирует эффект затухания и позволяет увеличить расстояние между компьютерами локальной сети. Цилиндрический разъем, коммутационная панель и пассивный концентратор не регенерируют сигналы, это довольно простые сетевые устройства. Однако активный концентратор может работать как многопортовый повторитель.

Глава 8

1. **в.** Немаршрутизируемым высокопроизводительным протоколом является NetBEUI. Его легко конфигурировать. Поскольку в нем не используется логическая адресация, он не поддерживает маршрутизацию в другие сети или подсети. Протокол NetBEUI используется для небольших рабочих групп с операционными системами Microsoft.
2. **а.** Частью адреса IPX, основанной на MAC-адресе устройства, является номер узла, идентифицирующий сетевое устройство. *Он записывается в шестнадцатеричной системе и совместно с номером сети используется для маршрутизации пакета IPX на принимающий компьютер.*
3. **а, д.** Протоколы транспортного уровня TCP и SPX, прежде чем начать передавать данные, устанавливают соединение. Протокол транспортного уровня UDP и протоколы сетевого уровня IP и IPX не устанавливают соединение.
4. **б, в.** IP-адрес представляет собой 32-разрядное двоичное число, состоящее из четырех октетов по восемь бит каждый. Компьютер обрабатывает IP-адреса как двоичные числа, однако их принято записывать десятичными числами с точками.
5. **в.** В методе классовой адресации может существовать до 16 384 сетей класса B, каждая из которых содержит 65 535 допустимых адресов хостов. Максимальное количество допустимых сетей класса A равно 126, каждая из них содержит более 16 млрд адресов. Допустимое количество сетей класса C равно 2 097 152, в каждой из них допускается до 254 хостов.
6. **б.** В сети класса C, не разделенной на подсети, первые три октета адреса идентифицируют сеть. Биты номера сети "маскируются" единицами, по восемь единиц на каждый из трех октетов: 11111111.11111111.11111111. В десятичной системе счисления это записывается так: 255.255.255. Биты номера хоста (последний октет) открыты, это обозначается нулями: 00000000. В десятичной системе это записывается так: 0. Следовательно, в десятичной системе маска подсети выглядит так: 255.255.255.0.

7. **б.** В адресе класса B старшие биты равны 10. Поэтому в десятичной системе диапазон первого октета составляет 128–191. Адреса класса A находятся в диапазоне 0–127, класса B — в диапазоне 192–223, а класса C — в диапазоне 224–239.
8. **в.** В методе CIDR (Classless Interdomain Routing) более экономное использование IP-адресов достигается путем отказа от старого метода классовой адресации. При использовании CIDR максимальные размеры сетей могут находиться в промежутках между максимальными размерами сетей классов A, B и C.
9. **г.** Служба DHCP (Dynamic Host Configuration Protocol) предназначена для автоматического присвоения адресов компьютерам, сконфигурированным как клиенты DHCP. Присвоение выполняется в четырехэтапном процессе переговоров об аренде адреса между сервером и клиентом DHCP (обнаружение, предложение, запрос и подтверждение).
10. **в.** Утилита ARP отображает IP-адреса на физические MAC-адреса устройств. Она запускается из командной строки, с ее помощью можно просматривать кэш отображенных адресов, удалять записи и добавлять постоянные пары адресов IP–MAC.

Глава 9

1. **б.** Точки соединения с главной магистралью называются узлами. Хосты — это отдельные компьютеры в Internet. Подсети являются частями, на которые разбиты сети. Серверы — это компьютеры, разделяющие свои ресурсы с другими компьютерами посредством сети.
2. **г.** Главные провайдеры Internet соединены друг с другом в пунктах NAP с помощью коммутационного оборудования. Провайдеры услуг Internet — это компании, оборудование которых подключено к магистрали Internet для предоставления коммутируемого или выделенного доступа в Internet своим заказчикам. vBNS — это часть проекта Internet2 Project, разрабатываемого совместно университетами и правительством США в целях создания высокоскоростной магистрали Internet, которую предполагается использовать как тестовый полигон для проверки новых коммуникационных технологий. Сеть vBNS составляют пять мощных компьютерных центров.
3. **в.** Гипертекст может содержать встроенные ссылки на документы в других текстовых файлах, на графические, звуковые файлы и т.д. Обычно гипертекстовые файлы хранятся на Web-серверах, доступ к ним осуществляется посредством адресов URL. Примером гипертекстовых файлов являются справочные файлы в формате HTML. В состав гипертекстовых файлов могут быть встроены графические, звуковые и другие объекты.
4. **в.** Этот адрес URL идентифицирует страницу по умолчанию на Web-сервере `bigserver`, расположенном в домене второго уровня `acme`, зарегистрированном в домене верхнего уровня `com`. Многие Web-серверы начинаются с `www`, однако это *не обязательно*. В данном примере используется протокол HTTP. Для создания Web-страниц используется язык разметки HTML.
5. **б.** Портал — это Web-узел, служащий стартовой точкой для пользователя Web. Метапоисковая служба обобщает результаты поиска, полученные многими по-

исковыми службами, а шлюз по умолчанию — это IP-адрес маршрутизатора в сети TCP/IP. Гиперссылки — это встроенные в документы HTML указатели на другие файлы.

6. **г.** Процедуры протокола IMAP (Interactive Mail Access Protocol) предоставляют пользователям возможность просматривать и управлять сообщениями без выгрузки их на локальный компьютер. Протокол SMTP (Simple Mail Transfer Protocol) используется для передачи электронных писем посредством Internet. Процедуры SNMP (Simple Network Management Protocol) — это утилиты мониторинга, сбора информации и управления, включенные в состав набора TCP/IP. Протокол POP (Post Office Protocol) используется для загрузки электронных писем с почтового сервера на пользовательский компьютер, на котором выполняется клиентская почтовая программа.
7. **в.** Протокол NNTP (Network News Transfer Protocol), который иногда называют Usenet, используется для управления группами новостей и получения доступа к ним. Для управления списками рассылки используются программы Listserv и Majordomo. Протокол Telnet используется для подключения к удаленному компьютеру с целью просмотра файлов и выполнения не нем приложений.
8. **а.** Система IRC (Internet Relay Chat) позволяет пользователям подключиться к серверу IRC и подписаться на канал, в котором они могут вести текстовые беседы в реальном времени, причем количество участников беседы может быть больше двух. Протокол Telnet используется для подключения терминала к удаленному компьютеру, просмотра его файлов и выполнения на нем приложений. Протокол IGMP (Internet Group Multicast Protocol) используется для коммуникации. Протокол FTP (File Transfer Protocol) используется для загрузки файлов с другого компьютера посредством сети.
9. **б.** Стандарт H.323 организации ITU (International Telecommunication Union) описывает процессы мультимедийной коммуникации в протоколах IP и IPX, такие как видеоконференции.
10. **а, г.** Протокол RIP (Routing Information Protocol) представляет собой дистанционно-векторный протокол динамической маршрутизации, работающий в IP. Он используется в сетях небольших и средних размеров. Протокол RIP менее эффективен и менее приспособлен для наращивания сети, чем протокол динамической маршрутизации на основе состояния каналов OSPF (Open Shortest Path First), в котором сети делятся на области.

Глава 10

1. **в.** В приложениях клиент/сервер для запроса данных, хранящихся на сервере базы данных, используется внешний интерфейс, представляющий собой пользовательское приложение, которое выполняется на клиентском компьютере. Сортировка данных и обработка запроса выполняются на сервере, а на клиентский компьютер возвращается только результат запроса.
2. **б.** Файл, каталог или принтер, доступ к которому предоставляется посредством сети, называется разделяемым ресурсом.
3. **а.** По сравнению с системой безопасности на уровне ресурсов, в которой отдельный пароль присваивается каждому ресурсу, система безопасности на

уровне пользователей обеспечивает более высокий уровень безопасности. В ней пользователь вынужден помнить только один пароль. Облегчается также выполнение задач администрирования.

4. **а, в, г.** Административная учетная запись создается в процессе установки операционной системы. Она используется для регистрации в операционной системе при первой загрузке. Административная учетная запись имеет неограниченный доступ ко всем сетевым ресурсам, поэтому для нее нужно устанавливать криптографически сильный пароль. Она используется для выполнения задач администрирования, например для создания новых учетных записей пользователей.
5. **а, г.** Символы верхнего и нижнего регистров и цифры допускаются в именах учетных записей пользователей в любой системе, однако пробелов и таких символов, как "+", необходимо избегать. В некоторых операционных системах ограничивается количество символов в имени, однако имена длиной до 8 символов распознаются в любой системе, даже в MS DOS.
6. **в.** Домен Windows представляет собой набор пользователей, компьютеров и ресурсов, администрирование которых выполняется из одного центра. Домены Windows 2000 (но не Windows NT) могут быть организованы в иерархические структуры, называемые деревьями. В свою очередь, деревья можно сгруппировать в лес.
7. **б.** Для создания учетных записей пользователей домена и управления ими в контроллере доменов Windows NT 4.0 используется программа User Manager for Domains. Программа User Manager доступна в системах Windows NT 4.0 Workstation и на отдельных серверах, однако она используется для создания локальных учетных записей пользователей, используемых только на конкретном компьютере.
8. **в.** Служба Active Directory компании Microsoft представляет собой новую службу каталогов, на основе которой строятся сети Windows 2000. Она во многом аналогична службе NDS (Novell Directory Services), причем обе они удовлетворяют стандартам LDAP (Lightweight Directory Access Protocol).
9. **г.** На серверах NetWare 3.*x* используется плоская база данных, которая называется Bindery. В ней хранится регистрационная информация данного сервера. Регистрационная информация не реплицируется на другие серверы сети. В сетях NetWare 4.*x* и выше используется NDS (Novell Directory Services) — иерархическая распределенная база данных, позволяющая получать доступ ко всем ресурсам сети с помощью единственной учетной записи пользователя.
10. **а, в.** В отличие от Windows и NetWare, операционная система UNIX чувствительна к регистру. В ней служебные программы, такие, как принтерный сервер, называются демонами. Административная учетная запись в UNIX называется root, а группы системы UNIX похожи на локальные группы Windows NT 4.0.

Глава 11

1. **в.** Каталог — это база данных, содержащая разнородную информацию. В объектно-ориентированной системе каталог содержит объекты, каждый из которых имеет атрибуты.

2. **б.** Если данные, хранящиеся в некоторой базе данных, физически находятся на разных компьютерах сети, то такая база данных называется распределенной.
3. **б, в.** Однородными базами данных являются служба NTDS (NT Directory Services) системы Windows NT и служба Bindery, используемая в сетях NetWare 3.x. Базы данных NDS (Novell Directory Services) и Active Directory компании Microsoft являются иерархическими.
4. **г.** Непрерывным называется пространство имен, в котором в состав имени дочерних объектов входят имена родительских объектов. Пример непрерывного пространства имен — дерево доменов Windows 2000.
5. **в.** Спецификации OSI X.500 определяют процедуры агента DSA, управляющего данными каталога, агента DUA, с помощью которого пользователи получают доступ к службе каталогов, и базы данных DIB, в которой хранится информация каталога.
6. **в.** Имя DN (Distinguished Name) идентифицирует полный путь к объекту каталога с помощью атрибутов DC, OU и CN.
7. **а.** В службе NDS (Novell Directory Services) есть два базовых типа объектов: контейнерные, которые могут содержать другие объекты, и листовые, не содержащие других объектов и представляющие ресурсы на концах ветвей.
8. **г.** В файле SysVol (Shared System Volume) хранятся сценарии и объекты стратегии группирования, используемые администратором для управления средой пользователя и задания его прав.
9. **б.** В пределах дерева доменов Windows 2000 все домены имеют двусторонние транзитивные доверительные отношения. Это значит, что пользователи, принадлежащие к одному домену, могут получать доступ к ресурсам другого домена, если, конечно, их учетные записи имеют соответствующие права доступа.
10. **в.** В списке контроля доступа собраны все права доступа, присвоенные объекту Active Directory.

Глава 12

1. **а, б.** Текстовые операционные системы, такие, как DOS или UNIX, более быстродействующие, чем графические, такие, как Windows, потому что в них выполняется меньше служебных операций, на которые расходуются дополнительные системные ресурсы (память, процессорное время и др.). Однако графические операционные системы легче изучить и пользоваться ими удобнее. Кроме того, предоставляемый ими графический интерфейс позволяет работать в многозадачном режиме, т.е. выполнять несколько приложений одновременно.
2. **в.** С помощью команды `winipcfg` на экран в графическом формате выводится конфигурационная информация TCP/IP в системах Windows 95/98. В операционных системах Linux и UNIX для этого используется команда `ifconfig`, в Windows NT/2000 —команда `ipconfig`, а на серверах NetWare, на которых выполняется TCP/IP, — команда `config`.
3. **г.** Суффикс, используемый для определения типа файла, называется расширением. Ветви файла — это две части файла Macintosh. Файловая таблица — это

база данных, поддерживаемая файловой системой для отслеживания физического размещения данных каждого файла на дисках.

4. **а.** В отличие от FAT32 и NTFS, файловая система FAT16 поддерживается всеми операционными системами Microsoft, включая DOS, Windows 3.*x*, Windows 9*x*, Windows NT и Windows 2000. В системе FAT16 не поддерживаются средства обеспечения безопасности на уровне файлов как в NTFS, кроме того FAT16 менее надежна, потому что в нее не включены средства текущего устранения ошибок. В системе FAT16 выполняется меньше служебных операций, поэтому для небольших разделов диска ее производительность выше, чем производительность FAT32 и NTFS, однако на практике чаще всего используются большие разделы, для которых производительность FAT32 и NTFS выше.
5. **г.** В системе NTFS поддерживаются разделы объемом до 16 Эбайт. В операционной системе DOS объем раздела не может превышать 2 Гбайт, а в FAT16 — 4 Гбайт, независимо от типа операционной системы. Файловая система FAT32 поддерживает разделы объемом до 4 Тбайт.
6. **в.** В операционной системе UNIX корневой каталог представляется символом / без буквы в качестве части маршрута. Этим же символом разделяются уровни иерархии дерева каталогов. Для сравнения: в системах FAT и NTFS уровни иерархии разделяются символом \.
7. **б.** В файловой системе UNIX для идентификации каждого файла и каталога и для их отображения на физическое положение данных на диске используются внутренние номера, называемые i-узлами. В других файловых системах этот метод не используется, хотя в Macintosh HFS (Hierarchical File System) операции с записями каталогов немного похожи на отображение i-узлов.
8. **в.** Служба CSNW включена в состав Windows NT Workstation, однако по умолчанию она не устанавливается. Установив ее, можно регистрироваться на сервере NetWare и получать доступ к его файлам. Служба Gateway Services for NetWare устанавливается на Windows NT Server для предоставления ее клиентам доступа к файлам NetWare. Служба File and Print Services for NetWare позволяет клиентам NetWare получать доступ к файлам серверов Windows NT/2000. Для коммуникации с сервером NetWare должен использоваться протокол, совместимый с IPX/SPX, поэтому при установке CSNW автоматически устанавливается протокол NWLink, следовательно, устанавливать его явно не нужно.
9. **а.** Файловая система SMBFS (Server Message Block File System) основана на коде Samba. Ее можно установить в Linux для получения доступа к ресурсам Microsoft. Протокол разделения файлов NCP (NetWare Core Protocol) используется на серверах NetWare. Компьютеры Linux могут сообщаться по сети, используя TCP/IP в качестве протокола транспортного уровня, однако они не могут получать доступ к ресурсам файлового сервера Microsoft без клиентской программы прикладного уровня SMB. Протокол PPP (Point-to-Point Protocol) предназначен для установки коммутируемого соединения, он не является протоколом разделения файлов.
10. **в.** В операционной системе OS/2 используется файловая система HPFS (High Performance File System). В системе OS/2 может использоваться также FAT16. В операционную систему Windows NT 3.*x* (но не в более поздние версии Windows) включена поддержка HPFS.

Глава 13

1. **в.** Протоколы разделения файлов называются также протоколами ядра, потому что разделение ресурсов — основа компьютерных сетей. Компьютеры объединяют в сети именно для разделения ресурсов. Сетевой/транспортный протокол — это набор (стек) протоколов, используемый в локальных и глобальных сетях. Канальный протокол используется для установки соединения между компьютерами. Этот термин часто обозначает протоколы удаленного доступа глобальных сетей, такие, как PPP (Point-to-Point Protocol) и SLIP (Serial Line Interface Protocol). Уровень 2 — это канальный уровень модели OSI, на уровне 2 работают канальные протоколы.
2. **б.** Как и TCP/IP (но не NetBEUI), протокол IPX/SPX является маршрутизируемым. Чаще всего он используется в сетях NetWare, однако его можно использовать и в сетях Microsoft. Иногда его применяют во внутренних сетях для повышения безопасности. Версия NetWare 5.*x* — первая сетевая операционная система семейства NetWare, работающая на чистом IP, протокол IPX/SPX для нее не нужен. Однако протокол IPX/SPX все еще поддерживается, его использование оказывается необходимым, если в сети работают серверы старых версий NetWare, с которыми должны сообщаться компьютеры NetWare 5.*x*. Протокол IPX/SPX конфигурируется быстрее и легче, чем TCP/IP, однако его быстродействие ниже и его труднее устанавливать, чем NetBEUI.
3. **а, г.** Разработанные компанией Microsoft спецификации NDIS (Network Driver Interface Specification) и ODI (Open Driver Interface) позволяют связывать несколько протоколов с одним адаптером или один протокол с несколькими адаптерами. Winsock — это интерфейс программирования приложений, а TDI (Transport Driver Interface) — промежуточный уровень в сетевой модели Windows NT.
4. **б.** Для разделения файлов в сетях Microsoft используется протокол SMB (Server Message Block). Клиентские и серверные программы SMB есть и в других сетевых операционных системах, с их помощью обеспечивается доступ к компьютерам Microsoft. Протокол NCP (NetWare Core Protocol) используется в сетях Novell. Система NFS (Network File System) используется для разделения файлов компьютерами UNIX. Протокол DLC (Data Link Control) используется для коммуникации с подключенными к сети лазерными принтерами и с мэйнфреймами IBM.
5. **б, г.** Служба GSNW включена в состав Windows NT Server и Windows 2000 Server. Она устанавливается на сервере Windows для предоставления клиентам Microsoft доступа к ресурсам сервера NetWare посредством шлюза. При этом дополнительное программное обеспечение на клиентском компьютере не требуется, однако сервер NetWare должен быть сконфигурирован с группой NTGATEWAY и пользовательской учетной записью этой группы, которая будет использоваться всеми клиентами шлюза. На серверах NetWare программа GSNW не устанавливается.
6. **б.** Программа Samba позволяет клиентам SMB (например, компьютерам Windows) получать доступ к файлам серверов UNIX. В состав Samba входит клиентская программа SMB, позволяющая компьютерам UNIX получать доступ к разделяемым ресурсам SMB. Система CDFS (Compact Disk File System) используется для организации данных на компакт-дисках. Термин Client Services

for UNIX ошибочен, он ничего не обозначает. Набор протоколов SNA (Systems Network Architecture) разработан компанией IBM для коммуникации несовместимых архитектур, например персональных компьютеров с мэйнфреймами.

7. **в.** Шлюз — это пакет программ, который связывает две сети различных типов с отличающимися протоколами. Шлюз преобразует данные из формата одного протокола в другой, что позволяет компьютерам двух сетей сообщаться друг с другом. Мосты используются для сегментации сетей в целях уменьшения их загрузки. Программное обеспечение сервера, т.е. сетевая операционная система, выполняется на сервере, она выполняет регистрацию и аутентификацию пользователей и предоставляет средства централизованного администрирования и хранения файлов. Программное обеспечение маршрутизатора передает пакеты из одной сети (подсети) в другую, На уровне оборудования для этого используется или выделенное устройство (маршрутизатор), или компьютер, имеющий интерфейсы с обеими сетями и работающий как маршрутизатор.
8. **г.** Программное обеспечение редиректора перехватывает запросы к ресурсам и перенаправляет их в сеть, а не на локальную магистраль компьютеров. Термин "платформа" означает архитектуру оборудования (например, платформа Macintosh, мэйнфреймов IBM или персональных компьютеров). Клиент — это программа, получающая доступ к ресурсам сервера. Директор — это просто директор, например магазина; к этому вопросу он отношения не имеет.
9. **а, в.** Файловая система CIFS, основанная на протоколе разделения файлов SMB, обеспечивает разрешение имен, разделение файлов и принтеров, аутентификацию и авторизацию пользователей и просмотр сети. Система CIFS не предоставляет средства коммутируемого доступа или безопасности на уровне файлов.
10. **а.** Демон SMB, называемый SMBd, — один из двух главных компонентов SAMBA. Он обеспечивает аутентификацию и авторизацию пользователей и разделение файлов и принтеров. Второй важный компонент — демон NMBd — обеспечивает просмотр сети и разрешение имен. Термина MBXd не существует. SMBFS (SMB File System) позволяет компьютерам Linux отображать разделяемые ресурсы SMB на сетевой каталог. Система SMBFS поставляется вместе с SAMBA, однако в ее состав не входит.

Глава 14

1. **в.** Ключ — это число или код, используемые для проверки целостности соединения. Пароль, представляющий собой последовательность цифровых, буквенных и других символов, используется для проверки того, действительно ли данный пользователь является владельцем учетной записи, ассоциированной с этим паролем. Криптография — это наука о шифровании. Аутентификация означает процесс проверки идентичности (в данном случае аутентичности) пользователя.
2. **б.** Методом грубой силы взломщик просто перебирает различные варианты пароля, пока не натолкнется на сработавший. Пароли можно вводить вручную, однако чаще всего варианты перебираются автоматически с помощью специальной программы или сценария. Дешифрование — это преобразование зашифрованного сообщения к исходному виду. Троянским конем (или агентом) называют программу, которая тайно устанавливается под видом полезной и

после установки выполняет задание злоумышленника. Атомная атака — это другое название атаки DoS.

3. **г.** Методом наводнения ping (или затопления ICMP) в систему передается огромное количество пакетов ICMP (Internet Control Message Protocol) для нарушения ее нормальной работы. Когда сообщения ICMP передаются по широковещательным адресам, для того чтобы нарушить работу всего сегмента сети, то это называется Smurf-атакой. Атаки SYN используют процесс установки соединения в протоколе TCP для переполнения очереди сервера, в результате чего он не может обрабатывать полезные запросы. Червь — это самовоспроизводимый зловредный код. Метод Ping of Death передает многочисленные пакеты ICMP, чтобы добиться превышения ограничения на длину передаваемого сообщения MTU (Maximum Transmission Unit).

4. **а, б.** Распространенными внутренними угрозами безопасности являются как промышленный шпионаж (продажа служащими компании сетевых данных конкурентам с целью материального вознаграждения), так и случайные нарушения, вызванные некомпетентностью или небрежностью пользователей. Подмена IP-адресов выполняется чаще всего извне сети, когда кто-либо из Internet эмулирует внутренние IP-адреса для получения доступа к ресурсам сети. Применение прокси-серверов повышает безопасность сети.

5. **б.** Чем длиннее пароль, тем труднее его взломать, поэтому хорошая стратегия безопасности должна предусматривать требование к длине паролей. Пароли, которые легко запоминаются пользователем, легко угадываются злоумышленником. Угадывание пароля затрудняется включением в него цифр и букв с разными комбинациями верхнего и нижнего регистров, поэтому такой метод составления паролей должен быть одним из требований стратегии безопасности. В среде с высокими требованиями к безопасности необходимо регулярно менять пароли.

6. **в.** В операционной системе Windows 2000 по умолчанию все права доступа к новому разделяемому ресурсу имеет каждый. Поэтому после создания ресурса необходимо изменить права доступа к нему. На серверах NetWare реализовано противоположное правило: по умолчанию права доступа к новому ресурсу не имеет никто. Для ресурса NetWare необходимо явно установить права доступа, иначе обратиться к нему никто не сможет.

7. **а.** Шифрование хорошо защищает данные, хранящиеся на диске, однако при передаче данных по сети рекомендуется применять дополнительные средства защиты, например протокол IPSec. Процедуры шифрования встроены во многие операционные системы, например в Windows 2000. Существуют также программы шифрования независимых компаний.

8. **в.** Протокол ESP (Encapsulating Security Payload) совместно с AH (Authentication Header) используется в IPSec для защиты передаваемых по сети данных. ESP обеспечивает конфиденциальность самих данных, а заголовки AH используются только для аутентификации отправителя. Средства ESP и AH можно использовать совместно или отдельно друг от друга.

