

Александр Кенин

# **Практическое руководство СИСТЕМНОГО АДМИНИСТРАТОРА**

Санкт-Петербург

«БХВ-Петербург»

2010

УДК 681.3.06  
ББК 32.973.26-018.2  
К35

**Кенин А. М.**

К35 Практическое руководство системного администратора. — СПб.: БХВ-Петербург, 2010. — 464 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0435-5

Практическое руководство к действию для системных администраторов, создающих и эксплуатирующих информационные системы офиса. Наряду с описанием коммерческих продуктов, рассматриваются решения на основе открытых кодов, не требующих приобретения лицензий. Автор обобщил собственный богатый практический опыт и интернет-ресурсы по теме в единое целое и представил рекомендации по установке, настройке и оптимизации основных служб офиса.

Рассмотрены особенности разворачивания операционных систем Windows и Linux (Ubuntu), программ корпоративной работы, мониторинга состояния серверов. Даны конкретные рекомендации по настройке основных сетевых служб, оптимизации почтового сервера, обеспечению безопасности при распределенной работе в Интернете. Описана технология разрешения проблем в работе операционной системы и прикладных программ, приведены многочисленные советы по их тонкой настройке. Подробно изложен процесс создания собственной бесплатной IP-телефонии офиса.

*Для системных администраторов*

УДК 681.3.06  
ББК 32.973.26-018.2

### **Группа подготовки издания:**

Главный редактор	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Григорий Добин</i>
Редактор	<i>Леонид Кочин</i>
Компьютерная верстка	<i>Натальи Караваевой</i>
Корректор	<i>Виктория Пиотровская</i>
Дизайн серии	<i>Инны Тачиной</i>
Оформление обложки	<i>Елены Беляевой</i>
Зав. производством	<i>Николай Тверских</i>

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.10.09.

Формат 70×100<sup>1</sup>/<sub>16</sub>. Печать офсетная. Усл. печ. л. 37,41.

Тираж 2000 экз. Заказ №

"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию № 77.99.60.953.Д.005770.05.09 от 26.05.2009 г. выдано Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов  
в ГУП "Типография "Наука"  
199034, Санкт-Петербург, 9 линия, 12

# Оглавление

<b>Введение.....</b>	<b>1</b>
От автора.....	1
Открытое программное обеспечение.....	2
Открытые стандарты и проприетарные решения.....	7
Windows и Linux.....	8
<b>Глава 1. Сетевая инфраструктура.....</b>	<b>9</b>
Строение сети передачи данных.....	9
Размеры сегментов сети.....	9
Выбор типа коммутаторов.....	10
Топология сети передачи данных.....	11
Ищем точку подключения компьютера.....	12
Контроль подключения к СКС.....	15
Предварительные настройки для использования протокола 802.1x.....	17
Настройка политики доступа на основе протокола 802.1x.....	18
Настройка коммутатора для работы с протоколом 802.1x.....	21
Обеспечение отказоустойчивой работы сетевой инфраструктуры.....	22
Отказоустойчивая топология сети передачи данных.....	22
Построение отказоустойчивой сети на основе протоколов второго уровня.....	23
Построение отказоустойчивой сети на основе протоколов третьего уровня.....	25
Время восстановления структуры сети.....	27
Настройка протокола IP.....	28
Протоколы UDP, TCP, ICMP.....	29
IPv6.....	29
Параметры TCP/IP-протокола.....	29
IP-адрес.....	29
Групповые адреса.....	30
Распределение IP-адресов сети малого офиса.....	31

Маска адреса .....	31
Шлюз (Gateway, default gateway) .....	33
Таблицы маршрутизации .....	33
Назначение адресов при совместном использовании подключения к Интернету .....	34
Порт.....	35
Имена компьютеров в сети TCP/IP .....	37
Проверка каналов связи .....	37
Диагностика линий связи.....	38
Диагностика IP-протокола .....	39
<b>Глава 2. Сетевые службы .....</b>	<b>47</b>
Служба автоматического назначения параметров IP-адреса.....	47
Адресация APIPA .....	47
Серверы DHCP .....	48
Настройка серверов DHCP в Windows .....	48
Установка и настройка сервера DHCP в Ubuntu .....	50
Обслуживание DHCP-сервером других сегментов сети.....	51
Отказоустойчивая конфигурация DHCP-сервера.....	52
Статическое разрешение имен .....	53
Серверы DNS.....	54
Основные понятия DNS.....	54
Основные типы записей DNS .....	57
Разделение DNS.....	58
Одинаковые имена локального домена и домена Интернета.....	58
Различные имена локального домена и домена Интернета.....	60
Установка сервера DNS .....	60
Установка DNS в Windows Server.....	61
Установка и настройка сервера DNS в Ubuntu .....	62
Динамическое обновление DNS.....	65
Обслуживание и диагностика неисправностей DNS-сервера.....	68
<b>Глава 3. Обеспечение доступа в Интернет.....</b>	<b>73</b>
Подключение к Интернету с использованием аппаратного маршрутизатора .....	73
NAT .....	75
Подключение к Интернету с использованием службы маршрутизации и удаленного доступа серверов Windows .....	76
Совместное использование интернет-подключения.....	77
Публикация компьютеров в Интернете при совместном использовании подключения.....	78
Ограничения совместного использования подключения к Интернету ....	79

Подключение к Интернету с помощью Microsoft ISA Server.....	79
Настройка прокси-сервера.....	81
Анализаторы логов.....	81
Поиск причин запрета трафика.....	82
Подключение к Интернету с использованием серверов Ubuntu .....	82
Настройка ufw.....	83
Межсетевой экран iptables.....	84
Последовательность обработки пакета (таблицы) .....	84
Использование iptables в Ubuntu .....	85
Правила iptables .....	86
Команды .....	87
Параметры .....	87
Опции .....	88
Настройка NAT .....	89
Очистка всех правил iptables .....	90
Назначение политик по умолчанию.....	91
Пример настройки iptables.....	91
Пользовательские цепочки команд.....	92
Некоторые полезные функции iptables.....	93
Отладка iptables.....	94
Настройка VPN-подключения к интернет-провайдеру.....	95
Прокси-сервер .....	98
Автообнаружение прокси-серверов .....	99
Установка и настройка прокси-сервера .....	101
Дополнительные настройки прокси-сервера.....	102
Как создавать собственные настройки .....	103
Настройка использования полосы пропускания.....	104
Блокировка рекламы, порносайтов и т. п. ....	106
Улучшение эффективности использования кэша прокси-сервера .....	107
Аутентификация доступа в Интернет .....	108
"Прозрачный" прокси-сервер .....	110
Анализ журналов работы прокси-сервера.....	110
Антивирусная проверка HTTP-трафика .....	113
<b>Глава 4. Готовим новый компьютер к эксплуатации.....</b>	<b>117</b>
Паспорт компьютера .....	117
Установка системных обновлений.....	118
Варианты установки программного обеспечения нового компьютера .....	118
Индивидуальная настройка серверов.....	119
Установка обновлений безопасности .....	120
Когда устанавливать обновления .....	120

