

# Содержание

<b>Благодарности</b> . . . . .	<b>26</b>
<b>Введение</b> . . . . .	<b>27</b>
От издательства . . . . .	28
<b>Глава 1. Открытые коммуникации</b> . . . . .	<b>29</b>
Эволюция открытых сетей . . . . .	30
Многоуровневая структура коммуникаций . . . . .	30
Эталонная модель OSI . . . . .	32
1. Физический уровень . . . . .	33
2. Канальный уровень . . . . .	34
3. Сетевой уровень . . . . .	34
4. Транспортный уровень . . . . .	35
5. Сеансовый уровень . . . . .	35
6. Представительский уровень . . . . .	37
7. Прикладной уровень . . . . .	37
Использование модели . . . . .	37
Эталонная модель TCP/IP . . . . .	40
Анатомия модели TCP/IP . . . . .	40
Итоги . . . . .	42
<b>Глава 2. TCP/IP и Интернет</b> . . . . .	<b>43</b>
История Интернета . . . . .	43
ARPANET . . . . .	44
TCP/IP . . . . .	44
NSF . . . . .	45
Интернет сегодня . . . . .	45
RFC и процесс стандартизации . . . . .	46
Источники информации о RFC . . . . .	47
Индексы RFC . . . . .	48
Краткое знакомство со службами Интернета . . . . .	48
Whois и Finger . . . . .	48
FTP . . . . .	48
Telnet . . . . .	49
Электронная почта . . . . .	49
World Wide Web . . . . .	49
Usenet . . . . .	49

Интрасети и экстрасети . . . . .	50
Интрасети . . . . .	50
Преимущества интрасетей . . . . .	50
Области применения интрасетей . . . . .	51
Предоставление внешнего доступа к интрасети . . . . .	51
Будущее Интернета . . . . .	52
NGI (Next Generation Internet) . . . . .	52
vBNS . . . . .	52
Internet2 (I2) . . . . .	53
Так кто же главный в Интернете? . . . . .	53
ISOC (Internet Society) . . . . .	53
IAB (Internet Architecture Board) . . . . .	53
IETF (Internet Engineering Task Force) . . . . .	54
IESG (Internet Engineering Steering Group) . . . . .	54
IANA (Internet Assigned Numbers Authority) . . . . .	54
ICANN (Internet Corporation for Assigned Names and Numbers) . . . . .	54
InterNIC и другие регистрирующие органы . . . . .	55
Редактор RFC . . . . .	55
Поставщики услуг Интернета . . . . .	55
Итоги . . . . .	56
<b>Глава 3. Общий обзор TCP/IP . . . . .</b>	<b>57</b>
Преимущества TCP/IP . . . . .	57
Уровни и протоколы TCP/IP . . . . .	58
Архитектура . . . . .	58
TCP . . . . .	59
IP . . . . .	61
Прикладной уровень . . . . .	63
Транспортный уровень . . . . .	63
Сетевой уровень . . . . .	64
Канальный уровень . . . . .	64
Telnet . . . . .	64
FTP . . . . .	64
TFTP . . . . .	65
SMTP . . . . .	66
NFS . . . . .	66
SNMP . . . . .	67
Место TCP/IP в системе . . . . .	68
Концепция интрасети . . . . .	69
Итоги . . . . .	69
<b>Глава 4. Имена и адреса в сетях IP . . . . .</b>	<b>70</b>
Адресация в протоколе IP . . . . .	70
Двоичная и десятичная запись . . . . .	71
Форматы адресов IPv4 . . . . .	72
Класс А . . . . .	73

Класс В . . . . .	74
Класс С . . . . .	74
Класс D . . . . .	75
Класс E . . . . .	76
Недостатки схемы адресации IPv4 . . . . .	76
Специальные IP-адреса . . . . .	77
Адресация сети . . . . .	78
Направленная широковещательная рассылка . . . . .	78
Ограниченная рассылка . . . . .	79
Нулевой IP-адрес . . . . .	79
IP-адрес хоста в текущей сети . . . . .	80
Обратная связь . . . . .	80
Исключение в схеме адресации IP . . . . .	81
Появление подсетей . . . . .	81
Подсети . . . . .	82
Пример использования подсети . . . . .	85
Маски подсети переменной длины . . . . .	87
CIDR . . . . .	88
Бесклассовая адресация . . . . .	89
Расширенное агрегирование маршрутных данных . . . . .	89
Суперсети . . . . .	89
Принцип работы CIDR . . . . .	90
Открытые адресные пространства . . . . .	91
RFC 1597 и 1918 . . . . .	91
Адресация в частных сетях . . . . .	92
Назначение адресов класса С . . . . .	94
Настройка IP-адресов . . . . .	95
Адресация в IP версии 6 . . . . .	96
Итоги . . . . .	98
<b>Глава 5. ARP и RARP . . . . .</b>	<b>99</b>
Механизмы адресации . . . . .	99
Адресация в подсетях . . . . .	100
Физические адреса . . . . .	100
Адрес LLC . . . . .	101
Сетевые кадры . . . . .	102
IP-адреса . . . . .	103
Общие сведения о протоколе ARP . . . . .	104
Кэш ARP . . . . .	105
Тип оборудования . . . . .	106
Тип протокола . . . . .	107
Длина аппаратного адреса (HLen) . . . . .	108
Длина протокольного адреса (PLen) . . . . .	108
Код операции . . . . .	108
Аппаратный адрес отправителя . . . . .	108
IP-адрес отправителя . . . . .	108

Аппаратный адрес получателя . . . . .	108
IP-адрес получателя . . . . .	108
Схема работы ARP . . . . .	109
Строение протокола ARP . . . . .	110
Сетевой мониторинг с использованием ARP . . . . .	111
Тайм-аут в кэше ARP . . . . .	111
ARP в мостовых сетях . . . . .	113
Дублирование адресов и ARP . . . . .	114
Дублирование IP-адресов клиентов TCP/IP . . . . .	114
Дублирование IP-адресов на серверах TCP/IP . . . . .	116
Проверка дублирования адресов ARP . . . . .	117
Proxy ARP . . . . .	117
RARP . . . . .	118
Схема работы RARP . . . . .	119
Сбой сервера RARP . . . . .	121
Основные и резервные серверы RARP . . . . .	121
Команда ARP . . . . .	122
Итоги . . . . .	122
<b>Глава 6. DNS . . . . .</b>	<b>123</b>
Система доменных имен: общие принципы . . . . .	123
Иерархическое строение DNS . . . . .	125
Делегирование полномочий . . . . .	126
Распределенная база данных DNS . . . . .	127
Домены и зоны . . . . .	127
Домены верхнего уровня в Интернете . . . . .	128
Выбор сервера имен . . . . .	128
Процесс разрешения имен . . . . .	128
Рекурсивные запросы . . . . .	128
Итеративные запросы . . . . .	129
Кэширование . . . . .	129
Запросы на обратное разрешение . . . . .	129
Безопасность DNS . . . . .	129
Ресурсные записи (RR) . . . . .	129
Ресурсные записи типа SOA . . . . .	130
Ресурсные записи типа A . . . . .	132
Ресурсные записи типа NS . . . . .	132
Ресурсные записи CNAME . . . . .	132
Ресурсные записи PTR . . . . .	133
Делегированные домены . . . . .	133
Ресурсные записи HINFO . . . . .	133
Ресурсные записи ISDN . . . . .	134
Ресурсные записи MB . . . . .	134
Ресурсные записи MG . . . . .	135
Ресурсные записи MINFO . . . . .	135
Ресурсные записи MR . . . . .	135

