

Содержание

О соавторах	33
Об авторах	34
Памяти Эви	35
Предисловие	36
Организация книги	36
Авторы	37
Контактная информация	37
Введение	38
Благодарности	39
От издательства	40
Часть I. Основы администрирования	41
Глава 1. С чего начать	43
1.1. Основные обязанности системного администратора	44
Управление доступом	44
Добавление оборудования	44
Автоматизация задач	44
Управление резервными копиями	44
Установка и обновление программного обеспечения	45
Мониторинг	45
Исправление проблем	45
Ведение локальной документации	45
Бдительный мониторинг безопасности	46
Настройка производительности	46
Разработка правил	46
Работа с поставщиками	46
Тушение пожаров	46
1.2. Предварительный опыт	47
1.3. Дистрибутивы Linux	48
1.4. Примеры систем, используемых в этой книге	49
Примеры дистрибутивов Linux	50
Пример дистрибутива UNIX	51
1.5. Обозначения и типографские соглашения	52
1.6. Единицы измерения	53
1.7. Man-страницы и другая онлайн-документация	54
Организация man-страниц	54
Команда man: чтение страниц интерактивного руководства	55
Хранение страниц интерактивного руководства	55
1.8. Другая официальная документация	56
Руководства по конкретным системам	56
Документация по конкретным пакетам	56

Книги	57
Документы RFC	57
1.9. Другие источники информации	57
Сохранение актуальности	58
Практические руководства и справочные сайты	58
Конференции	59
1.10. Способы поиска и установки программного обеспечения	60
Как определить, установлено ли программное обеспечение	60
Добавление нового программного обеспечения	61
Создание программного обеспечения из исходного кода	63
Установка с помощью веб-сценария	64
1.11. Где разместить программное обеспечение	65
1.12. Специализация и смежные дисциплины	66
Методология DevOps	66
Инженеры по надежности сайтов	66
Инженеры по безопасности	66
Сетевые администраторы	66
Администраторы баз данных	67
Инженеры центра сетевых операций	67
Технические специалисты центров обработки данных	67
Архитекторы	67
1.13. Литература	67
Системное администрирование и методология DevOps	68
Важные инструменты	68
Глава 2. Загрузка и системные демоны	69
2.1. Обзор процесса загрузки	69
2.2. Системные прошивки	70
BIOS или UEFI	71
Устаревший интерфейс BIOS	72
UEFI	72
2.3. Загрузчики	74
2.4. GRUB: универсальный загрузчик	74
Конфигурация GRUB	74
Командная строка GRUB	76
Параметры ядра Linux	76
2.5. Процесс загрузки FreeBSD	77
Вариант BIOS: boot0	77
Вариант UEFI	78
Конфигурация загрузчика	78
Команды загрузчика loader	79
2.6. Демоны управления системой	79
Обязанности демона init	80
Реализации демона init	80
Традиционный стиль init	81
Менеджер systemd против остального мира	82
Аргументы против init	82

2.7. Менеджер <code>systemd</code> в деталях	83
Модули и модульные файлы	83
Команда <code>systemctl</code> : управление менеджером <code>systemd</code>	84
Состояние модуля	85
Цели	87
Зависимости между модулями	88
Порядок выполнения	90
Более сложный пример файла	90
Локальные службы и настройки	91
Предостережения об управлении службами и запуском	92
Журнал <code>systemd</code>	94
2.8. Сценарии инициализации и запуска системы FreeBSD	95
2.9. Процедуры перезагрузки и выключения	96
Выключение физических систем	97
Выключение облачных систем	97
2.10. Что делать, если система не грузится?	97
Однопользовательский режим	98
Однопользовательский режим в системе FreeBSD	99
Однопользовательский режим с загрузчиком GRUB	100
Восстановление облачных систем	100
Глава 3. Управление доступом и привилегии суперпользователя	103
3.1. Стандартное управление доступом в UNIX	104
Контроль доступа к файловой системе	104
Владение процессом	105
Учетная запись суперпользователя <code>root</code>	106
Установка флагов <code>setuid</code> и <code>setgid</code>	106
3.2. Управление учетной записью <code>root</code>	107
Вход в учетную запись <code>root</code>	107
Команда <code>su</code> : замена идентификатора пользователя	108
Программа <code>sudo</code> : ограниченный вариант команды <code>su</code>	108
Отключение учетной записи <code>root</code>	115
Системные учетные записи, отличные от <code>root</code>	116
3.3. Расширения стандартной модели контроля доступа	117
Недостатки стандартной модели	118
PAM: подключаемые модули аутентификации	118
Kerberos: сетевая криптографическая аутентификация	119
Списки управления доступом к файловой системе	119
Возможности Linux	120
Пространства имен Linux	120
3.4. Современный контроль доступа	121
Отдельные экосистемы	121
Обязательный контроль доступа	122
Контроль доступа на основе ролей	123
SELinux: улучшенная безопасность Linux	123
AppArmor	125
3.5. Литература	126

Глава 4. Управление процессами	127
4.1. Компоненты процесса	127
Идентификатор процесса PID	128
Идентификатор родительского процесса PPID	128
Идентификатор пользователя UID и текущий идентификатор пользователя EUID	129
Идентификатор группы (GID) и текущий идентификатор группы (EGID)	129
Фактор уступчивости	130
Управляющий терминал	130
4.2. Жизненный цикл процесса	130
Сигналы	131
Команда kill: отправка сигналов	133
Состояния процессов и потоков	134
4.3. Команда ps: текущий контроль процессов	135
4.4. Интерактивный мониторинг процессов с помощью команды top	137
4.5. Команды nice и renice: изменение приоритета выполнения	139
4.6. Файловая система /proc	140
4.7. Команды strace и truss: отслеживание сигналов и системных вызовов	141
4.8. Процессы, вышедшие из-под контроля	143
4.9. Периодические процессы	145
Демон cron: команды расписания	145
Системные таймеры	150
Общее использование запланированных задач	153
Глава 5. Файловая система	155
5.1. Имена путей	157
5.2. Монтирование и демонтаж файловой системы	157
5.3. Структура файлового дерева	160
5.4. Типы файлов	162
Обычные файлы	164
Каталоги	164
Жесткая ссылка	164
Файлы символьных и блочных устройств	165
Локальные сокеты	166
Именованные каналы	166
Символические ссылки	166
5.5. Атрибуты файлов	167
Биты режима	167
Биты setuid и setgid	168
Дополнительный бит	169
Команда ls: просмотр атрибутов файла	169
Команда chmod: изменение прав доступа	170
Команды chown и chgrp: смена владельца и группы	172
Команда umask: задание стандартных прав доступа	173
Дополнительные флаги в системе Linux	173

5.6. Списки управления доступом	175
Предупреждение	175
Типы ACL	176
Реализация списков ACL	176
Поддержка ACL в системе Linux	177
Поддержка ACL в системе FreeBSD	177
Обзор POSIX ACL	178
Списки NFSv4 ACL	181
Глава 6. Инсталляция и управление программным обеспечением	187
6.1. Инсталляция операционных систем	188
Загрузка по сети на персональном компьютере	188
Настройка PXE	189
Использование Kickstart — автоматизированного инсталлятора Red Hat и CentOS	190
Автоматизированная инсталляция систем Debian и Ubuntu	193
6.2. Управление пакетами	196
6.3. Системы управления пакетами для Linux	198
Команда rpm: управление пакетами RPM	198
Команда dpkg: управление пакетами .deb	199
6.4. Использование высокоуровневых систем управления пакетами в системе Linux	200
Хранилища пакетов	201
APT: усовершенствованное средство управления пакетами	203
Настройка конфигурации хранилища	204
Пример файла /etc/apt/sources.list	205
Создание локального зеркала хранилища	206
Автоматизация работы системы APT	206
Система yum: управление выпусками для RPM	207
6.5. Управление программным обеспечением в системе FreeBSD	208
Базовая система	209
Менеджер пакетов pkg в системе FreeBSD	209
Коллекция портов	210
6.6. Локализация и настройка конфигурации программного обеспечения	211
Организация локализации	212
Структурные изменения	212
Ограничение количества выпусков	213
Тестирование	213
6.7. Литература	214
Глава 7. Сценарии и командная оболочка	215
7.1. Основы сценариев	216
Создание микросценариев	216
Хорошо изучите несколько инструментов	217
Автоматизируйте все, что возможно	217
Избегайте преждевременной оптимизации	218

Выберите правильный язык сценариев	218
Следуйте рекомендациям	220
7.2. Основы работы с оболочками	222
Редактирование команд	223
Каналы и перенаправление потоков	223
Использование переменных и кавычек	225
Переменные окружения	226
Команды фильтрации	227
7.3. Написание сценариев для оболочки sh	230
Выполнение	231
От команд к сценариям	232
Ввод и вывод данных	234
Пробелы в именах файлов	235
Функции и аргументы командной строки	235
Поток управления	237
Циклы	239
Арифметика	241
7.4. Регулярные выражения	241
Процесс сопоставления	242
Литеральные символы	242
Специальные символы	242
Примеры использования регулярных выражений	244
Захваты	245
Жадность, лень и катастрофический поиск с возвратом	246
7.5. Программирование на языке Python	247
Страсти по Python 3	247
Python 2 или Python 3?	248
Краткое введение в язык Python	249
Объекты, строки, числа, списки, словари, кортежи и файлы	250
Пример проверки ввода	252
Циклы	253
7.6. Программирование на языке Ruby	254
Инсталляция	255
Краткое введение в язык Ruby	255
Блоки	256
Символы и хеши опций	258
Регулярные выражения в языке Ruby	259
Язык Ruby как фильтр	260
7.7. Управление библиотекой и средой для Python и Ruby	260
Поиск и установка пакетов	261
Создание воспроизводимых сред	261
Несколько сред	262
7.8. Контроль версий с помощью системы Git	265
Простой пример Git	267
Ловушки Git	269
Коллективное кодирование с помощью системы Git	269

7.9. Литература	271
Оболочки и сценарии оболочки	271
Регулярные выражения	271
Python	272
Ruby	272
Глава 8. Управление учетными записями пользователей	273
8.1. Основы управления учетными записями	274
8.2. Файл <code>/etc/passwd</code>	274
Регистрационное имя	275
Зашифрованные пароли	276
Идентификатор пользователя	278
Идентификатор группы по умолчанию	278
Поле GECOS	279
Домашний каталог	279
Регистрационная оболочка	280
8.3. Файлы <code>/etc/shadow</code>	280
8.4. Файлы <code>/etc/master.passwd</code> и <code>/etc/login.conf</code> в системе FreeBSD	282
Файл <code>/etc/master.passwd</code>	282
Файл <code>/etc/login.conf</code>	283
8.5. Файл <code>/etc/group</code>	284
8.6. Подключение пользователей вручную: основные действия	285
Редактирование файлов <code>passwd</code> и <code>group</code>	286
Задание пароля	287
Создание домашнего каталога пользователя и инсталляция конфигурационных файлов	287
Установка прав доступа и владения	289
Конфигурирование ролей и административных привилегий	289
Заключительные действия	290
8.7. Добавление пользователей с помощью сценариев: <code>useradd</code> , <code>adduser</code> и <code>newusers</code>	290
Команда <code>useradd</code> в системе Linux	291
Команда <code>adduser</code> в системах Debian и Ubuntu	292
Команда <code>adduser</code> в системе FreeBSD	292
Команда <code>newusers</code> в системе Linux: добавление пользователей пакетом	293
8.8. Безопасное удаление учетных записей пользователей и файлов	294
8.9. Блокирование регистрационных имен пользователей	295
8.10. Уменьшение риска с помощью модулей PAM	296
8.11. Централизация управления учетными записями	296
Протокол LDAP и служба Active Directory	296
Системы “единого входа”	297
Системы управления учетными данными	297
Глава 9. Облачные вычисления	299
9.1. Облако в контексте	300
9.2. Выбор облачной платформы	301
Публичные, частные и гибридные облака	302

Amazon Web Services	303
Google Cloud Platform	303
DigitalOcean	304
9.3. Основы работы с облачными службами	304
Доступ к облаку	306
Регионы и зоны доступности	306
Виртуальные частные серверы	308
Сети	308
Хранилище	309
Идентификация и авторизация	310
Автоматизация	310
9.4. Облака: быстрый запуск VPS на платформе	311
Веб-службы Amazon	311
Интерфейс <code>aws</code> : управление подсистемами AWS	312
Google Cloud Platform	315
DigitalOcean	317
9.5. Контроль затрат	318
9.6. Литература	320
Глава 10. Журналирование	321
10.1. Местоположение файлов регистрации	323
Специальные журнальные файлы	325
Как просмотреть записи в журнале <code>systemd</code>	325
10.2. Журнал <code>systemd</code>	326
Настройка журнала <code>systemd</code>	327
Добавление дополнительных параметров фильтрации для журнала	328
Совместное использование с системой Syslog	328
10.3. Система Syslog	329
Чтение сообщений системы Syslog	330
Архитектура системы Rsyslog	331
Версии Rsyslog	331
Конфигурация Rsyslog	332
Примеры конфигурационных файлов	340
Отладка системы Syslog	343
10.4. Журнальная регистрация на уровне ядра и на этапе начальной загрузки	344
10.5. Управление журнальными файлами и их ротация	345
Утилита <code>logrotate</code> : кросс-платформенное управление журналами	345
Утилита <code>newsyslog</code> : управление журналами в системе FreeBSD	346
10.6. Управление журналами в крупном масштабе	347
Стек ELK	347
Graylog	348
Журналирование как услуга	348
10.7. Принципы обработки журнальных файлов	349
Глава 11. Драйверы и ядро	351
11.1. Ядра и системное администрирование	352
11.2. Нумерация версий ядра	353