Настройка обновлений с сервера интрасети.....	122
Нужно ли устанавливать все обновления? .....	124
Клонирование систем .....	125
WAIK .....	125
Дублирование жесткого диска.....	125
Подготовка к клонированию: утилита sysprep .....	126
Восстановление системы .....	128
Подготовка образа диска к восстановлению на отличающемся оборудовании .....	129
Клонирование компьютеров-членов домена.....	130
Сброс пароля администратора Windows .....	130
<b>Глава 5. Доменная организация информационной системы .....</b>	<b>135</b>
Структура домена Windows .....	135
Хозяева операций .....	137
Сервер глобального каталога (GC).....	138
Создание нового домена .....	139
Создание домена на серверах Windows .....	139
Настройка Ubuntu в качестве контроллера домена.....	140
Серверы Linux в качестве контроллеров домена.....	140
Настройка контроллера домена на сервере корпоративной почты Zimbra .....	141
Настройка параметров аутентификации .....	146
Добавление новых членов домена .....	149
Добавление Windows-систем .....	149
Модификация настроек Windows-систем при добавлении их в домен .....	151
Добавление Linux-систем в домен Windows .....	152
Диагностика службы каталогов.....	153
Обнаружение неисправностей AD.....	154
Средства тестирования AD.....	154
Проверка разрешения имен .....	158
<b>Глава 6. Настройка почтовой системы предприятия .....</b>	<b>161</b>
Варианты почтового обслуживания пользователей .....	161
Протоколы для работы с почтовыми ящиками.....	162
Создание простого POP3-сервера .....	163
Почтовый сервер Microsoft Exchange .....	166
Выбор компьютера для установки Microsoft Exchange.....	167
Установка Exchange Server.....	168
Настройка Exchange Server после установки.....	169
Настройка почтовых доменов .....	170

Настройка кодировки электронных сообщений .....	170
Настройка отправки автоматических сообщений .....	171
Настройка протоколирования сообщений .....	172
Настройка встроенной антиспам-защиты .....	174
Опциональные настройки .....	178
Настройка фильтрации вирусов .....	183
Контроль за работой сервера Exchange .....	185
Резервное копирование сервера Exchange .....	188
Обслуживание почтовых баз .....	189
Использование базы восстановления .....	193
Трассировка пользовательских сообщений в Exchange .....	195
Zimbra Collaboration Suite .....	195
Возможности совместной работы в ZCS .....	196
Установка Zimbra .....	197
Администрирование ZCS .....	199
Особенности пользовательских почтовых ящиков Zimbra .....	203
Почтовый клиент Zimbra .....	204
Интеграция с Microsoft Outlook .....	205
Особенности настройки фильтрации спама в ZCS .....	205
Резервное копирование Zimbra .....	206
Трассировка сообщений в Zimbra .....	207
Поиск неисправностей ZCS .....	208
<b>Глава 7. Организация корпоративных ресурсов .....</b>	<b>209</b>
Использование распределенной файловой системы .....	210
Создание DFS в Windows-системах .....	210
Репликация DFS в домене Windows .....	212
Репликация папок в рабочих группах .....	214
Настройка DFS в Ubuntu .....	215
Лимитирование предоставляемых файловых ресурсов .....	215
Настройка квотирования в Ubuntu .....	215
Настройка квотирования в Windows .....	218
Квотирование на уровне файловой системы .....	218
Квотирование общих папок .....	219
Блокировка записи в папки по типам файлов в Windows .....	221
Запрет записи на сетевые ресурсы Ubuntu по типам файлов .....	223
Корпоративные порталы .....	223
Установка Liferay на сервере Ubuntu .....	224
Установка eGroupware .....	226
Настройка диаграммы Ганта .....	229

Установка служб Windows SharePoint Services .....	230
Установка дополнительных шаблонов SharePoint .....	233
Настройка страниц узла .....	235
Используйте возможности штатных элементов SharePoint.....	236
Установка поискового сервера по общим ресурсам.....	237
Настройка автоматических оповещений об изменениях документов на чужих серверах .....	239
<b>Глава 8. Обеспечение удаленной работы пользователей .....</b>	<b>241</b>
Терминальный доступ .....	241
Терминальные серверы от Microsoft .....	242
Особенности установки ПО на сервере терминалов .....	243
Безопасность при работе с терминальным сервером .....	244
Удаленные приложения .....	245
Web-доступ к терминальному серверу. Шлюз терминалов.....	247
Некоторые особенности работы в режиме терминального доступа.....	248
Подключение к консоли.....	249
Командная строка управления терминальными сессиями .....	249
Терминальные серверы в Linux .....	250
Технологии доставки виртуального рабочего стола .....	250
Удаленное подключение пользователей к внутренней сети предприятия.....	251
Создание входящего VPN-подключения на рабочих станциях Windows .....	252
Создание входящих VPN-подключений на серверах Windows .....	253
Безопасное объединение локальных сетей офисов .....	253
Подключение офисов по VLAN.....	254
Подключение удаленных офисов с использованием VPN-серверов Windows .....	255
Фильтрация VPN-трафика .....	256
В случае разрыва канала при доменной организации офиса.....	257
Read-only domain controllers .....	258
Подключение удаленных офисов с использованием ПО Microsoft ISA Server .....	262
Подключение удаленных офисов с помощью VPN-серверов Ubuntu.....	262
Подключение "офис - офис" на основе технологии SSH .....	265
Применение Ubuntu для маршрутизации в сети филиалов .....	270
Управление оборудованием по сети Интернет .....	270
Intelligent Platform Management Interface .....	271
Управление оборудованием по сети IP.....	273
Утилиты удаленного управления Windows.....	274



<b>Глава 9. Мониторинг информационной системы .....</b>	<b>275</b>
Зачем нужен мониторинг .....	275
Системы мониторинга .....	276
Принципы мониторинга систем .....	277
Контроль журналов Windows .....	277
Operation Manager 2007 .....	281
Установка сервера Operation Manager 2007.....	282
Необходимые операции по настройке сервера после установки .....	284
Импорт пакетов мониторинга.....	284
Добавление контролируемых систем .....	285
Настройка оповещений SCOM.....	287
Немного о структуре объектов SCOM .....	288
Установка Nagios .....	289
Первичное подключение к Nagios .....	292
Немного о логике работы Nagios.....	293
Структура конфигурационных файлов Nagios .....	296
Описание команд Nagios.....	296
Описание шаблонов служб .....	297
Описания служб Nagios.....	298
Описание контролируемых систем в Nagios.....	299
Описание временных параметров .....	301
Использование встроенных в Nagios команд контроля.....	302
Настройка мониторинга серверов Windows .....	306
Настройка мониторинга серверов Linux .....	313
Установка плагина NRPE из исходных кодов .....	313
Установка NRPE из подготовленных пакетов для контроля Linux-системы .....	314
Установка дополнительных плагинов .....	315
Использование прокси-NRPE.....	315
Мониторинг журналов событий Windows .....	315
Мониторинг систем с использованием протокола SNMP.....	317
Мониторинг Windows-систем на основе WMI.....	322
Мониторинг коммутационного оборудования.....	326
Использование собственных программ мониторинга .....	330
Отображение собранных данных на графиках.....	331
Как это работает.....	332
Установка Nagiosgraph .....	332
Редактирование интерфейса Nagios.....	335
Завершение установки.....	337
Создание графиков новых служб.....	337
Автоматическое реагирование на сбой в работе контролируемых систем.....	337