Ресурсные записи MX . . . . .	135
Ресурсные записи RP . . . . .	136
Ресурсные записи RT . . . . .	136
Ресурсные записи TXT . . . . .	136
Ресурсные записи WKS . . . . .	137
Ресурсные записи типа X25 . . . . .	137
Итоги . . . . .	137
<b>Глава 7. WINS . . . . .</b>	<b>138</b>
NetBIOS . . . . .	138
Разрешение имен в NetBIOS . . . . .	141
Динамическое разрешение имен в NetBIOS . . . . .	143
Преимущества WINS . . . . .	144
Как работает WINS . . . . .	144
Настройка клиентов WINS . . . . .	146
Настройка WINS для прокси-агентов . . . . .	147
Настройка прокси-агента в NT 4 . . . . .	148
Настройка прокси-агента в Windows 95/98 . . . . .	148
Настройка сервера WINS . . . . .	148
Администрирование и сопровождение WINS . . . . .	149
Добавление статических записей . . . . .	149
Сопровождение базы данных WINS . . . . .	150
Архивация базы данных WINS . . . . .	153
Архивация данных реестра . . . . .	154
Восстановление базы данных WINS . . . . .	154
Сжатие базы данных WINS . . . . .	154
Репликация WINS . . . . .	155
Рекомендации по реализации WINS . . . . .	156
Интеграция служб разрешения имен . . . . .	156
Предоставление данных WINS через DHCP . . . . .	157
Разрешение имен NetBIOS через файл LMHOSTS . . . . .	158
Итоги . . . . .	160
<b>Глава 8. Автоматизированная настройка TCP/IP . . . . .</b>	<b>162</b>
Динамическая настройка конфигурации с применением BOOTP . . . . .	162
IP-адреса запросов/ответов BOOTP . . . . .	163
Потеря сообщений BOOTP . . . . .	166
Формат сообщения BOOTP . . . . .	166
Фазы BOOTP . . . . .	168
Дополнительные данные . . . . .	169
Динамическая настройка с использованием DHCP . . . . .	171
Распределение IP-адресов в DHCP . . . . .	171
Назначение IP-адресов в DHCP . . . . .	172
Формат сообщения DHCP . . . . .	175
Трассировка протокола DHCP . . . . .	178
Итоги . . . . .	189

<b>Глава 9. Обзор семейства протоколов IP</b>	<b>190</b>
Модель TCP/IP	190
Семейство протоколов TCP/IP	190
Протокол IP	191
Заголовок IPv4	192
Задачи протокола IP	193
Поврежденные пакеты	194
Протокол TCP	195
Структура заголовка TCP	195
Задачи протокола TCP	197
Протокол UDP	200
Структура заголовка UDP	201
Задачи протокола UDP	201
Сравнение TCP с UDP	202
Итоги	203
<b>Глава 10. Протокол IP</b>	<b>204</b>
Абстрактная модель IP	204
Размер дейтаграммы IP	207
Фрагментация в IP	209
Структура дейтаграмм IP	210
Структура заголовка IP	211
Сетевой порядок байтов	238
Трассировка IP	239
Итоги	247
<b>Глава 11. Транспортные протоколы</b>	<b>248</b>
Протокол TCP	248
Возможности TCP	250
Программная среда хостов TCP	258
Открытие и закрытие соединений TCP	260
Структура пакета TCP	261
Адаптивный тайм-аут в TCP	275
Снижение последствий перегрузки сети в TCP	278
Борьба с синдромом мелкого окна	279
Разрыв соединений TCP	282
Конечный автомат TCP	283
Протокол UDP	298
Структура заголовка UDP	300
Иерархия UDP и инкапсуляция	301
Трассировка UDP	302
Итоги	304
<b>Глава 12. IPv6</b>	<b>306</b>
Дейтаграмма IPv6	307
Классификация приоритетов	309
Потоковые метки	310

128-разрядные IP-адреса . . . . .	311
Заголовки расширения IP . . . . .	312
Хосты с несколькими IP-адресами . . . . .	320
Направленные, групповые и альтернативные адреса . . . . .	321
Переход с IPv4 на IPv6 . . . . .	323
Итоги . . . . .	325
<b>Глава 13. Маршрутизация в сетях IP . . . . .</b>	<b>326</b>
Основа маршрутизации . . . . .	326
Статическая маршрутизация . . . . .	327
Недостатки статической маршрутизации . . . . .	328
Дистанционно-векторная маршрутизация . . . . .	331
Топологическая маршрутизация . . . . .	334
Согласование в сетях IP . . . . .	336
Адаптация к топологическим изменениям . . . . .	337
Время согласования . . . . .	342
Построение маршрутов в сетях IP . . . . .	343
Хранение альтернативных маршрутов . . . . .	344
Механизм инициирования обновлений . . . . .	344
Маршрутные метрики . . . . .	345
Итоги . . . . .	346
<b>Глава 14. Шлюзовые протоколы . . . . .</b>	<b>347</b>
Шлюзы, мосты и маршрутизаторы . . . . .	347
Шлюз . . . . .	348
Мост . . . . .	348
Маршрутизатор . . . . .	349
Автономная система . . . . .	349
Знакомство со шлюзовыми протоколами . . . . .	349
Протоколы IGP и EGP . . . . .	350
Протокол GGP . . . . .	350
Протокол EGP . . . . .	351
Протоколы IGP . . . . .	352
Итоги . . . . .	352
<b>Глава 15. Протокол RIP . . . . .</b>	<b>353</b>
RFC 1058 . . . . .	353
Формат пакета RIP . . . . .	354
Таблица маршрутизации RIP . . . . .	356
Механика работы RIP . . . . .	358
Вычисление расстояний . . . . .	360
Обновление таблицы маршрутизации . . . . .	365
Проблемы адресации . . . . .	367
Топологические изменения . . . . .	370
Согласование . . . . .	371
Проблема бесконечного отсчета . . . . .	373

Недостатки RIP . . . . .	382
Ограничение количества переходов . . . . .	382
Фиксированные метрики . . . . .	382
Высокий уровень трафика при обновлении таблиц . . . . .	383
Медленное согласование . . . . .	383
Отсутствие распределения нагрузки . . . . .	383
Итоги . . . . .	384
<b>Глава 16. Протокол OSPF . . . . .</b>	<b>385</b>
Происхождение OSPF . . . . .	385
Принципы работы OSPF . . . . .	386
Зоны OSPF . . . . .	387
Типы маршрутизации . . . . .	389
Межсетевая маршрутизация . . . . .	390
Обновление маршрутных данных . . . . .	391
Знакомство со структурами данных OSPF . . . . .	394
Пакет подтверждения состояния канала . . . . .	400
Построение маршрутов . . . . .	401
Автоматическое вычисление . . . . .	401
Использование стоимости маршрутов по умолчанию . . . . .	402
Ручная настройка значений . . . . .	403
Дерево кратчайших путей . . . . .	404
Дерево кратчайших путей для маршрутизатора 3 . . . . .	404
Дерево кратчайших путей для маршрутизатора 2 . . . . .	406
Итоги . . . . .	407
<b>Глава 17. Протокол IPP . . . . .</b>	<b>408</b>
История IPP . . . . .	408
Протокол IPP с точки зрения пользователя . . . . .	409
Реализация IPP от HP . . . . .	411
Итоги . . . . .	412
<b>Глава 18. Протоколы удаленного доступа . . . . .</b>	<b>413</b>
Удаленное подключение . . . . .	413
ISDN . . . . .	414
Кабельные модемы . . . . .	414
DSL . . . . .	416
Радиосети . . . . .	417
RADIUS . . . . .	417
Аутентификация RADIUS . . . . .	418
Транспортировка дейтаграмм IP в протоколах SLIP, CSLIP и PPP . . . . .	420
Протокол SLIP . . . . .	420
Протокол CSLIP . . . . .	421
Протокол PPP . . . . .	422
Туннелирование удаленного доступа . . . . .	427
Протокол PPTP (Point-to-Point Tunneling) . . . . .	428
Агрегирование сеансов PPP . . . . .	429



Отдельный управляющий канал . . . . .	430
Поддержка других протоколов . . . . .	431
Аутентификация и защита . . . . .	431
Типы туннелей PPTP . . . . .	431
Добровольный туннель . . . . .	431
Принудительный туннель . . . . .	432
Туннельный протокол уровня 2 (L2TP) . . . . .	433
IPSec . . . . .	439
Итоги . . . . .	442
<b>Глава 19. Брандмауэры . . . . .</b>	<b>444</b>
Безопасность сети . . . . .	444
Функции брандмауэров . . . . .	446
Использование брандмауэров . . . . .	446
Прокси-серверы . . . . .	447
Пакетные фильтры . . . . .	448
Защита служб . . . . .	449
Электронная почта (SMTP) . . . . .	449
HTTP: World Wide Web . . . . .	450
FTP . . . . .	450
Telnet . . . . .	451
Usenet: NNTP . . . . .	452
DNS . . . . .	452
Построение собственного брандмауэра . . . . .	452
Использование коммерческих брандмауэров . . . . .	453
Итоги . . . . .	456
<b>Глава 20. Сетевая и системная безопасность . . . . .</b>	<b>457</b>
Шифрование . . . . .	458
Шифрование с парными ключами . . . . .	459
Шифрование с симметричным закрытым ключом . . . . .	460
DES, IDEA и другие . . . . .	461
Аутентификация с применением цифровых подписей . . . . .	463
Раскрытие шифров . . . . .	464
Защита сети . . . . .	465
Вход в систему и пароли . . . . .	466
Разрешения доступа к файлам и каталогам . . . . .	466
UUCP в системах Unix и Linux . . . . .	468
Приготовьтесь к худшему . . . . .	469
Итоги . . . . .	469
<b>Глава 21. Общая конфигурация . . . . .</b>	<b>470</b>
Установка сетевой платы . . . . .	470
Сетевые платы . . . . .	471
Настройка ресурсов . . . . .	472
Установка программного обеспечения сетевой платы . . . . .	473