9. **г.** В шифрах с секретным ключом (называемых также симметричными шифрами) как для шифрования, так и для дешифрования данных используется один и тот же ключ. В шифрах с открытыми/закрытыми ключами (асимметричных шифрах) используются два ключа: открытый, известный всем и распростра-

няемый свободно, и закрытый, известный только владельцу пары ключей. Иногда такие шифры сокращенно называют шифрами с открытыми ключами.

10. **б.** Алгоритм хэширования — это математическое преобразование, которое невозможно выполнить в обратном порядке. Хэширование сообщения выполняется в передающем и принимающем компьютерах. Если их результаты совпадают, значит, сообщение в процессе передачи не изменилось. Цифровые сертификаты распространяются доверительной третьей стороной для проверки аутентичности обладателя пары ключей. Билет на получение билета предоставляется системой аутентификации Kerberos для проверки на сервере аутентичности пользователя или системы.

Глава 15

1. **в.** С помощью пула модемов к серверу удаленного доступа подключают большое количество отдельных телефонных линий, в результате чего соединение с сервером могут устанавливать многие клиенты одновременно. Многоканальная связь означает группирование пропускных способностей каналов. Протокол BAP (Bandwidth Allocation Protocol) применяется в технологии многоканальной связи для динамического управления использованием пропускных способностей каналов. Устройства CSU/DSU (Channel Service Unit/Data Service Unit) используются с T-линиями.
2. **б.** Наиболее распространенной формой удаленного доступа является коммутируемое аналоговое соединение, в котором используются модем и обычная телефонная линия. Для установки удаленного доступа к сети используются также коммутируемые цифровые, выделенные цифровые и беспроводные соединения, однако они более дорогие, их оборудование трудно конфигурировать и поддерживать.
3. **а, г.** Для установки соединения посредством телефонной сети используются протоколы SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Протоколы сетевого/транспортного уровня IPX/SPX и NetBEUI используются для коммуникации удаленных серверов и клиентов после того, как соединение глобальной сети установлено.
4. **б.** Процедуры протокола PAP (Password Authentication Protocol) передают по сети незашифрованный пароль в обычном тексте, следовательно, это наименее безопасный из перечисленных методов. В протоколах CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol) и SPAP (Shiva PAP) для защиты пароля при передаче его по сети используется шифрование.
5. **в.** Многоканальный PPP объединяет пропускные способности двух B-каналов Basic Rate ISDN по 64 Кбит/с каждый, образуя таким образом соединение с пропускной способностью 128 Кбит/с. Удаленный сервер, с которым устанавливается соединение, должен быть сконфигурирован на поддержку многоканального соединения. Протокол BAP (Bandwidth Allocation Protocol) используется для динамического выделения пропускной способности многоканального соединения. Протокол PPTP (Point-to-Point Tunneling Protocol) используется для создания в Internet туннеля виртуальной частной сети. Широковещание означает передачу одного и того же сообщения одновременно всем компьютерам группы.

6. **а.** Процесс уменьшения частоты передаваемых модемом импульсов до тех пор, пока не будет установлена надежная связь, называется обратной настройкой. Такое название обусловлено тем, что сначала устанавливается максимальная частота, при которой связь невозможна, затем частота возвращается к своему оптимальному значению. Группирование на уровне оборудования — это метод объединения пропускных способностей каналов. Термин "ремодуляция" ничего не означает. Обратный вызов используется для обеспечения безопасности удаленного доступа.

7. **б.** Микросхема UART (Universal Asynchronous Receiver/Transmitter) управляет COM-портом и определяет максимальную скорость передачи. Порт USB (Universal Serial Bus) предоставляет некоторые дополнительные возможности и обеспечивает более высокую скорость обмена, чем стандартные последовательный и параллельный порты. UNC (Universal Naming Convention) определяет синтаксис задания пути к сетевому ресурсу. Протокол транспортного уровня UDP (User Datagram Protocol) работает в режиме без установки соединения.

8. **в.** Внутренние модемы дешевле, чем внешние. Внешние модемы легче устанавливать, потому что для этого не нужно открывать корпус компьютера или конфигурировать перемычки. Еще одно преимущество внешних модемов — сигнальные индикаторы, указывающие на состояние модема.

9. **в, г.** Шумы в телефонной линии не позволяют модему установить максимальную скорость, на которую он способен. Еще одной причиной низкой скорости передачи может быть несовместимость с модемом на другом конце, например если на этом конце установлен старый модем на 56 Кбит/с, поддерживающий технологию 56Kflex или X2, а на сервере удаленного доступа используется другой модем. Если имя пользователя или пароль введены неправильно, то соединение вообще не будет установлено. Входящий звонок по линии, для которой на телефонной станции установлена служба ожидания звонка, может повлечь отключение модема, однако ожидание само по себе не уменьшает скорость соединения.

10. **б.** Стандартный промышленный протокол RADIUS (Remote Authentication Dial-In User Service) обеспечивает централизованную аутентификацию и управление учетными записями. Коммутируемый сервер конфигурируется как клиент RADIUS, аутентификация выполняется сервером RADIUS. Метод NAT (Network Address Translation) предназначен для совместного использования подключения к Internet всеми компьютерами локальной сети путем отображения частных внутренних адресов на один внешний публичный адрес. RAID (Redundant Array of Independent Disks) предназначен для повышения отказоустойчивости и производительности дисков. Протокол RARP (Reverse Address Resolution Protocol) используется для определения IP-адреса компьютера на основе его физического MAC-адреса.

Глава 16

1. **б.** Процесс размещения заголовка одного протокола внутри заголовка другого протокола называется инкапсуляцией. Инкапсуляция выполняется при создании туннеля. Шифрование — это преобразование данных к такому виду, в котором ими не сможет воспользоваться постороннее лицо. Аутентификация — это процесс определения пользователя или компьютера. Авторизация означает

определение прав пользователя, т.е. можно ли ему предоставить доступ к данному сетевому ресурсу.

2. **а.** Туннель представляет собой логическое соединение "точка–точка", в котором поддерживается аутентификация и шифрование данных при их передаче с одного конца на другой. Протокол — это набор правил, которых придерживаются сообщающиеся друг с другом компьютеры. Шлюз — это маршрутизатор, установленный между двумя сетями (подсетями) и направляющий пакеты в другую сеть. Некоторые шлюзы, например GateWay Services for NetWare, транслируют протоколы пакетов. Соединение удаленного доступа является логическим соединением "точка–точка", однако в нем не обязательно выполняется аутентификация и шифрование, оно также не обязательно проходит через публичную сеть. Если эти три условия в соединении удаленного доступа выполняются, то оно называется соединением VPN (Virtual Private Network).
3. **б, г.** Протокол PPTP (Point-to-Point Tunneling Protocol) является расширением канального протокола PPP (Point-to-Point Protocol). Поэтому PPTP работает на канальном уровне (уровне 2) модели OSI. В протоколе PPTP для повышения безопасности путем шифрования данных используется не IPSec, а протокол MPPE (Microsoft Point-to-Point Encryption). Протокол IPSec используется совместно с L2TP (Layer 2 Tunneling Protocol).
4. **в.** Протокол IPSec может работать в транспортном режиме, например когда данные шифруются средствами IPSec, а инкапсулируются процедурами протокола L2TP. В режиме туннелирования IPSec выполняет инкапсуляцию самостоятельно. Протоколы туннелирования PPTP и L2F (Layer 2 Forwarding) не работают в обоих режимах. Интерфейс SSH (Secure Shell) используется для создания VPN в среде UNIX.
5. **в, г.** Главным преимуществом VPN является экономия денежных средств путем отказа от услуг междугородной телефонной связи. Применяя VPN, пользователи набирают телефонный номер своего локального провайдера, который расположен в этом же городе. Без VPN для установки соединения с удаленным сервером коммутируемого доступа пользователь вынужден платить за междугородный звонок. Расходы компании снижаются также за счет того, что для каждого пользователя не требуется отдельная телефонная линия и модем. Однако из-за необходимости обрабатывать дополнительные служебные сигналы при создании туннеля производительность VPN обычно немного ниже, чем производительность прямого удаленного соединения. Сети VPN, носителем которых является Internet, особенно при использовании коммутируемого соединения, обладают меньшей надежностью, чем прямое коммутируемое соединение.
6. **в.** Экстрасеть — это часть локальной сети компании, доступная для пользователей, не работающих в этой компании. Если доступ предоставляется путем туннелирования по публичной сети, то образуется экстрасеть VPN. Сетью internet (со строчной "i") называется любая сеть, состоящая из других сетей Сеть intranet во всем аналогична экстрасети, за исключением того, что доступ к ней предоставляется изнутри корпоративной сети. Она создается для служащих компании, а не для внешних клиентов и заказчиков. Подсеть — это часть сети.
7. **г.** Соединения "маршрутизатор–маршрутизатор" объединяют две отдельные локальные сети. С их помощью пользователи получают доступ к ресурсам на

другой стороне. Остальные три варианта ответа неудовлетворительны, так как пользователи инициируют соединение VPN чаще всего с помощью коммутируемого соединения с Internet, а не через маршрутизатор.

8. **а, в.** Как PPTP (Point-to-Point Tunneling Protocol), так и L2TP (Layer 2 Tunneling Protocol) используются для создания туннелей VPN, оба они работают на канальном уровне (уровень 2) модели OSI. Однако в PPTP используется протокол IP, поэтому PPTP не может использовать виртуальные каналы ATM и Frame Relay для туннелирования по сети, основанной на протоколе, отличном от IP. Множественное туннелирование между двумя точками поддерживает только L2TP.
9. **б.** Протокол CIPE (CryptoIP Encapsulation) реализован как драйвер ядра Linux. Его можно использовать для создания безопасного туннеля между двумя подсетями IP. Программа TunnelBuilder является программным продуктом независимой компании, предназначенным для создания VPN. Показатель производительности сети CIR (Committed Information Rate) не имеет непосредственного отношения к VPN. Демон VPNd — это программа туннелирования, в которой используется алгоритм шифрования Blowfish.
10. **а, б, г.** Аппаратные реализации сетей VPN поставляются в двух вариантах: на основе маршрутизаторов и на основе брандмауэров. Сети на основе маршрутизаторов легко устанавливать и эксплуатировать, в них поддерживается технология Plug and Play. В сетях VPN на основе брандмауэров может выполняться трансляция адресов. Средства многих программных VPN распространяются бесплатно или входят в операционные системы. Сети VPN на основе оборудования чаще всего дороже программных.

Глава 17

1. **а, в.** Даже самый высокопроизводительный сервер на основе персонального компьютера, используемый как сервер приложений, стоит на несколько тысяч долларов дешевле, чем мэйнфрейм. Использование персональных компьютеров в качестве клиентских позволяет выполнять некоторые пользовательские приложения локально, а некоторые — на сервере. Персональные компьютеры дороже, чем терминалы мэйнфрейма, однако они предоставляют больше возможностей.
2. **в.** В большинстве программных реализаций тонких клиентов, например в Microsoft Terminal Services, предусмотрено управление сеансами пользователей. С их помощью администратор может управлять вводом с клавиатуры или мышью пользователя, завершать сеанс и т.д. Пользователи не обязательно должны иметь одинаковые установки безопасности и права доступа, эти конфигурационные параметры устанавливаются отдельно для каждой учетной записи или группы. Использование терминалов облегчает резервное копирование данных, потому что они хранятся в одном месте — на сервере. Приложения модернизируются не на отдельных клиентских компьютерах, а только на сервере.
3. **б.** Протокол ICA (Independent Computing Architecture), используемый в программе MetaFrame компании Citrix, позволяет клиентам, отличным от Windows, устанавливать соединение с терминальным сервером Windows. Протокол RDP (Remote Desktop Protocol), используемый в системах Windows и включенный в состав Windows NT и Windows 2000 Terminal Services, предостав-

ляет доступ к терминальному серверу только клиентам Windows. Протокол X обычно используется клиентами UNIX для получения доступа к серверу X системы UNIX. Протокол DHCP (Dynamic Host Configuration Protocol) используется для присвоения IP-адресов компьютерам (включая тонких клиентов) при их подключении к сети TCP/IP.

4. **а, г.** Протокол RDP (Remote Desktop Protocol), используемый в Microsoft Terminal Services, поддерживает передачу клиентских документов на локальный параллельный порт LTP для печати и позволяет перенаправлять буфер обмена, т.е. передавать данные буфера между терминальным окном и локальным рабочим столом. Перенаправление порта COM и протоколы IPX/SPX и NetBEUI поддерживает только протокол ICA (Independent Computing Architecture).
5. **в.** Для присвоения ресурсов сервера X клиентским терминалам X используется XDMCP (X Display Manager Communication Protocol). Протокол X используется для коммуникации между клиентом и сервером. Его вариант LBX (Low Bandwidth X) разработан для медленных каналов глобальных сетей. Протокол RFB (Remote Frame Buffer) используется для предоставления удаленного доступа к графическому интерфейсу, выполняющемуся на другой платформе.
6. **б.** Стандарт PXE (Preboot Execution Environment), реализованный компанией Intel и другими производителями, обусловливает средства предоставления кода начальной загрузки бездисковой рабочей станции или другому компьютеру, загружающему свою операционную систему из сети. Остальные три определения PXE неправильные.
7. **б, в, г.** В технологии NC (Network Computer), разработанной компанией Sun Microsystems совместно с Oracle и IBM, поддерживается стек протоколов TCP/IP и выполнение аплетов Java. С NC поставляется Web-броузер. Эта система может работать на любой платформе и в любой операционной системе.
8. **а, б.** Операционная система Windows 2000 Terminal Services может работать как в режиме удаленного администрирования, в котором можно управлять сервером с удаленной рабочей станции, так и в режиме сервера приложений, в котором многие пользователи могут подключаться к терминальному серверу и выполнять приложения на рабочем столе Windows 2000.
9. **б, в.** В программе MetaFrame компании Citrix реализованы некоторые возможности технологии портала приложений Nfuse, что позволяет встраивать приложения в стандартный интерфейс Web-броузера. Кроме того, MetaFrame позволяет группировать серверы в ферму серверов для выравнивания загрузки и управления процессами лицензирования. Программа MetaFrame работает под управлением Windows NT 4.0 и Windows 2000. Аналогичная программа компании Ctirix для NT 3.51 называется Winframe. Для управления приложениями и создания новых соединений ICA (Independent Computing Architecture) в программе MetaFrame используется окно Program Neighborhood (Программное окружение).
10. **г.** Высокая производительность Java частично основана на поддержке многозадачности и компиляции по требованию. Аплеты Java должны выгружаться на клиентский компьютер, хотя некоторые вычисления могут выполняться и на сервере. Стандарты Java не универсальны, реализации разных поставщиков могут существенно отличаться. Виртуальная машина Java доступна почти на любой платформе, включая Windows и Macintosh, она не ограничена компьютерами UNIX.

Глава 18

1. **б.** Количество данных, которые можно фактически передать по сети от передающего компьютера к принимающему в единицу времени, называется пропускной способностью. Полоса пропускания — это теоретическая величина, характеризующая пропускную способность аналоговой линии. Показатель CIR (Committed Information Rate — согласованная скорость передачи) — это минимальная гарантируемая провайдером услуг пропускная способность соединения. Базовый уровень какого-либо показателя производительности используется для сравнения его значений в разных ситуациях.
2. **а.** Анализатор протоколов (иногда его называют сетевым монитором) — это инструмент (обычно программный), перехватывающий отдельные кадры или пакеты сообщения для их анализа. Монитор производительности представляет собой программный инструмент, который измеряет определенные показатели производительности, такие, как количество переданных байт в секунду. Рефлектометром временных интервалов называется устройство, предназначенное для обнаружения разрывов и коротких замыканий кабеля. Фильтры пакетов используются в анализаторе протоколов для просмотра пакетов заданного протокола либо пакетов с определенным входным или выходным адресом.
3. **а, в.** Программными анализаторами протоколов являются Network Monitor компании Microsoft, LANalyzer компании Novell и Sniffer Pro компании Network Associates. SNMP (Simple Network Management Protocol) — это утилита TCP/IP, используемая в задачах управления сетью, но с ее помощью нельзя перехватывать и анализировать пакеты. Программа TCPCON компании Novell является модулем NLM (NetWare Loadable Module), она используется для просмотра конфигурации и статистики TCP/IP.
4. **г.** Программа SMS (System Management Server) компании Microsoft содержит более полную версию программы Network Monitor, чем включенная в операционные системы Windows NT и Windows 2000. Программа OpenView компании Hewlett Packard предназначена для управления сетью. Tivoli — это аналогичная программа компании IBM. Протокол SMTP (Simple Mail Transfer Protocol) используется для обработки сообщений электронной почты.
5. **б, в.** Интерфейс в виде приборной панели используется в программах LANalyzer компании Novell и Sniffer Pro компании Network Associates. Программа Network Monitor выводит информацию в текстовом формате, а в Performance Monitor показатели производительности выводятся в виде диаграмм.
6. **а, г.** Программа SMS (System Management Server) используется для сбора информации об оборудовании и программном обеспечении, документирования устройств сети, управления лицензионными процессами, удаленного контроля рабочих столов пользователей, извещения администраторов о событиях в системе и развертывания в сети программного обеспечения. В состав SMS входит более полная версия программы Network Monitor, чем поставляемая с Windows NT и Windows 2000. SMS не поставляется ни с какой версией операционной системы Windows. SMS не обеспечивает коммуникацию сетей Windows с сетями мэйнфреймов IBM, это делает сервер SNA (Systems Network Architecture).

7. **б.** В протоколе SNMP (Simple Network Management Protocol) для сбора информации о сети используются три компонента: программа диспетчера, программа агента и база данных MIB (Management Information Base). Программа Network Monitor и другие анализаторы протоколов используются для перехвата пакетов и сохранения передаваемых в пакетах данных, однако SNMP в них не используется. Провайдер ASP (Application Service Provider) предоставляет клиентам в аренду программные приложения по сети.

8. **в.** Специалисты по электронике называют "лисой и собакой" тональный генератор и локатор. Такое название обусловлено тем, что "собака" (локатор) охотится за "лисой" (тональный генератор). Рефлектометр временных интервалов, осциллограф и цифровой вольтметр/омметр тоже являются устройствами, однако им не присвоены названия животных.

9. **г.** При возникновении неполадки необходимо в первую очередь проверить, правильно ли сетевой адаптер подключен к концентратору и нет ли видимых повреждений кабеля. Конфигурацию протоколов, целостность файлов и учетные записи пользователей следует проверять, только убедившись, что нет какой-либо физической неполадки.

10. **г.** Команда определения маршрута пакета в компьютерах Linux или UNIX правильно записывается как `traceroute`. Команды Linux/UNIX чувствительны к регистру, поэтому их нужно вводить в нижнем регистре, иначе они не будут распознаны и выполнены. Команда `TRACERT` является правильной в операционных системах Windows 9.*x*, Windows NT и Windows 2000. Команды Windows нечувствительны к регистру, поэтому можно ввести также `tracert`.

Словарь терминов

В словаре определяются используемые в книге наиболее распространенные термины и сокращения, применяемые в сфере коммуникационных технологий.

Цифры

3DES (triple DES). Тройной DES. Усиленный вариант алгоритма DES (Data Encryption Standard), используемый для шифрования наиболее ответственных данных. В тройном DES используются три отдельных ключа, а в DES — только один.

10Base2. Архитектура Ethernet на основе 50-омного тонкого коаксиального кабеля. Используются немодулированные сигналы. Пропускная способность равна 10 Мбит/с. Максимальная длина сегмента — 185 м. Архитектура 10Base2 специфицируется документом IEEE 802.3. *См.* Ethernet и IEEE 802.3.

10Base5. Архитектура Ethernet на основе стандартного (толстого) 50-омного коаксиального кабеля. Специфицируется документом IEEE 802.3. Используются немодулированные сигналы. Пропускная способность — 10 Мбит/с. Максимальная длина сегмента — 500 м. *См.* Ethernet и IEEE 802.3.

10BaseF. Архитектура Ethernet на основе волоконно-оптического кабеля. Пропускная способность — 10 Мбит/с. Используются немодулированные сигналы. Специфицируется стандартами Ethernet для 10BaseFB, 10BaseFL и 10BaseFP. *См.* 10BaseFB, 10BaseFL и Ethernet.

10BaseFB. Архитектура Ethernet на основе волоконно-оптического кабеля. Пропускная способность — 10 Мбит/с. Используются немодулированные сигналы. Максимальная длина сегмента — 2 000 м. Максимальное количество станций на сегмент — 1 024. Обычно используется дуплексный 62.5/125-микронный совместимый с FDDI кабель и разъемы ST или SMA.

10BaseFL. Архитектура Ethernet на основе волоконно-оптического кабеля. Пропускная способность — 10 Мбит/с. Используются немодулированные сигналы. Техническое исполнение обусловлено спецификациями IEEE 10BaseF, разработанными для замены FOIRL (Fiber Optic InterRepeater Link), хотя и предусмотрено взаимодействие с FOIRL. Максимальная длина сегмента 10BaseFL при использовании FOIRL составляет 1 000 м, а "чистого" 10BaseFL — 2 000 метров. *См.* 10BaseF и Ethernet.

10BaseT. Архитектура Ethernet на основе немодулированных сигналов и двух витых пар категории 3, 4 или 5. Одна пара предназначена для передачи, другая — для приема данных. Архитектура 10BaseT специфицируется документом IEEE 802.3. Пропуск-

ная способность составляет 10 Мбит/с. Максимальная длина сегмента приблизительно равна 100 м. *См.* Ethernet и IEEE 802.3.

100BaseFX. Архитектура Fast Ethernet. Пропускная способность составляет 100 Мбит/с. По кабелю передаются немодулированные сигналы. Используются два волокна оптического кабеля на сегмент. Чтобы не нарушилась синхронизация сигналов, длина сегмента 100BaseFX не должна превышать 400 м. Специфицируется стандартом IEEE 802.3. *См.* 100BaseX, Ethernet и IEEE 802.3.

100BaseT. Архитектура Fast Ethernet на основе неэкранированных витых пар. Пропускная способность составляет 100 Мбит/с. Используются немодулированные сигналы. Как и в 10BaseT, на которой она основана, в 100BaseT при отсутствии сигналов в кабеле, на него подаются служебные сигналы. Однако в 100BaseT эти служебные сигналы содержат больше информации, чем в 10BaseT. Архитектура 100BaseT специфицируется документом IEEE 802.3. *См.* Fast Ethernet и IEEE 802.3.

100BaseT4. Архитектура Fast Ethernet на основе четырех неэкранированных витых пар категории 3, 4 или 5. Пропускная способность составляет 100 Мбит/с. Используются немодулированные сигналы. Чтобы не нарушилась синхронизация сигналов, длина сегмента 100BaseT4 не должна превышать 100 м. Специфицируется стандартом IEEE 802.3. *См.* Fast Ethernet и IEEE 802.3.

100BaseTX. Архитектура Fast Ethernet на основе двух экранированных или неэкранированных витых пар. Первая пара используется для приема, вторая — для передачи данных. Пропускная способность равна 100 Мбит/с. Используются немодулированные сигналы. Чтобы не нарушилась синхронизация сигналов, длина сегмента 100BaseTX не должна превышать 100 м. Специфицируется стандартами IEEE 802.3. *См.* 100BaseX, Fast Ethernet и IEEE 802.3.

100BaseX. Спецификация Fast Ethernet архитектуры на основе волоконно-оптических кабелей, базирующейся на стандартах 100BaseFX и 100BaseTX. Определяется документом IEEE 802.3. Пропускная способность равна 100 Мбит/с. Используются немодулированные сигналы. *См.* 100BaseFX, 100BaseTX, Fast Ethernet и IEEE 802.3.

100VG-AnyLAN. Технология Fast Ethernet и Token Ring на основе четырех неэкранированных витых пар категории 3, 4 или 5. Пропускная способность равна 100 Мбит/с. Эта высокоскоростная технология, разработанная компанией Hewlett Packard, может работать на основе существующих сетей 10BaseT Ethernet. Специфицируется стандартами IEEE 802.3. *См.* IEEE 802.3.

A

Access layer. Уровень доступа. Уровень, на котором локальная сеть или группа локальных сетей (обычно Ethernet или Token Ring) предоставляет пользователям доступ к службам сети.

Access method. Метод доступа. 1. Метод доступа сетевого устройства к сетевому носителю. 2. Программное обеспечение SNA (System Network Architecture), управляющее потоками информации по сети.

Acknowledgment. Подтверждение. Сообщение, передаваемое одним сетевым устройством другому для подтверждения некоторого события (например, получения сообщения). Сокращенное обозначение — ACK.