<b>Глава 10. Поиск и устранение неисправностей .....</b>	<b>341</b>
Где найти помощь .....	341
Что может отказать .....	343
Неисправности кабельной подсистемы .....	344
Неисправности активного (коммутационного) оборудования .....	346
Неисправности аппаратной части компьютеров .....	346
Резервирование узлов компьютера .....	347
Контроль теплового режима работы системы .....	348
Ошибки программного обеспечения .....	349
Выяснение причин катастрофических ошибок в программном обеспечении .....	349
Восстановление "упавших" систем .....	352
Загрузка в безопасном режиме .....	352
Загрузка последней удачной конфигурации .....	353
Консоль восстановления .....	353
Режим восстановления в Windows XP SP2/Windows 2003 Server .....	354
Варианты восстановления Windows Vista/Windows Server 2008 .....	355
Восстановление реестра из файлов точек восстановления системы .....	356
Использование программ типа ERD Commander .....	358
Восстановление удаленных данных .....	358
Корзины .....	359
Восстановление из теневых копий .....	359
Восстановление данных с жестких дисков .....	361
Анализ производительности .....	362
Счетчики состояния системы .....	364
Оценка производительности процессора .....	365
Оценка использования оперативной памяти .....	367
Оценка дисковой подсистемы .....	367
Оценка работы сетевого адаптера .....	369
Счетчики прикладных программ .....	369
Server Performance Advisor .....	369
Диагностика доступа к ресурсам компьютера .....	371
<b>Глава 11. Организация IP-телефонии офиса .....</b>	<b>373</b>
Программная АТС .....	373
Подключение IP АТС к телефонным станциям общего пользования .....	374
IP-телефоны: выбор и необходимые настройки сети .....	375
Установка Asterisk .....	378
Локализация Asterisk .....	380
Первоначальная проверка Asterisk .....	380

Настройка АТС .....	383
Диагностика АТС .....	383
Настройка конфигурации SIP-телефонов .....	384
Настройка плана звонков.....	385
Синтаксис шаблонов номеров телефонных линий.....	389
Настройка плана звонков на разные периоды времени .....	390
Создание голосового меню .....	392
Настройка голосовой почты .....	393
Настройка групп вызова и перехвата звонка .....	394
Запись звукового сообщения .....	395
Телефонная книга .....	399
Конференции .....	400
Некоторые дополнительные возможности Asterisk .....	401
Функции и приложения в Asterisk.....	402
<b>Приложение. Базовые правила работы с Ubuntu.....</b>	<b>403</b>
Помощь .....	403
Установка Ubuntu.....	403
Настройка локализованной консоли .....	404
Настройка сетевых параметров.....	405
Настройка синхронизации времени.....	407
Установка программ .....	408
Установка последних обновлений.....	408
Обновление версии сервера .....	409
Установка и удаление программ.....	409
Переконвертация пакетов.....	412
Настройка параметров прокси-сервера для команды обновлений.....	412
Установка программ из исходных кодов .....	413
Изоляция приложений .....	416
Основные правила работы в Ubuntu .....	418
Графический интерфейс .....	418
Вход и выход пользователя, завершение работы.....	420
Работа в консоли .....	420
Работа в нескольких консолях.....	420
Путь к исполняемому файлу.....	421
Исполняемые файлы.....	421
Регистрозависимость.....	421
Автозаполнение .....	421
Фоновое выполнение команд .....	422
Перенаправление потоков.....	422
Подсказка по командам.....	424

---

Ссылки .....	424
Alias .....	424
Добавление пользователей .....	425
Права суперпользователя .....	426
Кто работает на компьютере .....	427
Несколько полезных команд .....	428
Права доступа .....	429
Принципы размещения данных в Ubuntu .....	430
Текстовый редактор VI .....	431
Команды для работы с файлами и дисками .....	433
Просмотр существующих дисков .....	433
Размеры папок и файлов .....	435
Подключение ISO-образа в Ubuntu .....	436
Подключение CD-ROM .....	437
Подключение flash-карт .....	437
Команды работы с файлами и папками .....	437
Поиск файлов .....	439
Создание шифрованного диска .....	440
Работа в Ubuntu с компьютеров под управлением Windows .....	441
Подключение Windows-сетевых дисков .....	444
Выполнение команд на удаленном компьютере .....	446
Создание и удаление демонов .....	447
Выполнение заданий по расписанию .....	447
Сброс пароля администратора .....	449
<b>Предметный указатель .....</b>	<b>451</b>

# Введение

## От автора

В каждой информационной системе есть компоненты, работа которых обеспечивает стабильность всех приложений. Администратору важно правильно настроить и сопровождать функционирование базовых служб. В этой книге мы рассмотрим вопросы, связанные с установкой, настройкой и обслуживанием системы передачи данных, базовых сетевых сервисов (DHCP, DNS и др.), систем обеспечения совместной работы пользователей (электронная почта, порталы) и контроля состояния информационной системы. Все то, с чем каждодневно приходится сталкиваться администратору.

В силу ограниченности ресурсов сопровождением информационных систем в малых и средних организациях часто занимаются специалисты, вынужденные одновременно работать в нескольких структурах. Часто им просто не хватает времени, чтобы изучить функции того или иного продукта, иногда внедрение и поддержка нового функционала просто расценивается как излишняя, неоплачиваемая нагрузка. Поэтому я постарался показать, как те или иные возможности современного программного обеспечения позволяют обеспечить более комфортную работу.

Настоящая книга предназначена в помощь тем системным администраторам, которые хотят наиболее эффективно задействовать возможности современных технологий. В ней я постарался изложить практические рекомендации по администрированию информационных систем, уделяя основное внимание конкретным советам по настройке применяемых продуктов. Те, кому важнее описание технологий и принципов, реализованных в информационных системах, могут обратиться, например, к моей книге "Самоучитель системного администратора. 2-е издание", БХВ-Петербург, 2008.

Учитывая, что в состав современных информационных систем входят как Windows-, так и Linux-компьютеры, рекомендации даны для обеих ОС.

В силу ограниченности объема издания я не смог уделить здесь достаточно внимания проблемам устранения неисправностей. При этом я постарался, по возможности, указать основные источники, к которым можно обратиться за получением подробной подсказки. Много практических рекомендаций по тюнингу операционных систем на основе Windows приведено в моей книге "Windows Vista: Народные советы", БХВ-Петербург, 2008.

В информационных технологиях очень важен показатель удовлетворенности клиента. Также и автору хотелось бы получить ваши отзывы, замечания, предложения, которые могли бы улучшить эту книгу, сделать ее более полезной на практике. Их можно отправить на адрес издательства или мне по электронной почте на [kenin@hotbox.ru](mailto:kenin@hotbox.ru).

## Открытое программное обеспечение

Базовые службы, которые рассматриваются в настоящей книге, давно уже основываются на открытых стандартах и не являются собственностью какой-либо компании. Эти решения могут быть реализованы как на коммерческом программном обеспечении, так и — при той же функциональности — на бесплатных программах. Зачастую мы платим существенные суммы за проекты, которые можно реализовать совершенно бесплатно, только потому, что лица, принимающие решения, заинтересованы в продаже и покупке дорогих продуктов.

### ЗАМЕЧАНИЕ

Мы говорим не только об откатах, которые стали "притчей во языцех" всей системы поставок в информационных технологиях. Проценты, которые получают фирмы-продавцы совершенно официально от вендоров за продажу программного обеспечения, являются основой существования таких организаций. И опрометчиво думать, что представители коммерческих структур будут рубить сук, на котором сами сидят.

Конечно, существует привыкание к продукту. Если вы изучили одну программу, то переход к другой неизбежно вызовет дискомфорт. Но это временное явление. Опасения, что системы на основе Linux требуют специальной подготовки специалистов, беспочвенны, ведь хорошим администратором систем Windows тоже невозможно стать, имея только домашний опыт работы в Интернете и практику ремонта компьютеров друзей и знакомых.