Версии ядер для системы Linux	353
Версии ядер FreeBSD	353
11.3. Устройства и их драйверы	354
Файлы и номера устройств	354
Проблемы управления файлами устройств	356
Создание файлов устройств	356
Управление современными файловыми системами	356
Управление устройствами в Linux	357
Создание правил и постоянных имен	359
Управление устройствами в системе FreeBSD	362
11.4. Конфигурирование ядра Linux	364
Конфигурирование параметров ядра linux	364
Сборка ядра	366
Добавление драйвера устройства в Linux	368
11.5. Конфигурация ядра системы FreeBSD	368
Настройка параметров ядра FreeBSD	368
Сборка ядра FreeBSD	369
11.6. Загружаемые модули ядра	370
Загружаемые модули ядра в Linux	371
Загружаемые модули ядра в системе FreeBSD	372
11.7. Загрузка	373
Загрузочные сообщения системы Linux	373
Загрузочные сообщения системы FreeBSD	377
11.8. Загрузка альтернативных ядер в облаке	378
11.9. Ошибки ядра	379
Ошибки ядра Linux	380
Паника ядра в системе FreeBSD	382
11.10. Литература	382
Глава 12. Печать	383
12.1. Система печати CUPS	384
Интерфейсы для системы печати	384
Очередь на печать	385
Множество принтеров	385
Экземпляры принтеров	386
Сетевая печать	386
Фильтры	387
12.2. Управление сервером CUPS	388
Настройка сетевого сервера печати	388
Автоматическое конфигурирование принтера	389
Конфигурирование сетевых принтеров	389
Примеры конфигурирования принтеров	390
Отключение принтера	390
Другие связанные с конфигурированием задачи	391
12.3. Советы по выявлению проблем	392
Повторный запуск демона печати	392
Регистрационные журналы	392

Проблемы с прямой печатью	393
Проблемы с печатью в сети	393
12.4. Литература	394
Часть II. Работа в сетях	395
Глава 13. Сети TCP/IP	397
13.1. Система TCP/IP и Интернет	397
Кто управляет Интернетом	398
Сетевые стандарты и документация	399
13.2. Основы работы в сети	400
Версии IPv4 и IPv6	401
Пакеты и их инкапсуляция	403
Стандарты формирования фреймов Ethernet	404
13.3. Адресация пакетов	405
Аппаратная адресация (MAC)	405
IP-адресация	406
“Адресация” имен машин	407
Порты	407
Типы адресов	408
13.4. IP-адреса	409
Классы адресов в протоколе IPv4	409
Подсети IPv4	410
Трюки и инструменты для арифметических вычислений, связанных с подсетями	411
CIDR: протокол бесклассовой междоменной маршрутизации	412
Выделение адресов	413
Частные адреса и система NAT	413
Адресация в стандарте IPv6	415
13.5. Маршрутизация	419
Таблицы маршрутизации	419
Директивы переадресации протокола ICMP	421
13.6. ARP: протокол преобразования адресов в IPv4 и IPv6	422
13.7. DHCP: протокол динамического конфигурирования хостов	423
Программное обеспечение DHCP	423
Схема работы DHCP	424
Программное обеспечение DHCP, созданное организацией ISC	425
13.8. Вопросы безопасности	426
Перенаправление IP-пакетов	426
Директивы переадресации протокола ICMP	426
Маршрутизация по адресу отправителя	427
Широковещательные пакеты эхо-запросов и другие виды направленных широковещательных сообщений	427
Подмена IP-адресов	427
Встроенные брандмауэры	428
Виртуальные частные сети	429
13.9. Основы конфигурирования сети	430
Присвоение сетевых имен и IP-адресов	430

Настройка сетевых интерфейсов и протокола IP	432
Настройка маршрутизации	433
Конфигурирование DNS	435
Сетевое конфигурирование в различных системах	435
13.10. Сетевое конфигурирование в системе Linux	436
Программа NetworkManager	436
Команда ip: ручное конфигурирование сети	437
Сетевое конфигурирование в системе Ubuntu	438
Сетевое конфигурирование в системе Red Hat и CentOS	438
Настройка сетевого оборудования в системе Linux	440
Опции протокола Linux TCP/IP	441
Переменные ядра, связанные с безопасностью	443
13.11. Сеть FreeBSD	444
Команда ifconfig: настройка сетевых интерфейсов	444
Конфигурация сетевого оборудования в системе FreeBSD	445
Конфигурирование сети во время загрузки системы FreeBSD	445
Конфигурирование протокола TCP/IP в системе FreeBSD	445
13.12. Сетевые проблемы	446
Команда ping: проверьте, работает ли хост	447
Команда traceroute: трассировка IP-пакетов	449
Пакетные анализаторы трафика	452
Утилита tcpdump: пакетный анализатор трафика из командной строки	453
13.13. Мониторинг сети	455
Программа SmokePing: постепенный сбор статистики об эхо-запросах	455
Программа iPerf: отслеживание производительности сети	456
Программа Sacti: сбор и отображение данных	457
13.14. Брандмауэры и система NAT	458
Утилита iptables в системе Linux: правила, цепочки и таблицы	458
IPFilter для UNIX-систем	463
13.15. Облачные сети	465
Виртуальное частное облако AWS (VPC)	465
Сеть на платформе Google Cloud Platform	472
Сеть DigitalOcean	473
13.16. Литература	474
История	474
Классика	474
Протоколы	475
Глава 14. Сетевые аппаратные средства	477
14.1. Технология Ethernet: сетевая панацея	478
Как работает Ethernet	479
Топология Ethernet	479
Неэкранированная витая пара	480
Оптическое волокно	482
Соединение и расширение сетей Ethernet	483
14.2. Беспроводные сети: локальная сеть для кочевников	487
Стандарты беспроводных сетей	487
Доступ клиентов к беспроводной сети	488

Беспроводные коммутаторы и точки беспроводного доступа	488
Безопасность беспроводных сетей	490
14.3. SDN: программно-коммутируемые сети	491
14.4. Тестирование и отладка сетей	491
14.5. Прокладка кабелей	492
Неэкранированная витая пара	492
Офисные точки подключения	492
Стандарты кабельных систем	493
14.6. Проектирование сетей	494
Структура сети и архитектура здания	494
Расширение сетей	494
Перегрузка	495
Обслуживание и документирование	495
14.7. Управление сетью	495
14.8. Рекомендуемые поставщики	496
Кабели и разъемные соединения	496
Тестовые приборы	497
Маршрутизаторы/коммутаторы	497
14.9. Литература	497
Глава 15. IP-маршрутизация	499
15.1. Подробнее о маршрутизации пакетов	500
15.2. Демоны и протоколы маршрутизации	503
Дистанционно-векторные протоколы	503
Топологические протоколы	504
Метрика стоимости	505
Внутренние и внешние протоколы	505
15.3. Основные протоколы маршрутизации	506
Протоколы RIP и RIPng	506
Протокол OSPF	507
Протокол EIGRP	508
BGP: протокол граничного шлюза	508
15.4. Многоадресатная координация протокола маршрутизации	508
15.5. Выбор критериев стратегии маршрутизации	509
15.6. Демоны маршрутизации	510
Демон <code>routed</code> : устаревшая реализация в протоколе RIP	511
Пакет <code>Quagga</code> : основной демон маршрутизации	511
Маршрутизатор <code>XORP</code>	512
15.7. Маршрутизаторы Cisco	512
15.8. Литература	515
Глава 16. DNS: система доменных имен	517
16.1. Архитектура DNS	518
Запросы и ответы	518
Поставщики услуг DNS	519
16.2. DNS для поиска	519
<code>resolv.conf</code> : конфигурация клиентского модуля распознавания	519
<code>nsswitch.conf</code> : кого я запрашиваю по имени?	520

16.3. Пространство имен DNS	521
Регистрация доменного имени	522
Создание собственных поддоменов	522
16.4. Как работает система DNS	522
Серверы имен	522
Авторитетные и кеширующие серверы	523
Рекурсивные и нерекурсивные серверы	524
Записи о ресурсах	524
Делегирование	525
Кеширование и эффективность	526
Неоднозначные ответы и балансировка загрузки DNS	527
Отладка с помощью инструментов запросов	527
16.5. База данных DNS	530
Команды синтаксического анализатора в файлах зон	530
Записи о ресурсах	531
Запись SOA	534
Записи NS	536
Записи A	537
Записи AAAA	537
Записи PTR	538
Записи MX	539
Записи CNAME	540
Записи SRV	541
Записи TXT	542
Записи SPF, DKIM и DMARC	542
Записи о ресурсах DNSSEC	542
16.6. Программное обеспечение BIND	543
Компоненты системы BIND	543
Файлы конфигурации	543
Инструкция include	545
Инструкция options	545
Инструкция acl	551
Инструкция key (TSIG)	552
Инструкция server	552
Инструкция masters	553
Инструкция logging	553
Инструкция statistics-channels	553
Инструкция zone	554
Инструкция controls для команды rndc	557
16.7. Расщепление DNS и инструкция view	558
16.8. Примеры конфигурации системы BIND	560
Зона локального хоста	560
Небольшая компания, предоставляющая консалтинговые услуги в области безопасности	561
16.9. Обновление файла зоны	564
Передача зоны	565
Динамические обновления в системе BIND	565

16.10. Вопросы безопасности DNS	568
Еще раз о списках управления доступом на сервере BIND	568
Открытые распознаватели	569
Работа в виртуальном окружении chroot	570
Безопасные межсерверные взаимодействия посредством технологий TSIG и TKEY	570
Настройка технологии TSIG для сервера BIND	571
Технология DNSSEC	573
Правила протокола DNSSEC	574
Записи о ресурсах DNSSEC	574
Настройка протокола DNSSEC	575
Генерирование пар ключей	576
Подписание зоны	578
Цепочка доверия в протоколе DNSSEC	580
Смена ключей DNSSEC	580
Инструменты DNSSEC	581
Отладка протокола DNSSEC	583
16.11. Отладка сервера BIND	584
Журнальная регистрация на сервере BIND	584
Некорректное делегирование	591
16.12. Литература	592
Книги и другая документация	593
Ресурсы в Интернете	593
Документы RFC	593
Глава 17. Система единого входа	595
17.1. Основные элементы системы единого входа	596
17.2. LDAP: “облегченные” службы каталогов	597
Особенности LDAP	597
Структура данных LDAP	598
OpenLDAP: традиционный LDAP-сервер с открытым исходным кодом	599
389 Directory Server: альтернативный LDAP-сервер с открытым исходным кодом	600
Создание LDAP-запросов	601
Преобразования файлов паролей и групп LDAP	602
17.3. Использование служб каталогов для входа в систему	603
Система Kerberos	603
Демон sssd: служба системной безопасности	606
nsswitch.conf: переключатель службы имен	607
Модули PAM: украшение или чудо аутентификации?	607
17.4. Альтернативные подходы	610
NIS: сетевая информационная служба	611
Утилита rsync: более безопасная рассылка файлов	611
17.5. Литература	611
Глава 18. Электронная почта	613
18.1. Архитектура почтовой системы	613
Пользовательские агенты	614

Агенты передачи	615
Транспортные агенты	615
Локальные агенты доставки	616
Хранилища сообщений	616
Агенты доступа	616
18.2. Структура почтового сообщения	617
18.3. Протокол SMTP	619
Вы прислали мне привет (EHLO)	620
Коды ошибок протокола SMTP	621
Аутентификация SMTP	621
18.4. Спам и вредоносные программы	622
Подделки	623
Технология SPF и спецификации Sender ID	623
Системы DKIM	624
18.5. Конфиденциальность и шифрование сообщений	624
18.6. Почтовые псевдонимы	625
Загрузка псевдонимов из файла	627
Направление почты в файл	628
Направление почты в программу	628
Хешированная база данных псевдонимов	628
18.7. Конфигурация электронной почты	629
18.8. Почтовый агент sendmail	630
Файл переключения	631
Запуск программы sendmail	631
Почтовые очереди	633
Препроцессор m4	634
Фрагменты конфигурации программы sendmail	635
Конфигурационный файл, построенный на основе эталонного файла с расширением .mc	636
Примитивы конфигурации программы sendmail	637
Таблицы и базы данных	637
Обобщенные макросы и функциональные возможности	638
Конфигурация клиентов	643
Параметры конфигурации препроцессора m4	644
Средства программы sendmail для борьбы со спамом	646
Ретрансляция	646
Безопасность и программа sendmail	649
Владельцы файлов	650
Права доступа	651
Безопасная пересылка почты в файлы и программы	651
Опции безопасности	652
Выполнение программы sendmail в виртуальном каталоге (для настоящих параноиков)	653
Отражение атак типа “отказ от обслуживания”	654
TLS: безопасный протокол транспортного уровня	654
Тестирование и отладка программы sendmail	655
Журнальная регистрация	656