ACL (access control list). Список контроля доступа. Список, используемый маршрутизатором Cisco для управления пропусканием пакетов через маршрутизатор (например, для предотвращения передачи пакетов с заданным IP-адресом на определенный интерфейс маршрутизатора).

Active Directory. Служба каталогов, используемая в сетях Windows 2000. Информация в ней хранится в иерархической базе данных.

Adapter. *См.* NIC.

Address resolution. Разрешение адресов. Метод согласования различных схем компьютерных адресов. Обычно этот термин означает метод отображения адресов сетевого уровня (уровня 3) на адреса канального уровня (уровня 2).

Address. Адрес. Структура данных или логическое соглашение, используемое для идентификации некоторой уникальной сущности, такой, как сетевое устройство.

ADSL (Asymmetric Digital Subscriber Line). Асимметричная абонентская цифровая линия. Услуга высокоскоростной связи, предоставляемая телефонными станциями в некоторых регионах. В качестве линий ADSL используются традиционные медные провода. Могут передаваться как данные, так и голос.

AI (Artificial Intelligence). Искусственный интеллект. Моделирование человеческого интеллекта, выполняемое машиной, особенно компьютерной системой. Моделируемые процессы включают обучение, логическое мышление и коррекцию ошибок.

Analog. Аналоговый сигнал. Сигнал, представляющий собой непрерывно изменяющуюся физическую величину, например напряжение в кабеле. Аналоговый сигнал в каждый момент времени находится в одном из бесконечного количества допустимых состояний. В традиционных телефонных линиях используются аналоговые сигналы.

ANSI (American National Standards Institute). Национальный институт стандартизации США. Добровольная организация, состоящая из корпоративных, правительственных и других учреждений. Координирует разработку и утверждение стандартов, принимает национальные стандарты США и представляет интересы Соединенных Штатов в международных организациях стандартизации. Организация ANSI содействует развитию международных стандартов и стандартов США, относящихся, в частности, к сетевым и коммуникационным технологиям. ANSI является членом IEC (International Electrotechnical Commission) и IOS (International Organization for Standardization).

API (Application Programming Interface). Интерфейс прикладного программирования. Набор процедур, программ и подпрограмм, с помощью которых программы приложений взаимодействуют с операционными системами и запрашивают различные услуги.

APIPA (Automatic Private IP Addressing). Автоматическая частная IP-адресация. Компонент операционных систем Windows 98 и Windows 2000. С его помощью компьютеры, сконфигурированные как клиенты DHCP (Dynamic Host Configuration Protocol), могут присваивать себе временные IP-адреса в случае недоступности сервера DHCP.

AppleTalk. Сетевая архитектура, используемая компьютерами Apple Macintosh. Программное обеспечение AppleTalk включено в операционные системы Macintosh.

Application layer. Прикладной уровень. Уровень 7 модели OSI. Этот уровень предоставляет сетевые службы пользовательским приложениям. Например, на этом уровне службы передачи файлов обслуживают приложения обработки текстов. *См.* OSI reference model.

Application. Приложение. Программа, непосредственно выполняющая задачу пользователя. Примерами сетевых приложений являются клиент FTP (File Transfer Protocol) и Telnet.

APPN (Advanced Peer-to-Peer Networking). Улучшенный протокол одноранговых сетей. Расширение исходной архитектуры SNA (Systems Network Architecture) компании IBM. В архитектуре APPN выполняется установка сеансов между одноранговыми узлами, явное динамическое вычисление маршрутов и назначение приоритетов потокам информации APPC (Advanced Program-to-Program Communications).

ARCnet Advanced Resource Computer Network. Вычислительная сеть с присоединенными ресурсами. К настоящему времени уже устаревшая архитектура на основе магистрали с передачей маркера, разработанная для небольших локальных сетей.

ARP (Advanced Research Projects Agency Network). Сеть Управления перспективных исследовательских программ США. Глобальная сеть, разработанная и введенная в действие в 1960-х годах Министерством обороны США и основными университетами. Со временем развилась в Internet.

ASCII (American Standard Code for Information Interchange). Американский стандартный код для обмена информацией. Восьмиразрядный код представления символов.

Asymmetric encryption. Асимметричное шифрование. Метод шифрования, в котором используется два ключа. Первый ключ называется открытым, он свободно распространяется и может быть известен всем. Второй ключ называется закрытым, его знает только владелец пары ключей. Первый ключ используется для шифрования данных, а второй — для дешифрования.

Asynchronous communication. Асинхронная коммуникация. Метод передачи данных, в котором сигналы передаются и принимаются через нерегулярные интервалы времени. Для обозначения начала и конца передачи используются стартовый и конечный биты.

ATM (Asynchronous Transfer Mode). Режим асинхронной передачи. Коммуникационная технология на основе коммутации пакетов, в которой для передачи данных с высокой скоростью используются 53-байтовые ячейки фиксированной длины. Для одновременной передачи данных в сеть многими компьютерами используются мультиплексоры.

ATP (AppleTalk Transaction Protocol). Протокол транзакций AppleTalk. Протокол транспортного уровня, предоставляющий услуги транзакций между сокетами без потерь. Это позволяет организовать обмен между двумя клиентами сокетов, в котором один клиент передает другому запросы на выполнение определенных задач, а другой передает отчет о результатах.

Attenuation. Затухание. Ослабление интенсивности сигнала с увеличением расстояния.

Audit. Аудит. Отслеживание и запись в журнал таких действий пользователей, как регистрация, получение доступа к объектам, использование прав доступа и т.д. Выполняется в целях обеспечения безопасности.

Authentication. Аутентификация. Проверка идентичности пользователя. Обычно выполняется на основе предопределенной учетной записи пользователя и ассоциированного с ней пароля. В усовершенствованных методах аутентификации используется сравнение отпечатков пальцев, анализ отпечатков голоса или сканирование сетчатки глаза.

Authorization. Авторизация. Проверка наличия у пользователя права доступа к данному сетевому ресурсу.

B

Back up. Резервное копирование. Создание копий данных и программ, из которых их можно легко восстановить в случае аварии.

Backbone. Магистраль. Кабель, к которому подключаются концентраторы, коммутаторы, маршрутизаторы и сегменты сети.

Bandwidth. Пропускная способность. Максимальное количество данных, которые можно передать по сети за единицу времени. Измеряется в битах в секунду.

Banyan VINES. *См.* VINES.

BAP (Bandwidth Allocation Protocol). Протокол распределения пропускных способностей. Метод управления использованием многих каналов в технологии многоканальной связи. В этом методе дополнительные линии подключаются, когда поток информации превышает пропускную способность, и отключаются, когда потребность в них отпадает.

Baud. Бод. Единица измерения скорости передачи данных. Равна одному биту в секунду. Названа в честь французского телеграфного инженера Бода (Baudot).

B-channel. B-канал. Один из каналов линии ISDN (Integrated Services Digital Network). По B-каналу передаются данные. Работает совместно с D-каналом, по которому передаются служебные сигналы. Типичная линия BRI (Basic Rate ISDN) состоит из одного D-канала на 16 Кбит/с и двух B-каналов по 64 Кбит/с каждый.

BDC (Backup Domain Controller). Резервный контроллер домена. Сервер в сети Windows NT, содержащий копию базы данных учетных записей SAM (Security Accounts Database) домена, которая используется для аутентификации регистрационной информации пользователей. Контроллер BDC может только читать данные SAM. Информация базы данных SAM реплицируется на многие контроллеры BDC контроллером PDC (Primary Domain Controller). Контроллер PDC выполняет также обновления базы данных SAM.

Binary. Двоичный. В двоичной системе счисления используются только две цифры: 0 и 1. С их помощью представляется любое двоичное число.

BIND (Berkeley Internet Name Domain). Служба имен доменов в Internet. Версия службы DNS (Domain Name System), выполняющаяся на компьютерах UNIX и предназначенная для отображения (разрешения) имен хостов на IP-адреса.

Bind. Связывать. Устанавливать связь между протоколом и сетевым адаптером.

Bindery. Однородная база данных на серверах NetWare 3.*x*, содержащая регистрационную информацию об учетных записях.

Bit. Бит. Единица измерения количества информации. Наименьшее количество данных, которые может обрабатывать компьютер. Бит данных содержит 0 или 1.

BOOTP (Boot Protocol). Протокол загрузки. Протокол, разработанный для предоставления бездисковым рабочим станциям IP-адресов и выгрузки операционной системы из сети TCP/IP. Предшественник протокола DHCP (Dynamic Host Configuration Protocol).

Bootstrap. Начальная загрузка. Простая предопределенная операция загрузки инструкций, автоматически загружающих в память другие инструкции или переводящих систему в режим конфигурирования.

BRI (Basic Rate ISDN). ISDN базового уровня. Линия ISDN (Integrated Services Digital Network), состоящая из двух B-каналов и одного D-канала. Предназначена для передачи голоса, видео и данных на основе технологии коммутируемых каналов.

Bridge. Мост. Устройство, соединяющее две сети (или два сегмента сети) с одинаковыми протоколами и передающее пакеты из одной сети в другую. Мосты работают на канальном уровне (уровень 2) модели OSI. В общем случае мост фильтрует, передает или возвращает поступивший пакет на основе его MAC-адреса.

Bridging. Создание моста. Установка и конфигурирование моста между двумя сегментами локальной сети.

Broadcast. Широковещательное сообщение. Сообщение, передаваемое всем компьютерам сегмента или подсети, а не одному принимающему компьютеру.

Broadcast Address. Широковещательный адрес. Специальный адрес, зарезервированный для передачи сообщения всем станциям. *См.* Broadcast.

Broadcast Domain. Широковещательный домен. Набор устройств, получающих широковещательные пакеты, переданные одним из устройств этого набора. Обычно широковещательный домен ограничен маршрутизаторами, потому что маршрутизаторы не передают широковещательных пакетов. *См.* Broadcast.

Broadcast Storm. Широковещательный шторм. Нежелательное сетевое событие, состоящее в том, что много широковещательных сообщений передаются одновременно по всем сегментам сети. Широковещательный шторм снижает пропускную способность сети и может стать причиной ее отключения. *См.* Broadcast.

Bus Topology. Шинная топология. Топология локальной сети, в которой все компьютеры соединены вдоль одной линии.

Byte. Байт. Восемь бит.

C

Cache. Кэш. Место временного хранения данных в целях повышения скорости вычислений. Например, на Web-броузерах в файлах кэша хранятся часто вызываемые Web-страницы, в результате чего при повторном обращении их можно быстро извлечь с локального диска, не пользуясь Internet.

Caching. Кэширование. Форма репликации, позволяющая использовать информацию, полученную в предыдущей транзакции, для обработки следующей транзакции.

Callback. Обратный вызов. Метод проверки сервером аутентичности удаленного пользователя. После ввода имени пользователя и пароля сервер разрывает соединение и тут же набирает известный телефонный номер данного пользователя.

Carrier. Несущая. Электромагнитная волна или переменное напряжение определенной частоты, модулированное сигналами данных.

Category 1 Cabling. Кабель категории 1. Одна из пяти марок неэкранированной витой пары, специфицированных стандартом EIA/TIA 568B. Используется для телефонных линий, для передачи данных непригоден. *См.* UTP.

Category 2 Cabling. Кабель категории 2. Одна из пяти марок неэкранированной витой пары, специфицированных стандартом EIA/TIA 568B. Может обеспечить пропускную способность до 4 Мбит/с. *См.* UTP.

Category 3 Cabling. Кабель категории 3. Одна из пяти марок неэкранированной витой пары, специфицированных стандартом EIA/TIA 568B. Используется в сетях 10BaseT. Пропускная способность кабеля — до 10 Мбит/с. *См.* UTP.

Category 4 Cabling. Кабель категории 4. Одна из пяти марок неэкранированной витой пары, специфицированных стандартом EIA/TIA 568B. Используется в сетях Token Ring. Пропускная способность кабеля — до 16 Мбит/с. *См.* UTP.

Category 5 Cabling. Кабель категории 5. Одна из пяти марок неэкранированной витой пары, специфицированных стандартом EIA/TIA 568B. Пропускная способность — до 100 Мбит/с. *См.* UTP.

Category 5e Cabling. Кабель категории 5e. Усовершенствованная марка неэкранированной витой пары категории 5. Пропускная способность — до 1,55 Гбит/с. *См.* UTP.

CCIE (Cisco Certified Internet Expert). Сертифицированный специалист по межсетевому обмену Cisco.

CCITT (Committee for International Telegraph and Telephone). Международный консультативный комитет по телеграфии и телефонии. Международная организация, расположенная в Женеве (Швейцария) и занятая разработкой стандартов телекоммуникации.

CCNA (Cisco Certified Network Associate). Сертифицированный специалист по сетям Cisco.

CCNP (Cisco Certified Network Professional). Сертифицированный профессионал по сетям Cisco.

Certificate. Сертификат. Информация, используемая для аутентификации и безопасного обмена данными в небезопасной сети с помощью шифра с открытыми/закрытыми ключами.

CHAP (Challenge Handshake Authentication Protocol). Протокол аутентификации с предварительным согласованием вызова. Средство обеспечения безопасности, поддерживаемое в линиях, в которых для предотвращения несанкционированного доступа используется инкапсуляция PPP (Point-to-Point Protocol). PPP не предотвращает несанкционированный доступ, но идентифицирует удаленного пользователя, после чего маршрутизатор или сервер доступа определяет, предоставить ли пользователю доступ.

CIDR (Classless Interdomain Routing). Бесклассовая междоменная маршрутизация. Метод определения частей IP-адреса, относящихся к сети и к хосту. Более эффективен и гибок, чем старый метод классовой адресации. В методе CIDR используется суффикс, определяющий длину адреса сети. Биты, не вошедшие в адрес сети, рассматриваются как адрес хоста.

CIFS (Common Internet File System). Общая файловая система Internet. Файловая система, основанная на протоколе разделения файлов SMB (Server Message Block). Используется в Samba для обеспечения коммуникации компьютеров Microsoft и UINX. В системе CIFS выполняются аутентификация, авторизация, разрешение имен, разделение файлов и принтеров и просмотр сетей.

Cipher. Шифр. Метод преобразования данных к виду, в котором ими не сможет воспользоваться постороннее лицо.

CIR (Committed Information Rate). Согласованная скорость передачи. Усредненная по минимальному приращению времени скорость передачи данных (в битах в секунду) по сети Frame Relay.

Circuit Switching. Коммутация каналов. Система коммутации, в которой между двумя абонентами на весь период сеанса связи должна существовать выделенная физическая цепь. Используется главным образом в традиционных телефонных сетях. Как метод доступа к каналу коммутация каналов противоположна методам конкуренции и передачи маркера, а как технология коммутации — методам коммутации сообщений и пакетов.

Circuit. Канал. Путь (маршрут) коммуникации между двумя точками.

Circuit-Switched Network. Сеть с коммутацией каналов. Сетевая технология, в которой соединение устанавливается путем замыкания электрической цепи (например, в традиционной телефонной сети). Электрическая цепь предоставляется абонентам на все время сеанса связи. В следующем сеансе этим же абонентам может быть предоставлена другая цепь.

Cisco IOS (Internetwork Operating System). Операционная система Cisco. Программная платформа, выполняющаяся на большинстве маршрутизаторов и коммутаторов Cisco. Предназначена для обеспечения работы сетевых служб и приложений.

Client/Server Application. Приложение клиент/сервер. Приложение, централизованно хранящееся на сервере и выполняющее задачи клиентов. Клиенты получают к нему доступ посредством сети. Централизованное хранение на сервере облегчает обеспечение безопасности и управление приложениями.

Client/Server Computing. Система клиент/сервер. Распределенная вычислительная сетевая система, в которой операции вычисления разделяются между двумя компонентами: клиентом и сервером. Оба термина (клиент и сервер) могут означать как программу, так и устройство. Другое название системы клиент/сервер — распределенная вычислительная система.

Client/Server. Клиент/сервер. Архитектура отношений между клиентскими и серверными сетевыми компьютерами.

Client. Клиент. Компьютер или программа, запрашивающая доступ к ресурсам или службам другого компьютера (сервера).

Cluster. Кластер. Группа компьютеров, в которой каждый компьютер работает так, будто вся группа — это один компьютер. Метод кластеризации используется для балансировки сетевой нагрузки и повышения отказоустойчивости сети.

CO (Central Office). Центральная АТС. Здание телефонной компании, в котором размещается оборудование коммутации каналов или абонентских линий и к которому подведены все кабели обслуживаемых абонентов.

Coaxial Cable. Коаксиальный кабель. Кабель, состоящий в общем случае из трех цилиндрических слоев: внутреннего проводника, изоляционного слоя и внешнего проводника. Иногда для лучшей защиты от атмосферных воздействий добавляется четвертый изоляционный слой вокруг внешнего проводника. В локальных сетях в настоящее время чаще всего используются два типа коаксиальных кабелей: 50-омный кабель для цифровых сигналов и 75-омный для аналоговых и высокоскоростных цифровых сигналов.

Collision Domain. Коллизионный домен. Область сети Ethernet, в которой распространяются пакеты, претерпевшие коллизию. Коллизию распространяют повторители и концентраторы. В то же время коммутаторы локальной сети, мосты и маршрутизаторы не распространяют коллизию.

Collision. Коллизия. Передача пакетов в кабель Ethetnet двумя узлами одновременно. Претерпевшие коллизию пакеты физически накладываются друг на друга, и оба повреждаются.

Connectionless Protocol. Протокол, не ориентированный на установку соединения. Протокол, в котором данные передаются без предварительной установки соединения, например UDP (User Datagram Protocol).

Connection-oriented Protocol. Протокол, ориентированный на установку соединения. Протокол, в котором для передачи данных между передающим и принимающим компьютерами предварительно нужно установить соединение. Примером такого протокола является TCP.

Console. Консоль. Терминальное оборудование, посредством которого в компьютер вводятся команды.

Contention. Конкуренция. Метод доступа, в котором сетевое устройство конкурирует с другими сетевыми устройствами за доступ к физическому носителю.

Convergence. Конвергенция. Распространение обновленной маршрутной информации по всем маршрутизаторам в методе динамической маршрутизации.

CPE (Customer Premises Equipment). Оборудование пользователя. Оборудование, установленное на территории пользователя и подключенное к сети телефонной компании. К нему относятся такие устройства, как терминалы, телефоны и модемы, предоставляемые телефонной компанией.

Cracker. Кракер. Хакер, специализирующийся на взломе паролей и пробных версий программ. *См.* Hacker.

CRC (Cyclical Redundancy Check). Контроль с использованием циклического избыточного кода. Метод проверки целостности принятого пакета данных. Код CRC вычисляется для пакета дважды: на передающем и принимающем компьютерах. Если результаты совпадают, значит, в процессе передачи пакет не изменился.

Crossover Cable. Перекрученный кабель. Отрезок нескольких неэкранированных витых пар Ethernet, концевые лепестки которых подключаются к устройствам перекрестно. Используется для прямого соединения двух компьютеров без концентратора или двух концентраторов без портов связи. Его еще иногда называют нуль-модемным кабелем.

Cryptography. Криптография. Наука о шифровании данных.

CSMA/CD (Carrier Sense Multiple Access Collision Detect). Множественный доступ с контролем несущей и обнаружением конфликтов. Метод доступа к сетевому носителю, в котором устройство, готовое передавать данные, предварительно проверяет, занят ли носитель (кабель). Если устройство определенный период времени не слышит в носителе никаких сигналов, то оно начинает передавать пакет. Если два устройства начинают передавать одновременно, то происходит коллизия пакетов, которую тут же обнаруживают оба устройства. В этом случае оба устройства передают пакеты повторно, переждав короткий случайный промежуток времени, чтобы коллизия не повторилась.

CSU/DSU (Channel Service Unit/Digital Service Unit). Устройство обслуживания канала/устройство обслуживания данных. Цифровое интерфейсное устройство, соединяющее оборудование пользователя с локальной цифровой телефонной линией.

Cybernetics. Кибернетика. Основатель кибернетики Норберт Винер (Norbert Weiner) определял ее как "теорию управления процессами в живых и неживых системах". Слово "кибернетика" часто используется в научно-фантастических романах и кинофильмах, герои которых — киборги — состоят из биологических и технических компонентов.

Cyborg. Киборг. Человек с имплантированными электронными и механическими органами, подключенный к сети таких же, как он, существ с целью разделения коллективной памяти и сознания.

D

D (Data) Channel. D-канал. Один из каналов линии ISDN ((Integrated Services Digital Network), по которому передаются служебные сигналы. Работает совместно с B-каналами, переносящими полезную информацию Другое название — Delta-канал. Типичная линия BRI (Basic Rate ISDN) состоит из одного D-канала на 16 Кбит/с и двух B-каналов по 64 Кбит/с каждый.

Daemon. Демон. Программа, непрерывно выполняющаяся на компьютере UNIX или Linux для обработки поступающих запросов. Обычно в конце имени программы ставится буква "d", например HTTPd (демон HTTP) выполняется на Web-сервере и отвечает на запросы HTTP.

Data Link Layer. Канальный уровень. Уровень 2 сетевой модели OSI. Разделен на два подуровня: MAC (Media Access Control) и LLC (Logical Link Control).

Data Store. Хранение данных. Хранение информации в файлах, в базах данных, на дисковых носителях и т.д.

Data Warehouse. Хранилище данных. Централизованное место хранения больших объемов данных в коммерческих сетях. Чаще всего реализуется на базе мэйнфрейма, мощного персонального компьютера, или группы компьютеров, на которых выполняется специальное программное обеспечение хранилища, например Windows 2000 Datacenter Server компании Microsoft.

Data. Данные. Информация, представленная в цифровой двоичной форме и предназначенная для обработки компьютерами или передачи по сети.

Datagram. Дейтаграмма. Порция данных вместе с маршрутной информацией. Для их передачи не нужно предварительно устанавливать соединение. Дейтаграммы IP — основной блок информации в Internet. Для обозначения логически сгруппированной порции информации на различных уровнях модели OSI и в разных сетевых каналах используются также термины "ячейка", "кадр", "сообщение", "пакет" и "сегмент".

DCE (Data Circuit-Terminating Equipment). Оконечное оборудование линии. Устройство, используемое для преобразования пользовательских данных из формата DTE (Data Terminal Equipment) в форму, принятую в линии глобальной сети.

DDNS (Dynamic DNS). Динамическая DNS. Тип DNS (Domain Name System), в которой выполняется динамическое обновление таблиц соответствия хостов и IP-адресов. Реализована в Windows 2000.

Dedicated Connection. Выделенное соединение. Соединение, зарезервированное для двух абонентов на весь период аренды, а не на период сеанса связи. *См.* Leased Line.

Default Gateway. Шлюз по умолчанию. Адрес маршрутизатора, на который по умолчанию передаются пакеты, предназначенные для адресата вне данной сети или подсети.

Default Route. Маршрут по умолчанию. Запись в таблице маршрутизации, применяемая для пакетов, следующая ретрансляция которых в таблице маршрутизации не определена явно.

Demarcation Point. Точка демаркации. Точка, в которой кончается CPE (Customer Premises Equipment) и начинается оборудование телефонной компании.

DES (Data Encryption Standard). Стандарт шифрования данных. Популярный симметричный метод шифрования с секретным ключом. В шифре DES используется

56-битовый ключ, применяемый к блокам данных размером в 64 бита. Усиленная версия DES называется 3DES (тройной DES).

Desktop Operating System. Настольная операционная система. Операционная система, выполняющаяся на рабочей станции или отдельном компьютере, за которым работает пользователь. Другое название — клиентская операционная система. Противоположное понятие — серверная операционная система. Под управлением настольных операционных систем выполняются рабочие приложения: текстовые редакторы, электронные таблицы, программы обработки графической информации и т.д.

Destination Address. Целевой адрес. Адрес сетевого устройства, на который передаются данные. *См.* Source address.

DHCP (Dynamic Host Configuration Protocol). Протокол динамического конфигурирования хостов. Протокол, предназначенный для динамического присвоения хостам IP-адресов. При его использовании адреса хостов, отказавшихся от них, автоматически используются повторно.

Dialup Connection. Коммутируемое соединение. Сетевое соединение, установленное по телефонной линии, в котором удаленный узел отключается по завершении сеанса связи. *См.* Dedicated Connection и Remote Access.

Digital. Цифровой. Цифровым называется сигнал, который может принимать только одно из дискретных значений, промежуточные значения для него являются запрещенными. Например, двоичный цифровой сигнал принимает значения 0 или 1.

Directory Service. Служба каталогов. Сетевая служба, предоставляющая доступ к центральной базе данных, в которой хранится информация о сетевых ресурсах (например, служба Active Directory компании Microsoft или NDS компании Novell).

Discrete State Signaling. Сигналы с дискретными состояниями. Синоним термина "цифровые сигналы".