Каждый программный продукт уникален. Но проанализируйте, какие операции вы *реально* выполняете с его помощью? В подавляющем большинстве случаев окажется, что все это можно сделать на бесплатном программном обеспечении. Зачем платить деньги за тот функционал, который не будет

востребован? Будем надеяться, что текущее состояние экономики заставит, наконец, считать деньги и оценивать эффективность выбора тех или иных продуктов.

Да, смена программы вызовет некоторое неудобство в начале работы. Я помню тот момент, когда мне в первый раз пришлось менять рабочий инструмент — вместо Microsoft Internet Explorer установил Firefox, поскольку более уже не мог мириться с медленной работой в Интернете из-за недостаточной мощности компьютера. Первые два дня я постоянно пересиливал себя в желании оставить все как есть, поскольку привык к какому-то сочетанию управляющих клавиш и т. п. Сейчас я открываю Internet Explorer только вынужденно, например, при обращении к Microsoft CRM, программе, которая работает только в окне своего обозревателя. А переход на OpenOffice вообще прошел незаметно: сначала я использовал OpenOffice в тех случаях, когда уставал искать нужное мне меню в ленте Microsoft Office 2007, а потом даже и не заметил, как полностью переключился на работу в бесплатном продукте, несмотря на наличие лицензии на коммерческое ПО.

Для большинства задач вполне реально найти бесплатный продукт, с помощью которого можно выполнить необходимые операции. Приведу небольшой перечень ссылок на программное обеспечение, с которым мне довелось работать (табл. 1).

**Таблица 1.** Некоторые ссылки на бесплатные программные продукты

Название программы	Ссылки	Примечания
OpenOffice	<a href="http://www.openoffice.org/">http://www.openoffice.org/</a>	<p>Пакет офисных программ, включает текстовый процессор, программы для работы с электронными таблицами, базами данных, презентациями. Форматы документов совместимы с продуктами Microsoft Office.</p> <p>Если загружать с сайта разработчика, то дополнительно необходимо устанавливать расширения для русского языка (проверка орфографии, переносы). Поэтому лучше воспользоваться специальной сборкой, полностью подготовленной для работы с русским языком с сайта компании "Инфра-Ресурс" — <a href="http://irs.ru/Produkty/OpenOffice.org">http://irs.ru/Produkty/OpenOffice.org</a></p> <p>Интерфейс русский</p>

Таблица 1 (продолжение)

Название программы	Ссылки	Примечания
Firefox	<a href="http://www.firefox.com/">http://www.firefox.com/</a>	Обозреватель Интернета. Особенность этой программы в том, что для нее созданы тысячи различных дополнений, расширяющих функциональность обозревателя: различные записные книжки, блокировщики рекламы, переводчики и т. п. Поэтому не ограничивайтесь загрузкой самой программы, а обязательно расширьте ее возможности установкой дополнений. Интерфейс русский
GIMP	<a href="http://www.gimp.org/">http://www.gimp.org/</a>	Графический редактор — в некотором смысле аналог Adobe Photoshop. Работает со слоями, содержит множество инструментов и фильтров для обработки изображений, различные кисти и т. п. Интерфейс русский
InfraRecorder	<a href="http://infrecorder.org/">http://infrecorder.org/</a>	Программа для записи, копирования CD- и DVD-дисков. Работает с аудио-, видеодисками, дисками с данными и с их образами. Интерфейс русский
FreeCommander	<a href="http://www.freecommander.com/">http://www.freecommander.com/</a>	Файловый менеджер. Для тех, кто привык работать с панелями Norton'a. Интерфейс русский
7Zip	<a href="http://www.7-zip.org/">http://www.7-zip.org/</a>	Архиватор. Может распаковать архивы форматов ARJ, CAB, CHM, CPIO, DEB, DMG, HFS, ISO, LZH, LZMA, MSI, NSIS, RAR, RPM, UDF, WIM, XAR и Z. Есть русскоязычный интерфейс



Таблица 1 (продолжение)

Название программы	Ссылки	Примечания
CCleaner	<a href="http://www.ccleaner.com/">http://www.ccleaner.com/</a>	Мощная программа для чистки реестра системы. Интерфейс англоязычный
Avast! AVG Avira PCTools Antivirus	<a href="http://www.avast.com/">http://www.avast.com/</a> <a href="http://free.avg.com/">http://free.avg.com/</a> <a href="http://www.free-av.com/">http://www.free-av.com/</a> <a href="http://www.pctools.com/free-antivirus/">http://www.pctools.com/free-antivirus/</a>	Некоторые антивирусные программы, лицензия которых предусматривает бесплатное применение в некоммерческих целях. В коммерческих целях можно использовать ClamWin ( <a href="http://www.clamwin.com/">http://www.clamwin.com/</a> ), но он не содержит антивирусного монитора в реальном режиме времени (позволяет сканировать файлы). В то же время на его основе созданы антивирусные серверы, сканирующие весь входящий трафик организации (как почтовый — см. раздел " <i>Zimbra Collaboration Suite</i> ", так и трафик Интернета (см. раздел " <i>Антивирусная проверка HTTP-трафика</i> ")
Microsoft Security Essentials	<a href="http://www.microsoft.com/security_essentials/">http://www.microsoft.com/security_essentials/</a>	Бесплатная антивирусная программа от Microsoft для защиты домашних компьютеров. Механизм сканирования и обнаружения вирусов практически не уступает лидерам. Полное сканирование системы производится в моменты неактивности. Работает в Windows XP с пакетами обновлений SP2 или SP3, Windows Vista и Windows 7 (в том числе для режима Windows XP) на 32-битовых и 64-битовых платформах. На момент подготовки книги русскоязычная версия продукта отсутствовала
ZoneAlarm	<a href="http://www.zonealarm.com/">http://www.zonealarm.com/</a>	Персональный межсетевой экран

Таблица 1 (продолжение)

Название программы	Ссылки	Примечания
COMODO Internet Security	<a href="http://www.personalfirewall.comodo.com/">http://www.personalfirewall.comodo.com/</a>	Система персональной защиты, включающая межсетевой экран и антивирусную проверку
PC Tools Firewall Plus	<a href="http://www.pctools.com/firewall/">http://www.pctools.com/firewall/</a>	Межсетевой экран для Windows Vista 32-bit, XP, 2000 и Windows Server 2003
Ad-Aware Free	<a href="http://lavasoft.element5.com/">http://lavasoft.element5.com/</a>	Программа для защиты от вредоносных кодов (SpyWare, mailware и т. д.)
PDF creator PDF converter	<a href="http://sourceforge.net/projects/pdfcreator/">http://sourceforge.net/projects/pdfcreator/</a> <a href="http://www.dopdf.com//">http://www.dopdf.com//</a>	Утилиты устанавливают в системе PDF-принтер: печать на этот принтер создает документы в формате PDF (исключается необходимость в программе Adobe Acrobat)
Foxit Reader	<a href="http://www.foxitsoftware.com/">http://www.foxitsoftware.com/</a>	Легкая альтернатива Acrobat Reader (тоже бесплатной программы)
StarDict	<a href="http://stardict.sourceforge.net/">http://stardict.sourceforge.net/</a>	Программа-переводчик
Inkscape	<a href="http://www.inkscape.org/">http://www.inkscape.org/</a>	Редактор векторной графики, сходный по возможностям с Illustrator, Freehand, CorelDraw
Фабрика форматов	<a href="http://www.formatoz.com/">http://www.formatoz.com/</a>	Программа для преобразования форматов аудио- и видео-файлов. Интерфейс русский
Cuneiform	<a href="http://www.cuneiform.ru/">http://www.cuneiform.ru/</a>	Программа оптического распознавания символов
Codendi Collabtive dotProject eGroupWare KForge OpenGoo Project.net ProjectPier Redmine Trac JotBug	<a href="http://www.codendi.com">http://www.codendi.com</a> <a href="http://collabtive.o-dyn.de">http://collabtive.o-dyn.de</a> <a href="http://www.dotproject.net">http://www.dotproject.net</a> <a href="http://www.egroupware.org">http://www.egroupware.org</a> <a href="http://www.kforgeproject.com/">http://www.kforgeproject.com/</a> <a href="http://www.opengoo.org">http://www.opengoo.org</a> <a href="http://www.project.net">http://www.project.net</a> <a href="http://www.projectpier.org">http://www.projectpier.org</a> <a href="http://www.redmine.org">http://www.redmine.org</a> <a href="http://trac.edgewall.org">http://trac.edgewall.org</a> <a href="http://www.jotbug.org">http://www.jotbug.org</a>	Программное обеспечение управления проектами, основанное на Web-интерфейсе. Поддерживает обычно управление ресурсами, контакты, систему обмена сообщениями, отслеживания событий, управления документами и т. д. Сравнительную характеристику продуктов можно уточнить на странице <a href="http://en.wikipedia.org/wiki/List_of_project_management_software">http://en.wikipedia.org/wiki/List_of_project_management_software</a>