18.9. Почтовый агент Exim	657
Инсталляция почтового сервера Exim	658
Загрузка почтового сервера Exim	659
Утилиты почтового сервера Exim	660
Язык конфигурации программы Exim	661
Файл конфигурации программы Exim	661
Глобальные параметры	662
Сканирование содержимого на этапе применения списков управления доступом	667
Аутентификаторы	667
Маршрутизаторы	668
Транспортные механизмы	672
Конфигурация <code>retry</code>	672
Конфигурация перезаписи	673
Функция локального сканирования	673
Регистрация	673
Отладка	674
18.10. Почтовый агент Postfix	675
Архитектура системы Postfix	675
Безопасность	677
Команды и документация системы Postfix	677
Конфигурация системы Postfix	678
Виртуальные домены	682
Управление доступом	683
Отладка	686
18.11. Литература	687
Литература по программе <code>sendmail</code>	688
Литература о системе Exim	688
Литература о системе Postfix	688
Документы RFC	688
Глава 19. Веб-хостинг	689
19.1. HTTP: протокол передачи гипертекста	689
Унифицированные указатели ресурсов (URL)	690
Структура транзакции протокола HTTP	691
Утилита <code>curl</code> : инструмент командной строки для работы с HTTP	694
Повторное использование TCP-соединений	695
HTTP на основе протокола TLS	696
Виртуальные хосты	696
19.2. Основы программного обеспечения для веба	697
Веб-серверы и прокси-сервер протокола HTTP	698
Балансировщики нагрузки	699
Кеши	701
Сети доставки контента	704
Языки веба	705
Интерфейсы прикладного программирования (API)	707
19.3. Облачный веб-хостинг	708
Сборка или покупка	709

Платформа как услуга	709
Статический хостинг содержимого	710
Бессерверные веб-приложения	710
19.4. Веб-сервер Apache <code>httpd</code>	711
Использование веб-сервера <code>httpd</code>	712
Конфигурация логистики веб-сервера <code>httpd</code>	712
Настройка виртуального хоста	714
Базовая аутентификация протокола HTTP	715
Ведение журнала	717
19.5. Веб-сервер NGINX	718
Установка и запуск NGINX	719
Настройка веб-сервера NGINX	719
Настройка TLS для NGINX	722
Балансировка нагрузки с помощью NGINX	723
19.6. Программное обеспечение Nginx	724
Проверки работоспособности	725
Статистика сервера	726
Липкие сессии	726
Прекращение использования TLS	727
19.7. Литература	728
Часть III. Хранение данных	729
Глава 20. Дисковая память	731
20.1. Добавление диска	732
Рецепт для Linux	733
Рецепт для FreeBSD	734
20.2. Аппаратное обеспечение для хранения данных	735
Жесткие диски	736
Твердотельные диски	739
Гибридные диски	742
Расширенный формат и блоки по 4 КиБ	743
20.3. Интерфейсы устройств для хранения данных	744
Интерфейс SATA	744
Интерфейс PCI Express	744
Интерфейс SAS	745
Интерфейс USB	746
20.4. Подключение и низкоуровневое управление накопителями	747
Проверка инсталляции на уровне аппаратного обеспечения	747
Файлы дисковых устройств	748
Непостоянные имена устройств	749
Форматирование дисков и управление сбойными секторами	749
Безопасное стирание дисков ATA	750
Команды <code>hdparm</code> и <code>smartctl</code> : параметры диска и интерфейса (Linux)	752
Мониторинг жесткого диска с помощью стандарта SMART	752
20.5. Программное обеспечение накопителей	753
Отображение устройств в системе Linux	755

20.6. Разбиение диска	756
Традиционное разбиение	758
Разбиение диска по схеме MBR	759
Схема GPT: таблица разделов GUID	759
Разбиение дисков в системе Linux	760
Разбиение дисков в системе FreeBSD	760
20.7. Управление логическими томами	761
Управление логическими томами в системе Linux	761
Управление логическими томами в FreeBSD	766
20.8. RAID: избыточные массивы недорогих дисков	767
Программная и аппаратная реализации системы RAID	767
Уровни системы RAID	767
Восстановление диска после сбоя	770
Недостатки конфигурации RAID 5	771
Команда mdadm: программное обеспечение RAID в системе Linux	772
20.9. Файловые системы	776
20.10. Традиционные файловые системы: UFS, ext4 и XFS	777
Терминология файловых систем	778
Полиморфизм файловых систем	779
Форматирование файловых систем	779
Команда fsck: проверка и исправление файловых систем	779
Монтирование файловой системы	781
Настройка автоматического монтирования	781
Монтирование USB-накопителя	784
Включение подкачки	784
20.11. Файловые системы следующего поколения: ZFS и Btrfs	785
Копирование при записи	785
Обнаружение ошибок	786
Производительность	786
20.12. Файловая система ZFS: все проблемы решены	787
ZFS в системе Linux	788
Архитектура ZFS	788
Пример: добавление диска	789
Файловые системы и свойства	789
Наследование свойств	791
Один пользователь — одна файловая система	792
Мгновенные копии и клоны	792
Неразмеченные логические тома	794
Управление пулом памяти	794
20.13. Файловая системы Btrfs:	
облегченная версия ZFS для Linux	796
Btrfs или ZFS	797
Настройка и преобразование хранилища	797
Тома и подтома	800
Снимки тома	800
Поверхностные копии	801
20.14. Стратегия резервного копирования данных	802
20.15. Литература	803

Глава 21. Сетевая файловая система NFS	805
21.1. Введение в протокол NFS	805
Конкуренция	806
Проблемы, связанные с состоянием	806
Проблемы производительности	807
Безопасность	807
21.2. Основные идеи, лежащие в основе протокола NFS	808
Версии и история протокола	808
Удаленный вызов процедур	809
Транспортные протоколы	810
Состояние	810
Экспорт файловой системы	810
Блокировка файлов	811
Вопросы безопасности	812
Идентифицирующее отображение в версии 4	813
Учетные записи <code>root</code> и <code>nobody</code>	814
Производительность версии 4	815
21.3. Серверная часть протокола NFS	815
Файл <code>exports</code> в системе Linux	816
Файл <code>exports</code> в системе FreeBSD	819
Демон <code>nfsd</code> : обслуживание файлов	820
21.4. Клиентская часть протокола NFS	822
Монтирование файловых систем NFS на этапе начальной загрузки	824
Ограничения экспорта привилегированными портами	824
21.5. Идентифицирующее отображение в протоколе NFS 4	825
21.6. Команда <code>nfsstat</code> : отображение статистики NFS	825
21.7. Специализированные файловые серверы NFS	826
21.8. Автоматическое монтирование	827
Таблицы косвенных назначений	828
Таблицы прямых назначений	829
Главные таблицы	829
Исполняемые таблицы	830
Видимость программы <code>automount</code>	830
Реплицированные файловые системы и программа <code>automount</code>	831
Автоматическое монтирование (V3; все, кроме Linux)	831
Специфика системы Linux	832
21.9. Литература	832
Глава 22. Файловая система SMB	833
22.1. Samba: сервер SMB для UNIX	834
22.2. Инсталляция и конфигурации пакета Samba	835
Совместное использование файлов с локальной аутентификацией	836
Совместное использование файлов с помощью учетных записей, прошедших аутентификацию Active Directory	836
Настройка общих ресурсов	837
22.3. Монтирование общих SMB-ресурсов	839
22.4. Просмотр файлов на общих SMB-ресурсах	840

22.5. Обеспечение безопасности Samba-сервера	840
22.6. Отладка Samba-сервера	841
Запрос состояния Samba-сервера с помощью команды <code>smbstatus</code>	841
Настройка журнала Samba-сервера	842
Управление наборами символов	843
22.7. Литература	843
Часть IV. Эксплуатация	845
Глава 23. Управление конфигурацией	847
23.1. Краткое введение в управление конфигурацией	848
23.2. Опасности управления конфигурацией	848
23.3. Элементы управления конфигурацией	849
Операции и параметры	849
Переменные	851
Факты	851
Обработчики изменений	852
Привязки	852
Пакеты и репозитории пакетов	853
Среды	853
Учет и регистрация клиентов	854
23.4. Сравнение популярных систем CM	855
Терминология	856
Бизнес-модели	856
Архитектурные параметры	856
Параметры языка	858
Варианты управления зависимостями	859
Общие комментарии по поводу системы Chef	861
Общие комментарии по поводу системы Puppet	862
Общие комментарии по поводу систем Ansible и Salt	863
Ода YAML	863
23.5. Введение в систему Ansible	865
Пример использования системы Ansible	866
Настройка клиента	868
Группы клиентов	870
Присваивание переменных	870
Динамические и вычисляемые группы клиентов	871
Списки задач	872
Параметры состояния	874
Итерация	874
Взаимодействие с Jinja	875
Визуализация шаблона	875
Привязки: сценарии и файлы сценариев	876
Роли	878
Рекомендации по структурированию базы конфигурации	879
Параметры доступа в системе Ansible	880
23.6. Введение в систему Salt	882
Настройка миньонов	884

Привязка значения переменной к миньону	886
Сопоставление миньонов	887
Состояния системы Salt	888
Система Salt и препроцессор Jinja	889
Идентификаторы состояний и зависимости	891
Функции состояния и выполнения	892
Параметры и имена	893
Привязка состояний к миньонам	896
Состояния высокого уровня	896
Формулы Salt	897
Среды	898
Документация	902
23.7. Сравнение систем Ansible и Salt	903
Гибкость развертывания и масштабируемость	903
Встроенные модули и расширяемость	903
Безопасность	904
Разное	904
23.8. Рекомендации	905
23.9. Литература	908
Глава 24. Виртуализация	909
24.1. Виртуальный жаргон	910
Гипервизоры	910
Динамическая миграция	913
Образы виртуальных машин	913
Контейнеризация	913
24.2. Виртуализация с помощью системы Linux	915
Платформа Xen	915
Инсталляция гостевой операционной системы на платформе Xen	916
Платформа KVM	917
Инсталляция гостевой операционной системы на платформе KVM и ее использование	918
24.3. Система FreeBSD bhyve	919
24.4. Компания VMWare	919
24.5. Гипервизор VirtualBox	919
24.6. Программа Packer	920
24.7. Программа Vagrant	922
24.8. Литература	922
Глава 25. Контейнеры	923
25.1. Основные концепции	924
Поддержка ядра	924
Образы	925
Сеть	926
25.2. Докер: механизм с открытым исходным кодом	926
Базовая архитектура	927
Инсталляция	928
Настройка клиента	929

Методики работы с контейнерами	929
Тома	933
Контейнеры данных	934
Сети Docker	934
Драйверы хранилищ	937
Изменение параметров настройки демона dockerd	938
Сборка образа	939
Реестры	942
25.3. Контейнеры на практике	944
Ведение журнала	945
Советы по безопасности	946
Отладка и устранение неполадок	948
25.4. Создание и управление контейнерными кластерами	949
Краткий обзор программного обеспечения для управления контейнерами	951
Kubernetes	951
Mesos и Marathon	952
Менеджер Docker Swarm	953
Контейнерная служба AWS EC2	953
25.5. Литература	954
Глава 26. Непрерывная интеграция и доставка	955
26.1. Основные концепции	957
Принципы и практика	957
Флаги функций	961
26.2. Конвейеры	961
Процесс сборки	962
Тестирование	963
Развертывание	965
Методы развертывания с нулевым временем простоя	966
26.3. Jenkins: сервер автоматизации с открытым исходным кодом	967
Основные концепции сервера Jenkins	967
Распределенные сборки	969
Конвейер как код	969
26.4. Подход CI/CD на практике	970
Тривиальное веб-приложение UlsahGo	971
Модульное тестирование UlsahGo	972
Знакомство с конвейером Jenkins Pipeline	973
Создание образа DigitalOcean	975
Обеспечение единой системы тестирования	977
Тестирование дроплета	980
Развертывание приложения UlsahGo на паре дроплетов и балансировщике нагрузки	980
Выводы, сделанные из демонстрационного конвейера	981
26.5. Контейнеры и упрощение среды CI/CD	982
Контейнеры как среда сборки	983
Контейнерные образы как артефакты сборки	983
26.6. Литература	984

