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

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 30.10.09.
Формат 70×100 1/16. 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

ISBN 978-5-9775-0435-5

Оглавление

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**.

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	**http://www.openoffice.org/**	Пакет офисных программ, включает текстовый процессор, программы для работы с электронными таблицами, базами данных, презентациями. Форматы документов совместимы с продуктами Microsoft Office. 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" — **http://i-rs.ru/Produkty/OpenOffice.org** Интерфейс русский

Таблица 1 *(продолжение)*

Название программы	Ссылки	Примечания
Firefox	**http://www.firefox.com/**	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	**http://www.gimp.org/**	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	**http://infrarecorder.org/**	Программа для записи, копирования CD- и DVD-дисков. Работает с аудио-, видеодисками, дисками с данными и с их образами. Интерфейс русский
FreeCommander	**http://www.freecommander.com/**	Файловый менеджер. Для тех, кто привык работать с панелями Norton'a. Интерфейс русский
7Zip	**http://www.7-zip.org/**	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	**http://www.ccleaner.com/**	Мощная программа для чистки реестра системы. Интерфейс англоязычный
Avast! AVG Avira PCTools Antivirus	**http://www.avast.com/** **http://free.avg.com/** **http://www.free-av.com/** **http://www.pctools.com/free-antivirus/**	Некоторые антивирусные программы, лицензия которых предусматривает бесплатное применение в некоммерческих целях. В коммерческих целях можно использовать ClamWin (**http://www.clamwin.com/**), 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 "*Zimbra Collaboration Suite*", так и трафик Интернета (см. раздел *"Антивирусная проверка HTTP-трафика"*)
Microsoft Security Essentials	**http://www.microsoft.com/security_essentials/**	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	**http://www.zonealarm.com/**	Персональный межсетевой экран

Таблица 1 *(продолжение)*

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

Таблица 1 *(окончание)*

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

Отметим еще страницу **http://www.manageengine.com/free-softwares-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 обращайте 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 расстояние 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, наличии 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*.

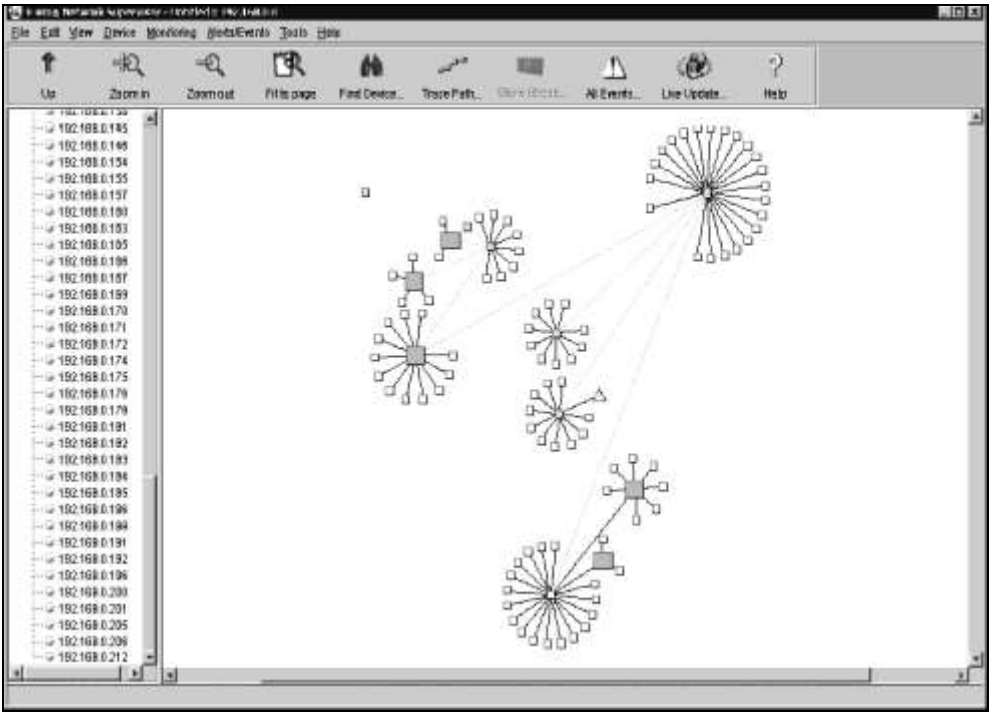

Рис. 1.1. Пример топологии реальной сети, построенной программой 3Com Network Supervisor

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).