Редиректоры и API . . . . .	474
Службы . . . . .	475
Сетевые интерфейсы . . . . .	476
Сетевые и транспортные протоколы . . . . .	476
Обязательные параметры конфигурации IP . . . . .	476
Настройка адреса основного шлюза . . . . .	478
Настройка адреса сервера имен . . . . .	479
Настройка адреса почтового сервера . . . . .	479
Регистрация доменного имени . . . . .	480
Разновидности конфигурации IP . . . . .	480
Настройка таблицы маршрутизации . . . . .	481
Инкапсуляция внешних протоколов . . . . .	482
Итоги . . . . .	483
<b>Глава 22. Настройка TCP/IP в Windows 95 и Windows 98 . . . . .</b>	<b>485</b>
Сетевая архитектура Windows 98 . . . . .	485
Установка сетевой платы . . . . .	486
Мастер установки нового оборудования . . . . .	487
Изменение параметров конфигурации сетевой платы . . . . .	489
Если Windows 98 не загружается . . . . .	490
Настройка TCP/IP в Windows 98 . . . . .	491
Сбор предварительной информации . . . . .	491
Установка TCP/IP . . . . .	492
Настройка реализации TCP/IP от Microsoft . . . . .	492
Статические конфигурационные файлы . . . . .	498
Настройка реестра . . . . .	498
Тестирование TCP/IP . . . . .	502
Итоги . . . . .	504
<b>Глава 23. Настройка TCP/IP в Windows 2000 . . . . .</b>	<b>505</b>
Установка TCP/IP . . . . .	505
Настройка IP-адреса . . . . .	507
Назначение IP-адресов при отказе сервера DHCP . . . . .	510
Настройка параметров DNS . . . . .	510
Настройка адресов WINS . . . . .	514
Безопасность и фильтрация TCP/IP . . . . .	516
Настройка служб разрешения имен . . . . .	518
Службы NetBIOS . . . . .	519
Механизмы разрешения имен . . . . .	521
Настройка кэша имен NetBIOS . . . . .	523
Настройка широковещательных запросов на разрешение имен . . . . .	524
Настройка файла LMHOSTS . . . . .	526
Настройка файла HOSTS . . . . .	532
Другие служебные файлы TCP/IP . . . . .	533
Файл NETWORKS . . . . .	533
Файл PROTOCOL . . . . .	534
Файл SERVICES . . . . .	535

Установка и настройка службы сервера FTP . . . . .	538
Установка и настройка службы сервера FTP на сервере Windows 2000 . . . . .	539
Настройка TCP/IP для печати из Windows 2000 на принтерах Unix . . . . .	541
Установка и настройка сетевой печати TCP/IP . . . . .	541
Печать в Windows 2000 из клиентов Unix . . . . .	543
Программы командной строки TCP/IP . . . . .	544
Итоги . . . . .	547
<b>Глава 24. Поддержка IP в Novell NetWare . . . . .</b>	<b>548</b>
Novell и TCP/IP . . . . .	548
IP и NetWare 4 . . . . .	548
NetWare 5 и NetWare 6 . . . . .	549
Традиционные решения: IP в NetWare 3.x–4.x . . . . .	550
IP Tunneling . . . . .	551
IP Relay . . . . .	551
LAN Workplace . . . . .	552
IPX-IP Gateway . . . . .	552
NetWare/IP . . . . .	553
NetWare 5/NetWare 6 — IP и все удобства Novell . . . . .	554
Полноценная поддержка IP . . . . .	554
Поддержка нескольких протоколов . . . . .	554
Варианты установки . . . . .	555
Установка NetWare 5 и NetWare 6 для IP . . . . .	555
Что необходимо знать перед установкой . . . . .	556
Установка NetWare 5 и NetWare 6 для IPX . . . . .	557
Что необходимо знать перед установкой . . . . .	557
Смешанная установка IPX/IP . . . . .	557
Что необходимо знать перед установкой . . . . .	558
Средства, упрощающие переход на IP . . . . .	558
NDS . . . . .	558
DNS . . . . .	559
DHCP . . . . .	559
DDNS . . . . .	559
SLP . . . . .	559
Режим совместимости . . . . .	560
Migration Agent . . . . .	560
Стратегии перехода . . . . .	560
Тестовая платформа . . . . .	561
Возможные сценарии перехода . . . . .	561
Итоги . . . . .	562
<b>Глава 25. Настройка TCP/IP в системе Linux . . . . .</b>	<b>563</b>
Подготовка системы к настройке TCP/IP . . . . .	564
Доступ к сетевому интерфейсу . . . . .	566
Настройка интерфейса обратной связи . . . . .	567
Настройка интерфейса Ethernet . . . . .	569

Служба имен . . . . .	571
Шлюзы . . . . .	573
Графические программы настройки сетевых интерфейсов . . . . .	574
Программа netcfg . . . . .	575
Программа linuxconf . . . . .	575
Настройка SLIP и PPP . . . . .	578
Настройка фиктивного интерфейса . . . . .	579
Настройка SLIP . . . . .	580
Настройка PPP . . . . .	581
Итоги . . . . .	583
<b>Глава 26. Whois и Finger . . . . .</b>	<b>584</b>
Протокол Whois . . . . .	584
Регистрация имен в Интернете . . . . .	585
Базы данных Whois . . . . .	586
Примеры . . . . .	589
Расширения Whois . . . . .	592
RWhois . . . . .	592
WHOIS++ . . . . .	592
Finger . . . . .	592
Команда finger . . . . .	593
Демоны Finger . . . . .	595
Finger в других системах . . . . .	596
Необычное применение Finger . . . . .	596
Итоги . . . . .	598
<b>Глава 27. Протоколы пересылки файлов . . . . .</b>	<b>599</b>
Роль FTP и TFTP в современном мире . . . . .	599
Пересылка файлов через FTP . . . . .	600
Подключения FTP . . . . .	600
Управляющий порт . . . . .	601
Порт данных . . . . .	602
Подключение с использованием клиентов FTP . . . . .	603
Интерактивный режим FTP . . . . .	604
Безопасность при использовании FTP . . . . .	612
Серверы и демоны FTP . . . . .	615
Анонимный доступ FTP . . . . .	616
TFTP . . . . .	618
Отличия TFTP от FTP . . . . .	618
Команды TFTP . . . . .	619
Итоги . . . . .	619
<b>Глава 28. Telnet . . . . .</b>	<b>620</b>
Знакомство с протоколом Telnet . . . . .	620
Виртуальный терминал . . . . .	622
Демон Telnet . . . . .	623

Использование Telnet . . . . .	625
Команда telnet в системе Unix . . . . .	625
Графические клиенты Telnet . . . . .	626
Команды Telnet . . . . .	627
Примеры использования Telnet . . . . .	629
Дополнительные возможности Telnet . . . . .	630
Безопасность . . . . .	630
Приложения Telnet . . . . .	631
Работа с другими службами TCP/IP через Telnet . . . . .	633
Итоги . . . . .	635
<b>Глава 29. Инструментарий удаленного доступа . . . . .</b>	<b>636</b>
R-команды . . . . .	636
R-команды и безопасность . . . . .	637
Запрет использования r-команд . . . . .	637
Альтернативы для r-команд . . . . .	640
Справочник r-команд . . . . .	641
Демоны r-команд . . . . .	641
rsh . . . . .	641
rcp . . . . .	642
rlogin . . . . .	642
rur . . . . .	643
ruptime . . . . .	643
rwho . . . . .	643
rexec . . . . .	644
Другие файлы . . . . .	644
Функциональность r-команд на других платформах . . . . .	646
Итоги . . . . .	647
<b>Глава 30. Протоколы совместного доступа к файловой системе: NFS и SMB/CIFS . . . . .</b>	<b>648</b>
Что такое NFS? . . . . .	648
Краткая история NFS . . . . .	649
Почему NFS? . . . . .	649
Реализация — как работает NFS . . . . .	649
RPC и XDR . . . . .	650
Жесткое и мягкое монтирование . . . . .	650
Файлы и команды NFS . . . . .	651
Демоны NFS . . . . .	651
Служебные файлы NFS . . . . .	654
Серверные команды NFS . . . . .	656
Создание общих ресурсов . . . . .	656
Отключение общих ресурсов . . . . .	658
Клиентские команды NFS . . . . .	659
Демонтирование ресурсов NFS . . . . .	661
Пример: организация совместного доступа и монтирование файловой системы NFS . . . . .	662