Глава 27. Безопасность	985
27.1. Элементы безопасности	986
27.2. Слабые места в системе защиты	987
Социальная инженерия	987
Уязвимости в программах	988
Распределенные атаки типа “отказ в обслуживании” (DDoS)	989
Инсайдерская информация	989
Ошибки конфигурации сети, системы или приложения	990
27.3. Основные вопросы безопасности	990
Обновления программного обеспечения	991
Ненужные службы	992
Удаленная регистрация событий	992
Резервные копии	993
Вирусы и черви	993
Руткиты	994
Фильтрация пакетов	994
Пароли и многофакторная аутентификация	995
Бдительность	995
Тестирование приложений на проникновение	995
27.4. Пароли и учетные записи пользователей	996
Изменение пароля	997
Хранилища и депоненты паролей	997
Устаревание паролей	998
Групповые и совместно используемые учетные записи	999
Пользовательские оболочки	999
Привилегированные учетные записи	999
27.5. Инструментальные средства защиты	1000
Команда nmap: сканирование сетевых портов	1000
Nessus: сетевой сканер нового поколения	1002
Metasploit: программа для выявления попыток проникновения	1002
Lynis: встроенный аудит безопасности	1003
John the Ripper: средство для выявления слабых паролей	1003
Vro: программная система для распознавания вторжения в сеть	1004
Snort: популярная программная система для распознавания проникновения в сеть	1005
OSSEC: система для распознавания вторжения в сеть на уровне хоста	1005
Fail2Ban: система отражения атаки методом перебора	1008
27.6. Основы криптографии	1008
Криптография с симметричными ключами	1009
Криптография с открытым ключом	1009
Инфраструктура с открытым ключом	1010
Протокол защиты транспортного уровня TLS	1012
Криптографические хеш-функции	1012
Генерация случайных чисел	1014
Выбор криптографического программного обеспечения	1015
Команда openssl	1016
Отладка TLS-сеанса с сервером	1017

PGP: довольно хорошая конфиденциальность	1017
Kerberos: унифицированный подход к сетевой безопасности	1018
27.7. Система SSH	1019
Основы OpenSSH	1019
Клиент ssh	1021
Аутентификация с помощью открытого ключа	1022
Демон ssh-agent	1024
Псевдонимы хостов в файле ~/.ssh/config	1025
Мультиплексирование соединения	1026
Проброс портов	1026
Демон sshd: сервер OpenSSH	1027
Проверка ключа хоста с помощью записи SSHFP	1029
Передача файлов	1030
Альтернативы для безопасного входа в систему	1030
27.8. Брандмауэры	1031
Брандмауэры, фильтрующие пакеты	1031
Принципы фильтрации служб	1031
Брандмауэры, осуществляющие инспекцию пакетов с отслеживанием состояния соединений	1032
Насколько безопасны брандмауэры	1032
27.9. Виртуальные частные сети (VPN)	1033
Туннели IPsec	1033
Так ли уж нужны виртуальные частные сети	1034
27.10. Сертификаты и стандарты	1034
Сертификаты	1034
Стандарты безопасности	1035
27.11. Источники информации по вопросам обеспечения безопасности	1038
Сервер SecurityFocus.com и списки рассылки BugTraq и OSS	1038
Блог Брюса Шнайера	1038
Отчет компании Verizon Data Breach Investigations	1038
Институт SANS	1038
Информационные ресурсы отдельных дистрибутивов	1039
Другие списки рассылки и веб-сайты	1039
27.12. Что нужно делать в случае атаки на сервер	1040
27.13. Литература	1041
Глава 28. Мониторинг	1043
28.1. Обзор мониторинга	1044
Инструментарий	1044
Типы данных	1045
Ввод и обработка	1045
Уведомления	1046
Контрольные панели и пользовательские интерфейсы	1047
28.2. Культура мониторинга	1047
28.3. Платформы мониторинга	1048
Платформы реального времени с открытым исходным кодом	1049
Платформы временных рядов с открытым исходным кодом	1050
Платформы визуализации данных с открытым исходным кодом	1052

Коммерческие платформы мониторинга	1052
Размещенные платформы мониторинга	1053
28.4. Сбор данных	1054
StatsD: протокол передачи общих данных	1054
Сбор данных из вывода команды	1056
28.5. Мониторинг сетей	1057
28.6. Мониторинг систем	1058
Команды для мониторинга систем	1059
Сборщик обобщенных системных данных <code>collectd</code>	1059
Утилиты <code>sysdig</code> и <code>dtrace</code> : трассировки выполнения	1060
28.7. Мониторинг приложений	1061
Мониторинг системного журнала	1061
Supervisor + Munin: простой вариант для некоторых предметных областей	1062
Коммерческие средства мониторинга приложений	1062
28.8. Мониторинг безопасности	1063
Проверка целостности системы	1063
Контроль обнаружения вторжений	1065
28.9. SNMP: простой протокол сетевого управления	1065
Организация протокола SNMP	1066
Операции протокола SNMP	1067
Net-SNMP: средства для серверов	1067
28.10. Советы и рекомендации по мониторингу	1069
28.11. Литература	1070
Глава 29. Анализ производительности	1071
29.1. Принципы настройки производительности	1072
29.2. Способы повышения производительности	1073
29.3. Факторы, влияющие на производительность	1075
29.4. Захваченные циклы центрального процессора	1076
29.5. Как анализировать проблемы производительности	1077
29.6. Проверка производительности системы	1078
Инвентаризируйте свое оборудование	1078
Сбор данных о производительности	1080
Анализ использования центрального процессора	1080
Управление памятью в системе	1082
Анализ использования памяти	1084
Анализ операций обмена с диском	1085
Утилита <code>fiio</code> : анализ производительности дисковой подсистемы	1086
Команда <code>sar</code> : сбор статистических данных и генерирование отчетов по ним	1087
Выбор планировщика ввода-вывода в системах Linux	1088
Программа <code>perf</code> : универсальный профилировщик системы Linux	1089
29.7. Помогите! Мой сервер тормозит!	1090
29.8. Литература	1092

Глава 30. Центры обработки данных	1093
30.1. Стойки	1094
30.2. Электропитание	1094
Требования к электроснабжению стоек	1096
Измерение	1098
Стоимость	1098
Удаленное управление	1098
30.3. Охлаждение и окружающая среда	1098
Оценка нагрузки на систему охлаждения	1099
Теплые и холодные отсеки	1101
Влажность	1102
Мониторинг окружающей среды	1102
30.4. Уровни надежности центров обработки данных	1103
30.5. Безопасность центров обработки данных	1103
Местонахождение	1104
Периметр	1104
Доступ к объекту	1104
Доступ к стойке	1105
30.6. Инструменты	1105
30.7. Литература	1106
Глава 31. Методология, политика и стратегии	1107
31.1. Великая единая теория: DevOps	1108
DevOps — это CLAMS	1109
Системное администрирование в мире DevOps	1112
31.2. Системы управления билетами и задачами	1113
Общие функции билетных систем	1113
Владелец билета	1114
Восприятие пользователями билетных систем	1115
Типовые билетные системы	1116
Диспетчеризация билетов	1116
31.3. Поддержка локальной документации	1117
Инфраструктура как код	1118
Стандарты документации	1118
31.4. Разделение окружающей среды	1119
31.5. Восстановление после аварий	1120
Оценка рисков	1120
Планирование мероприятий по восстановлению	1121
Подбор персонала на случай аварии	1123
Проблемы с безопасностью	1123
31.6. Инструкции и процедуры	1124
Различие между инструкциями и процедурами	1125
Лучшие практики применения инструкций	1126
Процедуры	1126
31.7. Соглашения о качестве оказываемых услуг	1127
Спектр услуг и их описание	1127

Стратегии управления очередями	1128
Показатели соответствия	1129
31.8. Соответствие законам и стандартам	1129
31.9. Правовые вопросы	1133
Конфиденциальность	1133
Реализация политики безопасности	1134
Контроль — это ответственность	1135
Лицензии на программное обеспечение	1135
31.10. Организации, конференции и другие ресурсы	1136
31.11. Литература	1137
Краткая история системного администрирования	1139
Рассвет компьютеризации: системные операторы (1952–1960)	1139
От узкой специализации к работе в режиме разделения времени (1961–1969)	1140
Рождение UNIX (1969–1973)	1140
UNIX становится знаменитой (1974–1990)	1142
Эра системных администраторов	1143
Документация по системному администрированию и обучение UNIX при смерти. Рождение Linux (1991–1995)	1145
Мир Windows (1996–1999)	1146
Расцвет UNIX и Linux (2000–2009)	1147
Системы UNIX и Linux в гипермасштабируемом облаке (2010– настоящее время)	1147
Завтрашний день UNIX и Linux	1148
Литература	1148
Предметный указатель	1149

Глава 14

Сетевые аппаратные средства



Независимо от того, работают ваши системы в центре обработки данных, в облаке или пусковой ракетной шахте, у них есть нечто общее — необходимость обмена информацией по сети. Возможность быстрой и надежной передачи данных необходима в любой среде. Если есть область, в которой технология UNIX затронула человеческие жизни и повлияла на другие операционные системы, то она связана с практической реализацией крупномасштабного пакетированного транспорта данных.

Сети проходят такую же эволюцию, как и серверы, поскольку физические и логические представления сети все больше разделяются уровнем виртуализации, имеющим собственную конфигурацию. В облаке такие конфигурации являются стандартными, но даже физические центры обработки данных в настоящее время часто включают в себя слой программно конфигурируемых сетей (software-defined networking — SDN).

Администраторы взаимодействуют с сетевым оборудованием реального мира менее часто, чем когда-то, но знакомство с традиционными сетями остается решающим навыком. Виртуализированные сети тесно имитируют физические сети в своих функциях, терминологии, архитектуре и топологии.

Многие сетевые технологии продвигались в течение долгих лет, но в результате появился очевидный победитель — Ethernet. Сегодня технологию Ethernet можно встретить всюду: от игровых приставок до холодильников. Глубокое понимание принципов работы этой системы чрезвычайно важно для успешной работы системного администратора.

Совершенно очевидно, что быстродействие и надежность сетей непосредственно влияют на результаты деятельности компаний. Однако в настоящее время сетевые технологии настолько всепроникающи, что состояние сети может повлиять на возможность вза-

имодействия между людьми, например возможность делать телефонные звонки. Плохая организация сети — это личная и профессиональная неудача, которая может иметь катастрофические социальные последствия. Кроме того, устранение этих недостатков порой обходится очень дорого.

Успешное создание сети зависит от по крайней мере четырех важнейших факторов:

- разработки разумной структуры сети;
- выбора высококачественного оборудования;
- правильной инсталляции и документирования;
- компетентной эксплуатации и сопровождения.

В этой главе рассматриваются принципы, инсталляция и функционирование сетей Ethernet. Мы также кратко опишем такие устаревшие технологии, как DSL (Digital Subscriber Line), которые обычно предстают перед конечными пользователями в облике — сюрприз! — технологии Ethernet.

14.1. ТЕХНОЛОГИЯ ETHERNET: СЕТЕВАЯ ПАНАЦЕЯ

Захватив более 95% мирового рынка локальных сетей (Local Area Network — LAN), технология Ethernet в самых разных формах проявляется почти всюду. Разработку стандарта Ethernet начал Боб Меткалф (Bob Metcalfe) из Массачусетского технологического института в рамках своей кандидатской диссертации, но в настоящее время она описана во многих стандартах IEEE.

В первоначальной спецификации Ethernet была определена скорость передачи данных 3 Мбит/с (мегабит в секунду), но почти сразу же она выросла до 10 Мбит/с. Как только в 1994 году была закончена работа над стандартом, предусматривавшим скорость 100 Мбит/с, стало ясно, что технология Ethernet будет лишь эволюционировать, а не вытесняться новой технологией. Это вызвало гонку технологий, в ходе которой производители старались создать все более быстродействующую версию Ethernet, и это соревнование еще не закончено. Основные этапы эволюции различных стандартов Ethernet приведены в табл. 14.1¹.

Таблица 14.1. Эволюция Ethernet

Год	Скорость	Название стандарта	Номер IEEE	Расстояние	Средство передачи ^a
1973	3 Мбит/с	Xerox Ethernet	–	?	Коаксиальный кабель
1976	10 Мбит/с	Ethernet 1	–	500 м	Коаксиальный кабель RG-11
1989	10 Мбит/с	10BASE-T	802.3	100 м	Медный кабель НВП категории 3
1994	100 Мбит/с	100Base-TX	802.3u	100 м	Медный кабель НВП категории 5
1999	1 Гбит/с	1000BASE-T ("gigabit")	802.3ab	100 м	Медный кабель НВП категорий 5е и 6
2006	10 Гбит/с	10GBASE-T ("10 Gig")	802.3ap	100 м	ВП категории 6а, 7, НВП категории 7а
2009	40 Гбит/с	40GBASE-CR4	P802.3ba	10 м	Медный кабель НВП
		40GBASE-SR4		100 м	ММ-оптоволокно

¹Мы не упомянули несколько менее популярных стандартов.

Окончание табл. 14.1

Год	Скорость	Название стандарта	Номер IEEE	Расстояние	Средство передачи ^a
2009	100 Гбит/с	100GBASE-CR10	P802.3ba	10 м	Медный кабель НВП
		100GBASE-SR10		100 м	ММ-оптоволокно
2018 ^b	200 Гбит/с	200GBASE-FR4	P802.3bs ^a	2 км	CWDM-оптоволокно
		200Gbase-LR4		10 км	CWDM-оптоволокно
2018 ^b	400 Гбит/с	400GBASE-SR16	P802.3bs	100 м	ММ-оптоволокно (16 жил)
		400Gbase-DR4		500 м	ММ-оптоволокно (4 жилы)
		400GBASE-FR8		2 км	CWDM-оптоволокно
		400Gbase-LR8		10 км	CWDM-оптоволокно
2020 ^b	1Тбит/с	TbE	TBD	TBD	TBD

^aММ — многомодовое, НВП — неэкранированная витая пара, ВП — витая пара, CWDM — разреженное спектральное мультиплексирование.