Distance-Vector Routing Protocol. Протокол дистанционно-векторной маршрутизации. Протокол маршрутизации, в котором оптимальный маршрут выбирается путем минимизации количества ретрансляций. Другое название — алгоритм Беллмана–Форда (Bellman-Ford). В этом протоколе каждый маршрутизатор передает соседним маршрутизаторам обновленные таблицы маршрутизации. Один из недостатков протоколов дистанционно-векторной маршрутизации — возможность зацикливания маршрутов. Однако эти протоколы значительно проще протоколов маршрутизации на основе состояния каналов.

DNS (Domain Name System). Служба имен доменов. Система, используемая в Internet для преобразования имен сетевых узлов в адреса.

DoD (Department of Defense). Министерство обороны США. Правительственная организация, отвечающая за оборону страны. Финансирует разработку коммуникационных технологий.

Domain. Домен. В сетях Windows так называется группа компьютеров, пользующихся одной регистрационной базой данных. Регистрация, аутентификация и администрирование в домене выполняются централизованно.

Dotted-Decimal Notation. Нотация с десятичными точками. Принятая форма записи IP-адреса в виде a.b.c.d. Каждое число (десятичное) обозначает один байт в 4-байтовом IP-адресе.

DSL (Digital Subscriber Line). Цифровая абонентская линия. Цифровая служба высокоскоростной передачи данных по медным телефонным проводам. Существуют следую-

щие ее варианты: ADSL (Asymmetric DSL), HDSL (High-Speed DSL), SDSL (Symmetric DSL) и VDSL (Very-High-Speed DSL).

DTE (Data Terminal Equipment). Терминальное оборудование. Интерфейс, используемый компьютером для передачи данных на модем или из него либо на другое последовательное устройство.

Dual Homing. Двойное подключение. Сетевая топология, в которой устройство присоединяется к сети в двух независимых точках, называемых точками подключения. Одна из точек доступа является первичным соединением, а вторая — резервным, приводимым в действие, когда первичное соединение терпит крах.

Dumb Terminal. Неинтеллектуальный терминал. Устройство ввода или вывода (обычно клавиатура или дисплей), передающее сигналы на центральный компьютер (чаще всего на мэйнфрейм) либо выводящее результаты вычислений. Неинтеллектуальный терминал не обладает собственными вычислительными мощностями.

Dynamic Routing. Динамическая маршрутизация. Метод маршрутизации, в котором маршрут автоматически настраивается исходя из топологии сети или загрузки каналов. *См.* Static Routing.

E

EMI (Electromagnetic Interference). Электромагнитные помехи. Помехи от внешних электромагнитных импульсов, способные нарушить передачу данных по медному кабелю.

Encapsulate. Инкапсулирование. Помещение данных в заголовок протокола. Например, данные Ethernet перед передачей в сеть инкапсулируются в заголовок Ethernet. Другой пример: при соединении мостом различных сетей весь пакет одной сети инкапсулируется в заголовок канального протокола, используемого в другой сети.

Encoding. Кодирование. Процесс представления битов данных уровнями напряжения в проводнике.

Enterprise Network. Корпоративная сеть. Сеть, принадлежащая какой-либо организации — корпорации, агентству, школе и т.д.

ESH (Encapsulating Security Header). Заголовок инкапсуляции безопасности. Новый способ обеспечения безопасности, используемый в IPv6. Называется также IPing Encapsulating Security Header.

ESP (Encapsulating Security Payload). Инкапсуляция безопасности полезной нагрузки. Протокол, используемый в IPSec для защиты данных, передаваемых по сети с помощью протокола сетевого уровня IP. Протокол ESP обеспечивает как аутентификацию, так и шифрование данных.

Ethernet. Спецификация локальной сети на основе немодулированных сигналов, изобретенная в Xerox Corporation и разработанная совместно компаниями Xerox Corporation, Intel и Digital Equipment Corporation. В сетях Ethernet используется метод доступа CSMA/CD (Carrier Sense Multiple Access with Collision Detect) и самые разные кабели. Пропускная способность — 10 Мбит/с. Спецификации Ethernet аналогичны стандартам IEEE 802.3. *См.* Fast Ethernet.

Exabyte. Эксабайт (Эбайт). Единица измерения количества информации, равная 10^{18}, или 1 000 000 000 000 000 000 байт.

F

Failover Server. Резервный сервер. Один из серверов кластера, подключенный к первичному серверу и готовый принять на себя его функции в случае аварии.

Fast Ethernet. Быстрая Ethernet. Спецификация Ethernet с пропускной способностью 100 Мбит/с. Скорость передачи данных в Fast Ethernet в 10 раз выше, чем в Ethernet 10BaseT, в то же время в ней сохранены все основные характеристики старой Ethernet — формат кадров, механизмы физической адресации, максимальный размер кадра и т.д. Это позволяет использовать в сетях Fast Ethernet существующие инструменты управления и приложения сетей 10BaseT. Fast Ethernet определяется в расширении документа IEEE 802.3. *См.* Ethernet.

Fault Tolerance. Отказоустойчивость. Способность системы восстанавливаться с неповрежденными данными после краха. Обычно отказоустойчивость базируется на избыточности. Например, отказоустойчивость дисков обеспечивается путем использования нескольких дисков, на которых хранятся одни и те же данные. Это позволяет восстановить данные после краха одного из дисков.

FDDI (Fiber Distributed Data Interface). Распределенный интерфейс передачи данных по волоконно-оптическим каналам. Стандарт локальных сетей на основе волоконно-оптического кабеля, определяемый документом ANSI X3T9.5. Пропускная способность — 100 Мбит/с. В качестве метода доступа используется передача маркера. Максимальная длина сегмента кабеля — 2 км. В сетях FDDI для обеспечения избыточности используется архитектура с двойным кольцом.

Fiber-Optic Cable. Волоконно-оптический кабель. Кабель, в котором данные передаются импульсами света. По сравнению с другими носителями волоконно-оптический кабель дороже, однако он нечувствителен к электромагнитным помехам и обладает более высокой пропускной способностью.

FPNW (File and Print Services for NetWare). Служба печати и файлов для NetWare. Служебная программа, устанавливаемая на сервере Windows NT/2000 для предоставления доступа к своим файлам и принтерам клиентам NetWare.

Filter. Фильтр. Процесс или устройство, отсеивающее передаваемые пакеты на основе определенных характеристик, таких, как адрес источника, целевой адрес или используемый протокол. Проанализировав параметры пакета, фильтр принимает решение, передать его дальше или отбросить.

Firewall. Брандмауэр. Маршрутизатор, сервер доступа либо несколько маршрутизаторов или серверов доступа, служащие буфером между частной и публичной сетями. Для обеспечения безопасности частной сети в брандмауэре используется список контроля доступа или другие методы проверки пакетов.

Flat Addressing. Прямая адресация. Схема адресации, в которой для определения местоположения узла не используется логическая иерархия адресов.

Flooding. Лавинная передача. Техника передачи потоков данных, используемая коммутаторами и мостами. Данные, полученные на одном интерфейсе, передаются на все интерфейсы этого же устройства, кроме того, по которому эта информация первоначально была получена.

Flow. Поток. Поток данных, передающихся по сети из одной точки в другую (например, с одной станции локальной сети на другую). По одному каналу может передаваться несколько потоков.

FQDN (Fully Qualified Domain Name). Полностью определенное имя домена. Сетевое имя, состоящее из имени хоста (отдельного компьютера) и имени домена, в котором он находится.

Fragment. Фрагмент. Часть большого пакета, разбитого на меньшие составляющие. В сетях Ethernet так иногда называют кадры, размер которых меньше минимально допустимых 64 байт.

Fragmentation. Фрагментация. Процесс разбивки пакета на меньшие части для передачи по сетевому носителю, не поддерживающему исходный размер пакета.

Frame. Кадр. Логически сгруппированная порция информации, передаваемая по носителю как единица данных канального уровня. Иногда так называют заголовок и трейлер, используемые для синхронизации и контроля ошибок и окружающие пользовательские данные кадра. Логически сгруппированную порцию информации на разных уровнях модели OSI и в различных коммуникационных цепях обозначают также терминами дейтаграмма, сообщение, пакет и сегмент.

Frame Relay. Промышленный стандарт коммутационного протокола канального уровня. Протокол Frame Relay более эффективен, чем X.25, который он призван со временем заменить.

FTP (File Transfer Protocol). Протокол передачи файлов. Протокол прикладного уровня, часть стека TCP/IP. Используется для передачи файлов между узлами сети. Протокол FTP описан в документе RFC 959.

Full Duplex. Дуплексная связь. Метод коммуникации, в котором информация передается в прямом и обратном направлениях одновременно.

G

Gateway Service for NetWare. Служебная программа, устанавливаемая на серверах Windows NT/2000 и предоставляющая клиентам сервера Windows доступ к ресурсам сервера NetWare. Доступ предоставляется путем трансляции запросов, поданных в протоколе SMB (Server Message Block), в протокол разделения файлов NCP (NetWare Core Protocol).

Gateway. Шлюз. Применительно к IP — устаревший термин, обозначавший устройство маршрутизации. В настоящее время такое устройство обозначают термином "маршрутизатор", а шлюз — это устройство или программа, выполняющая на прикладном уровне преобразование данных из одного протокола в другой. *См.* Router.

Gb (gigabit). Гбит (гигабит). Приблизительно 1 000 000 000 бит.

GB (gigabyte). Гбайт (гигабайт). 1 073 741 824 байт. (Байт равен 8 битам.)

Gbps (gigabits per second). Гбит/с (гигабит в секунду). Единица измерения скорости передачи данных.

GBps (gigabytes per second). Гбайт/с (гигабайт в секунду). Единица измерения скорости передачи данных.

Ghost. Программный продукт компании Symantec, предназначенный для копирования (клонирования) всех данных и структур данных с одного диска на другой с сохранением форматирования и размеров разделов, т.е. создания точной копии.

GHz. ГГц. Гигагерц. Единица измерения частоты электромагнитных волн, или переменного тока, равная 10^9 Гц. Применяется для измерения частоты сверхвысокочастотных сигналов и как характеристика быстродействия микропроцессора, установленного в компьютере. *См.* Hz.

GNOME (GUI Network Object Model Environment). Графический интерфейс и группа приложений операционной системы Linux, в которой используется рабочий стол, аналогичный рабочему столу Windows.

GPS (Global Positioning System). Глобальная система позиционирования. Система устройств, предназначенных для точного определения текущих географических координат пользователя. Работает на основе приема сигналов от трех из 24 спутников Земли, запущенных и управляемых Министерством обороны США. Портативный компьютер обрабатывает принятые от спутников сигналы по формулам тригонометрии и выводит на экран текущие координаты пользователя.

Group. Группа. Группа учетных записей пользователей, администрируемых как одно целое. Пользователи, являющиеся членами группы, имеют права доступа, присвоенные группе. Благодаря этому нет необходимости присваивать права доступа отдельно каждому пользователю.

Groupware. Программное обеспечение коллективного пользования. Программы приложений, разработанные для совместного использования. С их помощью пользователи могут совместно работать над одними и теми же документами или проектами. Примеры таких программ — Microsoft Exchange, Lotus Notes и Novell Groupwise.

GUI (Graphical User Interface). Графический интерфейс пользователя. Среда пользователя, в которой входные и выходные данные приложения представлены в графическом и текстовом виде. Пользователь управляет средой, выполняя с помощью клавиатуры и мыши операции над различными элементами управления, такими, как кнопки, пиктограммы, области ввода и т.д. Характерными примерами GUI являются интерфейсы операционных систем Windows и Apple Macintosh.

H

Hacker. Хакер. Специалист в области компьютерных и коммуникационных технологий, способный взламывать компьютерные системы с применением языков программирования низкого уровня.

HAL (Hardware Abstraction Layer). Уровень аппаратных абстракций. Часть архитектуры Windows NT/2000, служащая интерфейсом операционной системы с оборудованием. Уровень HAL предотвращает непосредственный доступ пользовательских приложений к оборудованию и повышает стабильность операционной системы.

Half Duplex. Полудуплексная связь. Метод коммуникации, в котором информация может передаваться в прямом и обратном направлениях, но не одновременно.

Handheld Computer. Карманный компьютер. Легкий компьютер небольших размеров, который можно носить с собой и пользоваться им в любом месте. Примеры портативных компьютеров — Palm Pilot и Pocket PC.

Handshake. Приветствие. Последовательность сообщений, обмениваемых между двумя или большим количеством сетевых устройств перед началом передачи данных в целях аутентификации и синхронизации.

Hardware Address. *См.* MAC Address.

Hardware Loopback. Аппаратная петля. Устройство, с помощью которого передающие контакты сетевого адаптера подключаются к принимающим контактам. Используется для проверки работоспособности сетевых адаптеров.

Hash Function. Хэш-функция. Математическая операция, выполняемая над исходными данными. Результатом операции является строка битов фиксированной длины, из которой невозможно получить исходные данные, выполнив обратную операцию.

HDLC (High-Level Data Link Control). Высокоуровневый протокол управления каналом. Синхронный бит-ориентированный протокол канального уровня, разработанный организацией ISO (International Standards Organization). Протокол HDLC определяет метод инкапсуляции данных в синхронных последовательных каналах на основе параметров кадра и контрольных сумм.

Header. Заголовок. Служебная информация, помещаемая перед данными при их инкапсулировании для передачи по сети.

Hertz. Герц (Гц). Единица измерения частоты, равная одному циклу в секунду.

Hexadecimal (Base 16). Шестнадцатеричная система счисления (по основанию 16). Система счисления, в которой для представления чисел от 0 до 15 используются цифры от 0 до 9 в их обычном значении (как в десятичной системе) и буквы от A до F. Шестнадцатеричное число равно сумме произведений: цифра первого справа разряда умножается на $16^0 = 1$, второго разряда — на $16^1 = 16$, третьего — на $16^2 = 256$ и т.д.

Hop. Ретрансляция. Прохождение пакета данных между двумя узлами, например между двумя маршрутизаторами.

Hop Count. Количество ретрансляций. Показатель, рассматриваемый как длина маршрута, т.е. расстояние между передающим и принимающим узлами. Такой показатель называется также метрикой маршрута. В протоколе RIP (Routing Information Protocol) количество ретрансляций является единственным критерием выбора маршрута.

Host. Хост. Компьютерная система в составе сети. Понятие хоста близко понятию узла, однако хост может быть только компьютерной системой, а узел — любой сетевой системой, включая серверы, маршрутизаторы и т.д. Хост является узлом. *См.* Node.

Host Address. Адрес хоста. *См.* Host Number.

Host Number. Номер хоста. Часть IP-адреса, указывающая на конкретный компьютер или хост.

HTML (Hypertext Markup Language). Язык разметки гипертекста. Простой язык форматирования гипертекстовых документов, в котором для задания форматов и шрифтов отдельных частей документа используются дескрипторы — специальные пометки в тексте. Документ в формате HTML интерпретируется и выводится на экран каким-либо Web-приложением, например Web-броузером.

HTTP (Hypertext Transfer Protocol). Протокол передачи гипертекста. Протокол, используемый Web-серверами и Web-броузерами для передачи гипертекстовых файлов.

Hub. Концентратор. 1. Устройство, к которому подключаются все кабели сети звездообразной топологии. Концентратором называют также многопортовый повторитель. 2. Компонент оборудования или программного обеспечения, содержащий многие независимые модули, подключенные к сети, или к межсетевому оборудованию. Концен-

траторы делятся на активные (регенерирующие и усиливающие передаваемый через них сигнал) и пассивные (просто повторяющие или размножающие сигнал).

Hybrid Network. Гибридная сеть. Сеть (локальная или глобальная), в которой используются программные и аппаратные компоненты различных типов.

Hyperlink. Гиперссылка. Элемент гипертекстового документа, связанный с другим файлом, документом или элементом этого же документа. На экране гиперссылка выглядит как слово или небольшая фраза, отмеченная другим цветом. Если щелкнуть на ней кнопкой мыши, то она активизируется, т.е. на экран выводится ассоциированный документ.

I

IAB (Internet Architecture Board). Координационный совет сети Internet. Организация исследователей и специалистов, занимающаяся вопросами развития и поддержания архитектуры Internet. Организует работу различных групп Internet — IANA, IESG и IRSG. Состав IAB назначается доверительными лицами организации ISOC (Internet Society). *См.* IANA, IESG, IRSG и ISOC.

IANA (Internet Assigned Numbers Authority). Агентство по выделению имен и уникальных параметров протоколов Internet. Организация, работающая под покровительством ISOC и входящая в состав IAB. Организация IANA делегирует полномочия распределения адресного пространства IP и присвоения имен доменов различным организациям, таким, как InterNIC.

ICANN (Internet Corporation for Assigned Names and Numbers). Организация по назначению имен и адресов Internet. Частная бесприбыльная организация, ответственная за распределение адресного пространства IP, работу службы DNS (Domain Name System) и управление корневыми серверами. Раньше эти функции выполнялись организацией IANA. *См.* IANA.

ICMP (Internet Control Massage Protocol). Протокол управляющих сообщений в Internet. Протокол сетевого уровня, сообщающий об ошибках и обеспечивающий восстановление связи в аварийных ситуациях. Один из четырех протоколов сетевого уровня семейства TCP/IP. Описан в документе RFC 792.

IEEE (Institute of Electrical and Electronic Engineers). Институт инженеров по электротехнике и электронике. Организация специалистов, занятая развитием коммуникационных технологий и разработкой сетевых стандартов. Стандарты IEEE локальных сетей на сегодняшний день широко распространены.

IEEE 802.1. Протокол IEEE для локальных сетей, являющийся введением в стандарты управления локальными и городскими сетями, стандарты мостов, работающих на подуровне MAC (Media Access Control) и стандарты STA (Spanning-Tree Algorithm), используемого для предотвращения зацикливания мостов.

IEEE 802.10. Протокол IEEE для локальных сетей, специфицирующий виртуальные частные сети — способ установления безопасного соединения частных сетей посредством публичной сети Internet.

IEEE 802.11. Протокол IEEE для локальных сетей, обусловливающий реализацию беспроводных локальных сетевых технологий.

IEEE 802.12. Протокол IEEE для локальных сетей, специфицирующий метод доступа к среде на основе запроса приоритетов, разработанный компанией Hewlett Packard и объединяющий преимущества технологий Ethernet, Token Ring и ATM (Asynchronous Transfer Mode) для скоростных локальных соединений.

IEEE 802.2. Протокол IEEE для локальных сетей, специфицирующий реализацию подуровня LLC (Logical Link Control), входящего в канальный уровень. Спецификации IEEE 802.2 обусловливают методы обработки ошибок, параметры кадров, управление информационными потоками и служебный интерфейс сетевого уровня (уровня 3). *См.* IEEE 802.3 и IEEE 802.5.

IEEE 802.3. Протокол IEEE для локальных сетей, специфицирующий реализацию физического уровня и подуровня MAC (Media Access Control), входящего в канальный уровень. В протоколе IEEE 802.3 используется метод доступа CSMA/CD (Carrier Sense Multiple Access with Collision Detect) для самых разных скоростей передачи и типов носителя. Расширения стандартов IEEE 802.3 специфицируют Fast Ethernet. Вариантами исходной спецификации IEEE 802.3 являются архитектуры 10Base2, 10Base5, 10BaseF, 10BaseT и 10Broad36. Вариантами Fast Ethernet являются архитектуры 100BaseTX и 100BaseFX.

IEEE 802.5. Протокол IEEE для локальных сетей, специфицирующий реализацию физического уровня и подуровня MAC (Media Access Control), входящего в канальный уровень. В протоколе IEEE 802.5 используется метод доступа на основе передачи маркера для скоростей передачи 4 и 16 Мбит/с по экранированным и неэкранированным витым парам. Функциональные и рабочие характеристики, специфицируемые протоколом IEEE 802.5, эквивалентны характеристикам архитектуры Token Ring компании IBM.

IEEE 802.6. Протокол IEEE, специфицирующий стандарты для сетей, относящихся к локальными, но имеющих размер больше размера локальных сетей, но меньше, чем у глобальных.

IEEE 802.7. Протокол IEEE для локальных сетей, специфицирующий скоростные технологии передачи данных с использованием телевизионных кабелей или метода FDM (Frequency Division Multiplexing), в котором по одному кабелю на разных частотах передаются разные сигналы.

IEEE 802.8. Протокол IEEE для локальных сетей, специфицирующий использование в сетях волоконно-оптических кабелей и технологии FDDI (Fiber Distributed Data Interface).

IEEE 802.9. Протокол IEEE для локальных сетей. Специфицирует передачу голоса и данных по линиям ISDN (Integrated Services Digital Network).

IESG (Internet Engineering Steering Group). Исполнительный комитет IETF. Руководящее подразделение IETF, утверждающее результирующие документы групп IETF.

IETF (Internet Engineering Task Force). Проблемная группа проектирования Internet. Специальная комиссия, состоящая более чем из 80 рабочих групп и отвечающая за разработку стандартов Internet. Организация IETF работает под покровительством ISOC (Internet Society).

IGRP (Interior Gateway Routing Protocol). Шлюзовый протокол маршрутизации в Internet. Протокол, разработанный компанией Cisco для решения проблем, связанных с маршрутизацией в больших неоднородных сетях.

IIS (Internet Information Server). Программа Web- и FTP-сервера компании Microsoft, работающая под управлением Windows NT/2000.

inode (i-node). i-узел. Описание отдельного файла в системе UNIX, включая информацию расположении файла на диске.

Input/Output. Ввод-вывод. Операция передачи данных в компьютер или из компьютера. Иногда обозначается как I/O.

Integration. Интеграция. Объединение программных и аппаратных продуктов разных поставщиков в одну систему.

Interface. Интерфейс. 1. Соединение двух систем или устройств. 2. В технологии маршрутизации — соединение сетей. 3. В телефонии — общая граница, определяемая общими характеристиками физического соединения, характеристиками сигналов и средствами обмена сигналами. 4. Граница между соседними уровнями модели OSI.

Internet Protocol. Протокол сети Internet. Любой протокол, входящий в стек протоколов TCP/IP. *См.* IP и TCP/IP.

internet. Сеть, состоящая из сетей. Не путайте с Internet!

Internet. Самая большая глобальная сеть, соединяющая десятки тысяч сетей, разбросанных по всему миру. Исследования и разработки Internet ориентированы на практические нужды корпоративных и индивидуальных пользователей. Сообществом Internet разработаны многие ведущие сетевые технологии. Internet в значительной степени развилась из ARPAnet. В свое время, чтобы не путать с более общим термином "internet", она называлась DARPA Internet (Defense Advanced Research Projects Agency).

Internetwork. Объединенная сеть. Набор сетей, соединенных маршрутизаторами и другими устройствами, работающий как одна сеть.

Internetworking. Межсетевой обмен. Средства объединения сетей. Термин относится к программным и аппаратным продуктам, процедурам, методам и т.д.

InterNIC. Организация, обслуживающая сообщество Internet путем предоставления пользователям помощи, документации и услуг обучения и регистрации имен доменов Internet, сетевых адресов и т.д. В прошлом она называлась NIC.

Interoperability. Межоперационное взаимодействие. Способность программных и аппаратных компонентов успешно взаимодействовать с компонентами и системами других поставщиков.

Intranet. Внутренняя сеть, доступ к которой могут получать только пользователи частной локальной сети организации.

IOS (Internetwork Operating System). *См.* Cisco IOS.

IP (Internet Protocol). Протокол Internet. Протокол сетевого уровня, входящий в стек TCP/IP и специфицирующий межсетевые службы, не ориентированные на установку соединения. В протоколе IP представлены средства адресации, спецификации типов услуг, безопасности, а также фрагментации и сборки. Определяется в документе RFC 791. В настоящее время IPv4 (Internet Protocol version 4) является наиболее распространенным протоколом коммутации пакетов, не ориентированным на установку соединения. *См.* IPv6.

IP address. IP-адрес. Адрес длиной 32 бита, присваиваемый хостам с помощью протокола TCP/IP. Каждый IP-адрес принадлежит одному из пяти классов (A, B, C, D или E) и записывается в виде четырех октетов, разделенных точками. В адрес входят номер сети, необязательный номер подсети и номер хоста. Номера сети и подсети используются для маршрутизации, а номер хоста — для определения конкретного хоста в сети или подсети. Для извлечения из IP-адреса номеров сети и подсети используется маска подсети. Иногда IP-адрес называют адресом Internet.

IP spoofing. Подмена (спуфинг) IP. Подделка IP-адреса. Метод спуфинга применяется, чтобы "ввести в заблуждение" механизмы сетевой безопасности, например фильтры или списки контроля доступа.

ipconfig. Утилита командной строки, используемая в Windows NT/2000 в целях получения конфигурационной информации TCP/IP для сетевого адаптера.