Распространенные проблемы NFS и их решения . . . . .	663
Ошибки при монтировании ресурсов . . . . .	663
Ошибки при демонтировании ресурсов . . . . .	664
Жесткое и мягкое монтирование . . . . .	664
Другие протоколы и продукты . . . . .	664
WebNFS . . . . .	665
PC-NFS и другие клиентские программы . . . . .	665
SMB и CIFS . . . . .	665
Другие продукты . . . . .	666
Итоги . . . . .	666
<b>Глава 31. Интеграция TCP/IP с прикладными службами . . . . .</b>	<b>667</b>
Применение браузера на представительском уровне . . . . .	668
Интеграция TCP/IP с унаследованными приложениями . . . . .	669
Использование TCP/IP в других сетях . . . . .	669
NetBIOS и TCP/IP . . . . .	670
IPX и UDP . . . . .	671
Итоги . . . . .	671
<b>Глава 32. Почтовые протоколы Интернета . . . . .</b>	<b>672</b>
Электронная почта . . . . .	672
История электронной почты . . . . .	672
Стандарты и их разработчики . . . . .	673
X.400 . . . . .	673
SMTP . . . . .	675
MIME и SMTP . . . . .	675
Другие стандарты кодировки двоичных данных . . . . .	676
Команды SMTP . . . . .	676
Коды состояния SMTP . . . . .	677
Расширение SMTP . . . . .	678
Заголовки SMTP . . . . .	679
Достоинства и недостатки SMTP . . . . .	679
Получение почты с применением POP и IMAP . . . . .	680
Протокол POP . . . . .	681
Протокол IMAP . . . . .	681
Сравнение POP3 с IMAP4 . . . . .	682
Нетривиальные возможности электронной почты . . . . .	683
Безопасность . . . . .	683
Спам и другие нежелательные сообщения . . . . .	686
Анонимный сервис электронной почты и пересылка . . . . .	686
Итоги . . . . .	687
<b>Глава 33. Служба HTTP . . . . .</b>	<b>688</b>
World Wide Web . . . . .	688
Краткая история Web . . . . .	688
Создатели и попечители Web . . . . .	688
Стремительное развитие Web . . . . .	689
Унифицированные указатели ресурсов . . . . .	689

Web-серверы и браузеры . . . . .	691
Протокол HTTP . . . . .	692
HTTP/1.1 . . . . .	692
MIME и Web . . . . .	695
Пример сеанса HTTP . . . . .	696
Нетривиальные возможности Web . . . . .	696
Средства, работающие на стороне сервера . . . . .	697
SSL и S-HTTP . . . . .	697
Языки Web . . . . .	697
Будущее Web . . . . .	701
HTTP-ng . . . . .	701
IIOP . . . . .	702
IPv6 . . . . .	702
IPP . . . . .	702
XML . . . . .	702
Итоги . . . . .	703
<b>Глава 34. Служба сетевых новостей и протокол NNTP . . . . .</b>	<b>704</b>
Usenet . . . . .	704
Конференции и иерархии . . . . .	705
Протокол NNTP . . . . .	707
Получение списка конференций . . . . .	708
Прием сообщений . . . . .	709
Отправка сообщений . . . . .	710
Спам и блокировка . . . . .	711
Итоги . . . . .	712
<b>Глава 35. Установка и настройка web-сервера . . . . .</b>	<b>713</b>
Принципы работы web-серверов . . . . .	713
Терминология web-серверов . . . . .	714
Популярные web-серверы . . . . .	716
Установка и запуск web-сервера Apache . . . . .	717
Загрузка, установка и настройка Apache . . . . .	717
Компиляция и установка Apache . . . . .	719
Настройка Apache . . . . .	720
Запуск и остановка Apache . . . . .	722
Загрузка двоичных файлов Apache . . . . .	723
Установка и настройка Apache в двоичном формате . . . . .	725
Использование Apache для Windows . . . . .	725
Другие web-серверы . . . . .	727
Итоги . . . . .	728
<b>Глава 36. Настройка и оптимизация протоколов в системах семейства Unix . . . . .</b>	<b>729</b>
Инициализация системы . . . . .	729
Процесс init и /etc/inittab . . . . .	729
Сценарии rc . . . . .	731

Конфигурационные файлы . . . . .	735
Определение сетевых протоколов в /etc/protocols . . . . .	735
Имена хостов в /etc/hosts . . . . .	736
Клиент DNS и файл /etc/resolv.conf . . . . .	742
Итоги . . . . .	743
<b>Глава 37. Реализация DNS . . . . .</b>	<b>744</b>
Серверы имен DNS . . . . .	744
Ресурсные записи . . . . .	745
Резольвер . . . . .	747
Настройка сервера DNS в Unix и Linux . . . . .	748
Ввод ресурсных записей . . . . .	748
Остальные файлы DNS . . . . .	749
Запуск демонов DNS . . . . .	754
Настройка клиента . . . . .	754
Windows и DNS . . . . .	754
Итоги . . . . .	755
<b>Глава 38. Управление сетью TCP/IP . . . . .</b>	<b>756</b>
Разработка плана сетевого мониторинга . . . . .	757
Анализ и диагностика сетевых проблем . . . . .	758
Средства управления сетью . . . . .	759
Анализаторы протоколов . . . . .	759
Экспертные системы . . . . .	761
Анализаторы на базе PC . . . . .	762
Поддержка протоколов управления сетью . . . . .	763
Интеграция со средствами сетевого моделирования . . . . .	764
Настройка SNMP . . . . .	765
Настройка SNMP в системе Windows . . . . .	765
Настройка SNMP в системе Unix . . . . .	767
Параметры безопасности SNMP . . . . .	768
Управление сетью и агенты SNMP . . . . .	768
Инструментарий и команды SNMP . . . . .	770
RMON и другие модули MIB . . . . .	771
Выработка требований . . . . .	772
Построение подробного списка информации . . . . .	772
Передача списка в службу поддержки . . . . .	772
Формулировка стратегии построения отчетов . . . . .	772
Определение показателей, используемых для оповещения об экстренных ситуациях (в реальном времени) . . . . .	772
Выбор информации для составления ежемесячных отчетов . . . . .	773
Выбор информации для оптимизации . . . . .	773
Обратная связь . . . . .	773
Реализация требований . . . . .	774
Оповещение служб поддержки . . . . .	774
Повторный анализ требований . . . . .	774



Информирование технической службы . . . . .	774
Пробные проверки . . . . .	774
Обучение технической службы . . . . .	774
Документирование диагностических процедур . . . . .	775
Упрощение систем управления элементами . . . . .	775
Использование искусственного интеллекта . . . . .	775
Итоги . . . . .	776
<b>Глава 39. Протокол управления сетью SNMP . . . . .</b>	<b>777</b>
Что такое SNMP? . . . . .	777
MIB . . . . .	779
Использование SNMP . . . . .	780
Unix и SNMP . . . . .	781
Настройка SNMP в Unix и Linux . . . . .	782
Команды SNMP . . . . .	783
Windows и SNMP . . . . .	784
Windows NT/2000 . . . . .	784
Windows 9x/ME . . . . .	786
Итоги . . . . .	789
<b>Глава 40. Безопасность передачи данных TCP/IP . . . . .</b>	<b>790</b>
Планирование сетевой безопасности . . . . .	790
Что такое сетевая безопасность? . . . . .	791
Почему важна сетевая безопасность? . . . . .	792
Уровни безопасности . . . . .	792
Пароли и файлы паролей . . . . .	793
Ограничение доступа к паролям . . . . .	794
Сетевая безопасность . . . . .	795
Типы атак . . . . .	795
Меры, обеспечивающие сетевую безопасность . . . . .	797
Настройка приложений . . . . .	799
Демон Интернета и файл /etc/inetd.conf . . . . .	799
Программы шифрования . . . . .	801
TCP Wrappers . . . . .	802
Порты . . . . .	803
Брандмауэры . . . . .	803
Пакетные фильтры . . . . .	804
Шлюзы приложений . . . . .	804
Приложения-фильтры . . . . .	804
Итоги . . . . .	804
<b>Глава 41. Инструментарий и методы диагностики . . . . .</b>	<b>805</b>
Наблюдение за состоянием сети . . . . .	805
Стандартные утилиты . . . . .	806
Проверка базового соединения . . . . .	806
Диагностика проблем на сетевом уровне . . . . .	810