Таблица 1 (окончание)

Название программы	Ссылки	Примечания
SugarCRM	<a href="http://www.sugarcrm.com/crm/community/sugarcrm-community.html">http://www.sugarcrm.com/crm/community/sugarcrm-community.html</a>	Бесплатная версия коммерческого пакета управления отношениями с клиентами (CRM)
Alfresco	<a href="http://www.alfresco.com/">http://www.alfresco.com/</a>	Система управления документами (Enterprise Content Management)

Отметим еще страницу <http://www.manageengine.com/free-software-download.html>, где представлен список утилит для администрирования системы, которые можно бесплатно загрузить и использовать в своей работе. Многие некоммерческие продукты можно загрузить с сайта Snapfiles (<http://www.snapfiles.com/>), специализирующегося на бесплатных или условно-бесплатных продуктах.

Это далеко не полный список доступных программ, но уже и он дает представление, насколько широко распространено программное обеспечение, с которым вы можете работать на законных основаниях.

Не следует также забывать, что многие коммерческие продукты имеют специальные выпуски, например, у всех коммерческих серверов баз данных есть "младшие" бесплатные "братья". Так, у Microsoft SQL Server 2008 существует бесплатная версия Microsoft SQL Server Express Edition. Эти редакции программ при определенных ограничениях функциональности (например, в случае Microsoft SQL Server Express Edition максимальный размер базы данных ограничен величиной 2–4 Гбайт в зависимости от версии, графическую оболочку управления нужно загружать отдельно и т. п.) позволяют использовать продукт бесплатно. Как правило, о наличии таких редакций продавцы ПО и разработчики проектов часто "забывают".

## Открытые стандарты и проприетарные решения

Любая реклама назойливо предлагает внедрить "самое-самое" решение какой-либо фирмы. Конечно, применяя уникальную технологию, вы можете получить более высокую производительность, чем в типовом решении, но при этом оказываетесь привязанными к конкретному вендору. И не всегда такой выбор окажется оправданным в перспективе.

Поэтому я бы советовал ориентироваться на решения, описанные в открытых стандартах. И только в случае невозможности такого выбора — применять проприетарные технологии.

Системные администраторы могут оказать серьезное влияние на выбор продукта через выдвижение технических требований. И если в меньшей степени заботиться "о выплате ипотеки", то даже конкурс можно организовать и провести так, чтобы он привел к покупке оптимального варианта.

## Windows и Linux

В реальности очень сложно предположить, какие программные продукты будут востребованы. Зависит это от множества факторов, как объективных (качество продукта в той или иной версии, стоимость владения и т. п.), так и субъективных (привычки, опасения выбора неизвестного продукта...). Однако можно уверенно сказать, что большинство информационных систем сегодня включают в себя как продукты на основе Windows, так и Linux-системы. Администратору важно уметь работать со всеми этими линейками. Именно поэтому в данной книге параллельно описаны реализации решений как на серверах Windows, так и на сервере Ubuntu — представителе многочисленной линейки Linux-операционных систем.

Почему для описания в книге выбрана именно операционная система Ubuntu? Это не жесткая рекомендация. Просто эта операционная система бесплатна, поддерживается крупнейшими вендорами оборудования, а для серверных редакций гарантируется длительная поддержка (пять лет с момента выпуска). Причем для обеспечения этой поддержки созданы специализированные фонды, в которые уже перечислены существенные финансовые средства.

### **СОВЕТ**

При выборе версий серверов Ubuntu обращайтесь внимание на параметр поддержки: наличие в обозначении символов LTS (Long Term Support) свидетельствует о таком длительном сроке.

Для тех, кто не знаком с основами Linux, в *приложении* даны краткие рекомендации по установке, обслуживанию и работе в операционной системе Ubuntu.

В своей организации вы вольны устанавливать любые версии программного обеспечения. Естественно, что в этом случае синтаксис некоторых команд будет отличаться от тех примеров, которые описаны в настоящей книге и базируются на реальных настройках серверов, выполненных автором в различных эксплуатируемых системах.

# Глава 1



## Сетевая инфраструктура

Как театр начинается с вешалки, так и любая информационная система — с ее инфраструктуры. Недостаточное внимание к качеству сети передачи данных может привести к постоянным проблемам при эксплуатации информационной системы.

### Строение сети передачи данных

Практически все сети предприятий сегодня базируются на технологии Ethernet и протоколе TCP/IP. Наличие других протоколов, как правило, наследовано исторически и обусловлено эксплуатируемым оборудованием.

Рассмотрим, что необходимо знать системному администратору при работе и модернизации таких сетей.

### Размеры сегментов сети

Длина медного кабеля от одного элемента активного оборудования до другого, например, от компьютера до коммутатора, в сети Ethernet не должна превышать 100 м. Обычно стандартами предусмотрена максимальная длина самого кабеля 90 м, а 10 м отводится на соединительные кабели.

#### **ЗАМЕЧАНИЕ**

На практике длина патч-кордов обычно составляет 1 м и более. Обратите внимание, что не имеет смысла применять самодельные короткие патч-корды, например, для подключения сервера к патч-панели, если оба этих элемента расположены рядом ("фирменные" кабели не могут быть короче ~ 60 см). При малой длине кабеля увеличивается уровень помех, возникающих при отражении высокочастотных сигналов от точки соединения кабеля и розетки. Это может привести к увеличению числа ошибок в линии.

В реальных сетях еще сохранились концентраторы (*хабы*). Для локальной 10-мегабитной сети, построенной на *концентраторах*, существует правило "5/4" — между любыми двумя сетевыми устройствами должно быть не более пяти сегментов сети с четырьмя концентраторами. При этом размер сети, построенной на витой паре, ограничен величиной 500 м. Ограничение на длину обусловлено самой природой Ethernet, принципами, на которых строится такая сеть, и не зависит от совершенствования элементной базы.