^bПромышленный проект.

^aМы немного сомневаемся и предполагаем, что этот вариант кодировки был неудачным совпадением.

Как работает Ethernet

Технологию Ethernet можно представить в виде великосветского раута, на котором гости (компьютеры) не перебивают друг друга, а ждут паузы в разговоре (отсутствия трафика в сетевой кабеле), чтобы заговорить. Если два гостя начинают говорить одновременно (т.е. возникает конфликт), оба они останавливаются, извиняются друг перед другом, ждут немного, а затем один из них начинает говорить снова.

В технической терминологии такая схема называется CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением конфликтов). Смысл этого названия заключается в следующем:

- контроль несущей (CS) — вы можете говорить одновременно с другими;
- множественный доступ (MA) — говорить могут все;
- обнаружение конфликтов (CD) — вы знаете, когда перебиваете кого-то.

Фактическая задержка при обнаружении конфликтов является случайной. Это позволяет избежать такого развития событий, при котором два компьютера одновременно передают сообщения в сеть, обнаруживают коллизию, ждут некоторое время, а затем синхронно возобновляют передачу, переполняя, таким образом, сеть конфликтами.

В настоящее время важность соглашений CSMA/CD осознали даже приверженцы коммутаторов, которые обычно ограничивают количество хостов в домене, в котором происходят коллизии, до двух. (Если продолжить аналогию с великосветским раутом, можно описать этот вариант как ситуацию, в которой два собеседника, как в старом кино, чопорно сидят на противоположных концах длинного обеденного стола.)

Топология Ethernet

С точки зрения топологии сеть Ethernet представляет собой разветвляющуюся шину, но без петель. У пакета есть только один путь следования между любыми двумя хостами, расположенными в одной сети. В сети Ethernet могут передаваться пакеты трех типов: однонаправленные (unicast), групповые (multicast) и широковещательные (broadcast). Пакеты первого типа адресованы одному хосту, второго — группе хостов, третьего — всем хостам сегмента.

Широковещательный домен — это совокупность хостов, которые принимают пакеты, направляемые по аппаратному широковещательному адресу. В каждом логическом сегменте сети Ethernet существует только один широковещательный домен. В ранних стандартах Ethernet и средствах передачи (например, 10Base5) понятия физического и логического сегментов были тождественными, поскольку все пакеты передавались по одному большому кабелю, в который втыкались сетевые интерфейсы компьютеров².

С появлением современных коммутаторов логические сегменты стали включать в себя множество (десятки и даже сотни) физических сегментов, к которым подключено всего два устройства: порт коммутатора и компьютер. Коммутаторы отвечают за доставку групповых и однонаправленных пакетов в физический сегмент, где расположен нужный адресат (адресаты); широковещательные пакеты направляются во все сетевые порты логического сегмента.

С появлением коммутаторов сегодняшние логические сегменты обычно состоят из многих физических сегментов (возможно, десятков или сотен), к которым подключены только два устройства: порт коммутатора и хост.³ Коммутаторы несут ответственность за сопровождение многоадресных и одноадресных пакетов к физическим (или беспроводным) сегментам, на которых находятся предполагаемые получатели. Широковещательный трафик пересылается всем портам в логическом сегменте.

Логический сегмент может состоять из физических сегментов, имеющих разную скорость передачи данных. Следовательно, коммутаторы должны иметь средства буферизации и синхронизации для предотвращения возможных конфликтов.

Неэкранированная витая пара

Неэкранированная витая пара (НВП) — самая популярная среда передачи данных в сетях Ethernet. Общая схема сети на основе НВП изображена на рис. 14.1.

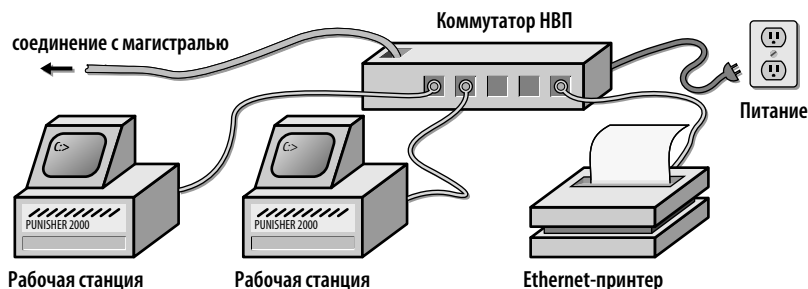


Рис. 14.1. Схема сети на основе НВП

²Мы не шутим! Подключение нового компьютера к сети предполагало прокалывание отверстия в изоляции кабеля с помощью специального соединителя, называемого «зуб вампира», который позволял добраться до центрального проводника. Этот соединитель затем зажимался винтами.

³Беспроводные сети — еще один распространенный тип логического сегмента Ethernet. Они ведут себя, скорее, как традиционные формы Ethernet, которые используют один кабель для соединения многих хостов сети (см. раздел 14.2).

Провода, используемые в современных локальных вычислительных сетях на основе неэкранированной витой пары, обычно подразделяют на восемь категорий. Эта система оценки параметров была впервые введена компанией Anixter, крупным поставщиком кабельной продукции, и впоследствии стандартизирована организацией TIA (Telecommunications Industry Association — ассоциация телекоммуникационной промышленности). Сегодня выделяются категории 1–7 и промежуточные категории 5e и 6a.

Организация ISO (International Organization for Standardization — Международная организация по стандартизации) тоже подключилась к процессу стандартизации кабелей и предложила собственную классификацию, которая почти в точности повторяет классификацию TIA. Например, кабель категории 5 в системе TIA эквивалентен кабелю класса D в системе ISO. Для наглядности в табл. 14.2 подытожены ключевые различия между основными современными стандартами кабелей. Эта таблица поможет вам произвести впечатление на своих друзей во время вечеринки.

Таблица 14.2. Характеристики кабелей НВП

Параметр ^a	Единица измерения	Категории						
		5 D ^b	5e	6 E	6a EA	7 F	7a FA	8 I
Ширина полосы	МГц	100	100	250	500	600	1000	2000
Затухание	дБ	24	24	21,7	18,4	20,8	60	50
NEXT	дБ	27,1	30,1	39,9	59	62,1	60,4	35,6
ELFEXT	дБ	17	17,4	23,2	43,1	46,0	35,1	–
Затухание отраженного сигнала (обратная потеря)	дБ	8	10	12	32	14,1	61,93	8
Задержка распространения сигнала	нс	548	548	548	548	504	534	548

^aNEXT (Near-end crosstalk) — ослабление перекрестной наводки на ближнем конце. ELFEXT (Equal level far-end crosstalk) — ослабление равноуровневой перекрестной наводки на дальнем конце.

^bВключая дополнительные спецификации TIA TSB 95 и ISO FDAM 2.

Кабель категории 5 поддерживает работу на скорости 100 Мбит/с. Кабели категорий 5e, 6 и 6a поддерживают скорость передачи 1 Гбит/с и в настоящее время используются в качестве стандарта. Кабель категории 6a лучше всего подходит для организации новых сетей, поскольку он особенно устойчив к помехам, возникающим из-за использования старых стандартов передачи сигналов (например, 10BASE-T). При прокладке кабелей категорий 5 и 5e были зафиксированы определенные проблемы. Кабели категорий 7 и 7a предназначены для передачи данных со скоростью 10 Гбит/с, а кабели категорий 8 — 40 Гбит/с.

Более быстродействующие стандарты требуют применения нескольких пар единственной пары. Для соединений 10BASE-T требуются две пары проводов категории 5. В соединениях 100BASE-TX предельная длина та же, но используются две пары проводов категории 5. Соединение 1000BASE-TX требует четырех пар проводов категорий 5e или 6/6a. Аналогично соединение 10GBASE-TX требует четырех пар проводов категорий 6a, 7 или 7a. Длина кабеля во всех стандартах ограничена 100 м.

Существуют провода с поливинилхлоридной и тефлоновой изоляцией. Выбор изоляции диктуется средой, в которой будут проложены кабели. В замкнутых помещениях, связанных с вентиляционной системой здания, обычно требуется тефлоновая изоляция⁴. Поливинилхлоридная изоляция дешевле и проще в эксплуатации.

⁴Конкретную информацию можно получить у пожарного инспектора или ответственного за пожарную безопасность.

Подключая четырехпарный НВП-кабель к коммутационным панелям и настенным розеткам RJ-45, придерживайтесь стандарта разводки TIA/EIA-568A. Этот стандарт, совместимый с другими вариантами RJ-45 (например, RS-232), позволяет избежать ошибок при разводке концов кабеля, независимо от того, есть ли свободный доступ к парам. Требования стандарта отражены в табл. 14.3.

Таблица 14.3. Стандарт TIA/EIA-568A для подключения четырехпарного НВП-кабеля к розетке RJ-45

Пара	Цвета	Контакты разъема
1	Белый/синий	5/4
2	Белый/оранжевый	3/6
3	Белый/зеленый	1/2
4	Белый/коричневый	7/8

Имеющаяся в здании проводка может не подходить для прокладки сетей, в зависимости от того, как и когда она прокладывалась.

Оптическое волокно

Оптическое волокно используется в тех ситуациях, когда применение медного кабеля по тем или иным причинам неприемлемо. Оптическое волокно передает сигнал быстрее, чем медный провод. Кроме того, оно является более устойчивым к электрическим помехам, что в некоторых приложениях очень важно. Там, где оптическое волокно не является абсолютно необходимым, обычно выбирают медный кабель, поскольку он дешевле и с ним легче работать.

Оптическое волокно бывает “многомодовым” и “одномодовым”. Многомодовое оптическое волокно обычно используется в зданиях или комплексах зданий. Оно толще, чем одномодовое, и может проводить несколько лучей света; это свойство позволяет использовать менее дорогую электронику (например, в качестве источника света можно использовать светодиоды).

Одномодовое оптическое волокно часто используется в магистральных приложениях, например для прокладки линий связи между городами и регионами. Оно может проводить только один световой луч и требует дорогой прецизионной электроники в конечных точках.

Стандарт TIA-598C рекомендует цветовую кодировку оптического волокна, представленную в табл. 14.4. Следует помнить основное правило: все элементы должны соответствовать друг другу. Оптическое волокно, соединяющее конечные точки, оптические кабели перекрестной коммутации и электронные приборы, установленные в конечных точках, должны иметь один и тот же тип и размер. Обратите внимание на то, что кабели OM1 и OM2 не являются взаимозаменяемыми, хотя и окрашены в один и тот же оранжевый цвет — проверьте размеры, указанные на кабелях, чтобы убедиться, что они соответствуют друг другу. Если вы нарушите это правило, то вам будет сложно обеспечить изоляцию в конечных точках.

На концах оптических волокон используются разъемы более чем 30 типов, и нет ни четких правил, ни принципов, регламентирующих их выбор. В каждой конкретной ситуации на выбор того или иного типа разъема влияют поставщики оборудования или параметры оптического волокна, уже проложенного внутри здания.

Таблица 14.4. Атрибуты стандартных оптических волокон

Количество мод	Название ISO*	Диаметр сердечника, мкм	Диаметр оптической оболочки, мкм	Цвет
Много	OM1	62,5	125	Оранжевый
Много	OM2	50	125	Оранжевый
Много	OM3	50 *	125	Голубой
Одна	OS1	8–10	125	Желтый

*В соответствии со стандартом ISO 11801.

°OM3 оптимизирован под лазерный луч.

Соединение и расширение сетей Ethernet

Сети Ethernet можно соединять с помощью устройств нескольких типов. На выбор устройств, описанных ниже, влияет их стоимость, причем более дешевые устройства описаны в первую очередь. Чем сложнее логические правила, по которым устройства перемещают биты из одной сети в другую, тем больше аппаратного и встроенного программного обеспечения необходимо и тем более дорогой становится сеть.

Концентраторы

Концентраторы (hub) иногда еще называют *повторителями* (repeaters). Это активные устройства, используемые для соединения сегментов сетей Ethernet на физическом уровне. Им требуется внешний источник питания.

Выступая в качестве повторителя, концентратор ретранслирует Ethernet-фреймы, но никак не интерпретирует их. Он “не имеет представления” ни о том, куда направляются пакеты, ни о том, какой протокол они используют. За исключением экзотических ситуаций, *концентраторы больше не должны использоваться в промышленных сетях*, и мы не советуем их использовать даже в домашних сетях. (Почему? Потому что коммутаторы (switches) значительно эффективнее используют полосу пропускания частот в сети и в настоящее время стоят недорого.)

Коммутаторы

Коммутатор соединяет сети Ethernet на канальном уровне. Его назначение — объединить две физические сети так, чтобы они выглядели как одна большая физическая сеть. В настоящее время коммутаторы являются промышленным стандартом для соединения устройств Ethernet.