Проверка маршрутов . . . . .	813
Проверка службы имен . . . . .	817
Диагностика сетевого интерфейса . . . . .	818
Диагностика на сетевом уровне (IP) . . . . .	819
Параметры конфигурации TCP/IP . . . . .	819
Диагностика проблем TCP и UDP . . . . .	825
Проблемы с сокетами . . . . .	825
Файл SERVICES . . . . .	826
Диагностика на прикладном уровне . . . . .	826
Проблемы разрешения имен . . . . .	827
Итоги . . . . .	827
<b>Приложение А. RFC и стандарты . . . . .</b>	<b>828</b>
Информационные ресурсы . . . . .	828
World Wide Web . . . . .	828
FTP . . . . .	829
Электронная почта . . . . .	829
Бумажные копии . . . . .	829
Тематический список полезных RFC . . . . .	829
Общие сведения . . . . .	830
TCP и UDP . . . . .	830
IP и ICMP . . . . .	830
Нижние уровни . . . . .	831
Загрузка . . . . .	831
DNS . . . . .	832
Пересылка и доступ к файлам . . . . .	832
Электронная почта . . . . .	832
Протоколы маршрутизации . . . . .	832
Политика и производительность маршрутизации . . . . .	833
Терминальный доступ . . . . .	833
Другие приложения . . . . .	834
Управление сетью . . . . .	835
Туннелирование . . . . .	835
OSI . . . . .	836
Безопасность . . . . .	836
Разное . . . . .	836
Список RFC по номерам . . . . .	836
<b>Приложение Б. Сокращения и акронимы . . . . .</b>	<b>837</b>
<b>Алфавитный указатель . . . . .</b>	<b>846</b>

# 2 TCP/IP и Интернет

*Нил Джеймисон (Neal S. Jamison)*

Благодаря протоколу TCP/IP Интернет стал тем, чем он является сегодня. В результате Интернет произвел в нашем стиле жизни и работы почти такие же революционные изменения, как печатный станок, электричество или компьютер. Настоящая глава посвящена истории Интернета, его попечителям и перспективам будущего развития. В ней рассматривается процесс превращения идей в стандарты, а также кратко представлены некоторые популярные протоколы и службы, в том числе Telnet и HTTP.

## История Интернета

История Интернета начинается с незапамятных времен. Рисунки на стенах пещер, дымовые сигналы, голубиная почта — все эти виды связи наводили наших предков на мысль, что должны существовать более совершенные способы. Затем появился телеграф, телефон и трансатлантическая беспроводная связь... и это уже было на что-то похоже. Потом были изобретены первые компьютеры — громадные устройства, выделяющие уйму тепла. По своей вычислительной мощности они уступали любому современному карманному калькулятору, однако эти гиганты помогали выигрывать войны и использовались при переписи населения. Впрочем, их было очень мало, никто не мог себе купить личный компьютер и уж тем более — установить его дома.

В 1960-х годах на смену электронным лампам пришли транзисторы, размеры и стоимость компьютеров начали падать, а интеллект и вычислительная мощность этих машин стали расти. В это время группа ученых уже начала работать над проблемой взаимодействия компьютеров. Леонард Клейнрок (Leonard Kleinrock), в те времена аспирант MIT, предложил концепцию технологии коммутации пакетов и опубликовал статью на эту тему в 1961 году. Тогда же Управление перспективного планирования научно-исследовательских работ ARPA (Advanced Research Project Agency) разрабатывало для себя (и для военных) новую систему связи, и работа Клейнрока дала необходимый импульс. ARPA объявило конкурс

на создание первой сети с пакетной коммутацией. Контракт достался небольшой фирме BBN (Bolt Beranek and Newman) из Массачусетса, занимавшейся акустикой. Так родилась сеть ARPANET. Это произошло в 1969 году.

## ARPANET

Исходная сеть ARPANET состояла всего из четырех хостов — по одному в Калифорнийском университете Лос-Анджелеса, в Стэнфордском научно-исследовательском институте, в университете Санта-Барбары и университете штата Юта. Эта маленькая сеть на базе протокола NCP (Network Control Protocol) позволяла своим пользователям регистрироваться на удаленных хостах, осуществлять печать на удаленном принтере и передавать файлы. В 1971 году Рэй Томлинсон (Ray Tomlinson), инженер из BBN, написал первую программу для работы с электронной почтой.

## TCP/IP

В 1974 году, всего через пять лет после рождения ARPANET, Винтон Серф (Vinton Cerf) и Роберт Кан (Robert Kahn) разработали протокол управления передачей *TCP* (Transmission Control Protocol). В начале 1980-х годов протокол TCP/IP, спроектированный с расчетом на независимость от базового компьютера и сети, заменил ограниченный протокол NCP, что позволило организовать взаимодействие с другими разнородными ARPANET-подобными сетями (интернетами). Так родился Интернет.

### ПРИМЕЧАНИЕ

Термин «интернет» (со строчной буквы «и») обозначает сеть, состоящую из разнородных компьютеров. Интернет (с прописной буквы «И») — ТА САМАЯ Сеть, объединяющая миллионы компьютеров и пользователей.

Распространению TCP/IP способствовало Министерство обороны, которое выбрало TCP/IP своим стандартным протоколом и потребовало его обязательного использования фирмами-подрядчиками. Примерно в то же время разработчики из Калифорнийского университета (Беркли) выпустили новую разновидность операционной системы Unix, 4.2BSD (Berkeley Software Distribution), которая распространялась бесплатно. Этот факт благотворно отразился на протоколе TCP/IP, плотно интегрированном с 4.2BSD. Версия BSD Unix была заложена в основу других систем семейства Unix, что объясняет господство TCP/IP в мире Unix.

Протокол TCP/IP обеспечил надежность связи, необходимую для начального развития Интернета, а ученые и инженеры начали включать в семейство TCP/IP новые протоколы и приложения. FTP, Telnet и SMTP поддерживались с самого начала. К числу новых пополнений семейства TCP/IP относятся IMAP (Internet Mail Access Protocol), POP (Post Office Protocol) и, конечно, HTTP.

## NSF

Исключительно важная роль в становлении Интернета также принадлежит сети NSFNet. Национальный научный фонд NSF (National Science Foundation) оценил важность работ по созданию ARPANET и решил создать собственную сеть. Сеть NSFNet соединяла несколько суперкомпьютеров, установленных в университетах и правительственных учреждениях. Популярность сети росла, и в NSF решили увеличить ее возможности за счет модернизации магистральных каналов связи. Сеть NFSNet начиналась с линий со скоростью 56 кбит/с, перешла на линии T-1 (1,544 Мбит/с), затем на T-3 (43 Мбит/с) и вскоре стала самым быстрым интернетом того времени.

На этом временном отрезке также создавались и другие сети, в том числе BITNET (Because It's Time Network) и CSNET (Computer Science Research Network). Сеть ARPANET продолжала расти невероятными темпами, с удвоением количества хостов за каждый год.

В конце 1980-х и начале 1990-х годов сеть NFSNet заменила старую и более медленную сеть ARPANET и стала официальной опорной сетью Интернета.

## Интернет сегодня

В 1992 году Европейская организация ядерных исследований CERN (Conseil Européen pour la Recherche Nucleaire) и Тим Бернерс-Ли (Tim Berners-Lee) выдвинули концепцию «Всемирной паутины» WWW (World Wide Web). Через год была выпущена клиентская программа WWW, которая называлась Mosaic. Эти два события превратили Интернет из текстовой среды, использовавшейся преимущественно учеными и студентами, в графическую среду, которая сегодня используется многими миллионами людей.

В апреле 1995 года сеть NFSNet была заменена более современной, коммерческой опорной сетью. В результате ограничения на подключения к хостам в Интернете были снижены и появился совершенно новый тип пользователей — коммерческий пользователь.