Хотя в 100-мегабитной сети обычно используются только коммутаторы, на практике в ряде организаций эксплуатируются и концентраторы. Стандартом предусмотрено в этом случае наличие не более *двух* концентраторов с расстоянием между ними не более 5 м.

При необходимости соединения устройств, отстоящих друг от друга на расстоянии свыше 100 м, целесообразны волоконно-оптические линии связи. На небольших расстояниях (порядка 100–300 м) применяются *многомодовые* оптические кабели. Длины сегментов определяются параметрами оптических приемников и передатчиков. (Эти значения отличаются от вендора к вендору и не всегда соответствуют параметрам стандартов.) Стоимость прокладки и эксплуатации такой линии практически соизмерима со стоимостью линии на витой паре. Для длинных соединений предназначен *одномодовый* оптический кабель. Соответствующее оборудование для одномодового кабеля (приемники и передатчики оптического сигнала) в несколько раз дороже, чем модели для многомодовой технологии.

Поскольку на практике эксплуатируются различные технологии, при проектировании расширения сети следует обращать внимание на совместимость использованных решений. Так, например, необходимо учитывать типы оптических разъемов, которые могут отличаться на оборудовании различных вендоров. Нужно принимать во внимание тип оптического кабеля (выпускаются более чем по пяти стандартам), длину волны и т. п.

## Выбор типа коммутаторов

В небольших сетях (и в больших на уровне доступа) традиционно задействуют коммутаторы второго уровня по модели OSI. Коммутаторов данного класса обычно достаточно для организации сети с не очень большим числом компьютеров — в одну-две сотни. Точно назвать границу, когда необходимо уже применять коммутаторы третьего уровня, сложно. Это зависит от специфики организации (имеющихся сетевых сервисов, реальной загрузки сети, наличия трафика реального времени — IP-телефонии и видеоконференций и т. д.). Коммутаторы третьего уровня нужны для того, чтобы разделить сеть на несколько независимых друг от друга сегментов. При этом передача информа-

ции из одного сегмента в другой осуществляется путем маршрутизации на коммутаторе третьего уровня.

### **ПРИМЕЧАНИЕ**

Для обеспечения надежности необходимо строить сеть с ядром на двух коммутаторах третьего уровня, работающих совместно (как отказоустойчивый стек и т. п.).

Коммутаторы лучше приобретать управляемые. Это обеспечит гибкость в настройке сети. Если в сети предполагается использование сервисов реального времени, то коммутаторы должны поддерживать режимы управления качеством передачи (QoS) и, по возможности, реализовывать режим гарантированного предоставления полосы пропускания.

## **Топология сети передачи данных**

На практике компьютерную сеть пытаются сначала строить по какому-нибудь проекту, а потом, по мере развития организации, подключают новые коммутаторы и структура принимает достаточно хаотичный вид. На рис. 1.1 показан пример топологии реальной сети, построенный бесплатной программой 3Com Network Supervisor. Если администратор не контролирует развитие сети, часто формируются каскады из четырех-пяти последовательно включенных коммутаторов, что неизбежно ухудшает качество системы передачи данных.

Администратору нельзя выпускать развитие сетей передачи данных из-под своего контроля: в любой момент он должен знать, как соединены между собой коммутаторы, и быть уверенным, что ни к одному порту не подключено неизвестное ему оборудование.

При построении сети внутри здания обычно придерживаются иерархии связей "здание – этаж – рабочее место": на этажах устанавливают коммутаторы уровня доступа, к которым подключают рабочие места пользователей, после чего эти коммутаторы соединяют каналами связи с коммутатором (-ами) на каком-либо этаже, который выполняет в этом случае роль ядра сети.

Традиционной проблемой большинства организаций является документирование своей кабельной подсистемы. Специализированные программные продукты, позволяющие поддерживать схемы сети и оперативно учитывать вносимые в нее изменения, стоят весьма дорого, а исходная документация быстро становится неактуальной после нескольких перемещений сотрудников и прокладки дополнительных каналов связи.

Существует много программ, которые позволяют автоматически воспроизвести структуру сети. Окно одной из таких программ — 3Com Network Supervisor — представлено на рис. 1.1. С помощью данных, собираемых про-

граммой, легко находить точки подключения компьютеров к коммутаторам, обнаруживать те или иные неисправности конкретной конфигурации.

### СОВЕТ

Найти и загрузить подобную программу из Интернета достаточно легко, если выполнить поиск по ключевым словам *network monitoring tool*.

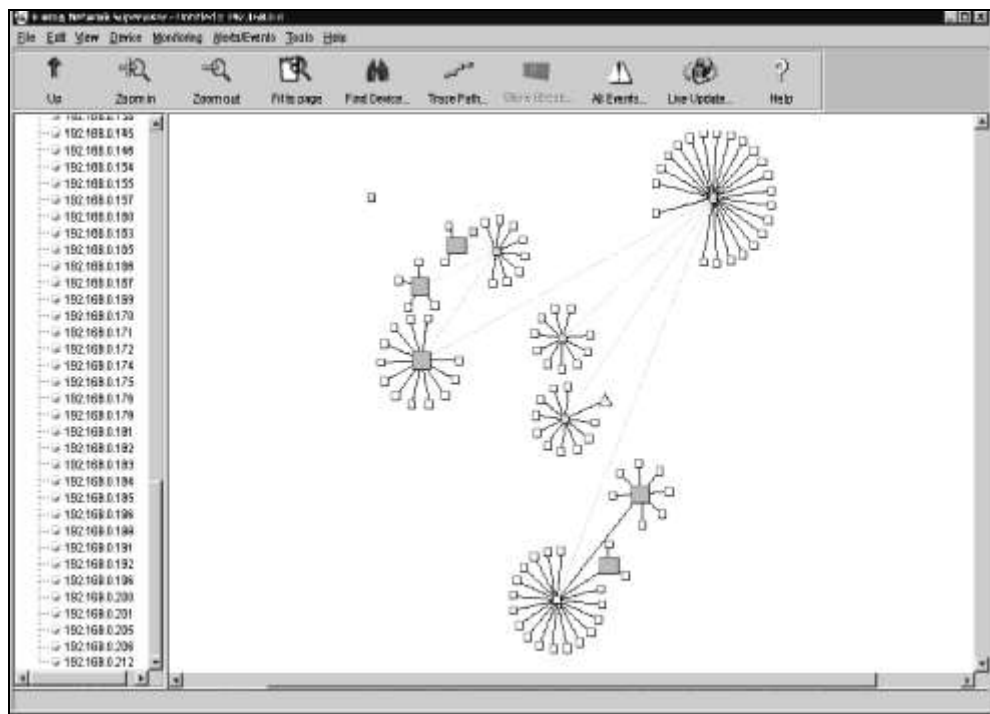


Рис. 1.1. Пример топологии реальной сети, построенной программой 3Com Network Supervisor

Естественно, что получаемая диаграмма тем точнее, чем более интеллектуальные активные устройства используются в сети. При эксплуатации неуправляемых устройств возможностей у администратора существенно меньше.

## Ищем точку подключения компьютера

Точку подключения компьютера к порту коммутатора можно определить только в пределах текущего сегмента сети (одной VLAN). За пределами данного сегмента вам будет доступна информация только о том, в какой сети (за каким маршрутизатором) находится этот компьютер.



На практике в небольших организациях часто, несмотря на все рекомендации, отсутствует актуальная схема сети, поэтому поиск точки подключения устройства требует много усилий. Чтобы найти, к какому коммутатору подключен компьютер, следует искать устройство, в таблице MAC-адресов которого зарегистрирована сетевая плата соответствующего компьютера. Такая информация доступна только с управляемых коммутаторов.