Коммутаторы принимают, регенерируют и ретранслируют пакеты на аппаратном уровне. Они используют алгоритм динамического обучения. Коммутаторы запоминают, какие исходные адреса поступают с одного порта, а какие — с другого. Пакет переходит из одного порта в другой только при необходимости. Первоначально пересылаются все пакеты, но через несколько секунд, когда коммутатор изучит расположение большинства хостов сети, запускается механизм фильтрации.

Поскольку между сетями пересылаются не все пакеты, каждый сегмент кабеля менее загружен, чем в случае, когда все компьютеры подключены к одному кабелю. А если учесть, что основной трафик имеет тенденцию к локализации, то увеличение реальной пропускной способности может оказаться заметным. Кроме того, коммутатор не влияет на логическую модель сети, поэтому его установка требует лишь незначительного вмешательства со стороны администратора.

Если сеть имеет петли, коммутатор может безнадежно запутаться, потому что пакеты, посылаемые одним компьютером, окажутся сразу на двух (или более) портах коммутатора. В одной сети Ethernet петлей не бывает, но после объединения нескольких таких сетей с помощью маршрутизаторов и коммутаторов топология изменится, вследствие чего может образоваться несколько путей к одному хосту. Некоторые коммутаторы решают эту проблему путем резервирования альтернативных маршрутов на тот случай, если основной маршрут станет недоступным. Они упрощают топологию видимой ими сети, отсекая дублирующиеся пути до тех пор, пока в оставшихся сегментах не окажется только по одному маршруту к каждому хосту сети. Другие коммутаторы создают между сетями двойные каналы и переключают трафик по циклическому принципу.

Коммутаторы должны просматривать каждый пакет, определяя, нужно ли его переслать в другой сегмент. Производительность этих устройств обычно измеряют как скоростью просмотра пакетов, так и скоростью их пересылки. Многие поставщики не указывают в диаграммах производительности коммутаторов размеры протестированных пакетов, поэтому реальная производительность может быть ниже объявленной.

Несмотря на то что быстроедействие коммутаторов Ethernet все время растет, эффективно использовать их можно при объединении в один логический сегмент не более сотни компьютеров. В крупных коммутируемых сетях часто возникают проблемы наподобие “широковещательных штормов”, поскольку широковещательный трафик должен проходить через все порты. Для решения этой проблемы нужно изолировать широковещательный трафик между коммутируемыми сегментами посредством маршрутизатора (создавая тем самым более одного логического Ethernet-сегмента).

Выбор коммутатора может представлять определенную трудность. В этом сегменте рынка очень высокая конкуренция, следствием которой являются многочисленные рекламные заявления, не всегда подтверждаемые на практике. Поэтому не стоит особо доверять данным, которые приводятся поставщиками; лучше прислушаться к советам независимых экспертов (просмотрите тесты, приводимые в журналах). В последние годы нередко случалось так, что чей-то продукт оказывался “лучшим” в течение нескольких месяцев, а затем, после попыток внесения улучшений, его производительность или надежность падала ниже критической отметки.

В любом случае убедитесь, что скорость объединительной панели коммутатора является достаточной. У хорошо спроектированного коммутатора эта скорость должна превышать сумму скоростей всех его портов.

Коммутаторы, позволяющие создавать виртуальные локальные сети

В крупных организациях можно использовать коммутаторы, позволяющие разбивать их порты (программным путем) на группы, называемые виртуальными локальными сетями (Virtual Local Area Network — VLAN). Виртуальная локальная сеть — это группа портов, принадлежащая к одному логическому сегменту, как если бы порты были соединены со своим собственным выделенным коммутатором. Подобное секционирование позволяет повысить степень изоляции трафика, что полезно с точки зрения как безопасности, так и производительности.

Трафиком между виртуальными локальными сетями управляет маршрутизатор или, в некоторых случаях, модуль маршрутизации или уровень программной маршрутизации самого коммутатора. Расширение этой системы, называемое *транкингом виртуальной локальной сети* (один из примеров реализации — протокол IEEE 802.1Q), позволяет разным коммутаторам обслуживать порты одной логической виртуальной локальной сети.

Важно помнить, что сами сети VLAN почти не обеспечивают дополнительной защиты. Для того чтобы обеспечить защиту, необходимо фильтровать трафик VLAN.

Маршрутизаторы

Маршрутизаторы (известные также как “коммутаторы третьего уровня”) направляют трафик на третьем сетевом уровне модели OSI. Маршрутизаторы доставляют пакеты адресатам на основании информации, хранящейся в TCP/IP-заголовках. Помимо простого перемещения пакетов, маршрутизаторы могут также выполнять ряд особых функций, например фильтрацию пакетов (в соответствии с правилами безопасности), разделение трафика по приоритетам (в соответствии с заданным качеством обслуживания) и обнаружение общей сетевой топологии.

Конфигурация маршрутизаторов бывает фиксированной или модульной.

- Устройства первого типа содержат сетевые интерфейсы, установленные в заводских условиях. Они обычно подходят для специализированных применений. Например, маршрутизатор с интерфейсами T1 и Ethernet может оказаться удобным, когда нужно подключить небольшую компанию к Интернету.
- Модульные маршрутизаторы имеют слотовую или шинную архитектуру, а интерфейсы к ним добавляются пользователями. Как правило, это более дорогие устройства, но зато они гибче в эксплуатации.

В зависимости от необходимой надежности и ожидаемого трафика, специализированный маршрутизатор может оказаться как дороже, так и дешевле системы UNIX или Linux, сконфигурированной в качестве маршрутизатора. Однако специализированное устройство, как правило, демонстрирует более высокую производительность и надежность. Это та область сетевого проектирования, где лучше заранее вложить чуть больше денег, чем потом иметь головную боль.

Автосогласование

С появлением разных стандартов Ethernet возникла необходимость, чтобы устройства могли идентифицировать конфигурацию своих соседей и согласовывать с ними свои настройки. Например, сеть не будет работать, если на одной стороне соединения она работает со скоростью 1 Гбит/с, а на другой — со скоростью 10 Гбит/с. Для выявления и решения этой проблемы организацией IEEE был разработан стандарт автосогласования Ethernet. В одних случаях он работает, а в других применяется неправильно и лишь усугубляет проблему.

Следует запомнить два золотых правила автосогласования.

- Вы *обязаны* использовать автосогласование всех интерфейсов, работающих на скорости 1 Гбит/с и выше. Этого требует стандарт.
- Если интерфейсы ограничены скоростями 100 Мбит/с и ниже, необходимо либо конфигурировать *оба конца* соединения, либо вручную настроить скорость и дуплекс (половинный или полный) *обеих* сторон. Если в режиме автосогласования настроить только одну сторону соединения, то в большинстве случаев она не сможет выяснить, какую конфигурацию имеет другая сторона. В результате конфигурация станет несогласованной и производительность упадет.

Для того чтобы выяснить, как задать стратегию автосогласования интерфейсов, прочитайте специальный раздел 13.10.

Передача электропитания по сетям Ethernet

Технология передачи питания по сетям Ethernet (Power on Ethernet — PoE) основана на передаче электропитания по той же неэкранированной витой паре (UTP Ethernet), по которой передается сигнал Ethernet. Данная технология регламентируется стандартом IEEE 802.3af. Это особенно удобно для систем связи, обеспечивающих передачу речевого сигнала по сети Интернет (Voice over IP — VoIP), или пунктов доступа к системе беспроводной связи (мы указали только два примера, но список можно продолжить), в которых требуется как маломощный источник питания, так и сетевое соединение.

По мощности питания системы PoE разделяются на четыре класса в диапазоне от 3,84 до 25,5 Вт. Промышленность, которая никогда не останавливается на достигнутом, уже работает над новым стандартом (802.3bt), предусматривающим более высокую мощность (более 60 Вт). Будет ли этого достаточно, чтобы подключить духовку Easy-Bake к сетевому порту в конференц-зале?⁵

Технология PoE порождает два обстоятельства, о которых должен знать системный администратор.

- Вы должны знать о существовании устройств PoE в вашей инфраструктуре, чтобы правильно спланировать доступ к портам коммутаторов, поддерживающих технологию PoE. Эти порты дороже, чем порты, не поддерживающие технологию PoE.
- Вычисляя расход электроэнергии на обслуживание коммуникационных шкафов, содержащих коммутаторы PoE, следует учитывать мощность устройств PoE. Обратите внимание на то, что вы не должны учитывать дополнительный расход электроэнергии на охлаждение коммуникационных шкафов, поскольку большая часть тепла, выделяемого из-за потребления мощности PoE, рассеивается за пределами шкафа (обычно по офису).

Гигантские пакеты

Технология Ethernet стандартизована для типичного пакета размером 1 500 байт (вместе с фреймом — 1 518 байт). Это значение было выбрано давно, когда сети были медленными и память для буферов была дефицитной. В настоящее время пакеты размером 1 500 байт выглядят крохотными в контексте гигабитных сетей Ethernet. Поскольку с каждым пакетом связаны накладные расходы и определенное время задержки, производительность сети можно повысить, если допустить более крупные размеры пакетов.

К сожалению, стандарты IEEE для разных типов сетей Ethernet запрещают использование крупных пакетов по соображениям совместимости сетей. Однако, поскольку скорость магистрального трафика часто во много раз превышает установленный предел, нестандартные большие пакеты Ethernet в современных сетях перестали быть редкостью. Подстрекаемые нетерпеливыми потребителями, производители сетевого оборудования негласно бойкотируют стандарт IEEE и обеспечивают поддержку крупных фреймов в своей гигабитной продукции.

Для использования так называемых *гигантских пакетов* (jumbo frames) необходимо лишь повысить максимально возможный размер пакета (maximal transmission unit — MTU) в интерфейсах сети. Повышение производительности зависит от вида трафика, но наибольший выигрыш достигается для крупномасштабных перемещений по протоколу TCP (например, в файловых службах NFSv4 или CIFS). Ожидается, что умеренное, но заметное повышение производительности должно составить примерно 10%.

⁵Для интересующихся этим вопросом: да, существует возможность загрузить небольшую систему Linux через порт сети PoE. Возможно, проще всего это сделать с помощью Raspberry Pi и коммутатора Pi PoE Switch HAT.

Тем не менее следует отметить следующее.

- Поддерживать и использовать гигантские пакеты должно все сетевое оборудование в подсетях, включая коммутаторы и маршрутизаторы. Их нельзя смешивать и подгонять.
- Поскольку гигантские пакеты являются нестандартными, обычно их необходимо разрешать явным образом. Устройства могут принимать гигантские пакеты по умолчанию, но, вероятнее всего, они не будут их генерировать.
- Поскольку гигантские пакеты представляют собой незаконное явление, не существует соглашения, насколько большими они могут или должны быть. Типичной величиной является 9000 байт или 9018 вместе с фреймом. Необходимо проверить, какой максимальный размер пакета может принять ваше устройство. Пакеты размером больше 9 Кбайт иногда называют сверхгигантскими, но это экзотическое название вас пугать не должно. Чем больше размер, тем лучше, по крайней мере в диапазоне до 64 Кбайт.

Мы одобряем использование гигантских пакетов в гигабитных сетях Ethernet, но будьте готовы к дополнительной отладке, если что-то пойдет не так, как надо. Лучше всего развернуть новую сеть, задав максимально возможный размер пакета по умолчанию, а позднее, когда надежность сети будет проверена, изменить эти настройки и разрешить гигантские пакеты.

14.2. БЕСПРОВОДНЫЕ СЕТИ: ЛОКАЛЬНАЯ СЕТЬ ДЛЯ КОЧЕВНИКОВ

Беспроводные сети состоят из беспроводных точек доступа (Wireless Access Points — WAP) и клиентов беспроводной сети. Точки WAP могут соединяться традиционными проводными сетями (обычная конфигурация) или с другими точками WAP без использования проводов (конфигурация известна под названием “беспроводная сеть”).

Стандарты беспроводных сетей

Распространенными стандартами беспроводных сетей в настоящее время являются IEEE 802.11g, 802.11n и .802.11ac Стандарт 802.11g работает на частоте 2,4 ГГц и обеспечивает доступ к локальной сети со скоростью, достигающей 54 Мбит/с. Радиус действия одной точки доступа колеблется от 100 м до 40 км, в зависимости от оборудования и физических особенностей местности.

Стандарт 802.11n обеспечивает скорость до 600 Мбит/с⁶ и может использовать частоты как 5 ГГц, так и 2,4 ГГц (при этом рекомендуется использовать диапазон 5 ГГц). Радиус действия точки доступа в стандарте IEEE 802.11n в два раза больше, чем в стандарте IEEE 802.11g. Приемником стандарта IEEE 802.11n является стандарт IEEE 802.11ac, поддерживающий производительность многостанционной сети на уровне до 1 Гбит/с.

Все эти стандарты обозначаются одним общим термином Wi-Fi. Формально говоря, метка Wi-Fi ограничена семейством стандартов IEEE 802.11. Однако это лишь один из многих видов аппаратного обеспечения Ethernet, доступных на рынке, поэтому все беспроводные сети Ethernet называются Wi-Fi.

⁶Скорость 600 Мбит/с в стандарте 802.11n является, скорее, теоретической. На практике полоса пропускания в окрестности точки WAP при оптимальной конфигурации может обеспечить скорость передачи данных не более 400 Мбит/с. Это объясняется различием между теоретическими и практическими возможностями оборудования и среды. В беспроводных сетях всякое бывает!