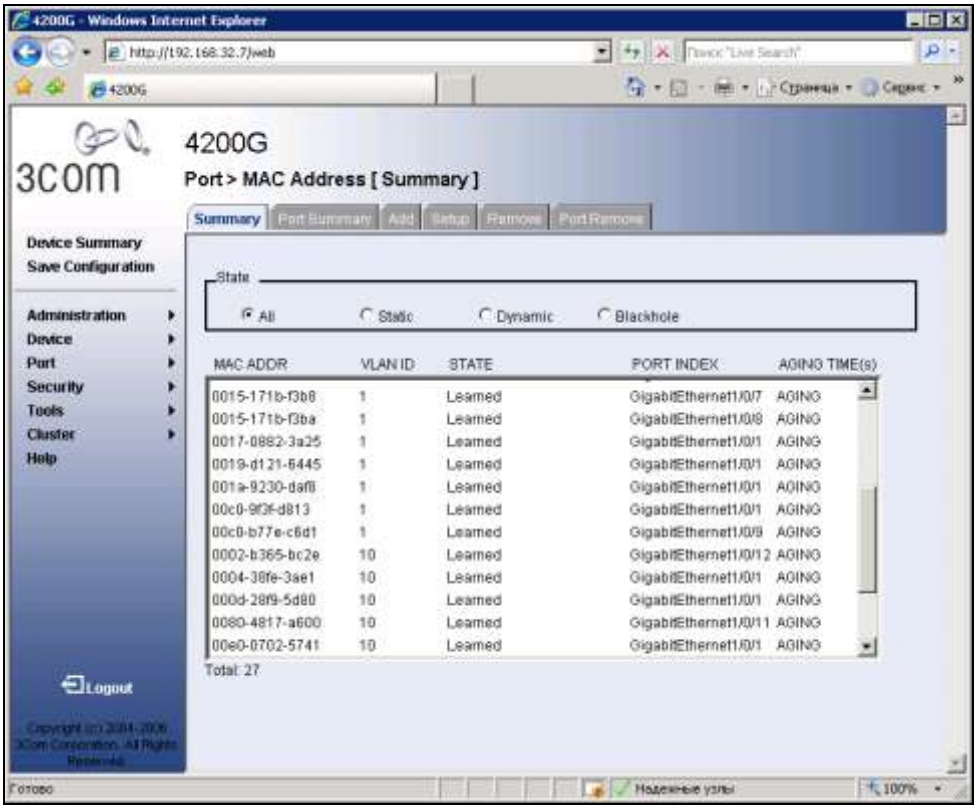

Рис. 1.2. Окно списка найденных на порту коммутатора MAC-адресов систем

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 искомый 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 802.1*x*. 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.

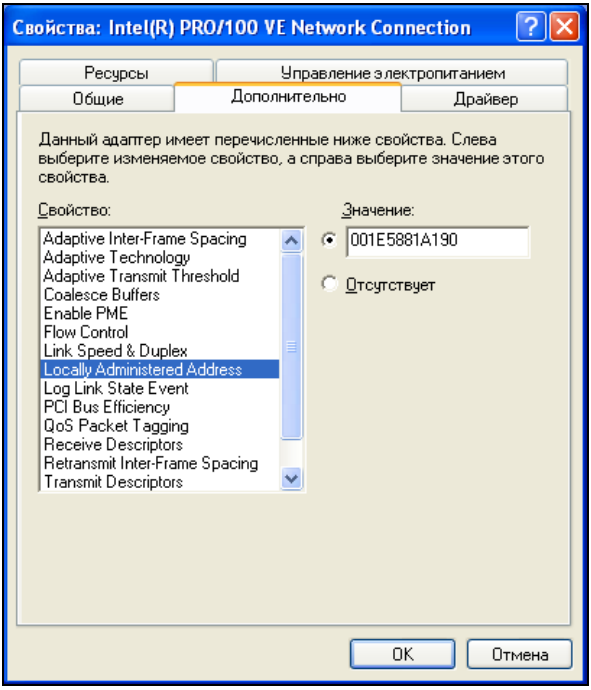

Рис. 1.3. Программная смена MAC-адреса компьютера

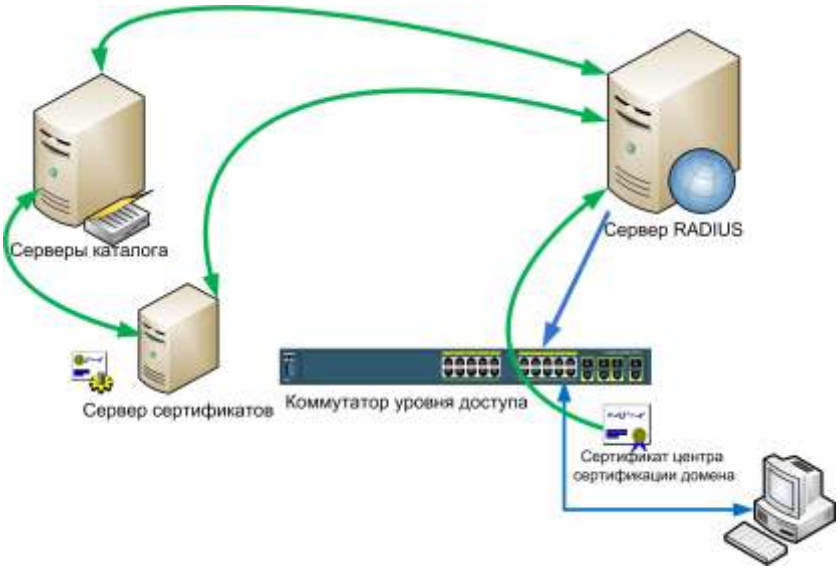

Рис. 1.4. Принципиальная схема взаимодействия компьютера, коммутатора и серверов системы при использовании протокола 802.1*x*

- 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 802.1*x* с учетом сертификатов, выданных удостоверяющим центром (например, внутренним центром сертификации). Опишем пример настройки коммутатора для такого случая.

Предварительные настройки для использования протокола 802.1*x*

Контроль подключения по протоколу 802.1.*x* 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 802.1*x* 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 802.1*x*, 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 устранит 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 802.1*x* 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 802.1*x*. 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 802.1*x*

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