### ЗАМЕЧАНИЕ

Существуют программы, позволяющие найти маршрут подключения искомого устройства через все коммутаторы сети. Но они эксплуатируются преимущественно в крупных организациях с разветвленной сетью.

Последовательность действий такова. Сначала определите MAC-адрес устройства, точку подключения которого вы хотите найти. Это значение становится известным для локальной системы после того, как с ним происходили какие-либо сетевые операции. Быстрее всего выполнить команду `ping` на IP-адрес компьютера. После получения ответа посмотрите таблицу arp-кэша локальной системы, в ней должна содержаться запись об удаленном MAC-адресе (листинг 1.1).

#### Листинг 1.1

```
>arp -a
Интерфейс: 192.168.29.100 --- 0x4
    Адрес IP                Физический адрес        Тип
192.168.29.1              00-1e-58-81-a0-89      динамический
```

MAC-адрес устройства отображен в столбце `Физический адрес`.

Точно такие же команды следует выполнить и на компьютерах Ubuntu, только вывод на экран результатов будет представлен немного по-иному. Хотя лучше вызвать команду `arp` без параметров (листинг 1.2).

#### Листинг 1.2

```
# arp
Address                HWtype  HWaddress          Flags Mask          Iface
192.168.32.120        ether   00:C0:9F:3F:D8:13  C                   eth0
192.168.177.85        ether   00:0D:28:F9:5D:80  C                   eth1
```

В этом листинге MAC-адрес устройства показан в столбце `HWaddress`.

После того как вы узнали MAC-адрес устройства, нужно найти его в таблице MAC-адресов на коммутаторе. Для этого необходимо подключиться к коммутатору одной из программ управления и выполнить поиск по этому значению (рис. 1.2).

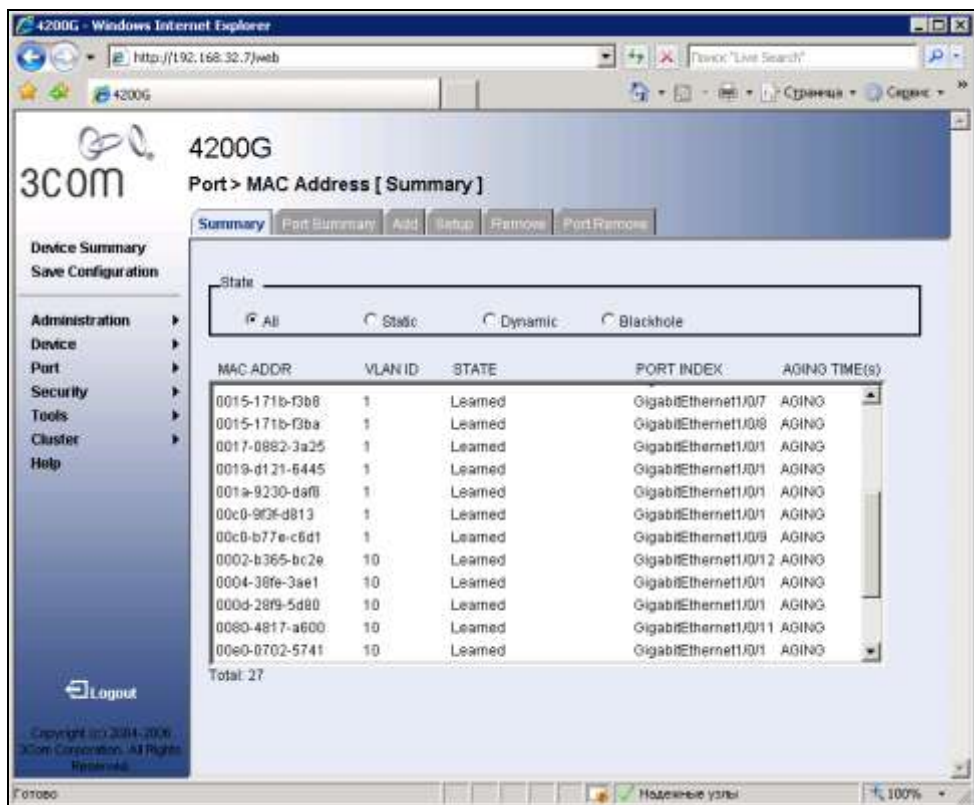


Рис. 1.2. Окно списка найденных на порту коммутатора MAC-адресов систем

На рис. 1.2 представлен графический интерфейс управления коммутатором 3Com4200G с отображением таблицы зарегистрированных MAC-адресов. Видно, что на некоторых портах имеются записи по нескольким MAC-адресам (например, на первом гигабитном порту). Это говорит о том, что данный порт является магистральным: через него коммутатор подключен к другому коммутатору и устройство нужно искать на удаленной системе.

Если на том порту коммутатора, на котором вы найдете зарегистрированным искомым MAC-адрес, есть еще MAC-адреса, значит, к данному порту подключен другой коммутатор. В этом случае нужно будет подключиться к сле-

дующему коммутатору и так по цепочке найти устройство, к которому подключена искомая система.

## Контроль подключения к СКС

Администратор обычно не контролирует порты сети передачи данных постоянно. А если к вашей сети злоумышленник сможет подключить свой компьютер, то это существенно облегчит ему последующие операции по доступу к коммерческой информации организации.

Существует два метода контроля подключаемых устройств. Первый, который поддерживается всеми управляемыми коммутаторами, заключается в контроле MAC-адреса устройства на данном порту. После подключения к порту любого оборудования, коммутатор запоминает его MAC-адрес, и каждая последующая попытка другого компьютера (точнее, устройства с другим MAC-адресом) работать через этот порт приведет к блокировке порта. Эта функциональность имеет различные названия среди вендоров активного оборудования, чтобы ее задействовать, достаточно активировать соответствующую функцию для порта.

Недостатки такого решения состоят, во-первых, в том, что сегодня существует много программных способов смены MAC-адреса компьютера, например, достаточно указать значение соответствующей опции (параметра *Locally Administered Address*) в настройках сетевого адаптера в Windows (рис. 1.3).

Во-вторых, блокировка порта резко увеличивает нагрузку на администраторов, поскольку предполагает необходимость ручных операций для возобновления работы в случае замены оборудования и в других штатных ситуациях.

В настоящее время для контроля доступа к локальной сети наиболее распространены решения на основе протокола 802.1x. Упрощенно схему проверки оборудования с использованием данного протокола можно представить следующим образом (рис. 1.4):

- При подключении устройства порт коммутатора не пропускает никаких данных в локальную сеть, кроме специальных пакетов аутентификации на заданный в его настройках сервер RADIUS.
- Сервер Radius, получив от устройства необходимые аутентификационные данные, проверяет соответствие их неким параметрам. Обычно используются сертификаты безопасности, выданные контроллерами домена. В этом случае, информация проверяется во взаимодействии с сервером сертификатов и сервером службы каталогов.
- В зависимости от результатов проверки сервер RADIUS дает коммутатору разрешение на открытие порта.