IPSec (IP Security). Протокол, используемый для защиты передаваемых по сети данных путем применения протоколов шифрования и аутентификации.

IPv6 (IP version 6). Версия, призванная заменить используемую в настоящее время версию IPv4. Поддерживает идентификатор потока в заголовке пакета. Устаревшее название — IPng.

IPX (Internet Packet Exchange). Межсетевой обмен пакетами. Протокол сетевого уровня (уровня 3), используемый в сетях NetWare для передачи данных от сервера на рабочие станции. Протокол IPX похож на IP и XNS (Xerox Network Standard).

IR (infrared radiation). Инфракрасное излучение. Излучение на частотах, более высоких, чем у радиоволн, но меньших, чем у видимого света. Используется в средствах беспроводной коммуникации, устройствах дистанционного управления, детекторах движения, устройствах ночного видения, в медицинском оборудовании и в системах управления летательными аппаратами.

IRSG (Internet Research Steering Group). Научно-исследовательская группа сети Internet. Группа, руководящая работой различных исследовательских групп и организующая семинары и конференции, посвященные вопросам развития Internet.

ISDN (Integrated Service Digital Network). Цифровая сеть связи с комплексными услугами. Предоставляемый телефонными компаниями протокол коммуникации, позволяющий передавать по телефонным сетям данные и голос одновременно.

ISO (International Organization for Standardization). Международная организация стандартизации. Несет ответственность за разработку и внедрение самых разных стандартов, включая стандарты коммуникационных технологий. Ею разработана популярная сетевая модель OSI (Open System Interconnection).

ISOC (Internet Society). Общество Internet. Международная бесприбыльная организация, основанная в 1992 году. Координирует функционирование и развитие Internet. Организация ISOC делегирует разнообразные полномочия другим группам, имеющим отношение к Internet, таким, как IAB. Штаб-квартира ISOC находится в Рестоне (Reston), штат Вирджиния. *См.* IAB.

ISP (Internet Service Provider). Провайдер услуг Internet. Компания, предоставляющая доступ в Internet другим компаниям и лицам с помощью средств удаленного коммутируемого доступа или выделенных линий.

IT (Information Technology). Информационные технологии. Термин охватывает самые различные области разработки и применения средств коммуникации и обработки информации, включая компьютеры и телефонию, а также создание, хранение и использование информации.

ITU-T (International Telecommunication Union, Telecommunication Standardization Sector). Международный союз телекоммуникации, сектор стандартов телекоммуникации. Международная организация, занятая разработкой стандартов коммуникации. Прежнее название — CCITT (Committee for International Telegraph and Telephone). *См.* CCITT.

J

Java. Язык программирования, разработанный специально для создания приложений Internet — так называемых аплетов, т.е. небольших приложений, встраиваемых в Web-страницы.

Java Virtual Machine (JVM). Виртуальная машина Java. Программа компании Sun Microsystems, используемая для обработки и вывода на экран аплетов Java.

JPEG, JPG. Распространенный формат графических файлов, часто используемый для изображений, встраиваемых в Web-страницы. Поддерживается Web-броузерами и обеспечивает относительно быструю загрузку изображений благодаря компактности файлов в этом формате.

K

Kb (kilobit). Кбит (килобит). Приблизительно 1000 бит.

KB (kilobyte). Кбайт (килобайт). Приблизительно 1000 байт.

KBps (kilobytes per second). Кбайт/с (килобайт в секунду). Скорость передачи данных.

Kbps (kilobits per second). Кбит/с (килобит в секунду). Скорость передачи данных.

Kerberos. Метод обеспечения безопасности, в котором аутентификация выполняется на основе зашифрованных "билетов", вследствие чего отпадает необходимость передавать по сети пользовательские пароли. Система Kerberos является стандартом Internet, ее средства аутентификации используются службой каталогов Active Directory системы Windows 2000.

Kernel. Ядро. Основа операционной системы компьютера, предоставляющая базовые услуги другим частям операционной системы.

L

LAN (Local Area Network). Локальная сеть. Высокоскоростная надежная сеть, покрывающая сравнительно небольшую территорию (до 2 000 м). В локальную сеть объединены рабочие станции, периферийное оборудование, терминалы и другие устройства, расположенные в одном или нескольких зданиях. Стандарты локальных сетей определяют типы кабелей и методы передачи данных на физическом и канальном уровнях модели OSI. Широко распространенные архитектуры локальных сетей — Ethernet, FDDI и Token Ring. *См.* VLAN.

LAN Link. Канал локальной сети. Средства объединения компьютеров в локальную сеть. Иногда их называют архитектурой локальной сети. Примерами распространенных архитектур являются Ethernet, Token Ring, FDDI, AppleTalk и ARCnet.

Latency. Задержка. Период времени между моментом, когда устройство запросило доступ к сети, и предоставлением разрешения передавать данные.

Layer. Уровень. Часть сетевых функций, определяемая их разделением соответственно модели OSI. Разделение сетевых функций и процедур на уровни упрощает задачи коммуникации двух компьютеров.

LDAP (Lightweight Directory Access Protocol). Упрощенный протокол службы каталогов. Упрощенная версия протокола DAP (Directory Access Protocol), являющаяся стандартом сетевых служб каталогов. В протоколе LDAP используется иерархическая древовидная структура каталогов и общие соглашения об именовании.

Leased Line. Выделенная линия. Линия передачи данных, зарезервированная для конкретного заказчика. *См.* Dedicated Connection.

Legacy. Наследие. Оборудование, приложения и данные, унаследованные от старых технологий.

Link-Layer Address. *См.* MAC Address.

Link. Канал. Путь прохождения данных, состоящий из кабелей и оборудования между передающим и принимающим компьютерами. Этот термин чаще всего используется в технологиях глобальных сетей. Иногда его называют линией.

Link-State Routing Protocol. Протокол маршрутизации на основе состояния каналов. Протокол маршрутизации, в котором каждый маршрутизатор распространяет по широковещательным или мультивещательным адресам информацию о "стоимости" передачи данных каждому из своих соседей. В процессе работы протокола создается устойчивый образ состояния сети, следовательно, зацикливания маршрутов не происходит. Однако это достигается ценой дополнительных вычислений и большей загрузки сети служебными сигналами по сравнению с протоколами дистанционно-векторной маршрутизации.

Linux. Операционная система, созданная Линусом Торвальдсом (Linus Torvalds) в университете города Хельсинки, Финляндия. Система Linux разработана на основе UNIX как дешевая и открытая операционная система для персональных компьютеров.

LLC (Logical Link Control). Управление логическим соединением. Более высокий из двух подуровней канального уровня модели OSI, специфицированный документами IEEE. На подуровне LLC контролируются ошибки, выполняется управление потоками, обработка кадров и адресация подуровня MAC (Media Access Control). Доминирующая спецификация подуровня LLC — документ IEEE 802.2 — включает варианты протокола LLC, как ориентированного, так и не ориентированного на установку соединения.

Load Balancing. Балансировка нагрузки. В технологии маршрутизации — распределение маршрутизатором потоков информации по всем своим сетевым портам для выравнивания расстояний от хостов-источников. Хороший алгоритм балансировки нагрузки использует информацию как о скорости передачи, так и о надежности каналов. Балансировка нагрузки повышает эффективность использования сегментов сети, увеличивая таким образом ее пропускную способность.

Load. Нагрузка. Объем данных, обрабатываемый компонентом сети, например маршрутизатором или каналом.

Local Loop. Локальная петля. Отрезок кабеля (обычно медного), выходящий за пределы демаркационной линии в центральный офис провайдера услуг глобальной сети.

Log. Журнал. Список поданных запросов на ресурсы, происшедших ошибок и других событий, проанализировав которые можно получить информацию, полезную для задач обеспечения безопасности, оптимизации или устранения неполадок.

Logical Addressing. Логическая адресация. Схема адресации, используемая протоколами сетевого уровня, такими, как IP или IPX.

Logical Topology. Логическая топология. Пути, по которым логически проходит информация, независимо от физической топологии сети.

Login. Регистрация. Представление себя операционной системе или приложению в целях получения доступа. Обычно регистрация предполагает ввод имени пользователя и пароля.

Loop. Петля, цикл. Замкнутый маршрут, по которому могут проходить пакеты, никогда не достигая адресата информации. Возникает при зацикливании маршрута в протоколах дистанционно-векторной маршрутизации.

Loopback Test. Тест обратной петли. Тест, в котором сигналы передаются, а затем направляются обратно в источник с некоторой точки пути коммуникации. Часто применяется для проверки работоспособности сетевого интерфейса.

M

MAC (Media Access Control). Управление доступом к среде. Одна из задач протокола канального уровня. Выполняется применением метода доступа к среде на основе 6-байтового (48-битового) адреса источника и целевого адреса.

MAC Address. MAC-адрес. Стандартизированный адрес канального уровня, необходимый для каждого порта или устройства, подключенного к сети. Сетевые устройства используют MAC-адреса для обнаружения в сети требуемого порта и для создания и обновления маршрутных таблиц. Длина MAC-адреса составляет 6 байт. Выделение MAC-адресов регулируется организацией IEEE. Другие названия MAC-адреса — физический адрес, адрес оборудования и адрес MAC-уровня.

Mac OS. Операционная система, используемая на компьютерах Apple Macintosh.

Machine Language. Машинный язык. Язык низкого уровня. Программа на машинном языке, представляющая собой последовательность нулей и единиц, управляет работой компьютера. Программами на машинном языке являются операционные системы, серверы, утилиты, сетевые службы, процедуры протоколов, пользовательские приложения и т.д. Программы на языках высокого уровня, например Basic или C++, автоматически преобразуются (транслируются) в программы на машинном языке.

Mainframe. Мэйнфрейм. Большой центральный компьютер, используемый для обработки огромного количества информации. Наиболее характерный пример мэйнфреймов — компьютеры компании IBM.

MAN (Metropolitan Area Network). Городская сеть. Сеть, охватывающая территорию большого города. Географически область действия городской сети больше, чем локальной, однако меньше, чем глобальной. *См.* LAN и WAN.

MAPI (Messaging Application Programming Interface). Интерфейс прикладного программирования электронной почты. Программный интерфейс, разработанный компанией Microsoft для передачи электронных сообщений. Поддерживается многими приложениями, например клиентской почтовой программой Eudora.

Mask. *См.* Subnet Mask.

MAU (Media Attachment Unit). Устройство подключения к среде. Устройство, используемое в сетях Ethernet и определяемое стандартом IEEE 802.3. Устройство MAU, которое может быть как встроено в станцию, так и поставляться в виде отдельного устройства, выполняет функции физического уровня: преобразование цифровых данных с интерфейса Ethernet, обнаружение коллизий и передачу данных в сеть. Иногда называют MSAU.

MB (megabit). Мбит (мегабит). Приблизительно 1 000 000 бит.

MB (megabyte). Мбайт (мегабайт). Приблизительно 1 000 000 байт.

Mbone. Часть Internet, используемая для передачи мультивещательных сообщений (сообщений, передаваемых многим пользователям одновременно), обычно потоковых аудио и видео. *См.* Multicast.

Mbps (megabits per second). Мбит/с (мегабит в секунду). Единица измерения скорости передачи данных.

MBps (megabytes per second). Мбайт/с (мегабайт в секунду). Единица измерения скорости передачи данных.

MBR (Master Boot Record). Главная загрузочная запись. Данные, хранящиеся в первом секторе диска. Содержит информацию о размещении файлов операционной системы, необходимую для их загрузки в память компьютера. Этот процесс называется загрузкой операционной системы.

MCP (Microsoft Certified Professional). Сертифицированный специалист Microsoft.

MCSE (Microsoft Certified Systems Engineer). Сертифицированный системный инженер Microsoft.

MCT (Microsoft Certified Trainer). Сертифицированный инструктор Microsoft.

MD5 (Message Digest 5). Односторонний алгоритм хэширования, результатом которого являются 128-битовые блоки кода.

Media. Носитель. Физическая среда, по которой передаются сигналы. Распространенные сетевые носители — витая пара, коаксиальный кабель, волоконно-оптический кабель и атмосфера, по которой передаются радиоволны, лазерный луч и инфракрасное излучение. Иногда носитель называют *физическим носителем*.

Megahertz. Мегагерц. Единица измерения частоты. Равен одному миллиону циклов в секунду. Используется для измерения частоты электромагнитных волн и переменного тока, а также как характеристика быстродействия микропроцессора. *См.* Hertz.

Memory Buffer. Буфер памяти. Область памяти, в которой коммутатор хранит передаваемые данные. В более широком значении — любая область памяти, предназначенная для промежуточного хранения данных.

Memory. Память. Устройство (обычно в компьютере), в котором хранятся данные. Называется также оперативной памятью или RAM (Random Access Memory). Доступ к оперативной памяти выполняется значительно быстрее, чем к дисковым накопителям. В отличие от дисковых накопителей, оперативная память предназначена для временного хранения данных — при выключении или перезагрузке компьютера содержимое памяти теряется.

Mesh. Ячейка. Сетевая топология, в которой каждое устройство соединено со многими другими. Ячеистые соединения избыточны, поскольку сигнал от узла к узлу может проходить многими путями. Это значительно повышает надежность сети. Топология сети может быть реализована как полная ячейка (в которой каждый узел соединен с каждым другим узлом) или как частичная ячейка (узел может быть соединен не со всеми другими узлами).

Message. Сообщение. Информация, логически сгруппированная на прикладном уровне. Чаще всего состоит из нескольких пакетов, т.е. порций информации, логически сгруппированных на более низких уровнях. Термины "дейтаграмма", "кадр", "пакет"

и "сегмент" используются для описания логического группирования информации на различных уровнях модели OSI и в различных каналах коммуникации.

Metadata. Метаданные. Определение или описание данных.

MIB (Management Information Base). База данных управляющей информации. База данных, используемая и поддерживаемая протоколом управления сетью, например SNMP (Simple Network Management Protocol). Значения объектов MIB обновляются и считываются с помощью команд SNMP обычно посредством графического интерфейса системы управления сетью. Объекты MIB организованы в древовидную иерархическую структуру, содержащую публичные и частные ветви.

Modem (Modulator-Demodulator). Модем (модулятор-демодулятор). Устройство, предназначенное для преобразования цифровых сигналов в аналоговые и наоборот. В передающем компьютере модем преобразует цифровые сигналы в аналоговые, которые можно передавать по аналоговым (обычно телефонным) линиям. В принимающем компьютере модем преобразует аналоговые сигналы обратно в цифровые. Таким образом, модем позволяет передавать цифровые сигналы по аналоговым линиям.

MSAU (Multistation Access Unit). *См.* MAU.

MTU (Maximum Transmission Unit). Максимальный передаваемый блок. Максимальный размер пакета в байтах, который может обработать данный (характеризуемый показателем MTU) интерфейс.

Multicast Address. Групповой адрес. Один адрес, указывающий на многие сетевые устройства.

Multicast. Многоадресная рассылка. Копирование пакетов сетью и передача их по предопределенному подмножеству сетевых адресов, определенных в специальной таблице.

Multiplexing. Мультиплексирование. Одновременная передача многих логических сигналов по одному физическому каналу.

Multivendor Network. Сеть многих поставщиков. Сеть, в которой используются компоненты более чем одного поставщика. Эксплуатировать и администрировать такие сети значительно сложнее сетей на основе компонентов одного поставщика.

N

NAK (negative acknowledgment). Негативное подтверждение. Ответ, переданный принимающим устройством передающему устройству и означающий, что полученная информация содержит ошибки.

Name Resolution. Разрешение имени. Установление взаимно однозначного соответствия между именем и сетевым адресом.

Name Server. Сервер имен. Сервер, разрешающий (отображающий) сетевые имена на сетевые адреса.

NAT (Network Address Translation). Трансляция сетевых адресов. Один из методов сокращения нехватки глобальных уникальных IP-адресов. Используя метод NAT, организации, имеющие неуникальные глобальные адреса, могут подключаться к Internet путем трансляции этих адресов в пространство глобальных маршрутизируемых адресов.

NCP (NetWare Core Protocol). Протокол ядра NetWare. Протокол разделения файлов, используемый для предоставления доступа к ресурсам сервера NetWare.

NCP (NetWare Control Program). Программа управления сетью. Программа, маршрутизирующая потоки данных между контроллерами коммуникации и сетевыми ресурсами.

NDIS (Network Driver Interface Specification). Спецификация стандартного интерфейса сетевых адаптеров. Спецификация, разработанная компанией Microsoft для адаптеров сетевых интерфейсов. Позволяет привязывать многие протоколы к одному адаптеру или многие адаптеры к одному протоколу.

NDS (Novell Directory Service). Служба каталогов компании Novell. Совместимая с LDAP (Lightweight Directory Access Protocol) служба каталогов, используемая в сетях NetWare 4.*x* и более высоких версий.

NetBEUI (NetBIOS Extended User Interface). Расширенный пользовательский интерфейс NetBIOS. Расширенная версия протокола NetBIOS, используемая такими сетевыми операционными системами, как LAN Manager, LAN Server, Windows for Workgroups и Windows NT. В протоколе NetBEUI формализованы транспортные кадры и добавлены некоторые дополнительные функции. В NetBIOS реализован протокол LLC2.

NetBIOS (Network Basic Input/Output System). Сетевая базовая система ввода-вывода. Интерфейс программирования приложений, используемый приложениями локальных сетей IBM для подачи запросов на сетевые услуги от процессов нижних уровней. Эти услуги могут включать установку и завершение сеанса или передачу информации.

NetWare. Популярная распределенная сетевая операционная система, разработанная компанией Novell. Предоставляет простой удаленный доступ к файлам и другие распределенные сетевые услуги.

Network Address. Сетевой адрес. Адрес сетевого уровня, указывающий на логическое, а не физическое устройство.

Network Administrator. Сетевой администратор. Человек, ответственный за поддержание и управление работой сети.

Network Analyzer. Сетевой анализатор. Устройство или программа, предоставляющая средства устранения неполадок в сети, включая анализаторы пакетов различных протоколов, заранее подготовленные проверочные программы, фильтры пакетов и средства передачи пакетов.

Network Interface Card. Сетевой адаптер, сетевая карта. Электронная плата, обеспечивающая передачу сигналов из компьютера в сеть и в обратном направлении.

Network Interface. Сетевой интерфейс. Граница между несущей сетью и частными устройствами и программами.

Network Layer. Сетевой уровень. Уровень 3 модели OSI. Обеспечивает установку соединения и выбор маршрута между передающим и принимающим хостами. На сетевом уровне выполняется маршрутизация пакетов. Приблизительно соответствует уровню управления маршрутом модели SNA (Systems Network Architecture).

Network Number. Номер сети. Часть IP-адреса, определяющая сеть, в которой находится хост.

Network Operating System. Сетевая операционная система. Операционная система, управляющая работой сети. Например, NetWare компании Novell или Windows NT/2000.

Network. Сеть. Совокупность компьютеров, принтеров, коммутаторов и других устройств, способных сообщаться друг с другом посредством среды передачи данных.

Networking. Объединение в сеть. Соединение сетевых устройств (компьютеров, периферийного оборудования, носителей и т.д.) в единую работоспособную систему коммуникации.

Neural Network. Нейронная сеть. Компьютерная сеть, моделирующая работу человеческого мозга путем соединения большого количества относительно простых процессоров.

NFS (Network File System). Сетевая операционная система. Набор протоколов распределенной файловой системы, разработанный компанией Sun Microsystems. Предоставляет удаленный доступ к файлам посредством сети. Протоколы NFS включают протоколы RPC (Remote Procedure Call) и XDR (External Data Representation). Эти протоколы являются частью большей системы, которую компания Sun называет ONC (Open Network Computing).

NLM (NetWare Loadable Module). Загружаемый модуль NetWare. Отдельная программа, которую можно загрузить в память и выполнить в сетевой операционной системе NetWare.

NLSP (NetWare Link Services Protocol). Протокол коммуникационных услуг NetWare. Протокол маршрутизации на основе состояния каналов и метода IS-IS (Intermediate System to Intermediate System). Реализация NLSP компании Cisco включает также объекты MIB (Management Information Base) и инструменты обмена маршрутной информацией и данными SAP (Service Advertising Protocol) между NLSP и другими протоколами маршрутизации в IPX.

Node. Узел. Конец сетевого соединения либо точка объединения двух или большего количества линий сети. Узлами могут быть процессоры, контроллеры или рабочие станции. Иногда под узлом подразумевают любое сетевое устройство или программу, которая может получать доступ к сети. Термин "узел" часто означает "устройство".

NWLink. Реализация стека протоколов IPX/SPX компании Microsoft. Включена в операционные системы Windows и автоматически устанавливается при установке клиентской части Microsoft для сервера NetWare. Это позволяет клиентам Microsoft получать доступ к серверам NetWare.

O

Octet. Октет. Восемь бит. В сетевых технологиях термин "октет" (взамен байта) иногда используется потому, что в некоторых компьютерных системах термин "байт" означает не восемь, а другое количество битов.

ODI (Open Data Link Interface). Открытый канальный интерфейс. Спецификация компании Novell, обусловливающая стандартный интерфейс для сетевых адаптеров, что позволяет многим протоколам использовать один сетевой адаптер.

Ohm. Ом. Единица измерения электрического сопротивления. При напряжении 1 В по сопротивлению 1 Ом течет ток величиной в 1 А.

Operating System. Операционная система. Программа, управляющая работой компьютера и всех остальных программ. Загружается в память перед началом работы компьютера. Предоставляет приложениям различные услуги (например, пользовательский интерфейс) и работает как промежуточное звено между оборудованием компьютера и приложениями.

OSI (Open System Interconnection). Взаимодействие открытых систем. Международная программа стандартизации, созданная организациями ISO (International Standards Or-

ganization) и ITU-T (International Communications Union) для разработки и внедрения стандартов на сетевые данные, облегчающих межоперационное взаимодействие оборудования разных поставщиков.

OSI Reference Model. Модель OSI. Модель сетевой архитектуры, разработанная организациями ISO (International Standards Organization) и ITU-T (International Communications Union). Состоит из семи уровней, каждый из которых определяет такие сетевые функции, как адресация, управление потоками, контроль ошибок, инкапсуляция и надежная передача данных. Самый нижний уровень (физический) является ближайшим к носителю. Два нижних уровня реализуются аппаратно и программно, а пять верхних — только программно. Самый верхний уровень (прикладной) является ближайшим к пользователю. Модель OSI нашла всеобщее применение в процессе обучения основам сетевых технологий. Немного похожа на нее модель SNA (Systems Network Architecture).

OSPF (Open Shortest Path First). Открытый протокол SPF. Иерархический протокол маршрутизации канального уровня, призванный заменить в Internet протокол RIP (Routing Information Protocol). Средства OSPF выполняют вычисление маршрутов минимальной стоимости, многомаршрутную маршрутизацию и выравнивание нагрузки.

P

Packet Switching. Коммутация пакетов. Метод коммуникации, в котором между узлами передаются пакеты данных.

Packet. Пакет. Логически сгруппированная порция информации. Пакет состоит из заголовка, содержащего служебную информацию, и (чаще всего) пользовательских данных. Термин "пакет" используется применительно к сетевому уровню. Для описания логически сгруппированных порций информации на других уровнях модели OSI и в разных каналах коммуникации используются также термины "дейтаграмма", "кадр", "сообщение" и "сегмент".

PAP (Password Authentication Protocol). Протокол аутентификации пароля. Протокол аутентификации, позволяющий одноранговым хостам PPP (Point-to-Point Protocol) аутентифицировать друг друга. Запрос на аутентификацию передается при попытке удаленного маршрутизатора установить соединение с локальным маршрутизатором. В отличие от CHAP (Challenge Handshake Authentication Protocol), протокол PAP передает пароль, имя хоста и имя пользователя открытым текстом, т.е. в незашифрованном виде. Поэтому PAP сам по себе не предотвращает несанкционированный доступ, а лишь идентифицирует удаленный хост, после чего маршрутизатор или сервер доступа определяют, следует ли предоставить пользователю доступ. Протокол PAP поддерживается только в PPP.

Patch Panel. Коммутационная панель. Устаревшее устройство коммутации, представляющее собой набор гнезд и штырьковых разъемов, вставляемых вручную. Продолжает использоваться в некоторых офисных телефонных станциях.

Patch. Заплатка. Небольшая программа, предоставляемая поставщиком операционной системы или приложения для того, чтобы, установив ее на компьютере пользователя, исправить обнаруженные недостатки операционной системы или приложения.