В настоящее время стандарты 802.11g и 802.11n стали общепринятыми. Трансиверы недороги и встроены в большинство ноутбуков. Кроме того, платы расширения также стоят недорого и доступны для любых персональных компьютеров.

Доступ клиентов к беспроводной сети

Вы можете настроить системы UNIX или Linux для подключения к беспроводной сети в качестве клиента, если у вас есть правильное оборудование и драйвер. Поскольку большинство беспроводных плат на базе персональных компьютеров все еще предназначены для системы Microsoft Windows, они могут не поставляться с завода с драйверами FreeBSD или Linux.

При попытке добавить беспроводное подключение к системе FreeBSD или Linux вам, скорее всего, понадобятся следующие команды:

- **ifconfig** — для конфигурирования интерфейса беспроводной сети;
- **iwlist** — для получения списка доступных точек доступа к беспроводной сети;
- **iwconfig** — для настройки параметров беспроводного соединения;
- **wpa_supplicant** — для аутентификации в беспроводной сети (или проводной сети 802.1x).

К сожалению, гонка продаж дешевого оборудования часто означает, что для настройки правильной работы беспроводного адаптера в системе UNIX или Linux может потребоваться много часов проб и ошибок. Планируйте все заранее или выясните в Интернете, какой адаптер лучше всего подходит для вашей операционной системы.

Беспроводные коммутаторы и точки беспроводного доступа

Все хотят иметь доступ к беспроводной сети в любом месте, и для обеспечения этой услуги доступно множество продуктов. Но, как и во многих других областях, вы получаете то, за что платите. Недорогие устройства часто удовлетворяют потребности домашних пользователей, но не могут хорошо масштабироваться в корпоративной среде.

Топология беспроводных сетей

Точки беспроводного доступа (Wireless Access Point — WAP) обычно представляют собой специализированные устройства, состоящие из одной или нескольких радиостанций и некоторой формы встроенной сетевой операционной системы, часто урезанной версии Linux. Одна точка WAP может обеспечить подключение нескольких клиентов, но их число ограничено. Хорошее эмпирическое правило состоит в том, чтобы одновременно обслуживать не более сорока клиентов с помощью одной корпоративной точки WAP. В качестве клиента может действовать любое устройство, которое обменивается данными по беспроводному стандарту, поддерживаемому вашими точками WAP.

Точки WAP имеют один или несколько “служебных идентификаторов сети”, а также идентификатор SSID, который служит именем беспроводной локальной сети и должен быть уникальным в определенной окрестности. Когда клиент хочет подключиться к беспроводной локальной сети, он выясняет, какие идентификаторы SSID доступны, и выбирает одну из этих сетей.

Вы можете сделать имя своего идентификатора SSID осмысленным и легко запоминающимся, например *Third Floor Public* (Третий этаж, открытый доступ), или избрести что-нибудь необычное. Некоторые из наших любимых имен SSID:

- FBI Surveillance Van (Служба наблюдения ФБР);
- The Promised LAN (Обещанная локальная сеть);
- IP Freely (Свободный IP);
- Get Off My LAN (Убирайся из моей локальной сети);
- Virus Distribution Center (Центр распространения вирусов);
- Access Denied (Доступ запрещен).

Нет ничего лучше, чем изобретательные чудачки... В простейших сценариях точка WAP объявляет единственный SSID, ваш клиент подключается к этому SSID и всё — вы в сети!

Тем не менее несколько аспектов беспроводной сети действительно просты. Что делать, если ваш дом или здание слишком большие, чтобы обслуживаться одной точкой WAP? Или что если вам нужно предоставлять разные сети различным группам пользователей (например, сотрудникам или гостям)? Для этих случаев вам необходимо стратегически структурировать свою беспроводную сеть.

Вы можете использовать несколько SSID для разбивки групп пользователей или функций. Как правило, вы сопоставляете их с отдельными виртуальными локальными сетями, которые затем можно маршрутизировать или фильтровать по желанию, как и проводные сети.

Частотный спектр, выделенный для беспроводной сети 802.11, разбивается на полосы, обычно называемые *каналами*. Точка WAP самостоятельно выбирает свободный радиоканал для объявления SSID. Клиенты и точка WAP используют этот канал для связи, формируя единый широкоэвещательный домен. Ближайшие точки WAP, скорее всего, будут выбирать другие каналы, чтобы максимизировать доступную полосу пропускания и минимизировать помехи.

Теория состоит в том, что по мере того, как клиенты перемещаются по окружающей среде, они будут отделяться от одной точки WAP, когда ее сигнал становится слабым, и соединяться с ближней точкой WAP с более сильным сигналом. Однако теория и реальность часто не согласуются друг с другом. Многие клиенты поддерживают связь с точкой WAP, излучающей слабый сигнал, и игнорируют лучшие варианты.

В большинстве ситуаций вы должны разрешить WAP автоматически выбирать свои предпочтительные каналы. Если вы должны вручную вмешаться в этот процесс, используя стандарты 802.11b/g/n, рассмотрите выбор между каналами 1, 6 или 11. Спектр, выделенный этим каналам, не перекрывается, поэтому комбинации этих каналов обеспечивают наибольшую вероятность широкого распространения — открытую беспроводную магистраль. Каналы по умолчанию для 802.11a/ac не перекрываются вообще, поэтому просто выберите свой любимый номер.

Некоторые точки WAP имеют несколько антенн и используют технологию множественного ввода и множественного вывода (multiple-input, multiple-output — MIMO). Эта практика может увеличить доступную полосу пропускания, используя несколько передатчиков и приемников, чтобы использовать преимущества смещения сигнала в результате задержки распространения. В некоторых ситуациях эта технология может обеспечить небольшое улучшение производительности, хотя, вероятно, не такое значительное улучшение, как широкая сеть антенн.

Если вам нужна физически большая зона покрытия, разверните несколько точек WAP. Если область полностью открыта, вы можете развернуть их в структуре решетки. Если существуют физические препятствия вроде стен, проведите исследование для определения наилучших вариантов размещения точек WAP с учетом физических атрибутов вашего пространства.

Дешевая беспроводная связь

Нам нравятся продукты Ubiquiti (ubnt.com) для недорогих, высокопроизводительных домашних сетей. Google Wifi — замечательное облачное решение, если вы поддерживаете связь с удаленными членами семьи. Другим вариантом является запуск урезанной версии Linux (например, OpenWrt или LEDE) на коммерческой точке WAP (см. сайт openwrt.org для получения дополнительной информации и списка совместимого оборудования).

Буквально десятки продавцов сейчас поставляют оборудование для точек беспроводного доступа. Вы можете купить их в Home Depot и даже в продуктовом магазине. Дешевые точки доступа (в диапазоне 30 долл.), вероятно, будут плохо работать при обработке больших файлов или наличии нескольких активных клиентов.

Дорогая беспроводная связь

Большая беспроводная связь означает большие деньги. Предоставление надежной беспроводной сети высокой плотности (в крупных больницах, спортивных учреждениях, школах, городах) представляет собой сложную задачу, связанную с ограничениями физических установок, плотностью пользователей и законами физики. В таких ситуациях вам нужны беспроводные устройства корпоративного класса, которые знают местоположение и состояние каждой точки WAP и активно настраивают каналы WAP, силу сигналов и группы клиентов, чтобы обеспечить наилучшие результаты. Эти системы обычно поддерживают прозрачный роуминг, который позволяет группе клиентов с определенной виртуальной локальной сетью и сессией беспрепятственно перемещаться между точками WAP.

Наши любимые крупные беспроводные платформы — это Aerohive и Meraki (последняя принадлежит компании Cisco). Эти платформы следующего поколения управляются из облака, что позволяет вам пить martini на пляже, контролируя свою сеть через браузер. Вы даже можете выбросить отдельных пользователей из беспроводной сети, не вставая с шезлонга. Уйди, противный!

Если вы развертываете беспроводную сеть в больших масштабах, вам, вероятно, придется приобрести анализатор беспроводной сети. Мы настоятельно рекомендуем аналитические продукты, разработанные компанией AirMagnet.

Безопасность беспроводных сетей

Традиционно безопасность беспроводных сетей очень низкая. Существует протокол WEP (Wired Equivalent Privacy), применяемый в сетях 802.11b и для шифрования пакетов, передаваемых с помощью радиоволн. К сожалению, в современной версии стандарта была обнаружена фатальная проектная недоработка, которая делает его практически бесполезным. Посторонний человек, находящийся за пределами здания, может получить прямой доступ к сети и остаться незамеченным.

Тем не менее недавно появившиеся стандарты Wi-Fi Protected Access (WPA) возродили доверие к безопасности беспроводных сетей. В настоящее время во всех новых инсталляциях должны использоваться стандарты WPA (в частности, стандарт WPA2), а не WEP. Без применения стандарта WPA2 беспроводные сети должны считаться полностью незащищенными и не должны использоваться за пределами предприятия. Даже дома не используйте стандарт WEP!

Для того чтобы запомнить, что стандарт WEP является незащищенным, а стандарт WPA — безопасным, просто расшифруйте аббревиатуру WAP (Wired Equivalent Privacy — конфиденциальность на уровне проводных сетей). Это название точно отражает суть дела; протокол WEP обеспечивает такую защиту, как проводная сеть, допускающая

непосредственное подключение посторонних лиц. (Иначе говоря, никакой защиты — по крайней мере на уровне IP.)

14.3. SDN: ПРОГРАММНО-КОММУТИРУЕМЫЕ СЕТИ

Как и при виртуализации серверов, разделение физического сетевого оборудования с функциональной архитектурой сети может значительно повысить гибкость и управляемость. Лучшим средством для достижения этих целей являются программно-коммутируемые сети (software-defined networking — SDN).

Основная идея SDN заключается в том, что компоненты, управляющие сетью (плоскость управления), физически отделены от компонентов, которые пересылают пакеты (плоскость данных). Плоскость данных программируется через плоскость управления, поэтому вы можете настраивать или динамически изменять маршруты передачи данных для достижения целей производительности, безопасности и доступности.

Как и многое в нашей отрасли, SDN для корпоративных сетей превратилась в маркетинговый трюк. Первоначальная цель состояла в том, чтобы стандартизировать независимые от поставщика способы перенастройки сетевых компонентов. Несмотря на то что некоторые из этих планов были реализованы, многие поставщики теперь предлагают собственные продукты SDN для предприятий, которые в какой-то мере степени противоречат первоначальной цели SDN. Если вы изучаете пространство предприятия SDN, выбирайте продукты, соответствующие открытым стандартам и совместимые с продуктами других поставщиков.

Для крупных поставщиков облачных вычислений SDN добавляет уровень гибкости, который уменьшает вашу потребность знать (или заботиться) о том, где определенный ресурс находится физически. Хотя эти решения могут быть коммерческими, они тесно интегрированы в платформы облачных провайдеров и могут упростить настройку вашей виртуальной инфраструктуры.

Сеть SDN и ее система управления, основанная на интерфейсах API, предлагают системным администраторам соблазнительную возможность интегрировать управление топологией сети с другими инструментами стиля DevOps для непрерывной интеграции и развертывания. Возможно, в каком-то идеальном мире у вас всегда есть производственная среда, поставленная и готовая к активации одним щелчком мыши. По мере того как новая среда продвигается к производству, сетевая инфраструктура магическим образом преобразуется, устраняя простои, заметные для пользователя, и необходимость планировать окна обслуживания.

14.4. ТЕСТИРОВАНИЕ И ОТЛАДКА СЕТЕЙ

Ключ к отладке сети — ее разбивка на сегменты и тестирование каждого из них до тех пор, пока не будет обнаружена неисправность. Загадочные лампочки на коммутаторах и концентраторах (обозначающие, к примеру, состояние канала и наличие трафика пакетов) помогают быстро выявить источник проблемы. Для того чтобы эти индикаторы работали так, как вы хотите, следует руководствоваться первоклассной документацией.

Как всегда, важно иметь под рукой нужные инструменты, чтобы выполнить работу правильно и без проволочек. На рынке предлагаются средства сетевой отладки двух типов (правда, наблюдается тенденция к их объединению).

Устройство первого типа — ручной кабельный тестер. Он измеряет электрические характеристики кабеля, включая его длину (для этого применяется особая технология,

называемая рефлектометрией во временной области). Такие устройства способны выявлять простейшие проблемы, например разрыв или неправильную разводку кабеля.

Нашим любимым инструментом тестирования локальных сетей является устройство Fluke LanMeter. Это универсальный анализатор, способный даже посылать эхо-пакеты протокола ICMP. Профессиональные варианты этого оборудования описаны на специальном веб-сайте. Для телекоммуникационных сетей WAN лучше всего подходит тестер T-BERD, выпускаемый компанией Viavi (viavisolutions.com).

Средства отладки второго типа — это анализаторы сетевых пакетов. Они просматривают сетевые пакеты на предмет наличия ошибок протоколов, неправильной конфигурации и прочего беспорядка. Эти анализаторы работают на уровне каналов, а не на электрическом уровне, поэтому они не могут распознавать проблемы, связанные с физическими повреждениями кабелей или электропитанием.