Протокол PPP (Point-to-Point Protocol) был создан в 1994 году, а в 1995 году он получил повсеместное распространение. PPP позволял использовать TCP/IP в телефонных линиях, что облегчало доступ в Интернет для домашних пользователей. В то же время стали появляться *поставщики услуг Интернета* (ISP, Internet Service Providers), которые обеспечивали подключение к Интернету домашних пользователей и организаций. Это привело к бурному росту количества домашних пользователей.

Интернет развивался (и продолжает развиваться!) ошеломляющими темпами — до 100 процентов в год.

В наши дни даже поверхностное знакомство с WWW наглядно показывает важность эволюции Интернета. Использование Интернета вышло за рамки академических и оборонных коммуникаций и научных исследований. Сейчас в Интернете можно покупать товары и выполнять банковские операции, а Web откры-

вает доступ к всевозможной информации, от кулинарных рецептов до текстов книг. Перспективы использования Интернета безграничны.

## RFC и процесс стандартизации

В процессе эволюции Интернета новые идеи и комментарии представлялись в виде документов, называемых *запросами на комментарии*, или RFC (Requests for Comments). В этих документах обсуждаются многие аспекты коммуникаций, связанных с Интернетом. Первый документ RFC (RFC 1) назывался «Host Software» и был написан в апреле 1969 года Стивом Крокером (Steve Crocker), аспирантом Калифорнийского университета в Лос-Анджелесе и автором восьми из первых 25 RFC. Тексты первых RFC чрезвычайно интересны для всех, кто интересуется историей Интернета. Спецификации протоколов Интернета, определяемые IETF и IESG, также публикуются в форме RFC.

Редактором RFC называется лицо, публикующее RFC и отвечающее за окончательное рецензирование документов. Роль редактора обсуждается ниже в этой главе.

Хорошим источником информации обо всех типах RFC является сайт <http://www.rfc-editor.org/>.

### ПРИМЕЧАНИЕ

Джон Постел (Jon Postel) внес важный вклад в создание ARPANET, а следовательно, и в создание Интернета. Он участвовал в создании системы доменных имен Интернета и в течение многих лет занимался ее администрированием; эта система продолжает использоваться и сейчас. Джон возглавлял Агентство по выделению имен и параметров протоколов Интернета IANA (Internet Assigned Numbers Authority) и был редактором RFC. Джон скончался в октябре 1998 года. Его памяти был посвящен RFC 2468 (Винтон Серф, октябрь 1998 года).

Документы RFC являются основным средством распространения новых идей в области протоколов, исследований и стандартов. Если исследователь хочет предложить новый протокол, научную работу или учебник по некоторой теме, он оформляет их в виде документа RFC. Таким образом, к числу RFC принадлежат описания стандартов Интернета, предложения по пересмотру старых и внедрению новых протоколов, описания стратегий реализации, учебники, сборники полезной информации и т. д.

Протоколы, которым суждено стать стандартами Интернета, проходят несколько стадий в соответствии со степенью завершенности: предложенный стандарт, проект стандарта и стандарт. По мере развития стандарта объемы аналитических и тестовых данных растут. После завершения этого процесса протоколу присваивается определенное число STD, то есть номер нового стандарта.

По мере совершенствования технологий некоторые протоколы заменяются своими улучшенными версиями или перестают использоваться. Такие протоколы помечаются как «исторические» («historic»). В некоторых RFC документируются результаты анализа и разработки новых протоколов, которые помечаются как «экспериментальные» («experimental»).

Протоколы, разработанные другими стандартизирующими организациями, конкретными фирмами-поставщиками или частными лицами, также могут представлять интерес и рекомендоваться для применения в Интернете. Спецификации таких протоколов также публикуются в виде RFC для удобства и простоты распространения в Интернет-сообществе. Такие протоколы помечаются как «информационные» («informational»).

Иногда протоколы получают широкое распространение без одобрения или участия IESG. В частности, это может быть связано с эволюцией протоколов по маркетинговым или политическим причинам. Некоторые из этих протоколов даже начинают играть важную роль в Интернет-сообществе, поскольку коммерческие организации используют их в своих интрасетях. Согласно официальной позиции IAB, при эволюции протоколов рекомендуется использовать процесс стандартизации; тем самым обеспечивается максимальный уровень совместимости и предотвращается возникновение конфликтных требований к протоколам.

Не все протоколы должны быть обязательно реализованы во всех системах, потому что из-за огромного разнообразия существующих систем в некоторых случаях реализация протоколов не имеет смысла. Например, к таким устройствам Интернета, как шлюзы, маршрутизаторы, терминальные серверы, рабочие станции и многопользовательские хосты, предъявляются совершенно разные требования. Не для всех из них нужны одни и те же протоколы.

## Источники информации о RFC

Тексты RFC хранятся в нескольких архивах. Возможно, поиски следует начинать с индекса RFC. Список индексов приведен в следующем разделе.

Существует несколько способов получения RFC: Web, FTP, Telnet и даже электронная почта. В табл. 2.1 перечислены некоторые архивы RFC, доступные через FTP.

**Таблица 2.1.** Архивы RFC, доступные через FTP

Сайт	Имя/Пароль/Каталог
ftp.isi.edu	anonymous/name@host.domain/in-notes
wuarchive.wustl.edu	anonymous/name@host.domain/doc/rfc

Некоторые архивы также рассылают RFC по электронной почте. Например, вы можете отправить сообщение по адресу [nis-info@nis.nsf.net](mailto:nis-info@nis.nsf.net) с пустой строкой темы и текстом «send rfcnnn.txt», где *nnnn* — номер нужного RFC.

Как и следовало предполагать, многие архивы также предоставляют доступ к документам через Web. Если вы захотите воспользоваться этой возможностью, поиски можно начать с сайта <http://www.rfc-editor.org>.

За дополнительной информацией о получении RFC обращайтесь по адресу <http://www.isi.edu/in-notes/rfc-retrieval.txt>.

## Индексы RFC

Полный индекс документов RFC занимает слишком много места, чтобы приводить его здесь. Впрочем, в Web представлены индексы в форматах ASCII, HTML и в специальном поисковом формате. Ниже перечислены некоторые примеры:

- Текстовый формат: <ftp://ftp.isi.edu/in-notes/rfc-index.txt>.
- HTML: <ftp://ftpeng.cisco.com/fred/rfc-index/rfc.html>.
- HTML by Protocol: <http://www.garlic.com/~lynn/rfcprot.htm>.

По адресу <http://www.rfc-editor.org/rfcsearch.html> находится поисковый механизм RFC.

## Краткое знакомство со службами Интернета

Без популярных протоколов и служб — таких, как HTTP, SMTP и FTP — Интернет был бы просто большим количеством компьютеров, связанных в бесполезный клубок. В этом разделе кратко описаны самые распространенные (и самые полезные) протоколы Интернета со ссылками на главы, в которых вы найдете дополнительную информацию.

### Whois и Finger

Служба и протокол Whois предназначены для получения информации о хостах и доменах Интернета. Обращаясь с запросом к любому из серверов баз данных Whois, клиенты Whois могут получить разнообразные сведения — контактные данные узлов и доменов, географические адреса и т. д. Whois используется в некоторых организациях (особенно в университетах) в качестве электронного каталога персонала.

Whois находится на хорошо известном порте TCP с номером 43. Подробное описание приведено в RFC 954.

Служба/протокол Finger предназначены для сбора информации о пользователе Интернета. В частности, вы можете узнать адрес электронной почты пользователя, определить, имеются ли у него непрочитанные сообщения и подключен ли он к Интернету в данный момент, и даже получить частичную информацию о том, над чем он в данный момент работает. Ввиду специфики этой службы некоторые администраторы предпочитают отключать ее на своих хостах. Finger ведет прослушивание на порту TCP с номером 79, а подробное описание приведено в RFC 1288.

За дополнительной информацией об этих службах обращайтесь к главе 29.

### FTP

Служба/протокол *FTP* (File Transfer Protocol) обеспечивает пересылку файлов по Интернету. Протокол FTP также относится к числу ранних протоколов, он появился еще в 1971 году. В наше время FTP повсеместно используется для



предоставления открытого доступа к файлам (через анонимный вход). Протокол FTP работает на хорошо известных портах TCP с номерами 20 и 21. Подробное описание приведено в RFC 959.

За дополнительной информацией о FTP и других протоколах пересылки файлов обращайтесь к главе 30.

## Telnet

Программа Telnet предназначена для эмуляции терминала в Интернете. Проще говоря, Telnet позволяет регистрироваться на удаленных хостах, не беспокоясь о совместимости терминалов. Telnet также принадлежит к числу самых первых протоколов и служб раннего Интернета (см. RFC 15). Telnet работает на хорошо известном порте TCP с номером 23. Подробное описание приведено в RFC 854.