PDA (Personal Digital Assistant). Цифровой персональный помощник. Переносное компьютерное устройство, используемое для хранения адресов и телефонных номеров, поддержания календаря, списка задач и т.д.

PDC (Primary Domain Controller). Первичный контроллер домена. Сервер NT в сетях Windows NT, поддерживающий главную копию базы данных SAM (Security Accounts Management) и реплицирующий ее копии "только для чтения" на каждый BDC (Backup Domain Controller).

Peer-To-Peer Computing. Одноранговая обработка. Метод обработки сетевой информации, в котором на каждом устройстве выполняются как клиентские, так и серверные части приложений. Термин означает также коммуникацию между реализациями одного и того же уровня модели OSI двух разных сетевых устройств, т.е. между уровнями одного ранга.

PGP (Pretty Good Privacy). Высокая конфиденциальность. Популярная бесплатно распространяемая программа шифрования с открытыми/закрытыми ключами. В программе используются алгоритмы шифрования RSA и DH/DSS. В последних версиях программы PGP устаревший алгоритм RSA оставлен только для совместимости с предыдущими версиями.

Physical Layer. Физический уровень. Уровень 1 модели OSI. Специфицирует электрические, механические, процедурные и функциональные условия активизации, поддержания и разрыва физического соединения систем. Приблизительно соответствует уровню физического управления модели SNA (Systems Network Architecture). *См.* OSI Reference Model.

Ping (Packet Internet Groper). Межсетевой анализатор пакетов. Утилита, предназначенная для передачи запросов и анализа ответов ICMP (Internet Control Message Protocol). Часто используется в сетях IP для проверки доступности сетевого устройства.

Point-To-Multipoint Connection. Соединение от точки к многим точкам. Один из двух фундаментальных типов соединения. В технологиях ATM (Asynchronous Transfer Mode) соединение от точки к многим точкам представляет собой однонаправленное соединение, в котором один источник (корневой узел) подключен к многим целевым системам (ветвям).

Point-To-Point Connection. Соединение от точки к точке. Один из двух фундаментальных типов соединения. В технологиях ATM соединение от точки к точке может быть как однонаправленным, так и двунаправленным.

Point-To-Point Link. Канал от точки к точке. Канал, предоставляющий один предустановленный путь коммуникации в глобальной сети от территории пользователя посредством несущей сети (например, сети телефонной компании) к удаленной сети. Называется также выделенным каналом или выделенной линией.

POP (Post Office Protocol). Протокол электронной почты. Протокол, используемый для загрузки клиентским почтовым приложением электронных сообщений с почтового сервера. Текущая версия — POP3.

Port. Порт. 1. Интерфейс в межсетевом устройстве (например, в маршрутизаторе). 2. Гнездо на коммутационной панели, в которое вставляется разъем RJ-45. 3. В терминологии IP — процесс верхнего уровня, принимающий информацию от нижнего уровня. Порты пронумерованы, причем многие номера ассоциированы с конкретными процессами. Например, SMTP (Simple Mail Transfer Protocol) ассоциирован с портом 25. Номер порта такого типа называется предустановленным адресом.

PPP (Point-to-Point Protocol). Протокол передачи данных "точка–точка". Протокол, специфицирующий соединения "маршрутизатор–маршрутизатор" и "хост–сеть" по

синхронным и асинхронным цепям. Разработан для замены протокола SLIP (Serial Line Internet Protocol).

PPTP (Point-to-Point Tunnelling Protocol). Протокол туннелирования "точка–точка". Протокол на основе PPP, предназначенный для установки виртуальных частных сетей, посредством которых пользователь может создать туннель в публичной сети, например в Internet. Таким образом пользователь получает безопасный доступ к удаленной частной сети.

Presentation Layer. Уровень представлений. Уровень 6 модели OSI. На этом уровне выполняется представление и форматирование данных и ведутся переговоры о синтаксисе передачи данных. Уровень 6 обеспечивает пригодность данных, принятых из сети, для использования приложением, а также пригодность данных, сгенерированных приложением, для передачи в сеть. *См.* OSI Reference Model.

PRI (Primary Rate Interface). Интерфейс основного уровня. Интерфейс ISDN (Integrated Services Digital Network) с основным уровнем доступа. PRI состоит из одного D-канала с пропускной способностью 64 Кбит/с и 23 B-каналов типа T1 или 30 B-каналов типа E1. При этом по D-каналам передаются служебные сигналы, а по B-каналам — голос или данные.

Private Key Encryption. Шифр с секретным ключом. Метод шифрования, в котором один и тот же ключ используется как для шифрования, так и для дешифрования данных. Другое название — симметричный шифр.

Protocol Stack. Стек протоколов. Набор взаимосвязанных протоколов коммуникации, работающих вместе и (как единая группа) специфицирующих коммуникацию на некоторых или на всех семи уровнях модели OSI. Все уровни модели покрывает не каждый протокол стека, однако часто один протокол относится к нескольким уровням. Характерным примером стека протоколов является TCP/IP.

Protocol Suite. Набор протоколов. Набор взаимосвязанных протоколов коммуникации, включающий дополнительные утилиты и другие протоколы, не обязательные для коммуникации. *См.* Protocol Stack.

Protocol. Протокол. Набор правил и соглашений, специфицирующих обмен информацией между сетевыми устройствами.

Proxy. Прокси. Устройство или программа, взаимодействующая с другим устройством или программой для поддержания эффективной работы сети.

PSTN (Public Switched Telephone Network). Коммутируемая телефонная сеть общего пользования. Традиционная аналоговая телефонная сеть. В США иногда применяется ее другое название — POTS (Plain Old Telephone Service — простая старая телефонная служба).

Public Key Encryption. Шифр с открытым ключом. Метод шифрования, в котором используются два ключа: открытый для шифрования данных и закрытый для их дешифрования. Другие названия — шифр с открытым/закрытым ключами, асимметричный шифр.

PVC (Permanent Virtual Circuit). Постоянный виртуальный канал. Виртуальный канал, установленный на длительное время. Использование постоянных виртуальных каналов экономит пропускную способность сети в ситуациях, когда канал должен существовать длительное время, поскольку при частых установках и разрывах каналы загружаются дополнительными служебными сигналами.

Q

QoS (Quality of Service). Качество обслуживания. Показатель производительности передающей системы, отражающий качество и доступность предоставляемой услуги.

Quantum Physics. Квантовая физика. Отрасль физики, изучающая законы взаимодействия элементарных частиц — электронов и протонов. Неделимые порции энергии, которыми обмениваются элементарные частицы, называются квантами.

Qubit. Q-бит. Квантовый бит.

Queue. Очередь. 1. Упорядоченный список элементов, ожидающих обработки. 2. В технологиях маршрутизации — набор пакетов, ожидающих продвижения на интерфейс маршрутизатора.

R

RADIUS (Remote Authentication Dial-In User Service). Служба удаленной аутентификации коммутируемого пользователя. Сетевая служба, обеспечивающая безопасную коммуникацию между удаленными клиентами и серверами.

RAID (Redundant Array of Independent Disks). Избыточный набор независимых дисков. Метод повышения отказоустойчивости, в котором для восстановления данных после краха одного из дисков информация хранится на многих дисках в различной конфигурации.

RAM (Random Access Memory). Память с произвольным доступом. Устройство компьютера, в котором хранятся данные, считываемые и записываемые микропроцессором. Другое название — оперативная память или просто память.

RARP (Reverse Address Resolution Protocol). Протокол определения сетевого адреса по местоположению узла. Один из протоколов стека TCP/IP, предоставляющий метод вычисления IP-адреса исходя из MAC-адреса.

RAS (Remote Access Service). Служба удаленного доступа. Сетевая служба, предоставляющая клиентским компьютерам возможность пройти процедуру аутентификации и установить коммутируемое соединение или соединение VPN (Virtual Private Network) с удаленным сервером. *См.* Remote Access.

Reassembling. Повторная сборка. Сборка на принимающем узле дейтаграммы IP из частей, на которые она была разобрана на передающем или промежуточном узле. Другое название этого процесса — дефрагментация.

Redirector. Редиректор. Программа, перехватывающая запросы на услуги или к ресурсам и определяющая, куда следует направить запрос.

Redundancy. Избыточность. 1. В сетевых технологиях — дублирование устройств, служб или соединений для того, чтобы при крахе одного из них нормальная работа сети не нарушилась. 2. Часть сообщения, которую можно устранить без потери информации. Вводится для повышения надежности связи: в случае порчи части передаваемых данных сообщение полностью восстанавливается на принимающем узле.

Registry. Реестр. В операционной системе Windows — иерархическая база данных, в которой хранится информация об инициализации приложений.

Remote Access. Удаленный доступ. Сетевое соединение между клиентом и сервером, установленное посредством телефонной линии, выделенного соединения или туннеля VPN (Virtual Private Network) в Internet.

Repeater. Повторитель. Устройство, регенерирующее электрические сигналы и передающее их в другой сегмент сети.

RFC (Request for Comments). Запросы на комментарии. Серия документов, служащих первоисточниками технической информации по Internet. Многие документы RFC утверждены организацией IAB (Internet Activities Board) как стандарты Internet. Большинство RFC документируют спецификации протоколов, например Telnet или FTP (File Transfer Protocol), однако среди них встречаются также носящие юмористический или исторический характер. Документы RFC доступны Web.

RFI (Radio Frequency Interference). Радиочастотные помехи. Помехи на радиоволновых частотах, нарушающие нормальную передачу данных по медным кабелям. Генерируются различными радиотехническими и электротехническими устройствами.

Ring Topology. Кольцевая топология. Сетевая топология, в которой сеть состоит из последовательности повторителей, соединенных один с другим, причем последний соединен с первым. Таким образом создается однонаправленный канал передачи данных в форме кольца. Каждая станция подключена к сети посредством повторителя. Однако несмотря на логически замкнутое кольцо, физически топология является звездообразной.

Ring. Кольцо. Две или более станции, объединенные в логически кольцевую топологию. Информация передается последовательно между активными станциями. На основе кольцевой топологии построены сети Token Ring, FDDI и CDDI (Copper Distributed Data Interface).

RIP (Routing Information Protocol). Протокол маршрутной информации. Протокол, поставляемый с системами UNIX DSD (Berkeley Software Distribution). Является наиболее распространенным протоколом набора IGP (Interior Gateway Protocol) в Internet. В качестве метрики маршрутизации (показателя качества маршрута) в RIP используется количество ретрансляций.

RJ (Registered Jack) Connector. Стандартный разъем RJ. Модульный разъем, используемый для присоединения медных кабелей. В аналоговых телефонных линиях обычно используется разъем RJ-11, а для неэкранированных витых пар Ethernet — разъем RJ-45.

ROM (Real-Only Memory). Память только для чтения. Энергонезависимая память, из которой микропроцессор может только читать данные, но не записывать.

Routed Protocol. Маршрутизируемый протокол. Протокол, пакеты которого можно маршрутизировать. Примерами маршрутизируемых протоколов являются AppleTalk, DECnet и IP.

Router. Маршрутизатор. Устройство сетевого уровня модели OSI, использующее какую-либо метрику (показатель качества маршрута) для выбора оптимального пути передачи сетевой нагрузки. Маршрутизаторы продвигают (передают) пакеты из одной сети в другую на основе информации сетевого уровня. Иногда их называют шлюзами, однако такое определение быстро устаревает.

Routing Protocol. Протокол маршрутизации. Протокол, выполняющий маршрутизацию пакетов по сети. Примеры маршрутизирующих протоколов — IGRP, OSPF и RIP.

Routing Table. Таблица маршрутов. Таблица маршрутной информации, хранящаяся на маршрутизаторе или другом межсетевом устройстве. В маршрутной таблице хранятся и постоянно обновляются маршруты к отдельным сетевым узлам и, в некоторых случаях, метрики этих маршрутов.

Routing. Маршрутизация. Процесс выбора пути к целевому хосту. В больших сетях задача маршрутизации чрезвычайно сложна вследствие большого количества вариантов маршрута и промежуточных узлов, которые пакет должен пройти на пути к целевому хосту.

RPC (Remote-Procedure Call). Вызов удаленной процедуры. Фундаментальное понятие систем клиент/сервер. Вызов RPC означает выполнение на сервере процедуры, созданной или определенной клиентом, с последующим возвращением результатов клиенту посредством сети.

S

SAM (Security Accounts Database). База данных учетных записей. В операционных системах Windows NT — база данных, в которой хранится информация об учетных записях пользователей, группах и ассоциированных с ними правах доступа.

Samba. Пакет программ, позволяющий компьютерам Windows и UNIX сообщаться друг с другом на основе протокола разделения файлов SMB (Server Message Block).

SAP (Service Advertising Protocol). Протокол извещения об услугах. Протокол набора IPX, информирующий сетевых клиентов (с помощью маршрутизаторов и серверов) о доступных сетевых ресурсах и услугах.

Scalability. Масштабируемость. Свойство сети, состоящее в возможности ее наращивания без радикальных изменений общей логической или физической структуры.

SDLC (Synchronous Data Link Control). Синхронное управление передачей данных. Коммуникационный протокол канального уровня SNA (Systems Network Architecture). Протокол SDLC является дуплексным ориентированным на биты последовательным протоколом, управляющим многими аналогичными протоколами, включая HDLC и LAPB.

Segment. Сегмент. 1. Часть сети, ограниченная мостами, маршрутизаторами или концентраторами. 2. В локальной сети на основе шинной топологии — непрерывная электрическая цепь, часто подключенная к другим сегментам с помощью повторителей. 3. В спецификациях TCP — порция информации транспортного уровня. Для описания логического группирования информации на разных уровнях модели OSI и в разных коммуникационных каналах используются также термины "дейтаграмма", "кадр", "сообщение" и "пакет".

Segmentation. Сегментация. Разбивка одного домена коллизий на два или более для уменьшения количества коллизий и перегрузки сети.

Serial Transmission. Последовательная передача. Метод передачи данных, в котором биты символов данных передаются последовательно по одному каналу.

Server. Сервер. Узел или программа, предоставляющая услуги клиентам. *См.* Client.

Session Layer. Сеансовый уровень. Уровень 5 модели OSI. На этом уровне устанавливается и поддерживается сеанс связи между приложениями, а также происходит управление этим сеансом. *См.* OSI Reference Model.

Session. Сеанс. 1. Связанный набор ориентированных на соединение коммуникационных транзакций между двумя или более сетевыми устройствами. 2. В системе SNA (Systems Network Architecture) — логическое соединение, обеспечивающее коммуникацию двух адресуемых сетевых модулей.

SHA1 (Secure Hash Algorithm). Безопасный алгоритм хэширования. Алгоритм одностороннего хэширования с 160-битовым дайджестом, разработанный организацией NIST (National Institute of Standards and Technology).

Share. Разделяемый, совместно используемый ресурс. Ресурс компьютера, доступный для других сетевых компьютеров.

Share-Level Security. Безопасность на уровне ресурсов. Метод управления доступом к сетевым ресурсам, основанный на присвоении отдельных паролей каждому ресурсу.

Simplex. Симплексная связь. Метод коммуникации, в котором информация может проходить между передающей и принимающей станциями только в одном направлении. Примером симплексной связи является традиционное телевидение.

Single-Vendor Network. Сеть одного поставщика. Сеть, в которой используется оборудование только одного поставщика. В таких сетях проблемы совместимости возникают довольно редко.

Sliding Window. Скользящее окно. Окно, размеры и расположение которого динамически изменяются на протяжении сеанса TCP.

SLIP (Serial Line Internet Protocol). Межсетевой протокол для последовательного канала. Стандартный протокол для последовательных соединений "точка–точка" на основе одного из вариантов TCP/IP. Протокол SLIP является предшественником PPP.

Smart Card. Интеллектуальная карта. В технологиях компьютерной безопасности — пластмассовая карточка, размеры которой совпадают с размерами кредитной карточки, содержащая регистрационную информацию во встроенной в нее микросхеме или на магнитной полоске. Применяется для регистрации и получения доступа к системе. Может использоваться как вместо ввода имени учетной записи и пароля с помощью клавиатуры, так и совместно с ним.

Smart Technology. Технология интеллектуальных устройств. Встраивание небольших микропроцессорных систем в домашние приборы, офисное оборудование и т.д. Это позволяет запрограммировать интеллектуальные устройства на выполнение определенных задач и на коммуникацию друг с другом и с владельцем устройства посредством сети.

SMTP (Simple Mail Transfer Protocol). Простой протокол электронной почты. Протокол, используемый для передачи электронных сообщений по Internet.

SNA (Systems Network Architecture). Системная сетевая архитектура. Сложная многофункциональная архитектура, разработанная в 1970-х годах компанией IBM. Во многом похожа на модель OSI и многим отличается от нее. Как и модель OSI, состоит из семи уровней.

SNMP (Simple Network Management Protocol). Простой протокол сетевого управления. Протокол управления сетью, используемый почти исключительно в сетях TCP/IP. Протокол SNMP предоставляет средства мониторинга и управления сетевыми устройствами, а также управления производительностью и средства конфигурирования, обеспечения безопасности и сбора статистической информации.

Socket Number. Номер сокета. Восьмибитовый номер, идентифицирующий сокет. В узле AppleTalk может быть присвоено до 254 номеров сокетов.

Socket. Сокет. 1. Программная структура в сетевом устройстве, работающая как конечная точка коммуникации (аналогично порту). 2. Адресуемая сущность внутри узла, подключенного к сети AppleTalk. Сокеты принадлежат программным клиентам, называемым кли-

ентами сокета. Сокеты AppleTalk делятся на две группы: SAS (зарезервированные для таких клиентов, как протокол ядра AppleTalk) и DAS (динамически присваиваемые процедурами DDP (Distributed Data Processing) по запросу от клиентов в узле). Сокеты в AppleTalk аналогичны концепции порта в TCP/IP.

SOHO (Small Office/Home Office). Небольшой офис/дом. Небольшой офис или жилой дом с несколькими пользователями, которым нужно более быстрое и надежное соединение, чем коммутируемая аналоговая линия.

Solaris. Операционная система на основе UNIX, разработанная компанией Sun Microsystems.

Source Address. Адрес источника. Адрес сетевого устройства, передающего данные. *См.* Destination Address.

Spanning Tree. Связующее дерево. Нециклическая часть сетевой топологии.

Spanning-Tree Algorithm. Алгоритм построения связующего дерева. Алгоритм, используемый в Spanning-Tree Protocol (протокол связующего дерева) для создания связующего дерева. Иногда его обозначают как STA.

Spanning-Tree Protocol. Протокол связующего дерева. Протокол моста, реализующий алгоритм связующего дерева. С его помощью мост динамически настраивает свою работу таким образом, чтобы обходить циклы в сетевой топологии путем создания связующего дерева. Для обнаружения циклов мосты обмениваются между собой сообщениями BDPU, а затем устраняют циклы, закрывая определенные интерфейсы мостов. Стандарт протокола связующего дерева описан в IEEE 802.1. Протокол связующего дерева основан на более раннем протоколе компании Digital Equipment Corporation. Версия IEEE этого протокола поддерживает мостовые домены и позволяет мостам создавать связующие деревья в расширенной локальной сети. По сравнению с версией Digital версия IEEE является предпочтительной.

SPID (Service Profile Identifier). Идентификатор услуги и линии. Номер, используемый некоторыми провайдерами услуг для идентификации услуги, на которую подписано пользовательское устройство ISDN (Integrated Services Digital Network). Устройство ISDN использует SPID при доступе к коммутатору, инициализирующему соединение с провайдером услуг.

Split Horizon. Расщепление горизонта. Метод, используемый протоколом IGRP (Internet Gateway Routing Protocol) для предотвращения выбора неверного маршрута. Расщепление горизонта предотвращает образование циклов между прилегающими маршрутизаторами и уменьшает количество обновляющих сообщений.

Spoofing. Подмена, спуфинг. Метод, используемый маршрутизаторами для того, чтобы заставить хост рассматривать интерфейс как подключенный и поддерживающий сеанс связи. Маршрутизатор подделывает ответы на служебные запросы хоста и "убеждает" его, что сеанс все еще существует. Применение спуфинга весьма полезно в такой среде маршрутизации, как DDR, в которой при отсутствии сообщений каналы с коммутируемыми цепями отключаются для уменьшения затрат. Термин "спуфинг" может обозначать также спуфинг IP.

SPX (Sequenced Packet Exchange). Последовательный обмен пакетами. Надежный протокол, ориентированный на установку соединений и дополняющий услуги обработки дейтаграмм, предоставленные протоколами сетевого уровня. Компания Novell создала

этот распространенный в сетях NetWare протокол транспортного уровня на основе протокола SPP набора протоколов XNS (Xerox Network Standard).

SQL (Structured Query Language). Язык структурированных запросов. Язык программирования, предназначенный для взаимодействия с базами данных. Является стандартом, утвержденным организациями ANSI и ISO. Термином SQL часто обозначают версию языка, используемую в системе типа клиент/сервер управления базами данных Microsoft SQL Server.

Standard. Стандарт. Набор официально утвержденных и широко используемых правил и процедур.

Star Topology. Звездообразная топология. Топология локальной сети, в которой хосты соединены с общим центральным коммутатором отдельными линиями типа "точка–точка".

Static Routing. Статическая маршрутизация. Метод маршрутизации, в котором маршруты явно сконфигурированы и введены в таблицу маршрутов. Был разработан и применялся раньше метода динамической маршрутизации.

Store-And-Forward. С промежуточным хранением. Технология коммутации пакетов, в которой кадры, прежде чем быть переданными в соответствующий порт, основательно обрабатываются. Обработка включает вычисление кода CRC (Cyclic Redundancy Check) и проверку целевого адреса. Кроме того, кадры временно хранятся, пока не станут доступны необходимые для их продвижения сетевые ресурсы (например, свободные каналы).

STP (Shielded Twisted-Pair). Экранированная витая пара. Пара медных проводников, используемая в качестве носителя в различных сетевых архитектурах. Провода экранированной витой пары для защиты от электромагнитных помех окружены защитным металлическим слоем — экраном.

Subnet Address. Адрес подсети. Часть IP-адреса, определяющая подсеть. Вычисление подсети выполняется путем наложения маски подсети.

Subnet Mask. Маска подсети. Маска, используемая для извлечения номеров сети и подсети из IP-адреса.

Subnet. Подсеть. 1. Один из небольших сегментов большой сети. 2. В сетях IP — часть сети, хосты которой имеют общий адрес подсети. Сеть сегментируется на подсети сетевым администратором для создания многоуровневой иерархической структуры маршрутизации и защиты сети от сложной адресации присоединенных сетей. 3. В модели OSI — набор ES и IS под управлением одного административного домена и с использованием одного сетевого протокола.

Surge. Скачок. Резкое увеличение напряжения электропитания — более 110% нормального напряжения в электросети.

SVC (Switched Virtual Circuit). Коммутируемый виртуальный канал. Виртуальный канал, устанавливаемый динамически по требованию и разрываемый при завершении передачи данных. Каналы SVC используются в ситуациях, когда передача данных происходит нерегулярно. *См.* PVC.

Switch. Коммутатор. Сетевое устройство, фильтрующее и передающее кадры на основе целевых адресов каждого кадра. Коммутаторы работают на канальном уровне модели OSI.

Switched Virtual Circuit. *См.* SVC.

Switching. Коммутация. Чтение кадра с одного интерфейса и передача его на другой интерфейс.

Synchronous Circuit. Синхронный канал. Канал, в котором сигналы передаются точно синхронизированными во времени. Такие сигналы передаются с одной и той же частотой, причем каждая порция сигналов предопределенной длины окружена стартовым и концевым управляющими битами, используемыми для синхронизации передатчика и приемника и отмечающими начало и конец порции.

T

T1. Цифровое оборудование глобальной сети, используемое для передачи данных в формате DS-1 со скоростью 1,544 Мбит/с по коммутируемым телефонным сетям с помощью кодов AMI и B8ZS.

T3. Цифровое оборудование глобальной сети, используемое для передачи данных в формате DS-3 со скоростью 44,736 Мбит/с по коммутируемым телефонным сетям.

TA (Terminal Adapter). Терминальный адаптер. Устройство, используемое для подключения ISDN BRI к одному из существующих интерфейсов, например к EIA/TIA-232. Иногда его не совсем точно называют модемом ISDN.

TCP (Transmission Control Protocol). Протокол управления передачей. Протокол транспортного уровня, ориентированный на установление соединения. Предназначен для надежной дуплексной передачи данных. Входит в стек протоколов TCP/IP.

TCP/IP (Transmission Control Protocol/Internet Protocol). Протокол управления передачей/протокол Internet. Набор протоколов, разработанный Министерством обороны США в 1970-х годах для создания всемирной сети сетей. Наиболее популярные протоколы набора — TCP и IP.