Существуют профессиональные анализаторы сетевых пакетов, но мы нашли свободно распространяемую программу Wireshark⁷ (wireshark.org), которая может выполняться на полнофункциональном ноутбуке. Именно ее можно считать наилучшим выбором. Более подробная информация об анализаторах сетевых пакетов приведена в разделе 13.12.

14.5. Прокладка кабелей

Если вы занялись прокладкой кабелей в здании, то самый ценный совет, который мы можем вам дать, звучит так: “Делайте все правильно с первого раза”. Это не та область, в которой можно скупиться или халтурить. Покупая качественные материалы, выбирая компетентного подрядчика для прокладки кабелей и устанавливая дополнительные разъемы (отводы), вы тем самым избежите многолетних мучений.

Неэкранированная витая пара

Кабель категории 6a имеет наилучшее соотношение цены и производительности на современном рынке. Его стандартный вариант — четыре пары проводов под одной оболочкой, что подходит для большинства соединений, включая RS-232 и гигабитные линии.

Спецификации кабеля категории 6a требуют, чтобы скрутка провода заканчивалась в точке контакта. Для того чтобы обеспечить это требование, необходимы специальное обучение и окончное оборудование. При этом необходимо использовать настенные розетки и коммутационные панели категории 6a. Самые хорошие отзывы заслужила продукция компании Siemon.

Офисные точки подключения

Многие годы идут споры, сколько точек подключения требуется для офиса. Одной точки подключения на офис явно недостаточно. Сколько же нужно — две или четыре? Мы рекомендуем четыре, обосновывая это следующими причинами.

- Их можно использовать просто для подключения телефонов и других специализированных устройств.
- Большинство пользователей предпочитают подключаться с помощью беспроводных сетей, а не проводов.
- Гораздо дешевле проложить весь кабель сразу, чем делать это поэтапно.

⁷Как и многие популярные программы, программа Wireshark часто подвергается атакам хакеров. Убедитесь, что вы используете самую последнюю ее версию.

- Средства, выделенные на приобретение проводов, лучше потратить на основную инфраструктуру, а не на оборудование отдельных офисов.

При прокладке кабеля в здании можно установить дополнительные розетки в коридорах, конференц-залах, столовых, туалетных комнатах и на потолках (для точек беспроводного доступа). Однако не забывайте о безопасности и размещайте открыто предоставляемые порты на “гостевой” виртуальной локальной сети, не допуская посторонних к своим внутренним сетевым ресурсам. Публикуя защищенные публичные порты, используйте стандарт аутентификации 802.1x.

Стандарты кабельных систем

Необходимость обеспечения всех видов деятельности внутри современных зданий обуславливает потребность в крупной и сложной кабельной инфраструктуре. Заглянув в обычный коммутационный шкаф, вы будете потрясены, увидев его стенки, сплошь покрытые непомятыми проводами одного цвета.

С целью улучшения оперативного контроля и стандартизации кабельных систем зданий в феврале 1993 г. организация TIA опубликовала административный стандарт на телекоммуникационную инфраструктуру коммерческих зданий (TIA/EIA-606). В 2012 г. появилась его обновленная версия TIA/EIA-606-B.

Этот стандарт устанавливает требования и принципы идентификации и документирования телекоммуникационной инфраструктуры. Он касается следующих аспектов:

- оконечной аппаратуры;
- кабелей;
- прокладки кабелей;
- расстояний между элементами оборудования;
- цветовой маркировки;
- символических обозначений стандартных компонентов.

В частности, определены стандартные цвета маркировки проводов (табл. 14.5).

Таблица 14.5. Таблица цветовой маркировки по стандарту TIA/EIA-606

Тип оконечного устройства	Цвет	Код ^а	Комментарии
Граничное	Оранжевый	150C	Центральная телефонная станция
Сетевые соединения	Зеленый	353C	Также применяется для вспомогательных электросетей
Общее оборудование ^б	Фиолетовый	264C	Основное оборудование коммутации и передачи данных
Магистраль первого уровня	Белый	—	Кабели
Магистраль второго уровня	Серый	422C	Кабели
Станция	Синий	291C	Горизонтальные кабели
Магистраль между зданиями	Коричневый	465C	Кампусные кабели
Разное	Желтый	101C	Служебные и сигнальные линии
Ключевые телефонные системы	Красный	184C	—

^аВ соответствии с цветовой моделью Pantone.

^бОфисные АТС, компьютеры, локальные сети, мультиплексоры и т.д.

14.6. ПРОЕКТИРОВАНИЕ СЕТЕЙ

В этом разделе рассматриваются вопросы, связанные с логическим и физическим проектированием сетей среднего размера. Представленные здесь идеи подходят для нескольких сотен хостов, но неприменимы ни для трех, ни для нескольких тысяч компьютеров, включенных в одну сеть. Также предполагается, что работа будет начата с нуля.

Основной объем работ по проектированию сети состоит из определения:

- типов сред передачи;
- топологии и способов прокладки кабелей;
- системы концентраторов, коммутаторов и маршрутизаторов.

Еще один ключевой вопрос проектирования сети связан с управлением перегрузкой. Например, файловые протоколы NFS и SMB очень сильно загружают сеть, поэтому такие файловые системы нежелательно подключать по магистральному кабелю.

Ниже анализируются аспекты, которые необходимо учитывать при проектировании сети.

Структура сети и архитектура здания

Структуру сети проще изменить, чем архитектуру здания, но обе они должны нормально сосуществовать. Если вам крупно повезло, т.е. представилась возможность проектировать сеть до постройки здания, будьте щедрым. К сожалению, в большинстве случаев здание и отдел технического обслуживания компании на момент проектирования сети уже существуют и налагают жесткие ограничения на структуру сети.

В уже построенных зданиях сеть должна адаптироваться к архитектуре, а не противостоять ей. В современных зданиях, помимо высоковольтной электропроводки, водопроводов, иногда имеются каналы для прокладки кабелей. Часто монтируются подвесные потолки — настоящий подарок для тех, кто прокладывает сеть. Во многих университетских городках существуют туннели, которые облегчают создание сетей.

Необходимо следить за целостностью брандмауэров.⁸ При прокладке кабеля через брандмауэр отверстие должно соответствовать диаметру кабеля и заполняться негорючим веществом. Выбирая кабель, учитывайте наличие приточной вентиляции. Если узнают, что вы нарушили правила пожарной безопасности, вас могут оштрафовать и заставить устранить недостатки, даже если для этого придется проложить заново всю сеть.

Логическая структура сети должна соответствовать физическим ограничениям зданий, в которых она будет функционировать. Приступая к проектированию, помните, что можно найти логически красивое решение, а затем вдруг обнаружить, что реализовать его физически сложно или вообще невозможно.

Расширение сетей

Прогнозировать потребности на десять лет вперед очень сложно, особенно в области вычислительной техники и сетей. Поэтому, проектируя сеть, всегда следует учитывать перспективы ее расширения и увеличения пропускной способности. Прокладывая кабель, особенно в труднодоступных местах, протягивайте в три-четыре раза больше пар,

⁸Речь идет о брандмауэрах в виде бетонных, кирпичных или огнеупорных стен, которые препятствуют распространению огня по всему зданию. Значительно отличаясь от сетевых брандмауэров, они не менее важны.

чем нужно. Помните: основная часть стоимости прокладки сети приходится на оплату труда, а не на материалы.

Даже если волоконно-оптические линии не планируется использовать немедленно, разумно будет все же проложить немного оптического волокна, особенно если известно, что впоследствии протянуть его будет гораздо труднее. Прокладывайте и многомодовый, и одномодовый кабели. Как правило, нужным оказывается как раз тот кабель, который не проложен.

Перегрузка

Сеть — как цепь: ее качество определяется самым слабым или самым медленным звеном. Производительность Ethernet, как и многих других сетевых технологий, при увеличении нагрузки падает.

Активно эксплуатируемые коммутаторы, нестыкующиеся интерфейсы, низкоскоростные каналы связи — все это может привести к перегрузке. Эффективный способ борьбы с ней заключается в локализации трафика путем создания подсетей и установки маршрутизаторов. Подсети можно использовать и для изоляции компьютеров, задействованных в отдельных экспериментах. Трудно проводить эксперимент на нескольких компьютерах, если нет надежного способа изолировать их физически и логически от остальной части сети.

Обслуживание и документирование

Опыт показывает, что удобство обслуживания сети напрямую зависит от качества документации на нее. Точная, полная, своевременно корректируемая документация абсолютно необходима.

Кабели следует маркировать во всех точках подключения. Рекомендуем вкладывать копии местных монтажных схем в коммутационные шкафы, чтобы при всех изменениях эти экземпляры можно было скорректировать на месте. Каждые несколько недель необходимо переносить все корректировки в электронную базу данных.

Стыки между крупными системами в виде коммутаторов или маршрутизаторов могут упростить отладку, поскольку позволяют изолировать части сети и отлаживать их по отдельности. Полезно также разграничивать административные области.

14.7. УПРАВЛЕНИЕ СЕТЬЮ

Если необходимо обеспечить нормальную работу сети, одни функции управления следует централизовать, другие — распределить, а третьи — оставить на локальном уровне. Требуется сформулировать и согласовать обоснованные “правила поведения добропорядочных граждан”.

Типичная крупномасштабная среда включает в себя:

- магистральную сеть, соединяющую здания;
- сети подразделений, подключенные к магистрالي;
- подсети рабочих групп в рамках подразделения;
- соединения с внешним миром (например, с Интернетом или периферийными филиалами).

При проектировании и реализации сетей следует предусматривать централизованные контроль, ответственность, сопровождение и финансирование. Поскольку подразделения, как правило, стремятся свести к минимуму собственные расходы, быстро растет число сетей с централизованной оплатой каждого соединения. Вот основные объекты централизованного управления:

- структура сети, в том числе принципы использования подсетей, маршрутизаторов, коммутаторов и т.д.;
- магистральный кабель, в том числе подключения к нему;
- IP-адреса и имена компьютеров, доменные имена;
- используемые протоколы (требуется обеспечить их взаимодействие);
- правила доступа в Интернет.

Имена доменов, IP-адреса и сетевые имена компьютеров в определенном смысле уже находятся под централизованным контролем таких организаций, как ARIN (American Registry for Internet Numbers) и ICANN, но координация использования этих элементов на локальном уровне также необходима.

Центральный орган управления имеет общее представление о сети, ее структуре, производительности и перспективах роста. Он может позволить себе иметь собственное контрольное оборудование (и обслуживающий его персонал) и следить за нормальной работой магистральной сети. Центральный орган может настоять на правильном выборе структуры сети, даже если для этого придется заставить подразделение купить маршрутизатор и создать подсеть для подключения к магистрале. Такое решение иногда необходимо для того, чтобы новое соединение не навредило работе существующей сети.

Если в сети работают разнородные компьютеры, операционные системы и протоколы, обязательно нужно иметь “высокоинтеллектуальный” маршрутизатор (например, компании Cisco), который будет служить шлюзом между сетями.

14.8. РЕКОМЕНДУЕМЫЕ ПОСТАВЩИКИ

Занимаясь более 30 лет инсталляцией сетей по всему миру, мы не раз обжигались на продуктах, которые не соответствовали спецификациям, имели завышенную цену, неправильно указанные характеристики или как-то иначе не оправдывали ожидания. Ниже приведен список поставщиков, которым мы доверяем и услугами которых рекомендуем пользоваться.

Кабели и разъемные соединения

AMP
(подразделение Tyco)
(800) 522-6752
amp.com

Anixter
(800) 264-9837
anixter.com

Black Box Corporation
(724)746-5500
blackbox.com

Belden Cable
(800) 235-3361
(765) 983-5200
belden.com

Siemon Company
(860) 945-4395
siemon.com

Newark Electronics
(800) 463-9275
newark.com

Тестовые приборы

Fluke
(800) 443-5853
fluke.com

Siemon
(800) 945-4395
siemon.com

Viavi
(844) 468-4284
vivasolutions.com

Маршрутизаторы/коммутаторы

Cisco Systems
(415) 326-1941
www.cisco.com

Juniper Network
(408) 745-2000
juniper.com

14.9. ЛИТЕРАТУРА

- ANSI/TIA/EIA-568-A. *Commercial Building Telecommunications Cabling Standard* и ANSI/TIA/EIA-606, *Administration Standard for the Telecommunications Infrastructure of Commercial Buildings*. Это стандарты телекоммуникационной промышленности для построения кабельных систем зданий. К сожалению, они не бесплатны. Посетите веб-сайт www.tiaonline.org.
- BARNETT DAVID, GROTH DAVID AND JIM McBEE. *Cabling: The Complete Guide to Network Wiring (3rd edition)*. San Francisco: Sybex, 2004.
- GORANSSON, PAUL, AND CHUCK BLACK. *Software Defined Networks, A Comprehensive Approach (2nd Edition)*. Burlington, MA: Morgan Kaufman, 2016.
- SPURGEON, CHARLES, AND JOANN ZIMMERMAN. *Ethernet: The Definitive Guide: Designing and Managing Local Area Networks (2nd Edition)*. Sebastopol, CA: O'Reilly, 2014.