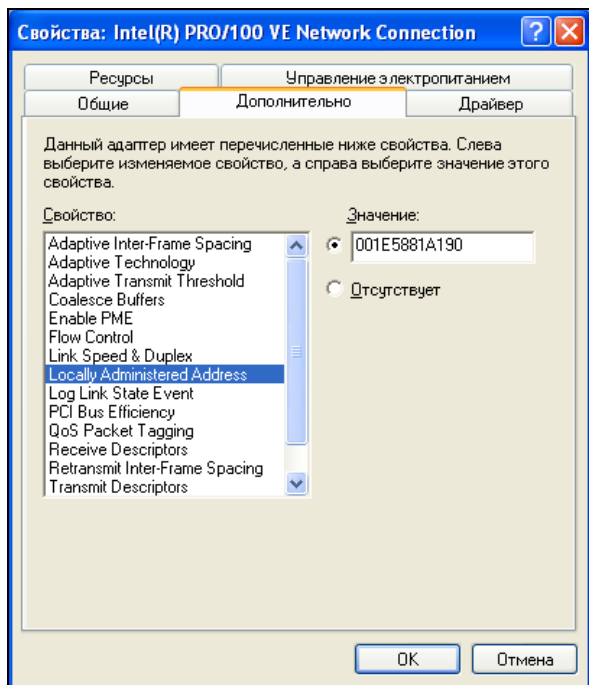


Рис. 1.3. Программная смена MAC-адреса компьютера

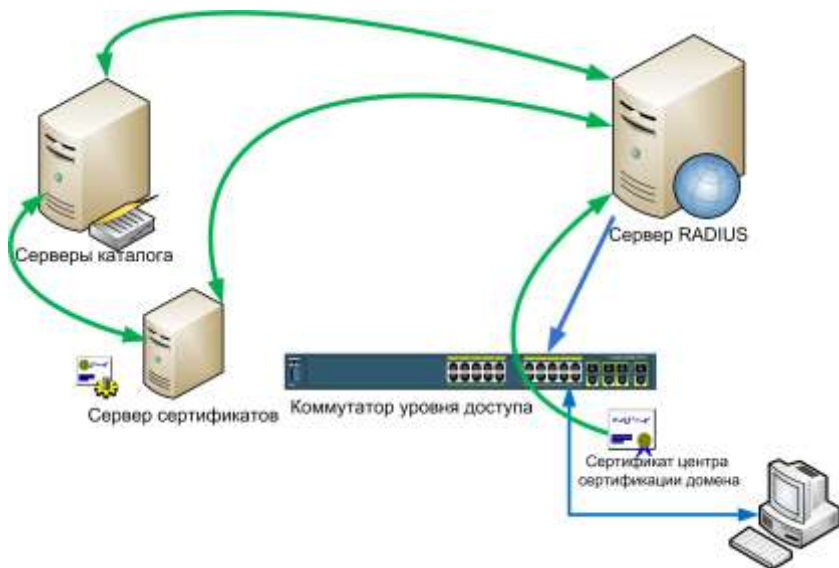


Рис. 1.4. Принципиальная схема взаимодействия компьютера, коммутатора и серверов системы при использовании протокола 802.1x

□ Коммутатор, получив разрешение, открывает доступ устройству в локальную сеть. Далее, в зависимости от настроек коммутатора, такая проверка может осуществляться периодически через некоторое время, порт может открываться для любых MAC-адресов и т. д.

Сервер RADIUS может не только давать разрешение на открытие порта, но и сообщать коммутатору некоторые данные настройки, например, номер виртуальной сети, в которую должен быть помещен порт этого устройства. Данную функциональность поддерживают не все коммутаторы.

Самая строгая проверка компьютера будет осуществляться по протоколу 802.1x с учетом сертификатов, выданных удостоверяющим центром (например, внутренним центром сертификации). Опишем пример настройки коммутатора для такого случая.

## Предварительные настройки для использования протокола 802.1x

Контроль подключения по протоколу 802.1x с использованием сертификатов требует развернутой системы PKI в организации: установленного центра сертификации, наличие процедур выдачи/отзыва сертификатов и т. п. Обычно это реализуется только в достаточно крупных фирмах, тем более что, например, идентификация сервера RADIUS предполагает получение им самим сертификата, который может быть выдан только сервером сертификации на основе Windows Server Enterprise Edition.

Поэтому в малых организациях можно ограничиться аутентификацией по MD5-откликам. Процедура настройки практически не отличается от описанной далее, за исключением того, что вместо сертификатов нужно выбрать опцию **MD5-отклик** в мастере настройки политик подключения.

**Настройка компьютера.** Аутентификация на базе протокола 802.1x осуществляется службой *Беспроводная настройка*. По умолчанию ее запуск на рабочих станциях установлен в режим *ручной*. Смените ее на автоматический режим. Далее, с помощью сертификатов можно аутентифицировать как *компьютер*, так и *пользователя*. По умолчанию операционная система Windows аутентифицирует пользователя. То есть до локального входа пользователя на компьютер, работа в сети будет невозможна. Если вы хотите аутентифицировать компьютер, то необходимо в его реестр с помощью команды `regedit` добавить параметр `HKLM\Software\Microsoft\EAPOL\Parameters\General\Global\AuthMode` со значением 2 и типом `DWORD`.

### ЗАМЕЧАНИЕ

Эти настройки можно определить централизованно с использованием групповой политики домена.

**Настройка домена Windows.** Учетные записи, которые будут аутентифицироваться по протоколу 802.1x, должны иметь разрешение на входящий звонок в свойствах учетной записи. Обратите внимание, что это касается и учетных записей *компьютеров*, если вы предполагаете авторизовать их сертификаты. Если вы планируете назначать компьютеры в отдельные VLAN в зависимости от членства в группах безопасности, то в этом случае необходимо создать столько групп безопасности, сколько различных настроек должно передаваться на коммутатор, и включить в эти группы соответствующие учетные записи. Для упрощения администрирования желательно создать групповую политику, предполагающую автоматическую выдачу сертификатов для компьютеров, входящих в домен. Это упростит операции ручного получения сертификатов для учетных записей компьютеров.

**Настройка сервера RADIUS.** Серверы RADIUS в операционных системах Microsoft носят название *Служба проверки подлинности в Интернете* (входит в состав *Сетевые службы* при выборе опции установки компонентов Windows). Для единообразия в этой книге мы будем называть эту службу как сервер RADIUS. Установите RADIUS-сервер на какой-либо системе Windows и зарегистрируйте его в службе каталогов (операция входит в меню свойств сервера IAS). Проверьте, что компьютер с сервером RADIUS включен в состав группы безопасности RAS and IAS Servers. Установите на сервер сертификат авторизации, предназначенный для серверов RAS и IAS (при ручном запросе сертификата необходимо выбрать соответствующий шаблон в мастере операций).

### **ЗАМЕЧАНИЕ**

В Windows 2008 сервер RADIUS включен в состав службы контроля доступа к сети (Network Access Protection, NAP). Для его установки достаточно добавить роль *Службы политики сети и доступа* в **Диспетчере сервера**. Сама настройка протокола 802.1x для доступа в локальную сеть принципиально не отличается от описанного далее примера для случая Windows 2003 Server.

Добавьте в качестве клиентов сервера RADIUS каждый коммутатор, на котором будет осуществляться авторизация на основе протокола 802.1x. При этой операции необходимо указать адрес коммутатора и пароль, который потребуется при связи с ним. Желательно указывать достаточно длинный пароль, не менее 23 символов, как рекомендуют разработчики. Для ключей целесообразно задать различные значения для каждого коммутатора.

## **Настройка политики доступа на основе протокола 802.1x**

После предварительных настроек можно приступить непосредственно к созданию правил доступа в локальную сеть на основе протокола 802.1x. Эти настройки носят названия *политик RADIUS-сервера*.