TDM (Time-Division Multiplexing). Мультиплексирование с разделением времени. Метод мультиплексирования, в котором по одной линии передаются одновременно разные сигналы. В этом методе время разделено на небольшие интервалы, каждый из которых отведен для определенного сигнала.

TDR (Time Domain Reflectometer). Рефлектометр временных интервалов. Устройство проверки кабелей, передающее в кабель тестирующие импульсы и определяющее время их возвращения. Используется для точного определения места разрыва или короткого замыкания кабеля.

Telephony. Телефония. Коммуникационная технология, объединяющая телекоммуникационную и компьютерную технологии.

Telnet. Стандартный протокол эмуляции терминала, входящий в стек TCP/IP. Протокол Telnet используется для установки удаленного терминального соединения, позволяющего пользователям регистрироваться в удаленной системе и получать доступ к ее ресурсам таким образом, будто это соединение с локальной системой. Определяется в документе RFC 854.

Terabyte. Терабайт. Единица измерения количества информации, равная 10^{12}, или 1 000 000 000 000 байт.

Terminator. Терминатор. Устройство, подключаемое к концу коаксиального кабеля для предотвращения отражения сигналов.

TFTP (Trivial File Transfer Protocol). Простейший протокол передачи файлов. Упрощенная версия FTP (File Transfer Protocol), используемая для передачи файлов по сети с одного компьютера на другой.

Thin Client. Тонкий клиент. Малопроизводительный компьютер, на котором выполняется простое программное обеспечение. Позволяет пользователю подключаться к серверу, получать доступ к рабочему столу и выполнять на сервере приложения, причем все вычисления выполняются на сервере, а не на клиентском компьютере.

Throughput. Пропускная способность. Показатель производительности канала, равный количеству информации, которое можно передать по каналу в единицу времени.

Timeout. Блокировка по времени. Событие, происходящее по истечении времени ожидания сетевым устройством сообщения от другого сетевого устройства. Обычно при этом первое сетевое устройство передает информацию повторно или разрывает сеанс связи.

Token. Маркер. Кадр, содержащий управляющую информацию. Получив маркер, сетевое устройство начинает передавать данные в сеть.

Token Bus. Эстафетная магистраль. Магистраль локальной сетевой архитектуры в шинной топологии на основе передачи маркера. Такая архитектура специфицирована документом IEEE 802.4.

Token Passing. Передача маркера. Метод доступа, в котором сетевые устройства получают доступ к физическому носителю при получении небольшого кадра, называемого маркером.

Token Ring. Локальная сетевая архитектура на основе передачи маркера, разработанная и поддерживаемая компанией IBM. При использовании кольцеобразной топологии пропускная способность составляет 4 или 16 Мбит/с.

TokenTalk. Программный продукт компании Apple Computer, работающий на канальном уровне и позволяющий использовать в сетях AppleTalk кабели Token Ring.

Tone Generator and Locator. Тональный генератор и локатор. Набор устройств, предназначенных для проверки неэкранированных витых пар путем подачи в провод тестирующего сигнала. Иногда эти устройства называют "лисой и собакой".

Topology. Топология. Физическая конфигурация сетевых узлов и носителей в структуре корпоративной сети.

Traceroute. Программа, использующаяся во многих системах (однако называться в них она может по-разному) для отслеживания пути пакета от передающего к принимающему компьютеру. Используется главным образом для устранения маршрутных неполадок между хостами. Существует также протокол отслеживания пути пакета, определяемый документом RFC 1393.

Tracert. *См.* traceroute.

Trailer. Трейлер. Служебная информация, присоединяемая к данным в процессе их инкапсуляции для передачи в сеть.

Transceiver. Трансивер. Часть сетевого интерфейса, предназначенная для приема и передачи сигналов. Некоторые сетевые адаптеры содержат встроенный трансивер, в других сетевых интерфейсах используется внешний трансивер.

Transport Layer. Транспортный уровень. Уровень 4 модели OSI. Сегментирует и собирает данные обратно в поток данных. На транспортном уровне действуют механизмы гарантированного соединения и надежной передачи данных. *См.* OSI Reference Model.

Trap. Прерывание. Сообщение, передаваемое агентом SNMP (Simple Network Management Protocol) на NMS, консоль или терминал при наступлении важного со-

бытия, например выполнении предопределенного условия или достижении порогового значения какого-либо показателя.

Tree Topology. Древовидная топология. Топология локальной сети, похожая на шинную, за тем исключением, что древовидная сеть может содержать ветви с многими узлами. Сигналы с одной станции передаются по всему носителю и принимаются всеми другими станциями.

Triple DES. *См.* 3DES.

Troubleshooting. Устранение неполадок. Процесс обнаружения, анализа, диагностирования и устранения проблем, возникающих при работе компьютера или сети.

TTL (Time To Live). Время жизни. Поле в заголовке IP, определяющее, как долго пакет следует полагать правильным.

Tunneling. Туннелирование. Создание в публичной сети туннеля виртуальной частной сети.

U

UDP (User Datagram Protocol). Протокол пользовательских дейтаграмм. Не ориентированный на установку соединения протокол транспортного уровня, входящий в стек TCP/IP. Это простой протокол, предназначенный для обмена дейтаграммами без подтверждения или гарантии доставки. При его использовании обработка ошибок и повторная передача должны выполняться другими протоколами. Определяется в документе RFC 768.

Unicast Address. Одиночный адрес. Адрес, определяющий единственное сетевое устройство.

Unicast. Одноадресная передача. Передача сообщений по единственному сетевому адресу.

UNIX. Мощная текстовая операционная система, разработанная в лаборатории компании Bell в 1969 году как интерактивная система с разделением времени. Со временем развилась в популярную открытую операционную систему. Часто используется на серверах в больших коммерческих сетях.

UPS (Uninterruptible Power Supply). Устройство бесперебойного электропитания. Резервное устройство электропитания, на которое автоматически переключается сетевое оборудование при отказе электросети. Устройства UPS обычно устанавливаются для файловых серверов и концентраторов.

URL (Uniform Resource Locator). Унифицированный указатель ресурса. Стандартизированная схема адресации, используемая для получения доступа к гипертекстовым документам и службам с помощью броузера.

USB (Universal Serial Bus). Универсальная последовательная шина. Интерфейс между компьютером и периферийным оборудованием, поддерживающий технологию Plug and Play и скорость передачи данных 12 Мбит/с.

User-Level Security. Безопасность не уровне пользователей. Метод обеспечения безопасности сетевых ресурсов, в котором каждому пользователю присваивается учетная запись, содержащая его права доступа ко всем необходимым ему сетевым ресурсам.

UTP (Unshielded Twisted-Pair). Неэкранированная витая пара. Скрученная пара медных проводов, используемая в разных сетевых архитектурах. Для неэкранированной витой пары не нужно, чтобы между устройствами было фиксированное расстояние, как для коаксиального кабеля. Широко используются пять типов неэкранированной витой пары: категории 1–5.

V

Virtual Circuit. Виртуальный канал. Логическая цепь, созданная для обеспечения надежной коммуникации между двумя сетевыми устройствами. Виртуальный канал определяется как пара VPI/VCI и может быть как постоянным (Permanent Virtual Circuit — PVC), так и временным (Switched Virtual Circuit — SVC). Виртуальные каналы используются в технологиях Frame Relay, X.25 и ATM (Asynchronous Transfer Mode).

VINES (Virtual Integrated Network Service). Виртуальная сетевая операционная система. Сетевая операционная система, разработанная и поставляемая компанией Banyan Systems.

Virus. Вирус. Программа, способная к саморазмножению. Создается со злым умыслом для повреждения других программ и файлов.

VLAN (Virtual LAN). Виртуальная локальная сеть. Группа устройств локальной сети, сконфигурированных (с помощью программ управления) на такой режим коммуникации, будто они подключены к одному кабелю, хотя фактически они могут быть расположены в разных сегментах локальной сети. Поскольку VLAN основаны на логических, а не на физических соединениях, они обладают чрезвычайно высокой гибкостью.

VoIP (Voice over IP). Передачи речи по сети IP. Метод передачи звуковых данных по локальной или глобальной сети либо по Internet с помощью пакетов IP. Называется также протоколом VoIP.

Volume. Том. Раздел жесткого диска.

VPN (Virtual Private Network). Виртуальная частная сеть. Соединение между удаленным клиентом и частной сетью (например, локальной сетью компании), в котором в качестве носителя используется публичная сеть Internet. Сеть VPN создается с помощью протоколов туннелирования и шифрования, что позволяет безопасно передавать данные по публичной сети.

W

WAN (Wide Area Network). Глобальная сеть. Компьютерная сеть, обслуживающая пользователей, находящихся в разных географических регионах, возможно, даже на разных континентах. В качестве носителей в глобальных сетях часто используются общедоступные каналы коммуникации, например телефонная сеть. Примерами технологий глобальных сетей являются Frame Relay, SMDS и X.25.

WAN Link. Канал глобальной сети. Канал коммуникации, соединяющий пользователей глобальной сети и состоящий из маршрутов передачи данных и работающего в них оборудования.

Waveform Signaling. Аналоговые сигналы. Сигналы, представляющие собой непрерывно изменяющуюся во времени физическую величину, например напряжение в кабеле. Количество состояний аналогового сигнала бесконечно.

Web Server. Web-сервер. Сервер, на котором хранятся документы Web. Пользователи получают доступ к документам Web с помощью специальной программы, называемой Web-броузером, работающей с протоколом HTTP (Hypertext Transfer Protocol).

Windows. Семейство популярных операционных систем, разработанных и поставляемых компанией Microsoft. Пользователи работают с системой с помощью удобного

интерфейса GUI. Операционная система позволяет выполнять многие приложения одновременно, причем каждое в своем окне. К семейству Windows принадлежат операционные системы Windows 1.*x*/2.*x*/3.*x*, Windows 95/98/ME, Windows NT/2000/XP.

WINS (Windows Internet Name Server). Служба имен Internet для Windows. Разработанный компанией Microsoft сервер имен NetBIOS, разрешающий имена NetBIOS на IP-адреса в сетях Microsoft.

Winsock (Windows Sockets). Сокеты Windows. Прикладной интерфейс программирования, используемый для обработки входных и выходных запросов для приложений Internet на компьютерах с операционными системами Windows.

Workgroup Server. Сервер рабочей группы. Сервер, обслуживающий определенный набор пользователей и предоставляющий услуги, например, обработки текстовых документов или разделения файлов, т.е. необходимые только некоторым членам группы.

Workgroup. Рабочая группа. Группа компьютеров и сетевых устройств, разделяющих ресурсы друг друга.

Worm. Червь. Вирус, способный размножаться по сети.

X

X Window. Графический пользовательский интерфейс операционных систем UNIX и Linux.

X.25. Стандарт организации ITU-T (International Telecommunication Union), специфицирующий соединения DTE (Data Terminal Equipment) и DCE (Data Communications Equipment), используемые для удаленного терминального доступа и коммуникации компьютеров в публичных сетях. К настоящему времени Frame Relay в значительной степени вытеснил X.25.

X.500. Набор стандартов распределенной службы каталогов, использующей DAP (Data Access Protocol).

XNS (Xerox Network Systems). Сетевой стандарт Xerox. Набор протоколов, первоначально разработанный в исследовательском центре в Пало-Альто. Многие компании (такие разработчики и поставщики программного обеспечения, как 3Com, Banyan, Novell и UB Networks) используют вариации XNS в качестве своего первичного транспортного протокола.

Z

Zone. Зона. Логическая группа сетевых устройств в архитектуре AppleTalk. Функционально зона аналогична домену или рабочей группе в сетях Microsoft. В базе данных DNS (Domain Name System) термин "зона" означает поддерево DNS, администрируемое как единая отдельная сущность.

Предметный указатель

A

ACPI (Advanced System Configuration and Power Interface), 367
Active Directory, 68; 305; 329
Adobe Pagemill, 262
ADSL (Asymmetric DSL), 173
AH (Authentication Header), 414
AltaVista, 266
Amaya, 263
AOL/Netscape Instant Messenger, 276
API (Application Programming Interface), 340
APIPA, 231
APM (Advanced Power Management), 367
AppleShare, 83
AppleShareIP, 316
AppleTalk, 71; 83; 153
Applshare, 375
APPN (Advanced Peer-to-Peer Networking), 393
ARCnet, 84; 155
ARPAnet, 31
AS/400, 393
Ask Jeeves, 267
ASP (Application Service Provider), 506
ATM (Asynchronous Transfer Mode), 177

B

Banyan VINES, 316
BAP (Bandwidth Allocation Protocol), 449
BDC (Backup Domain Controller), 304
BIND (Berkley Internet Name Domain), 240
Bindery, 309; 328
Blowfish, 483
BOOTP, 499
BOOTP-сервер, 62
BRI (Basic Rate ISDN), 172

C

CAP (Columbia AppleTalk Package), 388
Cat 1–5, 80
Cat 5e (Enhanced), 80
Cat 6 и 7, 80
CATV, 179
CCNA (Cisco Certified Network Associate), 47
CCNE (Cisco Certified Network Expert), 47
CCNP (Cisco Certified Network Professional), 47
CHAP (Challenge Handshake Authentication Protocol), 448
CIDR (Classless Interdomain Routing), 228
Client Services for NetWare (CSNW), 69; 387
CMIP (Common Management Information Protocol), 528
CNA (Novell Certified NetWare Administrator), 47
CNE (Novell Certified NetWare Engineer), 47
CompTIA, 47
config, 536
ConfigPPP, 376
Corel Linux, 312
CRC, 144
CSMA/CD, 128; 138
CSNW (Client Services for NetWare), 366
CSU/DSU (Channel Service Unit/Data Service Unit), 458
CSU/DSU (Channel Service Unit/Digital Service Unit), 167
CUseeMe, 276
cXML (Commerce XML), 478

D

DAP (Directory Access Protocol), 321
DDS (Digital Data Service), 174
Debian GNU/Linux, 313
Defense Data Network, 31
DES (Data Encryption
Standard), 418; 472
DHCP (Dynamic Host Configuration Protocol), 229
DHCP-сервер, 62
DIB (Directory Information Base), 326
DirectHit, 266
DN (Distinguished Name), 327
DNS (Domain Name System), 103; 324
DoS (Denial of Service), 406
DOSSHELL, 340
DSA (Directory System Agent), 326
DSL, 173
DSL (Digital Subscriber Line), 450
DUA (Directory User Agent), 326
DWDM (Dense Wavelength Division Multiplexing), 121

E

EAP (Extensible Authentication Protocol), 448
EFS (Encrypting File System), 352
EISA (Extended ISA), 195
Emac/W3, 263
Emacs, 313
ESP (Encapsulating Security Payloads), 414
Ethernet, 78; 137
EtherTalk, 71
Eudora, 270
Event Viewer, 532
Excite, 266

F

Fast Ethernet, 78; 142
FAT (File Allocation Table), 349
FCS (Frame Check Sequence), 150
FDDI (Fiber Distributed Data Interface), 151
FDM (Frequency Division Method), 121
FPNW (File and Print Service for NetWare), 391
Frame Relay, 177
FTP (File Transfer Protocol), 100; 248

G

Gateway Services for NetWare (GSNW), 69; 387
Gigabit Ethernet, 78; 81; 142
Gigabit Sniffer Pro, 522
Glassbook Reader for PC, 560
Google, 266
GPS (Global Positioning System), 42; 548
GSNW (Gateway Services for Netware), 101
GTE Cybertrust, 421
GUI (Graphical User Interface), 340

H

H.323, 276
HDSL (High Data Rate DSL), 173
Host Integration Server, 393
HPFS (High Performance File System), 349
HTML, 261
HTTP (Hypertext Transfer Protocol), 248

I

IAB, 286
IANA/ICANN, 286
ICA (Independent Computing Architecture), 498
IDSL, 173
IEC (International Electrotechnical Commission), 111
IEEE (Institute of Electrical and Electronics Engineers), 112
IEEE 802.3, 78; 138
IESG, 286
IETF, 286
IETF (Internet Engineering Task Force), 111
ifconfig, 537

IKE (Internet Key Exchange), 472
IMAP (Internet Message Access Protocol), 269
Infotainment, 554
Internet, 253
Internet Explorer, 264
Internet2, 255
Internet-телефония, 277
ipconfig, 537
IPing AH (Authentication Header), 549
IPing ESH (Encapsulation Security Header), 549
IPP (Internet Printing Protocol), 368
IPSec (IP Security), 367; 472
IPv4, 549
IPv6, 549
IPX/SPX, 70
IP-адрес, 104; 223
IP-маскирование, 184
IRC, 275
IrDA (Infrared Data Association), 205
ISA (Industry Standard Architecture), 194
ISDN (Integrated Services Digital Network), 172; 456
ISO (International Standardization Organization), 110
ISOC, 285
ITU (International Telecommunications Union), 111
i-узел, 353

J

Java, 506

K

KDE, 340
Kerberos, 421
Keywitness, 421

L

L2F (Layer 2 Forwarding), 472
L2TP (Layer 2 Tunneling Protocol), 367; 448
LANalyzer, 522
LANtastic, 316
LDAP (Lightweight Directory Access Protocol), 321
LDAPv3, 326
Linux, 311; 372
Linux Service for Macintosh, 388
LLC (Logical Link Control), 104
LOAF (Linux On A Floppy), 313
Local Area Network (LAN), 53
LocalTalk, 71; 83; 153; 375
LU (Logical Unit), 392
Lycos, 266
Lynx, 263; 374

M

MAC (Media Access Control), 104
Macintosh, 375
Macintosh HFS (Hierarchical File System), 349
Macromedia Dreamweaver, 262
MAC-адрес, 104
ManageWise, 525
MCA (Micro Channel Architecture), 195
MCP (Microsoft Certified Professional), 47
MCSE (Microsoft Certified Systems Engineer), 47
MD5 (Message Digest 5), 472
MD5 (Message Diggest 5), 421
MetaCrawler, 267
MetaFrame, 498; 504
Metropolitan Area Network (MAN), 53
Microsoft
  .NET, 507
  Client for NetWare Networks, 387
  FrontPage, 262
  MSN Messenger, 276
  NetMeeting, 276
  Outlook Express, 270
  Reader, 560
  Services for Macintosh, 388
  Services for UNIX, 372
Milnet, 31
Mirabilis ICQ, 276
MIRC, 276
MMC (Microsoft Management Console), 305
MPPE (Microsoft Point-to-Point Encryption Protocol), 476

MS DOS, 358
MSAU (Multistation Access Unit), 74; 147
MTU (Maximum Transmission Unit), 407

N

NAT (Network Address Translation), 183
NAU (Network Addressable Unit), 392
NC (Network Computers), 501
NCP (NetWare Core Protocol), 372; 386
NDIS (Network Driver Interface Specification), 385
NDS (Novell Directory Services), 309; 328
NetBEUI (NetBIOS Extended User Interface), 70; 219
NetBIOS (Network Basic Input/Output System), 102; 219
Netscape, 374
Netscape Mail, 270
NetWare 4.x, 309
NetWare 5.x, 310
Network Monitor, 520
Network Neighborhood, 362
Network+, 47
NFS (Network File System), 349; 374; 386
NIS (Network Information System), 313
NMBd, 394
NNTP (Network News Transfer Protocol), 248; 272
Northern Light, 266
NPC (Network Personal Computer), 501
NSFNet, 31
NTFS (NT File System), 349
N-разъем, 140
N-терминатор, 140

O

OBI (Open Buying on the Internet), 478
ODI (Open Datalink Interface), 385
Open Source Initiative, 311
OpenLinux, 312
OpenView, 527
Opera, 264
OS/2, 377
  Warp Server, 316
  Warp 4, 377
OS/400, 333
OSI (Open System Interconnection), 71; 97
OSI X.500, 321
OS-SONET, 178
OU (Organizational Unit), 305

P

PAD (Packet Assembler/Disassembler), 167
Palm, 390
PAP (Password Authentication Protocol), 448
PC Card, 195
PCI (Peripheral Component Interconnect), 195
PCMCIA (Personal Computer Memory Card International Association), 195
PDC (Primary Domain Controller), 304
Pegasus, 270
Performance Monitor, 519
PGP (Pretty Good Privacy), 416
ping, 533
Ping Of Death, 407
PnP (Plug and Play), 164
Pocket PC, 390
POP3 (Post Office Protocol), 269
POTS, 30
PPP (Point-to-Point Protocol), 374; 448
PPTP (Point-to-Point Tunneling Protocol), 448; 472
PRI (Primary Rate ISDN), 172
PSTN (Public Switched Telephone Network), 171
PU (Physical Unit), 392
PVC (Permanent Virtual Circuit), 178
PXE (Preboot Execution Environment), 500

Q

QNX Voyager, 263
QoS (Quality of Service), 104; 177
q-бит, 551

R

RAID, 436
RAS (Remote Access Service), 364
RDN (Relative Distinguished Name), 327
RDP (Remote Desktop Protocol), 498
RedHat Linux, 312
RFB (Remote Frame Buffer), 499
RG-11, 79; 200
RG-58, 199
RG-58 /U, 199
RG-58 A/U, 199
RG-59 C/U, 199
RG-8, 79; 200

S

SAM (Security Accounts Management), 304
SAMBA, 69; 315; 372; 388; 394
Sausage Software HotDog, 262
SavvySearch, 267
SCMA/CA, 128
Scripts, 313
SDS, 334
SDSL (Symmetric DSL), 173
Security Accounts Manager (SAM), 68
SHA (Secure Hash Algorithm), 421; 472
Slackware, 312
SLIP (Serial Line Internet Protocol), 374; 448
SMB (Server Message Block), 372; 386
SMBd, 394
SMBFS (SMB File System), 388
SMDS (Switched Multimegabit Data Service), 180
SMS (Systems Management Server), 524
SMSAU (Smart MSAU), 148
SMTP (Simple Mail Transfer Protocol), 100; 248; 269
SNA (Systems Network Architecture), 390
Sniffer, 519
Sniffer Distributed Analysis Suite, 522
Sniffer Pro High-Speed, 521
Sniffer Pro LAN, 521
Sniffer Pro WAN, 521
SNMP (Simple Network Management Protocol), 100; 527
SoftQuad HoTNetaL Pro, 262
SPAP (Shiva PAP), 448
SPID (Service Profile Identifier), 166; 456
SQL (Structured Query Language), 293
SSCP (System Service Control Point), 392
SSCP (System Services Control Point), 392
SSL (Secure Sockets Layer), 415
SuSE Linux, 313
SVC (Switched Virtual Circuit), 178
Switched 56, 175
System Monitor, 519
Systems Network Architecture (SNA), 69

T

TCP (Transmission Control Protocol), 234
TCP/IP, 222
TDM (Time Division Method), 121
Telnet, 100
TGT (Ticket-granting ticket), 422
Tivoli Enterprise, 526
Token Ring, 82; 146
TokenTalk, 71
TradeWave, 421

U

UART (Universal Asynchronous Receiver/Transmitter), 165
UDP (User Datagram Protocol), 103; 234
UNC (Universal Naming Convention), 306
UNIX, 311; 372
USB (Universal Serial Bus), 359
User Manager for Domains, 304
UUCP (UNIX-to-UNIX Copy Protocol), 374

V

VDSL (Very High Data Rate DSL), 173
Verisign, 421
vi, 313
VINES StreenTalk, 334
Voice over IP, 277

VPN (Virtual Private Network), 277; 469
VPNd, 483

W

W3C, 286
WBT (Windows-based Terminal), 493
Web-броузер, 263
Web-дизайнер, 261
Web-портал, 267
Web-сервер, 263
Wide Area Network (WAN), 53
Windows
  for Workgroups 3.11, 358
  Sockets (Winsock), 236
  2000, 303; 305
  2000 Professional, 367
  2000 Terminal Server, 496
  3.1, 358
  95a, 359
  95b, 359
  98, 359
  98 SE (Second Edition), 359
  CE, 502
  ME (Millennium Edition), 359
  NT, 303
  NT Workstation, 366
  NT 4.0, 304
Winframe, 498; 504
Winipcfg, 538
WINS, 240
Winsock (Windows Sockets), 102
World Wide Web, 260
WTO (World Trade Organization), 111

X

X Window, 311; 340; 505
X.25, 176
X.500, 325
XDMCP (XDM Communication Protocol), 498
xDSL, 173
XML (Extensible Markup Language), 478