За дополнительной информацией о Telnet обращайтесь к главе 31.

## Электронная почта

Протокол *SMTP* (Simple Mail Transfer Protocol) определяет Интернет-стандарт для работы с электронной почтой. Многие пользователи ежедневно используют этот протокол, даже не осознавая этого. SMTP дополняется другими протоколами и службами (такими, как POP3 и IMAP4), позволяющими выполнять операции с сообщениями на почтовом сервере и загружать их на локальный компьютер для чтения. Протокол SMTP работает на хорошо известном порте TCP с номером 25. Подробное описание приведено в RFC 821.

За дополнительной информацией о SMTP, а также других протоколах и службах для работы с электронной почтой обращайтесь к главе 35.

## World Wide Web

Протокол HTTP заложен в основу работы World Wide Web. В сущности, именно HTTP принадлежит основная заслуга в бурном развитии Интернета в середине 1990-х годов. Сначала появились первые клиенты HTTP (такие, как Mosaic и Netscape), которые позволяли наглядно «увидеть» Web. Вскоре стали появляться web-серверы с полезной информацией. В наше время в Интернете существует более шести миллионов web-сайтов, работающих на базе HTTP. Протокол HTTP работает на хорошо известном порте TCP с номером 80, а подробное описание его текущей версии, HTTP/1.1, приведено в RFC 2616.

За дополнительной информацией о HTTP, а также других протоколах и службах для работы в Web обращайтесь к главе 36.

## Usenet

Служба/протокол *NNTP* (Network News Transfer Protocol) обеспечивает публикацию, прием и пересылку новостей Usenet. Несомненно, Usenet — явление историческое. Это доска объявлений в масштабе Интернета, состоящая из конфе-

ренций (newsgroups) — форумов, в которых обсуждаются всевозможные темы. Протокол NNTP работает на хорошо известном порте TCP с номером 119, а его подробное описание приведено в RFC 977.

За дополнительной информацией о NNTP обращайтесь к главе 31.

## Интрасети и экстрасети

После произошедшей в 1991 году коммерциализации Интернета корпорации довольно быстро открыли новые возможности использования Интернета, его служб и технологий для экономии времени и денег, а также для получения стратегических преимуществ. Одним из самых масштабных применений этой технологии в наши дни стали интрасети.

### Интрасети

*Интрасетью* (intranet) называется корпоративная локальная сеть, в которой основным коммуникационным протоколом является TCP/IP. Прикладные службы интрасетей основаны на стандартных службах Интернета — HTTP, FTP, TELNET, SSH и т. д.

Проще говоря, интрасеть представляет собой конечную, замкнутую сеть, использующую технологии Интернета для совместного использования данных. Интрасеть может быть подключена к Интернету с установлением контрольных механизмов, предотвращающих несанкционированный доступ. Впрочем, интрасеть может вообще не иметь выхода в Интернет.

### Преимущества интрасетей

Корпоративные интрасети обладают многими преимуществами. Относительно низкая стоимость реализации и сопровождения обеспечивает компаниям очень высокий уровень прибыли на инвестированный капитал. Среди основных преимуществ интрасетей стоит выделить следующие:

- **Интрасети просты в использовании.** Пользовательский интерфейс интрасетей основан на обычном web-браузере, поэтому затраты на обучение персонала близки к нулю.
- **Интрасети упрощают доступ работников к информации.** Интрасети позволяют чрезвычайно эффективно организовать доступ работников к необходимой информации, будь то одностраничный служебный меморандум или 500-страничный телефонный справочник.
- **Интрасети снижают затраты на подготовку печатных материалов.** Распространение информации в крупной компании или организации традиционно считалось не только организационно сложной, но и очень дорогой задачей.
- **Интрасети расширяют возможности традиционных документов.** Найти имя или название товара в бумажном справочнике или каталоге не так уж сложно,

однако этот процесс часто бывает утомительным и занимающим много времени.

- **Интрасети повышают актуальность данных.** После вывода на печать документ может устареть. Таким образом, возникает опасность распространения копий устаревших и, возможно, — недостоверных документов.

Приведенный список не исчерпывает всех преимуществ интрасетей. Компании, установившие у себя интрасети, открыли для себя гораздо больше новых возможностей, чем перечислено выше. А при использовании таких Интернет-технологий и служб, как браузеры и web-серверы с открытыми исходными текстами, все эти преимущества удастся реализовать с относительно низкими затратами.

## Области применения интрасетей

Возможности применения интрасетей, повышающие эффективность и производительность труда в организациях, практически безграничны. Ниже перечислены некоторые популярные области применения интрасетевых технологий.

- **Управление кадрами.** Многие компании распространяют объявления о вакансиях, ведут базы данных с информацией о сотрудниках, распространяют всевозможные документы вроде анкет, табельных листков, отчетов о затратах и даже уведомлений о перечислении зарплаты на счет — и все это делается при помощи интрасетей.
- **Управление проектами.** Руководители проектов могут просматривать и обновлять электронные таблицы и графики Гантта, опубликованные в интрасети. Отчеты о состоянии проекта тоже могут публиковаться в интрасети для их просмотра и рецензирования руководителями.
- **Инвентаризационный учет.** Публикация инвентарных баз данных в электронном виде с доступом либо на уровне собственных форматов данных, либо через специальные приложения.
- **Управление файлами.** После установки мощного сервера интрасети, работающего на базе web-технологий, надобность в старом файловом сервере отпадет.

Интрасети удобны для корпоративных пользователей, однако предоставление доступа к корпоративным интрасетям внешним клиентам тоже приносит пользу. Так появились экстрасети, описанные в следующем разделе.

## Предоставление внешнего доступа к интрасети

Интрасети предназначены для совместного использования информации в рамках компании или организации. Следующим шагом в развитии этой идеи стали экстрасети. *Экстрасеть* (extranet) представляет собой интрасеть, предоставляющую контролируемый доступ определенной группе внешних пользователей. На практике экстрасети используются для обмена информацией со стратегическими партнерами (клиентами, поставщиками или службами доставки). Короче говоря, экстрасети относятся к сетям класса «бизнес-бизнес».

Некоторые области применения экстрасетей:

- проведение деловых операций на базе *EDI* (Electronic Data Interchange) или других технологий;
- взаимодействие с другими организациями в работе над совместными проектами;
- обмен новостями или другой информацией с партнерами.

Пример: крупная компания, занимающаяся доставкой товаров, может предоставить торговой компании доступ к своей интрасети, чтобы торговая компания могла согласовать данные о сроках поставки со своими покупателями.

## Будущее Интернета

По мере роста популярности и расширения областей практического применения Интернета совершенствуются и интернет-технологии. В настоящее время существует ряд проектов, направленных на улучшение этих технологий. Наиболее перспективными являются следующие проекты:

- NGI (Next Generation Internet);
- vNBS (Very high-speed Backbone Network Service);
- Internet2 (I2).

Все эти проекты более подробно рассматриваются в следующих подразделах.

### NGI (Next Generation Internet)

Как сообщил президент Клинтон в своем докладе о положении страны в 1998 году, инициатива Интернета следующего поколения *NGI* (Next Generation Internet) обеспечивает финансирование и координацию работы академических и федеральных учреждений, направленных на финансирование и построение интернет-сервиса следующего поколения.

За дополнительной информацией об инициативе NGI обращайтесь на сайт <http://www.ngi.gov>.

### vBNS

Национальный научный фонд начал работу над созданием экспериментальной опорной сети с огромной скоростью передачи данных. Этой опорной сети, оператором которой является MCI WorldCom, было присвоено название *vBNS* (Very high-speed Backbone Network Service). В ближайшем будущем vBNS послужит платформой для тестирования новых, высокоскоростных интернет-технологий и протоколов. В настоящее время сеть соединяет несколько суперкомпьютерных центров и точек доступа к сети на скоростях OC-12 (622 Мбит/с) и выше. В феврале 1999 года компания MCI WorldCom объявила об установке канала связи OC-48 (2,5 Гбит/с) между Лос-Анджелесом и Сан-Франциско.

Обращайтесь на сайт <http://www.vbns.net> за дополнительной информацией о vBNS.

## Internet2 (I2)

Испытательная сеть *Internet2* была создана для того, чтобы университеты, правительственные и промышленные организации могли совместно разрабатывать новые интернет-технологии. Партнерские организации связывались высокоскоростной сетью Abilene (до 9,6 Гбит/с). В I2 также задействована сеть vBNS, упомянутая в предыдущем разделе.

Обращайтесь на сайт <http://www.internet2.edu> за дополнительной информацией о I2. Информация о сети Abilene находится по адресу <http://www.ucaid.edu/abilene>.

## Так кто же главный в Интернете?

Огромные масштабы Интернета и множество высокотехнологичных инициатив, направленных на его совершенствование, наводят на мысль, что группа, ответственная за Интернет, трудится не покладая рук. Это не совсем так: никакой группы, «ответственной» за Интернет, не существует. У Интернета нет директора, главного администратора или даже президента. Оказывается, Интернет процветает в условиях анархической, неофициальной культуры 1960-х, в которых он был рожден. Тем не менее существует ряд групп, которые помогают следить за развитием технологий Интернета, за процессами регистрации и общими проблемами, связанными с управлением сетью таких огромных масштабов.

## ISOC (Internet Society)

Общество Интернета *ISOC* (Internet Society) объединяет на профессиональной основе свыше 150 организаций и 6000 физических лиц из более 100 стран мира. Эти организации и лица совместно решают вопросы, от которых зависит нормальная работа Интернета и его будущее. ISOC состоит из нескольких групп, отвечающих за стандарты инфраструктуры Интернета, в том числе IAB (Internet Architecture Board) и IETF (Internet Engineering Task Force).

Web-сайт ISOC находится по адресу <http://www.isoc.org>.

## IAB (Internet Architecture Board)

Координационный совет по архитектуре Интернета IAB (Internet Architecture Board) выполняет функции технического советника при Обществе Интернета. Эта небольшая группа (кандидаты в члены IAB представляются IETF и одобряются Советом попечителей ISOC) проводит регулярные заседания, на которых рассматриваются и вносятся новые идеи и предложения для последующей разработки в IETF и IESG.

Web-сайт IAB находится по адресу <http://www.iab.org>.

## IETF (Internet Engineering Task Force)

Проблемная группа проектирования Интернета IETF (Internet Engineering Task Force) является открытым сообществом сетевых проектировщиков, поставщиков и ученых, работающих над развитием Интернета. IETF проводит заседания только три раза в год, а большая часть работы выполняется через электронные списки рассылки. IETF делится на несколько рабочих групп, каждая из которых занимается определенной темой. К числу рабочих групп IESG принадлежат группы разработчиков *HTTP* (Hypertext Transfer Protocol) и *IPP* (Internet Printing Protocol).

Группа IETF открыта для всех желающих. Ее web-сайт находится по адресу <http://www.ietf.org>.

## IESG (Internet Engineering Steering Group)

Исполнительный комитет IETF — IESG (Internet Engineering Steering Group) — отвечает за техническое руководство деятельностью IETF и процессом выработки новых стандартов Интернета. IESG также следит за соблюдением правил ISOC в деятельности IETF. Кроме того, IESG окончательно утверждает спецификации перед тем, как они принимаются в качестве стандартов Интернета.

За дополнительной информацией о IESG обращайтесь по адресу <http://www.ietf.org/iesg.html>.

## IANA (Internet Assigned Numbers Authority)

Агентство по выделению имен и параметров протоколов Интернета IANA (Internet Assigned Numbers Authority) отвечает за назначение IP-адресов и управление пространством имен доменов. IANA также определяет номера портов протокола IP и другие параметры. Деятельность IANA осуществляется под патронажем ICANN.

Web-сайт IANA находится по адресу <http://www.iana.org>.

## ICANN (Internet Corporation for Assigned Names and Numbers)

Корпорация по выделению имен и параметров протоколов Интернета ICANN (Internet Corporation for Assigned Names and Numbers) создавалась как часть проекта по переводу администрирования доменных имен и пространства IP-адресов на интернациональную основу. Основной целью ICANN является перевод администрирования доменов и IP-адресов из правительственного в частный сектор. В настоящее время ICANN участвует в работе над системой SRS (Shared Registry System), благодаря которой процесс регистрации доменных имен должен стать открытым для честной конкуренции. Дополнительная информация о SRS приводится в следующем разделе.

За дополнительной информацией о ICANN обращайтесь по адресу <http://www.icann.org>.

## InterNIC и другие регистрирующие органы

Информационный центр Интернета InterNIC (Internet Network Information Center), работающий под управлением Network Solutions, Inc., был основным регистратором доменов верхнего уровня (.com, .org, .net, .edu) с 1993 года. Надзор за деятельностью InterNIC осуществляется Национальной администрацией по телекоммуникациям и информации NTIA (National Telecommunications & Information Administration), подгруппой Министерства торговли. InterNIC передал часть полномочий другим официальным регистрирующим органам (таким, как информационные центры Министерства обороны и Азиатско-тихоокеанского региона). В последнее время появились новые инициативы, направленные на дальнейшее разделение полномочий InterNIC. Одна из таких инициатив, SRS (Shared Registry System), направлена на внесение открытой и честной конкуренции в процесс регистрации доменов. В настоящее время свыше 60 компаний выполняют регистрирующие функции в рамках этой инициативы.

Основные регистрирующие органы перечислены в табл. 2.2.

**Таблица 2.2.** Основные регистрирующие органы Интернета

Имя	URL
InterNIC	<a href="http://www.internic.net/">http://www.internic.net/</a>
Информационный центр Министерства обороны	<a href="http://nic.mil">http://nic.mil</a>
Федеральный регистр США	<a href="http://nic.gov">http://nic.gov</a>
Информационный центр Азиатско-тихоокеанского региона	<a href="http://www.apnic.net">http://www.apnic.net</a>
RIPE (Rйseaux IP Europeйns)	<a href="http://www.ripe.net">http://www.ripe.net</a>
Совет регистрирующих органов (CORE, Council of Registrars)	<a href="http://www.corenic.org/">http://www.corenic.org/</a>
Register.com	<a href="http://register.com">http://register.com</a>

## Редактор RFC

Запросы на комментарии (RFC) представляют собой серию документов, которые, среди прочего, определяют стандарты Интернета. Дополнительная информация о RFC приведена в разделе «RFC и процесс стандартизации» выше в этой главе.

Редактором RFC называется лицо, публикующее RFC и отвечающее за окончательное рецензирование документов.

За дополнительной информацией о редакторе RFC обращайтесь на сайт <http://www.rfc-editor.org/>.

## Поставщики услуг Интернета

Коммерциализация Интернета в 1990 году была радостно встречена многочисленными поставщиками услуг Интернета, которые горели желанием приобщить к Интернету миллионы домашних пользователей и организаций. Поставщиком услуг Интернета, или *ISP* (Internet Service Provider), называется коммерческая

организация, которая устанавливает интернет-серверы в своих офисах или машинных залах. Серверы оснащаются модемами и обеспечивают поддержку протоколов PPP (Point-to-Point Protocol) или SLIP (Serial Line Internet Protocol), при помощи которых удаленные пользователи подключаются со своих персональных компьютеров к Интернету.

Поставщики услуг Интернета на коммерческой основе предоставляют удаленным пользователям доступ к Интернету. Большинство поставщиков также предоставляет учетную запись электронной почты на своем сервере, а некоторые даже открывают доступ к командному процессору системы Unix.

Более крупные поставщики обеспечивают коммерческие организации и других поставщиков высокоскоростными средствами связи (ISDN, усеченными каналами T-1 и даже выше).

## Итоги

В этой главе рассматривалась история Интернета, путь его развития и другие сопутствующие темы. Также она дает краткое представление о современном использовании интернет-технологий, интрасетях и экстрасетях.

Описание процесса стандартизации на базе RFC сопровождается ссылками, по которым вы найдете тексты RFC для дальнейшего изучения.

Также были описаны самые популярные службы Интернета со ссылками на последующие главы книги, содержащие дополнительную информацию.

Вы познакомились с организациями, которые привели Интернет к его современному состоянию и продолжают развивать его в соответствии с изменениями в технологиях и потребностях пользователей. Трудно предсказать, что ждет Интернет в будущем. Всего за несколько лет Интернет вырос из крошечной экспериментальной сети, использовавшейся немногочисленными учеными, в глобальную сеть с миллионами компьютеров и пользователей. Уверенно можно сказать только одно: с такими проектами, как NGI, I2 и vBNS, мы еще только начинаем видеть потенциальные возможности и области практического применения этой пленительной технологии.