Y

Yahoo Messenger, 276

А

Автономная система, 214
Автономный генератор электроэнергии, 433
Авторизация, 483
Адаптер DSL, 167
Адаптер ISDN, 166
Администрирование компьютерной сети, 514
Адрес конца туннеля, 472
Адрес памяти, 197
Активное обнаружение вторжения, 428
Активные пользователи, 515
Активный концентратор, 209
Активный план управления сетью, 514
Активный рабочий стол, 359
Активный раздел, 356
Алгоритм Диффи–Хеллмана, 419
Алгоритм хэширования, 420
Алгоритм шифрования, 417
Амплитуда, 118
Анализ информации, 539
Анализатор протоколов, 516
Аналоговый сигнал, 118
Аплет, 506
Аргумент, 343
Архитектура SNA, 390; 392
Архитектура сети, 106; 137
Асимметричный шифр, 419
Асинхронная передача, 123
Атака DoS, 406
Атака на основе социальной инженерии, 405
Атаки Smurf, 406
Атаки SYN, 407
Атрибут, 322
Аудио- и видеоконференция, 276; 445
Аудит, 296; 428
Аутентификация, 420; 448; 483
Аутентификация пользователя, 66
Аутентификация удаленного доступа, 448

Б

База данных Bindery, 68; 309
База данных учетных записей, 68
Базовый уровень, 515
Байт, 92
Бездисковая рабочая станция, 499
Безопасность
  на уровне доменов, 297
  на уровне пользователей, 64; 296
  на уровне ресурсов, 64; 295
  сети, 401
Беседа, 275
Бесклассовая адресация, 225; 228
Бесклассовый метод адресации, 224
Беспроводная среда, 43
Беспроводные глобальные сети, 181
Беспроводные сетевые технологии, 548
Беспроводные средства сетевой коммуникации, 203
Билет, 422
Билет на получение билета, 422
Бинарное дерево каталогов, 351
Биометрические устройства, 424
Биометрия, 424
Бит, 92
Битовая синхронизация, 122
Блокировка учетных записей, 463
Брандмауэр, 428
Быстрый вход, 360

В

Ветвление файлов, 354
Ветвь
  данных, 354
  источника, 354
Взаимная аутентификация, 448
Виртуальная FAT (VFAT), 350
Виртуальная частная сеть, 277; 469
Виртуальный канал, 178
Витая пара, 43; 141; 201
  неэкранированная, 201
  экранированная, 202
Вкладка
  Configuration, 360
  Identification, 361; 366
Внешний модем, 452
Внешний трансивер, 79
Внутренний модем, 452
Волновое сопротивление, 199
Волоконно-оптическая связь, 82
Волоконно-оптический кабель, 44; 202
Временное разделение каналов, 121
Время доступа, 355
Всеобщая связь, 552
Встроенный сетевой адаптер, 195
Вторичное кольцо, 151
Выделенная линия, 174
Выделенное соединение, 447
Выделенный сервер, 61
Вытесняющая многозадачность, 358

Г

Гарантированное изменение состояний, 123
Гибридная компьютерная сеть, 44
Гибридная сеть, 381
Глобальная сеть, 44; 56; 161
Глобальная служба каталогов, 323
Городская сеть, 44; 55
Гостевая учетная запись, 446
Графическая оболочка, 340
Графический интерфейс, 341
Группа
  безопасности, 299
  по умолчанию, 299
  распространения, 299
Группа безопасности, 413
Группировка пропускных способностей, 449
Группы, 296
Группы новостей, 272

Д

Дайджест сообщения, 420
Двоичная система, 92
Двоичные числа, 90
Двоичный язык, 89
Двойное кольцо, 151
Дейтаграмма, 235
Демилитаризованная зона (DMZ), 428
Демон, 260; 312
Демультиплексор, 121

Дерево, 323
Дерево доменов, 303; 330
Дерево каталогов, 348
Дескриптор, 261
Десятичная система, 90
Дефрагментация, 351
Дешифрование, 417
Динамическая DNS (DDNS), 240
Динамическая
маршрутизация, 213; 282
Динамические диски, 356
Дисковая квота, 352
Дискретные состояния, 118
Дистанционная диагностика, 41
Дистанционное образование, 560
Дифференциальное резервное
копирование, 434
Длинное имя файла, 350
Доверительное отношение, 331
Документ, 348
Документы RFC, 112
Домашние сети, 548
Домен, 43; 238; 303; 330; 360
Домен конфликтов, 145
Дорожка, 355
Доступ к файлам и принтерам, 361
Драйвер, 166
файловой системы, 350
Дуплексная передача, 124

Ж

Журнал операционной системы, 532

З

Заголовок, 143
IP, 237
инкапсуляции, 472
пакета, 94
Закон Мэрфи, 401
Запрос DHCP, 230
Зарезервированный адрес, 230
Затухание, 73; 119; 126
Зацикливание мостов, 211
Звездообразная топология, 75; 168
Звездообразное кольцо, 147
Зона, 154
Зуб вампира, 79; 140; 200

И

Идентификатор услуги и линии, 456
Идентификация
голоса, 425
отпечатков пальцев, 424
радужной оболочки, 424
Избыточность, 437
Импеданс, 199
Имперсонификация, 405
Имя домена, 238
Имя рабочей группы, 361
Имя совместно используемого
ресурса, 300
Индексная база данных, 266
Индикатор состояния модема, 452
Инкапсуляция, 98
Инкапсуляция данных, 469
Инкрементное копирование, 434
Инструменты администрирования, 298
Интеллектуальная карта, 423
Интеллектуальный дом, 553
Интеллектуальный концентратор, 209
Интерактивная беседа, 445
Интерфейс
графический, 341
маршрутизации, 280
пользователя, 340
текстовый (символьный), 340
Инфракрасные средства связи, 205
Инфраструктура открытых ключей, 421
Искусственный интеллект, 551; 561
Источник бесперебойного
питания, 432

К

Кабель
волоконно-оптический, 202
коаксиальный, 198
толстый, 200
тонкий, 199
Ethernet, 141
Кабельный модем, 457
Кадр, 94; 143
Кадр LLC (Logical Link Control), 149

Канальный уровень, 104
Каталог, 321
Квантование времени, 358
Квантовые сети, 551
Квантовый бит, 551
Киборг, 562
Класс IP-адреса, 223
Классовая адресация, 225
Классы адресов, 224
Классы объектов, 322
Кластер, 349; 437
Кластеризация, 437
Кластеры, 62
Клиент, 59; 63
  новостей, 272
  удаленного доступа, 443; 459
Клиентская операционная система, 44; 63
Ключ, 404; 417
Ключ сеанса, 422
Коаксиальный кабель, 43; 198
Кодирование, 117
Количество транзитных передач, 168
Коллизия, 139
Кольцевая топология, 73
Кольцеобразная топология, 168
Команда, 342
Комбинированный сетевой адаптер, 195
Коммуникация, 259
  персональных компьютеров с карманными компьютерами, 390
  персональных компьютеров с компьютерами Macintosh, 389
  персональных компьютеров с мэйнфреймами, 389
Коммутатор, 214
  уровня 2, 214
  уровня 3, 215
  уровня 4, 215
  сетевого уровня, 104
Коммутационная панель, 208
Коммутация
  каналов, 29; 171
  пакетов, 29; 176
Коммутируемое соединение, 364; 447
Коммутируемый маршрутизатор, 215
Коммутирующие концентраторы, 106
Комплекс серверов, 294
Комплект протоколов, 44
Компьютерная сеть, 32
Компьютерный вирус, 408
Конвергенция, 283
Консоль управления, 305
Контроллер домена, 297
Контроллер доменов, 61
Контроль носителя, 128
Конфигурация
  от шлюза к шлюзу, 478
Конфликт, 129
Конфликт данных, 82
Концентратор, 107
Кооперативная многозадачность, 358
Корпоративная сеть, 37
Криптоанализ, 417
Криптография, 417
Критерии оценки безопасности для сетей, 427
Крэкер, 405
Кэширование, 184

Л

Лес, 330
Лес доменов, 303
Листовой объект, 325
Логическая топология, 45; 72
Логический диск, 356
Логическое кольцо, 74
Локальная сеть, 44; 54
Локальная служба каталогов, 323

М

Магистраль, 77; 140
Магистраль Internet, 254
Магнитная головка, 355
Маркер, 82; 147
Маркер доступа, 297
Маршрут по умолчанию, 280
Маршрутизатор, 212; 279
Маршрутизация, 104; 278
  динамическая, 213; 282
  статическая, 213; 281
Маршрутизированное соединение, 185
Маска переменной длины, 232

Маска подсети, 231
Машинный язык, 90; 342
Маяк, 147
Мгновенная передача сообщений, 276
Межгалактическая сеть, 42
Межсетевой уровень, 109
Меры безопасности, 403
Метадескриптор, 265
Метапоисковые службы, 267
Метод
  доступа, 128
  инверсного мультиплексирования, 172
  сетевого доступа, 105
  удаления эха, 173
Метрика, 282
Механизм подтверждения, 103
Механизм поиска и выдачи результатов, 266
Микросхема UART, 165
Многомастерная репликация, 332
Многомодовый режим, 203
Многопортовый повторитель, 209
Многоуровневые глобальные сети, 169
Множественный доступ, 129
Модель
  DoD, 108
  Microsoft, 110
  OSI, 97
Модем, 162; 450
  DSL, 167
  PC Card, 453
  внешний, 164; 452
  внутренний, 162; 452
  кабельный, 457
  устранение неполадок, 454
Модемный пул, 445
Модулированный сигнал, 120
Модуляция, 117
Модуляция/демодуляция, 450
Мониторинг сети, 516
Мост, 210
Мост-маршрутизатор, 214
Мотивы внешнего вторжения, 404
Мультиплексирование, 119; 121
Мультиплексор, 121
Мэйнфрейм, 31; 292

Н

Национальный научный фонд США, 35
Нейронные компьютерные сети, 550
Немодулированный сигнал, 120
Непосредственное расширение спектра (DSSS), 206
Непрерывное пространство имен, 324
Несущий сигнал, 120
Неэкранированная витая пара, 201
Номер порта, 235
Номер сети, 221
Номер узла, 221

О

Обнаружение конфликтов, 129
Обратная совместимость, 351
Обратное обновление с устранением ошибки, 284
Обратный вызов, 461
Обращенное дерево, 323; 348
Объект, 322
Объект-потомок, 324
Ограничения IP, 549
Одномодовый режим, 203
Одноранговая сеть, 43; 63
  администрирование, 64
  безопасность, 64
Октет, 223; 407
Операционная система, 339
Организационная единица, 305
Отказ в обслуживании, 406
Отказоустойчивость, 356; 436
  системы, 31
Отказоустойчивый набор, 436
Открытие DHCP, 229
Открытый исходный код, 311
Относительно уникальное имя, 327
Относительный путь, 348
Отражение сигнала, 72

П

Пакет, 30; 94
Пакет протоколов, 98
Папка, 348
Пара ключей, 419

Параллельные вычисления, 551
Пароль, 404; 412
Пассивное обнаружение вторжения, 428
Паук, 266
ПВХ (поливинилхлорид), 43
Пейджер, 41
Первая оптическая телеграфная сеть, 28
Первичное кольцо, 151
Первичный контроллер
  домена, 68; 304
Первичный раздел, 356
Передача маркера (эстафетный
  доступ), 128
Перекрестные помехи, 126; 201
Перетаскивание, 342
Пиктограмма, 341
План резервного копирования, 433
Платформа, 389
Пленум, 43
Пленум-кабель, 198
Повторитель, 73; 107; 209
Пограничный маршрутизатор, 285
Поддержка длинных имен файлов, 350
Подмена IP-адреса, 407
Подсеть, 209
Подтверждение DHCP, 230
Подтверждение приема пакета, 103
Подуровень LLC, 105
Подуровень MAC, 104
Поиск информации, 265
Поисковые службы, 265
Поле
  состояния кадра, 150
  управления доступом, 150
  управления кадром, 150
Полное резервное копирование, 434
Полный путь, 348
Полудуплексная передача, 124
Полупроводниковый лазер, 203
Полуячеистая топология, 76
Пользовательская маска, 232
Помехи
  перекрестные, 126
  радиочастотные, 126
  электромагнитные, 125
Порт, 234
  ввода-вывода, 197
Портал, 267
Порядок связывания протоколов, 385
Последовательность устранения
  неполадок, 531
Последовательный порт, 164
Потоковый режим, 275
Почтовый ящик, 270
Права доступа, 66
Правила
  безопасности, 426
  предоставления доступа, 426
  прекращения доступа, 426
  создания имени пользователя, 298
  создания паролей, 412
Правило 5-4-3, 144
Преамбула, 143
Предложение DHCP, 229
Предотвращение конфликтов, 129
Преимущества цифровых
сигналов, 119
Прикладной уровень, 98
Приложение, 339
Приложения типа клиент/сервер, 293
Приоритеты запросов, 128
Провайдер услуг Internet, 256
Программа самозагрузки, 352
Продвижение IP, 278
Прокси-сервер, 62; 184; 428; 429
Промышленный шпионаж, 408
Пропускная способность, 57; 127; 517
Пропускная способность по
  требованию, 177
Простой прозрачный мост, 210
Пространство имен, 305; 323
Протокол, 96
  BAP, 449
  CMIP, 528
  DHCP, 229
  FTP (File Transfer Protocol), 248
  HTTP, 260
  HTTP (Hypertext Transfer
    Protocol), 248
  ICA, 498
  IMAP (Internet Message Access
    Protocol), 269
  IPP, 368
  IPSec, 367; 414; 472; 481; 482
  IPX/SPX, 220
  L2F, 472; 480

Протокол
L2TP, 367; 448; 480
MPPE, 476; 482
NCP, 386
NetBEUI, 220
NFS, 374; 386
NNTP (Network News Protocol), 272
NNTP (Network News Transfer Protocol), 248
OSPF, 285
POP3 (Post Office Protocol), 269
PPP, 374; 448
PPTP, 448; 472; 480
RDP, 498
RFB, 499
RIP, 283
SLIP, 374; 448
SMB, 386
SMTP (Simple Mail Transfer Protocol), 248; 269
SNMP, 527
SSH, 481
SSL, 415
TCP, 234
TCP/IP, 222
Telnet, 248
UDP, 234
UUCP, 374
XDMCP, 498
без установления соединения, 103
динамической конфигурации хоста, 229
канального уровня, 78
маршрутизации, 214
дистанционно-векторные, 282
на основе состояния каналов, 282
порядок связывания, 385
разделения файлов, 386
с установлением логических соединений, 103
сетевого уровня IP, 222
сетевого уровня IPX, 221
транспортного уровня SPX, 222
туннелирования, 479
шифрования, 479
ядра, 383
Протокольный шлюз, 390
Профиль оборудования, 368
Процедура APIPA, 231
Процесс, 96
Пул модемов, 166
Пул принтеров, 308
Пункт
MAE, 257
NAP, 257
Путь
относительный, 348
полный, 348

Р

Рабочая сеть, 357
Рабочая станция, 63
Рабочие группы, 54
Радиочастотные помехи, 126
Раздел, 356
Разделение
подключений к Internet, 302
приложения, 302
принтеры, 302
файлы и каталоги, 301
Разделяемые ресурсы, 59
Разделяемый ресурс, 300
Разрешение имен, 103; 237
Разъем
AUI, 107
BNC, 138; 207
MIC, 149
RJ, 207
RJ-45, 142
Расписание резервного копирования, 434
Распределенная глобальная сеть, 57
Распределенная служба каталогов, 323
Расширение файла, 346
Расширенный раздел, 356
Расщепление горизонта, 283
Реализация мер безопасности, 410
Редактор HTML, 262
Редиректор, 101; 391
Редиректор Windows–NetWare, 391
Режим обратного вызова, 461
Режим туннелирования
AH, 481

ESP, 481
Резервирование электропитания, 431
Резервное копирование данных, 433
Резервный контроллер домена, 304
Репликация, 332
Родительский объект, 324
Розетка, 208

С

Сбор информации, 539
Светодиод, 203
Связанные списки, 351
Сеансовый уровень, 101
Сегмент, 94
Сегментация сети, 209
Сектор, 355
Семейная локальная сеть, 554
Сервер, 43; 59
  BOOTP, 62
  DHCP, 62
  Web, 61
  аутентификации, 297
  кластерный, 62
  новостей, 272
  печати, 61
  приложений, 61
  приложений, 302; 503
  прокси, 62
  разрешения имен, 62
  регистрационный, 61
  телефонный, 62
  терминальный, 62
  удаленного доступа, 62; 166; 258; 443; 449; 460
  файловый, 61
  факс, 62
  электронной почты, 61
Сертификация, 46
Сетевая архитектура, 78
Сетевая модель, 43
Сетевая операционная система, 44; 291
Сетевой адаптер, 43; 106; 193
  выбор, 194
  комбинированный, 195
Сетевой администратор, 66; 387
Сетевой анализатор пакетов, 405
Сетевой интерфейс, 223
Сетевой компьютер, 501
Сетевой персональный компьютер, 501
Сетевой уровень, 104
Сеть, 223
  AppleTalk, 83
  ARCnet, 83
  Ethernet, 78
  IPX/SPX, 70
  NetBEUI, 70
  NetWare, 68
  TCP/IP, 70
  Token Ring, 82
  UNIX, 68
  Windows, 68
  администрирование, 66
  безопасность, 66
  в свернутом состоянии, 151
  глобальная, 56; 161
    распределенная, 57
    централизованная, 57
  городская, 55
  звездообразная, 74
  клиент/сервер, 43; 294
  локальная, 54
  одноранговая, 43; 63
  с кольцевой топологией, 73
  с коммутацией каналов, 171
  с коммутацией пакетов, 176
  с шинной топологией, 72
  с ячеистой топологией, 76
  смешанная, 69
  смешанная ячеистая, 76
Сжатие данных, 101
Сжатие на уровне файлов, 350
Сигнал
  аналоговый, 118
  цифровой, 118
Сигнатура сектора, 354
Симметричный шифр, 418
Симплексная передача, 123
Симплексный режим, 102
Синтаксис, 342
Синхронизация, 122
  потока данных, 101
Синхронная передача, 123
Система
  безопасности Kerberos, 368

глобального
позиционирования, 548
каталогов, 352
Скачкообразное переключение частот (FHSS), 206
Служба
RADIUS, 462
RADIUS (Remote Authentication Dial-In User Service), 448
vBNS, 255
имен доменов, 240
каталогов, 321
сервера, 295
Службы, 340
каталогов, 300
Служебные программы, 340
Смайлик, 269
Смешанные сети, 69; 76
Соглашения об именовании файлов, 347
Соединительное устройство, 206
Соединительные устройства, 44
Создание подсетей, 209
Сокет, 234
Составление и реализация плана действий, 539
Спам, 268
Спецификации TCSEC, 426
Спецификации TNI, 427
Списки рассылки, 271
Список
доступных разделяемых ресурсов, 60
контроля доступа, 296; 430
просмотра, 363
Справочные файлы, 345
Спул принтера, 308
Среда, 43
Стартовый бит, 123
Стартовый разграничитель, 150
Статическая маршрутизация, 213; 281
Стек (набор) протоколов, 44
Стратегия
групп, 330
удаленного доступа, 462
управления доступом, 413
Стробирование, 123
Строка инициализации модема, 451
Суперсеть, 228
Схема, 322
i-узлов, 353
Сценарии UNIX, 313
Сценарий соединения, 374

T

Таблица маршрутизации, 211; 280
Таблица размещения файлов, 349
Текстовый (символьный) интерфейс, 340
Телемедицина, 559
Телефон, 28
Терминал, 31
Терминал WBT, 500
Терминальная эмуляция, 274
Терминальные службы, 302
Терминальный адаптер, 166
Терминальный адаптер ISDN, 456
Терминальный сервер, 493
Терминатор, 72
Терминатор BNC, 207
Технологии электронной коммерции, 555
Технология
PnP (Plug and Play), 164
связи без установления соединения, 30
тонких клиентов, 495
Тип носителя сигналов, 106
Т-носители, 174
Т-образный разъем, 138
Толстая Ethernet, 139
Толстый коаксиальный кабель, 200
Тонкая сеть, 138
Тонкий коаксиальный кабель, 199
Топология, 167
звездообразная, 168
кольцеобразная, 168
логическая, 72
сети, 526
точечная, 167
физическая, 72
ячеистая, 169
Точечная топология, 167
Точка
доступа, 203

монтирования, 315
монтировки, 352
отправки (приема) данных, 392
присутствия, 256
Точки проверки, 101
Транзитивное доверительное отношение, 331
Транзитная передача, 168
Трансивер, 79; 107; 203
Трансиверный кабель, 139
Трансляция адресов, 182
Трансляция протоколов, 101
Транспортный уровень, 102
Требования к безопасности, 402
Трейлер, 95; 143
Триггерные обновления, 284
Троянский конь, 408
Туннель, 469; 471

У

Удаленный вызов процедур, 372
Удаленный доступ к сети, 443
Удаленный сервер, 364
Уж 100BaseT, 142
Узел, 63
Узкое место, 514
Узкополосная радиосвязь, 206
Универсальная группа, 299
Универсальное соглашение об именах, 306
Уникальное имя, 327
Управление доступом к сети, 104
Управление логическими связями, 104
Уровень
безопасности, 402
канальный, 104
обмена между хостами (транспортный уровень), 109
представления, 101
прикладной, 98
приложений/процессов, 108
сеансовый, 101
сетевого интерфейса, 109
сетевой, 104
транспортный, 102
физический, 105
Уровни процесса коммуникации, 96
Установки IRQ, 196
Устранение сетевых неполадок, 530
Утилита
ARP, 242
config, 246
ifconfig, 246
ipconfig, 246
lptrace, 247
nbtstat, 245
netstat, 243
ping, 242
traceout, 247
tracert, 247
winipcfg, 246
трассирования, 535
Утилиты дефрагментации, 351
Учетная запись, 296
администратора, 297
группы, 298
компьютера, 297; 300
пользователя, 297

Ф

Фаза, 118
Файл, 345
HOSTS, 239
LMHOSTS, 239
длинное имя, 350
расширение, 346
тип, 345
Файловая система, 347
Файловый сервер, 301
Факс-сервер, 62
Физическая топология, 45; 72
Физический доступ, 431
Физический уровень, 105
Фильтр питания, 432
Фильтрация
канала, 429
пакетов, 429
приложений, 429
Флаг, 343
Фрагментация файлов, 351

Х

Хакер, 404
Хост, 63; 223
Хост безопасности, 463
Хост трансляции адресов, 182
Хранилище данных, 294
Хэш, 420

Ц

Центр распределения ключей, 422
Централизованная глобальная сеть, 57
Централизованная система, 292
Централизованное управление, 65
Цилиндр, 355
Цифровая подпись, 420
Цифровой сертификат, 421
Цифровой сигнал, 118

Ч

Частота, 118
Частотное разделение каналов, 121
Червь, 408

Ш

Шестнадцатеричная система, 90
Шина, 72
Шина компьютера, 106; 194
Широковещательное сообщение, 225
Широковещательный адрес, 211
Широковещательный шторм, 213
Широкополосная радиосвязь, 206
Шифр, 417
Шифр с открытыми/закрытыми ключами, 419
Шифрование, 414; 417
Шифрование
  данных, 101
  файлов, 352
Шифротекст, 417
Шлюз, 58; 101; 391
  SNA (Systems Network Architecture), 101
  по умолчанию, 186; 278
  электронной почты, 101
Шредингеров кот, 552
Штепсель, 208
Шум, 125

Э

Экран, 202
Экранированная витая пара, 202
Экранированная сеть, 428
Экспертная система, 561
Экстрасеть, 476
Электрический телеграф, 28
Электромагнитные помехи, 125
Электронная книга, 559
Электронная коммерция, 37
Электронная почта, 268
Эмотикон, 269
Эхо-запрос ICMP, 242
Эхо-ответ ICMP, 242

Я

Ядро, 352
Язык программирования, 342
Ячеистая топология, 76; 169

Научно-популярное издание

Дебра Литтлджон Шиндер

Основы компьютерных сетей

Литературный редактор *Т.П. Кайгородова*
Верстка *О.В. Линник*
Художественный редактор *В.Г. Павлютин*
Корректор *З.В. Александрова*

Издательский дом "Вильямс".
101509, Москва, ул. Лесная, д. 43, стр. 1.
Изд. лиц. ЛР № 090230 от 23.06.99
Госкомитета РФ по печати.

Подписано в печать 30.04.2002. Формат 70×100/16.
Гарнитура Times. Печать офсетная.
Усл. печ. л. 52,9. Уч.-изд. л. 40,2.
Тираж 4000 экз. Заказ № 498.

Отпечатано с диапозитивов в ФГУП "Печатный двор"
Министерства РФ по делам печати,
телерадиовещания и средств массовых коммуникаций.
197110, Санкт-Петербург, Чкаловский пр., 15.